İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
ÖZEL HUKUK DOKTORA PROGRAMI

İŞ HUKUKUNDA DİJİTAL İZLEME

Ferman KAYA
116812006

Prof. Dr. Kübra DOĞAN YENİSEY

İSTANBUL
2024

İş Hukukunda Dijital İzleme

Digital Monitoring in Labour Law

Ferman KAYA

116812006

Tez Danışmanı : **Prof. Dr. Kübra DOĞAN YENİSEY**
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Prof. Dr. Gülsevil ALPAGUT**
İstanbul Üniversitesi
Prof. Dr. Mahmut KABAKCI
İstanbul Teknik Üniversitesi
Dr. Öğr. Üyesi Seda ERGÜNEŞ EMRAĞ
İstanbul Bilgi Üniversitesi
Dr. Öğr. Üyesi Hande HEPER
Kadir Has Üniversitesi

Tezin Onaylandığı Tarih : 15.02.2024
Toplam Sayfa Sayısı : 486

Anahtar Kelimeler (Türkçe)
1) İşyerinde Gözetleme
2) Dijital İzlemenin Sınırları
3) İşçinin Kişisel Verileri
4) İşverenin Dijital İzleme Hakkı
5) İş İlişkisinde Dijital İzleme

Anahtar Kelimeler (İngilizce)
1) Surveillance in the Workplace
2) Limits of Digital Monitoring
3) Employee's Personal Data
4) Employer's Digital Monitoring Right
5) Digital Monitoring in Labour Relationship

ÖNSÖZ

Bir tezin hazırlık aşaması, yazılması ve tamamlanması birçok kişinin değerli emeğini ve fedakarlığını içerir. Hiç şüphesiz bu emeğin en büyük payı beni "dijital izleme" konusunda yazmaya teşvik eden, bütün yoğunluğuna rağmen başlıklarda berraklaşmam için çabalayan ve pes ettiğim anlarda yazmaya döndüren değerli hocam Prof. Dr. Kübra Doğan Yenisey'e aittir. Sarf ettiği emek, kattığı akademik bakış açısı ve daha da önemlisi nezaketi ve erdemli yaklaşımları için kendisine teşekkürlerimi bu vesileyle de iletmeyi bir borç biliyorum. Yazım sürecinde zaman ayıran her aradığımda ve görüştüğümde teşvik edici ve yönlendirici kısa sohbetleriyle beni cesaretlendiren tez jürimde bulunan değerli hocam Prof. Dr. Gülsevil Alpagut'a; yine toplantılarda ve sunumlarda zaman ayırıp dinleyen, yorum yapan tez jürimde bulunan değerli hocam Dr. Öğr. Üyesi Seda Ergüneş Emrağ'a; zaman ayırıp, tezi değerlendiren ve önerilerde bulunan, tez jürimde yer alan değerli hocalarım Prof. Dr. Mahmut Kabakcı'ya ve Dr. Öğr. Üyesi Hande Heper'e teşekkürlerimi sunuyorum.

İş ve Sosyal Güvenlik Hukuku Anabilim Dalı asistanları Yeliz Yücel'e ve Neslişah Sakar'a ayırdıkları zaman ve katkıları için çok teşekkür ediyorum. Yine bu vesileyle belirmeliyim ki, idari tüm sorularımıza güler yüzüyle cevap verip, çözüm üretmeye çalışan fakülte idari asistanı Melda Otara'ya ve yaşamım boyunca bilgilenmeme katkı sağlayan tüm öğretmenlerime teşekkür ediyorum.

Son olarak, uzunca bir sürece yayılan tez yazım aşamasında zamanımı esirgediğim, kimi zaman stresimi ve yokluğumu yaşamak zorunda kalan sevgili çocuklarıma ve eşime destekleri ve anlayışları için teşekkür ediyorum. Sevgili anneme yaşam yolculuğunda kattığı her şey için çok teşekkür ediyorum.

İstanbul, 2024

Ferman KAYA

İÇİNDEKİLER

ÖNSÖZ ..... **iii**

İÇİNDEKİLER ..... **iv**

KISALTMALAR ..... **xiv**

ÖZET ..... **xvii**

ABSTRACT ..... **xix**

GİRİŞ **1**

I. Konunun Önemi **1**

II. Konunun Sınırlandırılması **5**

III. Konunun Sunulması **7**

BİRİNCİ BÖLÜM

DİJİTAL İZLEMENİN İŞYERİNDE KULLANILMASI VE VERİ KORUMA

§ 1. GÖZETLEMEDEN DİJİTAL İZLEMEYE İŞÇİNİN İZLENMESİ **9**

I. İş İlişkisinde Gözetleme, Gözetim ve İzleme Kavramları **9**

1. Gözetleme **10**

2. Gözetim **12**

3. İzleme **13**

4. Kavramların Kapsamları ve Dijital İzlemenin Tanımlanması **15**

II. Gözetlemenin İşyerinde Kullanılma Seyri ve İş İlişkisindeki Etkileri **18**

1. Gözetlemenin Tarihsel Gelişimi **18**

2. İşyerlerinde Gözetlemenin Araçsallaşması: Bilimsel Yönetim İlkeleri ve Ford Sosyoloji Departmanı **20**

3. Gözetlemeden Dijital İzlemeye İş İlişkisinde Denetimin Dönüşümü 23

a) İşverenin Denetim Aracı Olarak İzleme 23

b) Teknolojinin Veri İşleme Biçimini Değiştirmesi: Özel Hayatın Korunmasının Taleplere Konu Edilmesi 28

III. Yeni Çalışma Türlerinin Denetim Aracı Olarak Dijital İzleme 32

1. Gözetlemede Yeni Bir Eşik: Dijital İzleme 33

2. Yeni Çalışma Türlerinin Dijital İzlemeyi Tetiklemesi 36

§ 2. ÖZEL HAYAT VE KİŞİSEL VERİLERİN KORUNMASI 40

I. İş İlişkisinde Mahremiyet ve Özel Hayatın Gizliliğinin Korunması 40

1. Mahremiyet 41

2. Özel Hayatın Gizliliğinin Korunması 44

a) Özel Hayatın Gizliliğinin Hukuken Korunması ve Önemi 44

b) Özel Hayat Tanımı ve Kapsamı 51

3. Özel Hayat Kapsamında Bireyin Korunan Yaşam Alanları 57

a) Kamusal Alan – Özel Hayat Alanı Ayrımının Önemi 57

b) Yalnız Kalma Hakkı Tanımı ve Yeterliliği 59

c) Üç Alan Teorisi 61

aa) Kamuya Açık Ortak Hayat Alanı 61

bb) Özel Hayat Alanı 62

cc) Gizli Hayat Alanı..... 63

II. Veri Kavramı ve Kişisel Verilerin Korunması Hakkının Doğuşu..... 64

1. Veri Kavramı ve Verinin Artan Önemi 65

2. Kişisel Verilerin Korunması Hakkının Doğuşu 68

III. Kişisel Verilerinin Korunması 73

1. Özel Hayat ve Kişisel Verilerin Korunması İlişkisi 74

2. Bir İnsan Hakkı Olarak İşçinin Kişisel Verilerinin Korunması 78

3. İş Sözleşmesinin Ortaya Çıkardığı İlişkinin İşçinin Kişisel Verilerine Etkisi 84

§ 3. DİJİTAL İZLEME UYGULAMALARINDA TARAF MENFAATLERİ 87

I. Dijital İzleme: İşveren Menfaatleri Açısından 87

1. İş Görme Borcunun İfasını Denetleme ve İşyeri Verimliliğini Artırma 87

a) İşçinin Denetlenmesi 88

b) Verimliliği Artırma 90

2. İşverenin İdareye Karşı Yükümlülükleri ve Yasal Zorunluluklar..... 92

3. Güvenlik ve İşyerinde Mülkiyeti Korumak 95

4. İşverenin Diğer Menfaatleri 96

II. Dijital İzlemede İşçinin Tehlikeye Atılan Menfaatleri 97

§ 4. ULUSLARARASI METİNLERDE DİJİTAL İZLEME VE SINIRLARI 103

I. Birleşmiş Milletler Düzenlemeleri 103

II. ILO'nun İşçilerin Verilerini Korumaya İlişkin Çalışmaları ve ILO Uygulama Kodu 106

III. OECD Rehberleri ve Kişisel Verilerin Korunması 110

IV. Avrupa Konseyi'nin Dijital İzlemeye Konu Kişi Haklarına İlişkin Hukuki Metinleri 113

1. Avrupa İnsan Hakları Sözleşmesi'nin İlgili Düzenlemeleri 113

2. Kişisel Verilerin Korunmasına İlişkin 108 Sayılı Sözleşme ve 181 sayılı Ek Protokol 118

V. Avrupa Birliği Düzenlemelerinde Dijital İzleme ve Verilerin Korunması 121

1. Avrupa Birliği Temel Haklar Şartı 121

2. 95/46/ Sayılı Kişisel Verilerin Korunmasına İlişkin Direktif 124

3. 2002/58/ Sayılı E-Gizlilik Direktifi ve E-Gizlilik Tüzüğü Çalışmaları 126

4. 2016/679 Sayılı Genel Veri Koruma Tüzüğü 129

a) Genel Veri Koruma Tüzüğü'nün Hazırlanma Sebepleri 129

b) Genel Veri Koruma Tüzüğü'nün İş İlişkisine Etkisi 133

İKİNCİ BÖLÜM

DİJİTAL İZLEMENİN HUKUKİ DAYANAKLARI VE SINIRLARI

§ 5. DİJİTAL İZLEMENİN HUKUKİ ÇERÇEVESİ 139

I. Dijital İzlemenin Anayasal ve Yasal Dayanakları 139

1. Dijital İzleme Uygulamalarının Anayasal Dayanakları 140

2. Dijital İzleme Uygulamalarının Yasal Dayanakları 143

a) Genel Olarak Dijital İzlemenin Yasal Çerçevesi 143

b) Karayolu Trafik Kanunu ve Yönetmeliği 146

c) İnternet Kanunu'nun Bir Gereği Olarak İnternet Trafiğinin İzlenmesi 148

II. Dijital İzleme Uygulamalarının Sözleşmesel Dayanakları 150

1. Yönetim Hakkının Bir Parçası Olarak Dijital İzleme 150

a) Yönetim Hakkının Kaynağı ve Sınırları 151

b) Yönetim Hakkı Kapsamında Dijital İzleme ve Denetim 155

2. Gözetme Borcunun Bir Gereği Olarak Dijital İzleme 158

a) Genel Olarak İşverenin Gözetme Borcu 159

b) İşverenin İş Sağlığı ve Güvenliği Yükümlülükleri 162

c) İşyerinde Tacizin ve Siber Zorbalıkların Önlenmesi 167

d) Kamu Sağlığının Korunması: Covid-19 Pandemisinin Ortaya Çıkardığı Uygulamalar ve Dijital İzleme 171

3. Personel Yönetmeliğinde Yer Alan Kişisel Veri Düzenlemeleri 176

III. Ara Değerlendirme: İş İlişkisinde Dijital İzlemenin Dayanaklarının Değerlendirilmesi 180

§ 6. DİJİTAL İZLEMENİN HUKUKA UYGUNLUK ÖLÇÜTLERİ 184

I. İşçinin Kişisel Verilerinin Korunması: Borçlar Kanunu m. 419 – Kişisel Veri Koruma Hukuku İlişkisi 184

II. Kişisel Veri Koruma Hukuku Kapsamında Dijital İzlemenin Sınırları 191

1. Kişisel Veri ve Kişisel Verinin İşlenmesi Kavramı 192

2. Özel Nitelikli Kişisel Veriler 196

3. Dijital İzlemede Dikkate Alınacak Kişisel Veri Koruma Hukukunun Genel İlkeleri 197

a) Veri İşlemenin Hukuka ve Dürüstlük Kuralına Uygun Olması..... 198

b) İşlenen Kişisel Verilerin Doğru ve Güncel İşlenmesi 203

c) İzlemenin Belirli, Açık ve Meşru Amaç Kapsamında Gerçekleştirilmesi 204

d) Dijital İzlemenin Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması 206

e) İşlenen İşçi Verilerinin Belirli Bir Süre Kadar Muhafaza Edilmesi 208

4. Dijital İzlemede Kişisel Verilerin İşlenme Şartları 209

a) Açık Rıza Beyanı Kapsamında Dijital İzleme Gerçekleştirilmesi .. 209

aa) Açık Rızanın Unsurları 210

bb) Açık Rıza ile Diğer Veri İşleme Şartları Arasındaki İlişki 213

cc) İş İlişkisinde Açık Rızanın Geçerlilik Koşulları 215

b) Kanunlarda Açıkça Öngörülmesi 218

c) Bir Sözleşmenin Kurulması veya İfası İçin Zorunlu Olması..... 219

d) Fiili İmkansızlık Sebebiyle Veri İşlemenin Zorunlu Olması 221

e) Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesi 221

f) İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması 222

g) Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması 224

h) Veri Sorumlusu İşverenin Meşru Menfaati İçin Zorunlu Olması . 225

i. Özel Nitelikli Kişisel Verilerin İşlenme Şartları 226

5. Medeni Kanun'daki Hukuka Uygunluk Sebepleri ile Kişisel Veri İşleme Şartları İlişkisi 228

6. Dijital İzleme Uygulamalarında Veri Sorumlusu İşverenin Aydınlatma ve Veri Koruma Yükümlülükleri 233

a) Aydınlatma Yükümlülüğü 233

b) Teknik ve İdari Tedbirleri Alma Yükümlülüğü 239

c) Denetlenebilir ve Şeffaf Bir Veri İşleme Süreci Oluşturma Yükümlülüğü 243

d. Veri Sorumluları Siciline Kayıt Yükümlülüğü 244

7. Dijital İzlemede İşlenen İşçi Verilerinin Aktarılması 245

a) İşlenen Kişisel Verilerin Yurt İçinde Aktarılması..... 246

b) İşlenen Kişisel Verilerin Yurt Dışına Aktarılması 248

8. Dijital İzlemede İşçinin İşlenen Kişisel Verileri Üzerindeki Hakları . 249

III. Dijital İzlemeyi Sınırlandıran Genel Hukuk İlkeleri 251

1. Dijital İzlemenin Eşit Davranma Borcuna Uygun Uygulanması 252

2. Dijital İzlemenin Dürüstlük İlkesine Uygun Olması 257

3. Dijital İzlemede Ölçülülük Denetimi 261

a) Dijital İzlemenin Ölçülü Olması 262

b) Dijital İzlemede Ölçülülük İlkesi Kapsamında Gerçekleştirilen Denetimler 266

aa) Gereklilik 267

bb) Elverişlilik 268

cc) Orantılılık 268

c. Uygulamada Ölçülülük Denetimi 269

4. İşçi Adaylarının Dijital İzleme Uygulamalarıyla İzlenmesi: Culpa in Contrahendo Sorumluluğu 271

§ 7. DİJİTAL İZLEME YÖNTEMLERİNİN HUKUKEN DEĞERLENDİRİLMESİ.....277

I. İşçilerin İşyerine Giriş Sistemleri Vasıtasıyla İzlenmesi 278

1. İşyeri Girişlerini İzleyen Dijital İzleme Uygulamaları 278

a) Kimlik Bazlı Giriş Kartları 279

b) Biyometrik Veri Esaslı Giriş Sistemleri 279

2. Kişisel Veri Koruma Hukukunda Doğan İşveren Yükümlülükleri..... 281

II. İşyerinde Kamera İzlemesi 283

1. İşverenin Kamera izlemesindeki Menfaati 284

2. Kamera İzlemesinin Sınırları 285

a) Bilgilendirmenin Bulunduğu Kameralarla İzleme 285

b) Suçun Önlenmesi Amacıyla Gizli Kamera Gözetlemesi 289

aa) Avrupa İnsan Hakları Mahkemesi Kararlarında İşverenin Gizli Kamera Gözetlemesi 289

bb) Gizli İzlemenin Hukuki Değerlendirmesi 296

3. İşçilerin Duygu Durumunu, Vücut Isılarını, Seslerini İzleyen ve Analiz Eden Optik Sistemler 299

III. İş İlişkisinde Kullanılan Verimlilik ve İş Sağlığı Takip Uygulamaları 301

1. İşyerinde Verimlilik İzleme Uygulamalarının Kullanılması 302

a) İşçileri İzleyen Konum ve Hareket Bazlı Sistemler 302

b) Giyilebilir Teknolojilerle İşçilerin İzlenmesi 303

2. İşyeri Dışında Konum Bazlı Dijital Sistemlerle İzleme 308

3. İşçinin Konum Belirleme Sistemleri ve Giyilebilir Teknolojilerle İzlenmesinin Sınırları 311

IV. İşçinin Elektronik İletişiminin İzlenmesi 313

1. Elektronik İletişimin İzlenmesinde İşverenin Menfaatleri 314

2. İşverenin Elektronik İletişime İlişkin Talimatları ve Yükümlülükleri 316

3. Elektronik İletişim Araçlarının İzlenmesine İlişkin AİHM ve AYM Yaklaşımı 321

ÜÇÜNCÜ BÖLÜM

DİJİTAL İZLEMENİN HUKUKİ SONUÇLARI

§ 8. DİJİTAL İZLEMENİN İŞ İLİŞKİSİNDEKİ SONUÇLARI 331

I. Hukuka Uygun Dijital İzlemenin Sonuçları 331

1. Hukuka Uygun Dijital İzlemeye İşçinin Uyma Yükümlülüğü 331

2. Dijital İzlemede Elde Edilen Veri – Fesih İlişkisi 334

a) Geçerli Nedenle Fesih 334

b) Haklı Nedenle Fesih 339

aa) Hukuka Uygun Biçimde Elde Edilme 339

bb) Dijital İzlemede İşverenin Şeref ve Namusuna Dokunacak Sözler ve Davranışların Tespiti 341

cc) İşçinin İşverenin Diğer İşçisine Cinsel Tacizde Bulunması 342

dd) Dijital İzlemede İşçinin Sataşması ve İşyerinde Alkol, Uyuşturucu Kullanması Verisinin İşlenmesi 345

ee) Dijital İzlemede İşçinin Doğruluk ve Bağlılığa Uymayan Davranışlarının Tespit Edilmesi 345

ff) İşçinin Yapmakla Ödevli Olduğu İşleri Hatırlatılmasına Rağmen Yapmadığı Verisine Ulaşılması 347

gg) Dijital İzlemede İSG Önlemlerine Uygun Davranılmadığının Tespit Edilmesi 349

II. Hukuka Aykırı Dijital İzlemenin Sonuçları 350

1. İşçinin İş Akdini Haklı Nedenle Feshetmesi 351

2. İşçinin Çalışmaktan Kaçınma Hakkı 353

3. İşçinin Kişilik Haklarını Koruyan Davaları Açması 357

a) Kişilik Haklarına Saldırının Önlenmesi Davası 357

b) Saldırının Durdurulması Davası 358

c) Saldırının Hukuka Aykırılığının Tespiti Davası 360

d) Kararın Üçüncü Kişilere Bildirimi ve İlanı 360

III. Hukuka Aykırı Dijital İzleme: Kamusal Yaptırımlar..... 362

1. Hukuka Aykırı Dijital İzleme: İşverene Uygulanacak Ceza Yaptırımları 362

2. İşçinin Verilerini Hukuka Aykırı İşleyen İşverene Uygulanacak İdari Yaptırımlar 366

§ 9. DİJİTAL İZLEMENİN OLUMSUZ ETKİSİNİ SINIRLAMAYA YÖNELİK ÖNERİLER 368

I. Açık Rıza ve Aydınlatma Yükümlülüğünün Veri Korumada Yetersizliği 369

1. Açık Rıza ve Aydınlatma Yükümlülüğünün Sorunlu Yönleri 369

2. Aydınlatma Yükümlülüğü ve Açık Rızadan Önce Yeni Denetimlerin Geliştirilmesi İhtiyacı 375

II. Verilerin Doğrudan İşçiden Elde Edileceği Yöntemlerin Önceliklendirilmesi 378

III. İşçinin Bilişim Sistem ve Uygulamalarıyla Bağlantıyı Kesme Hakkının Yasal Çerçeveye Kavuşturulması İhtiyacı 382

IV. Dijital İzleme Uygulamalarında Veri Koruma Etki Değerlendirmesinin Zorunlu Olması Gerekliliği 386

V. İş İlişkisinde Otomatik Profil Oluşturan Yapay Zeka Destekli Dijital İzleme Uygulamalarının Sınırlandırılması 392

SONUÇ 398

KAYNAKÇA 405

ÇEVRİMİÇİ KAYNAKLAR 463

KISALTMALAR

AB :	Avrupa Birliği
AB/EU :	Avrupa Birliği/European Union
ABAD :	Avrupa Birliği Adalet Divanı
ABD :	Amerika Birleşik Devletleri
AİHM :	Avrupa İnsan Hakları Mahkemesi
AİHS :	Avrupa İnsan Hakları Mahkemesi
AMKD :	Anayasa Mahkemesi Kararlar Dergisi
AYM :	Anayasa Mahkemesi
BAG :	Bundesarbeitsgericht-Alman Federal İş Mahkemesi
BAM :	Bölge Adliye Mahkemesi
BİM :	Bölge İdare Mahkemesi
Bkz. :	Bakınız
BM :	Birleşmiş Milletler
C. :	Cilt
CFREU :	Charter of Fundamental Rights of the European Union
Çev. :	Çeviren
D. :	Daire
Dan. :	Danıştay
DEÜHFD :	Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi
dn. :	Dipnot
E. :	Esas
EC :	European Commission/Avrupa Komisyonu
EDPB :	European Data Protection Board/Avrupa Veri Koruma Kurulu
EÜHFD :	Erzincan Üniversitesi Hukuk Fakültesi Dergisi
FIPP :	Fair Information Practice Principles/Adil Bilgi Uygulama İlkeleri
GPS :	Global Positioning System/Küresel Konumlama Sistemi
GPRS:	General Packet Radio Service

GSM :	Global System for Mobile
GVKT/GDPR :	Genel Veri Koruma Tüzüğü/General Data Protection Regulation
HD. :	Hukuk Dairesi
HGK :	Hukuk Genel Kurulu
HMK :	Hukuk Mahkemeleri Kanunu
ILO :	Uluslararası Çalışma Örgütü
İBD :	İstanbul Barosu Dergisi
İDD :	İdari Dava Daireleri
İDDK:	İdari Dava Daireleri Kurulu
İHD :	İş Hukuku Dergisi
İHEB :	İnsan Hakları Evrensel Beyannamesi
İSG :	İş Sağlığı ve Güvenliği
İSGK :	İş Sağlığı ve Güvenliği Kanunu
İşK. :	4857 sayılı İş Kanunu
İÜHFD :	İstanbul Üniversitesi Hukuk Fakültesi Dergisi/Mecmuası
K. :	Karar
KTK :	Karayolu Trafik Kanunu
KVK Hukuku :	Kişisel Verileri Koruma Hukuku
KVK Kurulu :	Kişisel Verileri Koruma Kurulu
KVK Kurumu :	Kişisel Verileri Koruma Kurumu
KVKK :	Kişisel Verilerin Korunması Kanunu
Legal-İSGHD :	Legal İş ve Sosyal Güvenlik Hukukuna İlişkin Yargı
m. :	Madde
MERCEK :	Türkiye Metal Sanayicileri Sendikası Dergisi
MK :	Medeni Kanun
N. :	Numara
No :	Sayı
OECD :	Organisation for Economic Co-operation and Development/ Ekonomik Kalkınma ve İşbirliği Örgütü
para. :	Paragraf

RFID :	Radio-frequency identification/Radyo Frekansı ile Tanımlama
RG :	Resmi Gazete
s. :	Sayfa
S. :	Sayı
SBE :	Sosyal Bilimler Enstitüsü
STSK :	6356 Sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu
TBBD :	Türkiye Barolar Birliği Dergisi
TBK :	Türk Borçlar Kanunu
TCK :	Türk Ceza Kanunu
TDK :	Türk Dil Kurumu
vb. :	ve benzeri
vd. :	ve devamı
VERBİS :	Veri Sorumluları Bilgi Sistemi
Vol. :	Cilt
VPN :	Virtual Private Network/Sanal Özel Ağ
vs. :	ve saire
WP 29 :	Article 29 Working Party/29. Madde Çalışma Grubu
Yarg. :	Yargıtay
YCDK :	Yargıtay Ceza Dairesi Kararı
YHDK :	Yargıtay Hukuk Dairesi Kararı
YİBK :	Yargıtay İçtihadı Birleştirme Kararı
YKD :	Yargıtay Kararları Dergisi
Yön. :	Yönetmelik

ÖZET

Günümüz işyerlerinin önemli bir parçasına dönüşen bilişim sistemleri ve işverenlerin çeşitli amaçlarla kullandığı dijital izleme uygulamaları kişisel veri işleyen teknolojiler olduğundan işçilerin özel hayatı ve kişisel verileri üzerindeki hakları ile işverenin mülkiyet hakkı, iş sözleşmesinden doğan yönetim ve ekonomik hakları arasında bir çatışma ortaya çıkarmaktadır. İş ilişkisinde kullanılan dijital izleme uygulamalarından olan kamera gözetlemesi, iletişimi izleyen uygulamalar, konum ve hareket izleme sistemleri, giyilebilir teknolojiler ve biyometrik veri esaslı işyeri giriş ve izleme sistemleri işçilerin kişisel verilerini kişisel zamanı da kapsayacak biçimde işlemeye konu etmekte, büyük veri tabanlarında analize ve paylaşmaya olanak tanımaktadır.

Hukuk sistemimizde kişiliğin ve kişisel verilerin korunmasına yönelik yasal düzenlemeler gerçekleştirilmesine rağmen kişisel verileri koruma hukukumuzda dijital izleme, otomatik profil oluşturma ve işçi özelinde bir düzenleme yer almamaktadır. Ayrıca kişisel verileri koruma hukukunda veri koruma mekanizmaları olarak görülen aydınlatma yükümlülüğü ve açık rıza beyanı otorite/bağımlılık ilişkisinin bulunduğu iş ilişkisinde işçinin özgür iradesiyle açık rıza beyanında bulunmasının güç olması ve aydınlatma yükümlülüğünün bir formaliteyi tamamlaya dönüşmesi dikkate alınarak işçi verisini işlemeyi sınırlandıran yeni enstrümanlar üzerinde düşünmeyi gerektirmektedir.

Tezde işverenin dijital izleme hakkı ve sınırları incelemeye konu edilerek işyerine ilişkin riskleri üzerinde taşıyan işverenin dijital izleme hakkı ile işçinin kişilik hakkı ve özgürlükleriyle ilgili olan özel hayatı ve kişisel verileri üzerindeki haklarının hangi düzeyde adil dengeye kavuşturulabileceği değerlendirildi. İşverenin dijital izleme uygulamalarını kullanmadan önce veri koruma etki değerlendirmesi yapması, profil çıkarmanın istisnalara bağlanarak yasaklanması, verilerin doğrudan işçiden elde edileceği yöntemlerin önceliklendirilmesi ve işçiye

bilişim sistemleriyle bağlantıyı kesme hakkı tanınması gibi çözüm önerileri üzerinde duruldu.

Anahtar Kelimeler: İşyerinde Gözetleme, Dijital İzlemenin Sınırları, İşçinin Kişisel Verileri, İşverenin Dijital İzleme Hakkı, İş İlişkisinde Dijital İzleme

ABSTRACT

Information systems, which have become an important part of today's workplaces, and digital monitoring applications used by employers for various purposes, are technologies that process personal data, they create a conflict between employees' rights over their private life and personal data and the employer's property rights, management and economic rights arising from the employment contract. Camera surveillance, applications that monitor communication, location and movement tracking systems, wearable technologies and biometric data-based workplace entry and monitoring systems, which are among the digital monitoring applications used in employment relationships, process employees' personal data, including personal time, and enable analysis and sharing in big databases.

Although legal regulations have been made in our legal system for the protection of personality and personal data, our data protection law does not include digital monitoring, automatic profiling and any employee-specific regulations. In addition, the obligation to inform and explicit consent, which are seen as data protection mechanisms in data protection law, require consideration of new instruments that limit the processing of employee data, taking into account the fact that it is difficult for the employee to declare explicit consent with his free will in an employment relationship where there is an authority/dependence relationship and that the obligation to inform turns into a formality.

In the thesis, the employer's right to digital monitoring and its limits were examined and it was evaluated to what extent the digital monitoring right of the employer, who carries the risks related to the workplace, and the employee's rights on their private life and personal data, which are related to their personal rights and freedoms, can be balanced fairly. Solution suggestions such as the employer conducting a data protection impact assessment before using digital monitoring applications, prohibiting profiling with exceptions, prioritizing the methods to

obtain data directly from the employee, and granting the employee the right to disconnect from information systems were emphasized.

Keywords: Surveillance in the Workplace, Limits of Digital Monitoring, Employee's Personal Data, Employer's Digital Monitoring Right, Digital Monitoring in Labour Relationship

GİRİŞ

I. Konunun Önemi

Yaygınlaşan kitle iletişim araçlarının kişinin verilerini işleme biçimini ve kişi üzerindeki etkisini gözlemleyen Adorno, hayatının öznesi olma hakkının kişinin elinden alınmaya başlandığı[1] tespitinde bulunmuştur. Bu tespitten bugüne dünyamız, "kişi ne kadar hayatının öznesi?" sorusu üzerine daha az düşünüldüğü, dijital teknolojinin tetiklediği, her alanda hızlı değişimin yaşandığı bir döneme girdi. Bilgi ve yeni iletişim teknolojilerinin belirleyici olduğu bu değişim sürecinde, analog veri işleme süreci dijital "büyük veri" işleme sürecine dönüştü. Bu değişim bireysel alışkanlıkları, sosyal ilişkileri, üretimi ve tüketimi; işçi profilini, çalışma modelini ve işyeri yapılanmasını dönüştürdüğü gibi iş ilişkisinde yeni kavramlar ve çözülmesi gereken sorunlar ortaya çıkarmaktadır. Bilişim sistemleri vasıtasıyla işlenen verilerle bireylerin dijital kopyalarını oluşturabilen, kişinin algılarını ve alışkanlıklarını izleyerek etkileyebilen ve uzaktan denetlenmeyi kişisel veriler üzerinde istilacı sonuçlar ortaya çıkaracak biçimde olanaklı hale getiren teknolojik uygulamalar iş ilişkisinde kendine özgü kullanımlara konu edilmektedir.

İş hukukunda işçilerin özel hayatları ile kişisel verilerinin korunmasına ilişkin genişleyen yasal çerçeve ve işverenlerin işçileri hakkında daha fazla bilgi işleme ihtiyacının uzlaştırılarak adil bir dengenin kurulması gerekliliği, pandemi sebebiyle yaygınlaşan uzaktan çalışmada işçileri denetlemek için kullanılan çeşitli dijital izleme uygulaması kullanmanın ölçülülüğü, iş ilişkisinin tüm süreçlerine sirayet etmiş dijital izleme karşısında işverenin işçiyi gözetme borcunun veya kişisel veri mevzuatının işçinin özel hayatının gizliliğini ve kişisel verilerini korumak için öngördüğü mekanizmaların yeterliliği işyerinde dijital izlemenin ortaya çıkardığı sorunlara örnek gösterilebilir.

---

1) Theodor W. Adorno, Kültür Endüstrisi, (Çev. Nihat Ülner - Mustafa Tüzel - Elçin Gen), İletişim Yayınları, 6. Baskı, İstanbul, [2011], s. 110.

Bilişim teknolojilerinin işyerlerinde temel iş yapma araçlarına dönüştüğü; işini ifa etmenin yeri, zamanı ve biçiminin değişime uğradığı günümüzde işyeri veriminin artırılması, çalışma barışı, iş stresinin azaltılması, işçi sağlığı ve mutluluğu için tezin inceleme alanı açısından önemli olan şu soruların cevaplarının bulunması gerekmektedir. İşyeri verimini artırma, mülkiyeti, itibarı ve ticari sırları koruma, yönetim hakkı veya işçilerin iş saatlerinde oyun oynamasını, bahis sitelerinde gezinmesini; iş için tahsis edilen arabanın, telefonun ve bilgisayarın kişisel amaçlarla kullanılmasını, iş saatlerini iş dışı faaliyetler için geçirmesini ve işyerindeki veri gizliliği kurallarını ihlal edilmesini engelleme isteği işverenlere her durumda dijital izleme imkanı verir mi? İşverenlerin dijital izlemedeki meşru menfaatleri ve işyerine ilişkin haklı görülebilecek bu riskleri engelleme düşüncesi işverenlere, işçilerin özel hayat alanlarına taşacak şekilde denetim, kişisel verilerini bilgisi dışında işleme, işyerindeki tüm izlerini dijital uygulamalarla takip etme, işçilerin duygularını kontrol edebilecek dijital izleme uygulamalarını kullanma ve bu uygulamalarla elde ettiği verilere dayanarak iş akdini haklı sebeple feshetme hakkı tanır mı?

Bununla birlikte kişisel verilerinin işlenmesine ilişkin gerekli bilgilendirmenin yapıldığı ve açık rızanın alındığı durumlarda işçilerin, işçi adaylarının işe uygunluklarının ve gelecekteki performanslarının öngörülmesi amacıyla duygu durumlarının, olaylara verdikleri tepkilerin, sağlık verilerinin, biyometrik ve genetik verilerinin, sosyal medya hesaplarındaki verilerin analiz için yapay zeka sistemlerine yüklenmesi, algoritmik iş taranmasına[2] konu edilmesi mevcut hukuki düzenlemeler karşısında nasıl değerlendirilmelidir? Bu tür verilerin işlenmesine çoğunlukla ilgili gerçek kişinin bilgilendirilmesi yükümlülüğü[3], açık

2) Yüz binlerce işçisi bulunan firmalara algoritmik iş taraması hizmeti sunan, işçi adaylarının biyometrik ve duygu durumları dahil olmak üzere birçok kişisel veriyi işleyen "HireVue" ve "Pymetrics" gibi firmalar bu katmanlarda kişisel verileri işlemekte ve analize konu ederek işveren müşterilerine satmaktadır https://www.hirevue.com/about ve https://www.pymetrics.ai/mission .

3) AİHM kararlarında dijital izlemenin gerçekleştirilebilmesi için izlemenin niteliği, içeriği ve kapsamı konusunda işçinin önceden bilgilendirilmesi koşulunu aramaktadır (AİHM Büyük Daire Bărbulescu & Romanya kararı (Başvuru Numarası: 61496/08); Anayasa Mahkemesi de AİHM kararlarına atıf yaparak dijital izlemenin ancak önceden bilgilendirme yapılmasıyla hukuka uygun olacağı yönünde karar vermektedir (AYM, E.Ü. Kararı Başvuru Numarası: 2016/13010, Karar

rıza, sınırlı ve ölçülü veri işleme kapsamında yaklaşan kişisel veri mevzuatları bu durumlarda işçilerin kişisel verilerini ve özel hayatının gizliliğini korumada ne kadar yeterlidir? Dijitalleşmenin etkisiyle dönüşen iş ilişkisinde bu soruların cevaplarının bulunması ve işçilerin özel hayat alanlarına taşacak verilerin işlenmesi için vermiş olduğu rızanın hukuki düzenlemeler kapsamında tartışmaya konu edilmesi çalışma barışının sağlanması açısından önemlidir.

Dijitalleşme iş ilişkisi dahil her alana kolay uygulanabilme, kapsamlı denetleyebilme ve görece olarak daha ucuz olma özelliklerinden kaynaklı olarak değişime zorlamaktadır[4]. İş ilişkisinin önemli bir uygulaması haline gelen, her türlü işi yapmaya olanak veren yapay zeka uygulamaları ve cep telefonları ilgili kişi farkında olmadan kişisel verilerini ve metadata[5] verilerini işlemektedir. Dahası kavramları algılamaya duyarlı yapay zeka uygulamaları ve profilleme teknolojileri sayesinde gerçek kişilerin yaşam tarzları, kişisel tercihleri, web gezinme davranışları, güvenlik ve sağlık riskleri, duygu durumları, cinsel tercihleri gibi birçok katmanda veri toplamakta ve bunlar büyük veri tabanlarında işlenerek kişinin dijital kopyası oluşturulmaktadır[6].

Uzaktan çalışmanın Covid-19 pandemisinin etkisiyle sıkça gündeme geldiği günümüzde işverenler gelişen teknolojinin imkanlarından faydalanarak işçi

---

Tarihi: 17/9/2020; Aynı doğrultuda AYM, Ömür Kara ve Onursal Özbek Kararı § 50; AYM, Fırat Gerçek kararı, Başvuru Numarası: 2019/25604, Karar Tarihi: 21.09.2022 https://www.resmigazete.gov.tr/eskiler/2022/11/20221115-5.pdf); Yargıtay son kararlarında bu hususta AİHM ve AYM'nin belirlediği bu ölçüt kapsamında kararlar vermektedir. Bkz. Yargıtay 22. Hukuk Dairesi, E. 2017/21857 K. 2019/9884 T. 7.5.2019 kararı.

4) James R. Beniger, The Control Revolution Technological and Economic Origins of the Information Society, Harvard University Press, [1986], s. 174-175.

5) "Üst veri" veya "meta veri" olarak dilimize çevrilen "metadata" bir sistem kaynağını ya da verinin öğelerini (veri hakkında veri / veri hakkında bilgi) tanımlayan bilgilerden oluşur. Böylelikle bir kaynağın ne olduğu, nerede üretildiği, konusu, ne zaman erişildiği ve üretildiği gibi veri hakkında birçok veri işlenir. Bu veriler doğrudan gerçek kişiye ilişkin olmasa da bir kişiyi ve alışkanlıklarını belirleme, dijital izini takip etme imkanı sağladığından özel hayatın gizliliğini ihlal edebilir. Örneğin işyerinde işçilerin hareketlerine duyarlı sistemlerle veri toplanması doğrudan kişinin verileri olmamasına rağmen elde edilecek metadata verileriyle bir kişinin kimliği belirlenebilir. https://tr.wikipedia.org/wiki/Metadata (Erişim Tarihi: 10.05.2022).

6) Janine Berg, "Protecting Workers in the Digital Age: Technology, Outsourcing, and the Growing Precariousness of Work", Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall [2019], s. 79-80.

verimliliğini artırmak, işçileri denetim altında tutmak, uzaktan çalışma gibi yeni çalışma modelleri oluşturmak, işyeri güvenliğini sağlamak, temas durumunu takip etmek ve iş sağlığı ve güvenliğine ilişkin yükümlülükleri yerine getirmek amacıyla dijital izlemenin çeşitli türlerini kullanmaktadır[7]. Bunun yapılması işçinin özel hayatı[8] ile iş hayatı arasındaki sınırı bulanıklaştırmakta ve kişisel verilerinin iş ilişkisinin sınırlarını aşacak yoğunlukta işlenmesine sebebiyet vermektedir. Her hak aynı zamanda diğer haklar karşısında bir sınırlamayı, bazen de korumayı gerektirdiğinden[9] işverenin herhangi bir sınırlama olmaksızın işçileri dijital izlemeye tabi tutması ve işçilerin kişisel verilerini iş ilişkisini aşacak yoğunlukta işlemesi işçinin kişisel verileri üzerindeki haklarının ihlaline sebebiyet verebilmektedir[10].

Dijital izlemede işçi ve işverenin çatışan menfaatlerine işçi açısından insan hakkı olan ve Anayasa'da temel hak ve özgürlüklerden birisi olarak düzenlenen özel hayatın gizliliğinin korunması, haberleşme özgürlüğü, kişilik hakkı ve kişisel verilerinin korunması hakları; işveren açısından ise anayasal hak olan mülkiyetin korunması ve sözleşme özgürlüğü, yönetim hakkı ile ilgili olan verimliliğinin

7) Dijital izlemenin iş ilişkisinde artarak devam ettiğini ve uzaktan çalışmanın bir parçası haline geldiğini konu edinen bir haberde izlendiğini bilen bir işçi dijital izlemenin oluşturduğu etkiyi şu şekilde ifade etmiştir: "Öğle yemeğim sırasında beş dakikalık bir video izlemek bile beni geriyor, birinin YouTube'un ekran görüntüsünü görmesinden ve işten kovulma sebebi olmasından korkuyorum." Haber için bkz. https://www.bbc.com/worklife/article/20220621-the-employee-surveillance-that-fuels-worker-distrust (Erişim Tarihi: 24.06.2023).

8) Anayasa Mahkemesi, Serap Tortuk Kararında: "kişilerin özel hayat alanları içinde kaldığı açık olan eylemleri gerekçe gösterilerek mesleki hayata ilişkin gerçekleştirilen müdahalelerin demokratik toplum düzeninin gereklerine uygun" olmadığına karar vermiştir. Karara konu olayda kamuda işçi başvurucu özel hayat alanında meydana gelen, mesleki faaliyetiyle de ilgisi bulunmayan, başvurucuyla ilişkisi tam olarak saptanamamış bir sosyal medya hesabı üzerinde gerçekleştirilen paylaşımlar sebebiyle meslekten ihraç kararı verilmiştir. Anayasa Mahkemesi ihraca gerekçe gösterilen paylaşımların başvurucunun rızasıyla alenileştirildiğine dair bir bulgunun saptanamadığını, özel hayat alanına girebilecek eylemler nedeniyle başvurucunun meslekten çıkarılmasını Anayasa'nın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkına aykırı olduğuna hükmetmiştir. AYM. 21/1/2015 Tarih ve Başvuru No: 2013/9660 sayılı Serap Tortuk Kararı.

9) Rona Serozan, Hukukta Yöntem, Vedat Kitapçılık, İstanbul, [2015], s. 67.

10) AYM Genel Kurul Kararı, Ramazan Şahin Kararı, Başvuru Numarası: 2018/11988, Karar Tarihi 10.03.2022, Resmi Gazete 19 Nisan 2022, Sayı 31814; AYM Genel Kurul Kararı E. 2014/180 K. 2015/30 T. 19.3.2015; İstanbul BİM, 3. İDD, E. 2017/1689 K. 2018/62 T. 18.1.2018. KVK Kurulu, K. 2020/167, T. 27.2.2020 tarihli kararı.

artırılması, işyeri güvenliğinin sağlanması, iş sağlığı ve güvenliği kapsamında yasal yükümlülüklerin yerine getirilmesi örnek gösterilebilir. İş hukukunda bu menfaatlerin sınırlarının ortaya konması, dijital izlemenin iş ilişkisindeki uygulama alanlarının, etkilerinin belirlenmesi ve kişisel verileri korumaya ilişkin yasal düzenlemelerin yapay zeka, büyük veri, algoritmik analiz gibi izlemelerle çeşitlenen dijital izlemede işçileri koruyabilirliğinin incelenmesi, bu hususta önerilerin belirlenmesi tezin temel amacını oluşturmaktadır.

II. Konunun Sınırlandırılması

İşçileri dijital izleme uygulamaları vasıtasıyla birçok katmanda izleyip, denetim ve kayıt altında tuttuğundan modern dünyanın[11] taslak hukuki metinlere[12] konu ettiği konularından birisi olan iş ilişkisinde dijital izleme, ülkemizde hak ettiği ilgiyi henüz görememiştir. Hukuki, sosyolojik, siyasi, felsefi, ekonomi, etik ve teknik boyutu bulunan dijital izlemenin işçi üzerindeki etkileri tartışmalara konu edilmektedir. Bilişim teknolojilerinin ortaya çıkardığı bu olgunun iş hukuku açısından bir nebze de olsa açıklığa kavuşturulması amacıyla; dijital izlemenin iş ilişkisinde gerekliliği, görünümü, sınırları, etkileri ve dijital izlemede taraf menfaatleri ile işçinin verileri üzerindeki haklarının nasıl etkin korunabileceği yerli ve yabancı kaynaklar taranarak ortaya çıkarılacaktır.

Bu amacı gerçekleştirmek için iş hukukunda dijital izleme ulusal mevzuat, yabancı ülke düzenlemeleri, WP 29 Çalışma Grubu (Article 29 Working Party) ve European Data Protection Board (EDPB - Avrupa Veri Koruma Kurulu)

11) AB büyük hacimli kişisel veri işleyen teknoloji şirketlerinin dijital pazarda gücünü frenlemek için dijital piyasalar düzenlemesi ile işyerinde dijital izlemeye ilişkin yeni kurallar getiren bir dizi çalışma yapmaktadır. https://www.theguardian.com/technology/2022/mar/25/european-union-big-tech-googld-facebook-meta (Erişim Tarihi: 27.03.2022).

12) Avrupa Komisyonu, Dijital Hizmetler Yasası (Digital Services Act) çalışmasını hızlandırarak basit web sitelerinden internet altyapı hizmetlerine ve çevrimiçi platformlara kadar geniş bir çevrimiçi hizmetler kategorisini gerçek kişilere ilişkin profilleme oluşturmada ve kişisel verilerini işlemeye yeni kurallar getirmektedir. Böylelikle dijital ortamda kişisel verileri işlenen ilgililerin veri işleme süreçleri ve profillemelere karşı korunması hedeflenmektedir. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (Erişim Tarihi: 26.03.2022).

çalışmaları, Avrupa Birliği (AB) düzenlemeleri, Birleşmiş Milletler (BM), International Labour Organization (ILO/Uluslararası Çalışma Örgütü), Organisation for Economic Co-operation and Development (OECD/Ekonomik Kalkınma ve İşbirliği Örgütü) gibi uluslararası düzenlemeler kapsamında incelendi ve Avrupa İnsan Hakları Mahkemesi (AİHM), Avrupa Birliği Adalet Divanı (ABAD), Anayasa Mahkemesi ve Yargıtay kararlarında benimsenmiş ölçütler kapsamında değerlendirildi.

Dijital izlemenin birey üzerindeki etkileri onu hukuk dışında birçok disiplinin konusu haline getirmektedir. Tezde hukuki bakış açısı esas alındığından diğer disiplinlerdeki boyutu gerekli olduğu ölçüde değerlendirilecektir. Dijital izlemeyi bilişim teknolojileri kapsamında tüm uygulanan ve gelişen izleme yöntemleriyle değerlendirmek tezdeki hukuki bakış açısıyla uyuşmayacağı gibi konuyu teknolojinin uzmanları ölçüsünde değerlendirmek de mümkün değildir. Ayrıca bunun yapılması tezin amacıyla da örtüşmeyeceğinden gerektiği ölçüde bazı dijital izleme örneklerine değinilecek ve bunlar taraf menfaatleri açısında değerlendirmeye tabi tutulacaktır. Bu sınırlandırmanın bir diğer sebebi de teknolojinin durağan bir yapıda olmamasıdır. Kuşkusuz tespit edilecek ve sınırlandırılacak dijital izleme yöntemlerinden farklı izleme araçları teknolojik gelişmelere bağlı olarak gelecekte ortaya çıkacaktır.

İş hukukunda dijital izlemenin veri öznesi bir gerçek kişi olan işçi, işçi adayı ve eski işçidir. İşçinin kişilik hakları onun sahip olduğu bireysel değerlerin tümünü kapsar. Medeni Kanun'da kişiliği korumada genel nitelikli çerçeve düzenlemeler öngörülmüştür. Kişilik hakları konusunda "numerus clasus" ilkesi geçerli olmadığından kişiyi kişi yapan bütün değerler kişilik hakkı kapsamında değerlendirilmekte ve ihtiyaca göre ortaya çıkan değer korumadan faydalanmaktadır[13]. Türk Borçlar Kanunu (TBK) düzenlemeleri ise işverene,

13) M. Kemal Oğuzman/Özer Seliçi/Saibe Oktay Özdemir, Kişiler Hukuku, 16. Bası, Filiz Kitabevi, [2016], s. 164-165.

işçinin kişiliğini korumak ve saygı göstermek yükümlülüğü yüklemiştir (TBK m. 417). Dijital izleme işçinin temel hak ve özgürlükleri ile kişilik hakkıyla ilgili olduğundan anayasa hukuku, bireysel iş hukuku, borçlar hukuku, medeni hukuk, iş sağlığı ve güvenliği hukuku, ceza hukuku, internet hukuku ve kamu hukukunun diğer alanlarıyla kesiştiği yönleri bulunmaktadır.

Dijital izleme uygulamaları veri işleyen sistemler olduğundan esas itibariyle işçinin temel hak ve özgürlüğü ile kişilik hakkı olan özel hayatının gizliliği ve kişisel verileri üzerinde müdahaleci etkiler ortaya çıkarır. Dijital izlemenin etkilediği bu hakların niteliği ve düzenlendiği yasalar dikkate alındığında bunları toplu iş sözleşmesine konu etmek kanaatimce olanaklı değildir. Ayrıca dijital izleme işçinin ifade özgürlüğü ve haberleşme özgürlüğü hakları üzerinde doğrudan bir etki ortaya çıkarmaz. Zira ancak dijital izlemede elde edilen verinin iş sözleşmesi üzerindeki etkisi açısından ifade özgürlüğü değerlendirmesi yapılabilir. Haberleşme özgürlüğü ise elektronik iletişime ilişkin sınırlandırmalarda gündeme gelebilir. Bu sebeple tezde konu esas itibariyle bireysel iş hukuku ve dijital izlemede işçinin tehlikeye atılan hakları olan özel hayata saygı hakkı ve kişisel verilerin korunması hakkı dikkate alınarak ele alındı.

III. Konunun Sunulması

Tez giriş, üç bölüm ve sonuç kısmından oluşmaktadır. Tezin Birinci Bölümü'nde dijital izlemeye ilişkin kavramlar, dijital izlemenin iş ilişkisindeki kullanım seyri, işyerinde gözetlemenin dönüşümü, özel hayatın gizliliğinin korunması fikrinin gelişim seyri, işçinin özel hayatı ile kişisel verilerinin korunması arasındaki ilişki, kişisel verilerin korunması hukukunun doğuşu, dijital izlemede işçinin korunan değerleri, dijital izlemede taraf menfaatleri ve dijital izlemenin iş ilişkisindeki etkileri değerlendirilecektir. Ayrıca kişisel verilerin korunması mevzuatımıza kaynaklık eden Avrupa Birliği mevzuatının dijital izleme çerçevesinde değerlendirilmesi gerektiği düşüncesiyle Avrupa Birliği Genel Veri Tüzüğü düzenlemeleri, Avrupa Birliği Adalet Divanı (ABAD) kararları ve AİHM

kararları ilgili başlıklarda ele alındı. Kişisel verilerin korunmasına ilişkin tarafı olduğumuz uluslararası düzenlemeler olan Kişisel Verilerin Otomatik İşlenmesine İlişkin 108 sayılı Sözleşme ve 181 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması, Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol da dijital izleme kapsamında ele alındı.

İkinci Bölüm'de işyerinde dijital izleme; işverenin dijital izleme hakkı, dijital izlemenin sözleşmesel dayanakları, işverenin yönetim hakkı kapsamında dijital izleme gerçekleştirilmesi değerlendirildi. Bu bölümde aynı zamanda dijital izlemenin hukuka uygunluk ölçütleri, işçinin kişisel verilerinin korunması hakkı, işçinin kişisel verilerine ilişkin olan TBK m. 419 ile kişisel verileri korunması hukuku ilişkisi, kişisel verileri korumaya ilişkin düzenlemelerin bu hakları korumadaki yeterliliği, dijital izleme uygulama örneklerinde taraf menfaatlerin sınırları ve ölçülülük ilkesi kapsamında gerçekleştirilebilecek denetimler analiz edildi. Dijital izlemede işlenen kişisel verilerin hukuka uygunluk nitelendirmesinde nelerin dikkate alınması gerektiği bu bölümde ele alındı. Ayıca kişisel veri koruma hukukunun temel ilkelerinin uygulanma alanı ve kişisel veri işleyen veri sorumlularına veri koruma mevzuatının veri işlenmeden önce yükümlülükler yüklediğinden, iş ilişkisi bağlamında veri sorumlusu işverenin yükümlülükleri de bu bölümde analiz edildi.

Üçüncü Bölüm'de, dijital izlemenin iş hukukundaki sonuçları ve iş sözleşmesinin üzerindeki etkileri ele alınarak dijital izlemenin taraf menfaatleri açısından adil bir dengeye kavuşmasına yönelik öneriler oluşturuldu. Ayrıca hukuka aykırı ve hukuka uygun dijital izlemenin iş sözleşmesi ve taraf hak ve yükümlülükleri üzerindeki etkileri de bu bölümde ele alındı. Hukuka aykırı dijital izlemenin sonuçları, uygulanabilecek cezai yaptırımlar, işçinin haklarını ileri sürebileceği alanlar ve idari yaptırımlar da bu bölümde değerlendirildi.

BİRİNCİ BÖLÜM
DİJİTAL İZLEMENİN İŞYERİNDE KULLANILMASI VE VERİ KORUMA

§ 1. GÖZETLEMEDEN DİJİTAL İZLEMEYE İŞÇİNİN İZLENMESİ

Dijital izlemenin hukuki çerçevesini ortaya çıkarmak ve konunun açıklığa kavuşmasını sağlamak amacıyla öncelikle dijital izlemeyle ilişkili kavramlar açıklanacak, işyerinde gözetlemeye kaynaklık eden ve denetimle işyeri verimliliğinin artırılması kapsamında gelişen gözetlemeye ilişkin yaklaşımlar değerlendirilecek, bireyin özel hayatını ihlal etme ve kişisel verilerini işleme biçimini değiştiren teknolojinin bu hakların korunmasını sağlayan hukuki düzenlemelerin ortaya çıkmasındaki etkisi ele alınacaktır.

I. İş İlişkisinde Gözetleme, Gözetim ve İzleme Kavramları

İş hukukunda gözetleme, gözetim ve izleme nedir? Mahremiyet ve özel hayatın gizliliğinin korunması aynı içeriği mi işaret etmektedir? Kavramların neyi ifade ettiği ve üstlendikleri işlevlerin açıklığa kavuşturulması içeriğin anlaşılmasına rehberlik eder. Kavramların açıklığa kavuşturulmasının önemi Sokrates'in; "kavramların anlamları üzerinde anlaşabilseydik, asla birbirimizle kavga etmezdik" cümlesiyle güzel ifade edilmiştir[14]. Bu düşünceden hareketle konunun doğru kavramlar zemininde incelenebilmesi için gözetleme, gözetim ve izleme kavramları ile iş ilişkisinde uygulanan dijital izlemenin geçmiş arka planı aşağıda ele alınacaktır.

14) Aynur Yongalık, "İstisnalar Dar Yorumlanır Kuralı ve Değerlendirmesi", AÜHFD, C. 60, S. 1, Ankara [2011], s. 1-15, s. 5.

1. Gözetleme

Gözetlemeye ilişkin yapılan çalışmalar gözetlemenin insanlık tarihi boyunca öğrenme, denetleme[15], merak ihtiyacını giderme, örgütlenme, tedbir alma ve gelişmeleri izleme aracı olarak kullanıldığını ortaya koymaktadır[16]. Sosyal bilimlerde gözetleme kavramı ile ilgili birçok tanım[17] yapılmış olmakla birlikte en yaygın kullanılan tanım Lyon'un tanımdır. Lyon gözetlemeyi; "hakkında veri toplanan kişileri etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel verinin toplanması ve işlenmesi"[18] biçiminde tanımlamaktadır. Gözetleme sonucu elde edilen veri, öngörülen hedef doğrultusunda sistematik olarak analiz edilir ve gözetlenen ilgili kişinin (hedef işçi) davranışlarını etkilemek veya hakkında bir karar vermek için kullanılır[19].

Gözetleme sürecinde iktidarların veya işverenlerin gerçek kişilere ilişkin elde ettiği bilgi parçaları[20], toplumu veya işçileri denetim ve baskı altında tutmayı kolaylaştırdığından "gözetleme" kavramı zamanla olumsuz bir anlam yüklenmiş ve hiyerarşik bir güç ilişkisi içinde birisinin diğerini dikizlemesi[21] anlamını yüklenmiştir. Tanımlardan ulaşılan bir diğer sonuç da gözetlemenin her zaman bir hiyerarşik ilişki çerçevesinde ortaya çıkmasıdır.

Gözetlemeye ilişkin yapılan tanımlarda "etkileme, denetleme, yönetme" ve

---

15) Anthony Giddens, Ulus – Devlet ve Şiddet, (Çev. Cumhur Atay), Kalkedon Yayınları, İstanbul [2008], s. 8.
16) David Lyon, Elektronik Göz, (Çev. Dilek Hattatoğlu) Sarmal Yayınevi, İstanbul, [1997], s. 39.
17) Clarke, gözetlemeyi "bir kişi veya gurubun iletişim ve eylemlerinin sistematik olarak izlenmesi" biçiminde, Petersen "birisini veya bir şeyi izlemek ve bunları kayıt altına almak" olarak ve Ball/Webste: "insanlar, süreçler ve kurumlar hakkında bilginin kategorizasyonu, gözlemi ve kayıt edilmesi" biçiminde tanımlamaktadır. Aktaran, Muharrem Çetin/Sermin Asıl, "Günümüz Toplumunda Gözetim Olgusu", Üçüncü Sektör Sosyal Ekonomi, S. 52, C.1, [2017], s. 182 ve bu sayfada atıf yapılan yazarlar.
18) David Lyon, Gözetlenen Toplum, (Çev. Gözde Soykan), Kalkedon Yayınevi, İstanbul, [2006], s. 12-13.
19) Kirstie Ball, "Electronic Monitoring and Surveillance in the Workplace. Literature Review and Policy Recommendations", Publications Office of the European Union, Luxembourg, [2021], s. 10.
20) Elia Zureik, Theorizing Surveillance: The Case of the Workplace, Surveillance as Social Sorting Privacy, Risk and Digital Discrimination, (Ed. David Lyon), Routledge, London, [2003], s. 38.
21) https://sozluk.gov.tr/ (Erişim Tarihi: 04.06.2022).

"kişisel verilerin işlenmesine ilişkin her türlü işlem" unsurları ön plana çıkmaktadır. Bu kapsamda gözetlemeyi; kişiyi denetlemek, etki altına almak ve yönetmek amacıyla kişiye ait kişisel verilerin hemen veya sonra kullanmak üzere işlenmesine yönelik faaliyetler olarak tanımlayabiliriz[22]. İş hukukunda "elektronik gözetleme" ise; "elektronik nitelikli yardımcı araçların kullanımı ile işçinin durumu ya da davranış tarzları, yazıları, konuşmaları, hareketleri ile işçinin bağlantıda bulunduğu objeler ve işçinin çalıştığı işyeri bölümünün izlenmesi ve/veya kayıt altına alınması" biçiminde tanımlanmıştır[23]. Tanımda elektronik gözetleme, izleme ve kaydetme faaliyetlerini karşılayacak biçimde ele alınmıştır.

Gözetleme uygulamalarıyla denetim baskısı oluşturmanın işçilerin iş saatlerinde zamanı sadece iş görme borcunu ifaya ayırmalarını sağladığı ve bunun işyeri verimini artırdığına yönelik araştırma sonuçları gözetlemeyi iş ilişkisinin bir parçasına dönüştürmüştür[24]. Günümüzde gözetleme yoğun olarak bilişim sistemleri ve dijital izleme uygulamaları vasıtasıyla gerçekleştirilmekte ve bireyin izleme vasıtasıyla elde edilen verilerinin toplanması, işlenmesi, depolanması, geri getirilmesi, eşlenmesi ve pazarlanması gibi birçok süreci içinde barındırmaktadır. Ayrıca iş ilişkisinde işlenen bu veriler sadece işçinin iş görme borcunu ifa ettiği andaki faaliyetlerinden, isim veya iletişim bilgilerinden oluşmaz. İşçinin biyometrik verileri, genetik verileri, hastalık geçmişi, cinsel tercihleri, internet kullanım alışkanlıkları, internete erişimi olan nesnelerdeki dijital izleri gibi özel nitelikli kişisel verileri de içeren özel hayatın farklı katmanlarda yer alan verisi işlenmeye ve analize konu edilebilmektedir[25].

Önemle eklemek gerekir ki, gözetleme vasıtasıyla kişisel veri işleme faaliyetine ileride ele alınacak olan KVK hukuku düzenlemelerinin

22) Lyon, [2006], Gözetlenen Toplum, s. 2.
23) Zeki Okur, İş Hukukunda Elektronik Gözetleme, Legal Yayıncılık, İstanbul, [2013], s. 23.
24) Adriana Topo/Razzolini Orsola, "The Boundaries of the Employer's Power to Control Employees in the ICTs Age", Comparative Labor Law & Policy Journal, Vol. 39, No. 2, Winter, [2018], s. 391 vd.; Seumas Miller/John Weckert, "Privacy, the Workplace and the Internet", Journal of Business Ethics, Vol. 28, [2000], s. 256-257.
25) Lyon, [2013], Gözetlenen Toplum, s. 13.

uygulanabilmesi için bireyin verilerinin: "tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sistemini parçası olmak kaydıyla otomatik olmayan yollarla" işlenmesi gerekir[26]. Bu itibarla işyerinde insanlar tarafından gözle gerçekleştirilen gözetleme ve panoptikon gözetleme mimarisi birer gözetleme yöntemi olmasına rağmen bu faaliyetler kişisel verileri koruma mevzuatları kapsamında değerlendirilmez.

2. Gözetim

Gözetleme sözcüğü yerine "gözetim" sözcüğü kullanıldığı da görülmektedir[27]. Ancak "gözetim" nezaret, birisini, bir şeyi korumak ve himayesi altına almak anlamını barındırmaktadır[28]. Gözetim bu anlamıyla gözetlemenin diğer yüzü olan "korumak" anlamını yüklenmektedir[29]. Oysa gözetleme sadece korumak amacıyla gerçekleştirilmez. İş ilişkisi açısından bunun en tipik örneği işyeri güvenliğini sağlamak amacıyla gerçekleştirilen kamera gözetlemesidir. Güvenlik amaçlı kamera gözetlemesi bir yüzüyle işçinin güvenliğinin sağlanmasında gözetim; diğer yüzünde ise işçilerin işyerindeki faaliyetlerinin izlenmesi olanağını işverene vermektedir.

Ülkemizdeki gözetlemeye ilişkin çalışmalara baktığımızda "gözetim" kavramının hem bu olumlu anlamıyla hem de olumsuz anlam yüklenecek biçimde

---

26) Bir kişisel veri işleme faaliyetinin KVK hukuku kapsamında değerlendirilebilmesi için KVKK'nın kapsamını düzenleyen m. 2'deki kapsamda belirlenen koşullara uygun olması gerekir. Maddeye göre: "Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."

27) Mehmet Tekergül, İşyerinde Elektronik Gözetim Uygulamaları, Yüksek Lisans Tezi, Kadir Has Üniversitesi, [2010]; Fidan Karslıoğlu, Siber Gözetim: Toplumsal Denetim Aracı Olarak İnternetin Dönüşümü, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, [2014]; Uğur Dolgun, "Çalışma Yaşamında Gözetim", Sosyal Siyaset Konferansları Dergisi, S. 49, [2005}; F. Burcu Savaş, "İş Hukukunda Siber Gözetim", Çalışma ve Toplum, 2009/3, [2009]; Özgün Özger Bölükbaş, İnsan Hakları ve Elektronik Gözetim, Yüksek Lisans Tezi, Selçuk Üniversitesi, [2014]; İsmail Cem Bakır, Bilişim Çağında Toplu Gözetim ve Yasal Mevzuat Düzenlemeleri, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, [2020]; Neslihan Bulur, Gözetim Toplumu ve Yeni İletişim Teknolojileri: Z Kuşağı Üzerine Bir İnceleme, Yüksek Lisans Tezi, Galatasaray Üniversitesi, [2020].

28) Brian Martin, Antisurveillance, Information Liberation, Freedom Press, London, [1998], s. 115.

29) Lyon, [2013], Gözetlenen Toplum, s. 14.

hiyerarşik bir ilişkide birisinin diğerini dikizlemesi (gözetlemesi) anlamıyla kullanıldığı görülmektedir. Türk Dil Kurumu (TDK) "gözetim" sözcüğünü "gözetme işi, himaye, nezaret"; "gözetleme" sözcüğünü ise "gözetlemek işi, dikiz, dikizleme, erkete" ve "izleme" sözcüğünü ise, "takip" biçiminde tanımlamaktadır[30]. Aslında koruma, himaye gibi olumlu anlamlar barındıran gözetim sözcüğünü eylemi gerçekleştiren (gözeten) ile ilgili kişi (gözetilen) açısından değerlendirdiğimizde bu sözcüğün olumsuz bir anlam da barındıran dikizleme (gözetleme) sözcüğünü karşılamadığı aslında gözetlemenin sadece bir yüzü olan koruma anlamını taşıdığı anlaşılmaktadır[31].

3. İzleme

İngilizcedeki "monitoring" kelimesinin karşılığı olarak dilimizde "izleme" sözcüğü, "surveillance" kelimesinin karşılığı olarak da "gözetim" ve "gözetleme" sözcükleri kullanılmaktadır[32]. "Surveillance", Fransızca kökenli bir kelime olup, "üzerinde" anlamına gelen "sur" ve "gözetlemek" anlamına gelen "veiller" kelimelerinden türetilmiştir. "Veiller" kelimesi ise, Latincedeki "gözetlemek" anlamına gelen "vigilare" kelimesinden alınmıştır. Fransızca "surveiller" terimi "izlemek" ve "gözetlemek" anlamında kullanılmaktadır[33]. Yukarıda değerlendirildiği üzere yüklendiği anlam açısından gözetim kelimesinin kullanılması istenilen anlamı karşılamadığından "surveillance" sözcüğünün karşılığı olarak gözetleme sözcüğünün kullanılması daha uygundur.

ILO İşçilerin Kişisel Verilerinin Korunmasına İlişkin Uygulama Kodu'nda, izleme sözcüğünü: "bilgisayar, kamera, video ekipmanı, ses cihazı, telefon ve diğer iletişim ekipmanı gibi cihazların kullanımını, çeşitli kimlik ve konum belirleme

30) TDK Güncel Sözlük.
31) Graham Sewell, "The Discipline of Teams: The Control of Team-Based Industrial Work Through Electronic Surveillance", Administrative Science Quarterly, Vol. 43, [1998], s. 399.
32) https://www.oxfordlearnersdictionaries.com/definition/english/surveillance?q=surveillance (Erişim Tarihi: 01.12.2021).
33) Ian Kerr/Steve Mann, "Exporing Equiveillance", January 1, [2006], http://wearcam.org/anonequiveillance.htm.

yöntemlerini veya diğer herhangi bir gözetleme" yöntemini içerdiğini belirtmiş ancak izlemenin bunlarla sınırlı olmadığını vurgulamıştır[34].

İş ilişkisinde bazen yasal bir yükümlülüğü yerine getirmek, bazen de işyeri güvenliğini sağlamak ve iş verimliliğini artırmak amacıyla izleme uygulamaları kullanılabilmektedir. Genel bir kavram olan "izleme" sözcüğü kişisel verilerin işlenmesini gerektirdiğinden, işçinin özel hayat alanında bulunan verilerin işlenmesi ve kişisel verilerin işyeri veya işyeri dışında iş ilişkisi sınırlarını aşacak yoğunlukta elde edilmesi, kaydedilmesi, veri tabanlarında depolanması, aktarılması gibi kişisel veri işleme süreçlerini ortaya çıkarmaktadır. Bunun bir sonucu olarak kişiye ve onun kişilik haklarına yönelen ihlalin boyutu çeşitlenmekte, sadece kişiyi ve onun maddi mal varlığını korumaya odaklanmış hukuki koruma yöntemleri kişisel verileri korumakta yetersiz kalmaktadır[35].

İzlemeyi uygulama yöntemi ve amacı açısından gruplandırarak fiziksel izleme, psikolojik izleme ve teknik izleme olarak üç grup kapsamında da değerlendirilmiştir. Buna göre bir işçinin konumunun, eylemlerinin, konuşmasının veya özel yazışmalarının bilgisi veya iradesi dışında kamera, ses kayıt cihazları gibi araçlarla izlenmesi fiziksel gözetlemedir. Psikolojik izlemede sözlü veya yazılı testler kullanılır ve işçinin isteyerek vermediği veya ifşa ettiğini bilmediği ya da üzerine düşünmeden ifşa ettiği kişisel verilerin çıkarım yapmak amacıyla işlenmesi söz konusudur. Teknik izleme ise, kişi veya kişi grupları hakkındaki verilerin bilgisayar gibi veri işleme cihazları tarafından toplanması, aktarılması ve analizlere konu edilmesi biçiminde gerçekleşir[36].

---

34) ILO, "Protection of Worker's Personal Data", https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf, [1997], s. 1, (ILO, Personal Data, 1997), (Erişim Tarihi: 21.09.2021).
35) Samuel D. Warren/Louis D. Brandeis, "The Right to Privacy", Harvard Law Review, Vol. 4, No. 5, December [1890], s. 193.
36) Alan F. Westin, Privacy and Freedom, New York, Atheneum, [1967], s. 68.

4. Kavramların Kapsamları ve Dijital İzlemenin Tanımlanması

Günümüz toplumunu ifade etmek için kullanılan post-modern toplum, bilişim toplumu ve bilgi toplumu gibi kavramlar toplumsal değişimin yönüne işaret ederken "gözetleme toplumu[37]" ve "dijital izleme" kavramları ise, anılan toplumsal değişimlerden kaynaklı gelişmelerin ortaya çıkardığı araçların kullanılması sürecine gönderme yapmaktadır[38]. Bundan dolayı dijital izleme teknolojik gelişmelerin ortaya çıkardığı toplumsal yapının bir uygulaması ve denetim aracıdır.

Gözetlemenin, dijital izlemeye uygulamalarıyla gerçekleştirildiği günümüzde özel hayatın gizliliğinin ve kişisel verilerin korunmasına ilişkin önemli koruyucu düzenlemeler geliştirilmiştir. Öte yandan, dijital uygulamalar sayesinde özel hayat alanında kalan verilerin ve kişisel zamanların izlenebilmesi gerçekliği karşısında öngörülen hukuki düzenlemelerin koruyuculuğu üzerine yeniden düşünülmelidir[39]. Zira büyük veri analitiği, akıllı profilleme (insan analitiği) iletişimi yakalama uygulamaları, mobil cihazları izleme; genetik veriler, DNA testi ve biyometrik veriler vasıtasıyla izleme ve konum izleme örnekleri günümüz işverenleri tarafından hem işyerinde hem de işyeri dışında, hatta iş saatleri dışında kullanılabilmektedir[40].

Bu özelliğinden dolayı izleme kavramı daha geneldir ve gerçekleşme amacına bakılmaksızın iş ve işyeriyle ilgili süreçlere uygulanan tüm otomatik veya yarı otomatik veri işleme faaliyetlerini kapsamaktadır[41]. Gözetleme ise dar bir uygulama olarak hiyerarşik bir ilişkide daha çok gerçek kişiler ve optik sistemler

37) Lyon, "gözetlenen toplumlar" kavramını toplumsal kontrolü gerçekleştirmek ve yönetme işlevi için, bilişim teknolojilerine bağımlı olan bütün toplumları nitelendirmek için kullanmaktadır. Lyon, [2006], Gözetlenen Toplum, s. 11.
38) Lyon, [2006], Gözetlenen Toplum, s. 17.
39) Robert Sprague, "Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees", John Marshall Law Review, Vol. 42, No. 1, Fall, [2008], s. 88.
40) Sprague, [2008], Orwell Was an Optimist, s. 88-89.
41) James Rule/Peter Brantley, "Computerized Surveillance in the Workplace: Forms and Distributions", Sociological Forum, [1992], Vol. 7, No. 3, s. 420.

vasıtasıyla gerçekleştirilen izlemeyi ifade etmektedir[42]. Ayrıca gözetleme bir kişi veya grup hedef alınarak gerçekleştirilebilir ve esas olarak gözetlemede olumsuz bir davranışı engellemek veya bir suça ilişkin kanıt elde etme amacı bulunur[43].

İzleme kavramı genel bir kavram olarak gözetleme süreçleri dahil teknik tüm imkanlar kullanılarak gerçekleştirilen kişisel veri işleme faaliyetini ifade etmektedir. Bu özelliğinden dolayı izleme kişilerin, yerlerin, nesnelerin ya da süreçlerin sistematik, devamlı ve aktif veya pasif olarak takibini içeren tüm süreçleri kapsayan genel bir kavramdır. Örneğin işverenin, müşteri hizmetleri departmanı işçilerinin müşterilere verdiği cevapları inceleyerek hizmetin kalitesini ölçmek ve iyileştirmeler gerçekleştirmek amacıyla e-postaları izlemesi dijital izlemedir.

Önemle eklemek gerekir ki, bir kişisel veri işleme faaliyetinin dijital izleme olarak nitelendirilmesi için gerçekleştirilen izlemenin amacının bir belirleyiciliği bulunmamaktadır. Örneğin dijital izlemenin işçinin performansının ölçülmesi, bilgisayarda geçirdiği aktif sürenin harekete duyarlı dijital uygulamalarla takip edilmesi, işyeri güvenliği için belirli yerlerin kamera ile gözetlenmesi veya işverenin merakını gidermesi amacıyla gerçekleştirmesi bir farklılık oluşturmaksızın dijital izleme faaliyetini ortaya çıkarmaktadır[44]. Bu sebeple dijital izleme işçilerin iş dışındaki hayat alanlarını izleyebilme, yoğun kişisel veri işleme, basit, ucuz ve belirlenmesi güç dijital uygulamalarla gerçekleştirilebilme, tüm süreçleri kayıt altına alabilme ve profillemeyle işçileri detaylı analizlere konu edebilme özellikleriyle farklılaşmaktadır. Bu özelliklerinden dolayı dijital izleme uygulamaları kullanıldığında işçinin hayat alanları üzerindeki ihlalinin boyutu

42) Mihaela Vorvoreanu/Carl H. Botan, "Examining Electronic Surveillance in the Workplace: A Review of Theoretical Perspectives and Research Findings, in Acapulco", Mexico, [2000]. s. 3-4.
43) Carl Botan, "Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects", Communication Monographs, Vol. 63, No. 4, [1996], s. 294; https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/monitoring-and-surveillance (Erişim Tarihi: 22.09.2021).
44) Okur, [2013], Elektronik Gözetleme, s. 23-24.

çeşitlenebilmektedir[45].

AİHM'in iş ilişkisinden doğan ihtilaflara ilişkin olan kararlarına baktığımızda "gözetleme" ve "izleme" kavramlarının birbirinin yerine geçecek biçimde kullanıldığı görülmektedir[46]. Öte yandan örneğin López Ribalda ve Diğerleri & İspanya kararında AİHM delil elde etmek amacıyla gizli kamera gözetlemesi gerçekleştirilmesini tanımlamak için gözetleme (surveillance) sözcüğünü tercih ederken, genel bir takibi tanımlarken izleme (monitoring) sözcüğünü kullanmaktadır[47]. Anayasa Mahkemesi (AYM) kararlarına baktığımızda dijital izleme, izleme ve gözetleme kavramlarına ilişkin bir ayrım yapılmadığı, dijital izleme olarak nitelendirilecek olayları özel hayatın gizliliğinin korunması, kişisel verilerin korunması ve haberleşme hürriyeti çerçevesinde değerlendirmelere konu edildiği görülmektedir[48].

Kavramlara ilişkin tanımları değerlendirdiğimizde iş ilişkisinde izleme, gözetleme uygulamalarını da içeren, işçi ve yaptığı işle ilgili her türlü verinin kişisel zaman da dahil olabilecek şekilde teknolojik sistem ve uygulamalar vasıtasıyla işlenmesini ifade etmektedir[49]. Bu kapsamda iş ilişkisinde dijital izlemeyi; bilişim uygulamaları, internete entegre nesneler, algoritmik sistemler, konum belirleme sistemleri, optik teknolojiler ve giyilebilir akıllı zeka destekli sistemlerle işçinin işyerindeki veya kişisel zamanındaki kişisel veri içeren faaliyetlerini, davranışlarını, çalışma biçimini, dinlenme araları alışkanlıklarını, genel durumunu, yazılarını, internet trafik izlerini, görüntü – ses verilerini, yaşam rutinlerini belirli

45) Sam Sarpong/Donna Rees, "Assessing The Effects Of 'Big Brother' in A Workplace: The case of WAST", European Management Journal, Vol.32, Issue 2, April, [2014], s. 217-218.
46) Antovic and Mirkovic v. Montenegro, no. 70838/13, §8 AİHM, 2017; Bărbulescu v. Romania, app no 61496/08, AİHM, 2017; Halford v. the United Kingdom, app no 20605/92, 25 June 1997.
47) López Ribalda and Others v. Spain, 1874/13 and 8567/13, Judgment 17.10.2019, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12630%22]}.
48) AYM, Yasemin Çongar ve Diğerleri, Başvuru No: 2013/7054, 6.1.2015; AYM, E.Ü. kararı, Başvuru No: 2016/13010, 17.09.2020.
49) Sarpong/Rees, [2014], Big Brother' in A Workplace, s. 216.

bir amaç kapsamında veya soyut olarak işleme[50] faaliyeti olarak tanımlayabiliriz.

II. Gözetlemenin İşyerinde Kullanılma Seyri ve İş İlişkisindeki Etkileri

Tarih boyunca hiyerarşik iktidar alanı kurmak veya iktidar alanını korumak isteyen taraf bir şekilde toplumu, rakiplerini ve işçileri gözetlemenin yolunu aramıştır. Bu sebeple işçilerin izleme araçlarıyla denetim altına alınmasının günümüze özgü yeni bir uygulama olmadığını belirtmek gerekir.

1. Gözetlemenin Tarihsel Gelişimi

Sanayileşmeyle birlikte geleneksel gözetlemenin dönüştüğünü belirten Marx, sistematik gözetlemenin emek ve sermaye arasındaki mücadelenin bir unsuru haline geldiğini belirtir[51]. Jeremy Bentham ise, panoptikonda önerdiği merkezi gözetleme modelinin[52] sadece hapishanelerde değil aynı zamanda fabrikalarda, işçi evlerinde denetimi ve verimi artırma aracı olarak kullanılabileceğini ileri sürmüştür[53]. Bu kapsamda işverenin, işçiye yönelik otoritesinin somutlaşma biçimlerinden birisi olan dijital izlemenin iş ilişkisindeki yeri ve etkisi teknolojik gelişmelerle artmıştır.

İzlemenin aygıtı olarak tasarlanan panoptikon, Foucault'nun analizleri sebebiyle daha çok iktidarların hapishaneleri gözetlemesi ve Jeremy Bentham ile ünlenmiş olmasına rağmen aslında panoptikon ile işçileri denetim altında tutmanın

---

50) KVKK m. 3/1-e bendinde kişisel verilerin işlenmesi: "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi" biçiminde tanımlanmıştır.
51) Lyon, [1997], Elektronik Göz, s. 20.
52) Maša Galic/Timan Tjerk/Bert-Jaap Koops, "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation", Philosophy & Technology, Vol. 30, Issue 1, [2016], s. 9-37.
53) Armand Mattelart, Gözetimin Küreselleşmesi Güvenlileştirme Düzeninin Kökeni, (Çev. Onur Gayretli/Su Elif Karacan), Kalkedon Yayınları, İstanbul [2012], s. 14.

mimari tasarımı Samuel Bentham'a ait olup, işyerlerinin verimini artırma ve işçileri denetleme düşüncesinden ortaya çıkmıştır. Samuel Bentham tarafından 1789 yılında tasarlanan panoptikon, merkezi gözetleme ilkesine dayanarak işçilerin işyerinde denetim altında tutulması amacını taşımaktadır. Rusya ziyaretinde, kardeşinin işyerlerini gözetleyerek verimi artırmak için tasarladığı projeden etkilenen Jeremy Bentham ise, panoptik yapının içerisinde oluşturulacak sistemin felsefi boyutunu ortaya koymuştur[54].

İşyerleri için önerilen bir model olan ve gözetlemeye ilişkin çalışmalara kaynaklık eden Bentham'ın panoptikon gözetleme modeli, Foucault tarafından yoğun incelemeye tabi tutmuş ve üne kavuşması sağlanmıştır. Foucault'ya göre kullanım amacı ne olursa olsun bu yapıda gözetlemenin tüm açıklığıyla gerçekleştirilmesi için merkezi kuleye bir gözlemci yerleştirmek ve işyerine işçileri kapatmak yeterlidir[55]. Bu bağlamda Foucault'nun Hapishanenin Doğuşu isimli eserindeki analizler ve disiplin toplumu ile kontrol toplumu ayrımında değindiği işyerinde gözetlemenin "hem üretim aygıtının bir iç parçası, hem de disiplinsel iktidarın uzmanlaşmış bir çarkı olduğu ölçüde, belirleyici bir ekonomik işlemci[56]" haline geldiği tespiti temelde gözetlemenin disipline edici ve hiyerarşik iktidar kurmadaki etkisine vurgu yapmaktadır. Bu vurgu aslında işyerinin, işçi ile işveren arasındaki güç ilişkisini hiyerarşik olarak ortaya çıkarması ve hukuki olarak şekle büründürmesi özelliğiyle de örtüşmektedir[57].

---

54) Catherine Pease-Watkin, Bentham'ın Panoptikon'u ve Dumont'un Panoptique'i, (Ed. Barış Çoban/Zeynep Özarslan), Panoptikon: Gözün İktidarı, Su Yayınları 2. Baskı, İstanbul, [2016], s. 78-79; Jeremy Bentham, Panoptikon ya da Gözetim-Evi, XVIII. Mektup - Fabrikalar, (Ed. Barış Çoban/Zeynep Özarslan), Panoptikon: Gözün İktidarı, Su Yayınları 2. Baskı, İstanbul, [2016], s. 61.

55) Foucault, panoptikonu şu şekilde betimlemiştir: "Halka şeklinde bir bina ve ortasında bir kule ve kuleden halkanın iç cephesine bakan geniş pencereler… Kuleye bakan bina hücrelere ayrılmıştır. Hücrenin her biri bina boyunca derinlemesine uzanır. Bu hücrelerin iki penceresi vardır. Biri içeriye doğru açıktır, kulenin pencerelerine denk diğer, diğeri dışarıya bakarak, ışığın bir baştan bir başa hücreyi kat etmesini sağlar. Bu durumda merkezi kuleye bir gözlemci yerleştirmek ve her bir hücreye bir deli, bir hasta, bir mahkûm, bir işçi ya da bir öğrenci kapatmak yeterlidir." Michel Foucault, İktidarın Gözü, Seçme Yazılar, (Çev. Mehmet Ali Kılıçbay), Yapı Kredi Yayınevi, İstanbul, [2007], s. 86.

56) Michel Foucault, Hapishanenin Doğuşu, (Çev. Mehmet Ali Kılıçbay), İmge Kitabevi, [1992], s. 220.

57) Kübra Doğan Yenisey, İş Hukukunda İşyeri ve İşletme, Alman ve Fransız Hukuklarıyla Karşılaştırmalı Bir İnceleme, Legal Yayıncılık, İstanbul, [2007], s. 77.

George Orwell'in 1984[58] isimli distopik romanındaki her şeyi gözetleyen büyük biraderin gözü gözetlemenin totaliter yönünü hatırlatarak "kafatasınızın içindeki birkaç santimetreküp dışında, hiçbir şeyin"[59] bize ait olmadığını vurgulamaktadır. Huxley'in Cesur Yeni Dünya[60] isimli eserindeki her şeyi kurgulayan, gözetleyen ve şartlandırıcı kişilikler oluşturan iktidar şekli ve birçok merkezde kamera gözetlemesine olanak veren Synoptikon kavramı da temelde hegemonik iktidar alanlarına ve iktidarın oluşturulmasında en önemli aygıtlardan birisi olan gözetleme olgusuna gönderme yapmaktadır.

Günümüzde bilişim sistemleri, gelişen algoritmalar ve yapay zeka teknolojisi gözetlemeyi farklı bir boyuta taşımış ve toplu izlemenin önemli şekilleri olan omniptikon[61] olarak adlandırılan dijital izleme olgusu ortaya çıkmıştır. Toplumsalın bu aşamasında dijital izleme, tüketici veya işçi fark etmeksizin "manipüle edilen gönüllü", verilerini paylaşmaya hevesli iş birliği içinde kişilerin katkısıyla devam etmektedir[62].

2. İşyerlerinde Gözetlemenin Araçsallaşması: Bilimsel Yönetim İlkeleri ve Ford Sosyoloji Departmanı

Günümüzde yoğun olarak dijital izleme kavramıyla gündeme gelen işçiyi gözetleyerek denetim altında tutma ve izlemeyle işyeri verimini artırma düşüncesi yeni bir uygulama değildir. Örneğin işyerinde verimliliği artırmak için bilimsel

58) George Orwell, Bin Dokuz Yüz Seksen Dört, Çev. Celal Üster, Can Yayınları, [2021], s. 51-52.
59) Orwell, [2021], Bin Dokuz Yüz Seksen Dört, s. 51.
60) Aldous Huxley, Cesur Yeni Dünya, Çev. Ümit Tosun, İthaki Yayınları, [2021], s. 23 vd.
61) Robert D. Sprague, "From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace", The John Marshall Journal of Information Technology & Privacy Law, Vol. 25, Issue 1, Winter, [2007], s. 2; Jeffrey Rosen'in kullandığı "omniptikon" kavramı herkesin her zaman ve her yerde bilgisayar ağları vasıtasıyla herkesi toplu şekilde izlenmesini ifade etmektedir. Omniptikon sosyal ağların yaygınlaşmasıyla birlikte bireyin kendisini, kişisel verilerini gönüllü olarak kamuya açması sonucu yaygınlaşmıştır. Sinoptikon ise küçük bir grubun veya tek bir bireyin büyük bir çoğunluk tarafından izlenmesi halidir. Özellikle sosyal medyadaki influencer olarak ifade edilen kişilerin çokluk tarafından izlenmesi buna örnek gösterilebilir.
62) Zygmunt Bauman/David Lyon, Akışkan Gözetim (Çev. Elçin Yılmaz), 2. Basım, İstanbul, [2016], s. 150.

yöntemin kullanılmasını öneren Frederick Taylor, 1911 yılında yayımlandığı "Bilimsel Yönetim İlkeleri" isimli kitabında işyerinde verimliliğin artırılması için yapılması gerekenleri sıralamıştır.

Bilimsel yönetim yaklaşımında işçiler üzerinde mekanik bir disiplin oluşturularak kronometreli bir yönetici tarafından sürekli gözetlemeye tabi tutuluyordu. Yönetici, işçileri sadece zaman açısından ölçmekle yetinmiyor aynı zamanda devamlı gözetliyor, baskılıyor, denetliyor ve işçilere direktifler veriyordu[63]. Taylorizm olarak isimlendirilen bu yönetim biçiminin denetimsel gözetlemeyi büyük ölçüde gerçekleştirmeyi başardığı kabul edilmektedir[64]. İşçiler bu yönetim biçiminin ortaya çıkardığı denetim sebebiyle Taylorizmin gözü altında olduklarını hissederek iş görme borçlarını ifa etmek durumunda kalmışlardır[65].

İş süreçlerine mekanik hale gelmesi ve seri üretim gibi birçok yeniliğe imza atan Henry Ford ise, 20. yüzyılın başında Ford Motor Company isimli şirketinde Taylor'un yöntemlerini de kullanarak geliştirdiği işyeri modelinde üretim ve tüketimi yönetecek şekilde işçileri yoğun gözetleme altına tutacak yöntemler geliştirmiştir[66].

Ford Şirketi, işyerinde gözetlemeye dayalı denetimi yoğun olarak kullanırken, işçilerin iş yaşamı dışındaki yaşamını denetim altında tutmak için Ford Şirketi Sosyoloji Departmanı'nı kurmuştur. Sosyoloji Departmanı, işçilerin "Amerikan standartlarına" göre yaşayıp yaşamadıklarını araştırmak ve onlara karşı belirli politikalar belirlemek için özel hayatlarını aşırı biçimde gözetleyecek yöntemler uygulamıştır. Öyle ki işçilerin medeni halleri, işyerindeki davranışları,

63) Sprague, [2007], From Taylorism to the Omnipticon, s. 1-2; Lyon, [2016], Elektronik Göz, s. 54.
64) Lyon, [2016], Elektronik Göz, s. 168.
65) Lyon, [2016], Elektronik Göz, s. 166-168; Sprague, [2007], From Taylorism to the Omnipticon, s. 2.
66) Charlie Chaplin, Modern Times (Modern Zamanlar/Asri Zamanlar - 1936) isimli filminde işyerinde seri üretim sisteminin ve gözetlemenin işçiyi üretim aygıtının mekanik seri bir parçası olarak görülmesini ve işçinin bu beklenti karşısında içine düştüğü durumu gülünç bir şekilde ortaya koymuştur.

yaşam koşulları ve eğlence biçimleri gibi özel hayatın her katmanını ilgilendirebilecek kişisel veriler işlenmiş ve bunları kayıt altına alacak politikalar geliştirmiştir[67].

Bilimsel yönetim ilkeleri ve Ford Şirketi'nin işçileri gözetlemeye ilişkin yaklaşımlarıyla aynı dönemlerde Avrupa'da gözetlemeyi işyeri verimi ve kontrol için fonksiyonel gereklilik olarak kabul eden yönetim teorileri ortaya çıkmıştır. Örneğin, günümüzde yönetime ilişkin ders kitaplarında teorilerinin etkileri görülen ve modern yönetim teorisinin kurucularından birisi kabul edilen Henri Fayol, 1916'da yayımladığı "Genel ve Endüstriyel Yönetim" isimli yönetsel teorisinde işyerinde planlama, denetleme ve kontrol etmeyi (gözetleme) yönetim ve verimlilik fonksiyonları olarak tespit etmiştir[68].

Günümüzde işverenlerin işçilerin mesai saatlerindeki davranışlarını izlemek ve analiz etmek için kullandığı dijital izleme uygulamaları sebebiyle "Dijital Taylorizm" olarak nitelendirilen uygulamalar ortaya çıkardığı ileri sürülmektedir[69]. Bu anlamıyla dijital izleme iş ilişkisinin her yerindedir ve işçi farkında olmadan günlük yaşamının birçok alanına ilişkin veri işlemektedir[70]. Zira işçinin işini yapmasına olanak sağlayan Wi-Fi ve Bluetooth sinyalleri, GPS (Global Positioning System / Küresel Konumlama Sistemi) çipleri, otomatik plaka okuyucular, bilgisayar ağ verileri, internet protokol veri tabanları, finansal işlemler, tüketici alımları, kapalı devre kameralar, uzaktan biyometrik tanımlama ve insansız hava sistemleri işçi hakkında bilgi toplamaya yönelik bu yöntemler toplu olarak kişisel veri işlemekte ve işçilerin yaşam pratikleri hakkında derinlemesine bilgi

67) Stephen Meyer, "Adapting the Immigrant to the Line: Americanization in the Ford Factory, 1914-1921", Journal of Social History, Vol. 14, Issue 1, [1980] s. 1.
68) Vladimir Simic, "Managing Modern Enterprises", International Journal of Economics and Law, Vol.3, [2013], s. 138.
69) Daniel Susser/Beate Roessler/Helen Nissenbaum, "Online Manipulation: Hidden Influences in Digital World", Georgetown Law Technology Review, Vol.4, Issue 1, [2019], s. 30.
70) Robert G. Boehmer, "Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise form the Modern Sweatshop", DePaul Law Review, Vol. 41, Issue 3, [1992], s. 267.

sağlamaktadır[71].

3. Gözetlemeden Dijital İzlemeye İş İlişkisinde Denetimin Dönüşümü

Hiyerarşik bir iktidar alanı oluşturarak kontrol ve denetim olanağı sağladığından şekli, yoğunluğu ve uygulama alanı tarihsel süreç içinde değişmekle birlikte gözetlemenin iş ilişkisinde kullanılmasının insanlık tarihi kadar eskiye dayandığı anlaşılmaktadır[72]. Bu kapsamda gözetlemenin ve izlemeye dayalı denetimin işe alım ve iş süreçlerinin her zaman bir parçası olduğunu söyleyebiliriz.

a) İşverenin Denetim Aracı Olarak İzleme

Toplumsal gelişim sürecinde insanlar çeşitli sosyal ilişkiler kurarak yaşamlarını sürdürseler de bu insanların özgürlüklerinden vazgeçtikleri ve kamuya açtıkları özel hayat alanlarını alenileştirdikleri anlamına gelmez[73]. Zira kişinin özel hayat alanlarının bulunduğu ve bunların korunması fikri insanlık tarihi kadar eskiye dayanmaktadır. İlkel toplumlarda da kişinin mahremiyet alanının bulunduğu ve bazı mesleklerde kişisel verilerin korunması gerektiği[74] kabul görmüştür. Öte yandan, özel hayat[75] kavramının tüm toplumlarda aynı anlamı ifade eden doğal bir gerçeklik olmadığını, farklı toplumlarda ve farklı gruplar açısından çeşitli içeriklere gönderme yapan tarihsel bir kavram olduğunu belirtmek gerekir[76].

---

71) Allison Amatuzzo, "Wherever We Go, We Leave a Trail: Surveillance and Sousveillance in the United States and United Kingdom", Penn State Journal of Law and International Affairs, Vol. 7, Issue 2, [2019], s. 494.
72) Lyon, [2016], Elektronik Göz, s. 39.
73) Val Collins, "Privacy in the United Kingdom: A Right Conferred by Europe", International Journal of Law and Information Technology, Vol. 1, No. 3, Spring, [1994], s. 291.
74) Bunun en çarpıcı örneği geçmişi günümüzden 2500 yıl önceye dayanan Hipokrat yeminidir. Hipokrat yemininde doktorların hastalarının özel hayatlarına ilişkin elde ettiği verileri saklama ve açıklamama yükümlülüğü bulunmaktadır. Doktorların sır saklama yükümlülüğü tarihsel süreç içerisinde memur, avukat, bankacı gibi meslekler açısından da ortaya çıkmıştır. Oğuz Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayınları, İstanbul, [2008], s. 6.
75) Sultan Üzeltürk, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, Beta Yayınevi, İstanbul, [2004], s. 2-3.
76) Antoine Post, Özel Hayatın Sınırları ve Alanları, (Ed. Philippe Aries/Georges Duby), Özel Hayatın Tarihi 5, Birinci Dünya Savaşı'ndan Günümüze, (Çev. Şehsuvar Aktaş), Yapı Kredi Yayınları, İstanbul [2010], s. 15.

Tarihsel süreç içerisindeki görünümleri açısından gözetleme modern öncesi dönemlerde inşaatta, hayvancılıkta ve sulama kanallarında çalışan işçileri denetlemek, vergi toplamak ve vergi süreçlerini kayıt altına almak, göçebeleri denetim altında tutmak, düşmanların gücünü tespit etmek, savaşlara hazırlanmak gibi amaçlarla kişi temelli gerçekleştirilmiştir[77]. Bu denetim biçimi bazı gruplara ilişkin bilginin yönetilmesi imkanını ortaya çıkardığından aynı zamanda onları denetim altında tutma, iş gücünün başka kaynaklarda kullanılması olanağını beraberinde getirmiştir[78].

Gözetlemenin ortaya çıkardığı bu olanağın bir sonucu olarak gözetleme, modernite öncesi dönemlerde toplulukların, imparatorlukların, monarşilerin ve dinlerin esaslı bir denetim mekanizması olarak işlev görmüş toplumun, işgücünün ve kölelerin denetiminde önemli araçlardan birisi olarak kullanılmıştır[79]. Bu dönemde iktidarlar, din otoriteleri ve ekonomik gücü elinde bulunduran sınıflar çok geniş gözetleme yetkilerini kullanmışlardır[80]. Özellikle kölelerin çalıştırılması için yapılan düzenlemeler, kolonilerdeki tarım işgücünün izlenmesi, halkın kabilelere göre ayrılması, göçebelerin takip edilmesi, topluluğun yaşlarının ve isimlerinin kayıt altına alınması gözetleme pratiklerinin örnekleridir[81].

Matbaanın icadıyla birlikte devletler gözetlemeyi mekanik olarak kaydetme, belge ve metinlere geniş çapta ulaşabilme olanağını yakalamıştır. Bunun bir sonucu olarak gözetlemeye dayalı bir hiyerarşik ilişki ortaya çıkmış ve devletin gözetlemesi kurumlar üzerinde bir baskı aracına dönüşmüştür[82]. Ulus devletlerin ortaya çıkması ve sanayi devriminin etkisiyle gözetlemede teknik imkanlar da

77) Giddens, [2008], Ulus Devlet, s. 25-26;
78) Giddens, [2008], Ulus Devlet, s. 8; Dalibor Petrovıć, "The Ethics of Employees' Surveillance in the Context of Rapid ICT Development", The 4th International Conference Mechanical Engineering in XXI Century, April 19-20 [2018], s. 20; Uğur Dolgun, Şeffaf Hapishane Yahut Gözetim Toplumu, Ötüken Yayınları, İstanbul, [2008], s. 21.
79) Petrovıć, [2018], s. 20; Dolgun, [2008], Gözetim Toplumu, s. 21.
80) Alan Westin, The Origins of Modern Claims to Privacy, Philosophical Dimensions of Prvacy an Anthology, Ed. Ferdinand D. Schoeman, Cambridge University Press, [1984], s. 70.
81) Lyon, [2016], Elektronik Göz, s. 39-40.
82) Giddens, [2008], s. 66, 236-237.

kullanılmaya başlanmış ve toplumsalın bu evresinde gözetleme kamusal alanda bürokrasi, işyerlerinde ise bilimsel yönetim ilkeleri[83] olarak ifade edilen yönetim biçimleriyle uygulanmıştır. Bu dönemde işçilere yönelik disipline edici sıkı gözetleme ve denetim pratikleri uygulanarak üretim ve kârlılığın artırılması hedeflenmiştir. Sanayi devrimiyle birlikte ekonomide ve toplumsal yapıda gerçekleşen değişimler aynı zamanda insanların yaşama biçimlerini ve kentleşmeyi hızlandırmış, üretim geleneksel el emeği, tezgah üretiminden farklılaşarak makine seri üretimine dönüşmüştür. Böylelikle sermaye yoğunluklu işletmeler, işyeri, işçi ve işveren gibi iş hukukunu ilgilendiren birçok yeni kavram türemiştir[84].

Sanayi Devrimi'nin ortaya çıkardığı bu gelişmelere ve kitle iletişim araçlarının yaygınlaşmasına koşut olarak toplumda yeni mimari formlar, ev eşyaları, günlükler, mektuplar ve romanlar bir arzuyu yansıtmaya başladıkça, özel hayatın gizliliğinin korunması (privacy) gündeme gelmeye başlamıştır[85]. Bunda fotoğrafların haberlerin standart aksesuarı haline gelmesinin etkisi bulunmaktadır.

Bu dönemde özel hayatın gizliliğinin korunmasına yönelik ihlaller haksız fiil olarak görülmüş ve ceza yasalarını da içerecek şekilde çeşitli korumalarla korunmaya çalışılmıştır. Örneğin postalarda ve telgraf mesajlarında özel mektupların açılmasına karşı yasaklar, itirafçıların gizlilik içeren açıklamalarının korunması, makul olmayan arama ve el koymaya karşı yasal korumalar içeren düzenlemeler bir yönüyle özel hayatın gizliliğini korumada da rol üstlenmiştir. Tüm

83) Sprague, [2007], From Taylorism to the Omnipticon s. 2; Giddens, [2008], s. 66, 276-277.
84) Sarper Süzek, İş Hukuku, Beta Yayınevi, 18. Baskı, İstanbul, [2019], s. 6-36; Ali Güzel/Hande Heper, Sürekli İstihdamdan Geçici Atipik İstihdama! Mesleki Amaçlı Geçici İş İlişkisi, Çalışma ve Toplum, S.1, [2017], s. 13; Ünal Narmanlıoğlu, İş Hukuku - Ferdi İş İlişkileri, Beta Yayınevi, 5. Baskı, İstanbul [2014], s. 5; Ramazan Arslan/Havanur Ergün, John Hicks'e Göre Tarım Merkantilizminden Sanayi Devrimine Emeğin Evrimi, Hak İş Uluslararası Emek ve Toplum Dergisi, C. 1 S. 1, Ankara, [2012], s. 122-123, https://dergipark.org.tr/tr/download/article-file/84746; Nuri Çelik/Nurşen Caniklioğlu/Talat Canbolat, İş Hukuku Dersleri, Beta Yayınevi, 31. Baskı, İstanbul, [2018], s. 4-5.
85) Vernon Valentine Palmer, "Three Milestones in the History of Privacy in the United States", Tulane European and Civil Law Forum, 26, [2011], s. 72; Robert E. Mensel, Kodakers Lying in Wait Amateur Photography and the Right of Privacy in New York, 1885-1915 American Quarterly, Vol. 43, No. 1, March, [1991], s. 27.

bu gelişmeler özel hayatın gizliliğinin korunması fikrinin gelişimine uygun bir ortam ortaya çıkardığından, 19. yüzyıl aynı zamanda özel hayatın gizliliğinin korunması fikrinin gelişiminde büyük sıçramaların yaşandığı bir yüzyıl olmuştur. Bunda yaygınlaşan basının özel hayatın gizliliğini hiçe sayan yaklaşımlarının etkisi büyüktür[86].

Sözleşme özgürlüğünü zayıf taraf olan işçi lehine sınırlandırma düşüncesine dayanan ve temelde sanayi devriminin bir ürünü olan iş hukuku büyük ölçüde fabrika temelli üretim ve bu çevrede ifa edilen iş ilişkilerini esas alarak gelişmiştir. Günümüzün bilişim toplumunda bu modelin yerini hizmet sektörü temelli vasıflı işgücü almış, işyerinin sınırları ile işin yapılma ve takip edilme şekli önemli değişime uğramıştır[87]. Zira beşeri ilişkilere dayanan gözetleme döneminde başka bir gerçek kişi tarafından gerçekleştirilen, sanayi devrimiyle daha teknik bir niteliğe bürünen gözetleme işyerinde işverenin veya görevlendirdiği bir işçi vasıtasıyla fiili denetim şeklinde icra edilmiştir. Günümüzde ise dijital teknoloji, yazılımlar ve çeşitli yapay zeka uygulamaları sayesinde işçilerin çoğunlukla farkında olmadan dahil olduğu, işçi hakkında birçok verinin işlendiği, analiz edildiği ve bu uygulamaların işçilerin gündelik hayatının bir parçası haline geldiği dijital izleme olgusu ortaya çıkmıştır.

Bu olgu günümüz veri gizliliği uzmanlarını, veri işleyen veri sorumlularının birey davranışları, tercihleri, ilgi alanları, gelirleri ve benzeri konularda topladıkları verilerle bireyi yönlendirebilmek için kullanabilecekleri hususunda giderek daha fazla endişeye sevk etmektedir. Örneğin, Uber firmasının "ekonomiyi paylaşmak" gibi bir slogan altında sadece müşterilerin değil, aynı zamanda şoförlerin davranışlarını da yönlendirecek veriler topladığı; bu verilerle sürücü davranışlarını kârlılıklarını artırmak için kullandırabilecek dijital izleme uygulamaları tasarladığı

86) Palmer, [2011], History of Privacy, s. 69-73.
87) Ali Güzel, Fabrikadan İnternete İşçi Kavramı ve Özellikle Hizmet Sözleşmesinin Bağımlılık Unsuru Üzerine Bir Deneme, Kamu-İş İş Hukuku ve İktisat dergisi, S. 2, Haziran [1997], s. 83-85.

ve kullandığı tespit edilmiştir[88].

Günümüzde işçilerin izlenmesi iş görüşmeleri ve işin ifa edilmesi aşamaları da dahil olmak üzere neredeyse tüm hayat alanlarını kapsayacak şekilde çeşitlenmiştir. Bunun gerçekleşmesi işçilerin iş hayatı ve özel hayatı arasındaki ayrımı bulanıklaştırmakta ve dijital izleme giderek işçileri daha şeffaf hale getirmektedir[89]. Örneğin işyeri giriş kartlarındaki radyo frekanslarıyla izlemeye olanak tanıyan çip sistemi (Smart ID, RFID) işverene, işçinin işyerindeki hareketlerini gerçek zamanlı izleyebilme olanağı sağlamaktadır. İşçilerin kişisel verilerini işleyen kamera gözetlemesi, bilgisayarda yapılan işlerin izleri, internet trafik bilgileri, bilgisayar başında geçirilen aktif durumu tespit etmeye odaklı programlar, vuruş sayısına duyarlı klavyeler (Bilgisayarla Performans Yönetimi), konum belirleyici programlar, araçlara takılan GPS cihazları, RFID (Radio-Frequency Identification / Radyo Frekansı ile Tanımlama) izleme, e-postaların takibi, çiple izleme, giyilebilir teknolojilerle izleme, biyometrik tanıma gibi sistemler işverenlerce yoğun olarak kullanılarak işçiler hakkında bilgi toplanmaktadır.

Eklemek gerekir ki, tarihsel süreç içinde gelinen aşamada, iş ilişkisinde kullanılan çeşitli dijital uygulamalarıyla yoğun veri işlenmesi sebebiyle işçilerin özel hayatlarını şeffaflaştıran veri işleme faaliyetlerinin ve veri işlemeyi işyeri sınırları dışına taşıran dijital izleme uygulamalarının bazı ahlaki sorunlar ortaya çıkaracağına, insanlık onuruyla bağdaştırılmayacak olaylara sebebiyet verebileceğine ve bireysel özerkliği ortadan kaldırabileceğine ilişkin kaygılar dile getirilmektedir[90].

88) Susser/ Roessler/Nissenbaum, [2019], Digital World, s. 8.
89) Peter E. Blume, Data Protection and Privacy – Basic Concepts in a Changing World, Scandinavian Studies in Law, Vol. 56, Stockholm: Jure Law Books, [2010], s. 155.
90) Norman E. Bowie/Ronald F. Duska, Business Ethics, Englewood Cliffs, N. J Prentice Hall, [1990], s. 86.

b) Teknolojinin Veri İşleme Biçimini Değiştirmesi: Özel Hayatın Korunmasının Taleplere Konu Edilmesi

Fotoğrafçılığın ve kamera teknolojisinin ortaya çıkması ve bu aygıtların özel hayatın gizliliğini ihlalde gizli çekim gibi yeni örnekler ortaya çıkarması[91], halkın ilgisini çeken gizli çekimlerin gazetelerde yayımlanması özel hayatın gizliliğini korumada geleneksel yaklaşımların ve genel hukuk düzenlemelerinin yetersiz kaldığı, bireyin özel hayatını koruyacak hukuki düzenlemelerin gerektiği tartışmalarına sebebiyet vermiştir[92]. Zira haberlere eklenen fotoğraflar çoğunlukla habersiz çekildiğinden özel hayatın gizliliğinin ihlal edildiğine ilişkin tartışmaları körüklemiştir. Özellikle ilk ihlaller halkın merakının da yoğunlaştığı soylu aileler, siyasiler ve bu ihlaller ilgili dönemin ünlüleri, yöneticileri veya siyasi liderleriyle ilgili olmuştur[93].

Bu sebeple özel hayatın gizliliğinin ve verilerin korunması ihtiyacı teknolojik gelişmelerin bu alanlar üzerinde ortaya çıkardığı yeni ihlal biçimleriyle yakından ilişkilidir. Zira teknolojik gelişmeler kişinin verilerini işleme biçimini, hacmini ve özel hayatın gizliliğini ihlal etme şeklini değiştirmektedir. Özellikle bilgisayar ve cep telefonunun toplumsal hayatın ve iş ilişkisinin bir bileşeni haline gelmesi "özel ve genel mekan", "işyeri ve ev", "çalışma zamanı ve eğlence

91) Bkz. Marion Manola v. Stevens&Myers kararı; Entrikin, [2012], Be Let Alone, s. 210; Palmer, [2011], History of Privacy, s. 72.
92) Warren & Brandeis'in bu makaleyi yazmalarında Marion Manola v. Stevens&Myers gibi davaların etkisi büyüktür. Tiyatro – müzikal gösteri sanatçısı olan Manola'nın Broadway Tiyatrosu'ndaki bir gösteride tayt giymesi gerektiği bir anda, dosyada sanık olan "Castle in the Air" isimli firmanın yönetici Stevens ve fotoğrafçı Myers gizlice fotoğrafını çekmiş ve bu çekim New York Times'ta yayımlanmıştır. Bunun üzerine Stevens ve Myers'a dava açılmış ve ihtiyati tedbir istenmiştir. Mahkeme ihtiyati tedbirin kalıcı olmasına ve gazetenin toplanmasına karar vermiştir. Konunun mülkiyet hakkı, telif hakları kapsamında tartışılmasını yetersiz bulan Warren & Brandeis yasaların kişilerin özel hayatını koruyacak şekilde düzenlenmesi gerektiği fikrini öne sürmüşlerdir. Böylelikle makalede o tarihlerde ceza hukuku, telif hakları ve haksız fiil kapsamında tartışılan bu tür olaylara kişinin mahremiyet hakkı, yalnız kalma hakkı kapsamında yenilikçi bir tartışma başlatmışlardır. Dorothy J. Glancy, "Privacy and the Other Miss M", Northern Illinois University Law Review, Vol. 10, No. 3, Summer [1990], s. 401-490. http://law.scu.edu/wp-content/uploads/miss_m.pdf (Erişim Tarihi: 02.04.2022).
93) Mensel, [1991], Right of Privacy, s. 25-28.

zamanı", "burası ve orası" arasındaki ayrımları oradan kaldırmaktadır[94]. Bu sınırların ortadan kaldırılması soyut, araçları ve uygulama boyutu tam olarak tespit edilemeyen dijital izleme uygulamalarıyla gerçekleştirilmektedir. Dijital izlemenin bu özelliğinden dolayı ihlalin biçimini ve boyutunu tam olarak tespit etmek güçtür. Bu durum dijital izleme uygulamalarının işçinin hayat alanları üzerindeki ihlallerin gerçekleşme riskini büyütmektedir.

Dijital izleme teknolojileri hızla gelişip, bireyin özel hayatı ve kişisel verileri üzerinde ihlal edici sonuçlar ortaya çıkarmaya başlarken, 18. yüzyılın aydınlanmasının önde gelen belgeleri olarak kabul edilen Fransa'nın İnsan ve Yurttaş Hakları Beyannamesi'nde, 1804 tarihli Fransız Medeni Kanunu'nda ve 1900 BGB'sinde (Bürgerliches Gesetzbuch / Alman Medeni Kanunu) özel hayatın gizliliği hakkının korunmasına ilişkin bir düzenleme yer almamıştır[95]. Amerikan Anayasası'nda da doğrudan özel hayatın gizliliğini koruyan bir düzenleme yer almamış[96], fakat 15 Aralık 1791 tarihli Haklar Bildirgesi'nde (Bill of Rights) daha sonra Federal Yüksek Mahkeme'nin[97] özel hayatın korunması kararlarına[98] dayanak yaptığı maddelerden birisi olan Dördüncü Madde[99] (Fourth Amendment);

---

94) Zygmunt Bauman, Akışkan Modern Dünyadan 44 Mektup, (Çev. Pelin Siral), Habitus Yayıncılık, İstanbul [2012], s. 39.
95) Palmer, [2011], History of Privacy, s. 71-72.
96) Palmer, [2011], History of Privacy, s. 71.
97) Griswold v. Connecticut, 1879'da Connecticut, doğum kontrolünü gerçekleştirmek için herhangi bir ilacın, tıbbi cihazın veya diğer araçların kullanımını yasaklayan bir yasa çıkarmıştır. Yale Tıp Fakültesinden jinekolog C. Lee Buxton, Conneciticut'ta Planlı Ebeveynlik Başkanı olan Estelle Griswold ile birlikte New Haven'da bir doğum kliniği açmıştır. Bunun üzerine yasayı ihlal etmekten tutuklanmaları üzerine bu tutuklama Eyalet Yüksek Mahkemesi tarafından onanmıştır. Bunun üzerine Anayasa'nın evliliğin mahremiyetini ve bir çiftin doğum kontrol yöntemlerini kullanma konusunda danışmanlık almasını sınırlandırıyor mu? Tartışmasına sebebiyet vermiştir. Yargıç Douglas tarafından kaleme alınan kararda özel hayatın gizliliğinin korunması hakkının, Haklar Bildirgesi'ndeki çeşitli hükümlerinde çıkabilen bir hak olduğuna karar verilmiştir.
https://www.law.cornell.edu/wex/griswold_v_connecticut_(1965) (Erişim Tarihi: 01.09.2022).
98) Poe v. Ullman davasında [1961] Yargıç Harlan muhalefet şerhinde özel hayatın gizliliğinin korunması hakkını ve bununla ilişkili haklara ilişkin yeni bir yaklaşımı özetlemiş, Olmstead/Amerika Birleşik Devletleri [1928] kararında gizli dinleme ve 1965'ten bu yana Yüksek Mahkeme ünlü yargılamalar olan Roe v. Wade [1973] davasında özel hayatın gizliliğinin korunması hakkını kürtaj haklarına ve Lawrence - Teksas [2003] davasında sodomi yasalarını uygulayarak özel hayatın gizliliği hakkının farklı metinlerinde ortaya çıkan Anayasal bir hak olarak içtihat geliştirmiştir.
99) https://www.archives.gov/founding-docs/bill-of-rights-transcript (Erişim Tarihi: 02.09.2022).

kişiyi makul olmayan aramalara karşı korumakta ve kişilerin evlerinde güvende olmaları, belgelerinin, eşyalarının gizliliğinin ihlal edilmemesi güvence altına alınmıştır. Özel hayatın gizliliğinin korunması hakkını doğrudan koruyan bir düzenlemenin bu belgelerde yer almamasında ve özel hayatın gizliliğinin korunmasına ilişkin doğrudan düzenlemelerin yapılmamasında bu hakkın henüz siyasi veya hukuki bir talep olarak ileri sürülmemesinin etkisi büyüktür[100].

Bu sebeple özel hayatın gizliliğinin korunmasının talep edilen bir hak haline gelmesini E. L. Godkin medeniyet, teknoloji ve gelişmişlikle ilişkilendirerek "ilkel toplumlar için bu hakkın bilinmeyen uygarlığın lükslerinden birisi olduğunu" ifade etmiştir[101]. Ayrıca özel hayatın gizliliğini koruyan çağdaş normların "modern ve ileri değerler" olduğu, geçmişin ve günümüzün gelişmemiş toplumlarında bu değerlerin çoğunlukla bulunmadığının gözlemlendiği, bu sebeple veri gizliliğine ilişkin hukuki düzenlemelerin geç ortaya çıktığı ileri sürülmüştür[102].

Özel hayatın gizliliğinin korunmasının taleplere konu edilmesinin gelişmişlik ve teknolojiyle ilişkili olduğunu belirten Westin ise, özel hayatın korunmasının üç evrensel yönünün bulunduğunu belirtmektedir. İlk olarak birey ve grup mahremiyetine ilişkin ihtiyaçlar çerçevesinde orya çıkan sosyal normlar hemen hemen her toplumda mevcuttur. Bu sosyal normlar sayesinde bireysel alan, yakın aile grubu alanı ve bir bütün olarak toplumsal alan gibi mahremiyet alanları oluşmakta ve bu alanlar kendi içinde farklı biçimde gizlilik kurallarına tabi olmaktadır. İkincisi korunma ihtiyacı ve tehlikelerden kaçınma arzusu gibi etmenlerin ortaya çıkardığı kimlik aidiyeti ve manevi özlemlerde bütünleşen bir inzivaya çekilme halidir. Bunun hukuktaki ilk görünümü kişinin yalnız kalma, kendisiyle baş başa kalma hakkı kapsamında savunulmuştur[103]. Özel hayatın

100) Palmer, [2011], History of Privacy, s. 72.
101) Palmer, [2011], History of Privacy, s. 71-73; Mensel, [1991], Right of Privacy, s. 27.
102) Westin, [1984], Modern Claims to Privacy, s. 59,
103) Daniel J. Solove, "Conceptualizing Privacy", California Law Review, Vol. 90, No. 4, July [2002], s. 1099; Tarık A. Gümüş, Devletin Pozitif Yükümlülükleri Ekseninde Özel Hayata Saygı Hakkı, AİHS Uygulaması Çerçevesinde Bir İnceleme, Adalet Yayınevi, Ankara, [2016], s. 153; Batuhan Aktaş, Özel Hayatın Gizliliğini İhlal Suçu, Der Kitabevi, İstanbul, [2017], s. 9; J.

gizliliğinin korunmasının evrensel olan üçüncü görünümü ise bireyin başkalarının özel hayat alanını ihlal etme eğiliminde olması ve risklere karşı gerekli önlemleri almak için gözetleme davranışında bulunmalarıdır. Bireysel düzeyde bu bir çocuğun çevresini keşfetmeye giriştiği dönemdeki veya yetişkinlikte başkalarının başına ne geldiği merakının da tetiklediği daha fazlasını bilme merakından ortaya çıkmaktadır[104].

Teknolojinin yaygın kullanıldığı, toplumsal ilişkilerin karmaşıklaştığı ve iş ilişkisinin, nüfus hareketlerinin ve veri akışının yoğun olduğu toplumlarda özel hayatın gizliliğinin ihlal ve bireyin verilerini işleme biçimi çeşitlenmektedir[105]. Zira bu toplumsal yapıda bilişim uygulamaları kişi hayat alanının çeşitli katmanlarında yer alan verileri kişinin bilgisi dahi bulunmaksızın onların dijital kopyalarını oluşturabilecek biçimde işlemeye konu edebilmektedir[106]. Bu yönüyle bilişim teknolojilerinin kişisel verilerin korunması hukukunun doğumu ve gelişiminde başat bir role sahip olduğunu söyleyebiliriz[107].

İş ilişkisinde teknolojinin iş görmenin esaslı bir parçası haline gelmesiyle birlikte dijital izleme uygulamalarıyla işçilerin kişi hayat alanında kalan verileri de dahil olmak üzere birçok katmanda verisi işlenebilmektedir. Özellikle bilişim teknolojilerinin sağladığı kolaylıklar işçileri sürekli gözetleme, denetleme ve kayıt altına alma olanağını işverene vermiştir[108]. Dahası bilgisayar temelli teknoloji işin teknolojik ve organizasyonel yönlerini temelinden değiştirmekte ve işçileri üretim sürecine daha nitelikli yönleriyle dahil eden yeni yönetim tekniklerini ortaya çıkarmaktadır. Böylelikle dijital izleme teknolojileri ekip tabanlı yönetim

---

Lyn Entrikin, "The Right to Be Let Alone: The Kansas Right of Privacy", 53 Washburn L.J., [2012], s. 210-211.
104) Westin, [1984], Modern Claims to Privacy, s. 61-63.
105) Palmer, [2011], History of Privacy, s. 71-72.
106) Collins, [1994], Privacy in the United Kingdom, s. 291-292.
107) Elif Küzeci, Kişisel Verilerin Korunması Hakkı, Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, [2023], s. 20.
108) Gary T. Marx, "Surveillance and Society", Encyclopedia of Social Theory, [2005], http://web.mit.edu/gtmarx/www/surandsoc.html; Dolgun, [2008], Gözetim Toplumu, s. 17-18.

teknikleriyle birleşmekte işveren tarafından gerçekleştirilen hiyerarşik izlemenin yanında, iş organizasyonu içinde aynı düzeydeki ekip arkadaşları arasından da karşılıklı denetime dayalı yatay gözetleme olgusu ortaya çıkmaktadır[109]. Örneğin işverenin saha satış işçilerinin sahada gerçekleştirdiği ziyaretleri GPS, RFID gibi uygulamalarla izlemesi hiyerarşik izleme; saha satış ekibinin kendi içinde sahada birbirlerine yönelik bilgi alışverişi, izlemeye dayalı iş birlikleri ve performans kontrolü yatay gözetleme olarak nitelendirilmektedir.

Eklemek gerekir ki, özel hayatın ihlal edilme biçimini değiştiren teknolojik gelişmeler durağan bir yapıda olmayıp, sürekli gelişen ve dönüşen, yeni uygulamalarla gerçekleştirebilen değişken bir karakterdedir. Bilişim uygulamalarını ortaya çıkardığı bu durum "toplumların akışkan aşamada" olması kavramıyla açıklanmıştır[110]. Daima hareket halinde olan, fakat verilerin işlendiği veri tabanları ve bulut sistemler çoğunlukla ülke içinde dahi bulunmadığından kesinlik ve sınırlardan yoksun olan günümüz vatandaşları, işçileri, tüketicileri ve gezginleri dijital izleme vasıtasıyla takip edildiklerinin farkındadır, ancak bunun sınırlarını ve boyutlarını tespit edecek imkana sahip değildirler[111]. Bundan dolayı gözetlemenin yeni aşaması olan dijital izleme akışkan bir yapıda olup, hareket eden her şeyi veya bir amaç kapsamında tanımlanış kişilerin belirli verilerini izleyecek şekilde yürütülebilmektedir[112].

III. Yeni Çalışma Türlerinin Denetim Aracı Olarak Dijital İzleme

İş hukuku ile gerçek kişi verisini korumayı amaçlayan kişisel verilerin korunması hukuku arasında yeni teknolojilere paralel gelişen sıkı bir ilişki söz konusudur[113]. Dijital izlemenin ham maddesi veri olup, dijital izleme veri işleme

109) Sewell, [1998], The Discipline of Teams, 405-406.
110) Bauman/Lyon, [2016], Akışkan Gözetim, s. 7.
111) Bauman/Lyon, [2016], Akışkan Gözetim, s. 7-8, 16.
112) Bauman/Lyon, [2016], Akışkan Gözetim, s. 7-8.
113) K. Ahmet Sevimli, "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", Sicil İş Hukuku Dergisi, Yıl 6, s. 24, Aralık, [2011], s. 124.

esasına dayanan bilişim sistem ve uygulamalarından oluşmaktadır. İş ilişkisinde işçi verisini çeşitli türde uygulamalarla yoğun işlemeye konu edebilme imkanını işverene veren bilişim teknolojileri, işçi üzerinde işyeri stresine sebebiyet vermekte ve işçinin kişisel verileri üzerindeki haklarına yönelik müdahaleci sonuçlar ortaya çıkarmaktadır.

1. Gözetlemede Yeni Bir Eşik: Dijital İzleme

Sanayi devrimi sonrası gerçekleşen teknolojik gelişmelerle birlikte işyerinde işçileri sürekli gözetleme ve denetleme olanağının aygıtını temsil eden mimari yapı panoptikon, merkezi bir kuleye sahip on iki kenarlı bir çokgen olmanın ötesinde büyük ölçüde bilişim teknolojilerinin ve optiğin kapasitesiyle güçlenen işçileri dijital izleyebilen, onların verilerini büyük veri tabanlarında işleyen yeni bir denetleme biçimine dönüşmüştür[114]. Özellikle 20. yüzyılda gelişen bilgisayar teknolojisinin işyerinin ve iş yapma süreçlerinin bir parçasına dönüşmesiyle birlikte dijital uygulamalarla işçinin izlenmesi yeni bir yapıya bürünmüştür[115].

Gelişen teknolojinin etkisiyle iş hukukunun fabrika ve işyeri gibi geleneksel iş organizasyonu modeli değişime uğrayarak, işte veya işyerinde harcanan zaman yerine sonuçlar ve içerikler işçinin verimliliğinin değerlendirilmesinde belirleyici kriter haline gelmiştir[116]. Bilişim uygulamalarının iş ilişkisinin sosyal bağlamını bu şekilde bilgi toplumu temelinde değiştirmeye başlaması vasıflı işgücünü ön plana çıkarmakta ve bu işçiler bilgisayar, akıllı telefon, tabletler veya internete bağlanan farklı mobil cihazlarla iş görme borçlarını uzaktan ve dilediği zaman diliminde ifa edebilmektedirler[117].

---

114) Sprague, [2007], From Taylorism to the Omnipticon, s. 2.
115) Sprague, [2007], From Taylorism to the Omnipticon, s. 3-4.
116) Ali Güzel, "Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri", Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı, (Ed. Kübra Doğan Yenisey), Onikilevha Yayıncılık, İstanbul, [2021], s. 32.
117) Matteo Avogaro, "Right to Disconnect: French and Italian Proposals for a Global Issue", Law Journal of Social and Labor Relations, Vol. 4, No. 3, September/December, [2018], s. 111.

Dijital izleme denetimi dönüştürerek tespiti kolay olan işveren vekili veya kamera gözetlemesi vasıtasıyla gerçekleştirilen izlemeyi; tespiti güç, sınırları belirsiz, belirli kavramlara veya durumlara duyarlı algoritmalarla başlatılması mümkün olan ve işyerinde veya işyeri dışında işçilerin kişisel zamanlarında izlenme olgusunu ortaya çıkarmıştır. Gözetlemeyi bir kişi vasıtasıyla gerçekleştirilebilir olmaktan veya optiğin sınırlarının dışına çıkarıp, belirli amaçlar kapsamında kişiyi izleyebilmeyi algoritma esaslı uygulamalar sayesinde gerçekleştirilebilir hale getiren dijital izleme gelişen bilişim teknolojilerinin ortaya çıkardığı bir olgudur. Bu özelliğinden dolayı dijital izleme günümüzde iş ilişkisinin, yasamanın ve mahkemelerin esaslı sorunlarından birisi haline gelmiştir[118].

Dijital izleme uygulamalarının kullanıldığı işyerlerinde işçiler bir şekilde izlendiklerini bilir fakat bunun ne şekilde ve ne miktarda gerçekleştiğini tespit edemezler. Tespit edilsin ya da edilmesin, dijital izleme işçi hayat alanının tamamını ilgilendiren verileri işlemeye konu edebilmektedir. Zira dijital izleme uygulamalarıyla işçi hakkında sürekli ve otomatik olarak veri işlemek olanaklı olduğundan, belirli beklentiler kapsamında işlenmiş kişisel veriler teknoloji sayesinde daha önce mümkün olmayan ölçüde hızla otomatik olarak analiz edilebilmektedir[119]. Analiz sonucunda işçinin işlenmiş verileriyle ortaya çıkan bilgi işçi hakkında çeşitli çıkarımların yapılmasında kullanılır veya elde edilen bilgi kapsamında işçi belirli bir yönde davranışta bulunmaya yönlendirilebilmekte, denetim baskısı altında tutulmakta veya farklı alanlarda çalışmaya kanalize edilmektedir[120].

---

118) Avner Levin, "Dignity in The Workplace: An Enquiry Into the Conceptual Foundation of Workplace Privacy Protection Worldwide, ALSB Journal of Employment and Labor Law Vol. 11, No. 1, Winter, [2009], s. 64.
https://castle.eiu.edu/~alsb/Dignity%20in%20the%20Workplace%20final.pdf (Erişim Tarihi: 02.11.2022).

119) Boehmer, [1992], Artificial Monitoring and Surveillance, s. 767; Antonio Aloisi/Elena Gramano, Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context, Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall, [2019], s. 96-97.

120) Andrew Crayden, "A Modern-Day Gold-Rush: Applying Property Principles to Data Using Mineral Rights Concepts and the Rule of Capture", Vol 81, Issue 3, Louisiana Law Review, [2021], s. 964-965; Örneğin Facebook kullanıcılarının bilgisi olmadan onların verilerini işlediği ve

Ayrıca kameralarla, biyometrik veri okuyan sistemlerle, konum tespiti tabanlı teknolojilerle veya bunların farklı kombinasyonlarından oluşan teknolojik sistemlerle sürekli ve sistematik bir şekilde işçilerin izlenmesi ve verilerinin işlenmesi, bu verilerin tanımlanmış amaçlar kapsamında analizlere konu edilmesi işçinin temel hak ve özgürlüklerine orantısız müdahalelere sebebiyet verebilmektedir. Bireysel ve toplu hak aramaların sonucu şekillenen kişisel verileri koruma mevzuatları temelde bu riskleri azaltmak için veri işlemeyi sınırlandırma, açık rıza ve ilgili kişinin bilgilendirilmesi gibi mekanizmalar oluşturmaktadır[121].

İşyerinde gözetlemenin, kişisel zamanı da kapsayacak biçimde uygulanabilen dijital izlemeye dönüşmesi işçilerin işlerini yapma şekli hakkında bilgiler toplanıp, işlenerek elde edilen verilerle belirli kararlar alınabilmesi, işçileri işyeri ihtiyaçlarına göre kanalize edilebilmesi böylelikle işyeri verimini artırma ve rekabet avantajları yakalayabilmekle yakından ilişkilidir[122]. Ayrıca işverenler yasal yükümlülük kapsamında teknik ve idari tedbirler alarak işçileri tehlikelerden, zorbalıktan ve tacizden korumak amacıyla veya sözleşmeden doğan yönetim hakları bulunduğundan çeşitli dijital izleme yöntemi uygulayabilmektedirler. Eklemek gerekir ki, işverenlerin iş görmeleri için ücretini ödediği işçilerin işyerinde neler yaptığını bilme ve iş süreçleri denetim altında tutma isteği iş sözleşmesinin ortaya çıkardığı yönetim hakkının bir görünümüdür[123].

---

paylaştığı "Cambridge Analytica" analizleri sayesinde kişilere yönelik doğrudan seçim sonucunu etkileyecek şekilde propaganda yaptığına, böylelikle ABD seçimlerinde kişi tercihlerini değiştirmede etkili olduğuna yönelik bir skandal ortaya çıkarılmıştı. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal (Erişim Tarihi: 12.10.2021); Aloisi/Gramano, [2019], Artificial Intelligence Is Watching You, s. 99-100.

121) Marta Otto, "Workforce Analytics v. Fundamental Rights Protection in the EU in the Age of Big Data", Comparative Labor Law & Policy Journal, Vol. 40, No. 3, Spring, [2019], s. 389-390; Lee Andrew Bygrave, Data Protection Law, Approaching its Rationale, Logic and Limits, Kluwer Law International, [2010], s. 125, https://law.shu.edu/online/students/assignments/docs/eu-data-protection-privacy-law-readings.pdf

122) Aloisi/Gramano, [2019], Artificial Intelligence Is Watching You, s, 96.

123) TBK m. 399 düzenlemesi öncesi işverenin yönetim hakkının kanunlarda açıkça düzenlenmemesi bu hakkın bulunmadığı anlamına gelmez. Zira doktrinde kabul gördüğü üzere yönetim hakkı esas olarak kaynağını iş sözleşmesinden alır. Bu anlamda, TBK m. 399 düzenlemesinin varlığı da bu hakkın asıl kaynağının iş sözleşmesi olduğu kabulünü değiştirmez. Savaş Taşkent, İşverenin Yönetim Hakkı, İstanbul [1981], s. 10-11; Münir Ekonomi, İş Hukuku, C. I, Ferdi İş Hukuku, Üçüncü Bası, İstanbul, 1987, s. 7; E. Murat Engin, Türk İş ve Sosyal Güvenlik Hukukunda İşveren, Banka Sigorta İşçileri Sendikası, [1993], s. 70; Öner Eyrenci/Savaş

Dijital izleme uygulamalarındaki asıl mesele işverenlerin bu denetim ve işçi hakkında daha fazla bilgi sahibi olma isteğinin sınırının ne olacağıdır. Zira yapay zeka uygulamalarının da kullanılmaya başlandığı dijital izleme uygulamalarıyla işçilerin ateşinin, nabzının, klavye basış stilinin, yakın çevresindeki seslerin izlenmesi; kanın alkol oranının veya kullanılan ilaçların dijital sensörlerle tespit edilmesi, beyin dalgalarının haritasının uzaktan izlenebilmesi ve kayıt altına alınması ve bireyin profilinin çıkarılması[124] olanaklı hale gelmiştir[125]. Bu tür izleme tekniklerinin işçinin özel hayatı ve verileri üzerinde oluşturduğu müdahaleci etki, işçilerin bireysel ve toplu tepkilerine sebebiyet vermektedir. Bu hak aramaları dijital izlemenin sınırlandırılmasının ve işçi verilerinin işlenmesinin hukuka uygunluğuna ilişkin hukuki gelişmelerin dinamiğini oluşturmaktadır.

2. Yeni Çalışma Türlerinin Dijital İzlemeyi Tetiklemesi

Dijitalleşmenin işyerinin sınırları ve işin yapılma zamanı üzerindeki en belirgin etkisi bunları esneten sonuçlar ortaya çıkarmasıdır. İşin görüldüğü yer açısından çeşitli atipik çalışma türlerinin ortaya çıkmasını bilişim teknolojileri tetiklemiştir. Atipik çalışma biçimlerinden birisi olan uzaktan çalışma işçinin iş görme borcunu klasik işyerinin sınırlarının dışında bilişim teknolojileri vasıtasıyla ifa etmesi esasına dayanan bir çalışma biçimidir[126]. Üretiminin otomasyonlaşması,

---

Taşkent/Devrim Ulucan, Bireysel İş Hukuku, 7. Baskı, İstanbul, [2020], s. 24; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 204; Sarper Süzek, "İşverenin Yönetim Hakkı ve Sınırları", Prof. Dr. Metin Kutal'a Armağan, Ankara 1998, s. 225-226; K. Ahmet Sevimli, İşçinin Özel Yaşamına Müdahalenin Sınırları, Legal Yayıncılık, İstanbul, 2006, s. 82.

124) Bkz. § 9. V.

125) Charles Fried, Privacy [A moral analysis], Philosophical Dimensions of Privacy: An Anthology, Edited by: Ferdinand David Schoeman, Cambridge University Press, Second Edition, [2007], s. 204.

126) Sarper Süzek, "İş Akdinin Türleri", Mercek İş Hukuku Dergisi, Nisan [2001], s. 30-31; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 120; Hamdi Mollamahmutoğlu/Muhittin Astarlı/Ulaş Baysal, Bireysel İş Hukuku, 3. Baskı Lykeon Yayınevi, Ankara, [2019], s. 74 vd.; Murat Kandemir," Evde Çalışma ve 6098 sayılı Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXXII, S. 2, Prof. Dr. Berin Ergin'e Armağan, [2014], s. 143-166, s. 157; Orhan Ersun Civan, "İş Hukukunda Uzaktan Çalışma (Evden Çalışma / Tele Çalışma)", Legal İş ve Sosyal Güvenlik Hukuku Dergisi, S. 26, Temmuz, 2010, s. 542-543; Murat E. Engin, "Türk İş Hukukunda Evde Çalışma, Prof. Dr. Turhan Esener'e Armağan", Ankara, [2000], s.273; Sevil Doğan, İş Sözleşmesinde Bağımlılık Unsuru,

bilişim teknolojilerinin iş yapma süreçlerine nüfuz etmesi uzaktan çalışma[127] esasına dayanan iş tiplerinin yaygınlaşması işin yapıldığı yer, zaman ve ekipmanın iş ilişkisini nitelendirmede etkisini azaltmıştır[128].

Yeni çalışma biçimleri iş sözleşmesinin ayırt edici unsuru olan bağımlılık ilişkisini ve işverenin denetimini görünüşte zayıflatan sonuçlar ortaya çıkarmıştır. Bundan dolayı iş sözleşmesinin bağımlılık unsurunu zayıflatan çalışma türlerinde iş sözleşmesini nitelendirmek için "bir başkasının organizasyonuna dahil olma", "işverenin menfaate uygun bir şekilde onun organizasyonda iş görme" biçiminde bağımlılığı iş sözleşmesiyle ilişkilendiren yaklaşımlar gelişmiştir. Zira bağımlılığın tespitinde temel ilke işin yapılması biçimi, yapılma zamanı ve yeri hususlarında işverenin talimatlarına işçinin bağlı olmasıdır. İşçi, iş sözleşmesinin ortaya çıkardığı bu durum çerçevesinde işverenin emir ve talimatlarına (yönetim hakkı)

Doktora Tezi, [2016], s. 169 ve 537 no'lu dipnotta atıf yapılan yazarlar ve Federal İş Mahkemesi kararı.

127) Başlığı "Çağrı üzerine çalışma" olan İş Kanunu'nun 14. Maddesinin başlığı 06.05.2016 tarihinde 6715 sayılı Kanunu'nun ikinci maddesiyle "Çağrı üzerine çalışma ve uzaktan çalışma" biçiminde değiştirilerek dört ek fıkrada uzaktan çalışma düzenlendi. Ayrıca "Uzaktan Çalışma Yönetmeliği" de 10 Mart 2021 tarih ve 31419 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girdi. Böylelikle İş Kanunu m. 14/4'te uzaktan çalışma: "işçinin, işveren tarafından oluşturulan iş organizasyonu kapsamında iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirme esasına dayalı ve yazılı olarak kurulan bir iş ilişkisi" biçiminde tanımlanmış oldu.

128) Yargıtay iş sözleşmesinin bağımlılık unsurunu, bağımlılığın zayıflaması durumunda dikkate alınması gereken ölçütlerle ilgili şu şekilde karar vermiştir: "İş sözleşmesini eser ve vekâlet sözleşmelerinden ayıran en önemli ölçüt bağımlılık ilişkisidir. Her üç sözleşmede iş görme edimini yerine getirenin iş görülen kişiye (işveren-eser sahibi veya temsil edilen) karşı ekonomik bağımlılığı vardır. İş sözleşmesini belirleyen ölçüt hukuki-kişisel bağımlılıktır. Gerçek anlamda hukuki bağımlılık işçinin işin yürütümüne ve işyerindeki talimatlara uyma yükümlülüğünü içerir. İşçi edimini işverenin karar ve talimatları çerçevesinde yerine getirir. İşçinin işverene karşı kişisel bağımlılığı ön plana çıkmaktadır. İş sözleşmesinde bağımlılık unsurunun içeriğini işverenin talimatlarına göre hareket etmek ve iş sürecinin ve 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. Bu belirtilerin hiçbiri tek başına kesin ölçüt teşkil olmaz. İşçinin işverenin belirlediği koşullarda çalışırken kendi yaratıcı gücünü kullanması, işverenin isteği doğrultusunda işin yapılması için serbest hareket etmesi 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." Yargıtay 9. HD., E. 2022/5067, K. 2022/5701 T. 9.5.2022.

uyma borcu (itaat) bulunmaktadır[129].

Tele çalışma, uzaktan çalışma, evden çalışma ve pazarlamacılık sözleşmesi gibi atipik iş ilişkilerinde işverenin doğrudan işçiyi ve çalışma sahasını denetim altında tutmasına, işin yapılış biçiminin düzenlenmesinde belirleyici olmasına olanak bulunmamaktadır[130]. Bu sebeple öğretide uzaktan çalışmada işverenin iş sağlığı ve güvenliğine ilişkin yükümlülüğünün daha çok aydınlatma (bilgilendirme) yükümlülüğüne indirgendiği ve iş ilişkisindeki bağımlılık unsurunun zayıfladığı ifade edilmiştir[131].

Gerçekte işverenler gerçekleştirdikleri dijital izleme uygulamalarıyla bağımlılık unsurunu bilişim sistemleri üzerinde daha etkin bir biçimde yeniden inşa etmekte ve yaygınlaştırarak görünür kılmaktadırlar[132]. Harekete duyarlı dijital izleme uygulamaları, biyometrik verilerin işlenmesinin duygu algılama teknolojileriyle gerçekleştirilebilmesi işverenlere ve insan kaynakları departmanlarına işçilerin üzerinde hiyerarşik ilişkiyi yeni aygıtlarla kurma ve derinleştirme olanağını vermektedir[133]. Dahası uzaktan çalışmada işverenlerin evde çalışan işçileri mesai saatleri içinde kameralarını açmaya zorladığı örnekler

---

129) Gülsevil Alpagut, "Dijitalleşen Çalışma Yaşamında İş Sözleşmesinin Unsurları", Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı, On İki Levha Yayıcılık, (Ed. Kübra Doğan Yenisey / Seda Emrağ Ergüneş), İstanbul, [2021], s. 100-101; Süzek, [2019], İş Hukuku, s. 225 vd.; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 150 vd.; Süzek, [1998], Yönetim Hakkı, s. 225-226; Engin, [1993], İşveren, s. 70; Taşkent, [1981], Yönetim Hakkı, s. 10-11; Ekonomi, [1987], Ferdi İş Hukuku, s. 32; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 256.

130) Seda Ergüneş Emrağ, "4857 Sayılı İş Kanununun Değişik 14. Maddesi Işığında Tele Çalışma", Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, C. 13, S. 51, 2016, s. 1414; Canan Ünal Adınır, "Tele Çalışmada Verilerin Korunması", Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, (Ed. Kemal Şenocak), Yetkin Yayınları, Ankara, 2022, s. 955-960; Süzek, [2001], İş Akdi, s. 30-31; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 120; Mollamahmutoğlu/Astarlı/Baysal, İş Hukuku, s. 74; Kandemir, [2014], Evden Çalışma, s. 143-166, s. 157; Civan, [2010], Uzaktan Çalışma, s. 542-543; Engin, [2000], Evden Çalışma, s.273; Doktrinde tele çalışma ile uzaktan çalışmayı özdeş kavramlar olarak görüp incelemeye konu eden görüş ile tele çalışmayı üst bir kavram olarak görüp diğer atipik çalışma biçimleri olan evden çalışma, uzaktan çalışma biçimlerini kapsayan bir karam olarak nitelendirerek incelemeye konu eden yaklaşımlar bulunmaktadır. Bkz. Ergüneş Emrağ, [2016], Tele Çalışma, s. 1414 vd.

131) Murat Kandemir, İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma, Legal Yayıncılık, İstanbul, [2011], s. 131.

132) Avogaro, [2018], Right to Disconnect, s. 111-112.

133) Aloisi/Gramano, [2019], Artificial Intelligence Is Watching You, s. 96-97.

haberlere ve araştırmalara konu edilmektedir[134].

Uzaktan çalışmada işçinin özel hayatının gizliliği, kişisel verileri ve konut dokunulmazlığı gibi temel hakları gündeme geleceğinden işverenin denetim imkanı bu düzenlemeler kapsamında sınırlanmaktadır[135]. Yukarıda incelendiği üzere işçinin uzaktan çalışmada işverenin fiziki denetiminin dışına çıkması işverenleri anlık izleme, klavye yakalayıcısı, bilgisayar ekran fotoğraflayıcısı, giyilebilir saat, bileklik gibi dijital denetim ve izleme olanağı veren uygulamaları kullanmaya sevk etmektedir. Bu durum işçinin denetimini kişisel zamanını da kapsayacak biçimde gerçekleştirme olanağını işverene vererek denetimi yaygınlaştıran sonuçlar ortaya çıkarmıştır[136]. İşverenin, işçileri izlemek için bu tür programları kullanılmasına ilişkin görülen bir davada Alman Federal İş Mahkemesi bu yazılımların işçinin profilini çıkarabildiğini, bir ölçüte tabi olmaksızın bu tür uygulamaların kullanılmasını ve gizli biçimde işçilerin verilerini kayıt altına almasını hukuka aykırı bulmuştur[137].

Dijital izlemeyle gerçekleştirilen denetim aynı zamanda işçinin özel hayatının gizliliğinin nasıl ihlal edilebileceğinin ve işçi verilerini ihlal edici veri işlemenin yeni örneklerini ortaya çıkarmaktadır. Özellikle bilişim teknolojilerinin işyerlerinde işin yapılmasının esaslı parçasına dönüşmesi ve işin bir işyerinde yapılması zorunluluğunun ortadan kalkması işçilerin özel hayatları ve kişisel verileri üzerinde daha önce öngörülemeyen biçimde müdahaleler ve ihlaller ortaya çıkarabilmektedir. Dijital izleme uygulamalarla işçilerin dijital profillerinin

134) Gaye Baycık/Sevil Doğan/Dilek Dulay Yangın/Oğuzhan Yay, "Covid 19 Pandemisinde Uzaktan Çalışma: Tespit ve Öneriler", Çalışma ve Toplum, 2021/3, [2021], s. 1688; Ayrıca bkz. "İşverenin Evden Çalışanları Kamerayla İzlemesine Tepki Yükseliyor" başlıklı bir haber için bkz. https://ikmagazin.com/is-dunyasi/isverenin-evden-calisanlari-kamerayla-izlemesine-tepki-yukseliyor/ (Erişim Tarihi: 10.12.2022).
135) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 165.
136) Lothar Determann/Robert Sprague, "Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States", Berkeley Technology Law Journal, Vol. 26, No. 2, Spring, [2011], s. 982.
137) Alman Federal İş Mahkemesi – "BAG 2 AZR 681/16 sayılı Kararı" karar detayları için bkz. § 7. IV. 3.

oluşturulması, duygu algılama teknolojileri, konum izlemenin farklı boyutları, biyometrik ve genetik verilerle izleme, mobil cihazlardaki izlemeye olanak veren uygulamalar, bulut bilişim gibi yeni teknolojiler dijital izlemeyi farklı boyutlara büründürebilecektir[138]. Bu durum aşağıda ele alınacak dijital izlemenin hukuka uygunluk ölçütleri bakımından önem kazanacaktır[139].

§ 2. ÖZEL HAYAT VE KİŞİSEL VERİLERİN KORUNMASI

İş ilişkisinde işverenin iş sözleşmesinden kaynaklanan belirli haklarının varlığı (yönetim hakkı) ve işçinin, işverenin emir ve talimatlarına uygun işverene bağımlı olarak iş görmesi (itaat borcu) birlikte değerlendirildiğinde bu ilişkinin kendine özgü doğasının bir gereği olarak işçinin özel hayatının gizliliği ve kişisel verilerinin korunması haklarını sınırlandıran sonuçlar ortaya çıkardığı kabul edilmektedir[140]. Özel hayatın gizliliğinin korunması ile kişisel verilerin korunması hakları arasında yakın bir ilişki bulunmaktadır. Kişisel Verilerin Korunması Kanunu'nun (KVKK) amacının düzenlendiği m. 1'de bu husus özel hayata vurgu yapılarak şu şekilde hüküm altına alınmıştır: "kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir." Bu sebeple bu başlıkta özel hayatın gizliliği ve kişisel verilerin korunması haklarının dayandığı hukuki temeller ile koruduğu kişilik hakları ve değerleri ele alınacaktır.

I. İş İlişkisinde Mahremiyet ve Özel Hayatın Gizliliğinin Korunması

Bilişim sistemleri belirli durumlara özgülenen izleme algoritmalarına ve

138) Lotte Houwing, "Stop the Creep of Biometric Surveillance Technology", European Data Protection Law Review (EDPL), Vol. 6, No. 2, 2020, s. 175-176; Aloisi/Gramano, [2019], Artificial Intelligence Is Watching You, s. 96-97, 113.
139) Bkz. § 6.
140) AYM, Fırat Gerçek kararı, Başvuru Numarası: 2019/25604, Karar Tarihi: 21.09.2022, § 23; AYM, E.Ü. kararı, § 69; EU, [2018], Handbook, s. 98.

veri işleyen yapay zeka uygulamalarına olanak tanıdığından kişi özelinde dijital izleme uygulamaları gerçekleştirilebilmektedir. İş ilişkisindeki denetim biçimini dönüştüren dijital izleme işçilerin özel hayatı ve kişisel verileri üzerindeki hakları ile işverenin iş sözleşmesine ilişkin hakları arasında bir çatışma ortaya çıkarmaktadır. Modern hukuk sistemlerinde iş ilişkisinde işçilerin mesleki faaliyetlerinin ötesinde ilişkiler geliştirebilecekleri, bu sebeple işyerlerindeki faaliyetlerinde ve iletişimlerinde belirli bir makul gizlilik ve özel hayat beklentisine sahip olmaları gerektiği kabul görmektedir[141]. Bu itibarla işçinin dijital izlemeden etkilenen menfaatleri olan özel hayat ve kişisel verileri ifade etmek için kullanılan "mahremiyet", "özel hayatın gizliliği", "veri koruması" ve "kişisel verilerin korunması" kavramları ve kapsamları bu başlıkta değerlendirilecektir.

1. Mahremiyet

Antropolojik bulgulardan, çeşitli dinlerin kutsal metinlerindeki mahremiyete ilişkin hükümlerden ve eski dönemlerdeki hukuk metinlerinde[142] yer alan mahremiyeti korumayı da hedefleyen düzenlemelerden yola çıkarak gerçekleştirilen çalışmalarda kişinin mahrem alanını koruyan düzenlemelerin eskiden beri var olduğu tespit edilmiştir[143]. Ayrıca mahremiyet, özel hayat ve kişisel veri kavramlarının nitelendirdiği "kişi" sözcüğü aslında kendisini anonim hale getirme, gizlilik ve kendini başkalarına kapatma amacı güden "maske" kavramlarıyla yakın ilişkilidir. Zira "kişi" sözcüğü etimolojik olarak Etrüsk dilinde maske anlamına gelen "prosopon" kelimesinden gelmektedir. Romalı sanatçıların performanslarını sergileme anında kendilerini izleyicilerden soyutlamak amacıyla maske takmaları Latince "prosopon persona" olarak kavramsallaştırılmış ve maske

141) Evisa Kambellari, "Employee Email Monitoring and Workplace Privacy in the European Perspective", Iustinianus Primus Law Review, Vol. 5, No. 1, [2014], s. 1.
142) İngiltere'de 1361 yılında kabul edilen "Justices of the Peace Act" isimli hukuki düzenlemede mahremiyeti koruyucu düzenlemeler de öngörülmüş ve sulh hakimine başkalarını gizlice dinleyen ve izleyen insanları tutuklatma yetkisi verilmiştir. James Michael, "Privacy And Human Rights: An International and Comparative Study, with Special Reference to Development in Information Technology", Paris, [1994], s.15; https://www.legislation.gov.uk/aep/Edw3/34/1 (Erişim Tarihi: 06.10.2022).
143) Barrington Moore, Privacy, Studies in Social and Cultural History, New York, [1984], s. 276.

kişide vücut bulacak şekilde kullanıma girmiştir[144].

Maskenin oluşturduğu özel alan sayesinde kişi tanıdıkların, toplumun ve devletin kolayca ulaşamayacağı bir alanda kendisini ifade etme imkanını yakalamaktadır. Kişi kavramını somutlaştıran maske metaforu, aynı zamanda özel hayatın gizliliğinin korunmasının ikili boyutunu kavramamızı sağlamaktadır. Maske hem bireyin kendisini özgün bir şekilde toplumda ifade etme imkanını hem de başkalarının keyfi bakışlarına karşı korumayı sağlamaktadır. Bu itibarla özel hayatın gizliliği hakkı, daha genel bir bireysel özerklik özlemini güçlü bir şekilde ifade ettiği için, bu kavramın birey için "yalnız bırakılma hakkından" daha fazla hakkı kapsadığını söyleyebiliriz[145].

Uygulamada "özel hayatın gizliliği" ve "mahremiyet" kavramlarının bir arada, eş anlamlı olacak şekilde kullanıldığı örnekler bulunmaktadır. Aslında "özel hayatın gizliliği" bilişim toplumundaki gelişmelere bağlı olarak kişinin mahremiyet hakkını da kapsayan anayasal bir haktır. Öyle ki özel hayatın gizliliği hakkı sadece kişinin gizli (sır) alanını değil, kamu tarafından görülebilen, örneğin kişinin sadece sosyal medya arkadaşlarıyla paylaştığı bir fotoğrafı[146] gibi kişisel verileri üzerindeki haklarını da kapsayacak katmanlar yüklenmiştir. Bu anlamda kişinin içsel dünyasını işaret eden mahremiyet belki de en çok korumayı gerektiren hayat alanlarından sadece birisidir. Bu sebeple özel hayat sadece kişinin giz (mahrem) alanını değil[147], mahrem olmayan hayat alanının büyük bir kısmını da kapsamaktadır[148].

---

144) Koen Lemmens, "The Protection of Privacy between a Rights-Based and a Freedom-Based Approach: What the Swiss Example Can Teach Us", Tilburg Foreign Law Review, Vol. 11, No. 3, [2004], s. 606.
145) Lemmens, [2004], The Protection of Privacy between a Rights-Based, s. 606-607.
146) Yargıtay 12. CD., E. 2016/2244 K. 2017/5453 T. 21.6.2017; Aynı yönde Yargıtay 12. CD., E. 2019/1 K. 2019/10579 T. 23.10.2019.
147) Doktrinde mahremiyet ile özel hayatın eş anlamlı kullanıldığı da görülmektedir. Bkz. "Özel yaşam (mahremiyet, Privacy) ise, dış etkiden arınmış bir alan sağlayarak, sosyal baskıya karşı yalıtımı, mümkün kılar." Sevimli, [2006], Özel Yaşam, s. 20-21 ve 81. dipnotta atıf yapılan yazarlar.
148) Üzeltürk, [2005], Özel Hayatın Gizliliği, s. 2-3; Seda Arslan Durmuş, "İşçinin Özel Yaşamının İş İlişkisine Etkisi", DÜHFD, C. 25, S. 42, [2020], s. 143.

İngilizcede özel hayat kavramını ifade etmek için "privacy" kelimesi kullanılmaktadır. "Mahremiyet/gizlilik" (intimacy) sözcüğü ise, "kişinin herkesle paylaşmayacağı veya sadece yakınlarıyla paylaştığı ya da herhangi bir kimseyle paylaşmamak hakkının bulunduğu olay, inanç, duyguları" ve aidiyetleri[149] yani bireyin mahrem (gizli) alanını ifade etmektedir. Ne var ki, günümüzde bazen bireysel tercihe göre ifşa dahi edilen kişi hayat alanı sadece mahrem alandan oluşmamaktadır. Ayrıca mahremiyet "gizli" kavramını işaret edip ifade ederken, özel hayatın gizliliği kavramının bu şekilde belirli bir kavramı işaret ettiği temel bir kullanımı da bulunmamaktadır[150]. Bundan dolayı "mahremiyet" ile "özel hayatın gizliliği" kavramları aynı kapsamı ifade eden kavramlar değildir. Özel hayat kavramı daha geniş bir kavram olarak mahremiyet[151] kavramını da kapsamakta ve bireyin gizli hayat alanı ile kamusal alanına yansıyan diğer hayat alanlarını ve kişisel verilerini ifade etmektedir[152]. Bu sebeple bu kavramların birbirinin yerine kullanılması isabetli bir kullanım değildir.

Mahremiyet (intimacy) sözcüğü bireysel gizliliğe ya da doğası gereği samimi olarak adlandırılabilen ilişkilerdeki yakınlıktan kaynaklı, dar bir alanda kalan bilgileri ve eylemeleri ifade etmektedir[153]. Mahremiyet sadece bireyin kendisiyle yakın ilişkide olduğu kişilerle paylaştığı bilgileri[154] ve kişinin gizli alanında kalan bilgileri kapsamaktadır. Bu sebeple mahremiyet, "özel hayat"

149) Oya Araslı, Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi, Ankara [1979], (Yayınlanmamış Docentlik Tezi), s. 6; Elif Küzeci, Kişisel Verilerin Korunması, 4. Baskı, Onikilevha Yayıncılık, İstanbul, [2020], s. 19.
150) David Elliott/Eldon Soifer, "Privacy and Intimacy", Journal of Value Inquiry, Vol. 44, No. 4, December, [2010], s. 489-498, s. 491.
151) "Mahremiyet", kişisel gizlilik ve kişinin kendi dar gizli alanı anlamını ihtiva eden dar anlamda özel hayatı ifade etmektedir. "Özel hayatın gizliliği" kavramı ise kişisel gizlilik dahil olmak üzere kişinin özel ve kamuya açık hayat alanlarındaki verilerini ve gizliliğini kapsamına alan daha geniş bir kavramdır. TDK da mahremiyeti, "gizlilik" biçiminde tanımlarken; özel hayatı "kişinin kendisine özgü yaşayışı, yaşam tarzı, kendisini ilgilendiren tutum ve davranışı, öz yaşam, özel yaşam" biçiminde tanımlamaktadır. https://sozluk.gov.tr/ (Erişim Tarihi: 04.09.2022).
152) Güçlü Akyürek, Özel Hayatın Gizliliğini İhlal Suçu, 2. Baskı, Ankara, Seçkin Yayıncılık, [2014], s. 46; Üzeltürk, [2005], Özel Hayatın Gizliliği, s. 2-3; Elliott/Soifer, [2010], Privacy and Intimacy, s. 491-492.
153) Elliott/Soifer, [2010], Privacy and Intimacy, s. 490.
154) Robert S. Gerstein, Intimacy and Privacy, Edited by, Ferdinand David Schoeman, Cambridge University Press, Second Edition, Cambridge, [2007], s. 269.

kavramı kapsamında korunan kişi hayat alanlarının tamamını ifade etmekte yetersiz kalmaktadır. Mahremiyet kavramı kişi hayat alanının gizli katmanını ifade ettiğinden tezde bir gerçek kişi olabilen işçinin gizli hayat alanını da kapsayacak şekilde "özel hayatın gizliliği" kavramı kullanılmıştır.

2. Özel Hayatın Gizliliğinin Korunması

İş sözleşmesinin niteliğini belirleyen bağımlı çalışma, doğrudan işçinin özel hayatı üzerinde etkiler ortaya çıkarmaktadır[155]. Bu sebeple dijital izleme hakkı ve sınırlarına ilişkin bir inceleme yapılırken iş sözleşmesinin karakteristik özelliği ile dijital izleme uygulamalarının tehlikeye attığı işçinin temel haklarından birisi olan özel hayatın gizliliği hakkının iş ilişkisi özgünlüğünde incelemeye konu edilmesi gerekmektedir.

a) Özel Hayatın Gizliliğinin Hukuken Korunması ve Önemi

İnsan ruhu şeffaflıktan kaçışa, bazen de herkesin bakışından uzak kendisiyle baş başa kalabileceği alanlara gereksinim duyar[156]. İnsan özgürlüğü ve onuru ile yakından ilişkili olan bu gereksinimin bir sonucu olarak özel hayatın gizliliğinin korunması hakkı, bireyin yaşamını ne şekilde sürdüreceğini belirleme hakkını güvenceye alan ve bireysel manevi, zihinsel bütünlüğü korumayı amaçlayan temel insan hakları grubuna girmektedir[157].

Özel hayatın gizliliğinin korunması hakkı önceleri etik bir ilke olarak inceleme konusu edilen "insan onuru" kavramı ile ilişkilendirilerek

155) Sevimli, [2006], Özel Yaşam, s. 81 vd.; Gülsevil Alpagut, "İşyerinde Kamera Gözetlemesi ve AİHM Kararları ile Tespit Edilen Esaslar", Savaş Taşkent'e Armağan, (Ed. Kübra Doğan Yenisey), On İki Levha Yayıncılık, [2019], s. 291; Ulaş Baysal, "İş Hukukunda Kişisel Verilerin İşlenmesi", Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması, (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, [2023], s. 520.
156) Byung-Chul Han, Şeffaflık Toplumu, (Çev. Haluk Barışcan), 2. Baskı Metis Yayınları, İstanbul, [2017], s. 17.
157) İbrahim Ö. Kaboğlu, Özgürlükler Hukuku, 3. Baskı, Afa Yayınları, İstanbul, [1996], s. 292.

değerlendirilmiş ve fakat savaşların insanlık üzerinde bıraktığı büyük yıkımla birlikte uluslararası sözleşmelerde ve ulusal düzenlemelerde[158] yer bulmaya başlayan "insan onuru", "kişi dokunulmazlığı" kavramları hukuk düzenlemeleri kapsamında değerlendirilmeye başlanmış ve metinlerde hukuki birer kavram olarak yer bulmuştur[159]. Özel hayatın gizliliği kavramı bu kavramlar kapsamında değerlendirilmiş ve kamu hukukçuları bu hakkın bireysel özgürlük idealinin temelini oluşturduğunu ifade etmiştir[160]. Zira bu hak sayesinde herkes özel hayatını başkalarından (kamudan) gizleme, kendisiyle ilgili istediği kadar veriyi paylaşma ve böylece kişisel onurunu koruma imkanını yakalayabilmektedir[161].

Özel hayatın gizliliğinin korunmasının doğrudan olmasa da bir insan hakkı olarak korunabilirliği ve anayasalarda yer verilmesinin geçmişi ise, 18. yüzyıla kadar gitmektedir. Fransa'da devrimin esasını oluşturan ve 1789'da kabul edilen İnsan ve Yurttaş Hakları Beyannamesi ve ABD'de 1776 tarihli Virginia Anayasası'nın başlangıç kısmına ABD'de kabul edilen ilk insan hakları hukuki belgesi olan Haklar Bildirgesi'nin eklenmesi ve daha sonra ABD'de kabul edilen diğer anayasalarda bu modelin takip edilmesi insan haklarının anayasallaştırılmasının temelini oluşturmuştur[162].

Günümüzde anlam yüklediğimiz şekilde özel hayatın gizliliğinin korunması ancak bu kavramın 20. yüzyılda uluslararası hukuki belgelere konu edilmesiyle mümkün olmuştur. Özel hayat kavramının hukuki belgelere konu edilmesi onu

158) Leyla Şenel, Anayasalarda İnsan Hak ve Özgürlüklerinin Tanınması Sorunu, Oniki Levha, İstanbul, [2020], s. 100 vd.
159) "İş ve çalışma hürriyetinin ihlali" başlığını taşıyan TCK m. 117/II düzenlemesinde "insan onuru" ile bağdaşmayacak çalışma ve konaklama koşullarında kimsenin çalıştırılmayacağı düzenlenmiştir. TCK m. 117/II hükmü uyarınca: "Çaresizliğini, kimsesizliğini ve bağlılığını sömürmek suretiyle kişi veya kişileri ücretsiz olarak veya sağladığı hizmet ile açık bir şekilde orantısız düşük bir ücretle çalıştıran veya bu durumda bulunan kişiyi, insan onuru ile bağdaşmayacak çalışma ve konaklama koşullarına tabi kılan kimseye altı aydan üç yıla kadar hapis veya yüz günden az olmamak üzere adlî para cezası verilir."
160) Üzeltürk, [2005], Özel Hayatın Gizliliği, s. 10-11; Sevimli, [2006], Özel Yaşam, s. 27; Aktaş, [2017], Özel Hayatın Gizliliği, s. 8.
161) Lisa Guerin, Employment Law: The Essential HR Desk Reference, Berkeley, California, Nolo, [2011], s. 252.
162) Kaboğlu, [1996], Özgürlükler Hukuku, s. 34.

hukuki bir kavrama dönüştürmüş ve genel olarak kabul edilen temel bir hak haline getirmiştir. Böylelikle, 1948 tarihli "Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi'nin" 12. maddesinde özel hayatın gizliliğinin korunması: "Hiç kimsenin özel yaşamına, ailesine, konutuna ve haberleşmesine keyfi olarak karışılamaz, onur ve ününe saldırılamaz. Herkesin bu tür karışma ve saldırılara karşı yasal korunma hakkı vardır." biçiminde yerini almıştır[163]. Eklemek gerekir ki, bir hakkın elde edilmesi insanların ortak mücadelesini gerektirdiği gibi aynı zamanda hakkın varlığı hukuk ve devletin varlığıyla mümkündür[164].

Özel hayatın gizliliğinin korunmasını ilk kez diğer haklardan farklılıklarını esas alarak incelemeye konu ettiğinden ve bu hakkın kuramsal çerçevesini belirlemeyi denediğinden Warren & Brandeis'in "The Right to Privacy – Gizlilik Hakkı" başlıklı makalesinin özel hayatın gizliliğinin gelişiminde önemli bir etkisi bulunmaktadır[165]. Makalenin yayımlanmasından sonra ABD'de yüksek yargı içtihatları kapsamında özel hayatın gizliliği kavramı tartışmalara konu edilmeye başlanmıştır[166]. Benzer biçimde "özel hayat" kavramı Fransa'da 1819 tarihli Basın Kanunu'nun görüşmeleri esnasında kullanılmış ve fakat bu alanı doğrudan koruyan yasal düzenleme ancak 1868'de Ceza Kanunu'nda gerçekleştirilmiştir. İngiltere ve Almanya'da ise bu kavrama ilişkin ilk tartışmalar ve düzenlemeler 1950'ler gibi daha geç tarihlerde başlamıştır[167].

Ancak özel hayatın gizliliği hakkının hızlı gelişiminde, II. Dünya Savaşı'nın acımasızlıklarını katlandıran ve büyük insan kitlelerinin mahvına sebebiyet veren

---

163) Rona Aybay, Açıklamalı İnsan Hakları Evrensel Bildirgesi, Türkiye Barolar Birliği Yayını, Ankara, [2006], s. 15.
164) Rona Serozan, Medeni Hukuk Genel Bölüm ve Kişiler Hukuku, Vedat Kitapçılık, İstanbul [2013], s. 193.
165) Solove, [2002], Conceptualizing Privacy, s. 1099; Gümüş, [2016], Özel Hayata Saygı, s. 153; Aktaş, [2017], Özel Hayatın Gizliliği, s. 9; Entrikin, [2012], Be Let Alone, s. 210-211; Jed Rubenfeld, "The Right of Privacy", Harvard Law Review, Vol. 102, No. 4, February, [1989], s. 737-738; David Archard, The Value of Privacy, Privacy and the Criminal Law, Antwerpen-Oxford, [2006], s. 13.
166) Solove, [2002], Conceptualizing Privacy, s. 1088 vd.
167) Yusuf Ziya Polater, Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması, Adalet Yayınevi, Ankara [2010], s. 8.

bireylere ilişkin tutulan veri tabanlarının savaş zamanında kitleleri yok etme veya göçe zorlama gibi amaçlarla kullanılması etkili olmuştur. Bunun yapılması hem evrensel hem de bölgesel düzeyde ilk uluslararası insan hakları sözleşmelerinin taslağının hazırlanmasına yol açmıştır. İnsan Hakları Evrensel Beyannamesi (İHEB) m. 12 ve Avrupa İnsan Hakları Sözleşmesi (AİHS) m. 8 özel hayatın gizliliğini insan hakkı olarak düzenleyen ve koruyan önemli uluslararası hukuki düzenlemelerdir[168].

Bu düzenlemelerin etkisiyle özel hayatın gizliliğinin ve kişisel verilerin bireye ilişkin bir değer olarak korunması; 1950 tarihli Avrupa Konseyi'nin "Avrupa İnsan Hakları ve Ana Hürriyetlerini Korumaya Dair Sözleşmesi", 1969 tarihinde imzalanan "Amerikan İnsan Hakları Sözleşmesi", 1981 tarihli 108 No'lu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ve sınır aşan kişisel veriler için 181 sayılı Ek Protokol gibi uluslararası metinlerde düzenlemeye kavuşmuştur[169]. Böylelikle modern hukuk sistemlerinde kişiye ait verileri de koruyan özel hayatın gizliliğinin ve kişisel verilerin korunmasını sağlayan yeni yasal düzenlemelerin yapılmasının önü açılmıştır.

AİHS'nin 8. maddesinin kenar başlığı "özel hayata ve aile yaşamına saygı hakkı" biçiminde olup, madde metninde herkesin özel ve aile yaşamı, konut dokunulmazlığı ve haberleşme hürriyeti güvence altına alınmıştır. Maddenin ikinci fıkrasında bu hakka hangi hallerde müdahale edileceği sınırlı şekilde sayılmıştır. Günümüzde özel hayatın gizliliğinin korunması bütün modern demokratik hukuk düzenlerinde kabul görmüş temel bir anayasal haktır[170]. Özel hayatı korumayı amaçlayan bu uluslararası düzenlemelerin ortaya çıkmasında teknolojik gelişmelerin ortaya çıkardığı otomatik veri işlemenin ve özel hayatın ihlal ediliş

168) Jan C. Buitelaar, "Privacy: Back to the Roots", German Law Journal, Vol. 13, No: 3, [2019], s. 172-174.
169) Rona Aybay, İnsan Hakları Hukuku, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, [2015], s. 15 vd.
170) Ergun Özbudun, Anaysa Hukuku Bakımından Özel Haberleşmenin Gizliliği, Ankara Üniversitesi Hukuk Fakültesi 50. Yıl Armağanı, Ankara Üniversitesi Hukuk Fakültesi Yayınları, No. 406, C. 1, Ankara, [1977], s. 265.

biçimlerinin önemli bir etkisi bulunmaktadır.

Özel hayatın gizliliğinin ve kişisel verilerin korunmasını Kıta Avrupası'nda ve ABD'de farklı dinamiklerle gelişmiş ve korunmuştur. Teknolojik gelişmelerin özel hayat üzerindeki müdahaleci etkilerinin[171] bir sonucu olarak özel hayatın gizliliğinin korunması hakkı ABD'de yüksek yargı kararlarında tartışmaya konu edilmiş[172] ve Federal Yüksek Mahkeme'nin içtihatlarında yer almıştır. ABD'de içtihatlar kapsamında kabul gören özel hayatın gizliliğinin ve kişisel verilerin korunması hakkı doğrudan farklı sektöre ilişkin hukuki metinlerde düzenlenmiştir. Bu sebeple ABD ve Kanada'da çeşitli kanunlar kapsamında işçilerin mahremiyetini koruyan yasal düzenlemeler bulunmaktadır[173]. Eklemek gerekir ki, ABD'de bazı eyaletlerde gerçekleştirilen son yasal düzenlemeler işverenlerin işçilerin dijital olarak izlemesi ancak onları önceden bilgilendirmesi koşuluna bağlamakta ve işyerinde gerçekleştirilen dijital izlemeyle ilgili şeffaflığı artıran ve özel hayatı koruyan yasal düzenlemeler gerçekleştirilmektedir. Son olarak Mayıs 2022'de New York'ta gerçekleştirilen yasal düzenleme ile işverenlerin işçilerin internet erişimini, e-postalarını ve telefon konuşmalarını izlemesi veya bunlara erişimi engelleyen uygulamalar kullanabilmesi için öncesinde işçilere yazılı bildirim yapılması koşuluna bağlamıştır[174].

---

171) Bkz. Marion Manola v. Stevens&Myers yargılaması.

172) Warren/Brandeis, [1890], Privacy, s. 193 vd.

173) Olmstead / United States, 277 U.S. 438, 478 (1928), özel hayatın gizliliğinin korunması gerektiğini düşünen Brandeis kararda muhalif kalmıştır. Yargıç Brandeis uzun zamandır özel hayatın gizliliğinin korunması hakkını savunuyordu, muhalif kaldığı Olmstead kararından yaklaşık kırk yıl önce yayımlanmış ve özel hayatın gizliliğinin korunması açısından bir dönüm noktası niteliğindeki makalesinde, hukukta özel hayatın gizliliğinin korunması hakkının dayanaklarını ortaya koymuştur. Aktaran, David A Carrillo, "California Constitutional Law: Privacy", San Diego Law Review, Vol. 59, No. 1, February-March, [2022], s. 123. Nitekim Federal Yüksek Mahkeme bu kararından yaklaşık 40 yıl sonra Brandeis'in muhalefet şerhine uygun olarak Katz / United States [1967] davasında Mahkeme bu kavrama değinerek şunu belirtir: Bir işyerindeki, bir arkadaşının dairesindeki veya bir taksideki bir kişiden daha az olmamak üzere, bir telefon kulübesindeki bir kişi Dördüncü Değişikliğin korunmasına güvenebilir. Onu kullanan, kapıyı arkasından kapatan ve arama yapmasına izin veren ücreti ödeyen kişi, ağızlığa söylediği sözlerin dünyaya yayınlanmayacağını varsayma hakkına sahiptir. Katz/Amerika Birleşik Devletleri, 389 U.S. 347, 352.

174) Benzer yasal düzenlemeler ilk olarak Connecticut ve Delaware eyaletlerinde yürürlüğe girmiş New York bunları takip etmiştir. Aynı doğrultuda, Teksas'ta, işçilerin elektronik iletişimlerinin işveren tarafından izlenmesi, mahremiyetin ihlali olarak kabul edilmektedir. California, 2018'de

Özel hayatın ve kişisel verilerin korunmasını bir insan hakkı olarak kabul eden Kıta Avrupası'nda ise bireyin bu hakları ulusal ve uluslararası çeşitli düzenlemelere konu edilmiştir. AİHS'de özel hayatın gizliliği bir hak olarak tanınmış fakat bu kavrama ilişkin bir tanımın yer almamıştır. AİHS düzenlemeleri kapsamında kararlar veren AİHM özel hayatın bütün yönleriyle tanımlanmasının güç, geniş bir kavram olduğunu belirterek özel hayatın bir tanım kapsamında sınırlandırılmasının mümkün ve gerekli olmadığı yönünde kararlar vermektedir[175].

Ülkemizde özel hayatın gizliliğinin korunması 1961 Anayasasının 15. maddesindeki birinci cümlede yer alan: "özel hayatın gizliliğine dokunulamaz" biçimindeki düzenlemeyle anayasal çerçeveye kavuşmuştur. 1982 Anayasasında ise, 20. maddeden itibaren "Özel hayatın gizliliği ve korunması" başlığında "özel hayatın gizliliği" ve "haberleşme hürriyeti" kenar başlıklarını da kapsayacak şekilde özel hayatın korunmasına ilişkin düzenlemeler gerçekleştirilmiştir[176]. Böylelikle özel hayatın gizliliğinin korunması kamu hukukunda anayasal temel hakların ve cezai korumanın konusu; özel hukukta ise kişilik hakkının korunmasının bir görünümü olarak karşımıza çıkmaktadır[177].

Aslında özel hayatın gizliliğinin korunması benzer alanların korunmasına

---

CCPA'yı yürürlüğe koyduğundan beri işverenler, işçilerinin işlemiş oldukları verilere yasanın nasıl uygulanacağını konusunun açıklığa kavuşmasını beklemektedir. Bununla birlikte şimdiye kadar, istihdam verileri, CCPA'nın gereksinimlerinin çoğundan özel olarak muaf tutulmuştur. Ancak, 1 Ocak 2023'te yürürlüğe giren Kaliforniya Gizlilik Hakları Yasası'nda (CPRA) yer alan CCPA'da yapılan değişikliklerin bir sonucu olarak, birçok işçi verisi artık CCPA'nın düzenlemelerine tabi hale geldi. https://www.jdsupra.com/legalnews/data-privacy-laws-zeroing-in-on-7664079/ (Erişim Tarihi: 24.01.2023).

175) Hamide Zafer, "Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK m.132-134)", Beta Yayınevi, İstanbul, [2010], s. 32; Rüçhan Işık, Toplu Şikayet Prosedürü, Anayasal Sosyal Haklar –Avrupa Sosyal Şartı, Karşılaştırmalı Hukuk ve Türkiye, (Ed. İbrahim Ö. Kaboğlu), Legal Yayınevi, Şubat, [2012], s. 62.

176) Kaboğlu, [1996], Özgürlükler Hukuku, s. 68; Attila Özer, Gerekçeli ve 1961 Anayasası İle Mukayeseli 1982 Anayasası, Ankara, Kamu-İş Yay., 1996, s. 63 vd.

177) Yaşar Karayalçın, Türk Hukukunda Şeref ve Haysiyetin Korunması, 1962-1963 Öğretim Yılı Açılış Dersi, s. 252, https://dergipark.org.tr/tr/download/article-file/638117, s. 252-254, (Erişim Tarihi: 01.09.2022), (Karayalçın, [1962], Şeref ve Haysiyetin Korunması); Haluk Tandoğan, Şahsiyetin Akit Dışı İhlallere Karşı Korunmasının İşleyiş Tarzı ve Basın Yoluyla Olan İhlallere Karşı Özel Hayatın Korunması, 1962-1963 Öğretim Yılı Açılış Dersi, s. 2-3, https://dergipark.org.tr/tr/download/article-file/632430, s. 2-3, (Erişim Tarihi: 01.09.2022).

gönderme yapan evrensel bir ilke olsa da somut biçimi toplumsal özellikler, ekonomik ve kültürel çevre gibi yerel özgünlüklere göre farklılık gösterebilmektedir. Bu itibarla özel hayatın gizliliğinin korunması kavramının bilişim çağının ortaya çıkardığı yeni pratik kapsamında yeniden yorumlanması ve güncel bağlamında incelenmesi gerekmektedir. Zira doğal olarak sürekli değişen bağlam ve değişken ögelere bağlı neyin korunması gerektiği kavramın tanımlamasını zorlaştırmaktadır[178]. Öte yandan doktrinde bu hakkın temelde kişinin bağımsız ve özgürce karar alması, kendisine özgü özel bir alana sahip olması ve işlenmiş kişisel verileri üzerinde belirleyici bir hakimiyetinin bulunması olmak üzere üç unsuru barındırdığı kabul edilmektedir[179].

Dijital izlemenin ihlal edici etkiler oluşturduğu işçi haklarından birisi özel hayattır. Günümüzde kişiyle ilgili işlenen bilgiler özel hayatın gizli alanına sirayet edecek biçimde çeşitlenmiştir. Kişinin özel nitelikli verileri olan cinsel yaşamı, sağlık verisi, dini ve etnik aidiyet gibi hassas verileri bilişim uygulamalarıyla otomatik işlenebilmektedir[180]. Örneğin işyeri sınırlarında sona ermeyen, işverence iş görme borcunun ifası için işçinin kullanımına tahsis edilen laptop bilgisayar veya cep telefonu ile eve taşınabilen dijital izleme uygulamaları işçilerin internet arama geçmişi, e-posta yazışmaları, aktif çalışma süresi, lokasyon bilgileri, sağlık raporları, arama türüne göre özel nitelikli kişisel verileri gibi birçok katmanda verinin işlenebilme imkanını işverene vermektedir.

Belirtmek gerekir ki, hukukumuzda işçilerin özel hayatının korunmasına ilişkin özel bir düzenleme bulunmadığından konu, AİHM ve AYM içtihatları

178) Serge Gutwirth, Privacy and The Information Age, Lanham: Rowman & Littlefield Publishers Inc. [2002], s. 30-33.
179) Üzeltürk, [2005], Özel Hayatın Gizliliği, s. 3-4; Saadet Yüksel, Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale, Beta, İstanbul, [2012], s. 35.
180) Aloisi/Gramano, [2019], Artificial Intelligence Is Watching You, s. 120-121; Gail Lasprogata/Nancy J. King/Sukanya Pillay, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", Stanford. Tech. Law Review. 4, [2004], s. 9-10.

çerçevesinde şekillenmektedir. İşçinin özel hayatının gizliliğinin korunmadığı bir iş ilişkisinde, işçiden bağımsız olarak özel hayatına ilişkin verilerin habersiz elde edilmesi, depolanması, aktarılması, ilgili kişinin bunlara müdahale edememesi gibi ihlal edici uygulamalar ortaya çıkar. Bu sebeple modern hukuk sistemlerinde bunun önüne geçmek ve kişinin toplum içinde kendisini özgürce var etmesi, kişiliğini geliştirmesi ve çeşitli düzeylerde ilişkiler kurması amacıyla yasal düzenlemeler gerçekleştirilmiştir[181].

b) Özel Hayat Tanımı ve Kapsamı

Özel hayatın gizliliği ilk olarak basitçe "insanın yalnız kalma hakkı" kapsamında tanımlanmış ve tartışmaya açılmıştır[182]. Neredeyse tüm modern hukuk sistemlerinde her bireyin özel hayatının, kamunun (başkalarının) gözünden uzak tutma, koruma ve böylece kişisel onurunu koruma hakkı bulunduğu kabul görmüştür. Zira bireyin özel hayatını, mahremiyetini ve ailesini korumak, modern hukuk sistemlerinin temel amaçlarından birisidir[183].

Özel hayat kavramından ve bu kavramın koruduğu değerlerden ne anlaşılması gerektiği hususunda herkesçe kabul edilen ve üzerinde uzlaşı sağlanan bir tanım bulunmamaktadır. AİHM ve AYM kararlarında özel hayat geniş bir kavram olarak nitelendirilerek, özel hayata ilişkin sınırlandırıcı bir tanımlamanın yapılmamasının doğru olmayacağına karar verilmektedir[184]. AYM kararlarında tanımlanmasının zor olduğu vurgulanan bu kavramın içeriğinde nelerin bulunduğu örneklendirilerek bireyin maddi ve manevi bütünlüğü, sosyal varoluşu, ismi, sağlık

181) Durmuş Tezcan, Bilgisayar Karşısında Özel hayatın Korunması, Anayasa Yargısı Dergisi, C. 8, 1991, s. 386. https://ayam.anayasa.gov.tr/media/4797/dtezcan.pdf (Erişim Tarihi: 28.08.2022).
182) Warren/Brandeis, [1890], Privacy, s. 195.
183) Milica R. Kovac-Orlandic, "Employee's Right to Privacy: Where Is the Bound of the Employer's Right to Monitor Employees' Communications", Strani Pravni Zivot (Foreign Legal Life), Vol. 2020, No. 4, [2020], s. 86-86.
184) AİHM, [GK], [2017], Bărbulescu v. Romania, 61496/08, 05.09.2017, § 36; AYM, Ömür Kara ve Onursal Özbek kararı, Başvuru Numarası: 2013/4825, Karar Tarihi: 24.03.2016, § 43; AYM GK, Bülen Polat kararı, Başvuru Numarsı: 2013/7666, Karar Tarihi 10.12.2015, § 61.

bilgileri, cinsel yaşamı ve yönelimi, kişisel verileri, mesleki yaşamı[185], aile hayatı, kişisel gelişim bilgileri biçiminde ifade edilmektedir[186]. Özel hayat, bireyin yaşam sürecinde yaşayışının bir görünümü olarak ortaya çıkan, bireye ait hayat olayları, bireysel işlemler ve bilgiler biçiminde de tanımlanmaktadır[187]. En yaygın kullanılan tanım ise, "özel, aile ve konut yaşamını, maddi ve manevi bütünlüğü, onur ve saygınlığı, yanlış şekilde tanıtılmamayı, ilgisiz ve utanç kaynağı olabilecek gerçeklerin açık edilmemesini, özel fotoğrafların yetkisiz şekilde basılıp ve dağıtılamamasını, bireyin gizli şekilde alıp verdiği bilgilerin açıklanmamasını kapsar" biçimindedir[188].

Özel hayatın kapsamına bireyin fiziksel ve psikolojik bütünlüğü[189], kişinin kimliğini koruması, tercihlerini belirleyebilmesi, kişiliğini geliştirmesi ve kimlik değerleri[190], kişinin itibarı ve onuru kapsamında yer alan değerler[191], birey özerkliği ve bireyin kendi geleceğini belirleme hakkı, kişisel verilerinin korunmasını isteme hakkı[192] girmektedir. Bu sebeple özel hayatının gizliliğinin korunması hakkı anayasal bir insan hakkı olarak kişiye kendisini toplum içinde veya işyerinde ifade

185) AYM, Serap Tortuk, Başvuru Numarası: 2013/9660, Karar Tarihi: 21/1/2015.
186) AYM, Ömür Kara ve Onursal Özbek kararı, Başvuru Numarası: 2013/4825, Karar Tarihi: 24.03.2016, § 43; Murat Şen/Taylan Barın, Özel Hayata ve Aile Hayatına Saygı Hakkı Karar Özetleri, Anayasa Mahkemesi Yayınları, [2021], s. 1.
187) Arslan Durmuş, [2020], İşçinin Özel Yaşamı, s. 137; Sevimli, [2006], Özel Yaşam, s. 7; Akyürek [2014], Özel Hayat, s. 48; Kandemir, [2011], Tele Çalışma, s. 136.
188) Sevimli, [2006], Özel Yaşam, s. 19; Council of Europe, Parliamentary Assembly, Declaration on mass communication media and Human Rights, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en (Erişim Tarihi: 27.09.2023).
189) Beizaras and Levickas v. Lithuania, AİHM, Başvuru No: 41288/15, T: 14.01.2020, par.109, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200344%22]}; Nicolae Virgiliu Tănase v. Romanya, AİHM, Başvuru No: 41720/13, T: 25.06.2019, § 126, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12518%22]}; Denisov v. Ukraine, AİHM, Başvuru No: 76639/11, T: 25.09.2018, par. 95 https://www.icj.org/wp-content/uploads/2017/09/Ukraine-Denisov-v-Ukraine-Advocacy-legal-submission-2017-ENG.pdf, https://www.echr.coe.int/Documents/Guide_Art_8_TUR.pdf.
190) Üzeltürk, [2005], Özel Hayatın Gizliliği, s. 172; Breyer v. Almanya, AİHM, Başvuru No: 50001/12, T: 30.01.2020, § 73.
191) İHEB 12. maddesi ve BM Kişisel ve Siyasal Haklara Dair Uluslararası Sözleşme'nin 17. maddesinde bu kavramlar kullanılmıştır. AİHS madde 8 ise herkesin özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkı ifadeleriyle bu değerler korunmuştur.
192) Rotaru v. Romanya, AİHM, Başvuru No: 28341/95, T: 04.05.2000, par.43-44, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}; Flinkkilä and Others v. Finlandiya, AİHM, Başvuru No: 25576/04, T: 06.04.2010, par.75, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-98064%22]}

etme, özgürce yaşam tarzını belirleme ve ifşa edilmeme güvencesini vermektedir.

AİHM'in iş ilişkisine ilişkin kararlarından birisi olan Niemietz & Almanya[193] kararında mahkeme "özel hayat" kavramını sınırlamanın isabetli olmayacağını, kişi hayat alanına ilişkin birçok ögenin bu kavram içinde bulunduğunu tespit ettikten sonra, bireyin kendi hayat alanlarında dilediği gibi yaşayabileceği bir "iç çevrenin" bulunduğunu vurgulamıştır. Birey bu hayat alanına ilişkin olan çemberin içinde yer almayan dış dünyayı tamamen dışlar. Bu bağlamda, "özel hayat" kavramı, kişinin profesyonel faaliyetlerini içerebileceği gibi kamusal alanda gerçekleştirdiği faaliyetlerde ortaya çıkan veriyi de içerebilir[194].

AYM çeşitli kararlarında özel hayatın korunması hakkının bazı durumlarda kamusal alana doğru genişleyebileceğine, bireyin bu konudaki makul meşru beklentilerinin kamusal alanda da belirli koşullar çerçevesinde korunması gerektiğine karar vermiştir[195]. Danıştay belediye ve hastane olan işverenlere ilişkin

193) Karara konu olayda Bay Niemietz, Almaya'da Freiburg im Breisgau'da yaşamakta ve burada avukatlık yapmaktadır. İşçilerin maaşlarından kesinti yapmayı ve yükümlü oldukları Kilise Vergisini vergi dairesine ödemeyi reddeden bir işveren olan Bay J. aleyhine yürütülen cezai kovuşturmada 9 Aralık 1985'te Freising Bölge Mahkemesi Yargıcı Miosga'ya telefaksla bir mektup gönderilmesinde hakaret ifadeleri yer almış, bu isimsiz mektubu gönderen kişinin tespiti için Avukat Gottfried Niemietz'in ofis binaları, Bayan D'nin evi ve arabaları, Bayan G'nin evi ve arabalarının aranması için karar çıkarılmıştır. Federal Anayasa Mahkemesi, Münih I. Bölge Mahkemesi'nin başvuranın temyiz başvurusunun kabul edilemez olduğuna ilişkin 27 Mart 1987 tarihli kararının da anayasa hukuku açısından sakıncalı olmadığına karar vermiştir. Ayrıca, tutuklama emrinin fiilen infazına ilişkin olarak, Bay Niemietz, Mahkemeler Teşkilatı Kanununa Giriş Kanununun (Einführungsgesetz zum Gerichtsverfassungsgesetz) 23(1) maddesi uyarınca kendisine sunulan hukuk yolunu tüketmemiştir. AİHM bu başvuruda özel hayat kavramının tanımı, sınırı, korunma düzeyi, bireyin kendisine bıraktığı özel iç alanın varlığı, özel hayat hakkının içeriği ve neleri kapsadığı, mesleki faaliyetin bu kavramın dışında tutulmayacağı, AİSH m. 8'in kapsamı hususlarında önemli tespitler yapmış ve Bay Niemietz'in bürosunun aranmasını özel hayata müdahale olarak nitelendirmiştir.
https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57887%22]} (Erişim Tarihi: 18.12.2022); Gilles Dutertre, Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler, Avrupa Konseyi Yayınları, [2003], (2019 Güncellemesi), s. 201.
https://www.anayasa.gov.tr/media/3600/aihmkararlarindanornekler.pdf (Erişim Tarihi: 18.12.2022).

194) Fernández Martínez v. İspanya, kararı, dosya no: 56030/07, Karar Tarihi 12 Haziran 2014, para. 110; Oleksandr Volkov v. Ukrayna, karar no. 21722/11, karar tarihi 27 Mayıs2013, para. 165-66, http://hudoc.echr.coe.int/eng?i=001-115871; Von Hannover v. Almanya (No. 2), karar numaraları: 40660/08 ve 60641/08, karar tarihi: 7 Şubat 2012, § 95, http://hudoc.echr.coe.int/eng?i=001-109029.

195) AYM, Şengül Kayan kararı, 03.04.2014 tarih ve 2013/1614 Başvuru Numaralı kararı, § 34.

verdiği kararlarda işyerine giriş ve çıkışlarda yüz tanıma veya parmak izi tarama sistemlerinin kullanılmasını kamusal alanda da olsa bireyin özel hayatının gizliliğinin korunması hakkının bulunduğunu tespit ederek, bu uygulamaların özel hayatla ilgili olduğunu ve özel hayata orantısız bir müdahale oluşturduğuna karar vermiştir[196].

AİHM, Halford & Birleşik Krallık kararında ise işçinin işyerinde makul bir özel hayat beklentisinin bulunduğu ve bu makul beklentinin hukuken korunması gerektiğine karar vermiştir[197]. Kararda bu husus işçiye işini yapması için verilen iletişim araçlarının mülkiyetinin işverende bulunması tek başına bu araçların izlenmesi için geçerli sebep olmadığı biçiminde değerlendirmeye konu edilmiştir. Bu itibarla işçinin özel hayatının gizliliğinin korunacağına dair makul beklentisinin AİHS m. 8 kapsamında kamusal alanda da bulunsa korunması gerekmektedir. Zira işçinin özel hayatının korunması gibi temel haklarının kamusal alanla ilişkili de olsa korunması esası kabul görmüştür[198]. KVK hukuku açısından ise sözleşme ilişkisinin bulunması bir veri işleme hukuka uygunluk sebebidir. Sözleşme ilişkisinin varlığı veri işleme faaliyetini KVK hukuku ilkeleri dışına çıkarmadığından, veri sorumlusu işveren ancak KVK hukukunun öngördüğü yükümlülükleri yerine getirerek işçilerin kişisel verilerini işleyebilir.

Yukarıda incelendiği üzere, ilk kez tanımı yapıldığında özel hayat bireyin "yalnız kalabilme hakkı" biçiminde tanımlanmıştır[199]. Özel hayata ilişkin ilk tartışmalar sonrasında özel hayatın gizliliği; "bireylerin, grupların veya kurumların, kendileri hakkındaki bilgilerin ne zaman, nasıl ve ne ölçüde başkalarına iletileceğini

196) Danıştay 5. D., 10.12.2013, 2013/5730 E.- 2013/9526 K., Danıştay 13. D, 15.5.2006, 6811/1959.
197) AİHM, [GK], [2017], Bărbulescu v. Romanya, (Başvuru Numarası: 61496/08; AYM, E.Ü. kararı Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020; AYM, Ömür Kara ve Onursal Özbek kararı § 50; AYM, Fırat Gerçek kararı, Başvuru Numarası: 2019/25604, Karar Tarihi: 21.09.2022; Yargıtay 22. Hukuk Dairesi, E. 2017/21857 K. 2019/9884 T. 7.5.2019 kararı.
198) AİHM, Halford v. Birleşik Krallık, § 57-69, https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-58039%22]}; Ayrıca bkz. Niemietz v. Almanya kararı.
199) Warren/Brandeis, [1890], Privacy, s. 193-195.

kendileri belirleme (informational self-determination) hakkı" biçiminde tanımlanmıştır[200]. Tanımlamaların her biri özel hayatın gizliliği kavramının sadece bir yönünü vurguladıklarından tek başlarına kavramı ifade etmekte yetersiz kalmaktadır. Bu sebeple her olayın özgünlüğü dikkate alınarak özel hayatın gizliliğinin ortak kavramlar kapsamında açıklanması daha isabetli olacaktır[201]. Zira özel hayatın gizliliğinin korunması kavramının göreceli yapısının yanında birden fazla hukuk alanını ve kavramını ilgilendirmesi de özel hayat tanımlanmasını güçleştirmektedir[202].

Özel hayat "her şeye ilişkinmiş gibi görünür fakat aynı zamanda tek başına hiçbir şey ifade etmemektedir[203]". Bundan dolayı özel hayatın gizliliğinin korunması hakkını tek bir tanıma indirgeyerek açıklamaya çalışmak yerine benzer özelliklerden oluşan ortak kavramlarla açıklanmasının kavramını daha iyi anlaşılmasını sağlayacağını belirtmek gerekir[204]. Buna göre özel hayatın gizliliği; (1) yalnız kalma hakkı[205], (2) başkalarının erişimine karşı kendini sınırlama, (3) gizli alanlarını belirleme, bazı kişisel verileri kendisine ait alanda bırakma, (4)

200) Angela Vivarelli, "The Crisis of the Right to Informational Self-Determination", Italian Law Journal, Vol. 6, No. 1, [2020], s. 302-303.
201) Solove, [2002], Conceptualizing Privacy, s. 1126-1128, s. 1129.
202) Karayalçın, [1962], Şeref ve Haysiyetin Korunması, s. 252 vd.; Tandoğan, [1962], Özel Hayatın Korunması, s. 2-3; Çetin Özek, Türk Basın Hukuku, İstanbul Üniversitesi Yayınları, İstanbul, [1978], s. 259.
203) Daniel J. Solove, "A Taxonomy of Privacy", University of Pennsylvania Law Review, Vol. 154, No. 3, January [2006], s. 478, (Solove, [2006], Taxonomy of Privacy); Whitfield Diffie/Susan Landau, "Privacy on the Line, The Politics of Wiretapping and Encryption", USA, MIT Press, [2007], s. 141-143.
204) Solove, [2002], Conceptualizing Privacy, s. 1087-1156, s. 1092.
205) Warren/Brandeis, [1890], Privacy, s. 195; ABD'de alkollü içeceklerin satışının yasak olduğu (1920-1933 yılları arasında) yıllarda federal kamu görevlilerince, Roy Olmstead adlı kişinin telefonlarını hukuka aykırı olarak dinlendiği iddiası ABD Anayasa Mahkemesinin önüne getirilmiştir. İddiaya göre, federal kamu görevlilerinin Olmstead'in telefonlarını hukuka aykırı şekilde dinlediği ve bunun sonucunda özel yaşamın gizliliğinin ihlal edildiği ileri sürülmüştür. Anayasa Mahkemesi bu başvuruyu, Fourth Amendment'te (Dördüncü Anayasa Düzenlemesi) düzenlendiği şekliyle olay üst araması veya yakalama olmadığından ve telefon dinlemesine ilişkin de bir düzenleme bulunmadığı gerekçesiyle olayda hukuka aykırılık bulunmadığına karar vermiştir. Brandeis ise, makalede ileri sürdüğü yaklaşımı, ABD Anayasa Mahkemesi yargıcı olduğunda, Amerika Anayasa Mahkemesi Olmstead v. United States kararında "… yalnız bırakılma hakkı, hakların en geniş kapsamlısı ve medeniyete kavuşmuş olan insanlık tarafından en değer verilenidir" biçiminde yazdığı muhalefet şerhi ile sürdürmüştür. Olmstead v. United States, 277 U.S. 438, 1928, 478-479; Palmer, [2011], History of Privacy, § 94-95.

kişisel verileri üzerinde kontrol sağlama yeteneği, (5) kişiliğini koruma, (6) insan onurunu ve birey özerkliğini koruma kavramlarıyla ilişkilidir[206].

Tanım ve kavramlardan ortaya çıktığı üzere özel hayat kavramı kişinin hayat alanının farklı katmanlarını kapsayan genel bir kavram olarak her şeyden daha karmaşık bir şeyi ifade etmektedir[207]. Zira tanımlamasının ve sınırlarının belirlenmesinin güç olduğu bu kavramın[208] kapsamında kişinin sır alanı bulunabileceği gibi herkese açıkladığı kişisel verileri ve hangi verileri kimlerle paylaşacağına ilişkin kararını, kimin kendisiyle duygusal etkileşimde bulunabileceği yönündeki iradeyi de kapsamaktadır[209]. Bu aynı zamanda özel hayat kavramının sosyal dinamik bir kategori olarak hukuksal alanla etkileşim içinde olduğunu ve normu dönüştürdüğünü de göstermektedir. Bu itibarla özel hayatın gizliliği kavramı genel olarak kurumları, uygulamaları, faaliyetleri, toplumsal, bireysel yaşamı, bireysel tercihleri, kişiyi ve bunlara ilişkin hukuki metinlere de yansıyan sınırları ifade etmektedir[210].

Ayrıca kişilik hakkının bir görünümü olan özel hayat mutlak bir hak olduğundan birey bu hakkını herkese karşı ileri sürebilir. Özel hayat hakkının bir diğer özelliği de kişiye sıkı sıkıya bağlı olması ve tekelci bir hak olarak bu hakkın üzerindeki hakimiyetin sadece hakkın sahibine ait olmasıdır. Bu hak kişi tarafından devre konu edilemez ve vazgeçilmesi de olanaklı değildir[211].

Bu noktada eklemek gerekir ki, bilişim teknolojilerinin kişi hayat alanına gerçekleştirdiği müdahalenin boyutu büyük veri, akıllı profilleme gibi örneklerle

206) Solove, [2002], Conceptualizing Privacy, s. 1091-1093.
207) Ferdinand Schoeman, Privacy Philosophical Dimensions of The Literature, Philosophical Dimensions of Privacy An Anthology, Edited by, Ferdinand David Schoeman, Cambridge University Press, Second Edition, Cambridge [2007], s. 2.
208) AYM [GK], Bülent Polat kararı, Başvuru No: 2013/7666, 10/12/2015, § 61.
209) Niemietz v. Almanya, Başvuru No: 13710/88, 16 /12/1992, § 29.
210) Schoeman, [2007], Privacy An Anthology, s. 4.
211) Sevimli, [2006], Özel Yaşam, s. 28-29; M. Kemal Oğuzman/Özer Seliçi/Saibe Oktay-Özdemir, Kişiler Hukuku (Gerçek ve Tüzel Kişiler), 16. Baskı, Filiz Kitabevi, İstanbul, [2016], s. 162 vd.; Mustafa Dural/Tufan Öğüz, Kişiler Hukuku, Filiz Kitabevi, 23. Baskı, İstanbul, [2022], s. 95.

çeşitlendiğinden özel hayatın gizliliğinin korunmasının geniş bir perspektiften değerlendirilerek korumaya konu edilmesi gerekmektedir. Zira sadece gizli bilgilerin ele geçirilmesi veya ifşa edilmesiyle sınırlandırılan bir özel hayat koruması bireyi koruyamayacaktır. Ayrıca özel hayatı sınırlandıran tüm eylemler de özel hayata müdahale kavramı kapsamında değerlendirilerek gerekli nitelendirmenin yapılması gerekmektedir[212]. Özel hayatın gizliliğinin korunması kavramının kapsam ve katmanlarının çeşitlenmesi sebebiyle bireyin temel hak ve özgürlüklerinden birisi olan özel hayatın gizliliğin korunması ve kapsamının belirlenmesine yönelik çeşitli yaklaşımlar ortaya çıkmıştır.

3. Özel Hayat Kapsamında Bireyin Korunan Yaşam Alanları

Doktrinde özel hayatın gizliliği açıklanırken üç unsur ön plana çıkmaktadır. Bunlardan birincisi bireyin özerk ve yalnız kalabildiği bir alana sahip olması, ikincisi diğer insanların baskılarına maruz kalmadan kendi kararlarını alabilmesi ve kendisini özgürce ifade edebilmesi, üçüncüsü ise türlü vasıtalarla dolaşıma giren kişisel verileri üzerinde belirleyici olma ve hakimiyet kurabilme imkanıdır[213]. Bu başlıkta bireyin özel hayatın gizliliği kapsamında korunan yaşam alanları ele alınacaktır.

a) Kamusal Alan – Özel Hayat Alanı Ayrımının Önemi

TDK kamusal alan kavramını: "kamuya ait, kamu ile ilgili işlerin yapıldığı yer" biçiminde "özel" kelimesi ise "bir kişiyi ilgilendiren", "hususi", "resmi karşıtı" biçiminde tanımlamaktadır[214]. Kamusal alan – özel alan ayrımının kökeni Roma Hukuku'na dayanmaktadır. Romalılar kamusal alanı herkese açık olan, yaygın, devlete ve halka ait; özel alanı ise kişiye ait olan, resmi yönü bulunmayan, kişinin

212) Tandoğan, [1962], Özel Hayatın Korunması, s. 26.
213) Kaboğlu, [1996], Özgürlükler Hukuku, s. 189; Yüksel, [2012], Önleyici Denetim, s. 35; T. Ayhan Beydoğan, "Mahremiyet Hakkı (Özel Hayatın Gizliliği ve Korunması) Basın Hürriyetine Karşı: İngiltere Örneği", DüÇünen Siyaset, S. 10, Kasım, [1999], s. 113.
214) https://sozluk.gov.tr/ (Erişim Tarihi: 04.06.2023).

mahremi biçiminde tanımlamışlardır[215]. Bu tanımların dijital izleme uygulamalarının yaygın olarak kullanıldığı günümüz yaşam alanlarını ifade etmede yetersiz kaldığını belirtmek gerekir. Örneğin işçinin kamusal alanda katıldığı bir eğlencenin diğer işçiler ve işveren tarafından bilinmemesini istemesi bu katılımı özel hayat alanına ilişkin hale getirir. Bu sebeple işçinin bu eğlencedeki verilerinin ayrıca işlemeye konu edilmesi hukuka aykırı veri işleme olarak nitelendirilecektir. Eklemek gerekir ki, günümüzde kamusal alanda gerçekleşen olayların özel hayat alanına ilişkin olması veya kişinin mahrem alanında kalan verilerin kamusal alanda işlenmesi söz konusu olabilmektedir.

Özel hayatın gizliliğinde korunan bireyin özel alanında kalan hayat alanlarıdır ve özel bir yasal düzenleme olmadıkça bunlara müdahale edilemez. Kamusal alan ise kural olarak özel hayata dahil olmadığından, özel hayata dair düzenlemelerle korunması söz konusu değildir[216]. Örneğin güvenlik amacıyla sokakta belirli kişilere yönelik olmayan kamusal nitelikli kamera izlemesi işçi açısından özel hayata müdahale olarak nitelendirilemez.

Bu tespit kamusal alanda kalan durumlarda hiçbir biçiminde özel hayat beklentisi bulunmayacağı anlamına gelmemektedir[217]. Zira işçinin kamusal alanda kalan kişisel verileri de özel hayatın gizliliği ve KVK hukuku düzenlemeleri kapsamında korunmaktadır. Örneğin bir belediyede işçilerin işe devamlılıklarını takip etmek için parmak izi giriş sistemi kullanmaya başlamasını, Danıştay kişisel veri olan parmak izinin kamusal alanda da olsa özel hayatın gizliliği hakkı

215) Gülay Arslan, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı, Beta Yayınları, İstanbul 2011, s. 73.
216) Alpagut, [2019], Kamera Gözetlemesi, 278; Blume, [2010], Data Protection, s. 154; Küzeci, [2020], Kişisel Veriler, s. 152; AİHM, Friedl v. Avusturya kararında kamusal alanda gerçekleşen bir etkinlikte başvuranın görüntülerinin alınmasını sadece güvenlik amaçlı olmasını özel hayatın iç çemberine dahil olmadığını, fotoğrafların anonim kaldığına ve veri işlemeyle ilgili kişilerin kimliklerinin belirlenmesinin yapılmadığına dikkat çekmiştir.
217) Gürsel, [2016], İşçinin Kişisel Verileri, s. 22-23; Kambellari, [2014], Employee Email Monitoring, s. 1-2.

kapsamında bulunduğuna karar vermiştir[218].

Aşağıda incelendiği üzere, kişisel verilerin korunmasında kamusal alan özel alan ayrımı bulunmadığından işçinin kamusal alanda bulunan verileri de kişisel verilerin korunması hukuku kapsamında korunmaktadır. Dahası kişisel verileri koruma mevzuatlarında kamu ve özel ayrımı yapılmadığından kamunun da kişisel verilerin korunmasına ilişkin mevzuat kapsamında hareket etmesi gerekmektedir. Bu itibarla işçinin kamusal alanda işlenen verileri de veri koruma mevzuatı kapsamında korunmaktadır[219].

b) Yalnız Kalma Hakkı Tanımı ve Yeterliliği

Yeni teknolojiler karşısında kişinin korunan değeri ve hukuki korumanın ne şekilde gerçekleştirileceği tartışmalarının özel hayatın korunmasına ilişkin ilk tanımların ortaya çıkmasını sağlamıştır. Yüz otuz yıldan fazla bir süre önce özel hayatın korunmasını haksız fiil sorumluluğundan farklı bir değer olarak ele alan Warren & Brandeis'in makalesinde özel hayatın gizliliğini "yalnız bırakılma hakkı" çerçevesinde tartışılması bu kavramın farkının ortaya konması açısından önemlidir. Warren & Brandeis makale ile özel hayatın gizliliğinin korunması ve korunacak değer hususunda kuramsal ve hukuki bir çerçeve ortaya konmaya çalışılmıştır[220].

Makalede özel hayatın gizliliğinin korunması hakkı "yalnız kalma hakkı" (kişinin rahat bırakılma hakkı) olarak tanımlanmış[221] ve bu hakkın hakların en kapsamlısı ve özgür bireyler tarafından en çok değer verilen hak olarak

218) Danıştay 5. D., 2013/5730 E., 2013/9526 K., Karar Tarihi: 10.12.2013; Danıştay İDDK icra dairelerindeki kameralara ilişkin kararı için bkz. Danıştay İDDK., E. 2021/1603, K. 2021/2631 T. 24.11.2021.
219) Alpagut, [2019], Kamera Gözetlemesi, s. 188.
220) Solove, [2002], Conceptualizing Privacy, s. 1099; Gümüş, [2016], Özel Hayata Saygı, s. 9; Entrikin, [2012], Be Let Alone, s. 210 vd.
221) Irwin R. Kramer, "The Birth of Privacy Law: A Century Since Warren and Brandeis", Catholic University Law Review, Vol. 39, Issue 3, Spring, [1990], s. 703-704.

nitelendirilmiştir[222]. Özel hayatın gizliliğinin korunması hakkına ilişkin bu ilk tanımda özel hayatın gizliliği kavramı müdahale edilmemek ve tercihi doğrultusunda toplumsal alandan kendisini uzak tutma hakkına sahip olmayı ifade etmektedir. Makalede özel hayat ahlaki bir hak veya en azından bireye ilişkin önemli bir değer olarak nitelendirilmiştir. Ayrıca günün koşullarına göre değişecek şekilde özel hayat kavramının iktidar alanına bırakılmaması keyfi sonuçlar ortaya çıkarabilecektir[223].

Bilişim toplumunda yalnız bırakılma hakkının özel hayatın gizliliği kavramını açıklamakta yetersiz kaldığı kabul edilmektedir[224]. Zira toplumsal ve teknolojik gelişmelerle birlikte özel hayat alanı kamusal alana doğru genişlemiş, özel hayatın gizliliğinin korunması hakkının çoğunlukla devletin ihlallerine karşı ileri sürülen bir hak olması niteliği değişmiş, bu hak özel hukuk kişilerince de ihlal edilebilir bir yapıya bürünmüştür[225].

Yukarıda değerlendirildiği üzere, özel hayatın gizliliğinin korunması yalnız kalma hakkı, bireyin özel hayatının gizliliğinin korunması hakkı ve kişiliğinin korunması, bireyin kendi verilerinin kaderini tayin etme hakkı[226] ve bireyin verileri üzerindeki hakimiyetini sağlanması gibi görüşler kapsamında değerlendirmelere konu edilmektedir. Bu yaklaşımların her biri özel hayatın gizliliğini bir yönüyle korunur kılmaktadır. Oysa özel hayat kavramının dinamik niteliği dikkate alındığında özel hayatın tüm bu kavramlar dikkate alınarak değerlendirilmesi gerekmektedir.

---

222) Warren/Brandeis, [1890], Privacy, s. 195; Gary L. Bostwick, "A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision", California Law Review, Vol. 64, No. 6, December, [1976], s. 1447.
223) Miller/Weckert, [2000], Privacy, the Workplace, s. 256.
224) Richard A. Bruyer, "Privacy: A Review and Critique of the Literature", Alberta Law Review, Vol. 43, No. 3, [2006], s. 559.
225) Bărbulescu v. Romanya, § 112-123; AYM, E.Ü. Başvuru Numarası: 2016/13010, § 48.
226) Antoinette Rouvroy/Yves Poullet, The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, Reinventing Data Protection, Springer, [2009], s. 45-46.

c) Üç Alan Teorisi

Kıta Avrupası'nda özel hayatın gizliliği daha çok üç alan teorisi[227] kapsamında incelemeye konu edilmiş[228], ülkemiz doktrini de baskın olarak bu teori çerçevesinde gelişmiştir. Üç alan teorisinde kişi hayat alanlarının sınırlarını her zaman birbirinden kesin olarak ayırmak mümkün olmamakla birlikte, bu teoride kişinin "kamuya açık, kamuya mal olmuş yaşamı", "özel hayat alanı" ve "gizli, mahrem yaşam alanı" bulunmaktadır[229].

aa) Kamuya Açık Ortak Hayat Alanı

Ortak hayat alanı olarak da ifade edilen kamuya açık alanda kişinin başkalarınca bilinmesinden rahatsız olmadığı bilgiler yer alır. Bu alan tüm topluma açıktır ve birey toplumsal ilişkilere ortak hayat alanındaki bilgilerle katılır[230]. Kişinin kamusal hayattaki görünümü, tiyatroya gitmesi, sosyal medyada herkese açık paylaşımda bulunması, etkinliklere katılması, araç kullanması gibi toplumda bir özne olarak kendisini var etmesi ortak hayat alanının görünümlerindendir. Topluma açık olan ortak hayat alanı, özel hayatın gizliliği kapsamında değerlendirilmemekle birlikte bu alanının tamamen hukuki güvencenin dışında olduğu anlamına gelmez. Zira ortak hayat alanına ilişkin olan kişinin kendisini toplumda ifade etmesi sebebiyle ortaya çıkmış durumlar, kişiliğinin korunması, bilinmeme ve kişiliğini geliştirme özgürlüğü de hukuk tarafından korunur[231].

---

227) Sferler Kuramı olarak da isimlendirilen bu teoride kişinin özel yaşam alanı büyükten küçüğe, genişten dara doğru değişen çemberler içine alınarak değerlendirilir. Serozan, [2013], Medeni Hukuk, s 465-466.

228) Lemmens, [2004], The Protection of Privacy between a Rights-Based, s. 609.

229) Serozan, [2013], Medeni Hukuk, s. 465 Bilge Öztan, Medeni Hukukun Temel Kavramları, Yetkin Yayınları, 46. Baskı, Ankara 2021, s. 290-291; Oğuzman/Seliçi/Özdemir, [2016], Kişiler Hukuku, s. 188; Ergun Özsunay, Gerçek Kişilerin Hukuki Durumu, İÜHF Yayınları, İstanbul, [1979], s. 126; Sevimli, [2006], Özel Yaşam, s. 8-9.

230) Ahmet M. Kılıçoğlu, Şeref Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk, 5. Baskı, Ankara, [2016], s. 132-144; Serozan, [2013], Medeni Hukuk, s. 465; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 187-194.

231) Yargıtay: Özel hayat kavramının; kişinin sadece gözlerden uzakta, başkalarıyla paylaşmadığı, kapalı kapılar ardında, dört duvar arasındaki yaşantısı ve mahremiyetinden ibaret değil, herkesin bilmediği veya bilmemesi gereken, istenildiğinde başka kişilere açıklanabilen, tamamen kişiye özel

İleride detaylı ele alındığı üzere kişinin kamusal alandaki verileri de kişisel veri olarak korunmaktadır. Bu itibarla kişisel verilerin korunması hukukunun düzenlemelerinde öngörülmüş yükümlülükleri yerine getirmeden kişinin kamusal alandaki verilerini alenileştirilmiş veri olarak kabul edip, paylaşım iradesi dışında işlemeye konu edilmesi hukuka aykırı veri işleme olarak nitelendirilecektir[232].

bb) Özel Hayat Alanı

Özel hayat alanı kamuya açık olmayan kişinin ailesi, iş arkadaşları, dostları tarafından bilinen, çok yakındakilerle paylaşılan hayat alanını ifade etmektedir[233]. Günümüz insanının bir gerçekliği olan sosyal medya hesaplarında sadece belirli kişilerin erişimine açık yapılan paylaşımlarının da bu kapsamda değerlendirilmesi gerekmektedir. Zira kişi bu tür ortamlarda özel hayat alanını tamamen kontrol edemese de sınırlarını ve kimlerin bu bilgileri bildiği hususunda fikir sahibidir. Yargıtay işyerinde işçiler tarafından oluşturulmuş WhatsApp gruplarında yapılan paylaşımları esas alarak işçilere uygulanan yaptırımları özel hayata müdahale olarak değerlendirmektedir[234].

Özel hayat alanı, özel yaşamın korunması düzenlemelerinin kapsamında bulunduğundan, özel hayat alanına yönelik ihlallerde ilgili kişinin hakları

---

hayat olayları ve bilgilerin tamamını içermesi karşısında, kamuya açık alanda bulunulduğunda dahi, "kalabalığın içinde dikkat çekmezlik, tanınmazlık, bilinmezlik" prensibinin geçerli olduğu ve kamuya açık alana çıkan her kişinin, bu alandaki her görüntü veya sesinin kaydedilip, sürekli ve izinsiz olarak elde bulundurulmasına rıza gösterdiğinin kabulünün mümkün bulunmadığı nazara alınarak, sanığın sübut bulan zincirleme şekilde özel hayatın gizliliğini ihlal suçundan dolayı TCK'nın 134/1 ve 43/2. madde ve fıkrası atfıyla aynı Kanun'un 43/1. madde ve fıkraları gereğince mahkumiyetine karar verilmesi gerekirken, mağdurların kamusal alanda olmaları nedeniyle sanığa yüklenen özel hayatın gizliliğini ihlal suçunun oluşmadığına dair özel hayatı salt mekana indirgeyen ve yasal olmayan gerekçe ile sanığın beraatine karar verilmesi... bozma sebebi saymıştır. Yargıtay 12. CD., E. 2016/2244 K. 2017/5453 T. 21.6.2017; Aynı yönde Yargıtay 12. CD., E. 2019/1 K. 2019/10579 T. 23.10.2019.

232) KVK Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Yayın No: 1, [2019], Ankara, s. 76.

233) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 189; Sevimli, [2006], Özel Yaşam, 9; Ersan Şen, Özel Hayatın Gizliliği ve Korunması, Kazancı Kitap, İstanbul, [1996], s. 229-230.

234) Yargıtay 9. HD., E. 2016/14205 K. 2017/9526 T. 1.6.2017; Yargıtay 9. HD., E. 2016/14206 K. 2017/9527 T. 1.6.2017.

korunmaktadır[235]. Belirmek gerekir ki, kamu yararının bulunduğu olaylar ayrık olarak değerlendirilmektedir[236]. Özel hayat alanı kişinin adı, adresi, yaşı, diğer kimlik bilgileri, ailevi durumu, malvarlığı bilgileri, kişisel verileri gibi kimlik hakkını kapsamına almaktadır. KVK hukuku ve özel hayatın korunmasına ilişkin düzenlemeler bu verilerin hukuka uygun bir amaç bulunmaksızın ve ilgilinin açık rıza olmaksızın işlenmemesini güvence altına almaktadır[237].

cc) Gizli Hayat Alanı

Gizli hayat alanı ise, kişinin "gizli" (mahrem) kalmasında menfaatinin bulunduğu sırları, başkalarıyla paylaşılmasının ve öğrenilmesinin istemediği bütün sırlarını ifade etmektedir. Kişinin hastalıkları, yatak odası, özel mektupları, günlükleri, anı defterleri kişinin gizli alanı olarak kabul edilmektedir[238]. Bir olayın gizli hayat alanında kaldığının tespitinde olayın herkes tarafından bilinmemesi, izlenebilir olmaması (objektif şart) ve olayın gizli tutulması iradesi (sübjektif şart) iki koşulun varlığı aranmaktadır[239].

Gizli hayat alanı merkezde yer alan çekirdek alan dokunulmaz hayat alanıdır ve gizli alanı oluşturmaktadır. Gizli hayat alanı kişinin içsel benliği olarak kabul edilen inançları, duyguları, bedensel duyumları, özel durumları ve diğer insanlar hakkındaki düşünceleri gibi sır alanlarından oluşmaktadır. Aynı zamanda bu alan, korunması gereken özel hayata saygı hakkının büyük kısmını kapsar ve kişi bu alanı

---

235) Yargıtay 4. HD., E. 2014/10463 K. 2015/6652 T. 25.5.2015 tarihli kararında bu hususu: "Yukarıda belirtilen yasal düzenlemelerden de açıkça anlaşılacağı üzere kişinin özel yaşamının gizliliğine dokunulamaz. Kişinin sıfatı ve konumu ne olursa olsun rızası dışında kamuya açıklanamaz. Bunlar kişinin gizli alanını oluşturur. Kişinin hukuka aykırı şekilde konuşmalarının ve görüntüsünün gizlice kayda alınması onun kişilik haklarına ve özel yaşamına saldırı niteliği taşır. Bu ses ve görüntü kayıtlarının herhangi bir yolla kamuoyuna yansıtılması, ifşa edilmesi de kişilik haklarına yapılmış ikinci bir saldırı niteliğindedir." biçiminde değerlendirmiştir. Yargıtay Hukuk Genel Kurulu'nun 07/03/2007 tarih 2007/4-98 esas 2007/110 karar sayılı kararı da aynı doğrultudadır.

236) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 189-190.

237) Kaboğlu, [1996], Özgürlükler Hukuku, s.189.

238) Serozan, [2013], Medeni Hukuk, s. 466.

239) Kılıçoğlu, [2016], Hukuksal Sorumluluk, s. 86-87; Volkan Sırabaşı, İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi), Ankara [2007], s. 37.

yakınları, doktorlar ve psikologlar gibi çok az kişiye açıklanabilir[240]. Ayrıca bu alanın açıklandığı kişilerin açıklanan bilgileri ifşa etmeme yükümlülüğü bulunmaktadır[241]. Kişi hayat alanlarına ilişkin genel kabul gören bu üçlü ayrım kesin ve katı bir ayrım olarak görülmemeli kuramsal bir tutanak olarak kabul edilmelidir[242].

Özel hayat kavramını tanımlamak için iç içe geçmiş çemberler kapsamında değerlendirme yapan üç alan teorisinin, kişisel verilerin korunması hakkının öngördüğü korumalarla uyum gösteren yönleri bulunmaktadır. Örneğin kişisel verilerin korunması hukukunda "özel nitelikli kişisel veri" olarak düzenlenen ve işlenmesi daha katı kurallara bağlanan özel hayatın sır alanında bulunan kişinin cinsel yaşamı, sağlık bilgileri, ırksal kökeni ve dinsel inancı, felsefi tercihi özel hayatın aynı zamanda çemberler teorisinde gizli hayat alanı olarak değerlendirmeye konu edilmektedir[243].

II. Veri Kavramı ve Kişisel Verilerin Korunması Hakkının Doğuşu

Dijital izlemede işçiyi belirli veya belirlenebilir hale getiren görüntü, ses, araç kullanım alışkanlıkları, internet trafik izleri, işyeri giriş şifresi, bilgisayar kullanımı, smart ID kayıtları, biyometrik verileri, sağlık verileri gibi kişisel veya özel nitelikli kişisel verileri işlemeye konu edilmektedir. İş ilişkisinde kullanılan

240) Miller/Weckert, [2000], Privacy, the Workplace, s. 256.
241) İşyerinde işçilerin özel hayat alanlarına ilişkin çıkarımsamalara rehberlik eden bir diğer çalışma Antroplog Edward T. Hall'in sosyal mesafelerle ilgili çalışmalardır. Hall'in gerçekleştirdiği çalışma özel hayatın gizliliğinin neye göre tespit edilebileceğini tespitte yol gösterici niteliktedir. Hall, sosyal mesafeler çalışmasında kişinin etkileşim alanını fiziksel mesafelerin ölçülmesine göre belirleyerek özel hayat alanının samimi olan kişiler arasında 15 ila 45 santimetre arasında olduğunu ve 15 santimetrenin altındaki mesafenin mahrem alan olduğunu (fısıltılar, sarılmalar ve okşamaların bulunduğu alan); kişisel mesafenin 46 santimetre ile 120 santimetreye kadar çıktığını buna meslektaşlar arasındaki konuşmalar, toplantılar ve partiler gibi hayat alanının girdiğini; sosyal alanın 360 santimetreye kadar çıktığını ve işçilerle, müşterilerle ve iş arkadaşlarıyla kurulan ilişkinin buna örnek olduğunu belirtir. Genel alan ise kişinin 360 santimetre üzerindeki hayat alanının ve sınırı bulunmayan kamusal alanı, gruplara hitap etme bu alan kapsamında yer alır. Bert-Jaap Koops, "Privacy Spaces", West Virginia Law Review, Vol. 121, No. 2, Winter, [2018], s. 616 vd.; https://tretse.com/edward-t-hall-and-the-study-of-personal-space/ (Erişim Tarihi: 17.07.2022).
242) Serozan, [2013], Medeni Hukuk, s. 466, "3c" atıflı Hausheer / Aebbi-Müller.
243) Küzeci, [2023], Verilerin Korunması s. 52-53.

dijital izleme uygulamaları veri bazlı çalışan sistemler olduğundan veri kavramının ve kişisel veri koruma hakkının düşünsel arka planı bu başlıkta ele alınacaktır.

1. Veri Kavramı ve Verinin Artan Önemi

"Veri" işlenmemiş, çiğ bilgi olarak (enformasyon) bilginin ham maddesini oluşturmaktadır. Bu ham maddenin belli kategorilerde işlenmesi, düşünce ile sistemli hale getirilmesi, pişirilmesi[244] ve bir şeyle ilişkilendirilmesi veriden anlamı bulunan bilgiyi ortaya çıkarır[245]. Verinin yoğun işlemeye konu edildiği günümüzde kişilik haklarına yönelik ihlallerinin en bariz örneklerinden birisi dijital izleme ve diğer otomatik veri işleme uygulamalarıyla elde edilen verilerden oluşan "Big Data" (büyük veri)[246] veri tabanlarıdır. İşçi, tüketici, hizmet alıcısı gibi gerçek kişilerin verilerden oluşan büyük veri ulaştığı değer ve kullanıcısına sunduğu imkanlar sebebiyle 21. yüzyılın petrolü olarak nitelendirilmektedir[247]. Zira büyük veri ilgili kişinin profilini oluşturma olanağını kullanıcısına vererek bu kişinin algılarını, alışkanlıklarını yönlendirebilme ve denetimini olanaklı hale getirmektedir. Ayrıca işçilerin davranışları ve performanslarıyla ilgili oluşturulan

244) Peter Burke, Bilginin Toplumsal Tarihi, Tarih Vakfı Yurt Yayınları, (Çev. Mete Tunçay), İstanbul, [2001], s. 18.
245) Hüseyin Tokcan, Bilginin Üretimi ve Kullanımı Açısından Bilgi Yönetimi: Üniversite'de Akademik Yöneticilerin Bilgi Yönetimi Algıları Üzerine Bir Uygulama, Doktora Tezi, [2015], s. 11-12.
246) "Büyük veri" terimi tanımlanması zor bir kavramdır. Zira bu kavramın karşılığı kullanıldığı sektöre bağlı olarak değişir, ancak genel olarak bu terim; (1) büyük hacimli (2) karmaşık, yapılandırılmış ve çok hızlı veri kümeleri ve (3) çok çeşitli verilerin teknoloji aracılığıyla otomatik işlenmesini içermektedir. Büyük veri aynı zamanda sürekli tekrar eden veri yakalama, toplama ve işleme süreçlerinde gelişmiş teknolojik yeteneği ifade etmektedir. Timothy A. Asta, "Guardians of the Galaxy of Personal Data: Assessing the Threat of Big Data and Examining Potential Corporate and Governmental Solutions", Florida State University Law Review, Vol. 45, No. 1, Fall, [2017], s. 261-312, s. 267.
Büyük Veri, bir gerçek kişiye ilişkin bilgileri de içerebilir. Örneğin büyük veri içinde bir kişiyle ilgili herhangi bir bilgi ve bir ad, fotoğraf, e-posta adresi, banka bilgileri, sosyal ağ web sitelerindeki gönderiler, tıbbi bilgiler veya bir bilgisayar IP adresinden herhangi bir şey olabilir. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7041862/
247) https://customertimes.com/insights/data-is-the-new-oil/ (Erişim Tarihi: 27.02.2022). https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (Erişim Tarihi: 27.02.2022).

büyük veri işçileri değerlendirmek için de kullanılabilmektedir[248].

Veri izleme (dataveillance) ile elde edilen büyük veri aynı petrol gibi işlenmekte, rafine edilmekte, çeşitli pazarlarda alınabilmekte ve satılabilmektedir. Bu itibarla veri işleme süreçleri veri madenciliği (data mining)[249] biçiminde ifade edilerek yapılan iş petrol rafinerisine ve maden çıkarmaya benzetilmektedir. Veri madenciliği ile oluşturulan büyük veri sayesinde yeni yatırımlar, yeni işyeri modelleri, işçinin farklı işlere yönlendirilebilmesi ve performansını ölçme imkanını ortaya çıktığından bu veri yeni ekonominin temel enerji kaynağı olarak kabul edilmektedir. Büyük veri aynı zamanda işçilerin işe giriş ve çıkış saatleri, anketler veya fazla mesai talepleri gibi işçi verileri üzerindeki küçük analizler için veya veri kümeleri üzerinde çıkarım yapmak isteyen işverenler için yapay zeka destekli uygulamalara veri sağlamaktadır. Dahası yapay zeka temelli uygulamalar dijital izleme, bilgisayar veya telefonlar üzerindeki günlük işçi etkileşimi sonucu ortaya çıkan büyük veri üzerinde çıkarım yapma, veriye bir bağlam kapsamında anlam kazandırma olanağını işverenlere vermiştir[250].

Olaya ekonomi açısından bakıldığında yapılan iş masummuş gibi görünse de gerçekleştirilen veri işleme süreci insan hakları, kişilik hakları, kişisel veri ve özel hayatın gizliliğinin korunması kapsamında değerlendirildiğinde aynı şeyi söylemek mümkün değildir. Konuya bu çerçevede bakan akademik çalışmalarda veri madenciliği ağır eleştirilere tabi tutularak yapılan işin günümüzün kişinin özel hayatını şeffaflaştıran, ticari girişimler vasıtasıyla kişiyi kamu malı haline dönüştüren sinsi ve tehlikeli bir girişim olduğu ileri sürülmektedir[251]. Gerçekte giderek karmaşıklaşan toplumsal yapı ve iş ilişkisinde huzurun yakalanabilmesi ve

248) Darrell S. Gay/Abigail M. Kagan, "Big Data and Employment Law: What Employers and Their Legal Counsel Need to Know", ABA Journal of Labor and Employment Law, Vol. 33, No. 2, Winter [2018], s. 198.
249) Joseph S. Fulda, "Data Mining and Privacy", Albany Law Journal of Science & Technology, Vol. 11, No. 1, [2000], s. 107-108.
250) Gay/Kagan, [2018], Big Data and Employment Law, s. 196.
251) John J. Thauberger, "Right to Privacy", Saskatchewan Bar Review, Vol. 30, No. 3, September, [1965], s. 167-168; Wendi S. Lazar/Nantiya Ruan, "Is There a Future for Work", Georgetown Journal on Poverty Law and Policy, Vol. 25, No. 3, Spring, [2018], s. 351.

kişinin kişiliğine bağlı hakları üzerindeki haklarının korunabilmesi için işçinin çatışan menfaatleri işverenin menfaatlerinin uyumlu hale getirecek yasal düzenlemelerin yapılasına bağlıdır.

Kişisel verilerin korunması hakkının gelişmesinde öncü olmuş Anglo-Amerikan hukuk sistemi ile Kıta Avrupası hukuk sisteminde kavramın koruduğu değerler ve ifadelendirdiği kavramlar farklı bağlam ve dinamiklerle gelişim göstermiştir. Anglo-Amerikan hukuk sistemine dahil ülkelerde kişisel verilerin korunması kavramı yerine özel hayatın gizliliği (privacy) kavramı kullanılmaktadır. Kıta Avrupası'nda ise "veri güvenliği" ve "verilerin korunması" kavramları kabul görmüş ve bu kavramın ilk kez Almancada kullanıldığı tespit edilmiştir. Belirtmek gerekir ki, kişisel verilerin korunmasında korunan değer veri değil, verinin ilgili olduğu kişidir. Özel hayatın gizliliğinin korunması ve kişisel verilerin korunması bağlamında korunan kişi ise gerçek kişilerdir[252]. Bu sebeple KVK hukuku, veriyi değil verinin ilgili olduğu bireyi (iş ilişkisinde işçi) ve bireyin verileri üzerindeki haklarının korunmasını amaçlamaktadır[253]. Bu nedenle "verilerin korunması" (data protection) kavramının yanlış bir kullanım olduğu ve bunun kişisel verileri de içine alabilen her türlü verinin (veri güvenliği) güvenliği ile karıştırılabileceğini savunan yaklaşımlar da bulunmaktadır[254].

Ülkemizde kullanılan "veri koruma hukuku" ifadesi ise, tüm verilerin korunacağı anlamında bir kullanım değildir. Bu kullanımdan kast edilen gerçek kişinin verilerinin korunmasıdır. Zira ülkemiz kişisel verilerinin korunması düzenlemeleri gerçek kişiyi esas almakta ve veriyi değil verinin ilgili olduğu kişiyi korumayı amaçlamaktadır. Kişisel verilerin korunmasının anayasal dayanağı olan m. 20/3 hükmünde "kişisel veri" kavramı kullanılmış KVKK düzenlemelerinde de kişisel veri kavramı esas alınarak düzenlemeler gerçekleştirilmiştir[255]. Veri koruma

252) Küzeci, [2020], Kişisel Veriler, s. 18 vd.
253) Gürsel, [2016], İşçinin Kişisel Verileri, s. 40; Küzeci, [2020], Kişisel Veriler, s. 19.
254) Küzeci, [2020], Kişisel Veriler, s. 15.
255) KVKK m. 3/1 ç) İlgili kişi: "Kişisel verisi işlenen gerçek kişiyi", d) Kişisel veri: "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi." KVKK'nın amacını düzenleyen m.

hukuku ifadesinin kullanımının sebeplerinden birisi kişisel verileri koruma mevzuatımıza kaynaklık eden AB düzenlemelerinde "data protection" kavramının kullanılmasıdır. Öte yandan 1992 tarihli İsviçre Veri Koruma Kanunu'nda sadece kişisel verilerin değil tüm verilerin gizliliğinin korunması esasının benimsenerek düzenleme yapılmıştır. 1 Eylül 2023 tarihinde yürürlüğe giren İsviçre Veri Koruma Kanunu'nda ise kişisel veriler esas alınarak düzenleme yapılarak, önceki yaklaşım terk edilmiş ve kişisel verilerin korunması esası benimsenmiştir[256]. Bu itibarla "veri koruma hukuku" kavramının kullanılmasından ilgili gerçek kişinin verilerinin korunması ve kişisel verileri koruma mevzuatı anlaşılmalıdır.

İş Kanunu'nda işçi, iş sözleşmesine dayanarak çalışan gerçek kişi; işveren ise "işçi çalıştıran gerçek veya tüzel kişiye yahut tüzel kişiliği olmayan kurum ve kuruluşlar" (KVK hukukunda veri sorumlusu) biçiminde tanımlanmıştır (İş Kanunu m.2/1). KVKK'da verisi işlenen ilgili kişi, "gerçek kişi" biçiminde tanımlandığından (KVKK m. 3/1-ç) işçinin verilerinin işlenmesi için TBK m. 419/1 ile KVKK yükümlülüklerinin birlikte dikkate alınması gerekmektedir[257].

2. Kişisel Verilerin Korunması Hakkının Doğuşu

Özel hayatın gizliliğinin korunması hakkına göre nispeten yeni bir hak olan kişisel verilerin korunması hakkı gelişen teknolojinin ortaya çıkardığı ve çoğunlukla kamusal alanda yer alan kişisel verilerin otomatik veya kısmen otomatik olarak elde edilmesi, depolanması, aktarılması (veri işleme)[258] gibi kişisel veri

---

1 düzenlemesi: "Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir." biçimindedir. Bu düzenlemelerde görüleceği üzere veri değil verinin ilgili olduğu kişi korunmaktadır.

256) İsviçre Veri Koruma Kanunu, https://www.fedlex.admin.ch/eli/oc/2022/491/de Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), (Erişim Tarihi: 04.12.2023).

257) TBK m. 419 ile KVKK ilişkisi için bkz. § 6. I.

258) KVKK m. 3/1-e bendine göre kişisel verilerin işlenmesi: "Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi,

işleme faaliyetlerine bir tepki olarak gelişen hak arayışlarının bir sonucu olarak 1970'lerde ortaya çıkmıştır[259]. Bu hakkın ortaya çıkmasında ve gelişmesinde işverenlerin, işçilerin verilerini otomatik yöntemlerle işleyerek bir veri bankası oluşturmalarına işçilerin verdiği tepkiler öncülük etmiştir[260].

Bilişim teknolojilerinin işyerinde iş yapma sürecinin bir parçası haline dönüşmesinden önce işverenin işçileri üzerindeki denetimi ekonomik gücüne ve işyerine ilişkin düzenlemelerine bağlıyken teknolojik gelişmelere bağlı olarak bu teknoloji merkezli bir dijital denetime dönüşmüştür[261]. Bu sebeple dünyanın ilk modern kişisel veri koruma yasası kişisel verileri otomatik işlemeye konu eden teknolojilerin işyerinde kullanılarak işçilere ilişkin bir veri bankasının oluşturulması üzerine işçilerin eylemlerinin bir sonucu olarak 1970'de Almanya'nın Hessen Federal Eyaleti'nde kabul edilmiştir[262]. İlk yasal düzenlemeden kısa bir süre sonra 1973'te İsveç, 1977'de Almanya, 1978'de Fransa gibi ülkelerde kişisel veri korumaya ilişkin ilk düzenlemeler yapılmıştır[263]. Örneğin, 6 Ocak 1978'de düzenlenmiş olan 78-17 sayılı Fransız Veri Koruma Kanunu[264] m. 31'de ilgili kişinin açık rızası olmaksızın ırkı, kökeni veya siyasi, felsefi veya dini görüşleri, sendika üyeliğine ilişkin verilerin doğrudan veya dolaylı olarak bilgisayara kaydedilmesi ve saklanması yasaklanmıştır[265]. AB düzeyinde bu tarihlerde kişisel verilerin işlenmesinin hukuka uygun gerçekleştirildiğinin kabulü

---

sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi" ifade etmektedir.

259) Spiros Simitis, "From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union", Comparative Labor Law and Policy Journal, Vol. 19, No. 3, Spring, [1998], s. 351-353; Küzeci, [2020], Kişisel Veriler, s. 117-118.

260) Colin J. Bennett, "Regulating Privacy, Data Protection and Public Policy in Europe and the United States", Cornell University Press, [1992], s. 48-49; Küzeci, [2020], Kişisel Veriler, s. 118.

261) Matthew W. Finkin, "Privacy: Its Constitution and Vicissitudes - A Half-Century on", Canadian Labour and Employment Law Journal, Vol. 18, No. 2, [2015], s. 359.

262) Simitis, [1998], Employee Data, s. 351 vd.; Küzeci, [2020], Kişisel Veriler, s. 117; Bennett, [1992], Regulating Privacy, s. 48-49.

263) Michael D. Kirby, "Transborder Data Flows and the Basic Rules of Data Privacy", Stanford Journal of International Law, 16, [1980], s. 39 ve 35-38. dipnotlar.

264) ACT 78-17 of 6 January [1978] on Data Processing, Data Files and Individual Liberties, https://www.ssi.ens.fr/textes/a78-17-text.html#art31 (Erişim Tarihi: 07.08.2022).

265) İngilizce tam metni için bkz. https://www.ssi.ens.fr/textes/a78-17-text.html#art31

için ilgili kişinin rızasının alınması koşulu aranmıştır. Bu koşul kişisel verilerin korunmasına ilişkin olan 95/46 EC sayılı Direktif'in kabulüyle bu düzenlemeye de yansımıştır[266].

Verilerin korunmasına ilişkin düzenlemelerin ilk örneklerinin yapıldığı ülkelerden birisi de İsveç'tir. İsveç hükümeti kamu sektöründe verilerin otomatik sistemler üzerinden bilgisayar vasıtasıyla işlenmesi için 1960'lardan itibaren ciddi yatırımlar yapmıştır. Bu gelişmenin bir sonucu olarak 1960'ların sonlarına doğru kişisel verilerin işlenmesinin muğlak olduğu ve işlenen yoğun veri sebebiyle kişilerin özel hayatlarının şeffaflaştırdığı tartışmasını başlatmıştır. Bunun üzerine kişisel verilerin işlenmesinde şeffaflığın sağlanması için çalışmalar başlatılmış ve 11 Mayıs 1973 tarihinde İsveç Veri Kanunu yürürlüğe girmiştir. İsveç'te veri koruma mevzuatının bu kadar hızlı gelişmesinde bu ülkenin 1766'lara kadar giden belgelere erişim hakkı veren ve şeffaflığı öngören bir mevzuat geleneğine sahip olmasıdır[267].

Kişisel verileri koruma yasalarına öncülük eden AB üye ülkelerinin ve ABD'nin özel hayatın gizliliğini ve kişisel verilerin korunmasına ilişkin veri gizliliği yasaları, 1970'lerin Adil Bilgi Uygulama İlkelerinden (Fair Information Practice Principles-FIPP/ Adil Bilgi Uygulama İlkeleri) etkilenmiştir[268]. FIPP ilkeleri etkin veri güvenliğinin sekiz temel dayanağını ortaya koymuştur. Bu ilkeler:

---

266) Maria Dumitru, "Is There a Right of Option between the Processing of Personal Data Legal Bases Regarding General Data Protection Regulation 2016/679?", European Journal of Law and Public Administration, Vol. 6, No. 2, [2019], s. 287.

267) Jonathan Steele, "Data Protection: An Opening Door? The Relationship between Accessibility and Privacy in Sweden in an EU Perspective", Liverpool Law Review, Vol. 24, No. 1-2, January, [2002], s. 21.

268) ABD Federal Ticaret Komisyonu'nun Adil Bilgi Uygulama İlkeleri (FIPP'ler), 1970'lerde çevrimiçi kuruluşların kişisel verileri işleme ve kullanma biçiminin adil olması ve yeterli veri gizliliği korumasının sağlanmasına yönelik çalışmaların sonucu ortaya çıkmıştır. İlkeler, elektronik bir pazarda adil bilgi uygulamasına ilişkin yaygın olarak kabul edilen kavramlardan oluşmaktadır. OECD, 1980'de bu ilkelere benzer kavramları Kişisel Verilerin Mahremiyetinin Korunması ve Sınır Ötesi Akışına İlişkin OECD Kılavuz İlkeleri'nde önermiştir. Bu yönde önemli düzenlemeler içeren Avrupa Konseyi, Kişisel Verilerin Otomatik İşlenmesi Karşılığında Bireylerin Korunmasına İlişkin bir Sözleşme 1980'de kabul edilmiştir. Robert Gellman, Fair Information Practices: A Basic History, Version 2.22, April 6, [2022], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020 (Erişim Tarihi: 05.01.2023).

1) şeffaflık, 2) amaç belirleme, 3) kullanım sınırlaması, 4) veri minimizasyonu, 5) veri doğruluğu, 6) bireysel katılım, 7) güvenlik ve 8) hesap verebilirlik[269] başlıklarından oluşmaktadır. FIPP ilkelerinin geliştirilmesinde ABD öncü olmasına rağmen geçen sürede bu ilkeleri tam olarak benimsedikleri söylenemez. AB ise bu ilkelere sosyal değer olarak yaklaşmış ve FIPP ilkelerini veri koruma mevzuatlarına dahil etmek için bilinçli bir çaba göstermiştir[270].

AB düzenlemelerinde işçilerin işyerindeki mahremiyeti ve kişisel verilerin korunması insan onuru ile ilişkilendirerek açık bir insan hakkı olarak nitelendirmektedir. İşyeri mahremiyetine ilişkin bu temel yaklaşım AB hukukunun, konuyla ilgili ABD hukukundan farklı bir yönde gelişmesini sağlamıştır. Bu itibarla işyeri mahremiyetini insan onuru ile ilişkilendirerek işçilerin kişisel verilerinin gizliliğinin korunmasını amaçlayan ileri düzenlemeler AB'de yapılmıştır[271]. Örneğin Fransız yargı içtihatları işveren tarafından işçilerin özel kullanımına izin verse de vermese de e-postalarda gerçekleştirecek bir izlemeyi daha katı koşullara bağlamakta ve işçileri korumaktadır[272]. Aynı doğrultuda Almanya, İtalya, Hollanda, İspanya ve Birleşik Krallık gibi ülkeler de dahil olmak üzere bazı Avrupa Topluluğu Üye Devletleri, işçi iletişimlerinin sürekli olarak izlenmesini kesinlikle yasaklamakta ve dijital izlemeye yalnızca işçinin suç işlemesine ilişkin somut bulgular bulunması ve belirli işçilerin haklarının ihlal edilmesi gibi çok sınırlı durumlarda izin vermektedir[273].

İşçilerin verilerinin korunmasını doğrudan düzenleyerek işverenin yönetim hakkını sınırlandıran düzenleme Fransa'da 1992 tarihli Fransız İş Kanunu'nda

269) Justin Brookman, "Protecting Privacy in an Era of Weakening Regulation", Harvard Law & Policy Review, Vol. 9, No. 2, Summer, [2015], s. 357.
270) Bradyn Fairclough, "Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It", Journal of Corporation Law, Vol. 42, No. 2, Winter, [2016], s. 464.
271) Levin, [2009], Dignity in The Workplace, s. 103.
272) Determann/Sprague, [2011], Intrusive Monitoring ,s. 1031.
273) Determann/ Sprague, [2011], Intrusive Monitoring, s. 1032.

yapılan değişikliklerle gerçekleştirilmiştir[274]. Bu tarihte Fransız İş Kanunu'nun L.121-6 maddesini (sonraki değişiklikte 1221-6) yürürlüğe konarak işverenlerin işçi adaylarından veya işçilerden isteyeceği bilgilerin işçinin söz konusu işi yapma yetkinliklerine ve genel olarak mesleki yeteneklerine ilişkin olma şartına bağlamıştır[275]. Fransız İş Kanunu'na 1992 tarihinde yapılan eklemelerle işçilerin kişisel verilerini ilgilendiren beş başlıkta düzenleme yapılmıştır. Bu düzenlemelerin en önemli sonuçlarından birisi işçi özgürlüklerinin tehlikede olduğu durumlarda devreye girmesi ve işçinin verilerini korumasıdır. Örneğin, bir işveren sahada çalışan işçinin araçlarına lokasyon bazlı izleme ve anlık raporlama uygulaması takmayı planladığında veya bir işveren, işçinin kişisel verilerini ilgilendiren bir konuda bireysel bir karar verdiğinde iş kanununa eklenen bu düzenlemeleri gözeterek bilgilendirme yükümlülüğünü yerine getirmek zorundadır[276]. Eklemek gerekir ki, bu hususta henüz bir içtihat ortaya çıkmamışken Fransız doktrini iş başvurularında sabıka kayıtlarının ayrıntılarının istenmemesi gerektiğini genel olarak kabul etmekteydi[277].

Fransız İş Kanunu'nda işverenin, işçilerin verilerini dijital izleme uygulamalarıyla işlemesi durumunda, gerçekleştirilen izlemenin boyutunu, tüm yöntem ve tekniklerinin işçiye ve işçi adayına bildirilmesini zorunlu hale getirilmiştir. Ayrıca işveren, işçilerin hak ve özgürlüklerine dijital izlemeyle gerçekleştirilen müdahalenin meşru amaç kapsamında sınırlı ve ölçülü olduğunu ve kişisel verilerinin işlenmesinde orantılı hareket edildiğini belgelemekle yükümlüdür[278].

İş sözleşmesinin ortaya çıkardığı ilişkinin ayırt edici unsuru olan işçinin

---

274) Enik Pogace, "Employees' Data Protection in the Workplace and Its Legal Implications: A Comparative Overview of EU's Legal Framework", International In-House Counsel Journal, Vol. 10, No. 37, Autumn, [2016], s. 1-2.
275) Christophe Vigneau, "Information Technology and Workers' Privacy: The French Law", Comparative Labor Law & Policy Journal, Vol. 23, No. 2, Winter, [2002], s. 369.
276) Pogace, [2016], Employees' Data, s. 2.
277) Vigneau, [2022], The French Law, s. 369.
278) Vigneau, [2022], The French Law, s. 370.

işverene kişisel-hukuki bağımlılığı, AB'nin kişisel verilerin korunmasına ilişkin düzenlemelerinin işçinin rızasının sınırlı durumlarda geçerli olması kabulünü gerektirmiştir[279]. Bununla birlikte işçiler açısından özel bir düzenleme getiren Genel Veri Koruma Tüzüğü (GVKT / GDPR- General Data Protection Regulation) m. 88'de genel olarak ölçülülük ilkesi kapsamında işverenin ve işçilerin hakları açısından bir denge kurmaya çalışmış ve işçilerin kişisel verilerinin korunması için üye ülkelere spesifik düzenleme yapma yetkisi tanımıştır. Üye ülkeler iç hukuklarında GVKT ile çatışan düzenlemeleri bulunması halinde öncelikli olarak GVKT düzenlemelerini uygulayacaktır. Öte yandan iç hukuk düzenlemelerinde bireyin temel hak ve özgürlükleri ile kişisel verilerini koruyan daha lehe hukuki düzenlemeler yer alıyorsa ve bunlar GVKT ile çatışmıyorsa bu düzenlemeler uygulama alanı bulur[280].

III. Kişisel Verilerinin Korunması

Kamusal alanda bulunan, çoğunlukla özel hayata dahil olmayan ve korunması için özel bir düzenleme de bulunmayan işçi verileri, kişisel verilerin korunması hukukunun düzenlemeleri olmasa iş sözleşmesinin ortaya çıkardığı ilişkinin niteliği gereği hukuka uygunluk sebepleri kapsamında işveren, işçiye bilgi vermeksizin özel menfaati olan denetim hakkı kapsamında işlemeye konu edebilir. Bundan dolayı kişilik hakkı ve özel hayatın gizliliğini koruyan hükümler kapsamında işçinin kişisel verilerini korumak güçtür[281].

279) EU, [2018], Handbook, s. 136; Article 29 WP, Employment Context, s. 26; Christopher Kuner, European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, United Kingdom, [2007], s. 211.
280) F.J. Düwell/S. Brink, Die EU Datenschutz-Grundverordnung und der Beschäftigtendatenschutz, Neue Zeitschrift für Arbeitsrecht, s. 666; Aktaran, Atila Erkal, "Avrupa Genel Veri Koruma Düzenlemesi Bağlamında Memurların Kişisel Verilerinin Korunması Hakkı", Anayasa Yargısı, Cilt: 37, Sayı: 2, [2020], s. 219.
281) Alpagut, [2019], Kamera Gözetlemesi, s. 274; Blume, [2010], Data Protection, s. 154.

1. Özel Hayat ve Kişisel Verilerin Korunması İlişkisi

Kamu hukukunda insan hakkının, özel hukukta ise kişilik hakkının konusu olan kişisel verilerin korunmasının yasal düzenlemelere konu edilmesi özel hayatın gizliliğinin korunmasıyla yakından ilişkilidir. Bir dönem kişisel verilerin korunması hakkı özel hayatın gizliliğinin korunması hakkı kapsamında değerlendirilmiş ve korunmaya çalışılmıştır[282]. Aslında kişisel verilerin korunması hakkı, başta özel hayatın gizliliği ve ifade özgürlüğü olmak üzere birçok temel hak ve özgürlükle birbirini destekler veya bazı durumlarda yarışır. Özel hayata saygı hakkının fikri temellerinde gelişen kişisel verilerin korunması hakkı, özel hayatın gizliliğinin korunması hakkı ile birbirini destekleyen haklardır[283]. Zira bireyin özel hayatının gizliliğini koruyabilmek için onun başkalarının eline geçen verilerinin korunmasını da gerektirmektedir. Özel hayat bilişim uygulamalarındaki gelişmelerin (özellikle sosyal medyanın) etkisiyle kamusal alana doğru yayılım göstermiş ve mahremiyet alanıyla sınırlandırılmayacak geniş kapsamlı bir kavrama dönüşmüştür[284]. Kişisel veri ise bir kişiyi belirli veya belirlenebilir hale getiren her türlü bilgi olduğundan koruma için özel hayat tartışması yapmadan, bireyi belirleyen veya belirlenebilir hale getiren bir bilginin varlığı yeterlidir.

Birbirini destekleyen haklar olan kişisel verilerin korunması hakkı ile özel hayatın gizliliğinin korunması hakkı birbirinden farklı haklarıdır. Zira özel hayatın gizliliğinin korunması hakkı bireye hem rahatsız edilmeyen bir özel hayat alanı hem de özel alanına müdahaleler üzerinde kontrol imkanı sağlamaktadır. Bu alanlara yönelik müdahaleler daha çok kamu hukuku ve emredici özel hukuk düzenlemeleri kapsamında korunmaktadır. Özel hayatın korunması gibi anayasal bir hak olan kişisel verilerin korunması hakkı ise sadece kişinin özel hayatıyla sınırlı bir hak

282) Anayasa'nın 20. maddesinin üst başlığı "Özel hayatın gizliliği ve korunması" madde başlığı ise "Özel hayatın gizliliği" biçimindedir. Kişisel verilerin korunması m. 20'nin 3. fıkrasında Ek fıkra: 7/5/2010 tarih ve 5982 sayılı Kanun m. 2 ile eklenmiştir.
283) Küzeci, [2023], Verilerin Korunması, s. 51.
284) KVK Kurumu, Kişisel Verilerin Korunması Kanunu ve Uygulaması Rehberi, s. 8-9. https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf (Erişim Tarihi: 02.11.2022).

değildir. Kişisel verilerin korunması hakkı kişinin, onu belirli veya belirlenebilir hale getiren tüm bilgileri üzerindeki haklarını belirli işleme koşullarına bağlamaktadır[285].

Özel hayatın gizliliğini ve kişisel verileri koruyan düzenlemeler yasa hükmüne konu edilmeden önce işçilerin özel hayatı ve kişisel verileri haksız fiile ilişkin düzenlemeler[286], kişiliği koruyan medeni hukuk düzenlemeleri ve ceza hukuku normları kapsamında korunmaya çalışılmıştır[287]. İşçilerin özel hayatlarının ve kişisel verilerinin korunmasının ceza hukukunun ve medeni hukukun ek korumasından faydalanması kuşkusuz gereklidir fakat büyük veri, akıllı profilleme, giyilebilir teknolojiler ve üreten yapay zeka gibi dijital izleme uygulamaları karşısında işçinin kişisel verilerini bu düzenlemeler kapsamında korumak güçtür.

Teknolojik gelişmelerin otomatik veri işlemeyi olanaklı hala getirmesi ve bireyin özel hayatının gizliliğinin ihlal edilme biçimini değişmesinin de etkisiyle KVK hukuku farklı bir dinamikle gelişim sergilemiş ve bir gerçek kişiyi belirli veya belirlenebilir hale getiren her türlü bilginin hangi durumlarda, ne miktarda ve hangi yükümlülükler yerine getirilerek işlenebileceğini ve nasıl korunacağına ilişkin ilkeleri ortaya koymuştur[288]. Önemle belirtmek gerekir ki, kişisel verilerin korunması hukuku açısından bireyin bu haklarının korunması için ilgili kişiye

---

285) Peter Blok, Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en het Amerikaanse recht, Boom Juridische Uitgevers, 2002, Aktaran Cuijpers, [2007], Private Life, s. 312; Damla Gürpınar, "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk", DEÜ Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı- [2017], s. 681; Baysal, [2023], Kişisel Verilerin İşlenmesi, 527; Gürsel, [2016], İşçinin Kişisel Verileri, s. 114; Nazlı Elbir, Kişiliğin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması, Doktora Tezi, Ankara, [2020], s. 44.

286) Palmer, [2011], History of Privacy, s. 69-73; Finkin, [2015], Privacy, s. 360-361; David Price, "The Emergence of a UK Data Protection Law", Yearbook of Law Computers and Technology, 1, [1984], s. 131-132.

287) Edward J. Bloustein**,** Priacy As an Aspect of Human Dignity, Edited by, Ferdinand David Schoeman, Cambridge University Press, Second Edition, Cambridge [2007], s. 182.

288) Nurşen Caniklioğlu, "Kişisel Verilerin Korunması Açısından İşçilerin Hakları", Prof. Dr. Turhan Esener III. İş Hukuku Uluslararası Kongresi, (19-21 Nisan 2018), İstanbul, s. 246; Baysal, [2023], Kişisel Verilerin İşlenmesi, 527; Gürsel, [2016], İşçinin Kişisel Verileri, s. 114; Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 44; Bu konudaki tartışmalar ile AİHM ve ABAD kararları için bkz. Kokott/Sabotta, [2013], The distinction between privacy and data protection, s. 222- 228.

ilişkin bir bilginin varlığı yeterli olup, koruma ve yükümlülükler açısından kamu veya özel ayrımı da bulunmamaktadır[289].

Medeni Kanun'da kişiliği koruyucu değerler tahdidi olarak sınırlandırılmadığından kişiliği koruyucu düzenlemeler birçok durumda uygulama alanı bulmaktadır[290]. Ne var ki, dijital izlemeyi sınırlandıran kişilik hakkının korunmasına ilişkin olan MK, TBK ve İş Kanunu düzenlemeleri genel olarak gizli izleme ve kişilik haklarına bir saldırı söz konusu olduğunda uygulama alanı bulur. Başka bir ifadeyle bu düzenlemeler bireyin özel hayatının ihlali, kişisel verilerinin hukuka aykırı işlenmesi durumunda koruma sağlayan ve sözleşme ilişkisinin sınırlarını belirleyen düzenlemelerdir.

Dijital izleme uygulamalarıyla kişinin verilerinin işlenme düzeyinin arttığı; akıllı profilleme, duygu durumları, gen teknolojisi ve biyometrik verilerle izlemenin örneklerinin ortaya çıktığı günümüzde çoğunlukla kamusal alanda bulunan kişisel verileri kişilik hakkını korumaya yönelik hükümlerle korumak güç olduğundan özel yasal düzenlemelerin gerçekleştirilmesi zorunludur[291]. Aksi durumda iş sözleşmesi gibi hukuki ilişkilerin bulunduğu olaylarda korumayı hukuka aykırı saldırı düzeyine indirgeyen özel hukuk düzenlemeleri yeterli korumayı sağlamayacaktır. Zira özel hukuk düzenlemeleri özellikle işverenin koruma borcuna aykırı davranması, kişisel verileri hukuka aykırı işlemesi, özel hayat alanlarına iş ilişkisini aşacak şekilde müdahale etmesi durumunda devreye girmektedir.

Kanun hükmü kapsamında ancak bir gerçek kişi olabilen işçinin kişisel verileri anayasal bir hak olarak kişisel verilerin korunması hukukunun düzenlemeleri kapsamında korunmaktadır. Kişisel verilerin korunması hukuku düzenlemelerinde kamusal alan – özel alan, kişi bazında farklılıklar ve kamu

289) Alpagut, [2019], Kamera Gözetlemesi, s. 278-279.
290) Serozan, [2013], Medeni Hukuk, s. 453.
291) Serozan, [2013], Medeni Hukuk, s. 453-454.

kurumu veya özel kuruluş ayrımı bulunmadığından bir gerçek kişi olan işçinin verileri kişisel verilerin korunması hukuku kapsamında belirli işleme şartlarına tabi tutularak işlenmesi gerekmektedir[292].

Kişisel verilerin korunması hukuku kişiye ilişkin maddi olmayan değerleri korumayı garanti eden kişiliğe ve özel hayata saygı hakkına ilişkin düzenlemelerden farklı olarak kişisel verilere atfedilen maddi değeri ve bu verileri işleme hakkını da korumaktadır. Dahası ilgili kişinin verilerinin kanun hükmüne aykırı biçimde işlenmesi sebebiyle bir zararının oluşması halinde bunu genel düzenlemeler kapsamında tazmine konu edebilmesinin yanında kişisel verilerin korunması hukukunun düzenlemeleri kapsamında da zararlarını ileri sürülebilmesi mümkündür (KVKK m. 11/2-ğ). Ayrıca kişisel verilerin korunması hukuku kişiye ilişkin maddi olmayan (kimlik verileri, kişilik verileri, lokasyon verileri gibi) kamusal alanda paylaşılan kişisel veriler ile maddi değeri olan verileri (fotoğrafı, ilgili kişinin hususiyetini taşıyan eserleri vb.) de ilgili kişiyi belirlenebilir hale getirmesi kaydıyla işlenmesini aynı düzenlemeler kapsamında değerlendirerek koruma sağlamaktadır[293].

Eklemek gerekir ki, dijital izleme uygulamalarının bireyin verilerini otomatik işlediği durumlarda ve bireyin/işçinin özel alanına hukuka aykırı bir müdahale meydana geldiğinde onların haklarını etkin bir şekilde korunmasını isteyeceği kurum ve düzenlemelerin varlığı önemli hale gelmiştir[294]. Aksi durumda hukuka uygunluk sebeplerinin varlığı söz konusu olduğunda bireyin dijital kopyasının oluşturulması, verileri vasıtasıyla özel hayatının şeffaflaştırılması gibi sonuçlar ortaya çıkabilecektir. Kişisel verilerin korunması hukuku bu yönüyle de kendi özgünlüğünde gelişerek, bireyin işlenen verileriyle ilgili başvuru

292) Alpagut, [2019], Kamera Gözetlemesi, s. 274; Gürsel, [2016], İşçinin Kişisel Verileri, s. 181.
293) Colette Cuijpers, "A Private Law Approach to Privacy; Mandatory Law Obliged", SCRIPTed: A Journal of Law, Technology and Society, Vol. 4, No. 4, September, [2007], s. 315, (Cuijpers, [2007], Private Life).
294) Küzeci, [2020], Kişisel Veriler, s. 290; Kokott/Sabotta, [2013], The distinction between privacy and data protection, s. 223.

yapabileceği ve veri işleme sürecine ilişkin denetim ve kararlar oluşturabilen EDPB ve KVK Kurumu gibi bağımsız düzenleyici ve denetleyici otoriteler ortaya çıkarmıştır[295].

2. Bir İnsan Hakkı Olarak İşçinin Kişisel Verilerinin Korunması

Öğretide kişisel verilerin korunması gerçekleştirilen yasal düzenlemeler, veri korumanın ortaya çıktığı toplumsal yapı ve teknolojik gelişmeler esas alarak üç nesil yaklaşımı çerçevesinde incelemeye konu edilmektedir. Buna göre birinci nesil yasal düzenlemeler, büyük miktarda kişisel veri işleyen belirli veri sorumlularının (esas olarak devlet) kişisel verileri otomatik olarak işlenmesini düzenleme amacını gütmektedir. Bireysel bilgisayarların ortaya çıkması ve yaygınlaşmasıyla birlikte, kişisel verilerin daha geniş bir kitle (işletmeler veya özel kişiler) tarafından otomatik olarak işlenmesi gündeme gelince ikinci nesil olarak kabul edilen düzenlemeler ortaya çıkmıştır. OECD'nin ve ILO'nun metinleri, AB 95/46 sayılı Direktifi ve Avrupa Konseyi'nin 108 sayılı Sözleşmesi bu kapsamda değerlendirilmektedir. Bu düzenlemeler, yalnızca birkaç veri sorumlusuna (veri kontrolörüne) yönelik düzenlemeler olmaktan öte, genel olarak kişiyi bilgilendirme ve bireyin kişisel verileri üzerinde belirleyici olabilecek hakları içeren düzenlemelerden oluşmaktadır. Üçüncü nesil veri koruma düzenlemeleri olan AB Genel Veri Koruma Tüzüğü, internetin kitlesel olarak yaygınlaşması, sosyal medya siteleri, profil oluşturma, mobil cihazların kullanımı vb. üçüncü nesil bir düzenlemenin gerekliliği kapsamında ortaya çıkmıştır. GVKT'de bu hususları kapsayacak şekilde kişisel verilerin korunması esası benimsenmiştir[296].

AB üye ülkelerinde ve ülkemizde kişisel verilerin korunmasını insan hakkı olarak kabul görmüş anayasal güçte korunacak hukuki düzenlemelere konu

295) Karen E.C. Levy, "Relational Big Data", Stanford Law Review Online, 66, [2013-2014] s. 74.
296) Adrienn Lukács, Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary, Iurisperitus Publishers, Szeged, [2021], s. 55-56.

edilmiştir[297]. Kişisel verilerin korunması hakkı sadece kişinin bireysel çıkarlarıyla da ilişkili değildir. Zira kişisel verilerin korunması hakkı temel bir insan hakkı olarak insan onuru, itibarı, toplumsal varoluşu, aile ve ev hayatının gizliliğinin korunmasıyla da ilgilidir[298]. Dahası, Avrupa yaklaşımına göre kişisel verilerin korunması "insanlık onurunun bir tezahürü" olarak kabul gördüğünden, kişisel verileri işlenen ilgili kişiye herhangi bir tehdit olmadığında dahi bu hakları korunduğundan, veri sahiplerine verileri üzerinde bir hakimiyet alanı ve bir dereceye kadar kontrol imkanı vermektedir[299]. Ülkemiz hukuk sisteminde kişisel verilerin korunmasında Avrupa yaklaşımı esas alınmış olup, kişisel verilerinin korunması insan hakkı olarak anayasal düzeyde koruma sağlanacak biçimde düzenlemeye konu edilmiştir (Anayasa m. 20, KVKK m. 20)[300]. İş hukukunda anayasa düzenlemeleri doğrudan uygulama alanı bulduğundan işçinin özel hayatının gizliliğinin ve kişisel verilerinin korunması anayasal düzenlemeleri kapsamında korunmasının ortaya çıkardığı güçlü korumadan işçi de faydalanır[301].

Ülkemizde kişisel verilerin korunmasının bir insan hakkı olarak kabul gördüğü, 6698 sayılı KVKK'nın Genel Gerekçesi'nde "çağımızda insan haklarının korunması bilincinin gelişmesine paralel olarak, kişisel verilerin korunmasının da

297) Corien Prins, "Digital Diversity: Protecting Indentities Instead of Individual Data", Hetbinnenste Buiten, Leiden, [2010], s. 280-296; Küzeci, [2020], Kişisel Veriler, s. 74.
298) Avrupa Konseyi Parlamenterler Meclisi, özel hayatın gizliliğinin korunması hakkını "minimum müdahale ile kendi hayatını yaşama hakkı" olarak ifade etmiştir. Bunun aynı zamanda "özel, aile ve ev hayatı, fiziksel ve ahlaki bütünlük, onur ve itibar, yanlış bir ithama maruz bırakılmaktan kaçınma, alakasız ve utanç verici gerçeklerin ortaya çıkmaması, özel fotoğrafların izinsiz, özel iletişimin kötüye kullanılmasına karşı koruma, birey tarafından gizli olarak verilen veya alınan bilgilerin ifşasına karşı koruma." Haklarını kapsadığını deklare etmiştir. Council of Europe, Parliamentary Assembly: Declaration on mass communication media and Human Rights, Resolution 428 (1970) 23 January, [1970]; Bkz.
http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en. (Erişim tarihi: 11.09.2022).
299) Başak Bak, "Reviving a European Idea: Author's Right of Withdrawal and the Right to Be Forgotten under the EU's General Data Protection Regulation (GDPR)", SCRIPTed: A Journal of Law, Technology and Society, Vol. 19, No. 1, February, [2022], s. 145.
300) KVK Kurumu'nun görevlerinin düzenlendiği KVKK m. 20'de kurumun görevlerinden birisi de m. 20/1-ç bendinde: "…Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna" faaliyet raporunu sunma biçiminde düzenlenmiştir.
301) Süzek, [2019], İş Hukuku, s. 53; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 23 vd.

önemi her geçen gün artmaktadır" ve "Anayasa'nın 20. maddesinde yapılan düzenlemeyle, kişisel verilerin korunması temel bir insan hakkı olarak güvence altına alınmış" ifadeleriyle ortaya konmuştur[302]. Anayasa'da kişisel verilerin korunmasının temel bir insan hakkı olarak görülmesi aynı zamanda bu hakka ilişkin düzenlemelerin ancak kanunla gerçekleştirilebileceği, Cumhurbaşkanlığı Kararnameleri ile kişisel verilere ilişkin düzenleme yapılamayacağı sonucunu ortaya çıkarmaktadır[303].

Anayasamızda kişilik değerlerine ve kişiliğin korunmasına özel bir önem verilmiş ve kişinin "dokunulmaz" bir varlık olduğu kabul edilmiştir. Bunun bir sonucu olarak insanın maddi ve manevi varlığı her değerin üstünde yer alan bir değer olarak Anayasa'da yer almıştır. Anayasa m. 20/2'de ise bu dokunulmazlığın istisnaları sınırlı şekilde sayılmıştır[304]. Anayasa m. 20/2 ve 3'te özel hayatın gizliliği ve kişisel veriler, kişinin konutunun dokunulmazlığı Anayasa m. 21'de ve haberleşme hürriyeti: "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır." biçiminde m. 22'de düzenlenmiştir. Özel hayatın gizliliğinin korunmasına ilişkin düzenlemeler getiren bu maddelerin devamı fıkralarında bu haklara hangi durumda müdahale edilebileceğine ilişkin düzenlemeler getirmektedir. Bu itibarla Anayasanın 20. maddesinde güvence altına alınan özel hayatın gizliliği hakkı; kişinin şeref ve itibarının korunması, adının ve kimliğinin korunması, mesleki hayatında kişisel verilerinin korunması gibi birçok başlıkta güvenceler içermektedir.

Kişisel verilerin korunması aynı zamanda ifade özgürlüğüyle yakından ilişkidir. Zira "kişinin hak ve ödevleri" başlığında düzenlenen Anayasa'nın 25.

---

302) Mehmet Bedii Kaya/Furkan Güven Taştan, Kişisel Veri Koruma Hukuku-Mevzuat-İçtihat-Bibliyografya, 2. Baskı, İstanbul, [2019], s. 53-54.
303) Murat Volkan Dülger, "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, S. 5, [2018], s. 104.
304) Okur, [2013], Elektronik Gözetleme, s. 30 vd.; K. Ahmet Sevimli, "Türk Borçlar Kanunu m. 417 ve İş Sağlığı ve Güvenliği Kanunu Işığında Genel Olarak İşçinin Kişiliğinin Korunması", Çalışma ve Toplum, 2013/1, 36, s. 111; Süzek, [2019], İş Hukuku, s. 387-388; Zeki Hafızoğulları, "İnsan Hakkı Olarak Kişilik Hakları ve Kişilik Haklarının Korunması", AÜHF Dergisi, Yıl 1997, Cilt 46, Sayı 1, 1 – 40.

maddesinde "herkesin düşünce ve kanaat hürriyeti" bulunduğu ve kimsenin bunları açıklamaya zorlanamayacağı düzenlenmiştir. Aynı doğrultuda Anayasa m. 26'da ifade özgürlüğü düzenlenmiş ve herkesin düşünce ve kanaatini çeşitli vasıtalarla ifade etme ve yayma hakkı anayasal güvenceye alınmıştır. Düşünce ve ifade özgürlüğü hakkının kişisel verilerin korunması hakkı ile yakın ilişkili olduğu açıktır. İfade özgürlüğünün sınırları ise m. 26/2'de düzenlenmiş ve hangi durumlarda bunun sınırlandırılacağı sayılmıştır[305].

Öte yandan sosyal devlet niteliği aynı zamanda devlete kişinin maddi ve manevi varlığını koruma ve geliştirme için gerekli şartları oluşturma pozitif yükümlülüğünü yüklemektedir[306]. Zira, "devletin temel amaç ve görevlerinin" düzenlendiği Anayasa m. 5'te devlete bireyin maddi ve manevi varlığını korumak ve geliştirmek için bir şeyler yapma pozitif yükümlülüğü yüklemektedir[307]. Düzenlemeye göre devlet; "kişinin temel hak ve hürriyetlerini… sınırlayan engelleri kaldırma" ve "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlama" yükümlülüğü bulunmaktadır.

Eklemek gerekir ki toplu iş hukuku, işçi sendikası ile işveren veya işveren sendikası arasında pazarlık usulü ile belirli düzenlemeleri yapma olanağı vermektedir. Bu düzenlemeler de özel hayatın gizliliğini ve işçinin kişisel verileri üzerindeki haklarını ihlal edecek nitelikte olamaz[308]. Toplu İş Sözleşmesi (TİS) düzenlemeleri anayasal haklar olan "kanun önünde eşitlik" (Anayasa m. 10) ve özel hayatın gizliliğinin korunması düzenlemeleriyle ilgilidir. Aynı doğrultuda sendika üyeliği Anayasa m. 20 düzenlemesinin bir gereği olarak düzenlenmiş olan KVKK'da (m. 6/1) özel nitelikli kişisel veri olarak sayılmıştır. Bundan dolayı veri

305) Evra Çetin, İnsan Hakları Avrupa Sözleşmesi'nin 8-11. Maddeleri Bağlamında Çalışanların Hakları, İstanbul, [2015], s. 356 vd.
306) AYM'nin 25.2.1975 tarih ve 1973/38 E., 1975/23 K. sayılı kararı, AMKD, Sayı: 3, s. 214-294; Yılmaz Aliefendioğlu, "Anayasa Mahkemesinin İşlevsel Yönü", Amme İdaresi Dergisi, Yıl [1986], Cilt 19, Sayı 1, s. 23-54.
307) M. Yavuz Sabuncu, "Temel Hakların Anayasal Konumu Üzerine", İnsan Hakları Yıllığı, Yıl [1985-1986], Cilt 7, Sayı 1, s. 15-26; Anayasa Mahkemesi 60 Yıl 60 Makale, C. 1, [2022], s. 672.
308) Gürsel, [2016], İşçinin Kişisel Verileri, s. 187.

sorumlusu işverenin, işçinin sendika üyeliğine ilişkin verilerini özel nitelikli kişisel verilerin işlenme şartlarına uygun işlemesi zorunludur[309].

Kişisel verilerin korunmasının Anayasa m. 20/3'te temel haklar arasında sayılması bu hakka yönelik saldırılarda kişiyi hem devlete karşı koruma olanağı sağlamakta hem de devlete bu hakkı korumaya yönelik düzenlemeler yapma yükümlülüğü yüklemektedir. Böylelikle devlet veya işveren fark etmeksizin hiyerarşik ilişkinin güçlü tarafının bu alandaki keyfi güç kullanımını önlemekte veya gerçekleştirilecek müdahalelere sınırlamalar getirmektedir[310]. Temel hakların dikey etkisi kişiyi devletin keyfi güç kullanımına karşı koruyup bu taraflar arasındaki ilişkileri düzenlerken, özel hukuk ilişkilerini ilgilendiren yatay etki eş düzeydeki taraflar arasındaki ilişkiyi düzenler ve koruma sağlamaktadır. Aslında bu iki yönlü koruyucu etki birbirinden ayrılmaz ve temel hakkı somutlaştırmaktadır[311]. Anayasa, iş hukuku kaynakları arasında en üstte yer aldığından m. 20'nin iş ilişkisine doğrudan bir etkisi olduğu gibi, aynı zamanda devlete iş ilişkisinde Anayasa'nın 20. maddesinde temel hak olarak düzenlenmiş olan özel hayatın gizliliğinin ve kişisel verilerin korunmasında koruma yükümlülüğü de yüklemektedir.

AYM kararlarında devletin pozitif yükümlülüklerine vurgu yapılarak özel hukuk kişileri tarafından kişinin özel hayatının gizliliğine yönelik bir müdahalenin bulunması halinde bunun devletin pozitif yükümlülükleri kapsamında ele alınabileceğine karar vermektedir. Zira bu yükümlülük kapsamında devlet hem kamu makamlarına hem de diğer kişilerin ve bireyin kendisinin fiillerinden kaynaklı risklere karşı kişinin korunması yükümlülüğü bulunduğuna vurgu

309) Bkz. § 6. II. 4. i.
310) Zafer Gören, "Temel Hak Genel Teorisi", 4. Baskı, DEÜHFY, İzmir, [2000], s. 85; Detlev W. Belling/Nurten İnce, "Türk-Alman Hukukunda Temel Hakların Özel Hukuk İlişkilerine Etkisi", Legal Hukuk Dergisi, C.12, S. 137, [2014], s. 5; Meltem Caniklioğlu Dikmen, "Anlamı, Kapsamı ve Sınırlarıyla Temel Haklar ve Anayasalarımız", Mahmut Tevfik Birsel'e Armağan, DEÜHFY, İzmir, [2001], s. 462.
311) Belling/İnce, [2000], Temel Hak, s. 5; Zafer Gören, "Temel Hakların Düzenlenmesi ve Somutlaştırılması", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl 19, S. 38, Yaz, [2020/2], s. 3.

yapmaktadır[312].

İncelendiği üzere, iş ilişkisinde kullanılan dijital izleme uygulamalarının etkilediği işçinin temel hakları; özel hayata saygı hakkı, kişisel veriler, haberleşmenin gizliliği hakkı ve ifade özgürlüğü gibi haklarıdır. Bununla birlikte, dijital izleme uygulamaları veri işleyen sistemler olduğundan bu uygulamalarda işçinin asıl tehlikeye atılan hakları özel hayata saygı hakkı ve kişisel verileri üzerindeki haklarıdır. İş hukukunda "işçinin kişilik hakkı" kavramının işçi yönünden ortaya çıkardığı sonuç, genel olarak insan hakkı kavramının ortaya çıkardığı sonucun önemine benzetilmektedir[313]. Zira kişiliği oluşturan tüm değerleri ifade eden kişilik hakkı mutlak hak olarak kişiliği oluşturan tüm değerleri ifade ettiğinden, bu mutlak hakka yönelen her müdahalenin hukuka aykırı olduğu genel olarak kabul edilmektedir[314]. İş hukukunda yer alan sosyal kamu düzeni normları sayesinde devletin, özel hukuk ilişkisi olan iş sözleşmesine müdahalesi ve işçinin kişiliğini korumaya yönelik TBK m. 417 ve benzeri düzenlemelerde kişilik hakkını korumaya yönelik tercih kendisini bariz biçimde göstermektedir[315]. Bu noktada eklemek gerekir ki, işçinin ifade özgürlüğüyle ilgili olarak iş hukukunda doğrudan bir düzenleme bulunmadığından konu AİHM[316], AYM ve Yargıtay içtihatları çerçevesinde çözüme kavuşturulmaktadır.

---

312) AYM, Ömür Kara ve Onursal Özbek, § 46; AYM, Ali Çığır, Başvuru Numarası: 2015/19298, 8/5/2019, § 32-33; AYM, Erol Kumcu, Başvuru Numarası: 2015/18988, 9/5/2019, § 32-33; U.B., Başvuru Numarası: 2015/3175, 10/10/2019, § 33-34; AYM, Fırat Gerçek, Başvuru Numarası: 2019/25604, § 64-65.

313) Hayrunnisa Özdemir, "Haberleşmenin Gizliliği ve Kişisel Veriler", EÜHFD, C.13, S.1-2, [2009], s. 286.

314) Sevimli, [2013], İşçinin Kişiliğinin Korunması, s. 112; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 176.

315) Süzek, [2019], İş Hukuku, s. 33.

316) Ülkemiz 18 Mayıs 1954'te AİHS'yi onaylamış, 28 Ocak 1987'de bireysel başvuru hakkını tanımıştır. Mahkemenin zorunlu yargı yetkisini ise, 28 Ocak 1990 tarihinde kabul etmiştir.

3. İş Sözleşmesinin Ortaya Çıkardığı İlişkinin İşçinin Kişisel Verilerine Etkisi

Toplumsal gücün kullanılmasında düzenleyici bir teknik olan hukuk[317], dijital izlemede bir yanda işçinin özel hayatının gizliliğini ve kişisel verilerini korumada diğer yanda ise mülkiyetin korunması, yasal yükümlülük, işyeri verimliliğinin artırılması ve işyeri güvenliliğinin sağlanması gibi sebeplerle işverence dijital izleme uygulamaları kullanma hakkı arasında bir denge oluşturur[318]. Hukuki görünüm olarak eşit taraflar olan işçi ve işveren arasında hiyerarşik bir ilişki kuran iş sözleşmesi[319] gerçekte işçinin, işverene bağımlı olarak işverenin emir ve otoritesi altında iş görme borcunu ifa etmesi işçi ile işveren arasında kişisel bir bağımlılık ilişkisi ortaya çıkarmaktadır[320]. Bağımlılık ilişkisi işçiyi sözleşme ilişkisinde zayıf konumda bıraktığından, dengenin yasal düzenlemelerle ve toplu sözleşmelerle sağlanması gerekmektedir.

İşverenlerin kullandığı dijital izleme uygulamalarında, işçiyi belirli veya belirlenebilir duruma getiren her türlü bilginin işlenmesi kişisel veri işlenmesi olarak nitelendirilir[321]. Kişisel veri tanımı kapsamında işçinin gizli alanında kalan sırları, sosyal medya hesabında herkesle paylaştığı tatil fotoğrafı, konum bilgileri,

---

317) Paul Davies/Mark Freedland (Edited by), Kahn-Freund's Labour and the Law, Third Edition, Stevens&Sons, London, [1983], s. 14.
318) Paul F. Gerhart, "Employee Privacy Rights: Introduction and Overview", Comparative Labor Law Journal, Vol. 17, Issue .1, Fall, [1995], s. 5; Aloisi/Gramano, [2019], Artificial Intelligence Is Watching You, s. 97.
319) Kübra Doğan Yenisey, İş Hukukunun Emredici Yapısı, Beta Yayınevi, İstanbul, [2014], s. 1.
320) Süzek, [2019], İş Hukuku, s. 36.
321) KVKK m. 3/1-d bendinde kişisel veri: "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" ve GVKT m. 4/1'de kişisel veri: "tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir ('veri sahibi'); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir" biçiminde tanımlanmıştır. OECD tanımı da bu kapsamdadır, OECD Özel Hayatın Korunması ve Kişisel Verilerin Sınır Ötesi Aktarımına İlişkin Kılavuz İlkeler, 1980 ve Kılavuz'da 2013 yılında gerçekleştirilen revize. ILO'nun 1997'de kabul ettiği "İşçilerin Kişisel Verilerinin Korunması Hakkında Uygulama Kodu" benzer tanım yapılmıştır. ILO, Code of Practice on the Protection of Workers' Personal Data, https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf (Erişim Tarihi: 12.10.2022).

işçiye özgü davranışsal veya fizyolojik verileri, iş başvurusunda paylaştığı mesleki deneyim bilgileri gibi geniş bir yelpazede yer alan veriler kişisel veriyi oluşturmaktadır. Özellikle yeni iletişim araçları ve bilişim teknolojilerindeki gelişmelerin kişisel verilerin korunmasının önüne çıkardığı sorunlar, işçinin kendisini sosyal medyada alenileştirmesi[322] ve iş ilişkisinin işçinin özel hayatı üzerindeki sınırlandırıcı etkisi onların kişisel verilerinin diğer insanlara göre aynı düzeyde bir korumayı gerektirmemesi sonucunu ortaya çıkarmaktadır. Bu sebeple iş sözleşmesinin karakteristik özelliği olan bağımlılık unsuru sebebiyle özel hayatın gizliliği hakkı iş ilişkisinde sınırlanmakta ve işverenin, işçinin özel hayat alanı olarak nitelendirilebilecek konularda da belirli düzenlemeler yapmaları ve dijital izleme gerçekleştirmesi hukuka uygun görülmektedir[323]. Dahası sözleşme ilişkisiyle doğrudan doğruya ilişkili olduğu durumlarda kişisel veri işlenmesi KVK hukukunda açık rıza alınmaksızın veri işlemenin hukuka uygunluk sebebi olarak düzenlenmiştir (KVKK m. 5/2-c).

İşverenin, işçilerin özel hayatının gizliliğinin ve kişisel verilerinin korunması yükümlülüğü iş görüşmesi sürecinde işlenen verileri de kapsayacak şekilde, sözleşmenin yürürlüğü süresince ve sözleşmenin sona ermesi[324] ile bu verilerin imhasına kadar geçen dönemi kapsamaktadır. Bu itibarla özel hayatın gizliliğinin ve kişisel verilerin korunması hakkının işçiler açısından gözetilmesi

322) Yargıtay sosyal medyada herkese aleni paylaşılan fotoğrafın özel hayata ilişkin görüntü olarak kabul edilmese dahi bunun kişisel veri olduğunu ve TCK m. 136/1 kapsamındaki suçun işleneceğine karar vermektedir. Bu hususta Yargıtay 12. CD., 2021/2426 E., 2021/6589 K. ve 6.10.2021 tarihli kararında özetle: "Mağdurun twitterda paylaştığı fotoğrafı onun özel hayatına ilişkin görüntü olarak kabul edilemezse de kişisel veri niteliğinde olduğu açıktır, bu sebeple buradan alarak "bu tweettr daha neler gorucek:))))) hahah" şeklinde tekrar paylaşılması 136/1 kapsamında değerlendirilir. Bu itibarla fotoğrafın alınarak sanığın kendi sayfasında paylaşılmasının hukuka aykırı olduğunda tereddüt bulunmamasına karşın, sanık hakkında TCK. 136/1'deki kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet hükmü kurulması gerekirken katılanın fotoğrafını herkese açık şekilde Twitter'da paylaştığı, herhangi bir kısıtlama yapmadığından fotoğrafın başkaları tarafından görülmesinden ve paylaşılmasından rahatsızlık duymadığı, fotoğrafının alınmasının ve yorum yapılmasının yüklenen suçu oluşturmayacağı biçimindeki yasal ve yeterli olmayan gerekçelere dayalı olarak yazılı şekilde beraat hükmü kurulması yasaya aykırıdır." biçiminde karar vermiştir.
323) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 113-119; AYM, E.Ü. Başvuru Numarası: 2016/13010, § 47.
324) Alpagut, [2019], Kamera Gözetlemesi, s. 276.

gereken yerlerden birisi de işçi adaylarına ilişkin işverenlerin yaptığı internet ve sosyal medya araştırmalarında elde ettiği verilerle ilgili olmalıdır. Zira işverenler iş görüşmesinden önce işçi adaylarıyla ilgili olarak internet ve sosyal medya araştırması yapmakta, işçi adayının dijital izlerini takip etmek için çalışmalar yürütmektedir[325].

İş ilişkisinde uygulanan dijital izlemede kişisel verileri işlenen veri konusu grup birer gerçek kişi olan işçiler, işçi adayları ve eski işçilerdir. İş Kanunu'nda işçi iş sözleşmesiyle çalışan gerçek kişi olarak tanımlanmıştır. KVKK'da kişisel verileri işlenen ilgili kişi: "kişisel verisi işlenen gerçek kişi" biçiminde tanımlanmıştır (KVKK m. 3/1-c). İş Kanunu'nda işçinin özel hayatının gizliliğini koruyan doğrudan bir yasal düzenleme bulunmamakla birlikte Kanun işçilerin özel hayatlarının gizliliğinin korunması hususunda tamamen sessiz de kalmamıştır. Örneğin İş Kanunu m. 5/1'de işverenin eşit davranma borcu, m. 18/3'te fesih için geçerli sebep oluşturmayacak haller, m. 75'te işverenin işçi için oluşturacağı özlük dosyasında yer alan kimlik, eğitim bilgileri gibi işçi hakkında edinilen bilgilere ilişkin işverene yüklenen yükümlülükler ve m. 24/2 (b), (c) ve (d) bentlerinde düzenlenmiş olan işçinin haklı nedenle iş sözleşmesini derhal fesih hakkına ilişkin hükümler işçinin özel hayatının gizliliğinin korunmasına ilişkin olaylarda uygulama alanı bulan düzenlemeler barındırmaktadır[326]. İşçinin kişisel verilerinin korunmasını doğrudan düzenleyen hüküm ise, TBK m. 419/1'dir. İlgili başlıkta detaylı ele alınan düzenlemeye göre işveren, işçiye ait kişisel verileri, ancak işçinin işe uygunluğuyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde işleyebilir[327].

---

325) Sosyal Medya Geleceğinizi Karartmasın başlıklı yazı: https://www.gazeteduvar.com.tr/hayat/2016/10/25/sosyal-medya-geleceginizi-karartmasin (Erişim Tarihi: 11.03.2022).

326) Süzek, [2019], İş Hukuku, s. 399-401; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 182 vd.; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 323-324; Zeki Okur, "Türk İş Hukukunda İşçinin Kişisel Verilerinin Korunması Hakkı", İş Dünyası ve Hukuk, Prof. Dr. Tankut Centel'e Armağan, İstanbul Üniversitesi Yayınları No. 5006, İstanbul, [2011], s. 370, 399; Gürsel, [2016], İşçinin Kişisel Verileri, s. 40 vd.

327) TBK m. 419 ile kişisel verilerin korunması hukuku ilişkisi için bkz. § 6. I. 1.

§ 3. DİJİTAL İZLEME UYGULAMALARINDA TARAF MENFAATLERİ

Bu başlıkta işverenin dijital izleme uygulamalarını kullanma menfaatleri olan işçiyi denetleme, işyeri verimliliği, idareye karşı yükümlülükler, mülkiyeti korumak ve güvenlik başlıkları ele alınacaktır. Devamında işçinin dijital izlemede tehlikeye atılan menfaatleri ve devamlı izlenme düşüncesinin işçi üzerindeki etkisi değerlendirilecektir.

I. Dijital İzleme: İşveren Menfaatleri Açısından

İşverenin dijital izleme menfaati başlıca üç başlık kapsamında gruplandırılmaktadır. İlk olarak işverenler işyerindeki maddi ve maddi olmayan varlıkların mülkiyetini korumak, işyeri düzenini ve güvenliğini sağlamak, işyerleri sırlarını korumak, işyeri verimini artırmak, bilişim sistemlerinin güvenliğini sağlamak, bilişim sistemlerine yetkisiz erişimi engellemek, ağ güvenliğini sağlamak ve suçu önlemek[328] menfaatleri kapsamında dijital izleme gerçekleştirmektedir. İkinci olarak işveren, işçinin sözleşme yükümlülüğüne, işyeri prosedürlerine ve yasal düzenlemelere uygun işini ifa edip etmediğini denetleme menfaati kapsamında dijital izleme uygulamaları kullanabilir. Son olarak işveren TBK m. 417'de doğrudan düzenlenen koruma borcu ile İSGK kapsamındaki yasal yükümlülüklerini yerine getirme, işçinin bu prosedürlere uyduğunu denetleme ve işçinin sağlık ve güvenliğini sağlama menfaati kapsamında dijital izleme uygulaması kullanabilir[329].

1. İş Görme Borcunun İfasını Denetlemek ve İşyeri Verimliliğini Artırma

İşyeri veriminin artırılması doğrudan performans süreçlerini yönetmek ve

328) Kris Klein/Vivian Gates, Privacy in Employment: Control of Personal Information in the Workplace, Thomson Canada Limited, Toronto, [2005], s. 52.
329) Okur, [2013], Elektronik Gözetleme, s. 24.

işçileri denetlemekle ilgili olduğundan işverenler çeşitli dijital izleme uygulaması kullanabilmektedir. Bu uygulamalarda işçinin performansı ölçülerek zamanının ne kadarını işe ayırdığı, çalışma süresince neler yaptığı, interneti iş amacı dışında ne kadar kullandığı gibi soruların cevabını bulabilir[330].

a) İşçinin Denetlenmesi

İşverenin dijital izleme uygulaması kullanması önleme ve tespit amacıyla olmak üzere; "performansı izlemek için bilgi, bilişim cihazları kullanmak", "performans dışı olayları izlemek ve değerlendirmek için bilgi, bilişim cihazı kullanmak" ve "inceleme, araştırma, adli bilişim ve veri kurtarma kapsamında bilgi, bilişim cihazları kullanmak" olmak üzere üç başlık altında gruplandırılmaktadır[331]. Dijital izlemede denetim amacı ile denetim menfaati birbirinden farklı kavramlardır. Denetim amacı "önleme amaçlı" ve "tespit amaçlı" olarak iki amaç kapsamında gerçekleştirilebilir. Bu iki amacın birlikte bulunduğu örnekler de bulunabilmektedir. Örneğin önleme amaçlı dijital izleme ile suçun önlenmesi, sözleşmeye aykırılıkların önlenmesi hedeflenir. Önleme amaçlı dijital izlemeyle gerçekleştirilecek denetim aynı zamanda işçide işini sözleşme hükümlerine uygun gerçekleştirme baskısı oluşturacağından, işçinin iş dışı uğraşılarla zaman geçirmesini önleyebilir[332].

Tespit amaçlı dijital izlemeyle gerçekleştirilen denetimde ise, sözleşmeye aykırılık veya suç şüphesinin açıklığa[333] kavuşturulması amacı bulunmaktadır. Böylelikle işçinin hukuka aykırı davranışları belgelenir ve elde edilen deliller iş akdinin sona erdirilmesinde veya ortaya çıkabilecek diğer hukuki ihtilaflarda kullanılabilir[334].

---

330) Boehmer, [1992], Artificial Monitoring and Surveillance, s. 745-746.
331) Lasprogata/King/Pillay, [2004], Electronic Employee Monitoring, s. 18.
332) Okur, [2013], Elektronik Gözetleme, s. 25.
333) Köpke v. Almanya kararında AİHM, suç şüphesinin bulunması durumunda sınırlı ve kapsamı belirli olmak kaydı ile gizli kamera tedbirine başvurulabileceğine karar vermiştir. (Appl. No. 420/07), Judgment of ECHR of 05 October, [2010].
334) Okur, [2013], Elektronik Gözetleme, s. 25.

Dijital izleme uygulamalarıyla işçinin denetlenmesindeki işverenin menfaatleri iş görme borcunun ifasını denetlemek, mülkiyeti korumak, işyeri verimliliğini artırmak ve işyeri güvenliğini sağlamaktır[335]. Dijital izleme her yerde ve her an denetim gerçekleştirme olanağını işverene verdiğinden bu uygulamalarla gerçekleştirilen denetimlerle işçilerin performanslarının işyeri hedeflerine yaklaştırılması amaçlanır[336]. Ayrıca işverenin ekonomik menfaatleri ve işyerindeki organizasyonel riskleri taşıması iş sözleşmesinin bağımlılık unsuruyla birlikte değerlendirildiğinde işverenlerin işçilerini dijital izlemeyle denetleme hakkı bulunduğu ve yönetim hakkı kapsamında bu haklarını kullanabileceği genel olarak kabul edilmektedir[337].

İşçinin denetlenmesi işletmenin verimlilik hedefiyle yakından ilişkilidir. Zira işverenin işyerinin ekonomik gelişimini[338] ve devamlılığını sağlamak amacıyla ürettiği ürün ve hizmetlerde belirli bir kalite düzeyini yakalama hedefi bulunmaktadır[339]. Bu gereklilik işlerin hedeflere uygun yürütülmesi, bilişim teknolojilerini denetleyerek işçinin fiillerinden kaynaklanabilecek cezai ve hukuki

335) Boehmer, [1992], Artificial Monitoring and Surveillance, s. 745-746.
336) Sprague, [2007], From Taylorism to the Omnipticon, s. 5.
337) Süzek, [2019], İş Hukuku, s. 78-89; Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97; Taşkent, [1981], Yönetim Hakkı, s. 10-11; Ekonomi, [1987], Ferdi İş Hukuku, s. 32; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 256; Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 22; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 253; Gülsevil Alpagut, "İş Sözleşmesinin Şartlarında Değişiklik ve Yargıtay'ın Konuya İlişkin Bir Kararının Düşündürdükleri", Çimento İşveren, C. 18, S. 5, Eylül, [2004], s. 54; Ayşen Altıntepe, Türk İş Hukukunda İşverenin Yönetim Hakkı, İstanbul, [2014], s. 3 Aydın Başbuğ, İşverenin Yönetim Hakkı ve Çalışma Şartlarında Değişiklik, Ankara, [2008], s. 3; Z. Gönül Balkır, "İşverenin Yönetim Hakkının Kullanılması ve Etik Sınırları", Sicil İş Hukuku Dergisi, S. 12, İstanbul, [2008], s. 7; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 91; Murat Şen, İş Hukukunda Çalışma Koşullarında Değişiklik, Ankara, [2005], s. 51; Süzek, [1998], Yönetim Hakkı, s. 225-226; Ali Güzel, İş Hukukunda 'Yetki' ve 'Özgürlük', İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Turhan Esener'e Armağan, C. 15, S. 1, [2016], s. 93-126; Kara R. Williams, "Protecting What You Thought Was Yours: Expanding Employee Privacy to Protect the Attorney-Client Privilege from Employer Computer Monitoring", Ohio State Law Journal, Vol. 69, No. 2, [2008], s. 364 vd.
338) Doktrinde ekonomik gelişim "şahsi kişilik menfaati" olarak nitelendirilmektedir. Okur, [2013], Elektronik Gözetleme, s. 99; Ufuk Aydın, İş Hukukunda İşçinin Kişilik Hakları, Anadolu Üniversitesi Yayınları, Eskişehir, [2022], s. 19, (Aydın, [2022], Kişilik Hakları).
339) Okur, [2013], Elektronik Gözetleme, s. 30.

sorumluluğu ortadan kaldırmak, işyeri verimliliğini ölçmek, işyeri güvenliğini sağlamak veya işçiyi gözetme borcunun gerekliliklerini yerine getirmek gibi meşru amaçlara dayanmaktadır[340].

b) Verimliliği Artırma

Dijital izleme uygulamalarının asıl kullanılma nedeni işyeri veriminin, işçinin etkin denetlenmesiyle ilişkilendirilmesinden kaynaklanmaktadır. Bu sebeple iş ilişkisinde kullanılan dijital izleme uygulamalarındaki asıl amaç yapılan iş, işçi ve işyeri ile ilgili bilgi toplayarak verimliliği artırma isteğidir[341]. Zira iş sözleşmesinin ortaya çıkardığı ilişkinin doğası gereği işverenler sözleşmeden doğan hakları kapsamında işçileri dijital uygulamalarla denetleyerek işyeri verimini artırmayı amaçlarlar[342].

Dijital izlemenin işyerinde verimliliği artırma amacıyla kullanılmasında, kamera gözetlemesine ilişkin yapılan araştırmalarda dijital izlendiğini bilen işçilerin müşterilerle daha olumlu iletişim kurdukları ve yasal yükümlülükler kapsamında iş yapmak zorunda hissettikleri araştırmaları etkili olmuştur[343]. Bu araştırmaların etkisiyle 90'lı yıllardan itibaren işyerlerinde kapalı devre kamera sistemi (CCTV- Closed-Circuit Television/Kapalı Devre Televizyon) kullanımında bir patlama yaşanmıştır[344]. Örneğin mağazalara yerleştirilen kameraların işçileri disipline ettiği gibi hırsızlık olaylarını da büyük oranda önlediğine, işyerlerinde

340) Okur, [2013], Elektronik Gözetleme, s. 100; Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 44, s. 282.
341) Miller/Weckert, [2000], Privacy, the Workplace, s. 255-256.
342) Okur, [2013], Elektronik Gözetleme, s. 24.
343) Mark Reilly Simon, The Use Of Electronic Surveillance And Performance Measures in The Workplace: A Qualitative Investigation, Durham Theses, Durham University. Available at Durham E-Theses Online: http://etheses.dur.ac.uk/429/, Doktora Tezi, s. 1-4, (Erişim Tarihi: 04.12.2022).
344) Adrian Beck/Andrew Willis, Customer and Staff Perceptions of The Role of Closed Circuit Television in Retail Security, Crime At Work, (M. Gill, ed.), Macmillan Publishers Limited, [2005], s. 193 vd.; Michael McCahill/Clive Norris, Watching the Workers: Crime, CCTV and the Workplace, Macmillan Press, [1999], s. 208 vd.; Corey A. Ciocchetti, "Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy", Duke Law & Technology Review, Vol.26, Issue 1, [2001], s. 3.

kamera ile gözetlemenin nakit ve kredi kartı ödeme sisteminin kötüye kullanılmasının önüne geçtiğine ve bu tür sistemlerin soygunda da önemli ölçüde caydırıcı rol oynadığına ilişkin araştırmalarla ulaşılan bulgular elde edilmiştir[345].

İşçilerin konum belirleme sistemleriyle sahada çalıştıkları süre boyunca izlendiklerini bilmeleri onların araçları kurallara uygun kullanmalarını ve iş saatlerini iş görme borcunun ifası için verimli harcamayı yönlendirdiği tespit edilmiştir[346]. İşverenler işletme verimliliğini artırmak amacıyla işçilerin çalışma sürelerinde işleriyle ilgilenerek geçirmelerini, internetten gezinmemelerini, özel e-posta hesaplarıyla meşgul olmamalarını ve işyerinin kaynaklarını verimsiz amaçlar için harcamamalarını isterler[347]. Bu amaçla işveren, örneğin satış temsilcisi olan işçinin performansını değerlendirmek için işçinin müşterilere pazarlama faaliyeti kapsamında gönderdiği e-postaları veya müşterilerin göndermiş olduğu siparişe ilişkin e-postaları performans ölçümü kapsamında bir bilgisayar vasıtasıyla izleyebilir.

İşyerinde verimliliğin sağlanması amacıyla gelişim gösteren ve işyerinin dönüşümünün yeni dinamiği olan Endüstri 4.0[348] bilişim sistemleri temelinde gelişim gösterdiğinden aynı zamanda işçilerin verimlilik denetiminde işverene dijital veri sunmaktadır. İşyerindeki dijital dönüşümün sonucu iş süreçlerine yoğun teknolojinin dahil olması, hizmetin ve üretimin otomasyonlaşması, işçilerin bilişim teknolojileri temelinde çalışan makinelere temasının artması verilerinin ve izlerinin bu makinelerce işlenmesine yol açmaktadır.

Öte yandan, uzaktan çalışmada işçi verimliliğini denetleme ve artırma

345) McCahill/ Norris, [1999], Watching the Workers, s. 210-212.
346) Marian K. Riedy/Joseph H. Wen, "Electronic Surveillance of Internet Access in the American Workplace: Implications for Management", Information & Communications Technology Law, Vol. 19, No. 1, March, [2010], s. 90-91.
347) Riedy/Wen, [2010], Electronic Surveillance, s. 90.
348) Endüstri 4.0 için bkz. Kübra Doğan Yenisey, "Endüstri 4.0, Üretimin Değişen Yapısı ve İş Hukuku, Toprak İşveren Sendikası", 2019, S. 120, s. 1 vd. https://toprakisveren.org.tr/index.php/yayinlar/endustri-4-0-uretimin-degisen-yapisi-ve-is-hukuku/ (Erişim Tarihi: 16.06.2022).

amacıyla kullanılan dijital izleme uygulamalarının işçilerin çalışmalarıyla ilgili doğru veriler sunmadığı yönünde bulgular bulunmaktadır[349]. Örneğin klavye ve fare yakalayıcısı, bilgisayar ekranını izleyen dijital uygulamalarının işçi hakkında işlediği verilerin sonuçlarının ne kadar güvenilir olduğuna ilişkin bir araştırma yapan gazetecinin, bu uygulamaları amiriyle birlikte üç hafta boyunca denemesi sonucu iş verimliliği devamlı % 50'nin altında çıkmıştır. Dahası 14 saat çalıştığı bir günde verimlilik puanının dijital izleme uygulamasında % 22 çıktığı görülmüştür. Zira dijital izleme uygulamasının gazetecinin telefonda, toplantıda, araştırmada geçirdiği zamanı ölçmediği ve işle ilgili diğer olasılıkları dikkate almadığı ortaya çıkmıştır[350].

2. İşverenin İdareye Karşı Yükümlülükleri ve Yasal Zorunluluklar

İşverenlerin, çalışanların işyerinde sağlık ve güvenliğini sağlayacak teknik ve idari tedbirleri almaması ve işçilerin iş sağlığı ve güvenliği yükümlülüklere uygun iş görmesini gerektirecek bir iş düzeni oluşturmaması idari yaptırım sebebi olarak düzenlenmiştir (İSGK m. 26)[351]. Örneğin köprü, tünel veya gökdelen inşaatı işi yapan işverenin işçilerin inşaat alanında tehlikelere maruz kalmalarını engellemek için dijital izleme gerçekleştirilebilen giyilebilir teknoloji olan baretler kullandırmasında menfaatleri bulunmaktadır. İşçilerin diğer işçilere uygulayabildiği mobbing, taciz, zorbalık ve işçilerin yasal yükümlülükleri ihlal etmesinin idari yaptırımı işveren üzerinde doğabilir. Bunların engellenmesinde işverenin menfaatleri bulunduğundan işveren çeşitli dijital izleme uygulamaları kullanabilir.

İşverenlerin, işçilerin iş sağlığı ve güvenliği tedbirlerine uygun

349) Aiha Nguyen, "On the Clock and at Home: Post-COVID-19 Employee Monitoring in the Workplace", Data & Society, https://www.shrm.org/executive/resources/people-strategy-journal/summer2020/pages/feature-nguyen.aspx, (Erişim Tarihi: 16.11.2023).
350) Bkz. Nguyen, [2020], Post-Covid-19.
351 Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 380; Süzek, [2019], İş Hukuku, s. 907; Hâdi Haluk Sümer, İş Sağlığı ve Güvenliği Hukuku, 4. Baskı, Seçkin Yayınları, Ankara, [2019], 105.

oluşturulmuş işyeri prosedürleri kapsamında iş yapıp yapmadığını denetleme yükümlülüğü bulunmaktadır (İSGK m. 4/1-b). Bu yükümlülük işverenin, işçiye ve idareye karşı yükümlülükleri açısından dijital izleme menfaatini oluşturmaktadır[352]. Örneğin GPS ile donatılmış yüksek görünürlük sağlayan yelekler işçileri inşaat sahalarında tehlikeli bir bölgeye girdiklerinde onları uyararak işyeri güvenliğini artırabilir. Böyle ileri teknoloji ile donatılmış giyilebilir dijital izleme uygulamaları, coğrafi sınırlarla çevrili bir şantiyede işçileri takip ederek işçiye yönelik tehlikeyi azaltabilir[353]. Bu durumda böyle bir amaçla, aydınlatma yükümlülüğü yerine getirilerek sınırlı ve ölçülü dijital izleme uygulaması kullanılması hukuka aykırı olarak nitelendirilmez.

İşverenler işçiye ve idareye karşı yükümlülükleri kapsamında önleme ve tespit amacıyla dijital denetim gerçekleştirebilirler[354]. Bu halde örneğin işverenin işçilerin diğer işçiler tarafından taciz edilmesini engellemek için internet trafiğini izlemesi, işçilerin iş sağlığı ve güvenliği talimatlarına uygun davranmalarını sağlamak için dijital izleme uygulamaları kullanması ve varsa sözleşme yükümlülüklerine aykırı durumların ortaya çıkarabilmek ve İSGK açısından denetim baskısı oluşturarak işçilerin oluşturulan prosedürlere uygun giyinmesini ve işini sözleşmeye uygun ifa etmesini sağlaması önleme amaçlı dijital izleme örnekleridir. Ayrıca işveren işçilerin iş sağlığı ve güvenliği amacıyla oluşturulmuş işyeri talimatlarına uygun davranmadığını belgelendirmek amacıyla tespit amaçlı dijital izleme gerçekleştirilir[355].

Günümüzde işçilerin işyeri sistemlerini kullanarak telif haklarını ihlal eden video, müzik ve yayın indirme örneklerine de rastlanmaktadır. Ayrıca işyerinde internetten taciz ve konusu suç olan paylaşımlar yapılabilmektedir. İşverenin idareye karşı sorumluluğunun oluşmaması için bu tür ihlalleri engelleyecek bir

352) Okur, [2013], Elektronik Gözetleme, s. 24-25.
353) İş ilişkisinde kullanılan giyilebilir dijital izleme teknolojileri için bkz. § 7. III.
354) Okur, [2013], Elektronik Gözetleme, s. 25.
355) Okur, [2013], Elektronik Gözetleme, s. 25.

çalışma düzeni oluşturması gerekir[356]. Bunu engellemek için dijital izleme uygulamaları kullanılabilir. Belirtmek gerekir ki bu durumlarda dijital izleme işçilerin sistemleri kötüye kullanmasını engellediği ölçüde işverenin sorumluluğunu azaltır. Aynı husus izleme ile tespit edilen ihlale işverenin erken müdahaleyi gerçekleştirmesi durumunda da geçerlidir. Zira suistimal eyleme dönüşmeden tespit edildiği ölçüde izleme amacına ulaşır. Sonuç olarak işçilerin gerçekleştirdikleri siber zorbalıklardan, konusu suç olabilecek internet kullanımlarından, veri indirmelerinden ve paylaşmalarından işverenin idareye karşı sorumlulukları oluşacağından bu risklerin ortadan kaldırılması ve kontrol edilmesine yönelik dijital izleme uygulamalarının kullanılması makul karşılanmaktadır[357].

Ayrıca işverenlerin, TBK m. 417 kapsamındaki borçlarına uygun bir çalışma düzeni kurmaları ve İSGK m. 4 ve 5 işçilerin iş sağlığı ve güvenliği amacıyla alınan tedbirlere uyup uymadıklarını denetlemek için gerçekleştirilecek dijital izleme uygulamalarında işverenler açısından hukuka uygunluk sebebidir. Zira işçiler iş sözleşmesinden doğan iş görme borcunu ifa ederken yaşamını, ruhsal ve bedeni varlığını ortaya koyarak işin veya işyerinin riskleriyle karşı karşıya kalabilmektedir[358]. İş ilişkisinde görünüm kazanan bu niteliğin ve sosyal devlet ilkesinin de bir gereği olarak işçinin kişiliğini, vücut bütünlüğünü ve sağlığını gözetme borcu işverene yüklenmiştir[359]. Bu borç aynı zamanda işverene gerekli her türlü teknolojik tedbiri alma yükümlülüğü yüklediğinden KVK hukuku ilkelerine ve yükümlülüklerine uygun olması kaydı ile dijital izleme uygulaması kullanılması bu kapsamda değerlendirilir.

---

356) Riedy/Wen, [2010], Electronic Surveillance, s. 97; Gürsel, [2016], İşçinin Kişisel Verileri, s. 362.
357) Determann/ Sprague, [2011], Intrusive Monitoring, s. 984; Michael Rustad/Sandra R. Paulsson. "Monitoring Employee E-Mail And Internet Usage: Avoiding The Omniscient Electronic Sweatshops: Insights From Europe", Suffolk University Law School, The Berkeley Electronic Press, [2005], s. 17.
358) Süzek, [2019], İş Hukuku, s. 397; Erdem Özdemir, İş Sağlığı ve Güvenliği Hukuku Dersleri, Vedat Kitapçılık, İstanbul, [2020], s. 4 vd.
359) Levent Akın, İş Sağlığı ve Güvenliği ve Alt İşverenlik, Yetkin Yayınları, Ankara, [2013], s. 23.

3. Güvenlik ve İşyerinde Mülkiyeti Korumak

Bilişim sistemlerinin işyerlerinin başlıca iş yapma araçlarından birisine dönüşmesiyle birlikte önemli ekonomik değere sahip olan bilgi varlıkları internet korsanları tarafından saldırı hedefi haline gelmiştir. İşçilerin iş yapma yöntemiyle yakından ilişkili olan bilgisayar sistemlerinin güvenliğini yeterince sağlamayan işverenler, ticari sır niteliğindeki şirket bilgilerinin istenmeyen şekilde yayılması, ifşa edilmesi veya değiştirilmesi riskiyle karşı karşıya kalmaktadır. İşverenler bunun önüne geçmek için internet kullanımını ve içeriğini izleyerek güvenlik ihlallerini tespit edip, durdurmaya çalışmaktadır. Gizli, işyerine özgü ve ticari sır niteliğindeki bilgilerin dışarıdan yetkisiz erişime karşı korunması ve işçiler tarafından yetkisiz ve yasa dışı açıklamaların yasaklanması dijital izleme açısından meşru bir amaçtır [360].

İşverenlerin dijital izleme uygulamaları kullanarak yüksek bedellerle yatırım yaptığı işyerinin, iş makinelerinin, işe ilişkin fikri mülkiyet haklarının ve aletlerin mülkiyetini koruma ve güvenliğini sağlama düşüncesi dijital izleme için meşru amaçlardır[361]. Zira iş organizasyonu içinde işin ekonomik riski işverenler üzerindedir ve işverenler işyerine yüksek bedelli birçok yatırım gerçekleştirmektedirler. İşyeri varlıklarının, iş görme borcuna uygun kullanılması, hırsızlığa konu edilmemesi, fikri hakların ifşa edilmemesi, rakiplerle paylaşılmaması ve iş için tahsis edilmiş makine ve aletlerin tahsis amacına uygun kullanılması ve güvenliğinin sağlanması işyeri devamlılığı için önemlidir. İşverenin bu amaçlarla dijital izleme uygulaması kullanması ve dijital denetim gerçekleştirilmesi haklı görülebilir[362].

Eklemek gerekir ki, güvenlikle ilgili diğer önemli bir konu da işverenlerin,

---

360) Riedy/Wen, [2010], Electronic Surveillance, s. 91; Okur, [2013], Elektronik Gözetleme, s. 24-25.
361) Okur, [2013], Elektronik Gözetleme, s. 31-32.
362) Okur, [2013], Elektronik Gözetleme, s. 25.

işyeri iletişim sistemleriyle ilişkili önemli yasal risklerle karşı karşıya olmalarıdır. Zira işçiler fidye yazılımlarının işyeri sistemlerine sızmasına sebebiyet verecek internet programı yüklemeleri yapabilirler. Ayrıca endişe duyulan diğer konu işçilerin pornografik veya içerikleri suç teşkil eden, ırka ve cinsiyete göre ayrımcılık yapan web sitelerini ziyaret etmeleridir. Bunların yapılması işyeri güvenliği açısından riskler ortaya çıkaracağı gibi örneğin 5651 sayılı Kanun kapsamında işverenin sorumluluğu doğabilecektir. İşverenler bunların önüne geçmek, işyerindeki mülkiyeti korumak ve güvenliği sağlamak için çeşitli dijital izleme uygulaması kullanabilir[363].

4. İşverenin Diğer Menfaatleri

Özellikle e-ticaret, tele pazarlama benzeri bazı faaliyet alanlarında işverenin dijital izleme uygulamaları kullanması ispat açısından yasal bir zorunluluktan kaynaklanabilmektedir[364]. Örneğin faaliyet alanı müşteri hizmetleri olan bir işyeri, işçilerinin müşterileriyle iletişimlerini ve müşteri sorunlarına hangi türde çözümler geliştirildiğini takip etmek için dijital izleme gerçekleştirebilir. Aynı doğrultuda elektronik ortamda pazarlama faaliyetinde bulunan bir işveren, işçilerin gerçekleştirdikleri pazarlama faaliyeti esnasında tarafı oldukları sözleşmelerin ispatını sağlamak için e-postaların takibi, telefon görüşmelerini kayıt altına alma, işlem loglarının takibi, çalışma ortamını kamera ile gözetlenmesi gibi dijital izleme uygulamaları kullanabilir.

Diğer mevzuatlarda öngörülen yükümlülükler kapsamında işverenin dijital izleme uygulamaları kullanmada çeşitli menfaatleri bulunmaktadır. İşveren önleme ve tespit amacı kapsamında aydınlatma yükümlülüğünü yerine getirerek ve gerekli prosedürleri işçilerle paylaşarak bilişim sistemlerini, iletişim araçlarını

363) Sprague, [2007], From Taylorism to the Omnipticon, s. 5-6.
364) Hayrunnisa Özdemir, "İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması", EÜHFD, C. XIV, S. 1–2, [2010], s. 234.

izleyebilmektedirler[365]. Örneğin işverenin suç unsuru taşıyan içeriklere ulaşımı engellemek için internet trafiğini izlemesi, işçilerin iş sağlığı ve güvenliği talimatlarına uygun davranmalarını sağlamak için dijital izleme gerçekleştirmesi ve varsa sözleşme yükümlülüklerine aykırı durumları ortaya çıkarmak ve denetim baskısı oluşturarak ihlalin önlemesini sağlamak istemesi önleme amaçlı dijital izlemedir. İşverenler diğer mevzuatlardan kaynaklanan (vergi mevzuatı, ceza mevzuatı gibi) yükümlülükler kapsamında örneğin, işçinin sözleşmeye aykırı davranışlarının ortaya çıkarmak, suçu belgelendirmek, hukuka aykırı eylem ve işlemleri ortaya çıkarmak amacıyla tespit amacıyla dijital izleme uygulamaları kullanabilirler[366].

II. Dijital İzlemede İşçinin Tehlikeye Atılan Menfaatleri Açısından

İş ilişkisinde bulunan otorite/bağımlılık ilişkisini dengelemek amacıyla iş hukukunda nispi emredici normlar vasıtasıyla sözleşme adaleti sağlanmaya çalışılmıştır[367]. İş ilişkisinin zorunlu iş görme araçlarından birisine dönüşen bilişim teknolojileri, işçinin özel özel hayatı ile kişisel verileri üzerinde müdahaleci etkiler ortaya çıkarmaktadır. İşyerinde kullanılan bilişim teknolojileri işçinin verilerinin elde edilmesi, depolanması, analizlere konu edilmesi ve aktarılmasını kısaca işlenmesini kolaylaştırmıştır[368].

Dijital izleme uygulamalarıyla işçiye ilişkin oluşturulan verinin işçinin özel hayatını şeffaflaştırılmasına sebebiyet verdiğine ve devamlı izlenme kaygısının işçinin sağlığını olumsuz etkilediğine yönelik bulgulara ulaşılmıştır[369]. Dahası işçilerin yoğun dijital izlemeye maruz bırakan dijital yönetim uygulamalarının yaygınlaşması ve işin "platformlaştırılması" gizlilik endişelerinin yanında işçilerin

365) Okur, [2013], Elektronik Gözetleme, s. 25.
366) Okur, [2013], Elektronik Gözetleme, s. 25 vd.
367) Doğan Yenisey, [2014], Emredici Yapı, s. 168.
368) KVK Kurumu, [2019], Uygulama Rehberi, s. 53-54.
369) Paul M. Secunda, "The Employee Right to Disconnect", Notre Dame Journal of International & Comparative Law, Vol. 9, No. 1, [2019], s. 2-3; https://fherehab.com/learning/public-exposure-and-mental-health/ (Erişim Tarihi: 21.07.2022).

nesneleştirilmesi ve dijital bir ögeye dönüştürme riskini ortaya çıkarmıştır. Özellikle giyilebilir sistemlerin çalışma hayatına dahil edilmesi işçilerin biyometrik verileri sayesinde denetimini kişisel özellikleri özelinde gerçekleştirme imkanını işverene vermiştir[370]. Teknolojinin işçinin hayat alanlarını bu şekilde kuşatması ve kamusal veya özel alanda işçinin gündelik hayatın bir parçası haline gelmesi bu kuşatıcı müdahaleyi sınırlayıcı yeni hukuki yaklaşımlar üzerinde düşünmeyi ve algoritmik iş yönetimi ve yapay zekanın (AI - Artificial Intelligence) iş yaşamındaki olumsuz etkilerinin sınırlandırılmasına yönelik hukuki çerçevelerin geliştirilmesi gerektirmektedir[371].

Dijital izleme uygulamaları vasıtasıyla işçinin kişisel verilerinin işlenmesi, izlerinin takip edilmesi ve kayıt altına alınması onların özel hayatının gizliliği, haberleşme özgürlüğü, temel hak ve özgürlükleri ile kişilik hakları kapsamında sayılan kişisel verilerinin korunmasıyla ilgilidir[372]. Bu sebeple işverenin kullandığı dijital izleme uygulamaları işçinin bu hak ve menfaatleri üzerinde ihlal edici etkiler ortaya çıkarabilmektedir.

İşyerinde dijitalleşmenin yaygınlaşması, geleneksel izlemede bir unsur olarak varlığını gösteren gözetleme uygulayıcısının bedensel veya optik varlığını görünmez kılmış, fiziki izlemenin yerini tespit edilmesi güç bilişim arayüzleri almıştır. Bu değişim işçinin verilerini işlemeyi işyeriyle sınırlı olmaktan çıkarmış, işçinin özel hayat alanına taşacak şekilde kişisel veri işlenmesi olanağını işverene vermiştir. Bu gelişmeler aynı zamanda özel hayatın gizliliğini ve kişisel verileri koruyan hukuki düzenlemelerin ortaya çıkmasını tetiklemiştir[373].

---

370) Sara Riso, "Monitoring and Surveillance of Workers in The Digital Age" https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age (Erişim Tarihi: 18.12.2023)
371) Bauman/Lyon, [2016], Akışkan Gözetim, s. 147.
372) Küzeci, [2020], Kişisel Veriler, s. 74; Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 49; Şimşek, [2008], Kişisel Verilerin Korunması, s. 135-136; Hüseyin Can Aksoy, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara, [2010], s. 37.
373) Lyon, [2013], Gözetlenen Toplum, s. 24; Sprague, [2007], From Taylorism to the Omnipticon, s. 2-3.

Ayrıca işyerinde gizli gerçekleştirilen gözetleme veya sınırları belirsiz olan dijital izleme uygulamaları işçiler için korku ve güvensizlik ortamı yaratarak işyerindeki bireysel ilişkileri minimize edebilmektedir. Bu durum işçinin diğer işçilerle ilişki geliştirme, makul mahremiyet beklentisi gibi haklarını olumsuz etkileyerek işçiler için işyerini bir kaygı ve korku ortamına dönüştürmektedir[374]. Tüm bunların işçinin "maddi ve manevi varlığını geliştirme hakkını engelleyen zehirli bir ortam"[375] ortaya çıkaracağı söylenebilir. Ayrıca işyeri verimini artırmak amacıyla gerçekleştirilen dijital izleme işçileri bilgilendirmeden gerçekleştirilirse elde edilen verilerin kullanılması açısından hukuki sorunlar da ortaya çıkar[376].

İşçilerin özel hayatlarının gizliliği ve kişisel verilerinin korunması hakkı kaynağını anayasadan aldığından yönetim hakkını bu yönlü de sınırlandırır. WP 29 Çalışma Grubu görüşünde ifade edildiği üzere, işçiler her sabah işe geldiklerinde işyerinin kapısından içeri girmeden önce özel hayatlarının gizliliği ve veri koruma haklarından vazgeçmezler[377]. Fakat işçilerin bu hakları da sınırsız değildir, çünkü onların hakları da örneğin işverenin siber saldırıları engellemek için internet trafiğini takip etme, ticari sırlarını korumak için tedbir alma ve işyeri verimliliğini artırmak, güvenlik şirketin saygınlığını koruma gibi haklarıyla sınırlanır. Bu sebeple işyerinde iş ilişkisinin taraflarının hakları bakımında bir dengenin oluşturulması çalışma barışı açısından önemlidir[378].

Bilişim teknolojilerinin iş ilişkisinde daha önce olmadığı kadar büyüklükte işçi verisini işlemeye ve analize konu ettiği tartışmasızdır. Bu teknolojiler kullanılarak gerçekleştirilen izleme işçide sürekli izlendiği, işverenlerinin kendilerine güvenmediği ve dijital izleme uygulamalarıyla denetim altında tutulduğu düşüncesine yol açtığı, bunun işçilerde strese, ruhsal çöküntüye veya özel

374) Ball, [2021] Electronic Monitoring, s. 39.
375) Fazıl Sağlam, "Türk ve Alman Anayasa Hukukları Açısından Gizli Ses Kaydı", AÜSBFD, S. 1-4, Ankara, [1977], s. 110.
376) López Ribalda and Others v. Spain, § 97, § 131.
377) Hendrickx, [2002], Workers Personal Data, s. 23-24; ILO, Personal Data, [1997], s. 8.
378) WP29, Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace 5401/01/EN/Final, [2002], WP 55. s. 4.

hayatının gizliliğinin ihlal edildiğine ilişkin kaygılara sebebiyet verdiği tespit edilmiştir[379]. Birleşik Krallık Veri Koruma Otoritesi (ICO - Information Commissioner's Office) tarafından gerçekleştirilen bir araştırmada elde edilen sonuçlara göre halkın % 70'i işveren tarafından izlenmeyi rahatsız edici bulduğunu, kişisel verileri üzerindeki haklarının ihlal edileceğini ve özel hayat gizliliklerinin risk altında olduğunu ifade etmiştir[380].

ICO, işverenlerin kullandığı dijital izleme uygulamalarında uyması gereken yükümlülükler hususunda yayımladığı kılavuzda özellikle uzaktan ve diğer esnek çalışma türlerinde işçilerin ev mahremiyetinin korunmasını, ticari çıkarların hiçbir zaman işçilerin özel hayatları ve verileri üzerindeki haklarının önünde tutulmaması gerektiğini hatırlatmıştır. Bu kapsamda tüm işverenlere dijital izleme uygulaması kullanmadan önce işçilerin haklarını koruyacak bir yapı oluşturmalarını ve yasal yükümlülüklerini yerine getirmeleri gerektiği hatırlatmıştır. Aksi durumda işçilerin özel hayatları ve verileri üzerinde bir tehdit ortaya çıkarsa yaptırım uygulanması için harekete geçileceği vurgulanmıştır[381]. KVK Kurumu'nun bu kılavuza atıf yaparak bu yaklaşımı web sitesinde yayımlaması işçilerin dijital izleme uygulamalarıyla izlenmesi durumunda benzer yaklaşımı benimseyeceğini göstermektedir[382].

Dijital izleme uygulamalarıyla işçilerin kişisel verilerinin işlenmesi ve bu vasıtalarla işçilerin denetlenmesi işçilerin kararlarını etkileyebilir ve onların özgünlüğünü, hayatlarının öznesi olma hakkını sınırlandırabilir. Ayrıca devamlı izlendiği düşüncesi işçinin çalışma verimini, yaratıcılığını düşürebileceği gibi işçinin işe ve işyerine yabancılaşması işyeri verimi açısından olumsuz etkilere de

379) https://fherehab.com/learning/public-exposure-and-mental-health/ (Erişim Tarihi: 21.07.2022).
380) https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/ico-publishes-guidance-to-ensure-lawful-monitoring-in-the-workplace (Erişim Tarihi: 08.11.2023).
381) https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/ico-publishes-guidance-to-ensure-lawful-monitoring-in-the-workplace (Erişim Tarihi: 08.11.2023).
382) https://www.farkindaolguvendekal.org/bizden-haberler/secilmis-guncel-gelismeler-26/ (Erişim Tarihi: 08.11.2023.

sebebiyet verebilmektedir. Özellikle işverenin dijital izleme uygulamalarını gereğinden fazla müdahaleci, aşırı derecede kontrol edici uygulaması veya işçilerde meşru bir işyeri amacı için kullanılmadığı düşüncesi oluşturursa bu uygulamalar işçilerde kaygıya yol açmaktadır[383]. Bazı araştırmalarda ulaşılan sonuçlara göre işyerinde devamlı izlendiğini düşünen işçilerde kas ve sinir rahatsızlıkları artmakta, işyeri stresi ortaya çıkmakta ve dijital izleme işçinin üretkenliği ve yaratıcılığı üzerinde olumsuz etkiler oluşturmaktadır[384]. Dahası iş sözleşmesinin güven temelli bir ilişki ortaya çıkardığı düşünüldüğünde devamlı izlendiğini düşünen işçilerde kendilerine güvenilmediği duygusunun oluşmasına sebebiyet vermektedir[385].

Ayrıca işçilerde gereksiz olduğu algısı oluşan dijital izleme uygulamalarının işyerindeki etkisi verimliliğin düşmesi veya işçi istifaları biçiminde olabilmektedir[386]. Yapılan araştırmalarda işçilerin izlendiklerini bildiklerinde veya böyle bir ihtimalin bulunduğunu düşündüklerinde özgün düşüncelerini açıklamakta çekindikleri ve yaratıcı yönlerinin sekteye uğradığı tespit edilmiştir. Dahası özel hayatın gizliliğini ihlal eden dijital izleme uygulamalarının kullanıldığını düşünen işçilerin psikolojik rahatsızlıklara ve strese bağlı hastalıklara yakalandıkları görülmüştür[387].

Devamlı izlenme ve izlemeye dayalı denetim baskısının yıkıcı sonuçlar

---

383) Jeremias Adams-Prassl, "What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work", Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall, [2019], s. 130.

384) Abi Adams, "Technology and the Labour Market: The Assessment", Oxford Review of Economic Policy, Volume 34, Issue 3, Autumn, [2018], s. 349–361.); Gürsel, [2016], İşçinin Kişisel Verileri, s. 362.

385) Gürsel, [2016], İşçinin Kişisel Verileri, s. 363.

386) Myria Watkins Allen/Stephanie J. Coopman/Joy L. Hart/Kasey L. Walker, "Workplace Surveillance And Managing Privacy Boundaries", Management Communication Quarterly, Vol. 21 No. 2, [2007], s 175-176; Graeme Lockwood/Vandana Nath, "The Monitoring of Tele-Homeworkers in The UK: Legal and Managerial Implications", International Journal of Law and Management Vol. 63, No. 4, [2021], s. 398.

387) Graeme Lockwood, "Workplace Monitoring and Surveillance: The British Context", Athens Journal of Law (AJL), Vol. 4, No. 3, July, [2018], s. 206-207 ve bu sayfalarda atıf yapılan araştırmalar ve yazarlar; Hazel Oliver, "Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out", Industrial Law Journal, Vol. 31, No. 4, December, [2002], s. 325; Sarpong/Rees, [2014], Big Brother' in A Workplace, s. 218.

ortaya çıkardığına, iş stresini artırdığına[388] ilişkin verilen en çarpıcı örneklerden birisi Gazeteci Miwa Sado'nun çalışma biçimi sebebiyle geçirdiği kalp krizi ile hayatını kaybetmesidir. Yakın tarihli bu olayda Japon Gazeteci Miwa Sado'nun kısa dinlenmelerle 159 saat kayıt yapması, bağlantıda kalma ve izlenme baskısı, fazla mesaiye zorlanması gibi etmenlerle kalp krizi geçirip hayatını kaybettiği akademik makalelere konu edilmiştir[389]. Bunda teknolojik gelişmelerin ortaya çıkardığı işyeri ve ev arasındaki sınırı bulanıklaştırmanın, işi eve taşımanın, bilişim teknolojilerinin ve dijital izlemenin etkisi büyüktür[390]. Zira işverenlerin işçileriyle iş saatleri sonrası mesajlaşma imkanı, e-postalarla soru sorması, ek iş istemesi işyeri stresini tüm hayat alanına yayma sonucu ortaya çıkaracağı açıktır. Burada ortaya çıkan önemli sorunlardan birisi de hangi andan itibaren (bir dönem yaygın kullanılmış olan iş bitti düdüğü çaldıktan sonra) işverenin artık işçilerin hayatlarına bu tür sorularla veya dijital izleme uygulamalarıyla müdahale edemeyeceği hususunun; yani işçilerin özel hayatları üzerinde özerk hakları, anonim kalma hakları ve bağlantıda veya izleme altında olmama hakkının hangi anda ve yerde başladığının açıklığa kavuşturulmasıdır[391].

Bu sebeple özel hayat alanının korunmasında önemli ölçütlerinden birisi kişilerin anonim olarak hareket etme olanağının varlığıdır. Herkesin üzerinde taşıdığı cep telefonlarında GSM (Global System for Mobile) ve GPRS (General Packet Radio Service) gibi izleme olanağı bulunduğundan günümüzde kişinin anonim hareket etmesi giderek güçleşmektedir. İşçiler açısından daha da kaygı verici olanı iş ilişkisi gibi durumlarda doğrudan bir işçinin GPS vasıtasıyla izlenmesi ve kayıt altına alınması işçilerinin özel hayatlarının gizliliğini ortadan kaldırabilmesidir[392].

---

388) Adams, [2018], Technology and the Labour, s. 349 vd.
389) Secunda, [2019], Right to Disconnect, s. 2-3.
390) Secunda, [2019], Right to Disconnect, s. 3 vd.
391) Secunda, [2019], Right to Disconnect, s. 4; Elin Palm, "The Ethics of Workspace Surveillance", Doctoral Thesis in Philosophy from the Royal Institute of Technology nr 26, [2017], s. 15, (Palm, [2017], Workspace Surveillance).
392) Manon G. Guillemette/Isabelle Fontaine/Claude Caron, "Hybrid RFID-GPS Real-Time Location System for Human Resources: Development, Impacts and Perspectives", Proceedings of the 41st Hawaii International Conference on System Sciences in Waikoloa, Hawaii, January, [2008],

Günümüzde örneklerine denk geldiğimiz işçinin tuvalette geçirdiği zamanı[393], dakikada kaç tuş vuruşu yaptığı, bilgisayar başında ne kadar zamanı iş için harcadığı, işte neyle meşgul olduğu gibi hususların izlenmesi ve analizlere konu edilmesi işçi açısından işyeri stresini artıran örneklerdir[394]. Eklemek gerekir ki, dijital izlemenin verimlilik artışını ve işyeri prosedürlerine uygun iş yapmayı sağladığı gibi bazı olumlu bulgulara ulaşılması sürpriz sonuçlar değildir. Zira aynı olumlu etki panoptikon veya "bilimsel yönetim ilkeleri" gibi gözetleme temelli işyeri izlemelerinde de yakalanmıştır. Aslında üzerinde düşünülmesi gereken husus gerçekleştirilen dijital izleme uygulamalarının işçinin anayasal hakkı olan özel hayatının gizliliğinin korunması ve kişisel verileri üzerindeki hakları karşısında ne kadar mevzuata uygun ve ölçülü olduğudur.

§ 4. ULUSLARARASI METİNLERDE DİJİTAL İZLEME VE SINIRLARI

Uluslararası sözleşmelerde ve hukuki metinlerde bireyin özel hayatı ve kişisel verilerinin korunması, iş sözleşmesinin taraflarının dijital izlemedeki menfaatlerinin bu düzenlemelerdeki görünümü ve bunların ülkemiz veri koruma mevzuatı üzerindeki etkileri bu başlıkta ele alınacaktır.

I. Birleşmiş Milletler Düzenlemeleri

İşverenlerin girişimde bulunma ve istedikleri kişilerle sözleşme tarafı olma özgürlüğü ile işçilerin özel hayatlarının gizliliği ve kişisel verilerinin korunmasına

---

s. 406; Selen Uncular, "Teknolojinin Etkisiyle Dönüşen İş İlişkisinde Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme", Çalışma ve Toplum, C. 66, [2020/3], s. 1680.

393) "Türkiye sanayisinin merkez üslerinden olan Kocaeli'de otomotiv fabrikalarında yaşanan bir olay var ki şaşırmamak imkansız... Geçenlerde yemeğe çıkmadan önce tuvaletlerin kapısının kilitlendiğini gördük, sebebini sorunca da yemeğe çıkmadan önce herkes işi erken bırakıp tuvaletlere gidiyor bu da verimi düşürüyor dediler." https://www.kocaeligazetesi.com.tr/haber/1738379/bu-is-yerinde-tuvalete-gitmek-yasak (Erişim Tarihi: 05.10.2021).

394) Adam D. Moore, "Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy, Business Ethics Quarterly", Cambridge University Press, Jul., 2000, Vol. 10, No. 3, [2000], s. 697-698.

ilişkin hukuki gelişmelerde ve bunların birer anayasal hakka dönüşmesinde uluslararası düzenlemelerin önemli bir etkisi bulunmaktadır. Bu hakların gelişiminde öncü uluslararası kuruluşlardan birisi olan BM, II. Dünya Savaşı benzeri büyük bir yıkımla insanlığın karşı karşıya kalmaması için dünya barışını ve güvenliğini korumak, devletler arasında dayanışma, toplumsal ve kültürel iş birliği oluşturmak ve barışı tesis etmek için 51 devlet tarafından 1945 yılında kurulmuş ve günümüzde 193 üyesi bulunan bir kuruluş haline gelmiştir[395]. BM'nin kuruluş amacı, 26 Haziran 1945 tarihli Birleşmiş Milletler Antlaşması'nın 1. maddesinde düzenlenmiştir. BM'nin amacı maddede özetle; uluslararası barış ve güvenliği korumak, uluslararasında hak eşitliğini sağlamak ve dostça ilişkileri geliştirmek, herkesin insan haklarına ve temel haklara sahip olduğu bilincini geliştirmek ve uluslararası sorunları çözmede iş birliğini sağlamak biçiminde açıklanmıştır. Tezin konusu ile yakından ilgili olan insan haklarının ve temel özgürlüklerin geliştirilip güçlendirilmesini sağlama amacının hedefler arasında sayılması, üye ülkelerin bu hususta hukuki düzenlemeler gerçekleştirmesini etkilemiştir. Belirtmek gerekir ki, BM Şartı'nda, Antlaşma'dan doğan yükümlülüklerin üye devletler tarafından kabul edilmesi esası benimsenmiştir[396].

Devletler için yol gösterici nitelikte olan İHEB ve kurucu sözleşme olan Birleşmiş Milletler Şartı insan haklarının güvence altına alınması ve korunması açısından birçok uluslararası sözleşmeye ve ulusal anayasalara kaynaklık etmiştir[397]. Teknolojik gelişmelerin özel hayat alanına ilişkin verileri işlemeye konu etmesinin de etkisiyle 1948 tarihli İnsan Hakları Evrensel Bildirgesi'nin 12. maddesinde; "hiç kimsenin özel yaşamına, ailesine, evine ya da yazışmasına keyfi olarak karışılamaz, onuruna ve adına saldırılamaz. Herkesin, bu gibi müdahale ya

395) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 71; Gürsel, [2016], İşçinin Kişisel Verileri, s. 67; Sevimli, [2006], Özel Yaşam, s. 36 vd.; Okur, [2013], Elektronik Gözetleme, s. 39.
396) Mehmet Semih Gemalmaz, Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş, 6. Baskı, Legal, [2007], s. 833-846; Turgut Tarhanlı, Birleşmiş Örgütü ve İnsan Haklarının Korunmasına İlişkin Başlıca Usuller, (Ed. Turgut Tarhanlı), İnsan Hakları, YKY, İstanbul 2000, s. 407.
397) Aydın Aybay/Rona Aybay, Hukuka Giriş, İstanbul Bilgi Üniversitesi Yayınları, 4. Baskı, İstanbul, [2007], s.73.

da saldırılara karşı yasa tarafından korunma hakkı vardır." düzenlemesiyle özel hayatın gizliliği ilk kez uluslararası bir bildiriyle temel insan hakkı olarak kabul edilmiştir. Düzenlemede herkesin özel hayat alanı bulunduğu ve bu hayat alanına karşı müdahalelerin kanun ile koruma altına alınması hakkı bulunduğu vurgulanmıştır.

BM'nin 1966 tarihli Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin "Mahremiyet Hakkı" başlıklı 17. maddesi de özel hayatın gizliliğinin korunmasına ilişkin bir düzenlemedir. Madde 17 düzenlemesine göre: "Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir." Bu maddenin kapsam ve amacına ilişkin olarak BM İnsan Hakları Komitesi 16. Genel Yorumu[398] ile açıklık getirmiştir. Yine kişisel verilerin korunması açısından önemli bir rehber olan, 14.12.1990 tarihinde BM Genel Kurulu tarafından kabul edilen 45/95 no'lu Kılavuz ile bilgisayarda kişisel verilerin işlenmesine ve bu sistemler üzerinde kişisel verilerin düzenlenmesine ilişkin öneriler belirlenmiştir[399].

Bu düzenlemeler ülke hukuklarında benzer anayasal hakların ortaya çıkmasında etkili olduğu gibi, 1982 Anayasası'nın 90/V. düzenlemesinde temel hak ve özgürlüklere ilişkin milletlerarası anlaşmalar iç hukuk düzenlemelerinin üstünde

398) BM İnsan Hakları Komitesi Genel Yorum No. 16: Özel Hayatın Gizliliğinden ne anlaşılması gerektiği açısından önemlidir. Komite m. 17 ile ilgili şu yorumu yapmıştır: "Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz. Komite'ye göre, bu hak gerek Devlet otoriteleri, gerekse herhangi bir gerçek kişi veya tüzelkişiden kaynaklanan her tür müdahale ve saldırıya karşı koruma altına alınmalıdır. Maddeye göre taraf Devlet, bu hakka yönelik müdahale ve saldırıları yasaklama ve bu hakkı korumayı hedefleyen yasama tedbirlerini ve gerekli diğer tüm tedbirleri alma yükümlülüğü altındadır." "Keyfi müdahale" kavramı da 17. maddedeki hakkın korunmasıyla yakından ilgilidir. Komite'ye göre, keyfi müdahale, hukuka uygun olarak gerçekleştirilen müdahaleleri de kapsayabilir. Maddede keyfi müdahale kavramına yer verilmesinin nedeni, hukuka uygun müdahalelerin dahi Sözleşme'nin maddeleri ve amaçlan ile uyum içinde ve her halde olayın şartlarına göre makul olması gereğidir."
399) Gemalmaz, [2007], İnsan Hakları Hukuku, s. 434.

tutulmuştur. Bu itibarla iş hukuku açısından İHEB ve Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi düzenlemeleri önemli hukuk kaynağıdır[400].

II. ILO'nun İşçilerin Verilerini Korumaya İlişkin Çalışmaları ve ILO Uygulama Kodu

Hiyerarşik bir ilişkinin bulunduğu iş ilişkisinde çalışma barışışının sağlanması ve işçi refahının artırılması için kurulmuş olan Uluslararası Çalışma Örgütü (ILO - International Labour Organization) sosyal adalet ve evrensel insan hakları çerçevesinde emek haklarının elde edilmesi için çalışmalar yürütmektedir[401]. Birinci Dünya Savaşı'nı sona erdiren Versay Anlaşması'nın bir parçası olarak 1919 yılında kurulan ILO, çalışmalarını 1946'dan itibaren çalışma ilişkileri konusunda uzmanlaşmış bir kuruluş olarak BM çatısı altında yürütmektedir[402]. ILO üçlü yapısıyla işçilere, işverenlere ve devletlere eşit söz hakkı vererek insan onuruna yakışır çalışma şartlarının kadınlar ve erkekler için sağlanması amacıyla çalışmalar yürütmektedir[403].

ILO'nun çalışmalarına baktığımızda işverenlerin işyerinde belirli düzenlemeler yapması, kararlar alması ve uygulaması hususunda belirli haklara sahip olduğu kabul edilmektedir. Bununla birlikte ILO hukuki metinlerinde ortaya çıktığı üzere, işverenin dijital izleme gerçekleştirmesi iş ilişkisinin doğasının bir gereği olmasına rağmen sınırsız da değildir[404]. Özellikle iş hukukunun yönetim hakkını sınırlandırması, işverenin işçiyi gözetme borcu, gerçekleştirilecek dijital izleme ile ilgili işçilerin bilgilendirilmesi gerekliliği, işçinin özel hayatının

400) Kemal Başlar, Türk Mahkeme Kararlarında Avrupa İnsan Hakları Sözleşmesi, Ankara, Avrupa Konseyi Türkiye Temsilciliği Yayını, [2008], s. 17-18.
401) https://www.ilo.org/ankara/about-us/WCMS_372872/lang--tr/index.htm (Erişim Tarihi: 01.07.2022).
402) Süzek, [2019], İş Hukuku, s. 85-86; Tankut Centel, İş Hukuku, C. I, Bireysel İş Hukuku, İkinci Bası, İstanbul, [1994], s. 33-34, Ekonomi, [1987], Ferdi İş Hukuku, s. 7.
403 https://www.un.org/youthenvoy/2013/08/ilo-international-labour-organization/?gclid (Erişim Tarihi: 01.07.2022).
404)https://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@dialogue/documents/publication/wcms_209280.pdf

gizliliğinin ve kişisel verilerinin korunması yükümlülüğü asimetrik güç ilişkisinde işvereni sınırlar. Bu sınırlamaların bulunması, işverenin iş organizasyonu ve işyeri kurallarını belirleyebilmesi ve işçinin de işverene bağımlı olarak iş görmesi gerçekliğini değiştirmemektedir.

İş sözleşmesine özgün olan bağımlılık unsuru, her hukuk sisteminde iş sözleşmesini diğer sözleşmelerden farkını ortaya koymak için kullanılan ortak bir ölçüttür. Nitekim ILO'nun İş İlişkisi[405] (Rapor V-1) başlıklı belgesinde iş ilişkisi söz konusu olduğunda sık başvurulan kavramların bağımlılık, tabi olma, denetim ve kontrol gibi kavramlar olduğu ortaya çıkmaktadır. ILO, üye ülkelerin iş ilişkisine bakışını ortaya çıkarmak ve oluşturulacak bir raporun olası içeriğine ilişkin olarak üye ülkelere bir rapor ve anket göndermiştir. Bu ankette verilen cevaplarda üye ülkelerin iş ilişkisini tanımlarken bağımlılık, tabi olma, denetim gibi benzer kavramları kullandıkları ortaya çıkmıştır[406].

ILO'nun anketinde ortaya çıktığı üzere işverenin dijital izleme hakkı yabancı hukuk mevzuatlarında yasal bir düzenlemeye konu edilmemiş olsa da bu hakkın iş sözleşmesinden kaynaklandığı genel olarak kabul edilmektedir[407]. AB üyesi ülkelerle ilgili yapılan araştırmalarda da sözleşmenin yerine getirilmesinin kontrolünde, işçiyi korumada, iş performansını ölçmede ve mülkiyeti korumada iş sözleşmesine dayalı dijital izleme hakkının bulunduğu kabul görmektedir[408]. ILO Yönetim Kurulu'nun 1996 yılında kabul ettiği ve 1997 yılında yayımladığı İşçilerin Kişisel Verilerinin Korunması Hakkında Uygulama Kodu'nda işverenlerin,

---

405) ILO, The Employment Relationship, Report V(1), International Labour Conference, 95. Oturum, [2006], s. 6. https://www.ilo.org/public/libdoc/ilo/2005/105B09_8_engl.pdf. (Erişim Tarihi: 01.07.2022).
406) International Labour Conference, 95th Session [2006], s. 155-160; CJEU (ABAD), Judgment of 21. II. 1991—Case C-27/91 Union de Recouvrement des Cotisations de Sécurité Sociale et d'Allocations Familiales de la Savoie (URSSAF)
https://eur-lex.europa.eu/resource.html?uri=cellar:8275ac53-e4f0-4c82-82d7-15671106d69c.0002.06/DOC_1&format=PDF (Erişim Tarihi: 02.07.2022).
407) Okur, [2013], Elektronik Gözetleme, s. 28.
408) Frank Hendrickx, "Protection of Workers Personal Data in The European Union", Two Studies, EC, Manuscript Completed in July, [2002], s. 118-119, (Hendrickx, [2002], Workers Personal Data).

işçilerin kişisel verilerini işleme yöntemlerinden birisi olarak dijital izleme sayılmıştır (m. 3.3 ve m. 6). Uygulama Kodu'nda izlemenin tanımı tüm dijital mecraları ve gözetleme yöntemlerini kapsayacak şekilde yapılmıştır[409]. Uygulama Kodu'nda dijital izleme yasaklanmamış, uygulanması belirli koşullara bağlanmıştır. Buna göre dijital izleme uygulamalarıyla işçinin verileri işlenmeden önce işçi; izlemenin amacı, kapsamı, zaman aralığı, izleme yöntemleri, işlenecek veriler hususunda bilgilendirilmelidir[410]. Belirtmek gerekir ki, ILO kodu yasal olarak bağlayıcı olmamakla birlikte, üye ülkelere bu hususlarda referans bir düzenleme sunmaktadır.

Dijital izlemenin iş ilişkisini aşacak şekilde kullanılmasına veya işçi ile işçi adayının kişisel verileri üzerindeki haklarından feragat ettiğine ilişkin sözleşme düzenlemelerinin geçersiz olacağına ilişkin düzenlemeler (TBK m. 27 de bu kapsamda değerlendirilmelidir) ile Avusturya, Belçika, Almanya, Hollanda, Norveç, İspanya ve İsveç gibi ülkelerde bu tür sorunların önüne geçmek ve işverenle müzakereleri gerçekleştirmek üzere işçi konseylerinin kurulmasına yönelik yasal düzenlemeler bulunmaktadır[411]. Örneğin 2004'te Finlandiya'da düzenlenen "Act on the Protection of Privacy in Working Life" (Çalışma Hayatında Mahremiyetin Korunması Hakkında Kanun) isimli düzenleme işyerinde izlemeye ve mahremiyetin korunmasına yönelik önemli düzenlemeler getirmektedir. Yine Belçika'da toplu sözleşmeye ilişkin olan 81 Sayılı düzenleme online iletişimde işçinin özel hayatının gizliliğinin korunmasını öngörmektedir[412].

ILO'nun iş ilişkisine ilişkin raporunda ortaya çıktığı üzere, yabancı ülke mevzuatlarında da iş ilişkisinin karakteristik özelliği işverene "bağımlı" olarak iş

409) ILO, Code of Practice on the Protection of Workers' Personal Data, s. 1. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf (Erişim Tarihi: 02.07.2023).
410) Esra Yiğit, İşyerinde İnternet ve E-posta Kullanımının İzlenmesi ve Gözetlenmesi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, [2013], s. 5-6.
411) Catherine Delbar/Marinette Mormont/Marie Schots, New Technology and Respect for Privacy at the Workplace, Institut des Sciences du Travail, [2003], s. 28.
412) Clara Fritsch, "Reforming European Data Protection Law", (Serge Gutwirth / Ronald Leenes / Paul de Hert - Editors), Springer, [2015], s. 151-152.

görme biçiminde karakterize edilmektedir. Raporda ayrıca işverenin işyeri ve iş veriminin artırılmasıyla ilgili belirli yönetim hakları bulunduğu, bu hak kapsamda belirli düzenlemeleri yapma imkanına sahip olduğu genel olarak kabul edilmektedir. Bununla birlikte ILO düzenlemelerinde doğrudan işverenin dijital izleme hakkına ilişkin bir düzenleme yer almamaktadır. Alman, İsviçre, Avusturya, Fransa ve İspanya hukuk düzenlemelerinde işverenlerin yönetim hakkı ve dijital izlemeyi de gerektirecek yükümlülükleri bulunduğu kabul edilmekle birlikte, işverenlerin dijital izleme gerçekleştirmelerine ilişkin özel bir düzenleme bulunmamaktadır. Bu ülkelerde dijital izleme hususunda ortaya çıkan sorunlar, kişisel verilerin korunması mevzuatı, işçinin kişiliğinin korunması ve işçiyi koruyucu iş hukuku ilkeleri kapsamında çözülmektedir[413].

ILO çalışmalarında genel olarak dijital izlemede işçilerin izlenmesinin yeri ve şekliyle ilgili çeşitli ayrımlar yapılmaktadır. Bu ayrımlar izlemenin işyerinin fiziki alanında yapılması ile işyeri dışında yapılması, kamuya açık olan işyeri ile kamusal alanın dışında kalan işyerinde gerçekleştirilmesi, gizli izleme ve açık izleme şeklindedir[414]. Ayrıca, işverenin meşru menfaati kapsamında kamera gözetlemesiyle doğrudan işçilerin bir kısmının çalışma alanının veya işçiler hedef alınmaksızın işyerinin belirli yerlerinin kamera gözetlenmesi ile izlenmesine ilişkin de ayrımlar yapılmaktadır[415]. Örneğin üretim bandında riskli işler yapan işçilerin veya mülkiyeti korumak için deponun belirli bir kısmının izlenmesi ilk duruma örnek gösterilebilir. Diğer bir kamera gözetlemesi durumu ise doğrudan işçilerin değil, işyerinin girişi veya koridorlar gibi kısımlarının izlenmesidir. Güvenlik amacıyla işyerinin giriş kısmına yerleştirilen kameralar buna örnek gösterilebilir. Bu iki durumun işçiler için daha az müdahaleci olmasına yönelik gerekli özenin gösterilmesi için kamera gözetlemesinde işçilerin yüzlerinin mozaikleyen

413) Okur, [2013], Elektronik Gözetleme, s. 29-30; ILO, International Labour Conference, 95th Session, Report V(2A), [2006], s. 155-160; Kenneth A. Bamberger/Deirdre K. Mulligan, Privacy in Europe: Initial Data on Governance Choices and Corporate Practices, The George Washington Law Review, Vol. 81, No. 5, September, [2013], s. 1542.
414) Florian Höld, Die Überwachung von Arbeitnehmern, Hamburg [2006]; Aktaran Okur, [2013], Elektronik Gözetleme, s. 26, dipnot 23.
415) Alpagut, [2019], Kamera Gözetlemesi, s. 311.

uygulamalar kullanılabilmektedir.

Eklemek gerekir ki, ILO düzenlemelerinde önerildiği üzere her durumda gerçekleştirilecek dijital izleme uygulamasında işçilerin özel hayatlarına saygı hakkı dikkate alınmalı ve izlemenin işçilerin özel hayatlarının gizliliği ve kişisel verileri üzerindeki etkisi ortaya konmalı, daha az müdahaleci yöntemler aranmalı ve veri koruma hukukunun genel ilkelerine dikkat edilmesi gerekmektedir.

III. OECD Rehberleri ve Kişisel Verilerin Korunması

OECD, 14.12.1960 tarihinde Paris'te imzalanmış olan Paris Konvansiyonu ile kurulmuş olmasına rağmen geçmişi, II. Dünya Savaşı sonrası Avrupa'nın hızlı kalkınması, devletler arasındaki iş birliğinin teşvik edilmesi ve kalıcı barışın sağlanması amacıyla 1948 yılında kurulmuş olan Avrupa Ekonomik İşbirliği Teşkilatı'na (The Organisation for European Economic Cooperation - OEEC) dayanmaktadır[416]. Refah düzeyinin artırılması, ekonomik büyümeyi ve istihdamı desteklemek, iyi yaşama imkanlarının yaygınlaştırmak ve demokrasi ve pazar ekonomisine bağlı ülkeleri yakınlaştırmak için çalışmalar yürüten uluslararası bir kuruluş olan OECD, varlık amacını herkes için refahı, eşitliği ve fırsatı teşvik eden politikaları üretmek biçiminde açıklamaktadır[417].

OECD'nin araştırma ve politikaları üye ülkeler için bilgilendirme ve tavsiye niteliğindedir. Dolayısıyla OECD ilke ve rehberlerinin üye ülkelerin kendi iç hukuk düzenlemelerine dönüştürmeleri hususunda bir bağlayıcılığı bulunmamaktadır. Aslında Konsey, kişisel verilerin işlenmesiyle ilgili asgari gereklileri ortaya koyarak üye ülkelere bireysel özgürlükler, özel hayata saygı hakkı ve kişisel verilerin korunması ile ilgili olan ilkeleri kendi iç hukuklarında bu hususlarda yasal

416) https://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm (Erişim Tarihi: 16.07.2022).
417) https://www.oecd.org/about/ (Erişim Tarihi: 16.07.2022).

düzenleme yaptıklarında dikkate almalarını tavsiye etmektedir[418]. Dünyanın en büyük ve en güvenilir karşılaştırmalı sosyo-ekonomik veri ve analiz kaynaklarından biri olarak kendisini tanımlayan OECD, karar alma sürecini yönlendirmede de üye ülkelere yardımcı olmaktadır[419]. Bu itibarla özel hayatın gizliliğinin korunması, bilişim teknolojileri karşısında kişinin ve kişisel verilerinin korunmasıyla ilgili ilke ve kılavuz niteliğindeki birçok öncü çalışma OECD tarafından gerçekleştirilmiştir[420].

OECD üye ülkelerde serbest piyasa ekonomisinin sağlıklı işlemesi, gelişmesi ve demokrasinin güçlendirilerek istihdamın ve refahın artırılması amacıyla çalışmalar yapmakta, kılavuzlar ve tavsiye metinleri hazırlamaktadır. OECD metinlerine baktığımızda işverenin yönetim ve belirli kararları tek taraflı alma hakkının bulunduğu zımni olarak kabul edilmektedir. OECD Rehber İlkeleri'ndeki[421] tavsiye düzenlemelerle bu zımni kabule bir denge getirilmeye çalışılmış ve üye ülkelerde kişisel verilerin işlenmesi ve aktarılmasında veri sorumlularına belirli yükümlülükler getirilmiştir[422].

İşverenler gerçek kişileri çalıştırdıklarından aynı zamanda kişisel veri mevzuatı açısından birer veri sorumlusudurlar. Bilişim teknolojilerinin gelişmesine bağlı olarak birbirine daha bağımlı hale gelen küresel ekonomik düzende piyasa ekonomisinin sağlıklı işlemesi, üye ülkeler arasında iş birliğinin artırılması ve ticaretin gelişmesi için kişisel verilerin sınırlama olmaksızın güvenle aktarılması önemlidir. Bu kapsamda kişisel verilerin korunmasıyla ilgili ilk uluslararası metinler OECD tarafından hazırlanması[423] ve bu tür çalışmalara öncülük yapılması kişisel verilerin ekonomik boyutunun ve verilerin üye ülkeler arasında bir sınırlama

418) Küzeci, [2020], Kişisel Veriler, s. 160.
419) https://www.oecd.org/about/ (Erişim Tarihi: 16.07.2022).
420) OECD, [2013], The OECD Privacy Framework, s. 19-21.
421) OECD, The OECD Privacy Framework, s.14-15.
422)https://www.oecd-ilibrary.org//sites/1686c758-en/1/3/2/index.html?itemId=/content/publication (Erişim Tarihi: 08.07.2022).
423) OECD, The OECD Privacy Framework, [2013], s. 3-5. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Erişim Tarihi: 06.07.2022), (OECD, [2013], The OECD Privacy Framework).

olmaksızın güvenle aktarılmasının ekonomi üzerindeki öneminin bir belirtisi olarak da kabul edilmektedir[424].

Kuruluşundan kısa bir süre sonra özel hayatın gizliliğinin korunmasına ve gelişen teknolojiye bağlı olarak artan kişisel verilerin yoğun işlemeye konu edilmesinin önüne geçmek için çeşitli çalışmalar yapan OECD 1980 yılında, "Özel Yaşamın Gizliliğinin ve Kişisel Verilerin Sınır Ötesi Dolaşımının Korunması Hakkındaki Kılavuz"u yayımlamıştır[425]. Kılavuz uluslararası kabul görmüş ilk özel hayatın gizliliğinin korunması çerçeve metinlerini içermesi açısından önemlidir. Böylelikle OECD'nin 1980 tarihli Kılavuzu'nun içerdiği düzenlemelere uygun hareket eden devletler arasında kişisel verilerin kolaylıkla aktarılmasının temel kuralları ortaya çıkmıştır. Gelişen bilgi ve iletişim teknolojilerinin ortaya çıkardığı yoğun kişisel veri işleme olgusunun da bir sonucu olarak Kılavuz'un gözden geçirilmesi gündeme alınmıştır. Bu amaçla yapılan çalışmaların bir sonucu olarak, 11.07.2013 tarihinde OECD "Özel Yaşamın Gizliliğinin ve Kişisel Verilerin Sınır Ötesi Dolaşımının Korunması Hakkındaki Kılavuza İlişkin Tavsiye Kararı"nı kabul etmiştir. Konsey tarafından 2013'te yayımlanan "OECD Özel Yaşamın Gizliliği Çerçevesi" isimli kitapçıkta, Kılavuz'un düzenlemeleri ve düzenlemelerin açıklama bildirileri yer almıştır[426]. 2013'te yapılan gözden geçirmede Uzman Grubu, Kılavuz'un ikinci bölümünde yer alan sekiz temel ilkenin[427] korunması yönünde görüş bildirmiş, OECD Konsey'i de bu görüşü benimsemiştir.

Uzman Grubu, yeni iletişim ve bilgi teknolojilerinin ortaya çıkardığı

---

424) Küzeci, [2020], Kişisel Veriler, s. 160 vd.
425) OECD, [2013], The OECD Privacy Framework, s. 19.
426) OECD, [2013], The OECD Privacy Framework, s. 9-65.
427) OECD Rehber İlkeleri [1980], Rehber İlkeler, kişisel verilerin korunmasına ilişkin politikaların belirlenmesi ve yasal düzenlemelerin yapılmasında ölçüt olarak kullanılacak sekiz ilkeyi içermektedir. 2013 değişikliğinde Uzman Görüşüne uyularak korunan bu ilkeler şunlardan oluşmaktadır: 1. İlke: Veri toplamanın sınırlı olması ilkesi (m.7); 2. İlke: Verilerin belirli bir niteliği karşılaması (veri kalitesi) ilkesi (m.8); 3. İlke: Amacın belirliliği ilkesi (m.9); 4. İlke: Kullanımın sınırlı olması ilkesi (m. 10); 5. İlke: Veri güvenliği ilkesi (m. 11); 6. İlke: Açıklık ilkesi (m.12); 7. İlke: Bireyin katılımı ilkesi (m.13) ve 8. İlke: Hesap verilebilirlik ilkesi (m.14), OECD, [2013], The OECD Privacy Framework, s.14-15.

sorunları da dikkate alarak, 1980 tarihli Kılavuz'daki ilkelerin özünü koruyarak gizlilik yönetim programı, ulusal gizlilik stratejileri, veri güvenliği ihlal bildirimi gibi bazı yeni kavramlar önermiştir. Çerçeve metinde açıklandığı üzere Uzman Grubu'nun önerileri dikkate alınarak, 1980 tarihli Kılavuz'da iki tema doğrultusunda çalışmalar gerçekleştirilmiştir. OECD Konseyi'nin onayına sunulan güncelleme çalışmasında yer alan birinci konu, teknolojik gelişmelerin de etkisiyle özel hayatın gizliliğine yönelik ortaya çıkacak risklerin yönetilmesine ilişkin pratik uygulamalara odaklanılması; ikincisi ise özel hayatın gizliliğinin küresel boyutta korunması ve gündeme alınmasına yönelik çalışmaların yürütülmesidir[428].

IV. Avrupa Konseyi'nin Dijital İzlemeye Konu Kişi Haklarına İlişkin Hukuki Metinleri

Avrupa Konseyi, Avrupa ülkelerinde insan haklarını, kişi özgürlüğünü ve çoğulcu demokrasiyi geliştirmek ve hukukun üstün kılınması amacıyla 1949'da kurulmuş, günümüzde 46 üyesi bulunan ülkelerarası bir kuruluştur. Konsey insan hakkı olan özel hayatın gizliliğinin ve kişisel verilerin korunmasında öncü hukuki düzenlemelere imza atmıştır.

1. Avrupa İnsan Hakları Sözleşmesi'nin İlgili Düzenlemeleri

Konsey'in temel hak ve özgürlükleri düzenleyen en önemli düzenlemelerinden birisi, 4 Kasım 1950 tarihinde kabul edilen "İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme"dir[429]. AİHS insan haklarının korunması, özel hayatın gizliliğinin korunması, kişi hak ve özgürlüklerinin geliştirilmesi açısından önemli düzenlemeler içermektedir[430].

---

428) OECD, [2013], The OECD Privacy Framework, s. 4

429) https://www.goc.gov.tr/kurumlar/goc.gov.tr/yonetmelikler/Sozlesmeler/Avrupa-Insan-Haklari-Sozlesmesi.pdf (Erişim Tarihi: 19.07.2022).

430) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 72; Gürsel, [2016], İşçinin Kişisel Verileri, s. 69-70; Sevimli, [2006], Özel Yaşam, s. 36 vd.; Okur, [2013], Elektronik Gözetleme, s. 39 vd.; Tahir Muratoğlu, "Avrupa İnsan Hakları Mahkemesinin Kuruluşu Görevleri ve Yargılama Usulü", TAAD, Yıl: 7, S. 27 Temmuz,[2016], s. 313-315;

Avrupa Konseyi'nin önemli gündem konularından birisi de kişisel verilerin korunmasına ilişkin olmuştur. Özellikle teknolojik gelişmelerin yaygınlaşmasıyla ihlale açık temel haklardan birisi haline gelen özel hayatın gizliliğinin ve kişisel verilerin korunması Avrupa Konseyi'nin gündeminde önemli bir yer tutmuş ve dört yıla yayılan görüşmeler sonrası 108 sayılı "Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme" kabul edilmiştir. Bireyin özel hayatı ve kişisel verilerinin korunması hakkıyla yakından ilişkili olan AİHS düzenlemelerinin ve 108 sayılı Sözleşme'nin dijital izleme hakkının sınırlarına ve kişisel verilerin işlenmesinin koşullarına ilişkin referans düzenlemeler barındırdığını belirtmek gerekir[431].

Günümüzde insan hakları sadece kişiyi ve kişinin yaşadığı devleti ilgilendiren bir konu olmaktan çıkmış uluslararası hukuku ilgilendiren, diğer devletlerin ihlali gerçekleştiren devlete karşı belirli yaptırımlar uyguladığı bir düzeye gelmiştir[432]. Temel hak ve özgürlüklere ilişkin bu gelişmelerde ve benzer ulusal koruyucu enstrümanların ortaya çıkmasında AİHS'nin önemli bir etkisi bulunmaktadır[433]. Ülkemizin de tarafı olduğu AİHS'de özel hayatın gizliliğinin korunması "Özel ve Aile Hayatına Saygı" başlığında m. 8'de düzenlenmiştir. AİHS m. 8'e göre; "(1) Herkes özel ve aile hayatına, konutuna ve yazışmasına (haberleşmesine) saygı gösterilmesi hakkına sahiptir. (2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması

https://www.yargitay.gov.tr/documents/aihm2.pdf (Erişim Tarihi: 01.08.2022).
431) https://rm.coe.int/0900001680927ece s. 17-18, (Erişim Tarihi: 27.07.2022).
432) Şeref Ünal, Uluslararası Hukuk, Yetkin Yayınları, Ankara, [2005], s. 266.
433) Şeref Gözübüyük/Feyyaz Gölcüklü, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 7. Baskı, Turhan Kitabevi, Ankara, [2007], s. 2-4; Zafer Gören, "Temel Hakların Sınırlanması-Sınırlamanın Sınırları", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Yıl 6, S. 12, Güz/2, [2007], s. 44-46.

durumunda" mümkündür[434].

AİHS m. 8 özel hayata saygı hakkı kapsamında insan hakkı olarak koruma altına alınan kategorileri tanımlamaktadır. Bunlar; "özel hayata" ek olarak, özel hayatın belirli yönleri olarak kabul edilen "aile hayatı", "ev" ve "yazışmaları/haberleşmeyi" içermektedir. Maddede koruma altına alınan haklardan "özel hayatın korunması" diğer haklara göre daha geniş kapsamlıdır. Maddede özel hayata müdahale gerçekleştirilmeyeceği ve özel hayatın gizliliği hakkı güvence altına almakla birlikte, düzenlemenin 8/2. fıkrasında bu hakkın mutlak nitelikte olmadığı da düzenlenmiştir. Bu itibarla, AİHM kararlarında m. 8'in ihlal edilip edilmediğini incelerken iki koşulu inceler; bunlardan birincisi, m. 8'in 1. fıkrası kapsamında özel hayata saygı hakkına müdahale olup olmadığının denetlenmesi ve ikincisi, 8/2. fıkrada belirtilen kriterlere göre müdahalenin meşru olup olmadığının tespit edilmesidir[435].

Özel hayatın gizliliğinin korunması kavramının içeriğine kişisel verilerin girip girmediği meselesi tartışılmış olmakla birlikte, AİHM 1980'lerden beridir verdiği kararlarda[436] istikrarlı bir şekilde kişisel verileri de AİHS m. 8'in sağladığı güvenceler kapsamında değerlendirmektedir[437]. Öte yandan AİHM kararlarında[438] özel hayat, eksiksiz bir tanımı bulunmayan ve nerede başlayıp nerede sona erdiğinin kesin şekilde saptanmasının güç olduğu bir kavram olarak tespit edildiğinin de belirtilmesi gerekmektedir[439]. AİHM'e göre bu madde kapsamında güvence altına

434) Todor Kalamatiev/Aleksandar Ristovski, "The Right to Privacy in Employment and Its Protection under the European Convention on Human Rights", Iustinianus Primus Law Review, Vol. 11, No. Special Issue, [2020], s.3-4.
435) David Harris/Micheal O'Boyle/Colin Warbrick, Law of the European Convention on Human Rights, Second Edition, Oxford University Press, United States, [2009], s. 2-3.
436) AİHM Büyük Daire, S. And Marper v. The Unıted Kıngdom kararı, 04.12.2008, 30562/04 ve 30566/04, https://rm.coe.int/168067d216; EU, [2018], Handbook, s. 98-99.
437) Paul de Hert/Serge Gutwırth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", Reinventing Data Protection, Serge Gutwırth, Yves Poullet, Cecile de Terwangne, Sjaak Nouwt, Springer, [2009], s.19.
438) Arslan Öncü, [2011], Özel Yaşamın Korunması, s.182; Yargıtay HGK., E. 2014/56 K. 2015/1679 T. 17.6.2015.
439) Şen/Barın, [2021], Özel Hayata Saygı, s. 1.

alınan özel hayat kavramı, bir işçinin profesyonel hayatını dışlamaz ve kavramı sadece ev yaşamı ile sınırlandırmaz[440].

AİHM'in özel hayatın korunmasına ilişkin önemli yargılamalarından birisi olan Niemietz & Almanya[441] kararında mahkeme "özel hayat" kavramını sınırlamanın isabetli olmayacağını, kişi hayat alanına ilişkin birçok katmanın bu kavram içinde yer aldığını tespit etmiştir[442]. AİHM'e göre kişinin mesleki hayatı, mesleğini icra ederken ortaya çıkan veriler ve sınırlandırmalar, kişiliğini geliştirme özgürlüğü ve kendisini toplum içinde gerçekleştirme hakkı da özel hayat kavramı kapsamında değerlendirilir ve AİHS m. 8 korumasından faydalanır[443]. Böylelikle kişinin fiziksel ve ahlaki gelişimi bir bütünlük içinde dış müdahale olmaksızın korunması garanti edilmektedir[444]. Kişisel özerkliği korumayı amaçlayan bu kararlar aynı zamanda bireyin insan olarak kimliğinin ayrıntılarını oluşturma hakkını madde kapsamında koruma altına almaktadır[445].

AİHS m. 10'da ifade özgürlüğü temel bir hak olarak düzenlenmiş ve bunun haber ve görüş alma özgürlüğünü de kapsadığı metne işlenmiştir. İkinci fıkrada ise dijital izlemeye de dayanak olabilecek şekilde bu temel hakkın sınırları kamu güvenliği, suç işlenmesinin önlenmesi ve sağlığın veya ahlakın, başkalarının haklarının korunması biçiminde düzenlenmiştir[446].

Ayrıca belirtmek gerekir ki, AİHS'nin kabulünden sonra bilgi ve iletişim

---

440) WP29, Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55, [2022], s. 7.
441) https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57887%22]}, Niemitz v. Almanya, B. No: 137/1088, 16/12/1992, § 29.
442) Fernández Martínez v. İspanya, § 110; Oleksandr Volkov v. Ukrayna, § 165-66; Von Hannover v. Almanya (no. 2), § 95.
443) AİHM, Niemitz v. Almanya, B. No: 137/1088, 16/12/1992, § 29; Özpınar/Türkiye, B. No: 20999/04, 19/10/2010, § 45; Campagnano/İtalya, B. No: 77955/01, 23/3/2006, § 53; AYM, YÇ ve diğerleri, B. No: 2013/7054, 6.1.2015; AYM, EÜ kararı, B. No: 2016/13010, 17.09.2020.
444) William A. Schabas, The European Convention on Human Rights: a Commentary, Oxford University Press, Oxford, [2015], s. 370.
445) AİHM, Christine Goodwin v. the United Kingdom, Başvuru Numarası: 28957/95, 11 Temmuz 2002, § 90.
446) WP29, 5401/01/EN/Final WP 55, [2022], s. 7-8.

teknolojilerinde yaşanan hızlı gelişim ve dijitalleşme özel hayatın birçok katmanını ihlal edilebilir hale getirmiştir. AİHM kararlarına baktığımızda bu gelişmelere koşut olarak özel hayat kavramı için esnek bir yorum geliştirildiği ortaya çıkmaktadır[447]. Bu yorum şekli AİHS'nin gerekçesinde vurgulanan insan haklarını güvence altına almak ve geliştirmek amacıyla da örtüşmektedir.

Özel hayatın gizliliğini[448] AİHS ile yakından ilişkili bir diğer sözleşme Avrupa Konsey'i düzenlemesi "İnsan Hakları ve Biyotıp Sözleşmesi"dir. Sözleşme ile biyolojik ve tıbbi gelişmelerin insan onuruna ve insan haklarına aykırı düşecek şekilde kullanılmasının önüne geçmek hedeflemektedir. Biyotıp Sözleşmesi[449] toplum yararı veya bilimsel gereklilik gibi gerekçelerle insan yararını ihlal eden, insan onurunu geri plana iten ve kişinin bilgilenme hakkını engelleyen durumları önlemek için kabul edilmiştir[450]. Diğer yandan bu düzenlemelerin sağlık verilerini, özel hayatın gizliliğini ve kişisel verileri korumada yetersiz olduğuna ilişkin çeşitli eleştiriler de bulunmaktadır[451].

447) AİHM, Guide on Article 8 of the European Convention on Human Rights, Right to respect for private and family life, home and correspondence Updated on 31 August, [2021], s. 23-26;
Rehbere göre özel hayat kavramı, bireyin dış dünyaya sınırlandırdığı bir "iç çevre / giz alanı" ile sınırlı değildir (AİHM, [BD], Denisov v. Ukrayna, § 96). Bu itibarla 8. Madde, ister kişilik ister kişisel özerklik açısından olsun Maddede sağlanan güvencelerin yorumlanmasının altında yatan önemli bir ilke olan kişisel gelişim hakkını koruma, kendi tercihlerini yaşama ve geliştirme haklarını da kapsar. Aynı zamanda özel yaşam dış dünyayla ilişkiler, yani "özel sosyal yaşam" hakkını da kapsar (AİHM, [BD], Bărbulescu v. Romanya, § 71; AHİM, Botta v. İtalya, § 32, Guide on Article 8 of the European Convention on Human Rights, s. 23.
448) Sözleşme'nin "Özel Yaşam ve Bilgilendirilme" başlıklı III. Bölümü'nün 10. Maddesinde: "(1) Herkes, kendi sağlığıyla ilgili bilgiler bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir. (2) Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Bununla beraber, bireylerin, bilgilendirilmeme istekleri de gözetilecektir. (3) İstisnai durumlarda, 2. paragrafta belirtilen hakların kullanılmasında hastanın yararları bakımından kanun tarafından kısıtlamalar öngörülebilir" biçiminde özel yaşamın korunması ve ilgili kişinin bilgilendirilmesi ve bilgi edinmesi hususları düzenlenmiştir.
449) https://www.coe.int/tr/web/impact-convention-human-rights/convention-on-human-rights-and-biomedicine#/ (Erişim Tarihi: 01.08.2022).
450) Gözübüyük/Gölcüklü, [2007], İnsan Hakları, s. 8.
451) Şimşek, [2008], Kişisel Verilerin Korunması, s. 20 vd.

2. Kişisel Verilerin Korunmasına İlişkin 108 Sayılı Sözleşme ve 181 sayılı Ek Protokol

Yukarıda ele alındığı üzere kişisel verilerin korunması hakkı ile özel hayatın gizliliğinin korunması hakkı genellikle birlikte zikredilen haklardır, zira birbirini destekleyen bu iki hak arasında açık bir bağlantı bulunmaktadır[452]. Öte yandan bu haklar kapsamları ve düzenlendikleri metinler açısından birbirinden farklılıklar barındırmaktadır. Özel hayat KVK hukukunda merkezi bir yer işgal ederken, KVK hukukunun yalnızca veya hatta esasen özel hayatın gizliliğinin korunmasıyla ilgili olduğunu düşünmek yanıltıcıdır[453]. Zira kişisel veri koruma mevzuatı, bazı durumlarda geleneksel özel hayatın gizliliği kavramsallaştırmalarının ötesine geçerek farklı menfaatler arasında bir denge oluşturur. Dahası veri koruma mevzuatının odak ve gündeminin sürekli olarak geliştiği de açıktır. Bu değişiklikler bazen yasaların kendi metinlerinde ve bazen de veri koruma makamları (EDPB, CNIL - National Commission on Informatics and Liberty-, KVK Kurulu gibi) tarafından alınan karar ve eylemler yelpazesinde, özellikle de bağımsız düzenleyici ve denetleyici bir kurum olan veri koruma makamlarına geniş takdir yetkilerinin yer aldığı kararlarda da görülebilmektedir[454].

Kişisel verilerin korumasının gelişiminde önemli düzenlemelerden birisi Avrupa Komisyonu bünyesinde hazırlanan ve 1981'de imzaya açılan, 1985'de yürürlüğe giren 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ve "Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin" olarak 2001'de hazırlanan 181 sayılı Ek Protokol'dür. 108 No.lu Sözleşme 27 maddeden oluşmakta ve Sözleşmenin amacı; "Sözleşmeye taraf her ülkede, uyruğu ve ikametgahı ne olursa olsun her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi

452) § 2. IV. 1.
453) Lee A. Bygrave, "The Place of Privacy in Data Protection Law", University of New South Wales Law Journal, Vol. 24, No. 1, April, [2001], s. 282 vd.
454) Bygrava, [2001], The Place of Privacy, s. 282-284.

tutulması karşısında özel hayata saygı hakkını güvence altına almak" biçiminde düzenlenmiştir[455].

Geçen sürede kişisel veri işlemenin, global düzeyde veri akışının yoğunlaşması ve artan küreselleşme düzeyi sebebiyle her bireyin insan onurunun, insan haklarının ve temel özgürlüklerinin korunmasının gerekli olduğunu göz önünde bulundurarak, kişinin kendi verileri üzerindeki kontrol hakkının esas alındığı güncellemelerin yapılması gerekmiştir. Bu kapsamda, Sözleşme gelişmeler dikkate alınarak 2018 yılında güncellenmiştir[456].

Tüm AB üye devletlerinin onayladığı 108 sayılı Sözleşme, sınır ötesi yoğunlaşan veri akışı esas alınarak üye devletlerin iç hukuklarında ek düzenlemeler yapmaya ve Sözleşme'ye taraf olmayan ülkelere kişisel veri aktarılırken belirli yükümlülükleri yerine getirmeyi öngören 181 No'lu "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol" kabul edilmiştir[457]. Bu protokol ile Sözleşme'ye taraf devletler ülkelerinde uygulanmak üzer tamamen bağımsız denetleme gerçekleştirecek denetleyici makamlar kurma taahhüdünde bulunmuştur. Ülkemiz bu Protokolü 8 Kasım 2001 tarihinde imzalamış ve Protokol, 5 Mayıs 2016 tarih ve 29703 sayılı Resmi Gazete'de yayımlanarak bir iç hukuk düzenlemesi haline getirilmiştir[458].

Kişisel verilerin korunmasında 108 sayılı Sözleşme'nin önemi, bu konuda ilk bağlayıcılığı bulunan uluslararası sözleşme olması ve Sözleşme'ye taraf ülkelere

---

455) Ülkemiz, Sözleşme'yi 1981 yılında imzalamış olmasına rağmen Sözleşme'nin onaylanması ve iç hukuk açısından bağlayıcı hale gelmesi 18 Şubat 2016 tarih ve 29628 sayılı Resmi Gazete'de, ilgili Bakanlar Kurulu Kararnamesi ise 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete'de yayımlanmasıyla gerçekleşmiştir.

456) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (Erişim Tarihi: 06.08.2022).

457) EU, [2018], Handbook, s. 26.

458) KVK Kurumu, Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler Rehberi, s. 4. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/3a7934b6-406e-4911-a94d-795293aa0e3d.pdf (Erişim Tarihi: 10.11.2022).

kişisel verilerin korunmasında Sözleşme düzenlemelerine uyma yükümlülüğü yüklemesidir. Sözleşme'de kişisel veri: "kimliği belirli veya belirlenebilir bir gerçek kişi (ilgili kişi) hakkındaki her türlü bilgi" biçiminde tanımlanmıştır. Sözleşme'nin 3. maddesinde gerçekleştirilen kapsam düzenlemesiyle kamu sektörü ve özel sektör açısından bir farklılık öngörülmemiş, kamu ve özel fark etmeksizin herkes tarafından otomatik kişisel veri işlenmesi durumunda veya otomatik kişisel veri dosyası oluşturulması halinde Sözleşme kapsamındaki yükümlülüklerin yerine getirilmesi gerekmektedir. Sözleşme'nin diğer önemli bir özelliği, Sözleşme düzenlemelerinin AB Veri Koruma Direktifi 95/46/EC'ye önemli ölçüde ilham vermiş olmasıdır[459].

108 sayılı Sözleşme'nin modernize edilmesi amacıyla 18.05.2018 tarihinde "Kişisel Verilerin İşlenmesine ilişkin Kişilerin Korunması ile İlgili Sözleşmede Değişiklik Yapılmasına Dair Protokol" imzalanmıştır[460]. Modernleştirilmiş Sözleşme ile üye ülkeler arasında insan onuruna ve temel özgürlüklere saygı temeline dayanan bir kişisel veri işleme süreci oluşturulmak istenmiştir. Sözleşme'nin amacının düzenlendiği 1. maddede uyruğu veya yaşadığı yer neresi olursa olsun her bireyin kişisel verilerinin korunması hakkına sahip olduğu vurgulanmıştır. Bu düzenleme kişisel verileri işlerken insan haklarını, temel hak ve özgürlükleri ve özel hayatın gizliliğinin korunmasını gözetmeyi ve bunlar için gerekli mekanizmaları oluşturma yükümlülüğü getirmektedir. Ayrıca, Protokol ile aynı zamanda sınırlı ve ölçülü veri işleme, veri işlemenin hukuka uygun olması; genetik, biyometrik veri, sendika üyeliği, etnik köken gibi özel nitelikli kişisel verilerin işlenmesinin özel koşullara bağlanması ve veri işlemede şeffaflık yakalanması gibi düzenlemeler yapılmıştır. Aynı zamanda Modernleştirilmiş

459) Rebecca Wong, "The Data Protection Directive 95/46/EC: Idealisms and Realisms, International Review of Law, Computers & Technology, Vol. 26, No. 2-3, July-November, [2012], s. 229-231.

460) Danimarka'da gerçekleşen 128. Bakanlar Komitesi Oturumu'nda üye ülkelerde insan haklarına, hukukun üstünlüğüne ve temel özgürlüklere saygı temelinde kişisel verilerin işlenmesi için "108+ Sözleşmesi" olarak ifade edilen modernleştirilmiş sözleşme kabul edilmiştir. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (Erişim Tarihi: 05.11.2022).

Sözleşme'de yapay zeka uygulamalarındaki gelişmeler ve algoritmik karar verme süreçlerine ilişkin ilgili kişilere yeni haklar verilmiş ve veri koruma otoritelerinin yetkilerinin güçlendirilmesi hususları benimsenmiştir[461].

V. Avrupa Birliği Düzenlemelerinde Dijital İzleme ve Verilerin Korunması

AB'nin kişisel verilerin korunmasına ilişkin olan düzenlemesi, 24.10.1995 tarihli, "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Direktifi"dir[462]. GVKT'nin yürürlüğe girmesiyle 95/46 sayılı Direktif yürürlükten kalktığını belirtmek gerekir. Ayrıca, AB 95/46-EC sayılı Direktif ve 12.07.2002 tarihli Elektronik Komünikasyon Alanında Kişisel Özel Alanın Korunması ve Kişisel Verilerin İşlenmesi Hakkında Direktifi[463] (AB 2002/58-AT sayılı Direktif) kişisel verilerin tanımına, korumanın kapsamına, veri sorumlusu ve veri işleyenin yükümlülüklerine, özel nitelikli kişisel verilerin işlenme koşullarına ve ilgili kişiden açık rıza alınmasına ilişkin birçok hususta temel düzenlemeler getirmiştir.

1. Avrupa Birliği Temel Haklar Şartı

Temel hakları daha anlaşılır bir şekilde ortaya koyma ve bu haklara önemli bir yer verme düşüncesiyle 7 Aralık 2000 tarihinde Nice Zirvesi'nde Avrupa Parlamentosu, Konsey ve Komisyon Başkanları tarafından AB Temel Haklar Şartı[464] (Charter of Fundamental Rights of the European Union, CFREU)

461) CETS 223 – Automatic Processing of Personal Data (Amending Protocol), 10.X.2018 https://rm.coe.int/16808ac918 (Erişim Tarihi: 05.11.2022).
462) AB Resmi Gazetesi, 23.11.1995, No L 281/31 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.
463 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058 (Erişim Tarihi: 06.08.2022).
464) Şart, AB üyesi ülkelerin vatandaşlarına tanınan temel hak ve özgürlüklere ilişkin hakları resmileştirmek amacıyla 2 Ekim 2000'de düzenlenmiş ve 7 Aralık 2000 tarihinde onaylanmıştır. Temel haklar Şartı, Aralık 2009'da Lizbon Antlaşması ile birlikte yürürlüğe girmiştir. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (Erişim Tarihi: 06.08.2022).

imzalanarak ilan edilmiştir[465]. AB Temel Haklar Şartı'nın AİHS ile yakın bir bağlantısı bulunmaktadır. Zira madde 52/3'e göre; AİHS'de de güvence altına alınan temel haklar, Şart'ta da aynı anlam ve kapsama sahiptir[466]. Ancak bu asgari bir gereklilik anlamına gelmektedir. Şart'ın düzenlemeleri AB, AİHS veya tüm Üye Devletlerin taraf olduğu uluslararası anlaşmalarda tanınan insan haklarını ve temel özgürlükleri kısıtlayıcı veya olumsuz yönde etkileyecek şekilde yorumlanmaz[467]. ABAD da bu hususlara ilişkin olan birçok kararında doğrudan AİHM'in kararlarına atıfta bulunarak kararlar vermektedir[468]. Bu atıf Şart ile AİHS arasındaki yoğun ilişkinin bir diğer göstergesidir. Ayrıca AB Temel Haklar Şartı'nın 7. maddesi AİHS'nin 8. maddesine karşılık gelmektedir. Şart'ın bu düzenlemesi AİHS'nin 8. maddesini "yazışma/haberleşme" ifadesini kullanmayarak bir farkla birebir kapsamaktadır. Şart'ta "yazışma" yerine "iletişim" kelimesi kullanılarak teknolojik gelişmelere uygun olarak daha geniş bir kavram kapsamında özel hayatın korunması amaçlanmıştır[469]. Böyle olmasa dahi AİHM yazışma kavramını tüm iletişim süreçlerini de kapsayacak şekilde geniş yorumlamakta ve özel hayatın korunması kavramının kapsamına dahil etmektedir[470].

AB'de veri koruma hakkı anayasal düzeyde kabul görmüş olup, birliğin kendine özgü bir veri koruma rejimi bulunmaktadır. Bununla birlikte veri koruma

---

465) Yüksel Metin, "Avrupa Birliği Temel Haklar Şartı", Ankara Üniversitesi SBF Dergisi, C. 57, S. 4, [2002], s. 36.

466) https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2015/08/01/AB_TemelHaklarSarti.pdf (Erişim Tarihi: 06.08.2022).

467) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN m. 51-54.

468) ABAD, J. McB. v L. E., Dosyası, C-400/10, ECLI:EU:C:2010:582, PPU. 5 Ekim 2010, § 53-54, https://curia.europa.eu/juris/liste.jsf?language=en&num=C-400/10

469) AB Resmi Gazetesi, 2010/C 83/02,
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:FULL:EN:PDF

470) AİHM, Halford v. Birleşik Krallık Kararı No. 20605/92 (1997). Kararda kamu kurumlarınca gerçekleştirilen gizli izleme tedbirleri ve iletişimin dinlenmesi AİHS m. 8/1'deki haklara keyfî müdahalede bulunulması değerlendirilmiş ve bireyin bu haklarını koruyacak iç hukuk düzenlemelerinin de kişiye bu temel haklarını koruyucu haklar sağlamak zorunda olduğu ve kamu otoritelerinin hangi durumlarda gizli izleme yapılabileceğiyle ilgili bir şeffaflık oluşturulması gerekliliği kararda vurgulanmıştır. Telefon temelli dijital izlemeye ilişkin diğer birkaç karar için bkz. 02.08.1984 tarihli, 8691/79 başvuru no.lu Malone v. Birleşik Krallık Kararı; 25.03.1998 tarihli, 23224/94 başvuru no.lu Kopp/İsviçre Kararı; 01.07.2008 tarihli, 58243/00 başvuru no.lu Liberty & Diğerleri v. Birleşik Krallık Kararı.

hakkı AB Temel Haklar Şartı kabulünden önce mevcut olmasına rağmen, Şart daha ileri giderek, AİHS'den farklı olarak veri koruma hakkını, özel hayatın gizliliği hakkından ayrı olarak temel bir hak olarak düzenlemiştir. Şart'ın "Kişisel Verilerin Korunması" başlıklı 8. madde düzenlemesine göre; herkes, kişisel verilerinin korunması hakkına sahiptir ve kişisel veriler ancak meşru amaçlar için, ilgili kişinin rızası alınarak işlenebilir. Ayrıca ilgili kişi işlenen verilerine erişme ve hangi verilerinin işlendiğini bilme hakkına sahiptir. Madde 8'de ayrıca kişisel verilerin işlenmesinde belirlenen kuralların uygulamasını denetleyecek bağımsız bir otoritenin oluşturulması da düzenlenmiştir[471].

AB Temel Haklar Şartı'nda yer alan kişisel verilere ilişkin düzenlemenin önemi, bu hakkın aslında özel hayatın gizliliğinden farklı olarak kişiye ait bilinen bilgileri de korumasından ileri gelmektedir[472]. Zira özel hayatın gizliliği ile kişisel veriler ortak bir hakkın korunmasına gönderme yapmakla birlikte, kişiye ilişkin korunması gereken bazı bilgilerin gizli olmasına gerek yoktur. Kişisel verilerin korunmasına ilişkin düzenlemeler bu korumayı sağlayarak özel hayatın gizliliğinden farklılaşmaktadır[473]. Bu itibarla özel hayatın gizliliği ile kişisel verilerin korunması kapsamları ve tanımları açısından ayrışan hakları ifade etmektedir. AİHM'in kararlarında vurguladığı üzere özel hayat ve aile hayatı geniş kavramlardır ve birçok unsurdan oluşurlar. Kişisel verilerin korunmasına ilişkin düzenlemeler ise, özel hayata ve aile hayatına saygı gibi geniş kapsamlı kavramların ötesine geçerek bireyi belirli veya belirlenebilir duruma getiren tüm bilgileri korumaktadır[474].

İşverene işçilerin sağlık ve güvenliklerini sağlama, yeterli dinlenme süreleri

---

471) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
472) Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yayınları, 3. Baskı, İstanbul, [2019], s. 99.
473) Spiros Simitis, "Privacy - An Endless Debate", California Law Review, Vol. 98, No. 6, December [2010], s. 1993-1996.
474)https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf; Article 29 Data Protection Working Party, Opinion 4/2007 On The Concept of Personal Data, 01248/07/EN WP 136, [2007], s. 7 (Erişim Tarihi: 08.11.2022).

verme yükümlüğü yükleyen AB Temel Haklar Şartı'nın 31. maddesi dijital izleme açısından önemlidir. Zira işçilerin sağlığını ve güvenliğini temin etmek için dijital izleme uygulamalarını kullanmak gerekli ise, işveren meşru amaç kapsamıyla sınırlı olmak üzere bu yükümlülüğü yerine getirmelidir. Aynı değerlendirmeyi Çalışma Süreleri Direktifi (EC 2003/88/EC) için gerçekleştirmek mümkündür[475].

2. 95/46/ Sayılı Kişisel Verilerin Korunmasına İlişkin Direktif

Özel hayata saygı gösterilmesi hakkı kapsamında yıllarca oluşan literatür ve uygulama bireye önemli kazanımlar sağlamıştır. Ne var ki, özellikle gelişen teknoloji ve dijitalleşen dünya açısından kişinin gizli alanından başka, gizli olmayan ve belirli ilişkiler kapsamında bir yerle paylaştığı bilgilerinin de korunması gerektiği olgusunu ortaya çıkarmıştır[476]. Bu gelişmelerin bir yansıması olarak özellikle veri gizliliğinin korunması açısından ikinci nesil gelişmelerden en önemli düzenlemelerden birisi olan AB 95/46 EC sayılı Direktif[477], bu alana 2016'da Genel Veri Koruma Tüzüğü'nün (GVKT/GDPR) kabulüne kadar önemli katkılar sunmuştur. GVKT kişisel verilerin korunmasına ilişkin önemli değişikler getirerek bu alanı Tüzük düzeyinde üye ülkeler açısından bağlayıcı bir şekilde düzenlemiştir. Bu düzenlemelerde doğrudan işverenin dijital izleme uygulaması kullanmasına ilişkin bir madde yer almamakla birlikte, düzenlemelerdeki korumanın kapsamı ve kişisel verilerin işlenmesinin sınırlarına ilişkin düzenlemeleri birlikte değerlendirdiğimizde, zımni olarak veri sorumlusu olan işverenin dijital izleme hakkının bulunduğunun kabul edildiği ve işveren veri sorumlusunun veri işlemedeki yükümlülüklerine ilişkin düzenlemeler getirildiği ortaya çıkmaktadır[478].

---

475) AB Resmi Gazetesi, 2010/C 83/02, 30.03.2010, s. 397.
476) Paul De Hert/Vagelis Papakonstantinou, "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization", Preferably a UN Agency, I/S: A Journal of Law and Policy for the Information Society, Vol. 9, No. 2, [2013], s. 271-272.
477) Rupert Battcock, "Data Protection: Where Next", International Journal of Law and Information Technology, Vol. 3, No. 2, [1995], s. 158.
478) Wong, [2012], Data Protection Directive, s. 238.

Kişisel verilerin korunmasına ilişkin üye ülkelere tüzük düzeyinde kurallar getiren ve 25.05.2018 tarihinde yürürlüğe giren 2016/679 sayılı Genel Veri Koruma Tüzüğü (AB 2016/679 sayılı GDPR) de iş ilişkisinde kişisel verilerin işlenmesini, işverenin dijital izleme hakkını kural olarak kabul etmekte ve belirli sınırlamalar getirmektedir.

AB'nin dijital izleme yükümlülüğü öngören düzenlemelerden birisi de AB 2006/561 sayılı karayolu taşımacılığına ilişkin düzenleler getiren Tüzüktür. Tüzük, 85/3821 sayılı Karayollarında Kontrol Araçlarına ilişkin düzenlemeler getiren Tüzüğe gönderme yaparak karayollarında yük ve yolcu taşıyan araçları kullanan şoförlerin araçları kullanma süreleri ile dinlenme sürelerini kayıt altına alınacak şekilde takograf takılmasını öngörmektedir. Böylelikle araç sahipleri veya bağlı bulunduğu işveren araçlara gerekli elektronik cihazları takarak sürüş ve dinlenme sürelerini kayıt altına almakla yükümlüdür.

Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46 EC sayılı Direktif'in amacı başlangıç kısmında; malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımının sağlandığı bir iç pazarın ortaya çıkarılması ve işletilmesi, bu yapılırken aynı zamanda kişinin temel haklarının korunması ve güvence altına alınması, kişisel verilerinin güvenli aktarılması biçiminde açıklanmıştır. Bununla birlikte ikinci paragrafta özel hayatın korunması başta olmak üzere, bireyin temel hak ve özgürlüklerin korunması amacına da vurgu yapılmıştır[479].

95/46 EC sayılı Direktif'in 7. maddesine göre ilgili kişinin temel hak ve özgürlüklerini ihlal etmemek kaydı ile işverenin meşru menfaatlerinin bulunduğu durumlarda kişisel verilerin işlenmesi hukuka uygundur. Bu madde veri sorumlusu ile kişisel veri sahibinin hakları arasında bir dengelemeyi amaçlamakla birlikte kişisel veri sahibinin kişisel verilerinin korunmasına, işlemenin sınırlarına ilişkin

479) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0056&from=EN

makul beklentilerini boşa çıkarabilir. Bu husus dengelemek için 7. maddeye ve Direktif'teki bazı düzenlemelere ilişkin WP 29 Çalışma Grubu 2001, 2009[480] ve 2014'de görüşler açıklamıştır. Bu kapsamda işverenler meşru menfaatleri çerçevesinde dijital izleme gerçekleştirirken işçilerin hakları üzerinde bu izlemenin etkilerini göz önüne almalı[481] ve amaç için en az etkiyi oluşturacak izleme yöntemini uygulamalıdır[482]. Kişisel verilerin işlenmesine ve serbest dolaşımına ilişkin gerçek kişileri korumaya yönelik önemli yenilikler getiren ve "veri koruma yasalarının en kapsamlı ve başarılı uluslararası aracı[483]" olarak tanımlanan 95/46 EC sayılı Direktif 2016/679 sayılı Genel veri Koruma Tüzüğü'nün yürürlüğe girmesiyle yürürlükten kalkmıştır[484].

3. 2002/58/ Sayılı E-Gizlilik Direktifi ve E-Gizlilik Tüzüğü Çalışmaları

Elektronik iletişimin gizliliğine ilişkin olan 2002/58EC sayılı Direktif, AB'deki elektronik iletişimin gizliliğini korumak ve veri koruma direktifi olan 95/46 sayılı Direktifi tamamlamak, elektronik iletişim açısından temel hak ve özgürlükler ile özel hayatın gizliliğini korumak üzere kabul edilmiştir[485]. E-Gizlilik Direktifi elektronik bilgilerin gizliliği, internet trafik verilerinin işlenmesi, spam ve çerezler gibi alanlara ilişkin dijital izleme konularını ele almaktadır. Bu mevzuat kişilerin internette gezinme, cep telefonu, giyilebilir teknolojiler ve internete bağlı diğer cihazların işlediği verilerde kişinin gizliliğini korumayı hedeflemektedir[486].

Dijitalleşmenin yaygınlaşmasıyla çeşitlenen dijital izleme uygulamaları

480) Wong, [2012], Data Protection Directive, s. 232.
481) WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, [2014], s. 36-41.
482) WP29, Opinion 8/2001, [2001], s. 4.
483) Colin J. Bennett/Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, [2013], s. 112.
484) Maria Tzanou, "European Union Regulation of Transatlantic Data Transfers and Online Surveillance", Human Rights Law Review, Vol. 17, No. 3, September, [2017], s. 552.
485) Daniel B. Garrie/Rebecca Wong, "Spyware Technologies: Limiting the Horizons of Digital Privacy", Thomas M. Cooley Law Review, Vol. 23, No. 3, [2006], s. 486.
486) AB 2002/58EC sayılı Direktif, AB Resmi Gazetesi, L 201/37, 31.07.2002, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

dikkate alınarak 2009'da E-Gizlilik Direktifi çerezler esas alınarak güncellenmiştir[487]. Gerçekleştirilen güncellemenin yetersiz olduğu, Direktifin özellikle trafik verileri dışındaki konum verilerini düzenleyen 9. maddesinin yeterli koruma sağlamadığı, çerezler ile metaverileri etkili korumada başarısız olduğu ve üye ülkelerin çoğunun bunları hariç tutması hususunda Direktif eleştirilmiştir[488]. Direktifin düzenlenme hedeflerini ve amacını gerçekleştirmemesinde AB üye ülkeleri arasında farklı uygulamalardan kaynaklanmaktadır. Ayrıca teknolojideki gelişmelerin takip edilmemesi ve teknolojinin gelişim hızına uygun güncellemelerin yapılmaması ve Direktifin temelde klasik telekomünikasyon temelli gizliliğe odaklanması sebebiyle bireylerin akıllı telefonların çevrimiçi profil oluşturma, sosyal medyanın ve internetin ortaya çıkardığı sonuçlara karşı savunmasız bıraktığına ilişkin tespitler yapılmıştır[489].

GVKT, 25 Mayıs 2018 tarihinde 95/46 sayılı Direktifin yerini alarak tüm AB üye devletlerinde yürürlüğe girdi. Ne var ki, GVKT tüm veri işleme alanlarını kapsamamaktadır. Özellikle elektronik iletişim ve çevrimiçi iletişimde işlenen veriler için 2009'da çerezler açısından güncellenen 2002/58 EC sayılı Direktifi uygulanmaktadır. Bu direktif 2002 yılından kalma olduğundan ve 2001 ile 2002'de yayımlanan WP 29 Çalışma Grubu görüşlerinden[490] sonra iş ilişkisinde kişisel verilerin işlenmesinin gelişen teknolojiye bağlı olarak çeşitlenmesi ve sistematik bir hal alması, bu çalışmaların birçok hususta teknolojik gelişmenin gerisinde kaldığı eleştirilerine sebebiyet vermiş ve bu eleştiriler raporlarda ve görüşlerde yer

487) Jos Dumortier, "Evaluation and Review of the ePrivacy Directive", European Data Protection Law Review (EDPL), Vol. 2, No. 2, [2016], s. 247, Dumortier, [2016], ePrivacy; Garrie/Wong, [2006], Spyware Technologies, s. 488.
488) Dumortier, [2016], ePrivacy, s. 248.
489) Shara Monteleone, EPRS, European Parliamentary Research Service, Members Research Service PE 608.661, EU Legislation in Progress, September, [2017], s. 3-4.
490) WP29, Opinion 08/2001 on the processing of personal data in the employment context, WP 48, 13 Eylül 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf; WP29, Working document on the surveillance of electronic communications in the workplace, WP 55, 29 Mayıs, [2002], url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (Erişim Tarihi: 21.12.2022).

almıştır[491].

Bunun üzerine Avrupa Komisyonu, GVKT ile uyum sağlamak için 17 Ocak 2017 tarihinde Elektronik İletişimde Gizlilikle ilgili olarak 2017/0003 E-Gizlilik Tüzüğü'nü önermiştir. Tartışmalara açılan taslak metinlerde özellikle rıza kavramı üye ülkelerce endişeyle karşılanmıştır. Sürecin uzaması üzerine Avrupa Veri Koruma Kurulu (EDPB), GVKT ile elektronik iletişim sektöründe kişisel verilerin korunmasına ilişkin düzenlemeler öngören 2002/58 sayılı Direktif arasında sıkı bir bağ bulunduğunu ve bunların birbirini tamamladığını, E-Gizliliğe ilişkin olarak E-Gizlilik Tüzüğü'nün kabul edilmesi çağrısında bulunmuştur[492]. Geçen süreçte kabul edilen Tüzük, 19 Ekim 2022 tarihinde yayımlanmıştır. Kişisel verilerin korunmasını yakından ilgilendiren ve 25 Ağustos 2023'te yürürlüğe giren AB Dijital Hizmetler İçin Tek Pazar (Dijital Hizmetler Yasası – Digital Services Act - DSA) ve Dijital Market Yasası (DMA) kişisel verilerin korunması açısından önemli düzenlemelerdendir[493].

Avrupa Komisyonu E-Gizlilik Tüzüğü sosyal medya platformlarında sunulan iletişim hizmetleri için de geçerli olacak ve bu platformlar geleneksel telekomünikasyon operatörleri ile aynı düzeyde veri ve iletişim gizliliğini sağlayacaktır. Ayrıca Tüzükle, AB üye ülkelerinde yürürlüğü bulunan bir yasal düzenlemeyle tüm insanlara aynı düzeyde yasal koruma sağlanması amaçlanmıştır. Tüzük iletişimin içeriği, çerezler ve bunları kapsayan metadata verilerini yüksek bilgi gizliliği ve güvenliği kapsamında korumayı öngörmektedir. Ayrıca bu kişisel verilerin işlenmesi başkaca bir veri işleme şartı kapsamına girmiyorsa ancak açık rıza ile işlenebilecektir[494].

---

491) WP29, Opinion 2/2017 on data processing at work, 17/EN WP 249. s. 3.
492) Leyla Keser Berber/Ayça Atabey/Melis Mert, "E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler",vDergisi, [2019], C. 1, S.2, s. 67.
493) https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (Erişim Tarihi: 12.08.2022).
494) https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation (Erişim Tarihi: 12.08.2022).

4. 2016/679 Sayılı Genel Veri Koruma Tüzüğü

Dijital uygulamaların iş yapma süreçlerine ve nesnelere sirayet ettiği günümüzde kişiler ve işyerleri giderek artan şekilde çevrimiçi uygulamalarla işlerini yürütmektedir. Ağ üzerinde kişisel, sosyal ve eğlence amaçlı veya iş amaçlı birçok ihtiyacın karşılandığı ve iş görme açısından çevrimiçi uygulamaların hayati önemde olduğu söylenebilir[495]. Bu gelişmelerin ortaya çıkardığı karmaşık ve yoğun kişisel veri işleme olgusu kişisel verileri korumaya ilişkin düzenlemelerin koruyuculuğunu sorgulanır hale getirmektedir. Bu sorgulamaların sonucu ortaya çıkan ve kişisel verilerin etkin korunması için ileri koruyucu düzenlemelerin yer aldığı GVKT bu başlıkta ele alınacaktır.

a) Genel Veri Koruma Tüzüğü'nün Hazırlanma Sebepleri

Teknolojinin gelişim hızı ve çeşitlenen yeni veri işleme uygulamalarının yasal düzenlemelerin kapsamına dahil olup olmadığı tartışmalar neden olmaktadır[496]. Bu sebeple düzenleyici kurumlar, kapatılmadan önce WP 29 Çalışma Grubu görüşleri, sonrasında yerine kurulan EDPB görüş ve kararları ile yargı organları kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan kavramları özel hayatın gizliliği ve kişisel verilerin korunması açısından geniş yorumlayarak kararlar vermektedir[497].

GVKT ortaya çıkmış uygulamalar, görüşler ve dijitalleşmenin ortaya çıkardığı kişisel veri işleme biçimleri dikkate alınarak oluşturulmuş ve AB üye ülkelerinde doğrudan bağlayıcılığı bulunan, kişisel verilerin korunmasına ilişkin yeni ileri düzenlemelerin yer aldığı önemli düzenlemelerden birisidir. 2016/679 sayılı GVKT, 95/46 sayılı Direktif ile karşılaştırarak tüm değişiklikleri

495) Nina Gumzej, "Data Protection For The Digital Age: Comprehensive Effects of The Evolving Law of Accountability", Juridical Tribune, Volume 2, Issue 2, December, [2012], s. 83.
496) Vivarelli, [2020], Informational Self-Determination, s. 301.
497) EC, Evaluation Of The Implementation of The Data Protection Directive, Annex 2, [2012], s. 101-102.

karşılaştırmalı incelemek tezin amacıyla bağdaşmayacağından, sadece iş ilişkisi bağlamında, işçilerin haklarını korumaya odaklanan iş hukukunda dijital izlemeye ilişkin olan hükümlere ağırlık verilmiştir.

GVKT, genel olarak 95/46 sayılı Direktifin tercih ettiği sadece bir alana ait olmama prensibini devam ettirmiştir. Bundan dolayı, GVKT'de yer alan hükümler kullanılan teknolojik yapıdan bağımsız olarak her türlü kişisel veri işleme faaliyetinde uygulama alanı bulur. Diğer yandan bu iki düzenleme arasındaki en önemli fark, GVKT'nin AB'de veri koruma yasalarını birleştiren ve üye ülkelerce uyulması zorunluluğu bulunan bir düzenleme olmasıdır.

İşçiler hem kendilerine ilişkin işlemlerde hem de iş ilişkisinin bir gereği olarak sayısız kişisel veri paylaşırlar. GVKT'nin 4. maddesinin 1. fıkrasına göre, kişisel veriler: "kimliği belirli veya belirlenebilir bir gerçek kişiye (veri öznesi – ilgili kişi) ilişkin her türlü bilgi anlamına gelmektedir." Bu tanım, 95/46 sayılı Direktif'teki kişisel veri tanımını ile örtüşmektedir. AB'nin, böylesine geniş bir kişisel veri tanımını tercih etmesinde kişisel verileri etkin bir şekilde ve değişen şartlar kapsamında koruyabilmek için özellikle benimsediği kabul edilmektedir[498]. Ayrıca GVKT madde 4'ün devamında kişisel verilerin neleri kapsayabileceği bir örnek listesiyle açıklanmıştır. Buna göre; özellikle belirli bir gerçek kişinin adı, soyadı, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı verileri ya da ilgili gerçek kişinin fiziksel özelliği, takma adı, genetik bilgileri, davranışsal ve fizyolojik verileri, kültürel ve ekonomik verileri, statüsüne veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre bağlı olarak bir kişiyi doğrudan veya dolaylı olarak belirlenebilir hale getiren veriler kişisel veridir. İşçinin adı, telefon numarası, e-posta adresi, işyerindeki imajı, internet iletişimine ilişkin metadata verileri, IP adresi, çevrimiçi tanımlayıcılar[499] vb. tüm veriler kişisel veri olarak

498) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, 04.05.2022, L 119/33, s. 33.
499) GVKT İngilizce Metni, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Erişim Tarihi: 08.12.2022).

nitelendirilmektedir. Geniş bir kavram olduğu kabul edilen ve tanımı GVKT'da "her türlü bilgi" ifadesiyle yapılan kişisel veri kavramının kapsamında nelerin bulunduğu WP 29 Çalışma Grubu'nun 2007 tarihli kişisel veri kavramına ilişkin görüşünde daha detaylı bir şekilde açıklanmaktadır[500].

İşlenmesi halinde ilgili kişinin ayrımcılığa ve istenmeyen uygulamalara maruz kalma ihtimalini barındıran bazı kişisel veriler GVKT m. 9'da "özel kategorideki kişisel veri"[501] olarak düzenlenmiş ve bunların korunması için daha sıkı şartlar öngörülmüştür. Bu itibarla veri sorumlusu işverenin, işçilerin ırkı, etnik kökeni, dini veya felsefi inançları, sendika üyeliği, biyometrik ve genetik verileri, sağlık verileri, cinsel eğilimine ilişkin veriler, siyasi görüşleri gibi özel nitelikli kişisel verilerin işlenmesi söz konusu olduğunda daha katı koşulları yerine getirmesi ve buna göre teknik ve idari tedbirleri alması gerekmektedir[502]. Örneğin, belirlenebilme ölçütü açısından bir işçinin kendisine yakın hissettiği siyasi partinin sayfalarını beğenmesi, sosyal medya hesaplarını takip etmesi veya inançlarına yakın bulduğu bir inanç grubunu veya felsefi inancı takip etmesi, beğenmesi, cinsel tercihine yönelik internet trafik bilgileri dijital izlemeyle tespit edilebilir. Belirlenebilme ölçütüne uyan bu veriler aynı zamanda özel nitelikli kişisel veri olduğundan bu örnek açısından veri sorumlusu işveren bu verileri ancak GVKT'da öngörülen işleme şartlarının varlığında işleyebilir (aynı yönde KVKK m. 6). GVKT'de bunlar hassas (özel nitelikli) kategoride bulunan kişisel veri olarak düzenlendiğinden işlenmesi için belirlenen sıkı işleme koşullarının yerine getirilmesi gerekmektedir[503].

---

500) WP 29, Opinion 4/2007 on the concept of personal data Adopted on 20'th June, 01248/07/EN WP 136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, s. 1-26, (Erişim Tarihi: 08.12.2022).

501) KVKK m. 6/1'de özel nitelikli kişisel veriler sınırlı sayı ilkesine uygun olarak şu şekilde düzenlenmiştir: "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."

502) GVKT m. 9 temel ilke olarak bu tür verilerin işlenmesini yasaklamaktadır. Maddenin devamında ise bu verilerin işlenme koşulları istisnai olarak düzenlenmiştir.

503) Official Journal of the European Union, L 119/1, 4.5.2016, 51-54. Paragrafları, s. 10-11.

GVKT'de veri işleme faaliyeti madde 4'ün 2. paragrafında: "otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisi" biçiminde yapılmıştır[504].

Kişisel verilerin işlenmesinden neyin anlaşılması gerektiği geniş bir şekilde örneklendirilmiş ve temel olarak kişisel veriler üzerinde gerçekleştirilen herhangi bir işlemin kişisel verileri işleme kavramı kapsamında olduğu düzenleme altına alınmıştır. Bu tanım kapsamında örneğin, işçilerin sosyal medya profillerinin izlenmesi, sosyal medya paylaşımlarından ekran görüntüsü alınması, işçilerin işyerindeki hareketlerinin kayıt altına alınması, depolanması, düzenlenmesi, aktarılması gibi süreçlerin tamamı kişisel veri işleme olarak kabul edilir. Günümüzde kişisel veriler yoğun olarak otomatik sistemler üzerinde gerçekleştirilmesine rağmen, GVKT madde 4/2'de sayılan süreçlerin otomatik yollarla bir sistem üzerinde gerçekleştirilmesi ile (örneğin kamera, mobil cihazlar veya bilgisayarlar) manuel olarak işlenmesi arasında bir farkın bulunmadığını "otomatik yöntemlerle olsun veya olmasın" ifadesiyle ortaya koymaktadır[505].

İş sözleşmesi yasal olarak (hukukumuz açısından örneğin İş Kanunu m. 75) belirli tür verilerin işlenmesinin hukuki zemini oluşturur. Ancak verilerin elde edilmesi kadar aktarılması da GVKT veya KVKK kapsamında veri işleme olarak kabul edildiğinden sadece sözleşme ilişkisi bu aktarmanın yasal dayanağı olmaz. Ayrıca örneğin vergi mevzuatı ve SGK mevzuatı gibi mevzuatlarda işvereni bununla yükümlü kılan düzenlemelerin de bulunması gerekir. Aksi durumda verilerin aktarılması veri işleme süreci olarak kabul edildiğinden hukuka aykırı bir

504) Official Journal of the European Union, L 119/1, 4.5.2016, s. 33; KVKK m. 3/1-e bendinde kişisel verilerin işlenmesi benzer içerikte düzenlenmiştir.
505) Official Journal of the European Union, L 119/1, 4.5.2016, s. 33.

veri işleme söz konusu olabilecektir[506].

GVKT'de veri işlemenin taraflarından birisi olan veri sorumlusu, kişisel verilerin işlenmesinin amacını ve araçlarını tek başına veya başkalarıyla birlikte belirleyen, veri işleme süreçlerinin üzerinde belirleyici olan gerçek veya tüzel işi ile kamu otoritesi, ajans veya organ gibi aktörlerdir. Ayrıca GVKT m. 26'da "ortak kontrolörler" (ortak veri sorumluları) kavramı getirilmiş ve iki ya da daha fazla sayıda veri sorumlusunun kişisel verilerin işleme amaç, araç ve yöntemlerini ortak belirlediği durumlarda bunlar ortak kontrolör olarak nitelendirilmektedir[507]. Maddenin devamına göre bu kontrolörler kendi sorumluluklarını detaylandıran bir düzenleme kabul etmelidirler. Bu kapsamda örneğin dijital izlemede kişisel verilerin işlenmesinde bulunulan role uygun olarak işverenler, işveren kontrolör/ortak kontrolör veya işleyici olarak nitelendirilebileceklerdir. Belirli veya belirlenebilir kişisel verileri işlenen ilgili gerçek kişi ise işçi, işçi adayı veya eski işçi olabilecektir[508].

b) Genel Veri Koruma Tüzüğü'nün İş İlişkisine Etkisi

AB üye ülkeleri açısından öncelikli olarak bir gerçek kişi olan işçinin verilerinin işlenmesinde GVKT düzenlemelerinin dikkate alınması gerekmektedir. GVKT, tamamen veya kısmen otomatik araçlarla gerçekleştirilen kişisel veri işleme süreçlerini ve otomatik yollarla gerçekleştirilmeyen ancak işlenen kişisel verilerin bir veri kayıt sisteminin parçasını oluşturmasının amaçlandığı süreçlerde kullanılan veri işleme araçlarını kapsamaktadır[509]. Burada belirtilmesi gereken önemli bir husus iş ilişkisinde kişisel verilerin işlenmesine ilişkin olan WP 29 Çalışma Grubu'nun 8/2001 görüşünde işçilerin e-posta veya internet kullanımının izlenmesinin, kamera gözetlemesinin veya ses verilerinin işlenmesinin ve ayrıca

506) EU, [2018], Handbook, s. 98-99.
507) Official Journal of the European Union, L 119/1, 4.5.2016, s. 48-49.
508) Official Journal of the European Union, L 119/1, 4.5.2016, s. 48.
509) Official Journal of the European Union, L 119/1, 4.5.2016, s. 32.

çoğu manuel kaydın da kişisel verilerin korunması düzenlemeleri kapsamına girdiğinin vurgulanmasıdır[510]. Bu itibarla GVKT m. 6 ile 9'da öngörülmüş veri işleme şartlarının, işçilerin kişisel verilerinin işlendiği bu tür işleme biçimleri için aranması esastır[511]. Ayrıca gerçekleştirilen internet trafik kaydı izlemesi, e-posta takibi, kamera gözetlemesi veya diğer dijital izleme yöntemlerinde GVKT m. 12 ve devamı maddelerinde düzenlemiş olan şeffaflık düzenlemelerine uygun olmalı ve her durumda işçinin bilgilendirilmesi gerekmektedir[512].

Kişisel verilerin işlenmesi süreçlerinde şeffaflıktan ne anlaşılması gerektiği de önemlidir. WP 29 Çalışma Grubu 2017/2 görüşünde kişisel verilerin işyerinde işlenmesi hususlarına açıklık getirerek, işverenlerin kişisel verilerin işlenmesinde şeffaflığı yakalamaları için verileri işlenen ilgili kişilere haklarının açık ve sade bir dille açıklanması ve işlenen verilerine ne olacağı hususlarında bilgi verilmesi gereklidir. Bu aynı zamanda kişisel verilerin işlenmesinin özel amacının, kişisel verilerin toplandığı anda veri sahibi tarafından bilinmesi gerektiği anlamına gelmektedir[513].

İş ilişkisi temelde iş sözleşmesine ve kanunlarda öngörülmüş belirli yükümlülüklerin yerine getirilmesi temelinde yürüyen bir ilişki olduğundan GVKT m. 6/1-a kapsamında rıza aranmadan kişisel veri işlenebilir. Bununla birlikte iş sözleşmesi veya kanunlarda öngörülen düzenlemeler kapsamında kişisel verilerin işlenmesine olanak bulunmayan durumlarda açık rıza alınması gereklidir. Ne var ki, iş ilişkisi bağımlılık ilişkisi ile karakterize edildiğinden, veri sorumlusu işverenler ile işçiler arasında ekonomik ve diğer alanlardaki güç dengesizliği söz konusu olduğundan, görece olarak zayıf konumda olan, işe ihtiyacı bulunan işçinin ne kadar özgür irade ile rızasını açıkladığı da şüphelidir[514].

---

510) WP29, Opinion 8/2001, s. 24-25.
511) Official Journal of the European Union, L 119/1, 4.5.2016, s. 36-38.
512) WP29, Opinion 8/2001, s. 25.
513) EU, [2018], Handbook, s. 120.
514) EU, [2018], Handbook, s. 144.

Bu tür dengesizliklere ve bağımlılık unsuruna tipik örneklerden birisi, bir işverenin kişisel verileri iş ilişkisi bağlamında işlemesidir. Bu itibarla WP 29 Çalışma Grubuna göre; işçiler, iş ilişkisinde bulunan bağımlılık unsuru ve güç asimetrisi göz önüne alındığında, neredeyse hiçbir zaman özgürce rıza verme, reddetme veya vermiş olduğu rızayı geri alma konumunda değildir[515]. İş ilişkisindeki otorite/bağımlılık dikkate alındığında, işçiler ancak bir teklifin kabul edilmesi veya reddedilmesiyle ilgili hiçbir sonucun bulunmadığı istisnai durumlarda özgür rızalarını açıklayabilir[516] ve kişisel verileri üzerinde gerçek anlamda belirleyici olabilirler[517].

Kişisel verilerin işlenmesine ilişkin temel ilkeler GVKT m. 5'te düzenlenmiştir. Bu ilkeler her türlü veri işleme faaliyeti için geçerli olup, GVKT'nin veri işlemeye ilişkin rehber nitelikte temelini oluşturmaktadır[518]. Temel ilkeler aynı zamanda kişisel verilerin işlenmesini düzenler ve bireyin korunmasının ana çerçevesini belirleyerek GVKT'nin hükümlerinin uygulanmasında ve yorumlanmasında veri sorumlularına[519] ve yargı organlarına[520] rehberlik eder. Aslında bu temel ilkeler yeni değildir ve 95/46 sayılı Direktif ile kişisel verileri korumaya yönelik uluslararası düzenlemelerle paralellik arz etmektedir. GVKT m. 5 bu temel ilkeleri daha sistematik ve kapsamlı olarak düzenlemektedir. Maddede

515) Bu konuda daha detaylı bilgi için bkz. Article 29 Working Party 2001, Opinion 8/2001 on the processing of personal data in the employment context, WP 48, Bürüksel, 13 Eylül 2001; Article 29 Working Party 2005, Working document on a common interpretation of Article 26/1 of Directive 95/46/EC of 24 Eylül 1995, WP 114, Bürüksel, 25 Kasım 2005; Article 29 Working Party 2017, Opinion 2/2017 on data processing at work, WP 249, Bürüksel, 8 Haziran 2017.
516) Frederik J. Zuiderveen Borgesius/Sanne Kruikemeier/Sophie C. Boerman/Natali Helberger, "Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the ePrivacy Regulation", European Data Protection Law Review (EDPL), Vol. 3, No. 3, [2017], s. 358.
517) EU, [2018], Handbook, s. 144-145.
518) EU, [2018], Handbook, s. 116.
519) GVKT madde 5/2, veri sorumlularının veri işleme faaliyetlerini temel ilkelere uygun gerçekleştirmede ve kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasında doğrudan sorumlu olduğu düzenlemektedir. Aynı şekilde, madde 24/1 veri sorumlularının, kişisel verileri işlemenin GVKT'ye uygun olarak gerçekleştirildiğini ispatlamak ve bu hususu gösterecek uygun teknik ve organizasyonel önlemleri uygulayacağını belirtmektedir.
520) Prashant Mali, "GDPR Articles With Commentary & BU Case Laws", [2019,] s. 13-17. https://archive.org/details/GDPRArticlesWithCommentaryEUCaseLaws_201904/page/n33/mode/2up

hukuka uygunluk sebepleri, adalet ve şeffaflık[521]; veri işlemenin amaçla sınırlandırılması[522], veri işlemenin en az seviyeye indirilmesi[523], doğruluk[524], saklama süresinin sınırlandırılması[525], bütünlük ve gizlilik[526] temel ilkeleri yer almaktadır.

Kişisel verilerin işlenme şartları ve işleme faaliyetinin hukuka uygunluğu GVKT m. 6'da düzenlenmiştir. İş ilişkisi açısından önemli olan kişisel verileri hukuka uygun işleme, ilgili kişinin bir veya birden fazla spesifik amaç için kişisel verilerinin işlenmesine rıza göstermesi veya veri işlemeyi gerektirecek bir sözleşmeye veri sahibi ilgili kişinin taraf olmasıdır[527]. Bununla birlikte iş ilişkisinde yaygın olarak kişisel veri işlenmesine dayanak yapılan veri işleme şartları; sözleşme ilişkisinin bulunması, veri sorumlusu işverenin kişisel veri işlemede meşru menfaatinin bulunması ve veri sorumlusunun yasal bir yükümlülüğü yerine getirmesidir[528].

İşçilerin kişisel verilerinin işlenmesiyle doğrudan ilgili olan GVKT düzenlemesi m. 9/2-h ve m. 88'dir. Madde 9/2-h'de işçilerin özel nitelikli kişisel verilerinin işlenme şartları öngörülmüş ve m. 88'de "iş bağlamında işlemede" üye devletlerin özellikle: "işe alım, kanunla ya da toplu sözleşmeler yoluyla belirtilen yükümlülüklerin yerine getirilmesi de dahil olmak üzere iş sözleşmesinin yürütülmesi, çalışma, iş yerinde eşitlik ve çeşitlilik, iş sağlığı ve güvenliğinin yönetimi, planlanması ve düzenlenmesi, işverenin veya müşterinin mallarının

521) GVKT m. 5/1-a.
522) GVKT m. 5/1-b.
523) GVKT m. 5/1-c.
524) GVKT m. 5/1-d.
525) GVKT m. 5/1-e.
526) GVKT m. 5/1-f. Tüzüğün bu ilkeleri şemsiye hükümler niteliğinde olup, sonraki maddelerindeki daha ayrıntılı hükümler için bir referans olma işlevi görmektedir. Tüzüğün bu ilkeleri ayrıca, Modernize Edilmiş 108 sayılı Sözleşme'nin 5., 7., 8. ve 10. maddelerinde de yer almaktadır. Modernize Edilmiş Sözleşme ile Avrupa Konseyi veya AB seviyesindeki tüm veri koruma mevzuatları açısından bu genel ilkelerin uyumlu olması sağlanmaya çalışılmıştır. Ayrıca veri koruma mevzuatı yorumlarken bu şemsiye nitelikteki genel ilkeler akılda tutulmalıdır.
527) GVKT m. 6/1-a ve b.
528) GVKT m. 6/1-c ve f.

korunması ile ilgili amaçlar ve istihdam ile ilgili haklar ve menfaatlerin münferit ya da toplu olarak kullanımı ve bunlardan yararlanılmasına ilişkin amaçlar ve iş ilişkisinin sona erdirilmesine ilişkin amaçlar doğrultusunda çalışanların kişisel verilerinin iş bağlamında işlenmesine yönelik hakların ve özgürlüklerin korunmasının sağlanması amacıyla kanun veya toplu sözleşmeler çerçevesinde daha spesifik kurallar belirleyebileceği" hususlarına dikkat etmesi öngörülmüştür[529].

Düzenlemenin son cümlesi kapsamında üye ülkeler toplu iş sözleşmesi veya yasa çerçevesinde kişisel verilerin korunması ve işçilerin özgürlüklerinin temini için ülkelerine özgü kurallar öngörebileceklerdir. İş ilişkisine özel öngörülmüş olan GVKT m. 88 düzenlemesinin bir sonucu olarak işyerinde kişisel verilerin korunmasına ilişkin üye ülkeler arasında farklılıklar ortaya çıkabilecektir. Bununla birlikte GVKT hükümlerinin bir gereği olarak işçinin kişisel verilerinin işlenmesine ve saklanmasına ilişkin olarak bilgilendirilmesi, işçinin kişisel verilerinde bir ihlal meydana geldiğinde işveren bu ihlali işçiye bildirmekle yükümlüdür[530]. Örneğin yerel kanunlarda tehlikeli nitelikte olan bazı işler açısından işçilerin günlük çalışma ve dinlenme sürelerinin kayıt altına alınmasını, dijital izleme uygulamalarıyla işçilerin takip edilmesi (örneğin tehlikeli madde taşıyan tır şoförleri) ve bunun ilgili kurumlara bildirilmesini işveren açısından yükümlülük haline getirebilir[531].

GVKT m. 88'in işçilere yönelik koruyucu ek bir düzenleme getirmediği, iş ilişkisinde kişisel verilerin korunması büyük önem taşımasına rağmen AB'nin, tüm AB genelinde işçileri koruyucu tek tip bir kural koymayı başaramadığı hususları eleştirilere konu edilmektedir[532]. Kişisel veri özellikle ABAD, AİHS kararlarında

529) Official Journal of the European Union, L 119/1, 4.5.2016, s. 38, 84.
530) EU, [2018], Handbook, s. 331-332.
531) ABAD, C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 30 Mayıs 2013, § 19. ABAD, Worten yargılamasında ulusal yasaların kişisel veri işlenmesini gerektirecek spesifik düzenlemelerinin bulunabileceğine karar vermiştir.
532) Claudia Ogriseg, "GDPR and Personal Data Protection in the Employment Context", LLI, Vol. 3, No. 2, [2017], s. 3-4.

ve WP 29 Çalışma Grubu'nun, sonrasında yerine kurulan EDPB[533] çalışmalarında özel hayata saygı hakkı, özgürlük ve bireysel insan hakkı olarak kodlanmış olmasına rağmen, kişisel verilerin yoğun işlemeye konu edildiği iş ilişkisi açısından GVKT'da özel normlarla işçilerin korunmadığı belirtilmelidir[534]. İşçilerin haklarının korunmasında ölçülülük ilkesi kapsamında hareket edildiği, işçilerin kişisel verilere ilişkin haklarının korunması mutlak hak olarak kabul edilmediği ve GVKT m. 88 kapsamında her üye devlet kendi spesifik kurallarını düzenleyebilme hakkına sahip olduğundan GVKT'de işçilerin kişisel verilerinin etkin bir şekilde korunmadığı ifade edilmektedir[535].

İş ilişkisinde işçiler, kişisel verilerinin işlenmesine rıza göstermedikleri takdirde bunun meydana getireceği olumsuz sonuçlardan çekinebilirler. ABAD bir kararında pasaport için başvuran kişilerin parmak izlerinin alınmasına özgürce rıza göstermiş sayılamayacağını[536], çünkü insanların pasaporta ihtiyacı olduğuna karar vermiştir[537]. Bu itibarla, zorunluluk halinin bulunduğu durumlarda veya iş ilişkisi gibi bir sözleşmeye taraf olunmasının ihtiyaç olduğu ilişkilerde rıza özgürce verilmiş olmayacağından alınan rızanın geçersiz olduğuna karar verilmektedir. Özellikle dijital izleme açısından bakıldığında işçinin bir izleme uygulamasıyla karşılaştıktan sonra başkaca bir seçeneği bulunmadığı için verilerinin izlenmesini kabul etmesi durumunda gerçekte özgürce verilmiş bir rızanın varlığından bahsedilemez[538].

533) EDPB için bkz. https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en
534) Ogriseg, [2017], Employment Context, s. 3.
535) Ogriseg, [2017], Employment Context, s. 4.
536) Borgesius/Kruikemeier/Boerman/Helberger, [2017], s. 354.
537) Case C-291/12 Schwartz v Stadt Bochum [2013] ECLI:EU:C:2013:670, § 32, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0291&from=en
538) Borgesius/Kruikemeier/Boerman/Helberger, [2017], s. 355.

İKİNCİ BÖLÜM
DİJİTAL İZLEMENİN HUKUKİ DAYANAKLARI VE SINIRLARI

§ 5. DİJİTAL İZLEMENİN HUKUKİ ÇERÇEVESİ

İşverenin dijital izleme uygulamalarıyla işyeri verimini artırma, kalite standartlarını koruma, işyeri risklerini minimize etme, ticari işlemlerde delilleri kayıt altına alma ve işin işyeri prosedürlerine uygun görülmesi, sistemlerin güvenliği, işyerinde suçun önlenmesi amacıyla dijital izleme gerçekleştirmesi Anayasa'da düzenlenen mülkiyet hakkıyla ilgilidir[539]. İşverenin dilediği işçilerle iş sözleşmesine taraf olması ve sözleşme düzenlemeleriyle işin yapılma biçimini ve kurallarını belirlemesi anayasal haklardan birisi olan sözleşme özgürlüğü hakkından dayanağını almaktadır[540]. Ayrıca işverenin iş sözleşmesinden doğan kapsamlı borçlarından birisi olan işçiyi gözetme borcu işçinin kişiliğini, beden ve ruhsal bütünlüğünü ve kişisel verilerini koruma yükümlülüğünü işverene yüklemektedir[541]. İşverenin iş sözleşmesinden doğan yönetim hakkı ve işçileri gözetme borcu dijital izlemenin dayanaklarındandır. İşverenin kullandığı dijital izleme uygulamalarının dayanağı olan bu haklar ve yükümlülükler bu başlıkta değerlendirmeye konu edilecektir.

I. Dijital İzlemenin Anayasal ve Yasal Dayanakları

İş hukuku insanların emek sarf ettikleri tüm çalışmaları değil, sadece "bağımlılık" ilişkisi çerçevesinde gerçekleştirilen çalışmaları ve bu çalışmalar sonucu ortaya çıkan iş ilişkisini kapsamına almaktadır[542]. İş sözleşmesinde somutlaşan iş ilişkisi sözleşme taraflarına haklar ve yükümlülükler yükler ve işçinin

539) Okur, [2013], Elektronik Gözetleme, s. 31.
540) Süzek, [2019], İş Hukuku, s. 53; Okur, [2013], Elektronik Gözetleme, s. 30.
541) Baycık, [2006], Maden İşçileri, s. 102; Süzek, [2019], İş Hukuku, s. 386 vd.
542) Güzel, [1997], Fabrikadan İnternete, s. 87; Doğan Yenisey, [2007], İşyeri ve İşletme, s. 77; Süzek, [2019], İş Hukuku, s.225; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 118; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 1-2; Ekonomi, [1987], Ferdi İş Hukuku, s. 1; Tunçomağ/Centel, [2018], İş Hukukunun Esasları, s. 1.

temel hakları ile özel hayatının gizliliği ve kişisel verileri üzerinde belirli sınırlamalar ortaya çıkarır[543].

1. Dijital İzleme Uygulamalarının Anayasal Dayanakları

İş ilişkisinde işyerine ilişkin riskler ile ekonomik külfetler işverenin üzerindedir[544]. İşverenin işyerinin devamlılığını sağlayabilmesi ve iş sözleşmesinden doğan yükümlülüklerini yerine getirebilmesi amacıyla anayasada ve çeşitli kanunlarda işverene haklar tanınmış ve yükümlülükler yüklenmiştir. Zira işverenlerin üretim veya hizmet sunumu için edindiği eşyanın mülkiyetini ve işyeri faaliyeti kapsamında sunduğu mal veya hizmetin kalitesini koruyabilmesi ve idari yaptırımlarla karşılaşmaması ancak işyerinde faaliyetin yasalara uygun yürütülmesi, işçilerin denetlenmesi ve işyerine ilişkin belirli prosedür ve talimatlar oluşturulmasıyla mümkündür[545].

İş ilişkisinde dijital izleme uygulamalarının anayasal dayanağı işverenin mülkiyet, ekonomik ve verimlilik menfaatlerinde uygulama bulan anayasal hükümlerden kaynaklanmaktadır. İşverenin bu menfaatleri Anayasa m. 48'de düzenlenen çalışma ve sözleşme özgürlüğü ve m. 35'te düzenlenen mülkiyet hakkı kapsamında güvence altına alınmıştır[546]. Anayasal sözleşme özgürlüğü hakkı işverene istihdam edeceği işçiyi seçme ve iş sözleşmesinin içeriğini belirleme; bağımsız karar alma, özerk faaliyette bulunma ve işyerine ilişkin belirli prosedürler oluşturmada serbest davranabilme haklarına kaynaklık etmektedir[547].

İşverenin yönetim hakkının anayasal dayanağı olan ve Anayasa m. 35'te

543) Süzek, [2019], İş Hukuku, s. 395; Sevimli, [2006], Özel Yaşam, s. 64 vd.; Hendrickx, [2002], Workers Personal Data, s. 11-12.
544) Doğan Yenisey, [2007], İşyeri ve İşletme, s. 82.
545) Okur, [2013], Elektronik Gözetleme, s. 31.
546) Süzek, [2019], İş Hukuku, s. 78 vd.; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 238; Okur, [2013], Elektronik Gözetleme, s. 30.
547) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 244 vd.; Okur, [2013], Elektronik Gözetleme, s. 30-31.

düzenlenmiş olan mülkiyet hakkı işverenin uygulayacağı dijital izlemenin dayanağını oluşturmaktadır. Mülkiyeti koruma hakkı kapsamında işveren hırsızlığı önlemek, işçiye iş görme borcunun ifası için tahsis edilen eşyanın sözleşmeye uygun kullanılmasını sağlamak, işçiyi denetlemek ve elektronik iletişim araçlarının kötüye kullanımını engellemek gibi amaçlarla dijital izleme uygulamaları kullanabilmektedir[548]. Yukarıda ele alındığı üzere, ILO işçilerin kişisel verilerinin korunmasına ilişkin hazırlamış olduğu Uygulama Kodu'nda işverenin sağlık, güvenlik ve mülkiyetin korunması için gerekli olması halinde kişisel veri işleyebileceği ve izleme uygulamaları kullanabileceği ifade edilmiştir[549].

İşverenin dijital izleme uygulamaları ile veri işleme faaliyeti yürütmesi Anayasa m. 48/1'de düzenlenmiş olan sözleşme özgürlüğüne ilişkin düzenlemeden de kaynaklanabilir[550]. Girişim özgürlüğü işverene yasal düzenlemeler kapsamında kalmak kaydı ile ticari girişimde bulunma hakkı tanımaktadır. Anayasa'nın 48/1. maddesinde düzenlenen girişim özgürlüğü işverene istediği alanlarda ticari girişimde bulunma, iş organizasyonunu oluşturmada özgürlük, istediği kişilerle iş sözleşmelerine taraf olma, işyerine ilişkin talimatlar oluşturma, bağımsız karar alabilme, denetim ve belirli kuralları önceden düzenleme haklarını vermektedir. Girişim özgürlüğü aynı zamanda işverenin faaliyet konusu işte üretim aşamalarında ve personel planlamasında bağımsızca hareket etmesi özgürlüğünü içermektedir[551].

İşverenin girişimde bulunma hakkı Anayasa m. 48/2 kapsamında devletin aldığı tedbirlere uygun faaliyetini sürdürmesi düzenlemesi ve bu amaçla öngörülmüş yasal düzenlemeler kapsamında sınırlandırılmıştır. Anayasa Mahkemesi'nin çeşitli kararlarında vurguladığı gibi girişim özgürlüğü ile girişim özgürlüğünü sınırlayan düzenlemeler arasında dengenin kurulması aynı zamanda

548) Okur, [2013], Elektronik Gözetleme, s. 32.
549) ILO, Protection of workers' personal data, An ILO code of practice, m. 6/14-3. s. 4.
550) İş hukukunda sözleşme özgürlüğünün sınırlandırılması için bkz. Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 244 vd
551) Okur, [2013], Elektronik Gözetleme, s. 31; Süzek, [2019], İş Hukuku, s. 79.

"sosyal devletin" bir gereğidir[552]. Zira sosyal hukuk devleti ilkesi iş hayatını koruyan bir düzen kurma, ekonomik önlemler alma yükümlülüğünü devlete yüklemektedir[553]. Bundan dolayı işverenin mülkiyete ve sözleşme özgürlüğüne ilişkin hakları Cumhuriyetin niteliklerinin sayıldığı sosyal bir hukuk devleti olma ilkesiyle de yakından ilgilidir.

Girişim özgürlüğü kapsamında kurulan işyerinin tanımı İş Kanunu m. 2'de yapılmış olup, tanımdan işyerinin maddi unsurlar ile maddi olmayan unsurlardan oluştuğu ortaya çıkmaktadır. İşyerinin maddi unsurları görülebilen bina, makine, ham madde, araçlar gibi eşyalardan oluşur. Maddi olmayan unsurlar ise fikri ve sınai hakların mal ve hizmet üretiminde artan önemine binaen ön plana çıkmış: patent, buluş, know how, müşteri çevresi gibi şeylerden oluşur[554]. Bu hususların çoğu aynı zamanda mülkiyet hakkının konusu olduğundan Anayasa'da düzenlenen mülkiyet hakkına ilişkin güvenceler; işverene işyerini oluşturan maddi ve maddi olmayan varlıklarını hırsızlık, ticari sırların ifşası, kötüye kullanım gibi olaylara karşı korumaya yönelik çeşitli vasıtalarla denetim[555], başka bir söyleme dijital izleme gerçekleştirme hakkını tanır.

Aşağıda ayrıntılı olarak inceleneceği ve AİHM ve AYM kararlarında vurgulandığı üzere, dijital izlemeye ilişkin belirli politikaların oluşturulması, işçilerin bilgilendirilmesi ve gerektiğinde rızalarının alınması koşuluyla dijital izleme uygulamaları kullanılabileceği genel olarak kabul edilmektedir[556]. Sonuç

552) AYM, 1988/19 E., 1988/33 K. 26.10.1988, https://www.resmigazete.gov.tr/arsiv/20016.pdf
553) Süzek, [2019], İş Hukuku, s. 51-52; AYM, 2001/479 E., 2005/1 K., Karar Tarihi: 06.01.2005, Resmi Gazete: 18.10.2005, Sayı: 25970.
554) Doğan Yenisey, [2007], İşyeri ve İşletme, s. 17.
555) Okur, [2013], Elektronik Gözetleme, s. 32.
556) İleride detaylı ele alındığı üzere Bărbulescu v. Romanya kararında, Başvuran yerel mahkeme kararları sonrası AİHM'de Romanya'ya karşı dava açmıştır. 12 Ocak 2016 tarihinde, AİHM 4. Dairesi, bire karşı altı oyla, Başvuranın özel hayata ilişkin haklarının Romanya tarafından ihlal edilmediğine karar vermiştir. Daire, yerel mahkemelerin, Başvuranın özel hayatına saygı hakkı ile işverenin menfaati arasında kendi takdir alanları dahilinde adil bir denge kurduğunu ve hukuki dinlenme hakkının yerine getirildiğini ve Başvuranın bu fırsatlara sahip olduğuna karar vermiştir. Bu karar üzerine Başvuran, Büyük Daire'ye sevk talebinde bulunmuş ve talebi kabul edilmiştir. AİHM Büyük Daire, çalışanların mesajlaşmaların izlenebileceği konusunda işverenin önceden bilgilendirilmesi, izlemenin amacı ve sınırlarının belirtilmiş olması gerektiğine vurgu yapmıştır.

olarak işverenin mülkiyeti koruma, iş verimini artırma ve hukuki yükümlülükleri yerine getirmek amacıyla dijital izleme uygulamaları kullanılmasının değinilen anayasal dayanakları bulunmaktadır[557].

2. Dijital İzleme Uygulamalarının Yasal Dayanakları

İş ilişkisinde işverenin dijital izleme uygulamalarını kullanma hakkı doğrudan yasal düzenlemelere konu edilmemekle birlikte çeşitli kanunlarda dijital izleme uygulamalarına dayanak olabilecek yasal düzenlemeler bulunmaktadır.

a) Genel Olarak Dijital İzlemenin Yasal Çerçevesi

Ülkemizde dijital izlemeyi işveren ve işçi bakımında düzenleyen ya da doğrudan yasaklayan bir düzenleme bulunmamaktadır. Avrupa ve ABD veri koruma mevzuatlarında da dijital izlemeyi işverenler açısından doğrudan düzenleyen bir yasal düzenleme yer almamaktadır[558]. Bu itibarla işverenin dijital izleme uygulamaları kullanmasının, bu uygulamalarla işçinin kişisel verilerini

---

Aynı doğrultuda işveren izlemenin niteliği ve kapsamı özellikle mesajlarının içeriğine erişebilme hususunda işçi bilgilendirilmelidir. AYM, Genel Kurul E.Ü. kararında (2016/13010 Başvuru no, 27.06.2020 karar tarihi, R.G. Tarih ve Sayı: 14/10/2020-31274): Ancak işveren davalı taraf olarak yargılama sürecinde kişisel verilerin işlenmesinin hukuki dayanağı ve işlemenin amaçları, işlenecek verilerin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, işlemenin sonuçları ve verilerin muhtemel yararlanıcılarını gösterir bir bilgilendirme yapıldığını ortaya koyamamıştır. Bu bağlamda yargılama sürecinde feshin temel sebebini oluşturan e-posta iletişimine yönelik olarak böyle bir bilgilendirmenin yapılıp yapılmadığı derece mahkemelerince tartışılmamış, başvurucunun kendisi alenileştirmediği hâlde onun rızası alınmadan ve önceden bir bilgilendirme yapılmadan e-posta içeriklerine erişildiği yönündeki esaslı iddialarının karşılanmadığı anlaşılmıştır... Öncelikle işverenin işçinin kullanımına sunulan iletişim araçlarını denetlemesi ve çalışanın kişisel verilerinin işlemesine ilişkin olarak 4857 sayılı Kanun'da özel bir düzenleme olmadığı görülmüştür. Ancak Anayasa'nın 20. ve 22. maddelerinde yer bulan özel hayata saygı ile kişisel verilerin korunmasını isteme hakları ve haberleşme hürriyetine ilişkin güvenceler ile 6698 sayılı Kanun ile hukuk sistemimizde mevcut olan genel düzenlemelerin (bkz. §§ 22-29) iş hukuku uyuşmazlıklarında uygulanması yönünde bir engel olmadığı gözetildiğinde yasal altyapı oluşturmak bağlamında pozitif yükümlülüklerin yerine getirilmiş olduğu söylenebilir.

557) Alpagut, [2019], Kamera Gözetlemesi, s. 310.

558) Kambellari, [2014], Employee Email Monitoring, s. 2.

işlemesinin ve işçileri denetlemesinin genel olarak iş ilişkisinin doğasında bulunduğu, kaynağının da iş sözleşmesi olduğu kabul edilmektedir[559].

GVKT m. 6'da sözleşme ilişkisinin bulunması ve veri işleyenin meşru menfaati gibi durumlarda kişisel verilerin işlenebileceği düzenlenmiştir. KVKK m. 5/2-c bendinde "sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla" kişisel veri işlenebileceği hüküm altına alınmıştır. KVK hukukunda yer alan bu düzenleme aynı zamanda veri sorumlusu işverenin dijital izleme uygulaması kullanmasının dayanağını ve çerçevesini oluşturur. Ayrıca işverenlerin dijital izleme uygulaması kullanma hakkını belirleyen ve izlemenin sınırlarına ilişkin çalışmalar içeren WP 29 Çalışma Grubu'nun[560] 2001 yılın ait iş ilişkisinde kişisel verilerin işlenmesine ilişkin görüşünde işverenin dijital uygulaması kullanmasının gerekliliğine ve sınırlarına yönelik tespitler yer almıştır[561]. Bu görüş, iş ilişkisinde izleme uygulamalarına işverenin meşru menfaati açısından bir sınırlama getirilerek 95/46 EC sayılı Direktife (değişiklik sonrası GVKT m. 6) bir denge getirilmeye çalışılmıştır[562]. Görüşün "Gözetleme ve İzleme" başlığında kişisel verilerin işlenmesine ilişkin yükümlülüklerinin işçilerin e-posta kullanımı, internet erişimi, kamera kaydı ve konum verileri gibi işçilerin izlenmesi ve gözetlenmesi uygulamalarında da geçerli olduğu vurgulanmıştır[563].

AB üye ülkelerinde işverenin dijital izlemeyle denetleme hakkının dayanağına ilişkin yapılan araştırmalarda iş sözleşmesinin doğasında işverenlerin,

559) Okur, [2013], Elektronik Gözetleme, s. 29-30; ILO, International Labour Conference, 95th Session, Report V-(2A), [2006], s. 155-160; Bamberger/Mulligan, [2013], Privacy in Europe, s. 1542; Kambellari, [2014], Employee Email Monitoring, s. 1-2.
560) WP29 Çalışma Grubu, 25 Mayıs 2018 tarihinde GVKT'nin yürürlüğe girmesiyle ortadan kalkmıştır. WP29 Çalışma Grubu yerine GVKT kapsamında EDPB (The European Data Protection Board - Avrupa Veri Koruma Kurulu) kurulmuştur. AB genelinde kişisel verilerin korunmasına ilişkin bir yeknesaklık oluşturmayı hedefleyen EDPB, Brüksel'de merkezi bulunmakta ve üyeleri AB ulusal veri koruma makamları ve Avrupa Veri Koruma Denetçisi (EDPS) temsilcilerinden oluşmaktadır.
561) Bkz. § 4. V.
562) WP29, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP 48, [2001], s. 15.
563) WP29, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP 48, [2001], s. 4.

işçilerin sözleşmeye uygun iş yaptıklarını kontrol etme, işçinin performansını ölçme, makine ve teçhizatı kullanmada ve korumada gerekli özeni gösterdiği hususlarında sözleşmeye dayalı bir izleme haklarının bulunduğu genel olarak kabul gördüğü tespit edilmiştir[564]. Üye ülkelerde örneğin iş sağlığı ve güvenliği gereklilikleri, işveren makine ve teçhizatının korunması ve doğru kullanımının sağlanması, üretim süreçlerinin ve iş performansının denetlenmesi, kalite kontrolünün yapılması gibi amaçlar işçilerin izlenmesinin haklı gerekçeleri olarak kabul edilmektedir[565].

Ülkemizde işverenin işyerinde kullanacağı dijital izleme uygulamalarının dayanağı çeşitli kanunlarda, iş sözleşmesinde ve idari düzenlemelerden ortaya çıkmaktadır. İşverenin işçinin kişiliğini koruma ve gözetme borcu, yasal zorunluluklar, yönetim hakkı, işçinin işyeri talimat ve prosedürlerine uyma yükümlülüğü bunların başlıcalarıdır[566]. Ayrıca işverenin dijital izlemeye ilişkin hak ve yükümlülüklerinin bir gereği olarak örneğin; iş sözleşmesinden doğan ve TBK m. 399'da düzenleme ve talimatlar açısından kullanım şeklini somutlaştıran yönetim hakkı, TBK m. 417'de düzenlenmiş olan "işyerinde iş sağlığı ve güvenliğinin sağlanması için gerekli her türlü önlemi almak, araç ve gereçleri noksansız" bulundurma ve işçilerin cinsel ve psikolojik tacize uğramalarını önlemeye ilişkin her türlü tedbiri alma yükümlülüğü, İSGK m. 4'te düzenlenen işçilerin işle ilgili sağlık ve güvenliğini korumaya ilişkin genel yükümlülükleri ve özellikle maden, yeraltı çalışmaları, tehlikeli madde taşıyıcılığı gibi işlerde m. 5'teki risklerden korunma ilkelerinde öngörülen yükümlülükler, sağlık gözetimine ilişkin yükümlülükler getiren m. 15 ve 5651 sayılı Kanun kapsamında belirli işyerleri açısından internet trafiğinin kayıt altına alınması yükümlülüğü kapsamında dijital izlemenin farklı türlerini kullanmaktadır.

---

564) Hendrickx, [2002], Workers Personal Data, s. 119; Bu üstü kapalı kabulde AİHM içtihatlarında oluşturulan içtihatlara uygunluk dikkate alınmalıdır. Zira özel hayata saygı hakkının profesyonel hayatı da kapsadığı ve işçiye dijital izlemeye ilişkin bir bilgilendirme yapılmamışsa işçinin makul bir gizlilik beklentisi bulunduğu hususu için bkz. Copland v. Birleşik Krallık, § 41-42, 45.
565) Hendrickx, [2002], Workers Personal Data, s. 118-119.
566) Okur, [2013], Elektronik Gözetleme, s. 32-33.

Eklemek gerekir ki, işçinin iş sözleşmesinden doğan borçları da dijital izlemenin dayanağını oluşturabilir. Örneğin işverenin, işçinin işini özenle yaptığını ve işin işveren menfaatine uygun yerine getirildiğini denetlemede menfaati bulunmaktadır. İşçinin özen ve sadakat borcuna ilişkin yasal düzenleme bu yönüyle dijital izlemenin dayanağını oluşturur. Zira bu borç işçiye işini özenle yapma, işverenin haklı menfaatlerini koruma, işverene ait eşyaları, sistem ve tesisleri usulüne uygun kullanma, sır saklama, rekabet etmeme yükümlülüğü yüklemektedir[567]. İşveren işçilerin bu yükümlülüklerine uygun görevlerini ifa ettiklerini denetlemek için dijital izleme gerçekleştirme hakkına sahiptir[568].

b) Karayolu Trafik Kanunu ve Yönetmeliği

Karayolu yolcu ve yük taşımacılığı yapan işverenin dijital izleme uygulaması kullanmasının dayanaklarından birisi Karayolu Trafik Kanunu'dur (KTK). KTK m. 31 düzenlemesine göre: "kamyon, çekici ve otobüslerde ayrıca takograf, taksi otomobillerinde ise taksimetre" bulundurulması zorunludur. Karayolu Trafik Yönetmeliği'nin 98. maddesinde denetleme esaslarını da düzenlemiştir[569]. Madde kapsamında yük ve yolcu taşıması yapan belirli araçları işletenlerin, şoförlerin sürüş esnasındaki davranışlarını ve araç kullanma sürelerini denetleme yükümlülüğü bulunmaktadır[570]. Anılan maddede takograf ile izleme bir yükümlülük olarak düzenlenmiş ve bu kayıtların gerçekleştirilen denetimlerde sunulması esası benimsenmiştir.

İşverenler, KTK m. 31 düzenlemesinin öngördüğü yükümlülük kapsamında ve Yönetmeliğin 98. maddesine uygun olarak kamyon, çekici ve otobüs şoförlerini

567) Ömer Ekmekçi, "Türk Borçlar Kanunu Tasarısının Genel Hizmet Sözleşmesine İlişkin Hükümleri Üzerine", Mercek, Temmuz [2005], s. 1578; Okur, [2013], Elektronik Gözetleme, s. 34-35.
568) Okur, [2013], Elektronik Gözetleme, s. 35.
569) Karayolu Trafik Yönetmeliği Resmi Gazete'nin 18.07.1997 tarih ve 23053 sayılı mükerrer nüshasında yayımlanmıştır. Denetleme esaslarını da düzenleyen 98. Maddesinde ise 02.09.2004 tarih ve 25571 sayılı nüshasında yayımlanan değişiklikler gerçekleştirmiştir.
570) Okur, [2013], Elektronik Gözetleme, s. 37.

dijital izleme olanağı tanıyan takograf cihazı vasıtasıyla izleyebilir ve yol boyunca şoförlerin hızını, araç kullanım sürelerini, çalışma aralıklarını ve günlük zorunlu dinlenme uyup uymadıklarını denetleyebilir. Kamyon sürücülerinin bu verilerinin işlenmesine doğrudan yasa kaynaklık ettiğinden işveren ayrıca işçiden açık rıza almakla yükümlü değildir[571]. Öte yandan bir gerçek kişi olan kamyon sürücüsünün kişisel verileri işleneceğinden her durumda KVK hukukunun genel ilkelerine uygun bir dijital izleme uygulaması oluşturulması ve izlemenin boyutu ile ilgili şeffaflık sağlanarak sürücünün aydınlatma yükümlülüğü kapsamında bilgilendirilmesi gerekmektedir.

Bu noktada kısaca belirtmek gerekir ki, bir veri işlemenin yasal dayanağının bulunması bu hususu KVK hukuku dışına çıkarmaz, bu olsa olsa kişisel veri işlemenin bir hukuki sebebinin bulunduğunun, açık rıza alınmasına gerek olmadığının dayanağı olabilir. Bunun dışında yük ve yolcu taşıması yapan veri sorumlusu işverenler kanunda öngörülme veri işleme şartı kapsamında kişisel veri işlerken KVK hukukunun öngördüğü ilke ve yükümlülüklere uygun bir veri işleme süreci oluşturulmakla yükümlüdür. Bu kapsamda işlenen verinin korunması için teknik ve idari tedbirlerin alınması ve şeffaflık ilkesinin bir gereği olarak düzenlemelere uygun aydınlatma yükümlülüğünün yerine getirilmesi gerekir[572].

KTK hükümleri kapsamında işçinin dijital izleme uygulamaları ile izlenmesinde dikkat edilmesi gereken bir diğer husus kişinin/işçinin "araba sürüş biçiminin" davranışsal nitelikli biyometrik veri olduğudur[573]. Biyometrik veriler[574]

---

571) KVK Kurumu, Kişisel Verilerin İşlenme Şartları Rehberi, s. 2-3, https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari (Erişim Tarihi: 16.12.2022); KVK Kurumu, [2019], Uygulama Rehberi, s. 74.

572) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 97-99; KVK Kurumu, [2019], Uygulama Rehberi, s. 96.
https://kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF (Erişim Tarihi: 27.11.2023).

573) KVK Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, s. 5.

574) Bkz. § 6. II. 4. i.

KVKK m. 6/1'de özel nitelikli kişisel veri[575] olarak düzenlendiğinden işlenmesi ve korunması daha sıkı şekil şartlarına bağlıdır. Bu sebeple veri sorumlusu işveren KTK ve ilgili yönetmelik düzenlemelerine dayanarak dijital izleme uygulamalarıyla sürücüleri izlemesi halinde davranışsal biyometrik veri olan "araba sürüş biçimi" gibi özel nitelikli verilerin işlenmesi söz konusu olacaktır. Bu sebeple dijital izleme uygulamasıyla veri işleyen veri sorumlusu işverenlerin asgari olarak KVK Kurulu'nun 2018/10 sayılı Kararı'nda öngörülen düzenlemelere uygun bir veri işleme ve koruma süreci oluşturması zorunludur[576].

c) İnternet Kanunu'nun Bir Gereği Olarak İnternet Trafiğinin İzlenmesi

İşverenin dijital izleme uygulamaları kullanmasının yasal dayanaklarından birisi de 5651 sayılı Kanun'dur[577]. Bu kanunda öngörülen düzenlemeler kapsamında işverenler internet trafiğini izlemekle yükümlüdürler. İzlemeye ilişkin: "internet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesi" (5651 sayılı Kanun m. 2/-h bendi) biçimindeki tanımın yer aldığı 5651 sayılı Kanunda erişim, içerik, sosyal ağ ve toplu kullanım sağlayıcılarına internet kullanımına ilişkin belirli yükümlülükler öngörülmüş ve eşirim sağlayıcılarına internet trafik bilgilerini iki yıl süreyle saklama yükümlülüğü getirilmiştir. Ayrıca konusu suç teşkil eden içeriklerin kayıtlarının tutulması ve bu içeriklere erişimi engelleyici tedbirleri alma yükümlülüğü ticari amaçla olup olmadığına bakılmaksızın tüm toplu kullanıcı sağlayıcılarına bir yükümlülük olarak yüklenmiştir. Bu yükümlülüğün detayları da Kanun kapsamına çıkarılmış olan yönetmelikte[578] düzenlenmiştir.

---

575) Bkz. § 6. II. 2.
576) KVK Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, s. 14-15.
577) 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", Kabul Tarihi: 04.05.2007, 25.04.2007 tarih ve 26530 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.
578) İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, Resmî Gazete'nin 11.04.2017 tarih ve 30035 sayılı nüshasında yayımlanmıştır.

5651 sayılı Kanun'da iş ilişkisinde dijital izleme açısından önem arz eden husus, Kanun'un 2. maddesine dayanılarak düzenlenen Toplu Kullanım Sağlayıcılar Hakkında Yönetmelikte yer verilmiş olan toplu kullanım sağlayıcı tanımı kapsamında işverenin yasadan doğan internet trafiğini izleme yükümlülüğüdür. Toplu kullanım sağlayıcısı: "kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan gerçek ve tüzel kişileri" ifade etmektedir (Yönetmelik m. 3/1-g). Bu tanım kapsamında işçilerine internet ortamı kullanımı sağlayan işverenler toplu kullanım sağlayıcı olarak nitelendirilir[579]. Yönetmeliğin 4. maddesine göre toplu kullanım sağlayıcıları konusu suç olan içeriklere erişimi önleyecek tedbirleri almakla ve internet erişim bilgilerini iki yıl süre ile saklamakla yükümlüdürler (Yönetmelik m. 4/1-a ve b).

Ülkemizde 5651 sayılı Kanun'un bir gereği olarak internet trafik bilgilerinin (log kayıtları) işlenmesi ve bilişim suçlarını engellemek için ceza kanunları kapsamında dijital izleme gerçekleştirilmesi dayanağını yasadan alan dijital izleme biçimleridir. İşverenin bu tür dijital izleme uygulamaları kullanması işçilerin interneti veya diğer iletişim araçlarını özel amaçları için kullandıklarında elde edilen bilgilerin işçilerin aleyhine kullanılmasını gündeme getirmektedir. Örneğin bir işçinin sağlık sorunları bulunduğu gerekçesiyle iki günlük rapor alması, fakat aslında bu raporu arkadaşıyla tatile gitmek için kullandığının işveren tarafından e-posta, araç GPS veya telefon GSM verisi gibi bir dijital izleme uygulaması vasıtasıyla ya da işçinin sosyal medya hesaplarında gerçekleştirdiği paylaşımlarda[580] öğrendiğinde bu verinin işçi aleyhine kullanılması iş hukuku ve temel hak ve özgürlükler açısından çözülmesi gereken sorunlar ortaya çıkarmaktadır. Ayrıca kısaca belirtmek gerekir ki, bir hususun kanunda öngörülmesi bir veri işleme şartıdır (KVKK m. 5/2-a), fakat bu durum veri işlenmesi KVK hukukunun dışına çıkarmamaktadır. Bu sebeple 5651 sayılı Kanun hükümlerine uygun dijital izleme uygulaması kullanan veri sorumlusu işveren KVK

579) Yiğit, [2013], İşyerinde İnternet, s. 43.
580) AYM, Esin Ağar kararı, Başvuru Numarası: 2022/23522, Karar Tarihi: 15.11.2023, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2020/23522; Karar detayı için bkz. § 7. IV. III.

hukukunun ilkelerine uygun bir veri işleme faaliyeti yürütmekle yükümlüdür[581].

İnternet iletişiminin izlenmesinden kaynaklı ortaya çıkan sorunların işyerinde iletişim olanaklarının özel kullanımının yasaklanmasıyla kolayca çözülebileceği iddia edilmekle[582] birlikte internete erişim ve iletişim hakkının temel hak olarak kabul gördüğü günümüzde bunun işçilerin iletişim özgürlüğü üzerinde ölçüsüz bir müdahale ortaya çıkaracağı söylenebilir[583]. Bu hususların tartışmaya konu edildiği AİHM'in Copland & Birleşik Krallık[584] ve Bărbulescu & Romanya[585] kararlarında işçilerin iletişim hakkına ilişkin gerçekleştirilen tespitler bu açıdan özellikle önemlidir.

II. Dijital İzleme Uygulamalarının Sözleşmesel Dayanakları

İşverenin yönetim hakkı ile işçinin kişisel verileri üzerindeki hakları birbiriyle çatışan haklardır. İşveren iş sözleşmesinden doğan hakları kapsamında dijital izleme uygulamaları kullanırken işçinin kişilik haklarına ilişkin olan kişisel verileri üzerindeki haklarını gözeten bir dijital izleme faaliyeti gerçekleştirmekle yükümlüdür[586].

1. Yönetim Hakkının Bir Parçası Olarak Dijital İzleme

İş sözleşmesiyle iş ilişkisini tüm boyutlarıyla düzenlemeye olanak bulunmadığından işveren sözleşmeden doğan yönetim hakkı kapsamında işyerine

581) Detaylı bilgi için bkz. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği, m. 4-5; KVK Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, Nisan [2019], s. 6-7.
582) Erdem Özdemir, "İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkilerine Etkileri", Sicil İş Hukuku Dergisi, Haziran 2008, s. 21 ve 79. dipnotta atıf yapılan yazarlar.
583) EU, [2018], Handbook, s. 332.
584) AİHM, Copland v. Birleşik Krallık, Başvuru Numarası: 62617/00, 3 Nisan 2007.
585) AİHM, Bărbulescu v. Romanya, Başvuru Numarası: 61496/08, 5 Eylül 2017.
586) Sevgi Dursun Ateş, İşverenin Yönetim Hakkı, Seçkin Yayınları, Ankara, Mart, [2019], s. 463; Mustafa Alp, "Tele Çalışma (Uzaktan Çalışma)", (Ed: Süleyman Başterzi), Prof. Dr. Sarper. Süzek'e Armağan, Beta Yayıncılık, C. I, İstanbul, [2011], s. 830-831.

ilişkin belirli düzenlemeler yapabilir ve işçilere talimatlar verebilir. İşverenin yönetim hakkı işçinin yapmakla yükümlü olduğu işin kapsamını, tanımını, zamanını ve nerede yerine getirileceğini somutlaştırmaktadır[587].

a) Yönetim Hakkının Kaynağı ve Sınırları

İki tarafa borç yükleyen ve devamlı borç ilişkisi doğuran bir sözleşme olan iş sözleşmesi[588] kapsamında işverenin, işçinin iş görme borcunu sözleşmeye uygun ifasını bilmekte ve denetlemekte menfaati bulunmaktadır. Bu çerçevede işveren iş sözleşmesinden doğan yönetim hakkı kapsamında dijital izleme uygulamaları kullanabilir. İşverenin yönetim hakkı, iş sözleşmesinin ortaya çıkardığı ilişkinin karakteristik özelliği olan bağımlılığın işyerindeki görünümlerinden birisidir. Ülkemiz doktrininde işverenin yönetim (sevk ve idare) hakkının iş sözleşmesinden kaynaklandığı genel olarak kabul görmüştür[589]. İşçinin düzenlemelere ve talimatlara uyma borcunu düzenleyen TBK m. 399 ise yönetim hakkının kullanım şeklini somutlaştırmaktadır. Bununla birlikte işçinin iş görme borcunu iş sözleşmesinde, toplu iş sözleşmesinde veya işyerinin iş ilişkisine ilişkin diğer belgelerinde düzenlemek her zaman mümkün değildir. Bu gibi durumlarda iş sözleşmesinden doğan bir hak olan işverenin yönetim hakkı devreye girer ve işçinin iş görme borcunu somutlaştırır[590].

---

587) Taşkent, [1981], Yönetim Hakkı, s. 10-11; Süzek, [2019], İş Hukuku, s. 78-89; Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97; Ekonomi, [1987], Ferdi İş Hukuku, s. 32; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 256; Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 22; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 253; Alpagut, [2004], İş Sözleşmesinin Şartlarında Değişiklik, s. 54; Altıntepe, [2014], Yönetim Hakkı, s. 3; Başbuğ, [2008], Yönetim Hakkı, s. 3; Balkır, [2008], Yönetim Hakkının Etik Sınırları, s. 73; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 91; Şen, [2005], Çalışma Koşulları, s. 51; Süzek, [1998], Yönetim Hakkı, s. 225-226; Güzel, [2016], Yetki ve Özgürlük, s. 93-126.

588) Süzek, [2019], İş Hukuku, s. 232; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 125.

589) Alpagut, [2021], Dijitalleşen Çalışma s. 99; Süzek, [2019], İş Hukuku, s. 225 vd.; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 150 vd.; Süzek, [1998], Yönetim Hakkı, s. 225-226; Engin, [1993], İşveren, s. 70; Taşkent, [1981], Yönetim Hakkı, s. 10-11; Ekonomi, [1987], Ferdi İş Hukuku, s. 32; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 256.

590) Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97; Süzek, [2019], İş Hukuku, s. 78-89; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 199; Süzek, [1998], Yönetim Hakkı, s. 225-226; Engin, [1993], İşveren, s. 70; Taşkent, [1981], Yönetim Hakkı, s. 10-11; Ekonomi, [1987], Ferdi İş Hukuku, s. 32; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 256;

Bağımlılık unsurunun bir sonucu olarak işçi hem kişisel (hukuki) olarak hem de ekonomik yönden işverene bağımlı olduğundan eşit durumda değil, zayıf konumdadır. Yargıtay işçinin ekonomik bağımlılığının iş sözleşmesini, konusu iş görme olan diğer sözleşmelerden ayırt edici bir nitelik taşımadığını tespit etmektedir[591]. İş sözleşmesinde bulunan kişisel bağımlılık niteliğinden dolayı işçi ile işveren arasındaki güç ilişkisi hiyerarşik bir biçimde hukuki şekle bürünmektedir[592]. Bu sebeple yönetim hakkı iş hukukunun kaynakları arasında en alt sırada yer alır ve işverenin bu hakkı üstte yer alan iş hukuku kaynakları tarafından sınırlandırılır. Böylelikle anayasa, kanun, toplu iş sözleşmesi, bireysel iş sözleşmesi, genel iş koşulları ve işyeri uygulamaları gibi iş hukukunun kaynağı olan düzenlemelerde öngörülen normlara aykırı yönetim hakkı kullanımları işçi açısından bağlayıcı olmaz. Bu sınırlama aynı zamanda işçinin itaat borcunun da sınırını teşkil eder[593].

Yönetim hakkı sayesinde iş ilişkisinde işverenin işyerini düzenleme, denetleme ve talimatlar oluşturma hakkı bulunduğu kabul edilmektedir. Ayrıca bağımlılığın tespit edilmesinin ölçütü olan işin yapılma yeri, zamanı ve içeriğinin işverence belirlenmesi yönetim hakkının görünümleridir[594]. İş hukukunda

---

Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 22; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 253; Alpagut, [2004], İş Sözleşmesinin Şartlarında Değişiklik, s. 54 vd; Altıntepe, [2014], Yönetim Hakkı, s. 3; Başbuğ, [2008], Yönetim Hakkı, s. 3; Balkır, [2008], Yönetim Hakkının Etik Sınırları, s. 73; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 91; Şen, [2005], Çalışma Koşulları, s. 51-52; Güzel, [2016], Yetki ve Özgürlük, s. 93-126.

591) Yargıtay 22. Hukuk Dairesi, E. 2013/21270, K. 2014/32767, Karar Tarihi: 20.11.2014; Yargıtay 9. Hukuk Dairesi, E. 2015/1078, K. 2015/2742, Karar Tarihi: 29.01.2015; Yargıtay 9. Hukuk Dairesi, E. 2008/5973, K. 2009/24884, Karar Tarihi: 01.10.2009, Bu kararın incelemesi için bkz. Süleyman Başterzi, "İş İlişkisinin Kurulması, Hükümleri ve İşin Düzenlenmesi Açısından Yargıtay'ın 2009 Yılı Kararlarının Değerlendirilmesi", İş Hukuku ve Sosyal Güvenlik Hukuku Derneği (Türk Milli Komitesi), Yargıtay'ın İş Hukuku ve Sosyal Güvenlik Hukuku Kararlarının Değerlendirilmesi 2009, Kamu İş Yayını, Ankara, [2011], s. 3 vd.

592) Doğan Yenisey, [2007], İşyeri ve İşletme, s. 77.

593) Süzek, [2019], İş Hukuku, s. 80, 335; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 52; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 255; Ercan Akyiğit, İş Hukuku, 9. Baskı, Seçkin Yayıncılık, Ankara, [2013], s. 144, (Akyiğit, [2013], İş Hukuku); Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 124; Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97.

594) Alpagut, [2021], Dijitalleşen Çalışma, 100-101; Süzek, [2019], İş Hukuku, s. 80, 335; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 52; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 255; Akyiğit, [2013], İş Hukuku, s. 144; Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 124; Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97.

teknolojinin de etkisiyle yeni çalışma biçimleri olan tele çalışma, uzaktan çalışma, online çalışma gibi iş ilişkilerinin ortaya çıkması bağımlılığı işçinin işverenin iş organizasyonuna dahil olması ve onun menfaatine iş görmesi yoluyla tanımlanmasını gerektirmiştir[595].

İşçi, işverenin talimatlarına ve denetim menfaatine dürüstlük kuralları gerektirdiği ölçüde uymakla yükümlüdür. Dahası yönetim hakkı sadece fiili çalışma ilişkisine ilişkin hakları değil, aynı zamanda kimi işe alacağına veya kimi işten çıkaracağına ilişkin kararları, işyerine ilişkin talimatlar oluşturma, iş akışını düzenleme, işi denetleme, işyeri verimini artırmaya yönelik kararlar alma ve izleme gibi hakları da kapsar[596]. Bu aynı zamanda işverenin yönetim hakkı vasıtasıyla, özellikle işyerinin işleyişine ilişkin genel ve kalıcı kurallar oluşturma hakkına sahip olduğu anlamına gelmektedir[597].

İşverenin yönetim hakkının kaynağı; "mülkiyet hakkı[598]", "üretim araçlarını işletme hedefi kapsamında örgütleme", "işletme riskini taşıma" ve "iş ilişkisinin doğasında bir yönetim hakkının bulunduğu ve bu hakkı kullananın da işveren olması gerektiği" biçiminde görüşler kapsamında açıklanmıştır. Mülkiyet hakkı görüşü, iş ilişkisinin niteliğini mülkiyete indirdiğinden işveren için malikin hakları gibi bir sonuç ortaya çıkmaktadır. Ayrıca örneğin işçinin talimatlara uymaması mülkiyeti ihlal anlamına gelmez, fakat bu durum sözleşme ilişkisinin aykırılığıdır. Girişimcinin rizikoları taşıması yaklaşımı da işvereni girişimciye dönüştürdüğünden ve işçinin rizikolarını göz ardı ettiğinden yönetim hakkının kaynağını açıklamakta yetersizdir[599]. Bu itibarla doktrinde baskın görüş yönetim

595) Alpagut, [2021], Dijitalleşen Çalışma, 100-101.
596) Yargıtay 9. HD., E. 2007/27565 K. 2008/5286 T. 17.2.2008 tarihli kararında; "İşverenin yönetim hakkı kapsamında verdiği talimatlara işçi uymak zorundadır. İşçinin talimatlara uymaması, işverene duruma göre iş sözleşmesinin haklı ya da geçerli fesih hakkı verir." Biçiminde karar vermiştir. Aynı yönde: Yargıtay 9. HD., E. 2014/25004 K. 2014/40101 T. 25.12.2014; Yargıtay 22. HD., E. 2013/4347 K. 2013/4860 T. 8.3.2013; Yargıtay 22. HD., E. 2013/4343 K. 2013/4856 T. 8.3.2013; Yargıtay 9. HD., E. 2015/4786 K. 2015/12364 T. 30.3.2015.
597) Taşkent, [1981], Yönetim Hakkı, s. 9-11; Süzek, [2019], İş Hukuku, s. 79 vd.
598) Dursun Ateş, [2019], Yönetim Hakkı, s. 36-37.
599) Altıntepe, [2014], Yönetim Hakkı, s. 28 vd.

hakkının kaynağının iş sözleşmesi olduğu yönündedir[600].

Yönetim hakkına ilişkin olarak 6098 sayılı TBK'nın 399. maddesiyle yasal çerçevesi belirlenen düzenleme, aynı zamanda işverenin yönetim hakkının yasal dayanağını da oluşturmaktadır. TBK m. 399 hükmüne göre; işveren, işin görülmesi ve işçilerin işyerindeki davranışlarıyla ilgili genel düzenlemeler yapabilir ve işçilere özel talimat verebilir. İşçiler, işverenin düzenleme ve talimatlarına dürüstlük kurallarının gerektirdiği ölçüde uymakla yükümlüdür. Maddede belirtilen "genel düzenlemeler" işyerinde ilan edilmekle, başka bir söyleyişle işçi topluluğu açısından aleniyet kazanmakla; "özel talimatlar" ise işçiye bildirilmesiyle yürürlüğe girer[601].

İşverenin yönetim hakkının işin görülmesiyle ilgili olanları işin nerede, ne zaman, hangi sırayla ve hangi vasıtalarla yapılmasına ilişkinken; doğrudan işin yapılmasıyla ilgili olmayan, işçinin davranışlarıyla ilgili olan yönetim hakkı ise işyeri düzenini ve güvenliğini sağlamaya yöneliktir[602]. İşverenin işin görülmesi ve işçilerin işyerindeki davranışlarıyla ilgili yapacağı genel düzenlemeler veya vereceği özel talimatlara işçi uymakla yükümlüdür. İşverenin dijital izlemeye ilişkin uygulamaları kullanması da bu kapsamda değerlendirilmelidir. Örneğin işverenin işyerindeki internet trafiğini takip etmede olası siber sızmaların engellenmesi, ticari sırların ifşasının engellenmesi ve böylelikle şirketinin itibarının korunması gibi menfaatleri bulunmaktadır. Ayrıca işçinin özen ve sadakat borcu da işverene yönetim hakkını işyerinde ve işyeri dışında kullanmada haklı menfaatlerini koruma açısından dayanak işlevi görür[603]. Bu itibarla dijital izleme doğrudan işin yapılması, işyeri verimliliği, işyeri düzeninin ve güvenliğinin sağlanmasıyla ilgili

600) Süzek, [2019], İş Hukuku, s. 78; Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97; Dursun Ateş, [2019], Yönetim Hakkı, 41; Altıntepe, [2014], Yönetim Hakkı, 35 vd.; Hande Heper, İş İlişkisinde İşçinin İradesi; Doktora Tezi, İstanbul, Eylül, [2021], s. 350 vd.
601) Süzek, [2019], İş Hukuku, s. 80; Dursun Ateş, [2019], Yönetim Hakkı, 41; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 199.
602) Süzek, [2019], İş Hukuku, 79.
603) David Cabrelli/Rebecca Zahn, Theories of Domination and Labour Law: An Alternative Conception for Intervention? International Journal of Comparative Labour Law and Industrial Relations, Vol. 33, Issue 3, [2017], s. 345-346.

olduğundan yönetim hakkı kapsamında değerlendirilmelidir.

b) Yönetim Hakkı Kapsamında Dijital İzleme ve Denetim

Yönetim hakkı işverene dijital izleme gerçekleştirmek, elektronik iletişim araçlarının, sosyal medyanın ve diğer eşyaların hangi kapsamda ve hangi amaçla kullanılacağına ilişkin kurallar düzenleme hakkını vermektedir[604]. Belirtmek gerekir ki yönetim hakkı işverene işyeri sınırları dahilinde denetim, emir ve talimat verme hakkını tanımaktadır[605]. Gerçekte işyerinin devamlılığı, sermayenin doğru kanalize edilmesi ve belirli ekonomik hedeflere ulaşılabilmesi için yönetici bir iradenin varlığı gereklidir. Uzun bir süre işveren, işyerine ilişkin yönetimsel hakları kullanan, işin yürütümünü sağlayan, bunları gerçekleştirmek için kararlar alan ve uygulayan tek yetkili olduğu kabul görmüştür. Zira işletme rizikosunu taşıyan işverenin işyerinin verimini artırma, mali ve idari konularda prosedürler oluşturma; işçilere emir ve talimat verme, denetim gerçekleştirme hakları bulunduğu genel olarak kabul edilmiş ve bu konuda bir kavramlaşmaya uzun süre ihtiyaç duyulmamıştır. Sözleşme özgürlüğü ilkesinin de egemen olduğu bu dönmede işçi ile işverenin özgür iradeleriyle bir sözleşme içeriğini belirleyecekleri varsayılmıştır. Ne var ki, bağımlılık unsurunun ilişkisinin ayırt edici unsuru olduğu bir ilişkide görünürde sözleşme özgürlüğü bulunsa dahi işe ihtiyacı olan, ekonomik olarak dezavantajlı konumda bulunan ve güç asimetrisinin bulunduğu bir ilişkide sözleşme

604) Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97; Süzek, [2019], İş Hukuku, s. 78-89; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 199; Süzek, [1998], Yönetim Hakkı, s. 225-226; Engin, [1993], İşveren, s. 70; Taşkent, [1981], Yönetim Hakkı, s. 10-11; Ekonomi, [1987], Ferdi İş Hukuku, s. 32; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 256; Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 22; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 253; Alpagut, [2004], İş Sözleşmesinin Şartlarında Değişiklik, s. 54; Altıntepe, [2014], Yönetim Hakkı, s. 3; Başbuğ, [2008], Yönetim Hakkı, s. 3; Balkır, [2008], Yönetim Hakkının Etik Sınırları, s. 73; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 91 Şen, [2005], Çalışma Koşulları, s. 51; Güzel, [2016], Yetki ve Özgürlük, s. 93-126.

605) Ülkemiz doktrininde azınlıkta kalan bir görüşe göre işçilerin işyeri dışındaki davranışları işverenin menfaatlerini önemli ölçüde zedeleyici nitelikteyse ya da işyeri düzenini bozucu yansımaları oluyorsa işveren işçiye işyeri dışındayken de emir ve talimat verebilir. Doktrindeki baskın görüş ise işverenin işyeri sınırları içinde işçilere emir ve talimat verebileceğini aksi durumun yönetim hakkının amacına aykırı olacağını ileri sürmektedir. Detaylı bilgi için bkz. Doğan Yenisey, [2007], İşyeri ve İşletme, s. 98'de 115 ve 116 dipnotta atıf yapılan yazarlar.

özgürlüğünün varlığından bahsetmek güçtür[606].

İşverenin yönetim hakkı kapsamında işyeri güvenliğini ve düzenini sağlamak için bilişim sistemleri kullanması ve bu vasıtayla dijital izleme gerçekleşmesi makul karşılanmaktadır[607]. Bu aynı zamanda yönetim hakkının işverene tanıdığı iş görme ediminin şekli, yeri ve vasıtalarını belirleme hakkının bir görünümüdür[608]. İşveren yönetim hakkına dayanarak işçilerin bilişim teknolojilerini, interneti, e-posta hesaplarını, telefonu özel amaçlarla kullanılıp kullanamayacağına ve iş saatlerinde sosyal medya uygulamalarına girişleri sınırlandırmaya ilişkin personel yönetmelikleri oluşturabilir. Ayrıca işveren oluşturduğu talimatlara ve iş sözleşmesine uygun iş görme borcunun ifa edilip edilmediğini dijital izleme uygulamaları vasıtasıyla takip edebilir[609]. Bu denetim sonucunda ortaya çıkacak verinin hukuka uygunluğu dijital izlemenin boyutu ve içeriğine ilişkin işçilerin bilgilendirilmesi[610] ve kişisel verilerin işlenmesinin diğer hukuka uygunluk sebepleri yoksa[611] işçilerin açık rızasının alınmış olmasına

606) Süzek, [2019], İş Hukuku, s. 15 vd.; Doğan Yenisey, [2014], Emredici Yapı, s. 12-13; Sarper Süzek, "İş Hukukunda Yorum", İnan Kıraç'a Armağan, Galatasaray Üniversitesi, Ankara, 1994, s. 131; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 4; Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuk, s. 1 vd.; Kenan Tunçomağ/Tankut Centel, İş Hukukunun Esasları, Beta Yayınları, 9. Baskı, İstanbul, [2018], s. 14; Müjdat Şakar, İş Hukuku Uygulaması, Beta Yayınları, 11. Baskı, İstanbul, [2016], s. 5; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 36; Ali Güzel/Deniz Ugan Çatalkaya, "İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine", Prof. Dr. Ali Rıza Okur'a Armağan, İstanbul, [2014], s. 21; Erdem Özdemir, İş Hukukunda Mutlak Emredici Hükümlerin Yeri, AÜHFD, C. 54, S.3, Ankara, [2005], s. 95; Senyen Kaplan, [2018], Bireysel İş Hukuku, s. 3; Gaye Burcu Yıldız, "İş Hukukunun Etkinliği ve Amacı Üzerine Yeniden Düşünmek", Çalışma ve Toplum, [2018/2], s. 734.

607) Article 29 Working Party Working Document on Surveillance and Monitoring of Electronic Communications in the Workplace (Article 29 Data Prot. Working Party, Working Paper No. 55, Reference 5401/01, 2002), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (Erişim Tarihi: 02.10.2022); Determann/Sprague, [2011], Intrusive Monitoring, s. 1028.

608) Süzek, [2019], İş Hukuku, s. 78 vd.; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 199 vd.; Doğan Yenisey, [2007], İşyeri ve İşletme, s. 97; Süzek, [1998], Yönetim Hakkı, s. 225; Şükran Ertürk, İş İlişkisinde Temel Haklar, Seçkin Yayıncılık, Ankara, [2002], s. 94 vd.

609) Okur, [2013], Elektronik Gözetleme, s. 36.

610) Yargıtay 9. HD, E. 2009/447 - K. 2010/37516, T. 13.12.2010; Yargıtay 22. HD, E. 2016/6321 - K. 2016/13143, T. 3.5.2016; Yargıtay 22. HD. E. 2013/36288 –K. 2015/9548, T. 10.03.2015; Yargıtay 22. HD, E. 2011/16569 K. 2012/9111 T. 08.05.2012; Yargıtay 22. HD, E. 2017/21857 - K. 2019/9884, T. 07.05.2019.

611) KVKK m. 5/1'de veri işleme şartı ve m. 5/2'de ise açık rıza alınmaksızın kişisel veri işleme şartları düzenlenmiştir.

bağlıdır.

AYM işverenin işyeri verimini artırmak ve iş düzenini sağlamak amacıyla bilgi akışının denetimini sağlaması, işçilerin davranışlarından ve internet, e-posta kullanımlarından kaynaklı hukuki ve cezai sorumluluktan kendilerini korumak veya güvenlik endişelerini minimize etmek gibi meşru amaçlarla yönetim hakkı kapsamında kural olarak işçilerin kullanımına sunduğu bilişim sistemlerini denetleyebileceği ve dijital izleme uygulamaları kullanabileceğine karar vermektedir[612]. Dijital izlemenin ve denetimin hukuka uygun olması için işçinin gerçekleştirilecek izleme ve sınırlandırmalarla ilgili olarak önceden bilgilendirilmiş olması gereklidir. Ayrıca işverenin ticari gerekliliklerine uygun hazırlanmış kapsamı belirli olan işyeri yönetmelikleri, işyeri çalışma kuralları, bilişim teknolojilerini, araç ve gereçlerini kullanma prosedürlerinin işçiler açısından bağlayıcı olması için bunların tebliği ve duyurulması gerekmektedir[613].

Yargıtay, işverenin gerçekleştirdiği dijital izlemelerin ihtilafa yansıdığı kararlarında, işverenin mülkiyeti kendisine ait olan bilgisayar ve e-posta adresleri ile bu adreslere gelen e-postaları her zaman denetleme hakkına sahip olduğu yönünde kararlar vermiştir. Bu kararlarda yazışmaların kişinin özel hayatı olduğu

612) AYM, Genel Kurul Kararı, E.Ü. Başvurusu, Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020, § 69.

613) AYM, E.Ü. kararı Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020; Aynı doğrultuda AYM, Ömür Kara ve Onursal Özbek kararı § 50; AYM, Fırat Gerçek kararı, Başvuru Numarası: 2019/25604, Karar Tarihi: 21.09.2022; AYM Fırat Gerçek kararında işçinin izlemeye ilişkin önceden bilgilendirilmesi gerektiğini şu şekilde karara yansıtmıştır: "Demokratik bir toplumda iletişimin denetlenmesi ve kişisel verilerin işlenmesi süreci şeffaf bir şekilde gerçekleştirilmeli ve bunun bir gereği olarak da süreçle ilgili olarak çalışanlar işveren tarafından önceden bilgilendirilmelidir. Uluslararası hukuk ve karşılaştırmalı hukuk dikkate alındığında bu bilgilendirmenin -somut olayın özelliklerine uygun düştüğü ölçüde- en azından iletişimin denetlenmesi ile kişisel verilerin işlenmesinin hukuki dayanağı ve amaçları, denetlemenin ve veri işlemenin kapsamı, verilerin saklanacağı süre, veri sahibinin hakları, denetlemenin ve işlemenin sonuçları ile verilerin muhtemel yararlanıcıları hususlarını kapsaması gerekir. Ayrıca bildirimde iletişim araçlarının kullanımına ilişkin olarak işveren tarafından öngörülen sınırlamalara da yer verilmelidir. Bilgilendirmenin mutlaka belli şekilde yapılması şart olmayıp şeffaflığı sağlamak bakımından bireylere kişisel verilerin işlenmesine ve iletişimin denetlenmesine ilişkin süreçten yukarıda belirtilen kapsamda haberdar olma imkânı sağlayan uygun bir yöntem tercih edilebilir." https://www.resmigazete.gov.tr/eskiler/2022/11/20221115-5.pdf) §24/ii; Yargıtay kararlarında da bu yöndedir. Bkz. Yargıtay 22. Hukuk Dairesi, E. 2017/21857 K. 2019/9884 T. 7.5.2019 kararı.

yönündeki savunmalara itibar edilmemiştir. Ayrıca Yargıtay, işverenin bilgisayar verilerine delil olarak dayanmasında da herhangi bir hukuka aykırılık bulmamıştır[614]. Bir diğer kararda işçinin iş görme borcunun ifası için kendisine tahsis edilen bilgisayarda mesai saatleri içinde oyun, arkadaşlık ve erotizm içeren internet sitelerine girmesinin işyerinde olumsuzluğa yol açacağını ve bu durumda iş ilişkisinin devamının işverenden beklenemeyeceğine hükmetmiştir[615]. Yargıtay bir başka kararında dijital izleme yapmanın koşulunu belirtmiş ve bunun ancak işçiye bildirmekle mümkün olduğuna karar vermiştir[616].

2. Gözetme Borcunun Bir Gereği Olarak Dijital İzleme

Geniş kapsamlı bir işveren borcu olan gözetme borcunun kapsamı işverenin işçinin kişiliğini, sağlığını korumakla ve onun tehlikelerden uzak durmasını sağlamakla sınırlı olmayıp, işçinin kişisel verilerinin gizliliğinin korunmasını, bilgilendirilmesini ve işçinin işyerine getirdiği araç ve eşyanın korunmasını da kapsadığı kabul edilmektedir[617]. Borcun kapsamına işçi ve işyeri güvenliği için gerekli idari ve teknik tüm tedbirleri alma yükümlülüğü de girdiğinden işverenin bu amaçla gerçekleştirdiği dijital izleme uygulamaları işverenin gözetme borcu

614) Yargıtay 9. HD, E. 2009/447 - K. 2010/37516, T. 13.12.2010; Yargıtay 22. HD, E. 2016/6321 - K. 2016/13143, T. 3.5.2016; Yargıtay 22. HD. E. 2013/36288 –K. 2015/9548, T. 10.03.2015.
615) Yargıtay 22. HD, E. 2011/16569 K. 2012/9111 T. 08.05.2012.
616) Yargıtay 22. HD, E. 2017/21857 - K. 2019/9884, T. 07.05.2019. Bu karar dijital izleme açısından önemlidir. Zira işveren "klavye yakalayıcısı" niteliğinde bir dijital izleme aygıtı kullanmıştır.
617) Süzek, [2019], İş Hukuku, s. 386; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 321; Ekonomi, [1987], Ferdi İş Hukuku, s. 154; İlhan Ulusan, Özellikle Borçlar Hukuku ve İş Hukuku Açısından İşverenin İşçiyi Gözetme Borcu, Kazancı Hukuk Yayınları, İstanbul, [1990], s. 1, (Ulusan, [1990], İşçiyi Gözetme Borcu); Fevzi Demir, En Son Yargıtay Kararları Işığında İş Hukuku ve Uygulaması, Albi Yayıncılık, 11. Baskı, [2018], s. 212, (Demir, [2018], İş Hukuku ve Uygulaması); Tunçomağ/Centel, [2018], İş Hukukunun Esasları, s. 135; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 182; Haluk Hadi Sümer, İş Hukuku, Seçkin Yayıncılık, 25. Baskı, Ankara, [2020], s. 89; Akyiğit, [2013], İş Hukuku, 207; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 290 vd.; Kübra Doğan Yenisey, "Türk Borçlar Kanunu'nun Genel Hizmet Sözleşmesine İlişin Hükümleri ve İş Hukuku Açısından Önemi", İş Hukuku ve Sosyal Güvenlik Hukuku Akademik Forumu, Legal Yayıncılık, [2014], s. 93; Tankut Centel, "Türk Borçlar Kanunu'nda Genel Olarak İşçinin Kişiliğinin Korunması", Sicil İş Hukuku Dergisi, S. 24, [2011], s. 14.

kapsamında değerlendirilmelidir[618].

a) Genel Olarak İşverenin Gözetme Borcu

İş ilişkisinde işçinin kişiliğinin korunması onun kişiliğiyle sıkı sıkıya bağlı, devredilemez, dokunulamaz, vazgeçilemez temel hak ve özgürlükleriyle ilgilidir. Bu kapsamda işveren, işçinin kişilik değerleri olan maddi ve manevi varlığını koruma, bunları geliştirmesi için uygun çalışma ortamı oluşturma; işçinin şeref ve

618) Yargıtay'a göre; işveren, işyerinde olumlu çalışma koşullarını oluşturmakla yükümlüdür. Aynı zamanda; "işverenin işçiyi gözetme borcu, işçinin sadakat borcunun karşılığını oluşturur. İş sözleşmesinin işçi ile işveren arasında kişisel ilişki kuran niteliği, işçi yönünden işverenin işi ve işyeri ile ilgili çıkarlarını korumak, bu çıkarlara zarar verebilecek her türlü davranıştan kaçınmak; buna karşılık işveren açısından işçiyi korumak ve gözetmek biçimde kendini gösterir. İşveren gözetme borcu gereği işçinin kişiliğini korumak, onun kişilik haklarına saygı göstermek zorundadır. İşçinin kişiliğinin korunması, onun yaşamının sağlığının, bedensel ve ruhsal bütünlüğünün, şeref ve haysiyetinin, kişisel ve mesleki saygınlığının, özel yaşam alanının, ahlaki değerlerinin, genel olarak özgürlüğünün ve bu arada düşünce özgürlüğü ve sendikal örgütlenme özgürlüğünün korunmasını içerir." Yargıtay 22. HD., E. 2012/11485 K. 2013/1396 T. 31.1.2013; Yargıtay HGK., E. 2015/1890 K. 2017/383 T. 1.3.2017; Yargıtay HGK., E. 2015/3171 K. 2018/1143 T. 30.5.2018; Yargıtay 22. HD., E. 2017/29185 K. 2020/5817 T. 4.6.2020; "İşverenin gözetme ve koruma borcunu hiç veya gereği gibi ifa etmemesi halinde, isçi maruz kaldığı zarar durumuna göre, maddi ve manevi tazminat taleplerinde bulunabilir. Ayrıca bu borcun yerine getirilmemesi, işverenin kendisine düşen ifa hazırlıklarını yapmamış olması nedeniyle onun alacaklının temerrüdü durumuna düşmesine yol açabilir." Yargıtay 9. HD., E. 2009/42452 K. 2012/3132 T. 13.2.2012. "Bundan başka işveren, mevzuatta öngörülmemiş olsa dahi bilimsel ve teknolojik gelişmelerin gerekli kıldığı iş sağlığı ve güvenliği önlemlerini almak zorundadır. Bilim, teknik ve örgütlenme düşüncesi yönünden alınabilme olanağı bulunan, yapılacak gider ve emek ne olursa olsun bilimin, tekniğin ve örgütlenme düşüncesinin en yeni verileri göz önünde tutulduğunda işçi sakatlanmayacak, hastalanmayacak ve ölmeyecek ya da bu kötü sonuçlar daha da azalacaksa her önlem işverenin koruma önlemi alma borcu içine girer. Bu önlemler konusunda işveren iş yerini yeni açması nedeniyle tecrübesizliğini, bilimsel ve teknik gelişmeler yönünden bilgisizliğini, ekonomik durumunun zayıflığını, benzer iş yerlerinde bu iş güvenliği önlemlerinin alınmadığını savunarak sorumluluktan kurtulamaz. Gerçekten, çalışma hayatında süregelen kötü alışkanlık ve geleneklerin varlığı işverenin önlem alma borcunu etkilemez. İşverenlerce, iş güvenliği açısından yaşamsal önem taşıyan araç ve gereçlerin işçiler tarafından kullanılması sağlandığında, kaza olasılığının tamamen ortadan kalkabileceği de tartışmasız bir gerçektir. Nitekim, günümüzde gelişen sanayi ve teknoloji karşısında yukarıda açıklanan hükümler yeterli görülmemiş, insan yaşamının kutsallığı çerçevesinde işverenin, iş yerinde işçilerin sağlığını ve iş güvenliğini sağlamak için gerekli olanı yapmak ve bu hususta şartları sağlamak ve araçları noksansız bulundurmakla yükümlü olduğu 4857 sayılı İş Kanununun 77. maddesinin açık buyruğu iken, İş Kanununun 77. ve devamı bir kısım maddeler 30/06/2012 tarih ve 28339 sayılı Resmi Gazetede yayımlanan 6331 sayılı İş Sağlığı ve Güvenliği Kanununun 37. maddesiyle yürürlükten kaldırılmış olup, 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, işverenin sağlık ve güvenlik önlemlerini alma yükümlülüğünü daha ayrıntılı bir biçimde düzenlemiştir." Yargıtay 10. HD., E. 2020/7072 K. 2020/7833 T. 29.12.2020.

onurunu, özel hayat alanını ve kişisel verilerini koruma yükümlülüğü altındadır[619].

Gözetme (koruma) borcu aynı zamanda işçide, işverenin bu borcuna uygun davranmasını isteme hakkını ortaya çıkarmaktadır[620]. Gözetme borcu, işçinin sadakat borcunun karşılığını oluşturduğundan işverenin de işçilerinden sadakat borcuna uygun davranmalarını bekleme hakkı bulunmaktadır[621]. Eklemek gerekir ki, iş sözleşmesinde doğan borç ilişkisinde sadece dar anlamda ücret ve bağımlı iş görme borçları doğmaz. Bu borçların yanında iş sözleşmesinin ortaya çıkardığı hukuki ilişki sonucu sosyal temasla başlayan edimden bağımsız bazı koruma, zarar vermeme yükümlülükleri de ortaya çıkmaktadır. Böylelikle işçinin kişilik haklarının, bedensel ve ruhsal bütünlüğü değerlerinin korunması bir işveren yükümlülüğü halini almaktadır[622].

Gözetme borcu kapsamında işverenin, işçilerin kişiliğini koruyan, onların tacize ve psikolojik baskıya uğramalarını engelleyen bir çalışma düzeni oluşturma; işçinin ruhsal ve bedensel bütünlüğünü koruyacak her türlü önlemi alma yükümlülüğü bulunmaktadır[623]. TBK m. 417/1'de işverenin işçileri koruma borcu geniş anlamda düzenlenmiş (TBK m. 417/1), ikinci fıkrada ise işçinin sağlığını ve bedensel bütünlüğünü koruyan ve bu hususta işverene her türlü önlemi alma yükümlülüğü yükleyen dar anlamda koruma borcu (TBK m. 417/2)

---

619) Süzek, [2019], İş Hukuku, s. 386-387; Ugan Çatalkaya, [2016], Ulaşılabilir Olmama, s. 736; Sevimli, [2006], Özel Yaşam, s. 54 vd.

620) Ülkemiz doktrini işverenin "işçiyi gözetme borcunu kimi zaman "gözetme" yerine "koruma" sözcüğünü kullanarak, kimi zaman "gözetme (koruma)" biçiminde ifade edildiği, bazı eserlerde "gözetim borcu", bazılarında ise "iş güvenliğini sağlama borcu" kavramlarının kullanıldığı görülmektedir. Emine Tuncay Senyen Kaplan, "İşverenin Koruma ve Gözetme Borcunun Kapsamı", Kamu-İş Dergisi, C: 7, S. 2, [2003], s. 2 vd.; Okur, [2013], Elektronik Gözetleme, s. 67; Fuat Bayram, Borçlar Kanunu Tasarısı Işığında İşverenin İşçinin Kişiliğini Koruma Borcu, İş Hukuku ve Sosyal Güvenlik Komitesi, 30. Yıl Armağanı, Ankara, [2016], s.11; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 321; Tunçomağ/Centel, [2018], İş Hukukunun Esasları, s. 134; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 185; Süzek, [2019], İş Hukuku, s. 386; Aydın, [2022], Kişilik Hakları, s. 129; Sevimli, [2006], Özel Yaşam, s. 59.

621) Süzek, [2019], İş Hukuku, s. 386.

622) Başbuğ, [2008], Yönetim Hakkı, s. 3-4.

623) Süzek, [2019], İş Hukuku, s. 386; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 281; Gaye Baycık, İş ve Sosyal Güvenlik Hukuku Açısından Maden İşçileri, Yetkin Yayınları, [2006], s. 103.

düzenlenmiştir[624]. Birinci fıkrada işçinin kişilik haklarının korunmasının kapsamına, kişilik değerlerine dahil olan özel hayatın gizliliği, kişisel verilerin korunması gibi tüm hakların korunmasını gerekli kılar. Ayrıca işçinin korunmasından sadece beden bütünlüğü düşünülmemeli, işçinin ruhsal bütünlüğünü oluşturan değerlerin korunması için de gerekli tüm tedbirler alınmalıdır[625].

İşverenin gözetme borcunun gereği olarak alması gerekli önlemler çerçevesinde dijital izleme uygulamalarına başvurabilir. Örneğin işçinin güvenliğinin sağlanması için fabrika etrafında kamera izlenmesi gerçekleştirmesi bu kapsamda değerlendirilir. TBK m. 417 hükmünde sadece işçinin maddi kişilik değerlerini korumakla yetinilmemiş, aynı zamanda işçinin kişiliğinin korunması için gerekli her türlü önlemi alma yükümlülüğü de işverene yüklenmiştir[626]. Yargıtay da çeşitli kararlarında işverenin "gözetme ve koruma borcunun kapsamında isçilerin maddi ve manevi vücut bütünlüğünün, şeref, haysiyet ve özel yasam gibi kişisel değerlerinin korunması" bulunduğuna karar vermektedir[627].

Gözetme borcu işverene işçinin korunması için her türlü teknolojik tedbiri alma yükümlülüğü yüklerken, gerçekleştirilecek izleme uygulamasının da işçinin kişilik değerleri üzerinde müdahaleci etkiler oluşturmaması yükümlülüğü yüklemektedir[628]. Örneğin işverenin işyerine giriş ve çıkışta işçilerin güvenliğini giriş kartı sağlaması ve denetlemesi mümkünken iris taraması veya yüz tanıma sistemleriyle işyerine girişi zorunlu tutması kişilik hakkı üzerinde orantısız bir

---

624) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 281.
625) İstanbul BAM, 29. HD., E. 2018/2860 K. 2019/1534 T. 9.5.2019 tarihli kararında: İşverenin işçiyi gözetme borcunun, işçinin kişiliğinin, özel yaşamının, sağlığının, bedensel ve ruhsal bütünlüğünün, ahlaki değerlerinin korunmasını da içerdiği dikkate alındığında davacıya oğlunun sünnet düğünü için izin verilmemesi işçiyi gözetme borcuna aykırıdır. Belirtilen nedenle davacının düğün merasimi nedeniyle devamsızlığı haklı nedene dayanmaktadır.
626) Okur, [2013], Elektronik Gözetleme, s. 34; Bayram, [2016], İşçinin Kişiliği, s.11 vd.; Ekmekçi, [2005], Genel Hizmet Sözleşmesi, s. 157.
627) Yargıtay 9. HD., E. 2010/15688 K. 2010/38732 T. 20.12.2010; Yargıtay 9. HD., E. 2009/42452 K. 2012/3132 T. 13.2.2012; İstanbul BAM, 24. HD., E. 2018/1812 K. 2020/209 T. 13.2.2020.
628) Süzek, [2019], İş Hukuku, s. 386-387; Sevimli, [2013], İşçinin Kişiliğinin Korunması, s. 110.

müdahaledir[629]. Öte yandan örneğin çok tehlikeli sınıfta faaliyet gösteren bir yeraltı maden işinde işçileri giyilebilir çipli takip sistemi ile izlemek her türlü teknolojik tedbiri alma yükümlülüğü kapsamında değerlendirileceğinden, gerçekleştirilen dijital izlemenin dayanağı gözetme borcu olacaktır[630].

Öte yandan güvenliği sağlamak ve tehlikeleri önlemek gibi meşru amaçlar kapsamında gerçekleştirilen dijital izleme örneğin işçinin raporlu olduğu bir tarihte aslında tatile gittiğini veya mesaisinin çoğunluğunu sosyal medyada ve alışveriş sitelerinde gezinerek tamamladığı gibi verileri ortaya çıkarabilir[631]. İş hukuku açısından bu verilerin iş sözleşmesi üzerinde etkileri olacağını kabul edilmekle birlikte kişisel verilerin korunması mevzuatı açısından işçinin bilgilendirilmeden bu tür verilerinin işlenmemesi esastır. İlgili başlıkta detaylı incelendiği üzere[632], hukuka uygun gerçekleştirilmeyen dijital izlemenin sonucunda elde edilen verilerin işçinin aleyhine kullanılması mümkün olmayabilecektir[633].

b) İşverenin İş Sağlığı ve Güvenliği Yükümlülükleri

Anayasamızda çalışma hakkı ve çalışanların hayat seviyesini yükseltmeye ilişkin tedbirler[634] m. 48 ve 49'da kimsenin yaşına, cinsiyetine ve gücüne uymayan işlerde çalıştırılamayacağı m. 50'de ve sağlıklı, dengeli bir çevrede yaşama m. 56'da düzenlenmiş olup, bu düzenlemeler işçinin kişiliğini koruma, sağlık ve

629) Bkz. İşverenin parmak izi kayıt sistemi ile işyerine giriş ve çıkışı zorunlu tutulduğu bir işyerine ilişkin olarak, Anayasa Mahkemesi Genel Kurulu 10/3/2022 tarihli Ramazan Şahin (Başvuru Numarası: 2018/11988) kararında, Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar vermiştir.
630) Miller/Weckert, [2000], Privacy, the Workplace, s. 259.
631) Robert Sprague, Survey of (Mostly Outdated and Often Ineffective) Laws Affecting Work-Related Monitoring, Chicago-Kent Law Review, Vol. 93, Issue. 1, [2018], s. 224.
632) Bkz. § 8. I.
633) Yargıtay 22. HD, E. 2017/21857 - K. 2019/9884, T. 07.05.2019.
634) Süzek, [2019], İş Hukuku, s. 387-388; Sarper Süzek, İş Güveliği Hukuku, Ankara, [1985], s. 71; Z. Gönül Balkır, "İş Sağlığı ve Güvenliği Hakkının Korunması: İşverenin İş Sağlığı ve Güvenliği Organizasyonu", Sosyal Güvenlik Dergisi, C. 2, S. 1, Ocak, [2012], s. 15.

güvenliklerini sağlamaya ilişkin anayasal haklara örnektir[635]. Anayasa Mahkemesi iş güvenliği ile ilgili verdiği bir kararda, iş güvenliğini: "işyerinde çalışanların işin yapılmasıyla ilgili olarak ortaya çıkan tehlikelerden bedensel ve ruhsal olarak zarar görmemeleri için alınması gerekli ruhsal, teknik ve tıbbi önlemleri almaya yönelik sistemli çalışmalar" biçiminde açıklamıştır[636].

Çalışanların iş sağlığı ve güvenliğini sağlamak için önleme ve koruma amaçlı düzenlemeler kapsamında hazırlanmış olan 6331 sayılı İSGK, işverenlere çalışanların beden ve ruhsal sağlıklarını korumak için risk analizi yapma ve teknolojinin veya durumun gerektirdiği her türlü iş sağlığı ve güvenliği tedbirini alma borcu yüklemektedir[637]. Örneğin işyeri güvenliğini sağlamak ve çalışanların sağlığını korumak işverenin yasal yükümlülüğü olduğundan bu yükümlülük kapsamında işyeri etrafında ve girişlerde kamera gözetlemesi gerçekleştirmesi, tehlikeli inşaat sahasında konum bazlı sistemlerle dijital izleme uygulaması kullanılması, tehlikeli madde taşımacılığı yapan araçlarda GPS ile hız ve konum takibi yapılması, sürüş güvenliği ve kaza riskini önlemeye yönelik sürüş esnasında yolu izleyen sistemlerin kullanılması İSG yükümlülükleri kapsamında dijital izlemenin hukuka uygunluk sebebi olarak değerlendirilebilir[638]. Dahası işverenin teknik ve idari tüm tedbirleri alması yeterli olmayıp işçilerin alınan kişisel koruyucu tedbirleri uyguladıkları ve donatımları kullandıklarını da işveren denetlemekle yükümlüdür[639]. İşverenin bu denetimi dijital izleme ile yerine getirmesi mümkündür.

---

635) İbrahim Ö. Kaboğlu, Anayasa'da Sosyal Haklar: Alanı ve Sınırları, (Ed. İbrahim Ö. Kaboğlu), Legal Yayıncılık, [2012], s. 18.
636) AYM, E. 1988/51, K. 1989/18, T. 02.05.1989. Resmi Gazete, 04.01.1990 – 20392 sayı; Kaboğlu, [1996], Özgürlükler Hukuku, s. 19-20.
637) Gülsevil Alpagut, "İş Sağlığı ve Güvenliği Yasa Tasarısında İşverenlerin Yükümlülükleri ve Risk Değerlendirmesi", İşveren Dergisi, C. 50, S. 3, Ankara, Mayıs-Haziran [2012], s. 100-103; Süzek, [2019], İş Hukuku, s. 386; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 394.
638) Eric A. Szweda, "Applying the Personal Data (Privacy) Ordinance to Employee Monitoring", Hong Kong Law Journal, Vol. 43, No. 3, [2013], s. 953.
639) Seda Arslan, "İş Sağlığı ve Güvenliği Kanunu'na Göre İşverenin Genel Yükümlülükleri", Prof. Dr. Ali Rıza Okur'a Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 20, S. 1, [2014], s. 794.

İşverenin bu yükümlülükler kapsamında dijital izleme uygulaması kullanmasının dayanağı, İSGK m. 4'teki "her türlü tedbirin alınması" ifadesiyle somutlaşmaktadır. Zira bu düzenleme ve devamı düzenlemeler işverene işçinin beden ve ruhsal bütünlüğünü korumak için her türlü teknik ve idari tedbir alma, gerekli eğitimleri verme gibi mevzuatta öngörülen tedbirlerin yanında bilimsel ve tekniğin ortaya çıkaracağı işçinin sağlığını ve güvenliğini sağlayacak gelişmeleri takip etme ve uygulama yükümlülüğü de yüklemektedir[640].

İSGK kapsamında işverenlerin mesleki riskleri önleme, işle ilgili risk analizlerini yapma, risklerin önlenmesi için gerekli her türlü teknik ve idari tedbiri alma, gerekli araç ve gereçleri işçilere sağlama yükümlülükleri de bulunmaktadır[641]. Örneğin işverenin uzaktan çalışan işçilerin sağlık gözetimini gerçekleştirmek, kanunda öngörülen yükümlülüklerini yerine getirmek için işçinin klavye ve bilgisayarda aktif olduğu süreleri dikkate alan ve uzun süreli bilgisayar kullanımında uyarı veren, hareket etmesi gerektiğine ilişkin pop-up mesajları ekrana çıkaran bir dijital izleme uygulaması kullanabilir[642]. Bu örneğe uygun sağlık gözetimi denetimlerinde dijital izlemenin dayanağını İSG gereklilikleri oluşturmaktadır.

İSGK yükümlülükleri kapsamında gerçekleştirilen dijital gerçek zamanlı izleme tehlikeli işlerde veya acil durumlarda işçileri risklerden uzak tutabilir ve güvenliklerini sağlayabilir. Özellikle yeraltı maden işleri gibi bazı sektörlerde mevzuatın bir gereği olarak dijital izleme uygulaması kullanmak bir zorunluluktur. Bundan dolayı işverenlerin değinilen emredici düzenlemeler kapsamında gerekli

---

640) Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 369; Süzek, [2019], İş Hukuku, s. 397, 871-872; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 267; Senyen Kaplan, [2003], Koruma ve Gözetme, s. 436; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 92; Narter, [2014], İş Kazası ve Meslek Hastalığı, s. 55.

641) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 392; Gaye Baycık, "Çalışanların İş Sağlığı ve Güvenliğine İlişkin Haklarında Yeni Düzenlemeler", Ankara Barosu Dergisi, [2013/3], s. 111; Mahmut Kabakcı, "6331 Sayılı Kanun'un İş Sağlığı ve Güvenliği Anlayışı ve Risklerden Korunma İlklerinin (m.5) İşlevi", Sicil İş Hukuku Dergisi, S. 29, [2013], s. 68 vd.

642) Özdemir, [2020], İş Sağlığı, s. 68 vd; Baycık/Doğan/Dulay Yangın/Yay, [2021], Pandemide Uzaktan Çalışma, s. 1714.

uygulamaları kullanmaları gerekmektedir.

Dijital izleme tehlikeli sınıfta faaliyette bulunan veya önemli ticari ve sistemsel verileri işleyen bazı işyerleri için çeşitli kanunlar kapsamında işverene yüklenmiş emredici bir yükümlülük olduğundan, bu aynı zamanda yönetim hakkını sınırlandırmaktadır. Zira işverenler mesleki risklerin önlenmesi ve iş güvenliğinin sağlanması, risk ve kaza faktörlerinin ortadan kaldırılması için gerekli her türlü önlemi almakla yükümlüdürler[643]. İşverenin güvenli çalışma ortamı sağlama yükümlülüğü, işyerini işçiler için tehlikesiz şekilde tutma, işçilerin sağlık ve beden bütünlüğünü koruma, risk analizleri yapma, işçilere tehlikeler ve iş sağlığı ve güvenliği hususlarında bilgi verme[644] ve risklerin önlenmesi için her türlü teknik ve idari tedbiri alma gibi yükümleri içermektedir. Bu sebeple işverenin işçiyi koruma borcu geniş kapsamlı bir borç olup, kapsamına neyin girdiğini sınırlı bir şekilde tespit etme olanağı bulunmamaktadır[645]. Ayrıca işverenin gözetme borcu sadece işçinin beden bütünlüğünü ve sağlığını koruma kapsamında düşünülmemeli, bu borcun aynı zamanda işçinin bilgilendirilmesi (İSGK m. 16), kişiliğinin, çıkarlarının, özel hayatının ve kişisel verilerinin korunmasını da kapsamaktadır[646].

İşverenlerin, çalışanların iş sağlığı ve güvenliği için alması gereken tedbirler bilim, teknik ve tecrübelere ilişkin değerlendirmenin yapıldığı tarihteki ulaştığı düzeye göre belirlenmektedir[647]. Dahası işverenin sadece bu tedbirleri alması yeterli olmayıp, işçilerin bunları uyguladığını ve iş sağlığı ve güvenliği kapsamında alınmış önlemlere uyduğunu da denetleme yükümlülüğü bulunmaktadır. Bu

643) AB'nin 89/391/ECC sayılı Direktifinde de işverenin bu yükümlülüğü düzenlenmiştir. European Union: Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC)
644) Gülevil Alpagut, "6331 Sayılı İş Sağlığı ve Güvenliği Kanununun Genel Esasları", İÜHFM, C.LXXII, S. 2, [2014], s. 31, ; Caniklioğlu, [2012], İşveren Yükümlülükleri, s. 30.
645) Süzek, [2019], İş Hukuku, s. 386.
646) Sevimli, [2013], İşçinin Kişiliğinin Korunması, s. 110; Süzek, [2019], İş Hukuku, s. 386 vd.; Kadriye Bakırcı, İş Hukuku Açısından İşyerinde Cinsel Taciz, İstanbul, Yasa Yayıncılık, [2000], s. 155.
647) Nurşen Caniklioğlu, 6331 Sayılı İş Sağlığı ve Güvenliği Kanununda Öngörülen İşveren Yükümlülükleri, Türkiye Toprak, Seramik, Çimento ve Cam Sanayii İşverenleri Sendikası Çalışma Mevzuatı Seminer Notları, Antalya, 26-30 Eylül [2012], s. 36; Süzek, [2019], İş Hukuku, s. 398.

denetleme yükümlülüğü dijital izlemenin de dayanağını oluşturur.

İSG yükümlülüğü kapsamında dijital izleme uygulamaları kullanarak madende çalışan işçileri anlık takip etmek ve maden girişlerinde riskleri engelleyen kamera izlemeleri gerçekleştirmek maden işyerleri için hayati önemdedir. Bu sebeple Maden İşlerinde İş Sağlığı ve Güvenliği Yönetmeliği'nin Ek-1'inde yer alan "Sondajla Maden Çıkarılan İşlerin Yapıldığı İşyerleri ile Yeraltı ve Yerüstü Maden İşlerinin Yapıldığı İşyerlerinde Uygulanacak Asgari Genel Hükümler" belirlenmiştir. Buna göre bu işyerlerinde işverenler işçilerin giriş-çıkışlarını her an yer üstünde anlık takip edecek bir dijital izleme sistemi kurmakla yükümlüdür. Bu işyerlerinde işverenlerin işçilerin konumlarını, maden giriş ve çıkışlarını, işçilerin anlık hareketlerini dijital izleme ile takip etme yükümlülüğü bulunmaktadır[648].

Maden ve yeraltı işleri gibi işlerde, tehlikeli sınıfta faaliyet gösteren işyerlerinde giyilebilir teknolojilerle ve kamera izlemesiyle işçilerin işyerindeki tüm faaliyetlerinin izlenmesi gerekebilir. Bu durumlar gözetme borcunun yanında, kaynağını yasa ve idari düzenlemelerden alan yükümlülükler dijital izlemenin dayanağını oluşturmaktadır. Buna işçinin güvenliğini sağlamak için yeraltı kömür maden işinde tesis girişinde, çalışma alanlarında ve etrafında, park yerlerinde kamera gözetlemesi gerçekleştirilmesi ve işçilere dijital izleme imkanı verebilen giyilebilir baret ve yelek giydirilmesi; yeraltı ve yerüstü riskli inşaat işlerinde personel takip ve izleme sistemi[649] kullanılması örnek gösterilebilir.

---

648) Resmi Gazete'nin 19 Eylül 2013 tarih e 28770 sayılı nüshasında yayımlanan Maden İşlerinde İş Sağlığı ve Güvenliği Yönetmeliği'ne, Resmi Gazete'nin 10 Mart 2015 tarihli nüshasında yayımlanan değişiklikle Ek düzenlemeler yapılmıştır. Düzenlemeye göre "Ayrıca, yeraltı maden ocaklarında, yeraltında çalışacakların giriş-çıkışlarının ve bulundukları yerlerin her an doğru bir şekilde yerüstünde takip edilebileceği bir sistem kurulur. Bu sistemde kullanılan ekipmanlar, kablolar ve tamamlayıcı unsurların yeraltında yaşanan göçük, su baskını, patlama, yangın gibi acil hallere karşı korumalı olması ve bu hallerde de çalışabilir durumda olması sağlanır. Sistem tarafından tutulan kayıtlar en az bir yıl süreyle saklanır. Bu düzenleme daha sonra 2016'da eklenen ek cümle ile yürürlüğü 01.01.2017 tarihine ertelenmiştir.

649) Maden İşyerlerinde İş Sağlığı ve Güvenliği Yönetmeliği, Geçici Madde 3'te yeraltı maden işlerinde personel takip ve izleme sistemi kurma yükümlülüğü öngörülmüştür.

Sonuç olarak işveren, İSGK yükümlülükleri kapsamında riskleri ortadan kaldırmak için işçi verisi işleyen dijital izleme uygulaması ve izlemeye olanak veren sistemler kullanması gerekiyorsa bunları kullanmakla yükümlüdür. Örneğin, İSGK m. 15 işverene, işçilerin işyerinde maruz kalacakları riskleri dikkate alarak sağlık gözetimi yapma yükümlülüğü bulunmaktadır. Maddenin beşinci fıkrasında sağlık muayenesi yapılan ilgili işçinin özel hayatının gizliği ve itibarının korunması için işverene işlenen verileri gizli tutma yükümlülüğü getirmiştir. Bu yükümlülükler aynı zamanda dijital izlemenin dayanağını oluşturur. Eklemek gerekir ki, veri sorumlusu işveren İSG gereklilikleri kapsamında işlediği kişisel verilerde KVK hukukunun ilkelerini gözetmek ve öngörülen veri koruma mekanizmalarına uygun bir veri işleme süreci işletmesi, verilerin güvenliği için teknik ve idari tedbirleri almakla yükümlüdür. Ayrıca İSG yükümlülükleri kapsamında işlenen işçinin davranışsal biyometrik verisi, sağlık verisi özel nitelikli kişisel veridir. Bu verilerin işlenmesi için KVK hukukunun yükümlülüklerinin yerine getirilmesi gerekmektedir[650].

c) İşyerinde Tacizin ve Siber Zorbalıkların Önlenmesi

Psikolojik taciz, siber zorbalık ve tacizin diğer türleri (cinsel taciz, bedensel zarar, suça kışkırtılma, ihbar vb.) iş ilişkisindeki sorunların ön sıralarında yer almaktadır[651]. Bilişim sistemlerinin, sosyal medyanın ve anlık mesajlaşmanın iş ilişkisinin bir gerçeğine dönüşmesiyle birlikte yöneticilerden, diğer işçilerden veya üçüncü kişilerden işçiye uygulanan siber zorbalık örnekleri artmış ve bu

650) Bkz. § 6. II. 4. i.

651) Heinz Leymann, "The Content and Development of Mobbing At Work", European Journal of Work and Organizational Psychology, C. 5, S. 2, [1996], s.168; Tankut Centel, "Hukuki Boyutlarıyla Mobbing", Çalışma Hayatında Psikolojik Taciz (Mobbing) Paneli Çalıştayı Bildiriler Kitabı, Yayınlanmış Tebliğ, Ankara, [2013], s. 50; Pınar Tınaz/Fuat Bayram/Hediye Ergin, Çalışma Psikolojisi ve Hukuki Boyutlarıyla İşyerinde Psikolojik Taciz Mobbing, Beta Yayınevi, İstanbul, [2008], s. 3; Pınar Tınaz, "Mobbing: İşyerinde Psikolojik Taciz", Çalışma ve Toplum Dergisi, S. 3, [2006], s.12; Gökalp İzmir/Aygül Fazlıoğlu, İşyerinde Psikolojik Taciz (Mobbing) ve Çözüm Önerileri, Kadın Erkek Fırsat Eşitliği, Komisyonu Yayınları, Ankara, [2010], s. 5; Selahattin Samet Bilge, "Mobbing Terimi ve Türk Hukuk Düzeninde İncelenmesi", Ankara Üniversitesi Hukuk Fakültesi Dergisi, S. 65, C. 4, [2016], s. 1246.

davranışların işçi üzerinde yıkıcı etkiler bıraktığı gözlenmiştir[652]. İş yaşamında psikolojik şiddet, fiziksel şiddet ve cinsel şiddet türlerinin kesiştiği örneklerde görülebilmektedir. Cinsel şiddet fiziksel temas, şaka görünümlü cinsel taciz, cinsel saldırı, cinsel yorumlar, sosyal medyada cinsel söylentiler çıkarma, bilişim teknolojileri vasıtasıyla cinsel zorbalıklar uygulama, cinsel içerikli paylaşımlar gönderme gibi örneklerle cinsel taciz biçiminde mağdur üzerinde görünüme bürünür[653]. Cinsel şiddetin bu türleri iş ilişkisinde bulunan hiyerarşiye dayanarak cinsiyete yönelik gerçekleşmesi söz konusu olabilir. Cinsel şiddetin bu biçimde görünüm kazanması cinsiyete dayalı cinsel şiddet olarak ifade edilmektedir[654]. ILO, 190 sayılı Şiddet ve Tacizin Önlenmesi Sözleşmesi'nin m. 1/1-b düzenlemesinde, "toplumsal cinsiyete dayalı şiddet ve taciz" kavramı; "cinsiyet veya toplumsal cinsiyetlerinden dolayı kişilere yöneltilen veya belirli bir cinsiyet veya toplumsal cinsiyetten olan kişileri orantısız şekilde etkileyen şiddet ve taciz anlamına gelir ve cinsel tacizi içerir" biçiminde tanımlanmıştır[655].

Cinsel şiddeti de içerebilen siber zorbalık, bilişim sistemleri üzerinden sosyal medya ve diğer elektronik medya vasıtasıyla (e-posta, anlık mesajlaşma, Messenger, SMS, MMS, sosyal ağ siteleri, WhatsApp vb.) daha savunmasız konumda olan bireylere baskı uygulamak, zarar vermek biçiminde tanımlanmaktadır[656]. İşyerinde siber zorbalık ise, "belirli bir zaman içinde vuku bulan ve tekrarlanan ya da en az bir kere gerçekleşen ancak birinin özel hayatına haksız yere müdahale eden ve bunu geniş bir izleyici kitlesine sergileyen, bilgi ve iletişim teknolojisinin kullanımı aracılığıyla oluşan iş kaynaklı negatif tüm

652) Aktaranlar, Aysun Kanbur/Engin Kanbur, "İşyerinde Siber Zorbalık Ölçeği'nin Türkçeye Uyarlanması: Geçerlik ve Güvenirlik Sınama Çalışması", Psikoloji Çalışmaları - Studies in Psychology Cilt/Volume: 38, Sayı/Issue: 2, [2018], s. 242; Hatice Duygu Özer, "Pandemi Sürecinde Artan Tehlike: İşyerinde Siber Zorbalık", Selçuk Hukuk Kongresi 2020 Özel Hukuk Tebliğleri Tam Metin Kitabı, Nobel Akademi, [2020], s. 137.
653) Seher Demirkaya/Ceyhun Güler, "Çalışma Yaşamında İşçinin Kişilik Haklarının Korunması Bağlamında ILO'nun 190 sayılı Şiddet ve Taciz Sözleşmesinin değerlendirilmesi", Çalışma ve Toplum, 2021/4, [2021], s. 2758.
654) Demirkaya/Güler, Şiddet ve Taciz, s. 2758-2960.
655 https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-ankara/documents/genericdocument/wcms_719975.pdf (Erişim Tarihi: 19.11.2023).
656) Özer, [2020], İşyerinde Siber Zorbalık, s. 137 vd.

davranışlar" biçiminde tanımlanmaktadır[657]. Siber zorbalığa maruz kalan işçi kendisini savunmasız hissederek çaresiz ve bezgin bir yapıya bürünebilir[658].

Siber zorbalığı uygulayan kişi işyerinde bir amir, işveren, iş arkadaşı olabileceği gibi işyeri ortamı dışındaki üçüncü kişilerin de işçiye siber zorbalık uygulaması mümkündür. Bundan dolayı siber zorbalık sadece dikey bir ilişkide kaynaklanan saldırganlık değil, yatay düzeydeki ilişkilerde hatta işyeri dışındaki kişilerden kaynaklı zorbalıklar ortaya çıkabilmektedir. Bu sebeple siber zorbalık sadece statü ile ilişkilendirilerek nitelendirilemez[659].

ILO'nun 190 sayılı Sözleşmesi'nin temel ilkelerinden birisi olan m. 4/2 düzenlemesinde şiddet ve tacizin üçüncü kişilerden de gelebileceği göz önünde bulundurularak sözleşme tarafı ülkelere bunları engelleyecek tedbirleri almalarını temel ilke olarak düzenlemiştir[660]. Örneğin müşteri hizmetleri departmanında çalışan bir işçinin müşteriler tarafından aranarak veya anlık mesaj gönderilerek baskı altında tutulması üçüncü kişiler tarafından gerçekleştirilen siber zorbalığa örnektir. Bu sebeple fail veya fiilin gerçekleştiği yer açısından bir ayrım yapmak yerine siber zorbalığın iş ilişkisi temelinde ortaya çıkması yeterli görülmelidir[661]. 190 sayılı Sözleşme m. 3'te bu husus: "çalışma yaşamında iş sırasında meydana gelen, iş ile bağlantılı veya iş nedeniyle ortaya çıkan şiddet ve taciz" biçiminde düzenleme altına alınmıştır.

---

657) Ahmet Taşkın, "Mobbingin Benzer Kavramlardan Farkı", Sicil İş Hukuku Dergisi, S. 28, [2012], s.62; Özer, [2020], İşyerinde Siber Zorbalık, s. 138.

658) Tuija Muhonen/Sandra Jönsson/Martin Bäckström, "Consequences of cyberbullying behaviour in working life", International Journal of Workplace Health Management, Vol. 10, No. 5, [2017], s. 376 vd.

659) Özer, [2020], İşyerinde Siber Zorbalık, s. 139.

660) ILO, 190 Sayılı Sözleşme'nin 4/2 düzenlemesi şu şekildedir: "Her Üye, ulusal yasa ve koşullara uygun olarak ve temsili işveren ve işçi örgütlerine danışarak, çalışma yaşamında şiddet ve tacizin önlenmesi ve ortadan kaldırılması için kapsayıcı, bütünleşik ve toplumsal cinsiyete duyarlı bir yaklaşım benimser. Böyle bir yaklaşım, uygun olduğu durumlarda, üçüncü tarafların dahil olduğu şiddet ve tacizi dikkate almalı ve şunları içermelidir…"

661) Valerio De Stefano/Charalampos Stylogiannis/Mathias Wouters/Ilda Durri, "System Needs Update: Upgrading Protection Against Cyberbullying And ICT-Enabled Violence And Harassment İn The World Of Work", [2020], https://www.ilo.org/static/english/intserv/working-papers/wp001/index.html (Erişim Tarihi: 19.11.2023); Özer, [2020], İşyerinde Siber Zorbalık, s. 140.

Siber zorbalık ve taciz farklı formatlarda görünüm kazanabilmektedir. Örneğin bir işçiye ait e-postaları başkalarına göndermek, anlık mesajlaşma gruplarında bir çalışana rahatsız edici ithamlarda bulunmak, bir işçiyle ilgili asılsız söylentiler çıkarmak, cinsel içerikli gönderiler paylaşmak, bir işçinin dosyalarını silmek, çağrı merkezi çalışanlarının müşterilerin baskı ve şiddet içerebilen yaklaşımlarına izin vermek bunlara örnek gösterebilir. Bu yaklaşımlara maruz kalan işçinin üzerinde oluşacak işyeri stresi, psikolojik yıkım ve ortaya çıkan sağlık ve güvenlik riskleri aynı zamanda iş sağlığı ve güvenliğinin de konusudur[662].

İşverenlerin gözetme borcunu doğrudan düzenleyen TBK m. 417 siber zorbalık, taciz ve mobbingde doğrudan uygulama alanı bulur. Zira TBK m. 417/1 düzenlemesine göre işverenlerin, "işçilerin psikolojik ve cinsel tacize uğramamaları ve bu tür tacizlere uğramış olanların daha fazla zarar görmemesi için gerekli önlemleri alma" yükümlülüğü bulunmaktadır. Mobbing (psikolojik taciz) madde kapsamında sayılmış ve işverene, işçinin manevi kişilik hakları üzerinde sistematik, süreklilik gösteren kötü muamelelerden kaçınma ve bunlara işçilerin maruz kalmaması için gerekli tedbirleri alma yükümlülüğü yüklenmiştir[663].

İşverenler gözetme borcu kapsamında işçileri siber zorbalıklardan, taciz ve mobbingden korumak için gerekli tedbirleri almakla yükümlüdür. Uzaktan çalışan işçilerin bu olumsuzluklarla karşılaşmaması için dijital izleme uygulamaları kullanılması ve internet trafiğinin takip edilmesi gerekebilir. Aynı doğrultuda işyerinde tacizi engellemek amacıyla kamera gözetlemesi, iletişimin izlenmesi, e-posta, anlık mesajlaşmaların takibi gibi çeşitli dijital izleme uygulamaları kullanılabilir. İşyerinde ortak alanlara kamera konması, işyeri güvenliğinin sağlanması, siber zorbalığa karşı farkındalık eğitimlerinin verilmesi ve işçilerin bu tür olumsuzluklarla karşılaştıklarında başvurabilecekleri ve gerekli raporlamayı

662) Stefano/Stylogiannis/Wouters/Durri, [2020], Protection Against Cyberbullying, [2020]; Özer, [2020], İşyerinde Siber Zorbalık, s. 140-141.
663) Süzek, [2019], İş Hukuku, s. 389; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 182 vd.; Özdemir, [2020], İş Sağlığı, s. 88 vd.; Sevimli, [2013], İşçinin Kişiliğinin Korunması, s. 113 vd.

yapabilecekleri kanalların oluşturulması; işin niteliğine göre aydınlatma yükümlülüğünü yerine getirerek telefon, anlık mesajlaşma, internet trafiğini ve e-postaları dijital izleme uygulamalarıyla izleyerek siber zorbalığı önleyen tedbirler alınabilir[664].

İşverenler açısından işçileri siber zorbalıklardan korumak ve işyerinde tacizi engellemek dijital izlemenin dayanağını oluşturur. Önemle eklemek gerekir ki, bu dayanak işverene dilediği biçimde dijital izleme uygulamalarıyla işçileri izleme ve kayıt altına alma hakkını vermez. İlgili başlıklarda[665] detaylı incelendiği üzere işverenler bu meşru amaç kapsamında açık rıza almaksızın ve fakat KVK hukukunun veri işlemede şeffaflığı sağlamaya ilişkin olan aydınlatma yükümlülüğünü yerine getirmek ve genel ilkelere uygun bir veri işleme faaliyeti yürütmek zorundadırlar. İşverenler, KVKK m. 10 ve Tebliğ düzenlemelerine uygun olarak işçileri gerçekleştirilecek dijital izleme hakkında tam olarak bilgilendirmekle ve işlenen işçi verilerini meşru amacı gerçekleştirecek en az veriyi işleyecek şekilde bir uygulama geliştirmesi ve işlenen verilerin güvenliği için gerekli tüm teknik ve idari tedbirleri almakla yükümlüdür.

d) Kamu Sağlığının Korunması: Covid-19 Pandemisinin Ortaya Çıkardığı Uygulamalar ve Dijital İzleme

Covid-19'un pandemi olarak kabul edilmesiyle birlikte otelcilik gibi bazı hizmet sektörlerinde işsizlik, kısa çalışma ödeneği ve geçici madde kapsamında ücretsiz izin uygulamaları yaygınlaşırken, birçok ofis çalışanı işlerini evde görmeye başladı[666]. Dahası pandemi koşullarının bir gereği olarak farklı sektörde faaliyet gösteren birçok işyeri aniden uzaktan çalışmayı deneyimlemek durumunda kaldı[667].

664) Özer, [2020], İşyerinde Siber Zorbalık, s. 146 vd.
665) Bkz. § 6. II.
666) İbrahim Subaşı, "Küresel Covid-19 Salgını'nın Türk Bireysel İş Hukukuna Etkisi", İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi, S. 5, [2020], s. 128.
667) Jessica Vitak/Michael Zimmer, "Surveillance and The Future of Work: Exploring Employees' Attitudes Toward Monitoring in a Post-COVID Workplace", Journal of Computer-Mediated Communication, 2023, Vol. 28/4, [2023], s. 3.

Uzaktan çalışma her sektörde uygulanabilir olmamakla birlikte, pandemi sonrası işleri ağırlıklı olarak ofis ortamında olan çalışanlar için yeni bir normal olarak kabul gördü[668].

Uzaktan çalışmada çeşitli türde dijital izleme uygulamalarının kullanılmaya başlanması işçilerin uzaktan çalışmada nasıl denetlenebileceği, performanslarının nasıl ölçüleceği, performans ölçümünün isabet oranı[669], dijital izlemenin sınırlarının ne olması gerektiği, uzaktan çalışmada kullanılan dijital izleme uygulamalarının işçilerin özel hayatlarını ve kişisel verilerini ihlal etme olasılığı çerçevesinde tartışmalar ortaya çıkardı[670]. Yapılan araştırmalarda işverenlerin pandemi koşulları ortadan kalktıktan sonra da pandemi döneminde edindikleri dijital izleme deneyimlerini ve yeni denetim biçimlerini işçinin kişisel zamanını da kapsayacak şekilde izleme uygulamalarını kullanmaya devam ettirme eğiliminde oldukları sonucuna ulaşılmıştır[671]. Zira uzaktan çalışma mesai saati kavramını bulanıklaştırmakta, işçinin 7/24 çalışma düzeninde ulaşılabilir olma, kendisinde iş istenebilir olma, akşamları ve hafta sonları işçiden çalışmaya devam etmesi olanağını işverene vermektedir. Bu durumun başlıca sebeplerinden birisi işçilerin ev ortamında kolayca izlenebilmeleri, mobil sistemlere entegre çeşitli dijital izleme uygulamalarıyla denetlenebilir olmasından kaynaklanmaktadır[672].

---

668) Baycık/Doğan/Dulay Yangın/Yay, [2021], Pandemide Uzaktan Çalışma, s. 1705-1708; Abigail Adams-Prassl/Christopher Rauh/Teodora Boneva/Marta Golin, "Working from Home:The Polarising Workplace", VoxEU.org, https://voxeu.org/article/working-home-polarising-workplace, (Erişim Tarihi: 15.11.2023).

669) Nguyen, [2020], Post-Covid-19, https://www.shrm.org/executive/resources/people-strategy-journal/summer2020/pages/feature-nguyen.aspx, (Erişim Tarihi: 16.11.2023).

670) Vitak/Zimmer, [2023, Surveillance and The Future of Work, s. 3; Ball, [2021] Electronic Monitoring, s. 6.

671) Luisa Wieser/Martin Abraham, "Employee Acceptance of Digital Monitoringsystems While Working From Home, New Technology Work Employment", [2023], s. 1-34, https://onlinelibrary.wiley.com/doi/epdf/10.1111/ntwe.12280 (Erişim Tarihi: 16.11.2023); Zickuhr, [2021], Workplace Surveillance, https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/ (Erişim Tarihi: 16.11.2023).

672) Ivan Manokha, "Covid-19: Teleworking, Surveillance and 24/7 Work. Some Reflexions on the Expected Growth of Remote Work After the Pandemic", Political Anthropological Research on International Social Sciences (PARISS), [2020], s. 276, https://brill.com/view/journals/pari/1/2/article-p273_273.xml, (Erişim Tarihi: 15.11.2023).

Ayrıca salgının işçilere ilişkin işlenen veri miktarı ve çeşitliliğini önemli ölçüde artırdığı, işverenlerin uzaktan çalışmayı dijital denetimle sağlama eğiliminin işçilerin dijital parmak izleri (davranışsal biyometrik veri) olarak nitelendirilebilecek verilerini işlemeye ve analiz etmeye olanak tanıdığı tespit edilmiştir[673]. Uzaktan çalışmada işçiler hakkında veriyi elde etmenin en kolay yolu onların günlük yaşamda kullandıkları çeşitli teknolojik aletler ve bilişim sistemleridir[674]. Örneğin işçinin klavye aktif süresini bir yazılımla bilgisayar üzerinde takip etmek, bilgisayar ekranını tamamen kaydetmek veya belirli aralıklarla fotoğraflamak, internet trafiğini izlemek, sosyal medya davranışlarını, e-postalarını, kişisel zaman aktivitelerini bir bilişim uygulamasıyla izlemek ve kayıt altına almak kolaylıkla yapılabilmektedir.

Olaya kamu sağlığı açısından bakıldığında Covid-19 süresince hastalık vakasının tespit edilmesi ve temas takibi için Hayat Eve Sığar (HES) uygulaması, işyeri girişlerine ateş ölçer optik sistemler, sağlık verilerini işleyen uygulamalarla hastalık ve temas izleme uygulamaları kullanıldı. Bu uygulamaların bireysel gizliliği ihlal ettiği, işçilerle ilgili veri işleme çeşitliliğini artırdığına ilişkin çeşitli kaygılar dile getirildi[675].

Öte yandan, pandemi koşullarında kamu sağlığının korunması için iş ilişkisinde sağlık testleri ve aşı bilgisi gibi sağlık verileri KVK hukukunun kapsamı

673) Ball, [2021] Electronic Monitoring, s. 12; Vitak/Zimmer, [2023, Surveillance and The Future of Work, s. 4; Stephen Blumenfeld/Gordon Anderson/Val Hooper, "Covid-19 and Employee Surveillance", New Zealand Journal of Employment Relations, Vol. 45, No. 2, [2020], s. 42 vd.
674) Pandemi koşullarında çeşitlenen işveren dijital uygulama örnekleri için bkz. https://www.linkedin.com/pulse/how-covid-19-has-accelerated-use-employee-monitoring-dan-schawbel (Erişim Tarihi: 17.11.2023).
675) Isabela Possino,."Employee Monitoring: As Technology Advances Yet the Electronic Communications Privacy Act Stays in the Past", SMU Science and Technology Law Review, Vol. 26, No. 1, Spring/Summer [2023], s. 141; Sophia Maalsen/Robyn Dowling, "Covid-19 and The Accelerating Smart Home", Big Data & Society, Vol. 7, Issue 2, July-December, [2020], https://journals.sagepub.com/doi/epub/10.1177/2053951720938073, (Erişim Tarihi: 17.11.2023); ; John Paul M. Gaba/Joan Janneth M. Estremadura, "Data Protection of Biometric Data and Genetic Data", Ateneo Law Journal, Vol. 64, No. 3, February, [2020], s. 977.

dışında değerlendirilmiştir[676]. Zira kamu sağlığını korumak amacıyla işçi verilerinin işlenmesi veri koruma mevzuatımızda kanunun istisnalarından birisi olarak düzenlenmiştir (KVKK m. 28/1-ç). KVK Kurumu, Covid-19'un pandemi olarak kabul edilmesinin akabinde yayımladığı duyuruda kişinin özel nitelikli kişisel verileri (KVKK m. 6/1) de dahil olmak üzere birçok verinin salgın tedbirleri kapsamında işlenebileceğini, bu veri işleme faaliyetinin KVKK kapsamında olduğunu, Kanunun öngördüğü ilkelere uygun yükümlülüklerin yerine getirilerek temel ilkelerin gözetilmesini, kişisel verilerin korunması için gerekli teknik ve idari tedbirlerin[677] alınmasını, veri işlemede şeffaflığın (aydınlatma yükümlülüğü) sağlanmasını ve meşru amaç için sınırlı veri işlenmesine dikkat edilmesi gerektiğini duyurmuştur[678].

KVK Kurumu daha ileriki bir tarihte PCR testi ve aşı bilgisiyle ilgili gerçekleştirdiği duyuruda ise, Çalışma ve Sosyal Güvenlik Bakanlığı'nın 81 il valiliğine göndermiş olduğu 02.09.2021 tarihli yazıya atıf yaparak; "işyerlerinde karşılaşılabilecek sağlık ve güvenlik risklerine yönelik koruyucu ve önleyici tedbirler" kapsamında aşı olmayan işçilerin PCR testine tabi tutulabileceğini, bunun işyeri/işveren tarafından istenmesinin mümkün olduğunu, test sonuçlarını ve aşı bilgilerinin kayıt altına tutulabilmesinin kamu sağlığının korunmasıyla ilgili olduğundan KVKK m. 28/1-ç bendi kapsamında değerlendirilerek kanun kapsamının istisnası olduğunu, bu sebeple KVKK hükümlerinin bu durumlarda uygulanmayacağını belirtmiştir[679].

---

676) Bkz. KVK Kurumu, https://www.kvkk.gov.tr/Icerik/7055/COVID-19-PCR-TEST-SONUCU-VE-ASI-BILGISI-UYGULAMALARINA-ILISKIN-KAMUOYU-DUYURUSU (Erişim Tarihi: 18.11.2023).

677) KVK Kurulu, 31/01/2018 tarihli ve 2018/10 sayılı Kararı ile "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" belirlenmiştir. Sağlık verisi, biyometrik veri gibi veriler özel nitelikli kişisel veri olarak (KVKK m. 6/1) düzenlendiğinden veri sorumlusu işveren bu verileri işlerken kararda belirtilen asgari güvenlik tedbirlerini alması gerekmektedir. Kararın detayları için bkz. https://www.kvkk.gov.tr/Icerik/4110/2018-10

678) https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler- (Erişim Tarihi: 18.11.2023).

679) Duyuru içeriği için bkz. https://www.kvkk.gov.tr/Icerik/7055/COVID-19-PCR-TEST-SONUCU-VE-ASI-BILGISI-UYGULAMALARINA-ILISKIN-KAMUOYU-DUYURUSU (Erişim Tarihi: 18.11.2023).

KVK Kurumu duyurusunda ortaya çıktığı üzere kamu sağlığı ve işçilerin korunması söz konusu olduğunda iş ilişkisinde bu durumlar dijital izleme uygulamalarının dayanağını oluştur. Bu durumda dijital izleme uygulaması doğrudan kamu sağlığının korunmasına ilişkin olduğundan veri işleme KVKK kapsamında değerlendirilmeyecek (KVKK m. 28), işverenler aydınlatma yükümlülüğünü de yerine getirmeden dijital izleme uygulaması kullanabileceklerdir. Örneğin, Covid-19 kapsamında aşılı işçilerin takip edildiği dijital uygulamalar ve PCR testlerinin kayıt altına alındığı dijital izleme uygulamaları bu kapsamda değerlendirilebilir. GVKT'de kamu sağlığının korunması ve kamu yararının söz konusu olduğu durumlarda, özel nitelikli kişisel veri olan ve GVKT m. 9/1'de işlenmesinin yasak olarak düzenlenen kişisel sağlık verisinin işlenmesini GVKT m. 9/2-i bendine istisna olarak düzenlenmiştir[680].

İlgili başlıkta[681] detaylı ele alınmış olmakla birlikte bu başlık açısından önemli olduğundan belirtmek gerekir ki, işçinin özel nitelikli kişisel verisi olan "kişisel sağlık verisi" doğrudan kamu sağlığının korunması ve pandemi koşulları söz konusu değilse işverenin KVK hukukunun düzenlemelerde öngörülen içeriği ve unsurları barındıran bir aydınlatma metni ile işçileri bilgilendirmesi gerekmektedir. Ayrıca dijital izleme uygulamasıyla kişisel sağlık verisi işleniyorsa işçiden KVKK m. 6/2 kapsamında açık rıza alması zorunludur. İşverenin bu kapsamda hareket etmemesi kişisel veri işleme faaliyeti hukuka aykırı veri işleme olarak nitelendirilebilecektir[682].

KVKK m. 6/1'de sağlık verisi özel nitelikli kişisel veri olarak düzenlenmiş, ikinci fıkrada özel nitelikli kişisel verilerin ilgili kişinin açık rızası alınmaksızın işlenemeyeceği, üçüncü fırkada ise sağlık verisi ve cinsel hayat verisi ayrı tutularak

680) Mustafa Alp/İlke Gürsel, "Covid-19 Pandemisinde İşçilere Ait Sağlık Verilerinin İşlenmesi", Sicil İş Hukuku Dergisi, S. 44, [2020], s. 16-17.
681) Bkz. § 6. II.
682) Bkz. https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler- (Erişim Tarihi: 18.11.2023); Alp/Gürsel, [2020], Sağlık Verilerinin İşlenmesi, s. 22.

kanunda tahdidi olarak sayılan diğer özel nitelikli kişisel verilerin kanunlarda öngörülen hallerde veri sahibinin açık rızası olmaksızın işlenebileceği düzenlenmiştir[683]. Kişisel Sağlık Verileri Hakkında Yönetmelikte kişisel sağlık verisi: "Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler" biçiminde tanımlanmıştır (Yönetmelik m. 4/I-j). Bu kapsamda işçinin kişisel sağlık verisi KVKK m. 28/1-ç bendi istisnası ve pandemi koşulları dışında ancak ilgili kişinin açık rızası alınarak veya kamu sağlığının korunması, koruyucu hekimlik kapsamında sır saklama yükümlülüğü bulunanlar tarafından, KVKK m. 6/3 koşullarının varlığı halinde işlenebilir[684]. Ayrıca işçinin, veri sorumlusu işveren tarafından aydınlatma yükümlülüğü kapsamında bilgilendirilmesi de gerekmektedir. Bu yükümlülükler yerine getirilmedikçe dijital izleme uygulamalarıyla işçinin kişisel sağlık verisinin işlenmesi hukuka aykırı olacaktır[685].

3. Personel Yönetmeliğinde Yer Alan Kişisel Veri Düzenlemeleri

İşçi verilerini işlemeye ve dijital izlemeye ilişkin düzenlemelerin yer aldığı personel yönetmelikleri, işyeri prosedürleri, araç ve internet kullanım politikaları uygulamada dijital izlemenin dayanağı olarak görülebilmektedir. İşçilerin dijital izleme uygulamalarıyla izlendiğine, araçların GPS ile takip edildiğine ve özel kullanımın yasak olduğuna ve internet trafik bilgilerinin kayıt altına alınarak izlendiğine ilişkin kayıtların yer aldığı bu düzenlemelerin KVK hukuku düzenlemeleri kapsamında geçerliliğinin KVK hukukunun öngördüğü aydınlatma yükümlülüğünün unsurları açısından değerlendirilmesi gerekmektedir.

---

683) Alp/Gürsel, [2020], Sağlık Verilerinin İşlenmesi, s. 12-13.
684) Alp/Gürsel, [2020], Sağlık Verilerinin İşlenmesi, s. 21; Prof. Dr. Gülsevil Alpagut'un yaklaşımı için bkz. https://datassist.com.tr/blog/pandemi-suresince-calisanlarin-kisisel-verilerinin-korunmasi/ (Erişim Tarihi: 17.11.2023).
685) Bkz. KVK Kurulu'nun 08.12.2018 tarih ve 2018/143 karar numaralı "Sağlık verilerini Kanunun 6'ncı maddesinde yer alan işleme şartlarından birine dayanmadan üçüncü bir kişiye aktaran veri sorumlusu hakkında" Kişisel Verileri Koruma Kurulunun 05/12/2018 Tarihli ve 2018/143 Sayılı Karar Özeti".

İş ilişkisinde işçinin bağımlı çalışması ve işverende tutulan özlük dosyasında özel nitelikli kişisel verileri de dahil olmak üzere birçok verisi yer aldığından, işçi verileri işlenen herhangi bir kişi değildir. Yukarıda ele alındığı üzere işverenin işçi hakkında sahip olduğu bilgi yoğunluğu ve denetim boyutu dikkate alındığında dijital izlemenin işçinin hakları üzerindeki müdahaleci etkisi daha yoğun olabilmektedir. Bir gerçek kişi olan işçinin verilerinin işlenmesi KVK hukukunun kapsamında yer aldığından, KVKK'da öngördüğü düzenlemelere uygun[686] veri işleme faaliyetinin yürütülmemesi hukuka aykırı veri işleme nitelendirilecektir[687].

İş sözleşmesinde belirginleşen bağımlılık unsuru işçiye; işverenin iş organizasyonunu ve işin yapılma biçimini belirlediği işyerinde onun emir ve talimatları kapsamında iş yapma borcu yüklemektedir[688]. Bireysel iş sözleşmesinin bu özelliği aynı zamanda işverene mülkiyeti koruma, verimlilik ve belirli yükümlülükler kapsamında dijital izleme uygulamaları kullanma hakkı ve bu hakları da içeren işyerine yönelik personel yönetmeliği düzenleme hakkı tanımaktadır. İş sözleşmesinden ortaya çıkan bu hak işçinin özel hayatına saygı hakkı ve kişisel verilerinin korunması üzerinde sınırlandırıcı etkiler ortaya çıkarmaktadır[689].

İşverenler iş sözleşmesi kapsamında işyerinin düzeni, iş yapma biçimi, iş sağlığı ve güvenliği, çalışma disiplini ve çalışma koşullarıyla ilgili olarak önceden tek taraflı personel yönetmelikleri hazırlayabilmektedir. Personel yönetmelikleri hukuki niteliği itibariyle iş sözleşmesinin eki niteliği taşıdığından çalışmakta olan işçiler bakımından İş Kanunu m. 22 uyarınca işçinin yazılı kabulüyle bağlayıcı hale gelmektedir. İşçiler iş sözleşmesine taraf olduğunda bu personel yönetmelikleri de

686) Kişisel verilerin işlenmesinin hukuka uygunluk değerlendirmesi için bkz. § 6. II. 3. a.
687) KVK Kurumu, [2019], Uygulama Rehberi, s. 74.
688) Süzek, [2019], İş Hukuku, s. 228; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 118.
689) AYM, GK Kararı, E.Ü. Başvurusu, Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020, §54, R.G. Tarih ve Sayı: 14/10/2020-31274.

kendilerine tebliğ edilerek iş sözleşmesinin bir parçası haline getirilmektedir[690]. Her ne kadar işçinin kabulüyle bağlayıcı hale gelse de işverenin tek taraflı hazırladığı personel yönetmelikleri TBK m. 20 vd. düzenlemelerinde yer alan genel işlem koşullarının özelliklerini taşımakla[691] birlikte iş hukuku öğretisi koşulların gerçekleşmesinden dolayı bağlayıcılık kazanan personel yönetmeliklerinin iş sözleşmesinin bir eki olduğunu kabul edilmektedir[692]. Bu kapsamda işverenin önceden düzenlediği ve işçinin temel hak ve özgürlüklerine ilişkin haklarının sınırları dahilinde bulunan, işçilerin önceden tam olarak bilgilendirildiği personel yönetmelikleri dijital izlemenin dayanağını oluşturur.

Hukuken sorun personel yönetmeliklerinde KVK hukukunun gerekliliği olan hukuka uygunluk ölçütlerinin[693] yerine getirilip getirilmediği noktasında toplanmaktadır. Dijital izlemenin dayanağı olabilen personel yönetmeliklerinde yer alan kişisel verilerin işlenmesine ilişkin düzenlemelere dayanarak dijital izleme uygulamalarıyla kişisel veri işlemenin hukuka uygunluğu KVK hukukunun düzenlemelerine uygun bir veri işleme faaliyetinin yürütülmesine ve işçilerin, veriler işlenmeden önce "tam olarak[694]" bilgilendirilmesine bağlıdır[695]. KVK

690) Orhan Ersun Civan, Genel İş Koşulları, İstanbul, [2015], s. 65; Yeşim M. Atamer, Sözleşme Özgürlüğünün Sınırlandırılması Sorunu Çerçevesinde Genel İşlem Şartlarının Denetlenmesi, Beta Yayınevi, [2001], s. 125-126; Orhan Ersun Civan, "Genel İş Koşullarında Değişiklik Kayıtlarının Geçerliliği ve Denetimi", Prof. Dr. Turhan Esener'e Armağan, C. 1, Ankara, [2016], s. 790-791; Sarper Süzek, "Yeni Türk Borçlar Kanunu Çerçevesinde Genel İş Koşulları, Sicil, C. 24, Arlık, [2011], s. 5-6; Süzek, [2019], İş Hukuku, s. 60-61; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 193.

691) Civan, [2015], Genel İş Koşulları, s. 56-57, 66; Süzek, [2019], İş Hukuku, s. 61.

692) Süzek, [2019], İş Hukuku, s. 62; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 193-194; Yargıtay da personel yönetmeliğinde yer alan düzenlemelerin çalışma şartları meydana getirdiğine karar vermektedir. Yargıtay 22. HD, 2015/34150E., 2015/8689 K., Karar Tarihi: 03.03.2015.

693) Bkz. § 6.

694) AİHM, [GK], [2017], Bărbulescu v. Romanya kararı, § 30. Mahkeme, işverenin işyerine ilişkin belirli kurallar koymasında menfaati bulunduğunu, bu hak kapsamında sınırlandırmalar getirebileceğini ve izleme uygulamaları kullanabileceğini, bunun için işçinin "tam olarak bilgilendirilmesi" gerektiğine karar vermiştir.

695) KVK Kurumu, aydınlatma yükümlülüğüne ilişkin duyurusuna ve kararına bkz. https://www.kvkk.gov.tr/Icerik/2033/Aydinlatma-Yukumlulugu-#:~:text=Veri%20i%C5%9Fleme%20faaliyetinin%20ilgili%20ki%C5%9Finin,verisinin%20i%C5%9Flendi%C4%9Fi%20her%20durumda%20ayd%C4%B1nlat%C4%B1lmal%C4%B1d%C4%B1r. (Erişim Tarihi: 15.11.2023); Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul

hukukumuz açısından tam olarak bilgilendirilmeden anlaşılması gereken, KVKK m. 10 kapsamındaki "aydınlatma yükümlülüğünün" tüm unsurlarının bulunduğu ve aydınlatma yükümlülüğüne ilişkin Tebliğin m. 4 ve 5'te sayılan unsurları taşıyan bir aydınlatma metnidir[696]. Aksi durumda personel yönetmeliklerinde veya internet kullanım politikası ve diğer işyeri düzenlemelerinde "dijital olarak izleneceksiniz, internet trafiğiniz takip edilecektir, GPS ile sahada izleneceksiniz" biçimindeki bilgilendirmeler tam bilgilendirme olarak kabul edilmeyecektir. Zira personel yönetmeliğinde yer alan bu kayıtta izlemenin hukuka uygunluk sebebi, sınırı, amacı, işlenen veriler, işçinin hakları gibi hususlarda bilgi yer almamaktadır. Bu sebeple dijital izlemede elde edilen verinin işçinin aleyhine kullanılmasına olanak bulunmamaktadır[697].

AİHM Büyük Daire, Bărbulescu & Romanya kararında 95/46EC sayılı AB direktifinin genel ilkelerine ve tam bilgilendirmeye atıf yaparak bu niteliği taşımayan bildirimleri, personel yönetmeliğindeki ifadeleri tam bilgilendirme kapsamında değerlendirmemiştir[698]. KVK Kurumu yayımladığı rehberde aydınlatma yükümlülüğünün veri sorumluları için bir yükümlülük olduğunu ve bunun yerine getirilmesinin talebe bağlı olmadığını, kişinin bir hakkı olduğunu ve kişisel verilerin hukuka uygun işlenmesinin olmazsa olmaz şartı olduğunu vurgulamıştır[699]. Aydınlatma yükümlülüğünün veri sorumlusu tarafından yerine getirilmesi yükümlülüğü KVK hukukunun ilkelerinden olan hukuka uygunluk ilkesi ve şeffaflık ilkelerinin bir gereğidir[700]. Dolayısıyla aydınlatma yükümlülüğü

---

ve Esaslar Hakkında Tebliğ için bkz. https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm (Erişim Tarihi: 15.11.2023).

696) Bkz. § 6. II. 6. a.

697) AİHİM kararına konu olan olayda, Bărbulescu işyeri bilgisayarının özel işleri için kullanmayacağına ilişkin yasakları içeren işyeri iç prosedürünü imzalamıştır (§ 16-23). AİHİM işverenin bu tür prosedürler oluşturma hakkı bulunduğu tespit ederek, bunların işçi için bağlayıcı olması için "tam olarak bilgilendirilmesi" gerektiğine karar vermiştir Bkz. AİHM, [GK], [2017], Bărbulescu v. Romanya kararı, § 30, § 124-141.

698) AİHM [GK], [2017], Bărbulescu v. Romanya, § 124-141.

699) KVK Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, Nisan [2019], s. 6.

700) Küzeci, [2020], Kişisel Veriler, s. 248; Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 97; Murat Develioğlu, "Avrupa Birliği Genel Veri Koruma Tüzüğü", On İki Levha Yayınları, İstanbul, [2017], s. 83.

yerine getirilmeden personel yönetmeliklerinde yer alan ve aydınlatma yükümlülüğünün içerik ve usul unsurlarını barındırmayan düzenlemelerle dijital izleme uygulamaları kullanarak işçilerin kişisel işlemek süreci hukuka aykırı hale getirir[701].

III. Ara Değerlendirme: İş İlişkisinde Dijital İzlemenin Dayanaklarının Değerlendirilmesi

İşverenlerin iş sözleşmesinden doğan gözetme borcunun bir gereği olarak işçileri tacizden ve tehlikelerden korumak için gerekli her türlü idari ve teknik tedbiri alma yükümlülüğü bulunmaktadır. Örneğin işveren, köprü inşaatı işinde yüksekte çalışan işçilerin güvenliği sağlamak için anlık konum bazlı veya giyilebilir RFID etiketli giysilerle dijital izleme uygulaması kullanması gerekiyorsa bu yükümlülüğe uygun dijital izleme uygulamasını kullanmakla yükümlüdür. Aynı doğrultuda işverenler işyeri güvenliğini sağlamak, işçileri tacizden, siber zorbalıklardan ve mobbingden korumak için belirli ortak alanları kamera ile gözetlemek veya bunları engelleyici çeşitli dijital izleme uygulamalarını kullanmak zorunda kalabilir. Ayrıca işyeri verimini artırmak için bir üretim bandının izlenmesi veya uzaktan çalışmada ölçülü olması kaydı ile işçiler bilgilendirilerek yönetim hakkı kapsamında amaca uygun en az müdahaleci dijital izleme uygulamasının kullanılması mümkündür[702]. İleride detaylı olarak ele alındığı üzere, işyerinde bir suçu önlemek için sınırlı, amaca uygun ve süresi belirli olan dijital izleme uygulamaları da kullanılabilir. İşveren KVK hukukunun hükümlerinin gereklerini yerine getirerek[703] interneti ve e-posta hareketlerini, işçilerin sahadaki hareketlerini izleyebilir. Zira AB düzenlemelerine, ülkemiz içtihat ve doktrinine ve ILO çalışmalarına baktığımızda iş sözleşmesinin ortaya çıkardığı ilişki kapsamında işçileri denetleme ve dijital izleme dahil işyerinin sevk ve idaresine ilişkin belirli

701) KVK Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, Nisan [2019], s. 6 vd.
702) AYM, Genel Kurul Kararı, E.Ü. Başvurusu, Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020, § 68 ve § 69.
703) Bkz. § 6. II.

hakları bulunduğu genel olarak kabul edilmektedir[704].

AİHM ve AYM kararlarında işverenin işyerinin sevk ve idaresine yönelik haklarının teyit edildiği görülmektedir[705]. AYM'nin gözetleme, internetin ve e-postaların izlenmesiyle ilgili kararlarında işverenin ve işçinin çatışan menfaatleri kapsamında olaya yaklaşılmakta ve işverenin işyerinde huzur ve disiplinin sağlanması amacıyla keyfi ve sınırsız olmamak kaydı ile işyerine ilişkin kurallar belirleyeceği kabul edilmektedir. AYM'ye göre anayasal hak ve özgürlüklerin sağladığı güvencelere aykırı olmamak kaydıyla: "işletmenin ticari gerekliliklerine ve disiplin anlayışına göre belirlenen kuralların açık bir şekilde yer aldığı düzenlemelerin bulunduğu ve bu düzenlemeler karşısında çalışanların önceden bilgilendirilip uyarıldığı durumlarda, kapsamı belirli şekilde çalışanların özellikle çalışma saatleri içinde bir takım haklarının kısıtlanması ve kuralların dışına çıkılmamaya zorlanması amacıyla tedbirler alınması makul görülebilir" (§ 65)[706].

AİHM, işverenin iş sözleşmesinin eki niteliğindeki işyeri yönetmeliği, bilgi güvenliği taahhütnamesi, disiplin yönetmeliği ve seyahat yönetmeliği gibi metinlerle işçilerin internet ve kurumsal e-posta kullanımı konusunda yeterli düzeyde bilgilendirildiği ve bu düzenlemelerde kurumsal e-postaların kişisel amaçlarla kullanılmasının kesinlikle yasaklandığı ve bunların izlenebileceği konusunda başvurucu bilgilendirildiğinden[707]: "… başvuruculara kurumsal e-

704) Hendrickx, [2002], Workers Personal Data, s. 118.-119.
705) Bu konuya ilişkin son AİHM kararlarını incelediğimizde işverenin dijital izlemenin niteliği, içeriği ve kapsamı konusunda işçilerin önceden bilgilendirilmesi koşulunu yerine getirmesi kaydı ile dijital izleme yapabileceği ortaya çıkmaktadır. Bkz. AİHM, [GK], [2017], Bărbulescu v. Romanya kararı (Başvuru Numarası: 61496/08); AYM kararlarına baktığımızda, AYM'nin de AİHM kararlarına atıf yaparak işverenin aydınlatma yükümlülüğünü yerine getirmesi ve ölçülü olması kaydı ile dijital izleme yapabileceğine karar vermektedir. Bkz. AYM, E.Ü. kararı Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020; Aynı doğrultuda AYM, Ömür Kara ve Onursal Özbek kararı § 50; AYM, Fırat Gerçek kararı, Başvuru Numarası: 2019/25604, Karar Tarihi: 21.09.2022 https://www.resmigazete.gov.tr/eskiler/2022/11/20221115-5.pdf); Yargıtay kararlarında da bu yöndedir. Bkz. Yargıtay 22. Hukuk Dairesi, E. 2017/21857 K. 2019/9884 T. 7.5.2019 kararı.
706) AYM, Ömür Kara ve Onursal Özbek kararı § 65. Kararın tamamı için bkz. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/4825 (Erişim Tarihi: 13.01.2023).
707) Kübra Doğan Yenisey, Yargıtay'ın İş Hukuku ve Sosyal Güvenlik Hukuku Kararlarının Değerlendirilmesi 2016, On İki Levha Yayıncılık, Ankara 01-02 Aralık, [2017], s. 508-509.

posta hesapları üzerinden gerçekleştirdikleri kişisel yazışmaların korunması konusunda makul bir beklenti içinde oldukları sonucuna ulaşılamaz" biçiminde karar vermiştir[708].

İş hukuku açısından işverenin dijital izleme hakkı, yönetim hakkının kaynağı olan iş sözleşmesinde ortaya çıkmaktadır. Ayrıca işverenin yönetim hakkının kullanım biçiminin TBK m. 399'da somutlaştırıldığını belirtmek gerekir. Bu kapsamda işverenin işyerine ilişkin kararlar alması, genel düzenlemeler yapması ve özel talimatlar vermesi aynı zamanda dijital izlemenin de dayanağını somutlaştırmaktadır.

Dijital izlemenin sağladığı verimlilik avantajları, geniş çaplı denetim imkanı, görece olarak daha ucuz ve kolay uygulanması bu tür uygulamaların işyerinde kullanımı yaygınlaşmaktadır. Bunun iş ilişkisinde çalışma süresi, işyeri ve özel hayat alanı arasındaki sınırı bulanıklaştırıldığı ve dijital izlemenin işçilerin menfaatlerini zedeleyecek biçimde kullanılma olasılığını artırdığı belirtilmelidir. Özel hayatın gizliliğinin ve kişisel verilerin korunmasına ilişkin normların ortaya çıkmasına öncülük eden Anglo Amerikan ve Kıta Avrupası ülkelerinde işyerlerinin giderek daha fazla kişisel veriye dayalı yapay zeka uygulamalarını kullandığı ve işyerlerinin bu teknolojilere bağımlılığın arttığını söyleyebiliriz. Ne var ki, bu ülkelerde kişisel verileri korumaya yönelik politikalarda işveren ile işçiler arasında bir tercih yapmamış, temel ilkeler kapsamında kişisel verilerin işlenmesi, işçilerin işlenen verileri ile ilgili rızalarının alınması ve bilgilendirilmeleri yeterli görülmüştür.

Eklemek gerekir ki, günümüz bilişim dünyasında işçilerin diğer bireyler gibi sosyal medyada kişisel verilerini ifşa etmesi, farklı mecralarda sosyal medya

708) AYM, Ömür Kara ve Onursal Özbek kararı, § 66 ve 68; Ömer Ekmekçi/H. Burak Gemalmaz/Volkan Aslan/H. Hilal Yılmaz, Anayasa Mahkemesine Bireysel Başvurunun Temel Esasları ve İş ve Sosyal Güvenlik Hukukuna İlişkin Kararlar; On İki Levha Yayıncılık, İstanbul, [2022], s. 95-96.

kullanımları, diğer insanlarla bağlantı halinde olma hakları dikkate alındığında aslında özel hayatın gizliliğinin ve kişisel verilerin korunması hakkının bireyin nasıl yaşayacağına ve hangi verilerini paylaşacağına karar verme hakkı kapsamında ele alınması ve bunların korunmasına yönelik düzenlemelerin bu esaslar dikkate alınarak gerçekleştirilmesi gerekliliğini ortaya çıkarmaktadır[709].

Öte yandan işveren açısından bakıldığında dijitalleşmenin yaygınlaşması maddi olmayan mülkiyet haklarının riske girmesi ve ticari sırların ifşa edilmesi böylelikle işverenin haklarının tehlikeye girmesi ihtimalini artırmıştır. Yine suç unsuru taşıyan e-posta ve internet kullanımı, diğer işçiler üzerinde zorbalık işveren açısından bir risk ortaya çıkarmaktadır. Bu itibarla işçinin özel hayat alanına taşmayan, kişisel verilerinin iş ilişkisiyle sınırlandırıldığı bir çalışma ortamının kurulması, işverenin işyerine ilişkin hakları ile işçinin bu hakları yönünden adil bir dengenin kurulacağı mekanizmaların geliştirilmesi önemlidir.

Sonuç olarak gelişen bilişim sistem ve uygulamaları, işverenin hak ve yükümlülükleri kapsamında çeşitlenen dijital izleme uygulamaları işverenlerin hakları ile işçilerin kişilik hakkına ilişkin menfaatleri arasındaki çatışmayı daha görünür kılmaktadır[710]. Açıklandığı üzere işverenin işyerine ilişkin hakları, ekonomik ve ticari riskin işveren üzerinde olması, mülkiyet hakkı, suçun önlenmesi kapsamında dijital izleme uygulamaları kullanması bilişim sistem ve uygulamalarıyla iç içe geçmiş günümüz işyerleri için önemli bir ihtiyaçtır. Öte yandan iş ilişkisindeki güç dengesi açısından rıza ve bilgilendirme esaslı düzenlemeler öngören KVK hukuku düzenlemelerinin ve GVKT m. 88'deki özel düzenlemenin işvereninin dijital izlemeye ilişkin menfaatleri ile işçilerin özel

709) Anayasa Mahkemesi, kamu görevlisi olan başvurucunun sosyal medya hesabı üzerinde yaptığı bir paylaşım sebebiyle disiplin cezası almasını değerlendirdiği kararında, konuyu Anayasa m. 13 düzenlemesinde yer alan ölçülülük ve m. 26 düzenlemesindeki ifade özgürlüğü kapsamında değerlendirmiş ve ilgili kişiye gerçekleştirilen müdahalenin demokratik toplum düzeninin gereklerine uygun olup olmadığı vurgusunu yapmıştır. AYM, Lale Çalıkoğlu kararı, Başvuru No: 2018/36354, Karar Tarihi. 18.10.2022, Resmi Gazete'nin 17.11.2022 tarihli nüshasında yayımlanmıştır. Karar detayı için bkz. https://www.resmigazete.gov.tr/eskiler/2022/11/20221117-5.pdf

710) Finkin, [2015], Privacy, s. 349.

hayatları ile kişisel verilerine ilişkin haklarını çepeçevre düzenlendiğini söylemek güçtür. Bu itibarla salt iş ilişkisine ilişkin düzenlemeler getiren normlar değil, ilgili başlıklarda incelendiği üzere KVKK m. 4 ve 5'te ve GVKT m. 5 ve 6'da öngörülen ilkeler, m. 22'deki profil oluşturma ve m. 35'teki veri koruma etki değerlemesi gibi düzenlemelerin iş ilişkisinde dijital izleme uygulamaları vasıtasıyla kişisel veri işlenirken dikkate alınması gerekmektedir[711].

§ 6. DİJİTAL İZLEMENİN HUKUKA UYGUNLUK ÖLÇÜTLERİ

İş ilişkisinde kullanılan dijital izleme uygulamaları işçinin kişisel verilerini otomatik biçimde işler, analize olanak tanır, aktarır ve diğer veri işleme faaliyetlerine konu edebilir. Veri sorumlusu işveren tarafından dijital izleme uygulamaları vasıtasıyla işlenen işçinin kişisel verilerinin hukuka uygunluğu[712] genel olarak bu paragrafta incelemeye konu edilen hukuki ilke ve usullere uygun bir kişisel veri işleme faaliyetinin bulunmasına bağlıdır. Bu başlıkta iş ilişkisinde dijital izleme uygulamaları vasıtasıyla kişisel veri işlenmesi durumunda da uygulama alanı bulan ve kişisel veri işlenmesini belirli şartlara ve yükümlülüklere bağlayan hukuki düzenlemeler ele alınacaktır.

I. İşçinin Kişisel Verilerinin Korunması: Borçlar Kanunu m. 419 – Kişisel Veri Koruma Hukuku İlişkisi

KVK hukukumuzda iş ilişkisi özelinde bir düzenlemeye yer verilmemiş, kişisel verilerin korunmasında verisi işlenen ilgili gerçek kişi esas alınmıştır. KVK hukuku dışında "işçinin kişiliğin korunması" üst başlığında TBK m. 419'da "kişisel verilerin kullanılmasında" başlığıyla işçinin kişisel verilerinin işlenmesine ilişkin bir özel düzenleme öngörülmüştür[713]. TBK m. 419'da doğrudan işçinin kişisel

711) Bkz. § 9.
712) Kişisel verilerin işlenmesinin hukuka uygunluk değerlendirmesi için bkz. § 6. II. 3. a.
713) 818 sayılı BK'da yer alamayan maddenin gerekçesinde; "Maddenin birinci fıkrasında, teknolojik gelişmeler sonucu günlük yaşantının bir parçası hâline gelen ve bilgisayar ortamında saklanabilen verilerin kullanılması konusunda işçinin korunması amacıyla bazı sınırlamalar

verilerinin korunması düzenlenmiş ve özel kanun hükümleri saklı tutularak işçiye ait kişisel verilerin ancak işçinin "işe yatkınlığıyla" ilgili olduğu veya "iş sözleşmesinin ifası için zorunlu olduğu" ölçüde "kullanılabileceği" hüküm altına alınmıştır[714]. Genel bir kanunda özel nitelikte bir düzenleme olduğundan bu madde sadece TBK kapsamındaki iş ilişkilerinde değil, İş Kanunu'nun kapsamına giren iş ilişkilerinde de uygulama alanı bulur[715]. Dahası TBK m. 419/1 işçinin kişisel verilerinin işlenmesini "ancak" iş ilişkisiyle ilgili olma koşuluna bağlaması[716] dikkate alındığında işçi verilerinin başka amaçlarla işlenmesine sınırlama getirmektedir[717]. Maddede yer alan "işe yatkınlık" kavramı; işe uygun olma, iş için gerekli beceri, yetenek ve kapasitede olma durumunu ifade etmektedir[718]. Dolayısıyla TBK m. 419/1 işverene, işçinin performansı ve verimiyle ilgili verileri

---

yapılmıştır. Buna göre, işveren, işçiye ait kişisel verileri ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Maddenin ikinci fıkrasında ise, özel kanun hükümlerinin saklı olduğu belirtilmektedir." biçiminde yeterince açıklık içermeyen bir gerekçeye yer verilmiştir.

714) İsviçre Borçlar Kanunu m. 328b'nin iç hukukumuza aktarılması olan bu düzenleme, kaynak kanunda "verilerin işlenmesi" anlamına gelen bir ifade yer almaktadır. Ayrıca TBK m. 419/2'nin karşılığı olan İsviçre Borçlar Kanunu m. 328b'nin ikinci cümlesi: "Bundan başka 19 Haziran 1992 tarihli Federal Veri Koruma Kanunu hükümleri uygulanır." biçimindedir (1 Eylül 2023'te yürürlüğe giren değişiklikle cümle: "Diğer tüm hususlarda, 25 Eylül 2020 tarihli Veri Koruma Kanunu'nun hükümleri geçerlidir" biçimini aldı).TBK'nın hazırlandığı tarihte KVKK yürürlükte olmadığından TBK m. 419/2'den bunun anlaşılması gerekir ve işçilerin kişisel verilerinin işlenmesinde özel kanun olarak 6698 sayılı KVKK dikkate alınmalıdır. Sevimli, [2011], TBK Madde 419, s. 134. TBK Tasarısında 418. madde olarak gerekçesi yazılan m. 419'un gerekçesinde günlük yaşantının bir parçası haline gelen teknolojik gelişmelerin, bilgisayar ortamında saklanan verilerin kullanılmasına ilişkin bazı sınırlamalar getirildiği belirtilmiştir. Maddenin düzenlenmesinde İsviçre Borçlar Kanunu'nun 428b maddesi esas alınmıştır.

715) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 19; Tunçomağ/Centel, [2018], İş Hukukunun Esasları, s. 23; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 60; Düzenleme boşluklarının nasıl doldurulacağı ve TBK'nın iş hukuku ile ilişkisi için bkz. Süzek, [2019], İş Hukuku, s. 37-38.

716) Doktrinde, TBK m. 419'un öngördüğü ölçütlere uygun işçinin verilerinin işlenmemesinin, diğer veri işleme şartlarının varlığı halinde dahi (KVKK m. 5/2) veri işlemenin hukuka uygun olmayacağı savunulmuştur. Bkz. Yeliz Bozkurt Gümrükçüoğlu, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu", İş Hukukunda Yeni Yaklaşımlar (Ed. Kübra Doğan Yenisey/Seda Ergüneş Emrağ), Beta Yayınevi, İstanbul, [2017], s. 36-37.

717) Sevimli, TBK m. 419/1'de yer alan "ancak" kelimesinin diğer veri işleme şartlarının (üstün yarar vb.) ve açık rızanın uygulama alanını oldukça daralttığı görüşündedir. Sevimli, [2011], TBK Madde 419, s. 135.

718) Sevimli, [2011], TBK Madde 419, s. 120-139; Okur, yetkinlik kavramından ne anlaşılması gerektiğini, mesleki nitelikler ve kişisel nitelikler olarak ikiye ayırmaktadır. Mesleki niteliklerde işçinin dil bilgisi, eğitim düzeyi, genel ve mesleki eğitim düzeyi gibi bilgiler yer alırken, kişisel niteliklerde işçinin iletişim yeteneği gibi veriler yer almaktadır. Okur, [2013], Elektronik Gözetleme, s. 80.

işleyebilme ve işçinin özel hayatı ile kişisel verileri üzerinde keyfi tasarruflarda bulunamama açısından bir sınırlama getirmektedir[719].

Fıkrada yer alan "iş sözleşmesinin ifası için zorunlu olma" koşulu ise, iş ilişkisinin yönetimsel boyutunu ilgilendiren verilerin işlenmesiyle ilgilidir[720]. Örneğin tehlikeli sınıfta faaliyet gösteren bir işyerinde işe girişte işçilere sağlık testlerinin yapılması, işçilerden sağlık raporu ve sabıka kaydı istenmesi iş sözleşmesinin kurulması için gereklidir. Ayrıca işyeri güvenliğinin sağlanması için dijital izleme uygulaması kullanılması, işçilerin İSG kurallarına uygun iş gördüklerini denetlemek için dijital izleme uygulamaları kullanılması iş sözleşmesinin ifası için zorunlu veri işleme biçimleridir.

Öte yandan fıkrada yer alan "kullanabilir" sözcüğü ile kişisel verilerin "işlemesinin" kast edilip edilmediği belirsizdir. Zira, KVKK'da yer alan "işleme" kavramı kişisel verilerin elde edilmesinden imhasına kadar geçen sürede; elde etme, kaydetme, depolama, kopyalama, güncelleme, aktarma gibi veri üzerinde gerçekleştirilen tüm işlemleri ifade etmektedir. Kullanma kavramı ise daha dar anlamlı bir sözcük olarak işleme süreçlerinden birisi olan verinin elde edilmesi aşamasını kapsadığı izlenimi bırakmaktadır[721].

TBK m. 419/1 işçinin kişisel verilerinin işlenmesi açısından özel bir hüküm niteliğindedir. Kanaatimizce bu hükmün özel hüküm niteliğinde olması bu maddenin KVKK hükümleriyle birlikte uygulanmasının önünde engel değildir. Dahası birlikte uygulama, özel kanun düzenlemelerini saklı tutan TBK m. 419/2, KVKK'nın gerçek kişi esas alınarak düzenlenmesi ve kaynak kanundaki düzenlemede söz konusu fıkranın yerini alan atıf birlikte değerlendirildiğinde ulaşılması gereken sonuçtur. Belirtmek gerekir ki, TBK m. 419/1 işçinin verilerinin işlenmesi açısından bir sınırlama ve ölçüt ortaya koymakta, KVKK'da ise kişisel

719) Sevimli, [2011], TBK Madde 419, s. 134.
720) Okur, [2013], Elektronik Gözetleme, s. 80.
721) Sevimli, [2011], TBK Madde 419, s. 134.

verileri korunacak ve kanun kapsamında değerlendirilecek "ilgili kişi" kişisel verileri işlenen "gerçek kişi" olarak tanımlanmaktadır. İş hukuku açısından ancak gerçek kişi olabilen işçinin kişisel verileri işlendiğinde TBK m. 419'un ortaya koymuş olduğu iki ölçüt olan "işe yatkınlık" ve "iş sözleşmesinin ifası için zorunlu olduğu ölçüde" dikkate alınmalıdır. Öte yandan, TBK 419'da KVK hukukunun genel ilkeleri, aydınlatma yükümlülüğü, veri işleme şartları, verilerin aktarılma koşulları, özel nitelikli verilerin işlenme şartları, teknik ve idari tedbirler alma gibi düzenlemeler bulunmamaktadır. Sadece TBK m. 419/1 düzenlemesinden hareketle gerçekleştirilecek bir sınırlama işçiyi kişisel veri korumanın bu önemli koruma enstrümanlarının dışına çıkaracaktır. Eklemek gerekir ki, TBK m. 419'da işçinin kişisel verilerinin korunmasının hedeflendiği dikkate alındığında bu düzenlemeden sadece veri işleme süreçlerinin birisini (kullanabilir)[722] esas aldığını ve KVKK'yı dışladığını ileri sürmek maddenin düzenlenme amacıyla da örtüşmemektedir.

Belirtildiği üzere, TBK m. 419/2'de saklı tutulan özel kanundan KVKK'nın anlaşılması gerektiğinden işçiler açısından bu madde KVKK düzenlemeleriyle birlikte uygulama alanı bulur. Bu itibarla işçilerin kişisel verilerinin işlenmesinde, KVKK m. 4'te yer alan KVK hukukuna ilişkin şemsiye ilke niteliğinde olan genel ilkelerin, aydınlatma yükümlülüğüne ilişkin düzenlemelerin ve diğer kişisel veri koruma hükümlerinin dikkate alınması gerekmektedir[723].

Kanaatimizce KVKK yürürlüğe girdikten sonra TBK m. 419/1 açısından işçi verisini işlemede öngörülen iki sınırlandırmaya ilişkin olan tartışmalar önemini yitirmiştir. Zira, TBK m. 419/1'de işçinin kişisel verilerinin "işe yatkınlık" ve "iş sözleşmesinin ifası için zorunlu olduğu ölçüde işlenmesini" öngörmesi aynı

722) Okur, [2013], Elektronik Gözetleme, s. 77; Sevimli, [2011], TBK Madde 419, s. 134-135; TBK m. 419'a kaynaklık eden İsviçre Borçlar Kanunu m. 328b maddesinde "verilerin işlenmesi" kavramı kullanılmıştır.

723) Alpagut, [2019], Kamera Gözetlemesi, s. 309; Ulaş Baysal, "İşçiye Ait Taşınabilir İletişim Cihazlarının İş Amaçlı Kullanılması", Sicil İş Hukuku, S. 40, [2018], s. 72; A. Eda Manav, "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, S.2, [2015], s. 227-228, (Manav, [2015], Kişisel Veriler); Gürsel, [2016], İşçinin Kişisel Verileri, s. 401; Küzeci, [2020], Kişisel Veriler, s.393; Sevimli, [2006], Özel Yaşam, s.203.

zamanda 6698 sayılı KVKK m. 4/2-ç bendinde düzenlenmiş genel ilkelerden birisi olan "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesinin iş ilişkisi açısından somutlaşmış halidir[724]. Dahası KVKK m. 4/2-a bendi: "hukuka ve dürüstlük kurallarına uygun olma" ve 4/2-ç bendi: "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine uygunluk denetimi gerçekleştirmektedir. "Hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde" ifadesi ve KVKK m. 5/2-c bendinde düzenlenmiş olan "bir sözleşmenin kurulması veya ifasıyla 'doğrudan doğruya'[725] ilgili olması, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" kişisel veri işleme şartı ise, TBK m. 419/1'de öngörülen işçi verisini işlemenin ikinci koşulu olan "iş sözleşmesinin ifası için zorunlu olduğu ölçüde" ifadesiyle özdeş düzenlemedir[726].

Bu yönde yorum yapılması aynı zamanda TBK m. 419'un kaynak düzenlemesi olan İsviçre Borçlar Kanunu m. 328b düzenlemesinin arka planındaki veri korumaya ilişkin düzenlemelerin de bir gereğidir. Zira, 1992 tarihli İsviçre Veri Koruma Kanunu'nda AB 95/46 sayılı Direktif düzeyinde düzenlemeler yer almıyordu. Yeni İsviçre Veri Koruma Kanunu'nda, KVKK m. 5/2-c bendinde yer alan "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması" biçimindeki düzenlemenin "doğrudan doğruya" hükmü yer almamaktadır[727]. Ülke KVK hukukumuz açısından bu hüküm kapsamında hareket edildiğinde TBK m.

724) Alpagut, [2019], Kamera Gözetlemesi, s. 308-309.
725) KVKK'ya kaynaklık eden 95/46 sayılı Direktif'te de "doğrudan doğruya" sınırlandırması bulunmamaktadır. Bu hususun KVKK'da daha dar kaleme alındığını Yücedağ şu şekilde değerlendirmiştir: "KVKK m. 5(2)(c) bendinde düzenlenmiş olan hukuka uygunluk sebebi 95/45/AT sayılı Yönerge m. 7(b) bendinde düzenlenmiş olan hukuka uygunluk sebebine karşılık gelmektedir. Ancak KVKK m. 5 hükmündeki hukuka uygunluk sebebi, Yönerge'deki hükme nazaran daha dar kaleme alınmıştır. Yönerge'deki hükme göre sadece bir sözleşmenin ifası ile ilişki olma yeterlidir. Bu ilişkinin doğrudan doğruya olması gerekli değildir. Sözleşmenin ifası ya da kurulması ile doğrudan doğruya ilişki olma, o sözleşmenin kurulması ya da ifası için zorunlu olan bilgileri ifade eder." Bkz. Nafiye Yücedağ, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İÜHFM 2017, C. LXXV, S. 2, s. 777.
726) Alpagut, [2019], Kamera Gözetlemesi, s. 309-310; Canan Ünal, "İş Sözleşmesinin Kurulmasında Sağlığa İlişkin Veriler", İş Hukukunda Genç Yaklaşımlar III, (Ed. Prof. Dr. Tankut Centel), On İki Levha, [2018], s. 268-269.
727) Bkz. İsviçre Veri Koruma Kanunu, https://www.fedlex.admin.ch/eli/oc/2022/491/de Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), (Erişim Tarihi: 04.12.2023).

419/1'in öngördüğü iki koşul bulunmasa dahi KVKK m. 4/2-ç bendi ile KVKK m. 5/2-c bendi hükmü kapsamında aynı sonuca ulaşmak mümkündür. Bu itibarla İsviçre İş Hukuku'nda işçi verisinin korunması için belirleyici bir rolü bulunan m. 328b düzenlemesi, KVKK'da anılan özdeş düzenlemelerin bulunması sebebiyle Türk İş Hukuku için TBK m. 419 aynı düzeyde bir belirleyiciliğe sahip değildir.

Kanaatimizce iş ilişkisi özelinde düzenlemelerin KVKK'da yer almaması bir eksiklik olmakla birlikte kanunda gerçek kişi esas alınarak düzenleme yapılması tüm KVKK hükümlerin iş ilişkisi için uygulanır hale getirmektedir. Ayrıca bu yorum yukarıda ele alındığı üzere özel kanun düzenlemelerini saklı tutan TBK m. 419/2 düzenlemesiyle örtüşmektedir. Dahası işçinin verileri gibi ciddi bir konuyu tek bir hükümle düzenlemek ve korumak olanaklı olmadığından ve bu şekilde hareket etmek TBK m. 419 hükmünün işçinin kişisel verilerini, kişiliğini koruma amacıyla da bağdaşmayacağından özel kanun olan KVKK'nın hükümlerinin dikkate alınması gerekmektedir[728].

Gelinen aşamada, GVKT ile uyumu sağlamak için İsviçre Federal Veri Koruma Kanunu'nda değişiklikler yapıldı ve bu değişiklikler 1 Eylül 2023'te yürürlüğe girdi. Değişikliklerden birisi de TBK m. 419'a kaynaklık eden İsviçre Borçlar Kanunu'nun 328b hükmünün son cümlesinde gerçekleştirildi ve 1 Eylül 2023 itibariyle yürürlüğe giren madde: "İşveren, çalışana ilişkin verileri, yalnızca bu verilerin çalışanın işe uygunluğuyla ilgili olduğu veya iş sözleşmesinin ifası için gerekli olduğu ölçüde işleyebilir. Diğer tüm hususlarda, 25 Eylül 2020 tarihli Veri Koruma Kanunu'nun hükümleri geçerlidir[729]" biçimini aldı. İsviçre'deki iş ilişkisi için m. 328b düzenlemesinin getirdiği iki ölçüt önemli sınırlamalar olarak görülebilir. Hukukumuz açısından ise, az yukarıda açıkladığımız üzere KVKK'nın değinilen maddelerinden hareketle TBK m. 419/1 ile aynı sonuca ulaşmak mümkündür. İsviçre Federal Mahkemesi m. 328b hükmü kapsamında vermiş

728) Okur, [2011], İşçinin Kişisel Verileri, s. 378; Sevimli, [2011], TBK Madde 419, s. 135.
729) https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en#fn-d8e8681 (Erişim Tarihi: 03.12.2023).

olduğu kararlarda m. 328b'nin işçinin kişisel verilerini işlemede bir amaç ve orantılılık sınırlaması getirdiği, "işe uygunluk" veya "iş sözleşmesinin ifası için gerekli olmadığı" durumlarda veri işlemenin hukuka aykırı olduğuna karara vermektedir[730].

Federal Mahkeme iş ilişkisinde dijital izlemeyle ilgili 2021'de verdiği bir kararda[731] işverenin, işçinin kullanımına tahsis ettiği telefondaki ve dizüstü bilgisayarındaki verilere erişemeyeceğini, bunların üçüncü kişilerle paylaşılmasının kişilik haklarının ihlali olacağına karar vermiştir. Federal Mahkeme bu kararda m. 328b düzenlemesini uygulamış ve ilk defa Veri Koruma Kanunu'nun genel ilkelerinden birisine atıf yaparak işverenin 1992 tarihli Federal Veri Koruma Kanunu[732] m. 4/2 hükmünde öngörülen iyiniyet ve orantılılığın bulunması durumunda veri işleyebileceğine karar vermiştir[733]. Başka bir söylemle İsviçre Federal Mahkemesi bu kararında m. 328b ile Federal Veri Koruma Kanunu

730) İsviçre Federal Mahkemesi, 4A_518/2020, § 4.2.4, 25 Ağustos 2021 tarihli kararı. https://www.bger.ch/ext/eurospider/live/de/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F25-08-2021-4A_518-2020&lang=de&type=show_document&zoom=YES& (Erişim Tarihi: 05.12.2023).

731) İsviçre Federal Mahkemesi, 4A_518/2020 sayılı 25 Ağustos 2021 tarihli Kararda: "İşveren, işçinin e-postalarına ve mesajlarına yalnızca yaklaşan mahkeme işlemlerine hazırlanmak, yani işçinin cinsel taciz davranışını kanıtlamak ve işçinin fazla mesai yapıp yapmadığını doğrulamak amacıyla eriştiğini savunmuştur. Federal Mahkeme, iş ilişkisine ilişkin mahkeme işlemleri öncesinde delillerin toplanmasının Borçlar Kanunu m. 328b kapsamına girdiğini ve prensip olarak bu işlemin yasal olduğunu tespit etmiştir. İşveren ayrıca, işyeri iç düzenlemelerinin şirket bilgisayarları ve cep telefonlarının yalnızca iş amacıyla kullanılması gerektiğini öngörmesi nedeniyle söz konusu mesajlara erişme hakkına sahip olduğunu savunmuştur. Federal Mahkeme, işverenin bu tür elektronik cihazların özel kullanımına tolerans göstermesi nedeniyle (işçinin işverene teslim etmeden önce özel verilerini şirket telefonundan silmesinin istemesiyle kanıtlanmıştır), sadece iş amaçla kullanımdan bahsedilmeyeceğini tespit etmiştir. Federal Mahkeme her halükarda, işverenin işçinin iş performansına ilişkin verileri diğer işçileri sorgulamak ve/veya mahkeme işlemlerinde delil olarak göstermek gibi daha az müdahaleci yöntemlerle elde etmesinin mümkün olduğu durumlarda, işverenin mahkeme sürecinde kendini savunma konusundaki menfaatleri, işçinin menfaatlerinden üstün tutulamaz veya işçinin özel hayatına müdahaleyi haklı kılamayacağına karar vermiştir. Federal Mahkeme bu durumlarda veri işlenmesi orantısız olduğunu ve işçinin manevi tazminat alma hakkı doğacağına karar vermiştir. Bu davada, işçiye 5.000-CHF tazminat ödenmesine karar verilmiştir. Son olarak federal yargıçlar, işçinin özel mesajlarının "yasa dışı olarak işlenmesi" (elde edilmesi) durumunda bu delillerin mahkemede kullanılamayacağına ve bu nedenle yargılama kapsamından çıkarılması gerektiğine karar vermiştir."

732) 1 Eylül 2023 tarihinde yürürlüğe giren Federal Veri Koruma Kanunu öncesinde yürürlükte olan 1992 tarihi Federal Veri Koruma Kanunu m. 4/2 "veri işlemenin iyi niyetle ve ölçülü yapılması" ilkesini düzenlemiştir. https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en

733) İsviçre Federal Mahkemesi, 4A_518/2020 Kararı, § 4.2.1. (Erişim Tarihi: 05.12.2023).

hükmünü birlikte uygulamıştır.

Önemle eklemek gerekir ki, TBK m. 419/1 sınırlamaları ve özdeş KVKK düzenlemeleri iş görüşmelerinden iş akdinin sonra ermesine kadar geçen tüm aşamalardaki kişisel veriler işlenirken uygulama imkanı bulan temel ilkeleri barındırmaktadır. İş görüşmesi süreci de bu aşamaların dışında görülemez. Bu sebeple işveren, işçi adaylarının verilerini işlemede ve işçi adaylarına yönelik dijital izleme uygulamalarında hukuka uygun davranmakla yükümlüdür[734]. Son olarak KVKK'nın kapsamını düzenleyen m. 2'de yer alan bir diğer sınırlandırma olan, "herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen" ifadesine, KVK Kurumu yayımladığı Uygulama Rehberinde kişisel verilerin "herhangi bir kritere göre bir kağıda kaydedilmesi" biçiminde geniş bir yorum geliştirmiştir[735]. Bu yorum bir kağıda belirli bir kritere göre kişisel veri yazmak veya bir klasöre kişisel veri içeren belgeleri eklemek de veri kayıt parçası olarak nitelendirmeye olanak verdiğinden, TBK m. 419/1'in işçinin kişisel verilerini korumada kapsayıcılık açısından KVKK'dan daha geniş bir uygulama alanı ortaya çıkardığını söylemek güçtür.

II. Kişisel Veri Koruma Hukuku Kapsamında Dijital İzlemenin Sınırları

Kişisel verileri koruma mevzuatı bir gerçek kişiyi belirli veya belirlenebilir hale getiren her türlü veri işleme faaliyetinin belirli ilke ve şartlar kapsamında

734) Sevimli, [2006], Özel Yaşam, s. 146; Ünal, [2018], Sağlığa İlişkin Veriler, s. 269.
735) KVK Kurumu, Uygulama Rehberinde bu hususu: "Kanunda kişisel verilerin kısmen veya tamamen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi bakımından da herhangi bir fark öngörülmemiştir. Bu doğrultuda kişisel verilere ulaşımı kolaylaştıracak şekilde, belirli bir kritere göre yapılandırılmış her türlü sistem Kanun kapsamında değerlendirilecektir… Dolayısıyla Kanun otomatik olmayan yollarla işlenen verileri tamamen kapsam dışında bırakmamaktadır. Burada önemli olan otomatik olmayan yollarla işlenen verilerin veri kayıt sisteminin parçası olup olmadığıdır. Örneğin, herhangi bir kritere bağlı olmaksızın kişilerin ad ve soyadlarının rastgele bir şekilde kağıtta yer alması hali Kanun kapsamına girmemekle birlikte, söz konusu isimlerin belirli bir kritere göre bir kağıda kaydedilmesi halinde, bu veri kaydı Kanun kapsamında değerlendirilecektir" biçiminde ifade etmiştir. KVK Kurumu, [2019], Uygulama Rehberi, s. 37-38; Veri Kayıt sistemi KVKK m. 3/1-h bendinde: "Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini" biçiminde tanımlanmıştır.

gerçekleştirilmesini zorunlu kılan, iş ilişkisi açısından veri sorumlusu işverene veri işleme faaliyetinde yükümlülükler yükleyen çeşitli sınırlandırıcı enstrümanlar (aydınlatma yükümlülüğü, KVK Kurumu vb.) ve hükümler içermektedir. Bu başlıkta KVK hukukunun dijital izlemeyi sınırlandıran ve veri sorumlusu işverenin dijital izleme uygulamalarıyla veri işleme faaliyetine hukuka uygunluk nitelendirmesi yapmak için gerekli olan ölçütler ele alınacaktır.

1. Kişisel Veri ve Kişisel Verinin İşlenmesi Kavramı

KVKK'da işçi ve işveren için özel bir düzenleme yer almamakla birlikte gerek ulusal gerekse uluslararası hukuki düzenlemelerde "kişisel veri" bir gerçek kişiyi belirli veya belirlenebilir hale getiren her türlü bilgi (KVKK m. 3/1-d)[736] tanımı kapsamında hüküm altına alındığından işverenler, işçinin verisini işledikleri veri işleme faaliyetlerinde KVKK'da öngörülmüş olan hükümlere uygun davranmakla yükümlüdürler. Kanun'da gerçekleştirilen tanımda bir verinin kişisel veri olarak nitelendirilmesinin unsurları ortaya çıkmaktadır. Buna göre bir verinin kişisel veri olarak nitelendirilebilmesi için; a) bir gerçek kişiye ait, b) bir bilginin bulunması ve c) bu bilgiyle gerçek kişinin belirli veya belirlenebilir hale getirilmesi gerekmektedir. Bu unsurlar bulunduğu sürece bir bilginin kişisel veri olarak nitelendirilmesi için nesnel veya öznel olması, gizli veya aleni olması, doğru veya yanlış olması, dijital izlemeyle veya başka bir vasıta ile elde edilmesi ve bilimsel ölçütler barındırmaması bir önem arz etmez[737].

---

736) KVK Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu Rehberi, s. 17-18; Küzeci, [2020], Kişisel Veriler, s. 10; Avrupa Konseyi'nin 108 sayılı Sözleşmesi m. 2/ a; AB 95/46/EC sayılı Yönerge m. 2/a; OECD Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler m. 1/b; AYM, E. 2010/40, K. 2012/8, 19.01.2012, Resmi Gazete, 06.03.2013/ 28579; 95/46/EC sayılı Direktif'in yerini almış olan 2016/679 sayılı GVKT m. 4/1'de kişisel veri: "tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir (veri sahibi); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir" biçiminde tanımlanmıştır.

737) Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, s. 6-9,https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (Erişim Tarihi: 15.10.2022); Küzeci, [2020], Kişisel Veriler, s. 10-12.

"Kişisel verilerin işlenmesi" ise, kişisel verilerin elde edilmesi ile imhası, silinmesi veya anonimleştirilmesi arasında geçen sürede elde etme, kaydetme, depolama, güncelleme, aktarma gibi veri üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir[738]. GVKT m. 4/2'de gerçekleştirilen tanım KVKK'da gerçekleştirilen tanımla aynı yöndedir. 108 sayılı Sözleşmesi'nde ise verilerin işlenmesi faaliyeti, GVKT düzenlemesinden farklı olarak otomatik işleme ile sınırlı tutulmuştur. Belirtmek gerekir ki KVK hukuku düzenlemeleri kişisel verilerin işlenmesini yasaklamaz; bu düzenlemeler temelde veri sorumlularının kişisel veri işlenmesini belirli ilkeler kapsamında gerçekleştirmesini ve ilgili kişinin verileri üzerinde bir hakimiyet alanını oluşturmayı hedeflemektedir[739].

Kişisel veri işleme faaliyetinin KVKK kapsamında değerlendirilebilmesi için veri işlemenin otomatik sistemlerle (bilgisayar, işlemci bulunan cihazlar, telefon, algoritmalar) veya bir veri kayıt sisteminin parçası olması kaydı ile otomatik olmayan yollarla işlenmesi gerekmektedir[740]. Ayrıca kişisel veri koruma hakkının ortaya çıkabilmesi için verinin işlemeye konu edilmesi gerekmektedir. Ancak bu durumda kişinin verileri üzerindeki hakları gündeme gelir ve temel hak ve özgürlüklerini koruyucu düzenlemeler devreye girer[741].

Özellikle dijital izleme açısından gerçek kişiyi "belirlenebilir" hale getiren bilgiler önemlidir. Zira işyerinde bir işçinin kimliğini doğrudan işaret etmeyen fakat birkaç bilginin bir araya gelmesiyle veya bir grup bilgi ile ilişkilendirildiğinde bir işçinin tespit edilebilmesi halinde kişisel veri işlendiği kabul edilmelidir. Örneğin dijital izlemeyle elektronik iletişimin izlendiği bir uygulamada işlenen takma isim tek başına bir kişisel veri değildir, fakat bu takma ismin başka bir veri ile ilişkilendirildiğinde bir işçiyi belirlenebilir hale getirmesi durumunda kişisel veri

738) KVK Kurumu, [2019], Uygulama Rehberi, s. 53-54.
739) Okur, [2011], İşçinin Kişisel Verileri, s. 398.
740) KVK Kurumu, [2019], Uygulama Rehberi, s. 54.
741) Şimşek, [2008], Kişisel Verilerin Korunması, s. 4; Aydın Akgül, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Basım Yayım, İstanbul [2014], s. 77.

işleme faaliyetinin bulunduğu kabul edilmelidir[742].

Aynı husus işyerinde işçilerle gerçekleştirilen mülakatlar, performans değerlendirmeleri ve müşteri şikayetleri için de geçerlidir. Örneğin bir işyerinin müşteri hizmetleri departmanında çalışan işçilerin hafta sonu bir müşteriye vermiş oldukları cevaptan şikayetçi olan müşterinin bu birime ilişkin işverene göndermiş olduğu şikayet e-postası, o tarihte kimlerin çalıştığı ve kimin soruya cevap verdiği bilgileriyle ilişkilendirildiğinde bir işçiyi belirlenebilir hale getireceğinden gerçekleştirilen şikayet kaydında yer alan bilgiler de kişisel veridir. Aynı durum GPS ve benzeri konum izleme uygulamaları için de geçerlidir. Örneğin GPS, RFID veya Geofence gibi konum izleme imkanı veren dijital izleme uygulamalarının kayıt altına aldığı konuma dayalı bilgiler tek başına kişisel veri değildir. Bu veriler örneğin o tarihte satış için bölgede kim bulunduğu bilgisiyle eşleştirildiğinde veya aracın ilgili tarihte hangi işçide olduğu bilgisiyle birlikte değerlendirildiğinde bir gerçek kişi verisine ulaşılıyorsa, işlenen veri kişisel veri halini alır.

Kişisel veri tanımında "her türlü bilgi" ifadesi tercih edilerek geniş bir hareket alanı bırakılmıştır. Teknolojik gelişme hızı dikkate alındığında ve veri işleme türleri zamanla değişeceğinden bu biçimde geniş bir tanım yapılması isabetlidir. Zira teknolojik gelişmelere bağlı olarak kişiyi belirlenir hale getirecek veri parçacıkları da çeşitlenmektedir. Ayrıca ilk başta kişisel veri gibi görünmeyen bilgiler, başka bilgilerle ilişkilendirildiğinde bir gerçek kişiyi tanımlama potansiyeli taşıyabilir. Nitekim GVKT m. 4/1-a tanımı da bu yöndedir ve fıkranın devamında örneklerle nelerin kişisel veri olabileceği örneklendirilmiştir. Tanım kapsamında bir bilgi bir kişi doğrudan belirtebilir (belirteç) bunların en tipikleri isim-soyisim, kimlik bilgiler ve kişinin görüntüleri gibi doğrudan verilerden oluşmaktadır. Öte yandan bir bilgi bir kişiyi doğrudan belirtmez dolaylı olarak kişiyi belirlenebilir hale getirebilir[743]. Bu kişisel verilere ilgili kişinin telefon numarası, araç plakası,

742) Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 12; KVK Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu Rehberi, s. 18.
743) EU, [2018], Handbook, s. 89-91.

sosyal güvenlik numarası örnek gösterilebilir.

Ayrıca GVKT'deki tanım kapsamında, işlenen kişisel veriler, bir grup veri konusu kişi içinde diğer tüm kişilerden "farklı" ise, grup üyelerinin veya kimliği belirlenebilir bir veri öznesinin, henüz kimliği belirlenmemiş olmasına rağmen, işlenen veri tanımlanmış bir veri konusuyla ilgili olabilir[744]. Örneğin web sitelerinde çerez kullanımı[745] (cookies) tüketici alışkanlıklarını belirlemek ve davranışlarını yönlendirmek kadar işyerinde çalışan işçilerin ilgi alanlarını, çalışma alışkanlıklarını ve internet trafik izlerini tespit etmek için de kullanılmaktadır[746]. Aynı doğrultuda metadata verileri doğrudan kişisel veri olarak nitelendirilecek veriler barındırmamakla birlikte bu veri kümelerinde bir gerçek kişiyi, bir işçiyi belirlemek mümkündür. Bu itibarla kişisel veri tanımındaki "her türlü bilgi" ifadesi veri koruma otoritelerine ve yargıya olayı nitelendirmede hareket alanı bırakmamaktadır.

Anonim bir veri bulunuyorsa veya veri sonradan anonim hale getirilmişse[747] bu veride kişisel veri bulunmayacağından kişisel verileri koruma mevzuatı kapsamında bir yükümlülük doğmayacaktır. Zira anonim verilerde kişisel verideki anahtar bilgi çıkarıldığından, kalan veriyle bir kişiyi belirlemek veya belirlenebilir

744) Laura Bachnakova Rozenfeldova/Gabriela Dobrovicova, "The Analysis of the Application of Personal Data Protection Norms by Collaborative Platforms", EU and Comparative Law Issues and Challenges Series, Vol. 6, [2022], s. 647.

745) Çerezler (cookies) Web sitesinin doğru çalışması için zorunlu verilerin işlenmesine dayanabileceği gibi, ziyaretçinin kullanım alışkanlıklarını analiz etmeye, izlerini takip etmeye yönelik ticari ve analiz çerezleri biçiminde de olabilir. Çerezlere ilişkin düzenlemeler 12 Temmuz 2002 tarihli Avrupa Parlamentosu ve Konseyi'nin 2002/58/EC sayılı Direktifi'nde yer almıştır. Ülkemizde çerez kullanımına ilişkin bir düzenleme bulunmamasına rağmen KVK Kurumu, Haziran 2022'de yayımladığı "Çerez Uygulamaları Hakkında Rehber" ile çerez kullanımına KVKK kapsamında sınırlamalar getirmiştir. Şüphesiz bunun bu şekilde yapılması Kanun'da olmayan bir hususun düzenlenmesidir. Bu itibarla ülkemizde çerezleri de kapsayacak bir yasal düzenlemenin yapılması gereklidir. Çerez Uygulamaları Hakkında Rehber için bkz. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf (Erişim Tarihi: 15.10.2022).

746) Bachnakova - Rozenfeldova/Dobrovicova, [2022], Personal Data, s. 658.

747) Kişisel verinin anonim hale getirilmesi, işlenen verinin başka verilerle ilişkilendirilse, eşleştirilse dahi bir gerçek kişiyi belirlenebilir hale getirmeyecek hale getirilmesidir. KVK Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu Rehberi, s. 46.

hale getirmeye olanak yoktur[748]. Öte yandan uygulamada anonim hale getirmek ile veriyi şifrelemek birbiriyle karıştırılabilmektedir. Veriyi şifrelemek anonim hale getirmek değildir, zira veri üzerindeki şifre kaldırıldığında bir gerçek kişiyi belirlemek mümkün hale gelmektedir. Bu itibarla işyerinde dijital izlemenin şifrelenerek gerçekleştirilmesi işverenin yükümlülüğü açısından bir fark oluşturmayacaktır.

2. Özel Nitelikli Kişisel Veriler

Kural olarak özel nitelikli kişisel verilerin işlenmesi yasaktır[749]. Zira özel nitelikli kişisel verilerin başkaları tarafından bilinmesi halinde ilgili kişinin ayrımcılığa maruz kalmasına ve mağdur olmasına sebebiyet verebilir. Sınırlı sayıda belirlenmiş olan bu tür veriler kişisel veri mevzuatlarında özel nitelikli (hassas) kişisel veri olarak düzenlenmiş ve daha sıkı işlenme ve koruma şartlarına bağlanmıştır[750]. KVKK m. 6/1'de nelerin özel nitelikli kişisel veri olduğu sınırlı bir şekilde sayılmıştır. Bunlar, "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerinden" oluşmaktadır.

Özel nitelikli kişisel verilerin daha sıkı korunmasındaki amaç bu verilerin işlenmesi halinde ilgili kişi hakkında dezavantajlı durumları ortaya çıkarma olasılığıdır. Örneğin işçinin aslında bulaşıcı olmayan, fakat toplum tarafından bulaşıcı olduğu sanılan bir hastalığa yakalandığının işyerinde duyulması halinde tüm işçilerin hasta işçiden uzaklaşması, onunla bir araya gelmemesi, hatta işyerinden ayrılması için baskıya maruz kalması işçi için yıkıcı sonuçlar ortaya çıkarabilir. Bu sebeple işverenin özel nitelikli kişisel veri olan sağlık verilerinin

748) EU, [2018], Handbook, s. 94; KVK Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu Rehberi, s. 46-47.
749) Gürsel, [2016], İşçinin Kişisel Verileri, s. 167.
750) KVK Kurumu, [2019], Uygulama Rehberi, s. 80.

diğer işçilere ifşa etmemesi, bu verilere erişimi olan işçilerle veri gizliliği anlaşması yapması gerekmektedir[751].

Dijital izleme açısından önemli olan husus bir işçinin cinsel yönelimine ilişkin izler barındıran elektronik iletişim izlemesinde işlenen veriler, sendikalı işçilere yönelik geçekleştirilen dijital izleme uygulamaları, araç kullanım veya klavye basış tarzı biçimindeki davranışsal biyometrik verilerin işlenmesi durumunda özel nitelikli kişisel veri işleme faaliyeti olarak nitelendirileceğidir. Bu durumda veri sorumlusu işverenin Kanun'da öngörülen özel nitelikli kişisel veri işleme şartlarına ve bu verilerin korunmasına ilişkin KVK Kurulu tarafından yayımlanmış asgari teknik ve idari tedbirlere uygun bir veri işleme faaliyeti oluşturması zorunludur[752].

3. Dijital İzlemede Dikkate Alınacak Kişisel Veri Koruma Hukukunun Genel İlkeleri

KVKK'da düzenlenmiş olan genel ilkeler kişisel verilerin işlenmesinde yönlendirici şemsiye ilkeler olmaları sebebiyle KVK hukukunun temelini oluşturmaktadır[753]. Bu ilkeler aynı zamanda her türlü kişisel veri işleme faaliyeti için geçerli olduğundan, KVKK hükümlerinin yorumlanmasında yol gösterici büyük bir rol oynarlar. Kişisel verilerin işlenmesinde veri sorumlularının temelde nelere dikkat etmeleri gerektiği KVKK m. 4'te "genel ilkeler" başlığında düzenlenmiştir. Düzenlemeye göre kişisel veriler ancak 6698 sayılı KVKK ve diğer kanunlarda öngörülmüş olan usul ve esaslar dikkate alınarak işlenebilir. Kişisel

751) KVK Kurumu özel nitelikli kişisel verilerin işlenmesinde, veri sorumluları tarafından alınacak asgari tedbirlerle ilgili olarak 2018/10 KVK Kurul kararını yayımlamıştır. KVK Kurulu'nun "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" başlıklı Kişisel Verileri Koruma Kurulu'nun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı için bkz. https://www.kvkk.gov.tr/Icerik/4110/2018-10 (Erişim Tarihi: 16.10.2022).
752) KVK Kurul Kararı, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı. https://www.kvkk.gov.tr/Icerik/4110/2018-10 (Erişim Tarihi: 30.10.2022).
753) KVK Kurumu, [2019], Uygulama Rehberi, s. 63.

veriler işlenirken hukuka ve dürüstlük kuralına uyulmalı, işlenen verilerin doğru ve güncel olması sağlanmalı; belirli, açık ve meşru amaçlar için kişisel veri işlenmeli, işlenen kişisel veriler işleme amacıyla bağlantılı olmalıdır ve amaçla bağlantılı sınırlı ve ölçülü veri işlenmelidir. Bu başlıkta dijital izleme uygulamaları vasıtasıyla kişisel veri işlenmesinde dikkate alınması gereken genel ilkeler değerlendirmeye konu edilecektir.

a) Veri İşlemenin Hukuka ve Dürüstlük Kuralına Uygun Olması

Kanunlarda ve diğer hukuki metinlerde öngörülmüş olan düzenlemelere uygun kişisel veri işlenmesi zorunluluğu "hukuka ve dürüstlük kuralına uygun" kişisel veri işleme temel ilkesi ile somutlaşmaktadır. Hukuka ve dürüstlük kuralına uygunluk ilkesi kapsamında veri sorumlusu kişisel veri işlerken dürüstlük ilkesi kapsamında verisi işlenen ilgili kişinin menfaatlerini ve makul beklentilerini gözetmelidir[754]. KVKK m. 4/2-a bendinde dürüstlük ilkesine uygunluk "hukuka" uygunluk şartını da içermektedir. Hukuka ve dürüstlük kuralına uygun kişisel veri işleme genel ilkesi kapsayıcı bir düzenlemedir. Zira "hukuka uygun" ifadesine kanunlara uygunluk dahil olduğu gibi evrensel insan haklarına[755] ilişkin düzenlemelere ve evrensel hukuk ilkelerine uygun kişisel veri işlenmesi de dahildir[756].

Doktrinde bir görüş, "KVKK m. 5 ve m. 6 hükümlerinde düzenlenmiş olan hukuka uygunluk sebepleri, hukuka uygunluğun tespitinde dikkate alınmalı, KVKK'nın getirdiği diğer yükümlülüklere ve veri koruma düzenlemelerine aykırılıklar (aydınlatma yükümlülüğü, teknik tedbirler), bu genel ilke kapsamında değerlendirilmemelidir"[757] diğer bir görüş ise "veri işlemenin hukuka uygun kabul

754) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf (Erişim Tarihi: 18.10.2022).
755) Küzeci, [2020], Kişisel Veriler, s. 229.
756) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2.
757) Nafiye Yücedağ, "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", Kişisel Verileri Koruma Dergisi, C. 1, S. 1, [2019], s. 49; GVKT genel ilkeleri için aynı yönde

edilebilmesi için işleme faaliyetinin veri koruma kanununa ya da diğer yasal gereklilikleri ihlal etmeyecek şekilde gerçekleştirilmesine bağlıdır"[758] aynı yönde bir diğer görüşte kişisel verilerin hukuka uygun işlendiğinden bahsetmek için "kişisel verilerin işlenmesinde her aşamanın mevzuata ve sair hukuk kurallarına uygun biçimde gerçekleştirilmesi"[759] gerekmektedir. Kişisel verilerin hukuka uygun işlendiğinden bahsetmek için birincil ve ikincil mevzuata uygunluk gerektiği "kişisel verilerin hukuka uygun olarak işlenmesi, veri işleme surecinin tamamında birincil ve ikincil mevzuata uygun hareket edilmesini ifade eder"[760] biçiminde ileri sürülmüştür.

Kanaatimizce kişisel verilerin işlenmesinin hukuka uygunluk değerlendirmesini yaparken sadece genel ilkelere (KVKK m. 4) ve kişisel veri işleme şartlarına (KVKK m. 5 ve 6) uygunluğu yeterli görmek verisi işlenen ilgili kişinin bilgisi olmadan kişisel verilerinin işlenmesi sonucunu ortaya çıkarır. Bu sonucun KVK hukukunun amacına uymadığı açıktır. Nitekim, KVK Kurumu yayımladığı rehberlerde hukuka uygunluk için gerçekleştirdiği: "genel olarak hukuk normlarına ve evrensel hukuk ilkelerine uygunluktur. Hukuka uygunluğun kapsamı geniş olup, mevzuata uygunluk da buna dahildir" açıklaması dikkate alındığında Kurum'un yaklaşımının da bu yönde olduğu ortaya çıkmaktadır[761]. Dahası KVKK'nın genel ilkelerinin düzenlendiği m. 4/1 hükmü: "Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir" biçimindedir. Tüm bu hususlar birlikte değerlendirildiğinde veri işlemeyi hukuka uygun olarak niteleyebilmek için KVKK'da öngörülen usul ve esaslara (KVKK m. 4 ve 12 dahil olmak üzere aradaki tüm hükümlere ve bunlara dayanılarak düzenlenen ikincil mevzuata) uygun bir veri işleme faaliyetinin

---

değerlendirme, M. Serdar Çekin, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha Yayıncılık, İstanbul, [2020], s. 69-70.

758) Gürsel, [2016], İşçinin Kişisel Verileri, s. 220; A. Eda Manav Özdemir, "İşçinin İzlenmesi ve Gözetlenmesi", Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, (Ed. Kemal Şenocak), Yetkin Yayınları, Ankara, [2022], s. 884.

759) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 144; Küzeci, [2020], Kişisel Veriler, 228.

760) Baysal, [2023], Kişisel Verilerin İşlenmesi, s. 531.

761) KVK Kurumu, [2019], Uygulama Rehberi, s. 64.

gerçekleştirilmesi zorunludur[762].

GVKT m. 5'te "kişisel verilerin işlenmesine ilişkin ilkeler" düzenlenmiş ve m. 5/1-a'da kişisel verilerin hukuka uygun, adil ve şeffaf bir biçimde işleneceği kuralına yer verilmiştir. KVKK m. 4/2-a düzenlemesinde hukuka uygunluktan ne anlaşılması gerektiği tanımlanmadığından KVK Kurumu bu konuda bir rehber yayımlayarak temel ilkelere açıklık getirmeye çalışmıştır[763]. GVKT m. 5'te ve 6'da "hukuka uygun" işlemeden bahsedilmiş fakat bu kavrama ilişkin bir tanım yapılmamıştır. GVKT'nin gerekçesinin 40. paragrafında işlemenin hukuka uygun olmasının ölçütleri sayılmış ve bunlar ilgili kişinin rızasının alınması veya üye ülkenin hukuklarında GVKT'ye uygun hazırlanmış düzenlemelerde yer alan meşru sebepler kapsamında işlenmesi açıklamasına yer verilmiştir[764].

Kişisel verilerin işlenmesinde hukuka uygunluğa, ilke olarak atıf yapan GVKT m. 5/1-a düzenlemesi veri sorumlusuna hesap verebilir bir veri işleme süreci oluşturma yükümlülüğü yüklemektedir. Hesap verebilirlik ilkesi bu yönüyle bir şemsiye ilke olarak kişisel veri işleme sürecini hukuka uygun, adil ve şeffaf olmasını zorunlu hale getirerek diğer beş fıkrada düzenlenmiş olan ilkelerin de özünü oluşturmaktadır[765]. Benzer bir ilke veri işlemede genel ilkelerin düzenlendiği

---

762) Doktrinde kişisel verilerin işlenmesinin KVKK'da yer alan beş sütun üzerinde nitelendirilmesi gerektiği görüşü için bkz. "Genel hatlarıyla bakıldığında KVKK kapsamında hukuka uygun kişisel veri işleme faaliyetinin beş farklı sütun üzerine oturtulduğu görülmektedir. Bunlardan ilki KVKK m. 4'te düzenlenen genel ilkelere uygunluktur. Bu ilkelere uygunluk kümülatif olup hukuka uygun bir işlemeden söz edilebilmesi için tüm ilkelere uygun davranılması gerekmektedir. İkinci sütun KVKK m. 5'te ve özel nitelikli kişisel veriler için KVKK m. 6'da düzenlenen hukuki sebeplerden birinin mevcut olmasıdır. Her iki düzenlemede de açık rızaya ve açık rızanın aranmadığı hukuki sebeplere yer verilmiştir. Üçüncü sütun KVKK m. 10'da düzenlenen aydınlatmanın yapılmasıdır. Dördüncü sütun KVKK m. 11'de yer alan ilgili kişi haklarına riayet edilmesidir. Beşincisi ve sonuncusu ise KVKK m. 12'de düzenlenen veri güvenliği tedbirlerine uygunluktur." Eylem Aksoy Retornaz/Osman Gazi Güçlütürk, "Yapay Zekada Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler", Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması, (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, [2023], s. 418.

763) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi, s. 1-5.

764) Dumitru, [2019], Personal Data, s. 290-291.

765) Paolo Balboni/Martim Taborda Barata/Anastasia Botsi/Kate Francis, "Accountability and Enforcement Aspects of the EU General Data Protection Regulation - Methodology for the Creation

KVKK m. 4/2-a düzenlemesinde "hukuka ve dürüstlük" ilkesine atıf yapılarak gerçekleştirilmiştir.

Başlığı "kişisel verilerin işlenme şartları" olan KVKK m. 5 ve başlığı "özel nitelikli kişisel verilerin işlenme şartları" olan m. 6'da maddelerin lafzında açıklık olmamakla birlikte esasen hukuka uygunluk sebepleri düzenlenmiştir[766]. Aynı yönde GVKT m. 6'da kişisel veri işleme faaliyetinin hukuka uygunluk sebepleri sayılmış ve m. 6/1'de veri işlemenin hukuka uygun olması için genel bir ölçüt getirmekte işleme faaliyetinin ancak fıkranın devamı bentlerinde düzenlenen hükümlerden en az birisine dayanması durumunda hukuka uygun olacağı kuralı benimsenmiştir[767]. KVK hukukumuzda da veri işlemenin hukuka uygunluk sebeplerinden (kişisel veri işleme şartları m. 5 ve 6) birisine dayanması zorunludur. Doktrinde belirtildiği üzere genel hukuka uygunluk sebeplerine (MK ve TBK hukuka uygunluk sebepleri) başvurmak yerine veri işleme faaliyetinin KVKK'da hüküm altına alınmış bir hukuka uygunluk sebebine dayanması aranmalıdır[768].

Hukuka ve dürüstlük ilkesine uygun veri işlemeyle yakından ilişkili olan "adil veri işleme" kavramı, WP 29 Çalışma Grubu'nun, iş ilişkisine ilişkin olan 2001 tarihli görüşünde ifade edilmiştir[769]. WP 29 Çalışma Grubu görüşüne göre veri işlemenin "adil olmasına" dikkat edilmeli, bunun gerçekleştirilebilmesi için ilgili kişinin verilerinin adaletsizliğe yol açmayacak şekilde işlenmesi gerekir[770]. Ölçülülük ilkesiyle de ilişkili olan bu yorum veri sorumlusu işverenlere veri işlerken ek bir öz kontrol gerçekleştirme yükümlülüğü yüklemektedir. Veri işlemenin adil olması aynı zamanda kişisel verileri işlerken veri sorumlularına etik

---

of an Effective Compliance Framework and a Review of Recent Case Law", Indian Journal of Law and Technology, Vol. 15, Issue 1, [2019], s. 115.
766) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 49.
767) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 48; Çekin, [2020], Kişisel Veriler s. 69.
768) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 48.
769)https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf (Erişim Tarihi: 21.10.2022).
770) WP29, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final WP 48, [2001], s. 18.

bir yaklaşım sergilemeleri gerektiği biçiminde de yorumlanabilir[771]. Doktrinde genel olarak dürüstlük kuralına uygun kişisel veri işleme ilkesinden, veri işleme sürecinde ilgili kişinin çıkarlarının gözetilmesi ve makul beklentilerinin dikkate alınması gerekliliğinin anlaşılması gerektiği kabul edilmektedir[772]. KVK Kurumu yayımladığı Uygulama Rehberi'nde hukuka ve dürüstlük kurallarına uygun olma ilkesi bu görüş kapsamında açıklanmıştır[773].

Sonuç olarak, KVKK'da yer alan şemsiye ilkelerden birisi olan m. 4/2-a'da yer alan kişisel verilerin işlenmesinde "hukuka ve dürüstlük ilkesine" uygun hükmü diğer ilkelerin özünü oluştur ve bu ilkelerle birlikte kişisel verilerin işlenmesinde adil ve şeffaf bir sürecin oluşturulmasını sağlar[774]. Hukukumuzda MK m. 2'de düzenlenmiş olan dürüstlük ilkesine bu maddede atıf yapılmasının amacı, veri sorumlularının hakkın kötüye kullanılmasının önüne geçilmesi düşüncesidir[775]. Örneğin iş ilişkisinde işverenin, TBK m. 417 kapsamında işçinin kişiliğini korumak, psikolojik ve cinsel tacize uğramalarını engellemek için dijital izleme uygulaması kullanması durumunda; bu düzenlemenin amacına uygun işçileri en az etkileyecek yöntemle ve az veri işleyecek şekilde dijital izleme gerçekleştirmesi, ilgili işçilerin bilgileri dışında bir veri işlenmesinin önüne geçmesi yükümlülüğü bulunmaktadır[776]. GVKT m. 5'te dürüstlük kuralına atıf yapılmamış, kişisel verilerin işlenmesinde "hukuka uygun, adil ve şeffaf" bir işleme sürecinin esas alınması öngörülmüştür. Maddenin devamında adil veri işlemeden anlaşılması gerekenin verileri işlenen ilgili kişinin veri işlemenin kapsamı ve amaçları hakkında bilgilendirilmesi ve şeffaf bir yapının oluşturulması gerekliliği anlaşılmaktadır[777].

771) EU, [2018], Handbook, s. 142.
772) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 49; Çekin, [2020], Kişisel Veriler, s. 69-70;
773) KVK Kurumu, [2019], Uygulama Rehberi, s. 64.
774) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 48-49.
775) Dülger, [2019], Kişisel Veriler, s. 263.
776) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 3.
777) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 48.

b) İşlenen Kişisel Verilerin Doğru ve Güncel İşlenmesi

Veri sorumlusu işveren, dijital izleme uygulamalarıyla işçinin kişisel verilerini işlerken dikkate alması gereken genel bir diğer ilke KVKK m. 4/2-b bendinde düzenlenmiştir. Düzenlemeye göre işlenen kişisel veriler "doğru ve gerektiğinde güncel olmalıdır." Veri sorumlusu işveren, işçinin verisini işlemek için bu ilke hükmünde öngören sınırlamaya uygun bir veri işleme faaliyeti yürütmesi gerekmektedir. Zira işçi ile ilgili verinin doğru olmaması onun işyerindeki imajı ve kariyeri üzerinde olumsuz sonuçlara sebebiyet verebilir. Doktrinde verinin doğru ve güncel olması ilkesinin, hem olgulara ilişkin bilgilerin doğruluğunu hem de değer yargılarına ilişkin bilgilerin doğru olmasını kapsadığı ifade edilmektedir[778].

Aynı ilke 108 sayılı Sözleşme'nin 5. maddesinde "otomatik işlemeye konu olan kişisel veriler" üst başlığında m. 5/1-d bendinde "doğru bilgileri yansıtır ve gerektiğinde güncellenir" biçiminde düzenlenmiştir[779]. GVKT m. 5'te "kişisel verilerin işlenmesine ilişkin ilkeler" başlığında m. 5/1-d bendinde "doğruluk" ilkesi biçiminde düzenlenmiştir[780]. Bu düzenlemelerle veri sorumlularına aktif bir özen yükümlülüğü yüklenmiştir[781].

Bu ilke kapsamında korunan değer ilgili kişinin doğru ve güncel olmayan veriler sebebiyle zarar görmesini engellemektir. Doğru ve güncel veri işlenmesiyle hem veri sorumlusu, kişisel veri işlerken varmak istediği yararı gerçekleştirir hem de verileri işlenen ilgili kişinin menfaatlerinin zarar görmesi engellenmiş olur[782]. Bunun veri sorumlusu açısından önemi büyüktür. Zira yanlış ve güncel olmayan bilgiler kapsamında yanlış sonuçlara ulaşılması işyeri ve işçinin kişilik hakkı

778) Çekin, [2020], Kişisel Veriler, s. 103; Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 51.
779) 108 sayılı Sözleşme m. 5 için bkz. https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf (Erişim Tarihi: 20.10.2022).
780) GVKT m. 5/1-d düzenlemesine göre: "kişisel veriler doğru ve gereken şekilde, güncel tutulur; işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır."
781) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 6.
782) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 6.

açısından riskli sonuçlar ortaya çıkarır[783].

Dijital izleme uygulamalarının veri işleme ve analiz biçimi dikkate alındığında verinin doğru ve güncel tutulması güçleşebilir. Bu sebeple veri sorumlusu işverenin dijital izleme uygulamasıyla işçinin verisini işleme faaliyetinde işlediği verilerin güncelliğini belirli aralıklara denetlemesi, işleme amacı ortadan kalkmış veriyi silmesi ve gerekirse doğruluğuyla ilgili işçiyle teyitleşmesi gerekmektedir. WP 29 Çalışma Grubu da bu hususta yayımlamış olduğu görüşte verinin doğru ve güncel olması için işçiyle teyitleşmeyi önermiştir[784].

c) İzlemenin Belirli, Açık ve Meşru Amaç Kapsamında Gerçekleştirilmesi

Kişisel verilerin "belirli, açık ve meşru amaçlar" için işlenmesi ilkesi veri sorumlusu tarafından veri işleme amacının belirlenmesini, amaç kapsamında değerlendirme yapmasını ve veri işlemenin sebebinin ilgili kişi tarafından açık bir şekilde anlaşılmasını zorunlu hale getirmektedir[785]. Ayrıca bu ilke kapsamında veri işlemenin amacının bulunmadığı, tüm veri işleme faaliyetini içeren genel amaçlar için kişisel veri işlenmesi yasaklanmaktadır. KVKK m. 4/2-c bendinde düzenlenen bu ilke GVKT m. 5/1-b ve 108 sayılı Sözleşme'nin 5. maddesinde de yer almaktadır[786]. Bu ilke kapsamında verileri işlenen ilgili kişinin hangi verilerinin, hangi kapsamda, ne amaçla işlendiği ve hangi haklarının bulunduğu hususunda anlaşılabilir bir şekilde bilgilendirilmesi gerekir[787].

Meşru amaç kavramı veri işleme amacın hukuka uygun olmasını ifade etmektedir. Veri işleme amacının veri işleme faaliyetine başlamadan önce

783) Küzeci, [2020], Kişisel Veriler, s. 243.
784) Gürsel, [2016], İşçinin Kişisel Verileri, s. 228.
785) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 52.
786) EU, [2018], Handbook, s. 283.
787) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 8.

belirlenmesi ve sonraki veri işlemelerin bu amaç kapsamında kalması gerekmektedir. Örneğin işveren aydınlatma yükümlülüğünü yerine getirerek tıbbi mümessil olan işçinin iş sözleşmesine uygun müşteri ziyaretlerini gerçekleştirdiğini tespit etmek için araç veya mobil cihazlara yüklediği GPS, Geofencing uygulamaları vasıtasıyla dijital izleme gerçekleştirebilir. Burada meşru amaç işçinin mesai saatleri içinde iş görme borcunu sözleşme yükümlülüklerine uygun ifa edip etmediğinin denetlenmesi için lokasyon verilerinin işlenmesidir. İşverenin bu izleme uygulamalarını mesai saatleri dışında kullanması, işin ifa edilmesi amacı dışında izleme gerçekleştirmesi veya işçinin dinlenme anı aktivitelerini izlemek için kullanması meşru amaç kapsamında değerlendirilemez.

Belirli ve açık bir meşru amaç kapsamında kişisel verileri işlenmesi ilkesinin bir gereği olarak veri işleme sürecinde şeffaflık oluşturulmalı ve ilgili kişinin işlenen verileriyle ilgili olarak, veri işleme faaliyetinden önce bilgilendirilmesi gerekmektedir[788]. Eklemek gerekir ki, sadece veri sorumlusu işverenin veri işlemenin meşru amacını bilmesi bu genel ilkeye uygun veri işleme olarak kabul edilemez. Aynı doğrultuda ilgili kişinin bilgilendirildiği metinde anlaşılması güç kelimelerin seçilmemesi, veri işleme amacının açık ve belirli[789] bir

788) Article 29 Data Protection Working Party, Opinion 3/2013 On Purpose Limitation, 02.04.2013, 00569/13/EN WP 203, s. 15, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (Erişim Tarihi: 21.10.2022).

789) KVK Kurulu, aydınlatma metninde muğlak ifadelerin kullanılmasına idari para cezası uygulamış ve aydınlatma metinlerinde "sayılan kişisel veriler dahil olmak üzere ancak bunlarla sınırlı olmaksızın" ifadelerine yer verilmesini muğlak olarak değerlendirerek veri sorumlusu işverene idari para cezası uygulamıştır. Kararda özetle şu husus değerlendirilmiştir: "Diğer taraftan, bu metnin içerik olarak da açık rıza kapsamında ilgili kişiyi bilgilendirdiğinden ya da aydınlatma yükümlülüğünü yerine getirdiğinden söz edilemeyeceği zira, metinde çeşitli kişisel veri kategorileri sıralandıktan sonra "(…) sayılan kişisel veriler dahil olmak üzere ancak bunlarla sınırlı olmaksızın (…)" ifadesine yer verildiği ve hangi kişisel verilerin işleneceği (kategorik olarak) hususunun muğlak bırakıldığı, işlenecek veri kategorileri sıralandıktan sonra veri işleme amaçları da art arda sıralanmak suretiyle hangi veri kategorisinin hangi amaçla işleneceğine dair herhangi bir açıklamaya yer verilmediği, metinde "…. uygun gördüğü diğer üçüncü kişilere ve/veya yurt dışında paylaşılabileceği" ifadesinin yer aldığı bu kapsamda kimlere aktarım yapılacağının muğlak bir şekilde veri sorumlusuna bırakıldığı, ayrıca metinde biyometrik veri niteliğini haiz olan parmak izinin veri kategorileri içerisinde dahi sayılmadığı…" KVK Kurulu'nun "İşverenin, işçisine ait kişisel verileri ve özel nitelikli kişisel verileri; aydınlatma yükümlülüğünü yerine getirmeden ve hukuka aykırı işlemesi" hakkında 20/05/2020 tarihli ve 2020/404 sayılı Karar Özeti.

şekilde ilgili kişiye bildirilmesi gerekmektedir[790]. Ayrıca veri sorumlusu işveren diğer veri işleme şartları yoksa ilgili şeffaflık ilkesinin bir gereği olarak kişinin açık rızasını almalı ve işlenen verilerle ilgili bir şeffaflık oluşturmalıdır (VERBİS kaydı gibi)[791].

Eklemek gerekir ki, bazı veri işleme faaliyetlerinde veri işlemenin amacı belirlidir fakat ilgili kişi bilgilendirilirken kullanılan dil anlaşılmayacak biçimde teknik ifadeler içerebilir. Bu ilke kapsamında bunun da önüne geçilmek istenmiş olup, veri sorumlusuna aydınlatma yükümlülüğünü yerine getirirken sade ve açık bir dil kullanma yükümlülüğü yüklenmiştir[792].

d) Dijital İzlemenin Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması

Meşru amaç kapsamında veri işleme ilkesiyle yakından ilişkili olan KVKK m. 4/2-ç bendi veri sorumlusu işverenlere dijital izleme uygulamalarıyla gerçekleştirecekleri kişisel veri işleme süreçlerini amaçla bağlantılı ve mümkün olan en az veri ile gerçekleştirilme yükümlülüğü yüklemektedir. Dahası bu en az veri ile gerçekleştirme ölçülü olmalı, yani amaçla arasında makul bir dengenin kurulmuş olması gereklidir[793]. Bu ilke aslında ölçülülük ilkesi[794] kapsamında gerçekleştirilen üç aşamalı denetimin uygulanmasını da gerektirmektedir[795].

GVKT m. 5/1-c bendinde ve 108 sayılı Sözleşme'nin 5/1-c bendinde de amaçla bağlantılı ölçülü veri işlenmesi düzenlenmiştir. Bu düzenlemelerde temelde "veri minimizasyonu" hedeflenmiş ve veri sorumlularına kişisel veri işleme süreçlerini amaçla bağlantılı en az veri ile gerçekleştirme yükümlülüğü

790) Article 29 Data Protection Working Party, Opinion 3/2013 On Purpose Limitation, [2013], s. 15-17.
791) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 9.
792) Küzeci, [2020], Kişisel Veriler, s. 231.
793) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 10-11.
794) Ölçülülük ilkesi kapsamında "elverişlilik", "gereklilik" ve "orantılılık" testleri gerçekleştirilir. Bkz. § 6. III. 3.
795) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 59.

yüklemiştir[796]. Veri minimizasyonu ilkesi kişisel verilerin yalnızca işlenme amacı için kesinlikle gerekli olması koşulunu aramaktadır[797]. Bu itibarla kişisel veriler işlenmeden amaç gerçekleştirilebiliyorsa süreç kişisel veri işlenmeden gerçekleştirilmelidir[798]. Aynı doğrultuda OECD'nin 2013 tarihli Tavsiye Kararı'nın 7. maddesinde kişisel verilerin işlenmesinde sınırlamaların olması gerektiğini ve bu verilerin işlenmesinin kanun veya adli mercilerin kararları kapsamında işlenmesinin zorunlu olması halinde kişisel verileri işlenen ilgili kişinin rızasının alınması gerektiğini tavsiye etmiştir.[799]

Amaçla bağlantılı sınırlı ve ölçülü veri işleme ilkesi, kişisel verilerin işlenmesinde belirlenen amaçla veri işlemenin bağlantılı olmasını aramakta ve amaçla bağlantısı bulunmayan verilerin işlenmesini yasaklamaktadır. Bu ilke aynı zamanda mevcut olmayan ve sonradan gerçekleşeceği varsayılan amaçlar için kişisel veri işlenmesini engellemektedir[800]. Örneğin, İş Kanunu m. 14 düzenlemelerine tabi olarak uzakta çalışan bir finans analisti işçinin çalışma performansını ölçmek için aydınlatma yükümlülüğü de yerine getirilerek aktif bilgisayar kullanımı veya bir finansal analiz programını aktif kullanmasını takip eden dijital uygulama kullanması amaçla bağlantılı sınırlı ve ölçülü veri işlemeye örnek gösterilebilir. Ne var ki, işverenin bu örnekte uzakta çalışan işçinin tüm internet trafiğini, sosyal medya hesaplarını dijital izleme vasıtasıyla kayıt altına alması "amaçla bağlantılı sınırlı ve ölçülü veri işleme" ilkesine aykırı olacaktır.

---

796) EU FRA, Handbook, s. 125; ABAD, İrlanda Dijital Haklar davasında kamuya açık elektronik iletişim hizmetleri veya ağları tarafından işlenen kişisel verilerin yetkili makamlara olası iletimi için muhafaza edilmesine yönelik ulusal hükümleri uyumlu hale getirmeyi amaçlayan Veri Saklama Direktifi'nin geçerliliğini değerlendirmiş ve "organize suç ve terörizmi" önlemek gibi amaçları bulunan Direktifin "tüm bireyleri ve tüm elektronik iletişim araçlarını ve yarıca tüm internet trafik verilerinin işlenmesini" herhangi bir ayrım, sınırlama ve istisna uygulamaksızın düzenlemesini veri minimizasyonu ilkesi açısından sorunlu bulmuştur. CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014, § 44-57.

797) Bart van der Sloot, "Is This the End for the Re-Use of PSI?", European Data Protection Law Review (EDPL), Vol. 7, No. 3, 2021, s. 474.

798) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 10 vd.

799) OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, [2013], s. 14.
https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Erişim Tarihi: 23.10.2022).

800) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 10.

İşveren bu durumda gelecekte olabilecek riskleri engellemek için bu şekilde bir veri işleme faaliyeti gerçekleştirdiğini belirtmesi hukuka aykırılığı ortadan kaldırmayacaktır.

e) İşlenen İşçi Verilerinin Belirli Bir Süre Kadar Muhafaza Edilmesi

KVKK m. 4/2-d bendinde kişisel verilerin "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" ilkesi düzenlenmiştir. Bu ilke kapsamında veri sorumlusu işveren dijital izleme uygulamaları vasıtasıyla işlediği kişisel verilerde KVKK m.7'ye uygun bir silme ve m. 12 düzenlemesine uygun teknik ve idari tedbir alma süreci oluşturmalıdır[801]. Benzer düzenleme GVKT m. 5/1-e bendinde ve 108 sayılı Sözleşmenin 5/4-e bendinde gerçekleştirilmiş ve kişisel verilerin amaçla bağlantılı bir süre kadar işlenmesini[802] veri sorumlusunun yükümlülüğü haline getirmektedir[803]. Bu ilke ile kişisel verilerin ne kadar süre ile işleneceği hususunda ilgili kişinin veri sorumlusu tarafından bilgilendirilmesi amaçlanmıştır[804].

Kişisel verilerin imhası, silinmesi ve yok edilmesinin usul ve esaslarının belirlenmesi için "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik" yayımlanmıştır[805]. Yönetmelik kapsamında kişisel verilerin işlenmesinin amacının ortadan kalkması, hedefin gerçekleşmemesi veya değişmesi durumlarında veri işlemenin amacı kalmayacağından bu durumda

---

801) KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 12.
802) Örneğin, AİHM, S. v. Marper, davasında her iki başvurana karşı yürütülen cezai kovuşturmanın bir mahkeme kararıyla beraatle sonlandırıldığını göz önünde bulundurarak, iki başvuranın parmak izlerinin, hücre örneklerinin ve DNA profillerinin süresiz olarak saklanmasının demokratik bir toplumda orantısız ve gereksiz olduğuna karar vermiştir. AİHM, S. and Marper v. the United Kingdom [GC], No. 30562/04 ve 30566/04, 4 Aralık 2008; Aynı doğrultuda: AİHM, M.M. v. the United Kingdom, No. 24029/07, 13 Kasım 2012.
803) EU, [2018], Handbook, s. 129.
804) Nicoleta Maria Cristolovean, "Reflections on Personal Data Processing That Is Necessary for the Entering or Performance of a Contract", Jus et Civitas: A Journal of Social and Legal Studies, Vol. 8, No. 2, [2021], s. 44.
805) Resmi Gazete, 28 Ekim 2017 tarih ve 30224 sayı.
https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm

kişisel veriler kanunlarda öngörüldüğü sürenin sonunda periyodik imhaya tabi tutulmalıdır.

Eklemek gerekir ki, kişisel verilerin yok edilmemesi aynı zamanda TCK m. 138'de suç olarak düzenlenmiştir. Kanunların belirlediği süreler geçmiş olmasına rağmen kişisel verileri sistem içinde yok etme yükümlülüğü bulunanlar bu yükümlülüğe uygun olarak işlem yapmalıdır. Aksi durumda görev yerine getirilmediğinden yok etme yükümlülüğü bulunanlar bir yıldan iki yıla kadar hapis cezası ile cezalandırılır[806].

4. Dijital İzlemede Kişisel Verilerin İşlenme Şartları

Kişisel verilerin işlenme şartları KVKK m. 5'te tüm veriler, m. 6/2 ve 3'te ise özel nitelikli kişisel veriler açısından hüküm altına alınmıştır. KVKK m. 5'te "kişisel verilerin işlenme şartları" başlığında hukuka uygunluk sebepleri: "açık rıza, kanunlarda açıkça öngörülme, fiili imkansızlık, bir sözleşmenin kurulması ve ifasıyla doğrudan ilgili olma, hukuki yükümlülükleri yerine getirme, ilgilinin alenileştirmesi, bir hakkın tesisi için zorunlu olma ve veri sorumlusunun meşru menfaati" biçiminde düzenlenmiştir. Aynı hususta GVKT m. 6'da "işleme faaliyetinin hukuka uygunluğu" başlığında düzenleme yapılmıştır[807]. İşverenin kullanacağı dijital izleme uygulamalarında veri işleme faaliyetinin bu hukuka uygunluk sebeplerinden birisine dayanması zorunludur. Bu başlıkta kişisel veri işlemenin meşru zemini oluşturan[808] bu veri işleme şartları ele alınacaktır.

a) Açık Rıza Beyanı Kapsamında Dijital İzleme Gerçekleştirilmesi

KVKK m. 5/1'de ilgili kişinin açık rızası bulunmaksızın kişisel verilerinin işlenmesi yasaklanmıştır. Bu fıkra hükmü kapsamında kural olarak kişisel verilerin

806) Bkz. § 8. III.
807) GVKT m. 6 ve gerekçesi için bkz. https://gdpr-info.eu/art-6-gdpr/ (Erişim Tarihi: 23.10.22).
808) Çekin, [2020], Kişisel Veriler, s. 70-71.

işlenmesi ilgili kişinin açık rızasına bağlıdır[809]. İkinci fıkrada ise belirli hukuka uygunluk sebeplerine dayanması şartıyla kişisel verilerin işlenebileceği durumlar hüküm altına alınmıştır.

aa) Açık Rızanın Unsurları

KVK hukukunda rızaya yönelik genel olarak iki yaklaşım bulunmaktadır. Bunlardan birisi ABD'de yaygın olarak uygulanan "bildirim ve seçim" yaklaşımıdır. Bu yaklaşımda veri sorumluları kişisel verileri korumaya yönelik bir bilgilendirme bildirimi yayımlarlar ve sonrasında ilgili kişi buna aykırı bir irade ileri sürmedikçe veri işlenmesine rıza gösterildiği kabul edilmektedir[810]. AB yaklaşımı bundan farklı olarak GVKT'da "açık rızanın" unsurlarının varlığı aranmış ve ilgili kişinin kişisel verilerinin işlenmesine ilişkin özgür iradesiyle olumlu bir irade beyanında bulunması koşulu öngörülmüştür[811]. AB ve ülkemiz kişisel verileri koruma sistemlerinde zımni rıza geçersiz kabul edilmiş ve açık rıza yaklaşımı ile ilgili kişiden olumlu bir irade açıklamasının veri sorumlularınca herhangi bir yöntemle ispatlaması koşulu aranmıştır.

Bu noktada belirtilmesi gereken bir diğer önemli husus iş ilişkisinde hangi durumlarda açık rıza alınarak kişisel veri işleneceği, hangi durumlarsa sadece aydınlatma yükümlülüğünün yeterli olacağı ve diğer veri işleme şartları kapsamında kişisel veri işlenebileceği her bir olay özelinde değerlendirilmesi gerektiğidir[812]. Zira kişisel veri işleme faaliyetini diğer veri işleme şartları kapsamında yürütmek mümkünken açık rıza alınması KVK Kurul kararlarında ve

809) Çekin, [2020], Kişisel Veriler, s. 84.
810) Bildirim ve seçim (bazen "bildirim ve onay" olarak da adlandırılmaktadır), çevrimiçi uygulamalarda ilgili kişiden onay alınması için kullanılmaktadır. Bildirim, genellikle bir gizlilik politikasında veya kullanım şartları sözleşmesinde yer alan şartların sunumunda oluşmaktadır. Seçim ise genellikle "kabul ediyorum" sekmesine tıklayarak veya yalnızca Web sitesini kullanarak şartların kabul edildiğini gösteren bir eylemdir. Robert H. Sloan/Richard Warner, "Beyond Notice and Choice: Privacy, Norms, and Consent", J. High Tech. Law, [2013], s. 3.
811) Daniel J. Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law", The George Washington Law Review, Vol .91, Issue 1, January 15, [2023], s. 5.
812) Yücedağ, [2017], Genel Hukuka Uygunluk Sebepleri, s. 775.

rehberlerinde hakkın kötüye kullanılması olarak değerlendirilmektedir. KVK Kurul kararlarında ve rehberlerinde ortaya çıktığı üzere KVK Kurulu diğer veri işleme şartları varken açık rıza alınarak kişisel veri işlenmesini ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla aldatıcı biçimde veri işleme faaliyetinin yürütülmesi olarak yorumlamaktadır[813].

KVKK m. 3/1-a bendinde açık rızanın unsurları "belirli bir konuya ilişkin", "bilgilendirmeye dayanan" ve "özgür iradeyle açıklanan" biçiminde oraya çıkmaktadır (GVKT m. 4/11'de aynı unsurlar). GVKT ve 95/46EC sayılı Direktif ve 108 sayılı Sözleşme'deki tanım da bu çerçevededir. İş ilişkisi açısından veri işleme çoğunlukla kanunda öngörülme, sözleşme ilişkisi ve meşru menfaat kapsamında işlenmektedir. Öte yandan özel nitelikli kişisel veriler işlendiğinde KVKK m. 6/2 ve 6/3 bentleri kapsamında açık rızanın alınması gereken durumlar olabildiği gibi diğer veri işleme şartlarının bulunmadığı durumlarda işçinin açık rızasının alınarak kişisel verileri işlenmelidir.

Açık rıza kapsamında kişisel verinin işlenmesi, açık rızanın unsurları dikkate alındığında bu haliyle kişisel verileri koruyan düzenlemelerin içinde en katı rıza biçimini oluşturmaktadır. GVKT ve KVKK açık rızanın varlığı için belirli bir konuya ilişkin olma, bilgilendirmeye dayanması ve özgür iradeyle açıklanması gibi unsurların varlığını aramıştır[814]. Örneğin web sitesi üzerinden açık rıza alınacaksa aydınlatma beyanından farklı bir sekmede bilgilendirme unsurunu taşıyan bir metinle ilgili kişinin bu kutucuğu işaretleyerek açık rızaya ilişkin rızasını

813) Kişisel veri işleme süreci KVKK'da açık rıza dışındaki hukuka uygunluk sebepleri olarak düzenlenmiş olan m. 5/2 düzenlemelerinden birisinin kapsamına giriyorsa bu işleme şartı kapsamında açık rıza almaksızın kişisel veri işlenmelidir. Aksine açık rıza alınması dürüstlük ilkesine aykırı bulunmaktadır. Bu husus KVK Kurul kararlarına ve KVK Kurum rehberlerine şu şekilde yansımaktadır: "Veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılması; ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla aldatıcı ve veri sorumlusunca hakkın kötüye kullanımı niteliğinde olacaktır. Nitekim, ilgili kişi tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğer kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesi hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına gelecektir." KVK Kurumu, [2019], Uygulama Rehberi, s. 22.

814) GVKT m. 4/11 ve gerekçesi; KVKK m. 3/1-a.

açıklaması gerekir. KVKK m. 3/1-a bendinde AB esası benimsenmiş ve açık rızanın bulunduğunu kabul etmek için değinilen üç unsurun varlığı aranmıştır. KVK Kurumu da yayımladığı rehberlerde açık rızadan ne anlaşılması gerektiğine açıklık getirmiştir[815].

Yukarıda açıklandığı üzere, KVKK m. 5/1'de kişisel verilerin ilgili kişinin açık rızasının alınmaksızın işlenmeyeceği düzenlenmiştir[816]. Aynı düzenleme GVKT m. 6/1-a bendinde yer almakta ve ilgili kişinin bir amaca yönelik olarak verdiği kişisel verilerin işlenmesi onayı veri işleme koşulu olarak sayılmıştır[817]. GVKT m. 4/11 düzenlemesinde açık rıza tanımı 95/46 EC sayılı Direktife göre detaylandırılmış ve "ilgili kişinin kendisiyle ilgili kişisel verinin işlenmesine, özgür iradesiyle, özel, bilgilendirilmiş ve kuşkuya yer vermeyecek kesinlikte bir beyan veya iradesini ortaya koyan açık bir davranışla onay vermesi" biçiminde yapılmıştır[818]. Açık rızanın alınma şekli açısından bir koşul KVKK'da ve GVKT'de[819] öngörülmemiş, açık rızanın Kanun'da öngörülen unsurları taşıması ve bunun ispatlanabilir bir yöntemle yerine getirilmesi yeterli görülmüştür[820]. Ayrıca açık rıza işçinin kişisel verilerinin işlenmesinin hemen öncesinden alınabileceği gibi açık rızanın alınmamasının sebebinin ortadan kalkmasından sonra da işçilerden

815) KVK Kurumu, Açık Rıza Rehberi, s. 4-6.
816) KVKK m. 5'te kişisel verilerin işlenmesinin hukuka uygunluk nedenleri, "Kişisel verilerin işlenme şartları" başlığında: "(1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. (2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) 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. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması." biçiminde düzenlenmiştir.
817) W. Gregory Voss, "Airline Commercial Use of EU Personal Data in the Context of the GDPR", British Airways and Schrems II, Colorado Technology Law Journal, Vol. 19, No. 2, [2021], s. 400.
818) GVKT m. 4 ve açık rıza tanımı için bkz. https://gdpr-info.eu/art-4-gdpr/
819) EU, [2018], Handbook, s. 56; Article 29 - Data Protection Working Party, Opinion 15/2011 on the definition of consent, s. 25. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf (Erişim Tarihi: 24.10.2022).
820) KVK Kurumu, 100 Soruda Kişisel Verilerin Korunması Rehberi, Ankara, 2019, s. 27.

açık rıza alınabilir.

bb) Açık Rıza ile Diğer Veri İşleme Şartları Arasındaki İlişki

İşçinin açık rızasını alarak dijital izleme uygulamalarıyla kişisel veri işlenmesi hukuka uygunluk sebeplerinden birisidir. KVKK m. 5 ve 6'da öngörülen açık rıza kişisel veri işleme şartı, diğer kişisel verileri işleme şartlarından üstün değildir[821]. Bu sebeple veri sorumlusunun (iş ilişkisinde işveren) öncelikli olarak kişisel veri işlemenin hukuki şartını araştırması, diğer veri işleme şartları mevcutsa açık rıza almaksızın, KVKK'nın diğer yükümlülüklerini yerine getirerek kişisel veri işlemesi gerekir. Yukarıda açıklandığı üzere AB düzenlemelerinde yer alan usul KVK Kurumu tarafından benimsenerek, diğer veri işleme şartları mevcutken açık rıza alınarak kişisel veri işlenmesi dürüstlük kuralına aykırı bulunmaktadır[822].

KVKK m. 5 ve 6'nın lafzına baktığımızda kanun koyucunun açık rızaya hiyerarşik olarak bir üstünlük tanıdığı izlenimi oluşmaktadır[823]. Gerçekte KVK Kurulu yayımladığı kararlarda açık rızaya, diğer veri işleme şartlarının bulunmaması durumunda gidilmesi gereken bir veri işleme şartı olduğunu, açık rızaya bir üstünlük tanınmadığının, aksi durumda dürüstlük ilkesine aykırı veri işleme söz konusu olabileceğini, ayrıca açık rıza beyanında dönme söz konusu

821) KVK Kurulu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun Uygulanmasına Yönelik Soru Cevaplar, s. 21; Yücedağ, [2017], Genel Hukuka Uygunluk Sebepleri, s. 773-774.

822) KVK Kurulu, "Veri sorumlusu tarafından Kanunun 5 inci maddesinin (2) numaralı fıkrasının (c) bendi kapsamında sözleşmenin taraflarına ait kişisel veri işlenmesi durumunda ayrıca açık rıza alması ve de açık rızayı üyeliğin ve hizmetin dolayısıyla sözleşmenin bir koşulu olarak dayatmasının; Diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği, ayrıca hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı" biçiminde değerlendirme yaparak veri sorumlusuna KVKK m. 18 kapsamında idari yaptırım uygulamıştır. https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi (Erişim Tarihi: 16.10.2023).

823) KVK Kurulu, kaynak Avrupa Birliği düzenlemeleri ve WP 29 Çalışma Grubu ile EDPB kararlarını esas alarak, açık rıza veri işleme şartına ancak diğer veri işleme şartları (KVKK m. 5/2) bulunmadığı durumlarda başvurulması gereken bir şart olduğunu vurgulamıştır. Bu sebeple kişisel verilerin işlenmesinde açık rıza diğer veri işleme şartlarının bulunmadığı durumlarda dikkate alınmalıdır. Ayrıca hiyerarşik olarak açık rızaya bir üstünlük tanınmadığı KVK Kurul kararlarında ortaya çıkmaktadır. Bkz. https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi (Erişim Tarihi: 16.10.2023).

olduğundan bu durumda açık rıza beyanından dönen ilgili kişi için veri işleme faaliyetini durdurma ve imha ve silme işleminin gerçekleştirilmesi gerektiğini, bunun da çalışma ilişkisi gibi sürekli borç ilişkisi doğuran sözleşmeler açısından sürdürülmesinin olanaksız olduğunu vurgulamıştır[824].

Eklemek gerekir ki, KVKK'da kişisel verilerin açık rıza kapsamında işlenmesine dört maddede atıf yapılarak hüküm altına alınmıştır. Buna göre: m. 5/1'de "kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez", m. 6/2'de "özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır", m. 8/1'de "kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılmaz", m. 9/1'de "kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz" düzenlemeleriyle açık rıza Kanun'da bir kişisel veri işleme hukuka uygunluk sebebi olarak düzenlenmiştir[825].

Açık rıza ilgili kişinin beyanıyla meydana gelerek hukuki sonuçlar doğurduğundan tek taraflı bir hukuki işlemdir[826]. Bu itibarla, tek taraflı bir hukuki işlem olan açık rıza beyanını hukuki işlemlere ilişkin düzenlemeler kapsamında değerlendirmek gerekir. Ayrıca diğer kanunlardaki düzenlemeler saklı kalmak kaydı ile KVKK'da açık rızanın alınması ve aydınlatma yükümlülüğünün yerine getirilmesi bir şekil şartına bağlanmamıştır. Öte yandan KVK hukukuna özgü olarak bu irade açıklanmasının varlığını veri sorumlusu ispat etmekle yükümlüdür[827].

---

824) KVK Kurulu yayımlamış olduğu: "Açık Rızanın Hizmet Şartına Bağlanması" başlıklı kararında: "Diğer kişisel veri işleme şartlarının varlığı durumunda açık rıza alınmasının ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla veri sorumlusunca hakkın kötüye kullanılması anlamına geleceği" biçiminde karar vererek konuyu açıklığa kavuşturmuştur. https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi, (Erişim Tarihi: 13.08.2022).
825) KVK Kurumu, Açık Rıza Rehberi, s. 1.
826) Fikret Eren, Borçlar Hukuku Genel Hükümler, Yetkin Yayınları, Ankara, [2019], s. 172.
827) KVK Kurumu, [2019], Uygulama Rehberi, s. 48.

cc) İş İlişkisinde Açık Rızanın Geçerlilik Koşulları

İş ilişkisinin ortaya çıkardığı otorite/bağımlılık ilişkisinde, işe ihtiyacı olan işçinin rıza taleplerini reddetme olanağının zayıf bir olasılık olması veya işçinin bir zarara uğrayabileceği kaygısı taşıması durumunda açık rızanın bulunduğunu söylemek güçtür[828]. Ayrıca herhangi bir kaygı taşımadan verilen açık rıza, aynı zamanda dilediği zaman bu iradeden dönme hakkını da veri sahibi işçiye vermektedir[829]. Bu durumda iş ilişkisi için yönetilmesi güç sonuçlar ortaya çıkar. Bundan dolayı dijital izleme uygulaması kullanmadan önce öncelikle diğer veri işleme şartlarının (KVKK m. 5/2) varlığı araştırılmalı, başkaca bir veri işleme hukuka uygunluk sebebi yoksa işçinin açık rızasına başvurulmalıdır. Örneğin işverenin iş sağlığı ve güvenliği tedbirlerine yönelik dijital izleme uygulamaları kullanması "kanunlarda açıkça öngörülmesi", "veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" gibi hukuka uygunluk sebebi olarak düzenlenmiş hükümlerle ilgilidir. Bu durumda veri sorumlusu işverenin açık rıza almak yerine bu veri işleme şartları kapsamında işçiyi aydınlatma yükümlülüğü kapsamında dijital izleme uygulaması ile ilgili bilgilendirmesi (KVKK m. 10) dijital izleme uygulamasının gerçekleştirilmesi için yeterlidir. İşverenin bu şekilde hukuka uygunluk sebepleri bulunmasına rağmen işçiden açık rıza alarak kişisel veri işlemesini KVK Kurumu ilgili kişinin yanıltılması ve yanlış yönlendirilmesi olarak nitelendirerek dürüstlük kuralına aykırı bulmaktadır[830].

Açık rızanın varlığından bahsetmek için işçinin belirli bir konuda işlenen kişisel verileri hususunda bilgilendirilmesi ve ilgili işçinin işlenmesine izin verdiği

828) WP29 On the processing of personal data in the employement contex, Opinion 8/2001, 5062/1/EN/Final WP 48, [2001], s. 23.
829) KVK Kurumu, Açık Rıza Rehberi, s. 6.
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf (Erişim Tarihi: 15.11.2022).
830) KVK Kurumu, Kişisel Veri İşleme Şartları Rehberi, s. 2-3. https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari

verilerin sınırını bilerek "olumlu bir irade beyanında" bulunması gereklidir[831]. İradenin sakatlandığı veya belirli bir konuya ilişkin bilgilerin bulunmadığı açık rıza beyanı geçersiz olacaktır. Bu itibarla salt açık rızanın varlığı verilerin hukuka uygun olarak işlendiği anlamına gelmez. Özellikle bilinçli verilmiş ve sakatlığa uğratılmamış bir iradenin varlığı açık rızanın geçerliliği açısından önem arz etmektedir. Bu ayrıca TBK m. 26 ve 27'nin de bir gereğidir, zira kanunun emredici hükümlerine, ahlaka ve kişilik haklarına aykırı iradede açıklamaları geçersizdir[832]. Örneğin işçinin itiraz hakkının bulunmadığı bir açık rıza alma süreci ya da özel hayat alanının birçok katmanını dijital izlemeye tabi tutan bir rıza beyanı veya işçinin mesleki ve ekonomik varlığını tehlikeye atan açık rıza beyanı geçerli olmayacaktır. KVK Kurumu da yayımladığı rehberde işçilere rıza göstermeme imkanının etkin bir şekilde sunulmadığı veya işçilerin rıza vermemesi halinde kendisi için muhtemel olumsuzluklara sebebiyet vereceği durumlarda rızanın özgür irade ile verilmiş sayılmayacağını kabul etmektedir[833].

İş ilişkisi açısından işçinin iradesinin sakatlanmamasının bir diğer görünümü, işçinin açık rıza beyanından her zaman dönme hakkına sahip olduğu ve olumsuz irade beyanında bulunması halinde iş sözleşmesinin bundan etkilenmeyeceği yönünde bir güvenceye sahip olması gerekliliğidir[834]. Aksi halde rızanın varlığından bahsedilmeyeceği gibi iş ilişkisinin doğası gereği duraksamada bulunduğu durumlarda işçi lehine yorum ilkesi kapsamında konunun açıklığa kavuşturulması gerekir[835].

Kişisel verileri işlenen işçi istediği zaman kişisel verilerinin işlenmesine ilişkin verdiği açık rıza beyanından dönebilir. KVKK'da veri sahibinin bu hakkı

831) KVK Kurumu, Açık Rıza Rehberi, s. 3.
832) Helvacı, [2012], Gerçek Kişiler, s. 108; Küzeci, [2020], Kişisel Veriler, s. 233.
833) KVK Kurumu, 100 Soruda Kişisel Verilerin Korunması Rehberi, s. 26.
834) Article 29 - Data Protection Working Party, Opinion 15/2011 on the definition of consent, [2011],s. 25.
835) Süzek, [2019], İş Hukuku, s. 20; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 26.

herhangi bir şarta ve istisnaya da bağlanmamıştır[836]. Bu durumda açık rızanın geri alınması ileriye doğru etki oluşturur ve veri sorumlusu işverenin veri işleme faaliyetine son vermesi, işleme amacı ortadan kalkmış verileri imha etmesi gerekir[837]. Bu noktada belirtilmesi gereken önemli bir husus da kişilik hakkının korunması açısından Medeni Kanun m. 23 kapsamında ilgili kişinin açık rıza beyanını geri almaktan önceden feragat ettiğine ilişkin beyanda bulunmasının, buna yönelik yazılı belge vermesinin geçersiz olacağıdır. İşçi açık rızadan dönme hakkını veri sorumlusu işverene karşı, "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"in 5. maddesindeki öngörülmüş usullerden birisiyle kullanabilir[838]. Örneğin işverenin tüm işçilerin sağlık raporlarını, ilaç kullanımı ve aşı bilgilerini bir mobil uygulama üzerinden takip etmek için işçilerden açık rıza alması durumunda, işçilerden birisinin açık rıza beyanından dönmesiyle birlikte işlenme koşulu ortadan kalktığından KVKK m. 6/3'te belirlenmiş sağlık verilerinin işlenmesinin durdurulması gerekir.

Gerek WP 29 Çalışma Grubu[839] gerekse yerine kurulan EDPB[840] çeşitli görüşlerinde, iş ilişkisinde gerçekleştirilecek dijital izlemeye ilişkin alınacak rızanın özgür iradeye dayanmasına olanak bulunmadığını ve bunların hukuken geçerli olarak kabul edilmemesi gerektiği yönünde görüş açıklamıştır. KVK Kurumu yayımladığı rehberlerde aynı görüşü benimsemiştir[841]. Öte yandan iş

836) Sevimli, [2006], Özel Yaşam, s. 66; Selen Uncular, Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Seçkin Yayınları, 2. Baskı, Ankara, [2018], s. 59.
837) https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar (Erişim Tarihi: 21.11.2023); KVK Kurumu, Açık Rıza Rehberi, s. 6-7.
838) Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, Resmi Gazete'nin 10 Mart 2018 tarih ve 30356 sayılı nüshasında yayımlandı. https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm (Erişim Tarihi: 25.10.2022).
839) Article 29 WP, Rızanın tanımı için bkz. Opinion 15/2011 (WP 187), s. 12-14; İstihdam bağlamında kişisel verilerin işlenmesine ilişkin görüş için bkz. Opinion 8/2001 (WP 48) Bölüm 10, İşyerinde elektronik iletişimin izlenmesi, dijital izleme ile ilgili bkz. (WP 55) paragraf 4.2; İşyerinde veri işlemeye ilişkin görüş için bkz. Opinion 2/2017 (WP 249), paragraf 6.2, s. 6-7; EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, s. 9.
840) EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, [2020], s. 9 vd.
841) KVK Kurumu, Açık Rıza Rehberi, s. 6. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf

ilişkisinde işçiden kişisel verilerinin işlenmesi için açık rıza alınmasını fazla mesai, esaslı değişiklik gibi birçok konuda rıza alınmasıyla kıyaslayarak açık rızanın özellikle menfaatler dengesine uygun olduğu durumlarda geçerli olduğu değerlendirmesi yapılamaz. Zira bir menfaat karşılığı işçinin iradesini etkileyerek açık rızasını almak iradeyi sakatlayan bir durumdur. Örneğin dijital izleme uygulamalarıyla saha faaliyetlerinin izlenmesine veya uzaktan çalışmada kamerayı devamlı açık tutmasına açık rıza vermesi karşılığında işçiye prim verilmesi durumunda işçi bu yönde bir menfaati elde etmek amacıyla rıza beyanını açıkladığından özgür iradeyle verilmiş geçerli bir rızanın varlığından bahsedilmeyecektir[842]. Bu durumda işçinin açık rıza beyanını bir menfaat karşılığında etkilemek söz konusudur. Örnekleri açık rızanın tüm unsurları açısından değerlendirdiğimizde işçinin temel hak ve özgürlüklerine ilişkin olan haklarından kendisine sağlanan bir menfaat karşılığında vazgeçtiği ve iradesinin bu suretle sakatlığa uğratıldığı sonucuna ulaşılmaktadır[843].

b) Kanunlarda Açıkça Öngörülmesi

Kişisel verilerin açık rıza dışındaki işlenme şartları KVKK m. 5/2. fıkrasında düzenlenmiştir. Fıkrada öngörülen diğer veri işleme şartlarının bulunması durumunda kişisel veriler ilgili işçiden açık rızası alınmaksızın işlenebilir. Örneğin işverenin, işçinin özlük dosyasını oluştururken işleyeceği veriler İş Kanunu m. 75'te öngörülmüştür. Bu kanun hükmü kapsamında işçinin kişisel verileri açık rıza alınmaksızın işlenebilir[844]. KVKK m. 5/2-a bendinde hüküm altına alınmış olan "kanunlarda açıkça öngörülme" veri işleme şartı

842) KVK Kurumu bir kararında rızanın özgür iradeyle verilmesini şu şekilde değerlendirmiştir: "açık rızanın ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılması gerektiği, rızanın özgür iradeyle verilmiş olmasının kişilerin verileri üzerinde kontrol hakkına sahip olması ve bireylere gerçek bir seçim hakkının tanınmış olması ile sağlandığı, birey rıza vermemenin sonucunda hizmetten yararlanamıyor ise yani reddin bir yaptırımı var ise bu bireyin karar verme mekanizmasını etkileyecek bir duruma sebebiyet verebileceği…" https://kvkk.gov.tr/Icerik/7192/2022-137 (Erişim Tarihi: 21.11.2023).
843) EU, [2018], Handbook, s. 145.
844) Küzeci, [2020], Kişisel Veriler, s. 396; Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 136.

kapsamında kişisel veri işlenebilmesi için, kanunlarda açık bir düzenleme bulunması veya kanunda ikincil mevzuata yönlendirme yapılması söz konusu ise bu düzenlemelerde veri işlenmesi öngörülmesi durumunda kişisel veri işlenebilir. Örneğin, yukarıda değinilen özlük dosyasını tutmaya ilişkin hüküm kapsamında işveren, işe aldığı işçilerin kimlik bilgilerini, sigorta bildirimlerini, performans değerlendirme formlarını ve eğitim bilgilerini bu madde hükmüne uygun olarak özlük dosyasında işleyebilir[845]. 5510 sayılı Kanun kapsamında işverenin SGK bildirimlerini gerçekleştirmesi işçin kişisel veri işlemesi bu hükme uygun veri işlemeye örnek gösterilebilir.

Yukarıda açıklandığı üzere, KVKK m. 5/2 düzenlemesinde yer alan veri işleme şartının varlığı halinde açık rıza alınması hakkın kötüye kullanılması olarak değerlendirilecektir[846]. Önemle eklemek gerekir ki, veri işlemenin hukuki dayanağının bulunması veri sorumlusunu, KVKK m. 10'da öngörülen aydınlatma yükümlülüğünü ortadan kaldırmamaktadır. Bundan dolayı veri sorumlusu işverenin dijital izleme uygulaması vasıtasıyla veri işlemeye başladığı her durumda aydınlatma yükümlülüğünü yerine getirilmesi gerekmektedir. Diğer bir husus da KVKK m. 5'teki veri işleme şartlarının KVKK'nın kapsamının istisnası olan m. 28 düzenlemesiyle karıştırılmaması gerektiğidir. Zira KVKK m. 28/1'de sayılan durumlarda veri işlenmesi halinde KVKK hükümleri uygulanmaz.

c) Bir Sözleşmenin Kurulması veya İfası İçin Zorunlu Olması

Kişisel verilerin işlenmesi bir "sözleşmenin kurulması veya ifası" için gerekli olabilir. Bu veri işleme hukuka uygunluk sebebi KVKK m. 5/2-c bendinde "bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması" biçiminde

845) KVK Kurumu, Kişisel Verilerin İşlenme Şartları Rehberi, s. 6. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf (Erişim Tarihi: 25.10.2022).
846) KVK Kurulu kararı, 08.07.2019 Tarih ve 2019/206 Karar sayılı. https://kvkk.gov.tr/Icerik/6709/2019-206 (Erişim Tarihi: 03.04.2020).

düzenlenmiştir. KVK Kurumu'nun yayımladığı Rehberde[847] bu veri işleme şartına açıklık getirerek amaçla sınırlı olması gerektiğine vurgu yapılmıştır. GVKT m. 6/1-(b) bendinde de benzer bir düzenleme yer almakta, fakat sözleşmenin uygulanması veya bir sözleşme yapılmadan önce ilgili kişinin talebiyle belirli işlemler yapılması için gerekli olması yeterli görülmüştür[848]. ILO'nun Kişisel Veri Uygulama Kodu'nun "Genel İlkeler" başlıklı 5. maddesinin 1. fıkra düzenlemesinde kişisel verilerin adil biçimde işlenmesi ve iş sözleşmesinin ifasıyla ilgili olma koşulu aranmış ve işçinin istihdamı ile doğrudan doğruya ilgili olan nedenlerin varlığı halinde kişisel verilerin işlenebileceği düzenlenmiştir[849].

İş ilişkisinde işçinin kişisel verilerinin işlenmesinin asıl dayanağı iş sözleşmesidir. Bu nedenle veri sorumlusu işveren dijital izleme uygulamalarıyla işçi verisini işlemeye başlamadan önce, iş sözleşmesiyle ilgili olan ve KVKK'da açık rıza almaksızın veri işlemenin şartlarından birisi olan KVKK m. 5/2-c hükmü kapsamında değerlendirme yapması gerekmektedir. Eğer veri işleme faaliyeti doğrudan doğruya iş sözleşmesinin kurulması ve ifasıyla ilgiliyse bu durumda veri sorumlusu işveren açık rıza almaksızın dijital izleme uygulaması vasıtasıyla işçinin kişisel verisini işleyebilir.

Yukarıda ele alındığı üzere, KVKK'nın genel ilkelerinden birisi olan "amaçla bağlantılı sınırlı ve ölçülü veri işleme" ile eş değer düzenleme olan TBK m. 419/1 düzenlemesini birlikte değerlendirdiğimizde iş ilişkisinde her veri işleme faaliyetinin iş sözleşmesiyle doğrudan doğruya ilgili olma veri işleme şartı kapsamında değerlendirilmesine olanak bulunmamaktadır. Örneğin veri sorumlusu işveren, iş sözleşmesinin unsurlarından birisi olan işçinin ücretini ödemek için banka hesap bilgilerini işleyebilir[850]. Öte yandan, işverenin işyerinde güvenlik amacıyla kamera gözetlemesi gerçekleştirmesi, mülkiyeti korumak için internet

847) KVK Kurumu, [2019], Uygulama Rehberi, s. 75.
848) EU, [2018], Handbook, s. 151.
849 ILO, Protection of workers' personal data, [1997], s. 2.
850) WP 29, Opinion 8/2001 on the processing of personal data in the employment context. 5062/01/EN/Final WP 48, [2001], s. 15.

trafiğini izlemesi doğrudan doğruya iş sözleşmesinin ifasıyla ilgili değildir. Bu uygulamalar işverenin meşru menfaati, mülkiyete ilişkin hakları kapsamında kalmaktadır. Bundan dolayı işverenin hangi veri işleme şartı[851] kapsamında uygulamaları kullandığını belirlemesi ve işçiyi bu tespit sonrası aydınlatma yükümlülüğü kapsamında bilgilendirmesi ve KVKK m. 5/2'deki diğer veri işleme şartları yoksa açık rıza alarak kişisel veri işlemesi gereklidir.

d) Fiili İmkansızlık Sebebiyle Veri İşlemenin Zorunlu Olması

KVKK m. 5/2-b bendinde; "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" durumu kişisel verilerin işlenmesinin hukuka uygunluk sebebi olarak düzenlenmiştir[852]. Bu hüküm kapsamında örneğin işçinin çalışmak için gittiği orman, maden veya deniz işinde kendisinden haber alınamaması durumunda işçinin üzerinde bulunan telefon, çipli kart, GPS sinyali göndericisi gibi teknik araçlarla yerinin tespit edilmeye çalışılması, bu esnada verilerinin işlenmesinde, dijital izleme gerçekleştirilmesinde fiili imkansızlık bulunması sebebiyle kişisel verileri işlenebilir. Öte yandan, fiili imkansızlık ortadan kalktıktan sonra işçinin işlenen verileriyle ilgili bilgilendirilmesi (aydınlatma yükümlülüğü) ve işlenen kişisel verilerle ilgili KVKK yükümlülüklerinin yerine getirilmesi gerekir.

e) Veri Sorumlusunun Hukuki Yükümlülüğünü Yerine Getirmesi

İş ilişkisinde işveren hukuki yükümlülüklerini yerine getirmek amacıyla kişisel veri işlemek zorunda kalabilir. Bu husus KVKK m. 5/2-ç bendinde; "veri

851) Kişisel veri işleme faaliyetinin amacına bağlı olarak bir faaliyette aynı anda birden fazla sayıda kişi kişisel veri işleme şartı (KVKK m. 5/2) bulunabilir. Örneğin, fabrika etrafında kamera gözetlemesi gerçekleştirilmesi hem işverenin meşru menfaati, hem de hukuki yükümlülükleri yerine getirmek veri işleme şartlarına dayanır. Bkz. KVK Kurumu, Kişisel Verilerin İşlenme Şartları Rehberi, s. 3-4.
852) KVK Kurumu, [2019], Uygulama Rehberi, s. 74-75.

sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" düzenlemesiyle açık rıza almaksızın kişisel veri işlemenin hukuka uygunluk sebeplerinden birisi olarak düzenlenmiştir. Örneğin çok tehlikeli sınıfta faaliyet gösteren bir akaryakıt rafinerisinde işçilerin çalışma sahasında dijital izleme uygulamalarıyla takip edilmesi TBK m. 417 kapsamında "işverenin, işyerinde iş sağlığı ve güvenliğinin sağlanması için gerekli her türlü önlemi alma" yükümlülüğü kapsamında bir hukuka uygunluk sebebidir[853].

Nitekim, KVK Kurumu'na yapılan bir başvuruda veri sorumlusu üniversitenin kişisel verileri içeren belgeleri web sitesinde yayımladığı, aslında TÜBİTAK Başkanlığı tarafından kişisel verileri de ihtiva eden belgelerin YÖK Başkanlığı'na bilgi amaçlı gönderildiğini, sonrasında bu belgelerin bilgi amaçlı üniversitelere gönderildiği, gizli ibareli söz konusu belgelerin veri sorumlusu üniversite tarafından tüm personele e-posta ile gönderildiği ve web sayfasında yayımladığı şikayete konu edilmiştir. KVK Kurulu, konuyla ilgili kanun ve Doçentlik Yönetmeliği'ni de incelemeye konu ederek bu paylaşımı yapmada veri sorumlusu üniversitenin KVKK m. "5/2-ç ve e" bentleri kapsamında bir hukuki yükümlülüğünün bulunduğuna karar vermiştir[854]. Aynı doğrultuda işverenin, elektronik ortamda SGK primlerini ödemek için, işçilerin bilgilerini SGK ile paylaşması hukuki yükümlülüğün yerine getirilmesi düzenlemesi kapsamında değerlendirilir[855].

f) İlgili Kişinin Kendisi Tarafından Alenileştirilmiş Olması

Sosyal medya platformlarının yaygınlaşması işçilerin birçok kişisel verisini bu dijital uygulamalar üzerinde alenileştirmesini beraberinde getirmektedir. KVKK

853) Bkz. § 5. II. 2. b.
854) KVK Kurulu, "Veri sorumlusu Üniversitenin ilgili kişinin kişisel verilerini içeren belgeleri internet sitesinde yayımlaması" hakkında Kişisel Verileri Koruma Kurulunun 04/11/2021 tarihli ve 2021/1127 sayılı Karar Özeti" https://kvkk.gov.tr/Icerik/7267/2021-1127 (Erişim Tarihi: 25.10.2022).
855) Sevimli, [2006], Özel Yaşam, s. 146; Küzeci, [2020], Kişisel Veriler, s. 393.

m. 5/2-d bendinde ilgili kişinin kişisel verilerini alenileştirmesi kişisel veri işleme şartı olarak düzenlenmiştir. GVKT m. 6'da sayılan kişisel verilerin işlenmesinde hukuka uygunluk nedeni olarak alenileştirme düzenlenmemiştir. Alenileştirmenin verileri işlenen ilgili kişi açısından ortaya çıkardığı risk, bu istisna dar yorumlanmadığında özel hayatın gizliliğinin ihlaline sebebiyet verebileceğidir. Bu sebeple alenileştirmeye ilişkin değerlendirme yapılırken meşru amaç kapsamında sınırlı ve ölçülü veri işlendiğine dikkat edilmelidir[856].

KVK Kurul kararlarında[857] ve KVK Kurum rehberlerinde[858] alenileştirme dar yorumlanarak "alenileştirme iradesi" kapsamında veri işleme ile sınırlandırılmıştır. Örneğin bir işçinin sosyal medya hesabında arkadaşlarıyla katıldığı bir iş yemeğinin fotoğrafını paylaşması işveren açısından bu yemekle ilgili bir iç yazışmada bu veriyi kullanması alenileştirme iradesine uygundur. Öte yandan işverenin bu örnekteki fotoğrafı pazarlama kampanyasında kullanması alenileştirme iradesine aykırı veri işleme olarak nitelendirilecektir. Aynı husus bir işçi adayının bloğunda iş teklifleri için özgeçmişini yayımlaması durumu için de geçerlidir. İşverenin bu özgeçmişi işe alım için değerlendirmesi, bu amaçla özgeçmişteki telefonla işçi adayı ile iletişime geçmesi alenileştirme iradesine uygunken, telefon numarasını pazarlama faaliyeti için araması alenileştirme iradesine aykırı veri işleme olarak kabul edilecektir.

---

856) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 144; Küzeci, [2020], Kişisel Veriler, 398.

857) "Veri sorumlusu işveren tarafından eski işçisi olan ilgili kişinin kurumsal e-posta hesabına aydınlatma yapılmaksızın erişilmesi" hakkında Kişisel Verileri Koruma Kurulu'nun 25/11/2021 tarihli ve 2021/1187 sayılı Karar Özeti, Karar Tarihi: 25/11/2021, Karar No: 2021/1187. KVK Kurul'u kararda çalışma ilişkisinde kişisel verilerin işlenmesini AİHM ve AYM kararları kapsamında değerlendirmiştir. Kararda alenileştirme veri işleme şartına şu şekilde açıklık getirilmiştir: "…Buna göre, ilgili kişinin kendisi tarafından alenileştirilen, bir başka ifadeyle ilgili kişinin alenileştirme iradesi ile herhangi bir şekilde kamuoyuna açıklamış olduğu kişisel veriler, ayrıca ilgili kişinin açık rızası olmaksızın alenileştirme amacı ve Kanunun 4. maddesinde düzenlenen genel ilkeler kapsamında işlenebilecektir." şeklinde açıklanan "alenileştirme" kavramı ile ilgili olarak "Kişisel Verilerin İşlenme Şartları" başlıklı rehberde de "kişisel verinin aleni kabul edilebilmesi için ait olduğu kişinin aleni olmasını istemesi gerekir. Başka bir ifade ile, alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin varlığı gerekir. Yoksa bir kişinin kişisel verisinin herkesin görebileceği bir yerde olması aleni olmasını sağlamaz. Ayrıca, alenileştirme durumunda kişisel verinin amacı dışında da kullanılmaması gerekmektedir."
KVK Kurumu, [2019], Uygulama Rehberi, s. 44.

858) KVK Kurumu, [2019], Uygulama Rehberi, s. 44.

İlgili kişinin web sitesinde veya sosyal medyada paylaşmış olduğu verilerinin alenileştirilmesi iradesi dışında işverenlerin işlemeye konu etmesi hukuka aykırı olacaktır. KVKK Kurul'u bu hususta vermiş olduğu bir kararda alenileştirme iradesi dışında verinin işlenmesinin hukuka aykırı olacağını; "alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin ne olduğuna bakılması gerektiği, bir kişinin kişisel verisinin herkesin görebileceği bir yerde olmasının aleni olmasını sağlamayacağı, alenileştirme durumunda kişisel verinin alenileştirme amacı kapsamında kullanılması gerektiği, somut olayda, alenileştirme bulunuyor olsa dahi ilgili kişinin reklam faaliyetleriyle ilgili kendisiyle iletişim kurulması amacıyla söz konusu kişisel verileri alenileştirmemiş ise, gerçekleştirilecek olan kişisel veri işleme faaliyetinin hukuka uygun olmayacağının değerlendirildiği"[859] biçiminde ifade etmiştir.

g) Bir Hakkın Tesisi, Kullanılması veya Korunması İçin Zorunlu Olması

KVKK m. 5/2-e bendinde; "bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" durumu veri işlemenin hukuka uygunluk sebebi olarak düzenlenmiştir. Buna göre örneğin işverenin işçilere ücret ödeme borcu bulunmaktadır, bu borç kapsamında ücretin ödenebilmesi için işçinin banka hesap bilgilerini işlemesi gerekir. İşverenin bu kapsamdaki veri işleme faaliyeti iş sözleşmesiyle (KVKK m. 5/2-c) ilgili olduğu gibi bir hakkın kullanılması veya korunmasıyla ilgili olma hukuka uygunluk sebebiyle de ilgilidir.

Bentte yer alan "hakkın tesisi" ifadesinde hakkın kime ait olduğuna ilişkin bir belirlilik olmamakla birlikte genel olarak KVKK m. 5 veri sorumlusu açısından kişisel verilerin işlenme şartlarını düzenlediği hususu dikkate alındığında, m. 5/2-e bendinin veri sorumlusuna yönelik olduğu anlaşılmaktadır. Doktrinde bu kişisel

859) KVK Kurul Kararı, K. 2020/67, Karar Tarihi: 27.01.2020; Aynı yönde KVK Kurulu, K. 2022/861, Karar Tarihi: 01.09.2022

veri işleme şartından bulunan hak kavramının belirsiz ve geniş bir anlama sahip olması ve "zorunlu olma" şartının ise bendin anlamını muğlaklaştırması sebebiyle eleştirilmiştir[860].

h) Veri Sorumlusu İşverenin Meşru Menfaati İçin Zorunlu Olması

KVKK m. 5/2-f bendine göre; "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" durumunda kişisel veri açık rıza alınmaksızın işlenebilir. KVK Kurumu yayımladığı rehberde ve KVK Kurulu kararlarında[861] meşru menfaatin sınırları, koşulları ve hangi durumlarda bu veri işleme şartı kapsamında kişisel veri işleneceğini somutlaştırmıştır[862]. Buna göre öncelikli olarak, KVKK m. 5/2 düzenlenen kişisel veri işleme şartlarına ilişkin olarak istisnaların dar yorumlanması kuralı kapsamında bir sınırlandırmanın yapılması gerekmektedir. Ayrıca kişisel verilerin işlenmesinin veri sorumlusuna sağladığı menfaat ile ilgili kişinin verileri, temel hak ve hürriyetleri üzerindeki haklarının arasında bir dengenin kurulması gerekmektedir[863].

Meşru menfaatin bulunması veri işleme şartının uygulanabilmesi için öncelikli olarak halihazırda meşru menfaatin bulunması ve bunun belirli ve açık olduğunun tespit edilmesi, sonrasında ise bu menfaatin kişisel verileri işlenen ilgili kişinin temel hak ve özgürlüklerine zarar verip vermediğinin değerlendirilmesi gerekir[864]. Örneğin işverenin satış temsilcisi olan işçilerini kendilerine ayrılan bölgelerde müşteri ziyaretlerini gerçekleştirip gerçekleştirmediklerini GPS gibi dijital izleme uygulamalarıyla tespit etmesinde bir meşru menfaati vardır[865].

---

860) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 142; Küzeci, [2020], Kişisel Veriler, 400.
861) Kişisel Verileri Koruma Kurulu'nun 25/11/2021 tarihli ve 2021/1187 sayılı Karar Özeti, Karar Tarihi: 25/11/2021, Karar No: 2021/1187. Karar detayı için bkz. https://kvkk.gov.tr/Icerik/5434/2019-78 (Erişim Tarihi: 28.10.2022).
862) KVK Kurumu, [2019], Uygulama Rehberi, s. 78.
863) KVK Kurumu, [2019], Uygulama Rehberi, s. 78.
864) KVK Kurumu, [2019], Uygulama Rehberi, s. 79.
865) KVK Kurulu, akaryakıt dağıtıcısı olan bir başvurucunun "istasyonlarda plaka bazlı otomatik sistemlerle kişisel veri işlenmesiyle" ilgili başvurusu ile ilgili verdiği kararda meşru menfaati şu

Eklemek gerekir ki, bu yöntemle dijital izleme uygulaması kullanırken işçilerin bilgilendirilmesi ve işçinin özel hayat alanını gasp edecek nitelikte bir dijital izlemenin gerçekleştirilmesi meşru menfaat veri işleme şartına aykırı olacaktır.

Belirtmek gerekir ki, işyeri güvenliğinin sağlanmasında işverenin mülkiyet hakkından ve gözetme borcundan doğan hak ve yükümlülükleri bulunmaktadır. Bu meşru menfaat kapsamında işverenin fabrikanın güvenliğini sağlamak için işyerine girişte ve işyerinin etrafına kamera yerleştirip kamera gözetlemesi gerçekleştirmesi hukuka uygundur (KVKK m. 5/2-f). İşveren bu meşru menfaat kapsamında işçilerin temel hak ve özgürlüklerini ihlal etmeden kameraların bulunduğu yerlere katmanlı aydınlatma işaret ve ifadelerini ekleyerek kameranın işlediği görsel ve işitsel kayıtları işleyebilir[866].

i. Özel Nitelikli Kişisel Verilerin İşlenme Şartları

Yukarıda değerlendirildiği üzere, işlenmesi halinde ilgili kişinin dezavantajlı duruma düşmesine sebebiyet veren veriler özel nitelikli kişisel veri olarak düzenlenmiştir. Sınırlı sayıda olan (KVKK m. 6/1) bu verilerin işlenmesi ve

---

şekilde değerlendirmiştir: "Bununla birlikte, 6698 sayılı Kanunun 5 inci maddesinin ikinci fıkrasının (f) bendine göre "ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması" hali tespit edilirken veri sorumluları tarafından; Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması, Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi, Meşru menfaatin halihazırda mevcut, belirli ve açık olması, İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması, Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması, Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması, Kişisel verilerin bir veri kayıt sisteminde amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması, Kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması, Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması hususlarının değerlendirilmesi gerektiği…" KVK Kurulu, K. 2019/78 karar Tarihi: 25.03.2019.

866) KVK Kurumu, Aydınlatma Yükümlülüğü Rehberi, s. 14,19.

korunması daha sıkı koşullara bağlanmış ve KVKK m. 6/2'de kural olarak açık rıza dışında işlenmesi yasaklanmıştır[867]. KVKK m. 6/3'te ise özel nitelikli kişisel verilerin işlenmesi diğer hukuka uygunluk sebeplerinin varlığı (KVKK m. 5/2) halinde işlenebileceği "sağlık" ve "cinsel hayata" ilişkin veriler ayrı tutularak hüküm altına alınmıştır[868]. Buna göre, "sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ancak kanunlarda öngörülen hallerde; sağlık ve cinsel hayata ilişkin kişisel veriler, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar" tarafından[869] işlenebilecektir.

Önemle belirtmek gerekir ki sağlık ve cinsel hayata ilişkin veriler dışındaki özel nitelikli kişisel verileri açık rıza olmaksızın işleyebilmek için kanunlarda öngörülmüş olması gerekmektedir (KVKK m. 5/2 ve 6/3). Ayrıca bu verilerin korunması için KVK Kurulu tarafından asgari koruma tedbirleri 2018/10 sayılı Kurul Kararı'nda belirlenmiştir. Veri sorumlusu işveren örneğin dijital izleme ile işçinin biyometrik verisini işlemesi halinde bu verilerin korunması için Kurul Kararı'nda öngörülen asgari koruma tedbirlerini almakla yükümlüdür[870].

KVK Kurumu özel nitelikli kişisel verilere ilişkin yayımladığı rehberde, özel nitelikli kişisel verilerin kural olarak işlenmesinin yasak olduğunu ifade ederek, tüm temel hak ve özgürlüklerde olduğu üzere bu yasağın da mutlak olmadığını, bu hakkın da Anayasa m. 13 hükmü çerçevesinde sınırlandırılabileceğini, özellikle yaşam hakkı, haberleşme özgürlüğü gibi temel hak ve özgürlüklerin özel nitelikli kişisel veri işlenmesini gerektirdiğini ifade

867) KVK Kurumu, [2019], Uygulama Rehberi, s. 80.
868) Gürsel, [2016], İşçinin Kişisel Verileri, s. 167 vd.
869) KVK Kurumu, Özel Nitelikli Kişisel Verilerin İşlenme Şartları Rehberi, s. 2. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/0ef45a05-ac30-4f35-bc4b-3b2cbefc9864.pdf (Erişim Tarihi: 13.12.2023).
870) KVK Kurul Kararı, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı. https://www.kvkk.gov.tr/Icerik/4110/2018-10 (Erişim Tarihi: 30.10.2022).

etmiştir[871]. Bu kapsamda örneğin işverenin tehlikeli sınıfta faaliyet gösteren dinamit, havai fişek üreten tesise biyometrik verilerle girişi sağlaması, işyerinde biyometrik esaslı takip gerçekleştirmesi yaşam hakkının korunmasıyla ilgili olduğundan özel nitelikli kişisel veriler aydınlatma yükümlülüğü yerine getirilerek dijital izleme uygulamaları vasıtasıyla işlenebilecektir. İlgili başlıkta ele alındığı üzere aynı husus kamu sağlığının korunması için de geçerlidir. Kamu sağlığının korunması gerektiğinde KVKK m. 28/1'deki istisna kapsamında veri işlenebilir.

5. Medeni Kanun'daki Hukuka Uygunluk Sebepleri ile Kişisel Veri İşleme Şartları İlişkisi

Medeni Kanun'daki hükümler kapsamında hukuka uygunluk sebebi değerlendirmesi yapılırken iki unsur dikkate alınmaktadır. Bunlardan ilki bir kişinin temel veya özel olarak düzenlenmiş koruma normlarını ihlal etmesi biçiminde ortaya çıkar. İkinci unsur ise temel veya özel koruma normlarını ihlal eden kişinin bu şekilde davranmasına izin veren bir düzenlemenin bulunmasıdır[872]. Genel olarak hukuka uygunluk sebepleri üç başlık çerçevesinde ele alınmaktadır. Bunlardan birincisi kamu menfaatinin bulunması, ikinci olarak özel bir menfaatin bulunması durumudur. Böyle bir durumda çatışan diğer menfaate göre bu menfaatler üstün tutulur. Üçüncü hukuka uygunluk sebebi ise hakkı etkilenen kişinin buna rıza göstermesi halidir[873]. Rızanın geçerli olabilmesi için rıza beyanının kişiliği koruyan düzenlemelere aykırı olmaması ve rızanın bilgilendirme ile özgür iradeye dayanması gerekmektedir[874].

Medeni Kanun m. 24/2'de öngörülen hukuka uygunluk sebepleri ile TBK m. 63'te hüküm altına alınan "hukuka aykırılığı kaldıran hâller" genel düzenlemelerdir ve kişisel verileri özel olarak düzenleyen KVKK'nın genel ilkeleri,

871) KVK Kurumu, Özel Nitelikli Kişisel Verilerin İşlenme Şartları Rehberi, s. 2.
872) Eren, [2019], Borçlar Genel, s. 676.
873) Eren, [2019], Borçlar Genel, s. 677.
874) Bkz. § 6. II. 4. a.

aydınlatma yükümlülüğü, verinin aktarılması ve korunması gibi veriyi koruyucu düzenlemeler bu genel düzenlemelerde yer almamaktadır. Ayrıca, Medeni Kanun m. 24/2'de hüküm altına alınan rıza "açık rıza" olmayıp, rıza zımni olarak da gösterilebilir. Bu sebeple işveren, dijital izleme uygulamaları vasıtasıyla kişisel veri işlerken genel hükümler yerine, hukuka uygunluk sebeplerini özel olarak düzenlemiş olan KVKK m. 5 ve 6 hükümlerini dikkate alması, sayılan genel düzenlemeler hukuka uygunluk nitelendirmesinde dikkate alınmaması gerekmektedir[875].

İş hukuku kişilik haklarının korunmasında işçiye sınırsız bir özgürlük vermez ve işçinin bu hakları üzerinde sınırlandırıcı sonuçlar ortaya çıkarır[876]. Bu durum kişisel verilerin işlenmesi dışındaki yönetim hakkına yönelik uygulamalarda daha bariz bir şekilde kendisini gösterir. Örneğin bir havayolu şirketinin uçuş ekibine alkol ve uyuşturucu testi yapması; çok tehlikeli sınıfta faaliyette bulunan bir nükleer enerji tesisine biyometrik veri esaslı girişlere izin verilmesi ve işyerinde işçilerin izlenmesinde hem işverenin hem de üçüncü kişilerin üstün nitelikte kamusal ve özel menfaatleri bulunmaktadır. Bu durumlarda ayrıca KVKK m. 5/2 kapsamında hukuka uygunluk sebebi (örneğin meşru menfaat, hakkın kullanılması ve korunması) dayanak yapılarak gerçekleştirilecek dijital denetim KVK hukukuna ilişkin yükümlülüklerin de yerine getirilmesi[877] kaydı ile hukuka uygun kabul edilecektir.

Genel hükümlere göre kişilik hakkına ilişkin bir nitelendirme yapmak gerektiğinde kişilik hakkı ihlal edilen kişinin rızasının hukuka aykırılığı ortadan kaldırabilmesi için rızanın Medeni Kanun m. 23 ve TBK m. 26 ve 27/1

875) Yücedağ, MK ve TBK'nın hukuka uygunluk sebeplerinin dikkate alınmayacağını şu şekilde ifade etmektedir: "KVKK'da hukuka uygunluk sebepleri özel olarak düzenlendiğinden, daha genel nitelikte olan MK m. 24(2) ve TBK m. 63 ve 64 hükümlerinde yer alan hukuka uygunluk sebepleri işlemenin hukuka uygunluğunun tayininde dikkate alınmaz. Kişisel verinin işlenmesinin hukuka uygun olup olmadığı değerlendirilirken dikkate alınması gereken hükümler KVKK m. 5 ve 6 hükümleridir." Yücedağ, [2017], Genel Hukuka Uygunluk Sebepleri, s. 771-772.
876) Süzek, [2019], İş Hukuku, s. 395; Sevimli, [2006], Özel Yaşam, s. 65 vd.;
877) Bkz. § 6. II.

düzenlemelerine uygun olması gerekmektedir[878]. İşçinin özgürlüklerinden vazgeçmesi veya bunları ahlaka ve hukuka aykırı olacak şekilde sınırlandırmasına ilişkin açıkladığı rıza beyanı bu düzenlemeler kapsamında geçersizlik yaptırımıyla karşı karşıya kalacaktır[879]. Medeni Kanun hükümlerinde öngörülen rıza açısında da ilgili kişinin rızasının geçerliliği, rızanın sonuçları hakkında bilgi sahibi olması ve rızanın özgür iradeyle verilmiş olmasına bağlıdır[880]. Ayrıca kişilik hakkı zedelenen ilgili kişinin rızasından bahsedebilmek için kişinin rıza gösterebileceği üzerinde tasarruf etme hakkı bulunduğu ve sınırlarının belirlendiği[881] bir hakkın bulunması gerekir. Örneğin işçinin işyerinde geçirdiği bir iş kazasıyla ilgili görüntüleri, işverenin benzer kazaları önlemek için vereceği bir eğitimde kullanması için rıza gösterebilir. Kişinin üzerinde tasarruf etme imkanı bulunmayan haklarda kişinin rıza göstermesi veya verilen rızanın dışındaki haklara gerçekleştirilen müdahale hukuka aykırı olacaktır. Özellikle kişinin kişilik hakkına yönelmiş her türlü müdahaleye önceden rıza göstermesi geçersizdir[882].

Medeni Kanun m. 24'te öngörülen üstün nitelikli kamu veya özel yararın bulunması halinde kişiliğe saldırı hukuka aykırı görülmez[883]. Özel yarar kişiye veya üçüncü bir kişiye ilişkin olabilir[884]. Örneğin işçinin geçirdiği bir kaza sonrası yaralanması durumunda, hayatının kurtarılması için tıbbi müdahale yapılması, ameliyata alınmasında işçinin özel yararı bulunmaktadır. Aynı doğrultuda örneğin bir salgın hastalıkta işçiye aşı yaptırma zorunluluğu getirilmesinde veya termal

878) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 208-209; Dural/Öğüz, [2022], Kişiler Hukuku, s.139; Bilge Öztan, Şahsın Hukuku: Hakiki Şahıslar, Turhan Kitabevi, Ankara, 2000, s.148, Öztan, [2021], Temel Kavramlar, s.2 61; Hüseyin Hatemi, Medeni Hukuka Giriş, On İki Levha Yayınları, İstanbul, [2004], s. 92; Serap Helvacı, Türk ve İsviçre Hukukunda Kişilik Hakkını Koruyucu Davalar, Beta Basım, İstanbul, [2001], s. 99-100.
879) Sevimli, [2006], Özel Yaşam, s. 65
880) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 209; Yargıtay 22. HD., E. 2015/28830 K. 2018/15646 T. 25.6.2018.
881) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 208.
882) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 208; Serozan, [2013], Medeni Hukuk, s. 467-468; Serap Helvacı, Gerçek Kişiler, Legal Yayınevi, 4. Baskı, İstanbul 2012, s. 145; Helvacı, [2001], Koruyucu Davalar, s. 107.
883) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 214; Serozan, [2013], Medeni Hukuk, s. 467-468.
884) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 214.

kamera özelliği bulunan sistemlerle işçinin sağlık verisini işlemede üstün kamu yararı bulunmaktadır. Bu durumlarda kişinin, kişiliğine gerçekleştirilen müdahaleler hukuka aykırı olarak nitelendirilemez[885]. Bu genel hukuka uygunluk sebebi kişisel veriler açısında KVKK m. 5/2-b bendinde yer alan: "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" hükmüne paralel bir hukuka uygunluk sebebi öngörmektedir.

Kanunun verdiği bir yetkinin kullanılması durumu hukuka aykırılığı ortadan kaldıran bir diğer hukuka uygunluk sebebidir. Kişinin hürriyeti ve güvenliği (Anayasa m. 19), özel hayatının gizliliğinin korunması (Anayasa m. 20), konut dokunulmazlığı (Anayasa m. 21) ve haberleşme hürriyeti (Anayasa m. 22) Anayasa kapsamına kapsamında güvenceye alınmıştır. Diğer yandan Anayasa m. 28'de basının hür olduğu ve sansür edilemeyeceği güvence altına alınmıştır. Bu itibarla bir kişinin karıştığı bir suçta suçüstü yakalanması halinin haberleştirilmesinde kişinin görsellerinin ve isminin kullanılması kişilik hakkına hukuka aykırı olarak saldırı şeklinde yorumlanamaz. Aynı doğrultuda kişinin Anaysa m. 74 kapsamında tanınan dilekçe hakkını kullanarak kamu denetçisine başvuruda bulunması başvuruya konu ilgili kişinin hakkının zedelenmesi biçiminde değerlendirilmez[886]. KVKK'da ise bu hukuka uygunluk sebebiyle paralellik oluşturacak şekilde kişisel verilerin işlenme şartı olarak m. 5/1-a bendinde "kanunlarda öngörülme" hukuka uygunluk sebebi olarak düzenlenmiştir.

Kamu menfaati ve özel yarar bulunması durumlarını örneklediğimizde, örneğin maden işlerinde çalışan işçilerin çalışma alanlarında anlık konum bazlı dijital izlenmesinde kamu yararı bulunmaktadır. Bu durumda işçi işyerinde özel hayatına saygı hakkının ihlal edildiğini ileri süremeyecektir. Yine nükleer santral

885) Serozan, [2013], Medeni Hukuk, s. 472-473; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 218-219.
886) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 233.

faaliyetini yürüten bir işyerinde, işyerine girişte işçilerin parmak izi veya retina taraması ile girmesinin koşul haline getirilmesi; akaryakıt tanker sürücülerinden alkol ve uyuşturucu testi[887] istenmesi örneklerinde kamu menfaati de bulunmaktadır. Sahada müşteri ziyareti gerçekleştiren işçilerin lokasyon bilgilerinin dijital izleme uygulamalarıyla takip edilmesi, araç tahsis edilen personelin araç kullanırken işyeri talimatlarına uygun davranıp davranmadığını kontrol etmede işverenin özel menfaati bulunmaktadır. Bu durum işçinin özel hayat ve kişisel verileri koruma menfaatlerini sınırlandırır.

Medeni Kanun m. 24/2 kapsamında işçinin vereceği rıza açık veya örtülü olması mümkünken[888], KVKK özgür iradeye dayanan açık rıza şartı aranmıştır. Medeni hukukta rızanın geçerlilik şartları; bilgilendirmeye dayanması, rıza iradesinin dışa vurulmuş olması ve rızanın ahlaka aykırı olmaması biçiminde ifade edilmiştir[889]. Belirtmek gerekir ki, kişisel verileri işlenen ilgili kişi açık rıza beyanından döndüğünde bu ileriye etki eder ve rıza kapsamında yapılmış işlemleri hukuka aykırı hale getirmez. Örneğin iş kazası geçiren işçinin fotoğraflarının ve olay anı görüntülerinin işveren tarafından eğitim amaçlı kullanılmasına vermiş olduğu rızadan döndüğünde bu geçmişte gerçekleştirilen eğitimleri hukuka aykırı hale getirmez. Aynı durum işçinin sosyal medyada belirli arkadaş gruplarına paylaştığı fotoğraflarının işveren tarafından kullanılmasına ilişkin verilmiş olduğu rıza için de geçerlidir[890].

887) Yüksek güvenlik gerektiren tesislerde (nükleer santral gibi) uyuşturucu testi yapılabileceğine ilişkin AİHM kararı için bkz. Wretlund v. Sweden. https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-23775&filename=WRETLUND%20v.%20SWEDEN.docx&logEvent=False

888) Sevimli, [2006], Özel Yaşam, s. 65 ve 324. dipnotta atıf yapılan yazarlar; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 213.

889) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 208-209; Serozan, [2013], Medeni Hukuk, s. 467-468; Dural/Öğüz, [2022], Kişiler Hukuku, s. 139; Helvacı, [2012], Gerçek Kişiler, s. 119.

890) Yargıtay 6. HD, 2003/3322 E., 2003/8240 K., 23.06.2003 T. sayılı kararında, fotoğrafın çekilmesi ve yayımlanması için verilen rızadan dönülmesi halinde sonrasında hukuka aykırı kullanım bulunduğunu ileri sürerek kişiliğe saldırı bulunduğunu ileri sürmenin mümkün olmadığına karar vermiştir. Ancak rızanın alınmasından sonra fotoğrafların yayımlanması olayı hukuka aykırı hale getirir.

6. Dijital İzleme Uygulamalarında Veri Sorumlusu İşverenin Aydınlatma ve Veri Koruma Yükümlülükleri

Kişisel verilerin KVKK temel ilkelerine ve m. 5 ve 6 hükümlerine uygun işlenmesi veri sorumlusu işverenin belirli yükümlülükleri yerine getirmesini ortadan kaldırmaz. İş ilişkisi açısından veri sorumlusu işveren, işçiyi veri işleme faaliyetinden önce işlenen verileri ile ilgili olarak aydınlatma yükümlülüğüne uygun bilgilendirmesi, kişisel verilerin işlenmesi için tüm teknik ve idari tedbirleri alması ve kişisel verileri işlerken denetlenebilir ve şeffaf bir veri işleme faaliyeti oluşturması gerekir. Bu itibarla KVK hukuku kapsamında veri sorumlusunun şeffaflık ilkesiyle ilgili olan aydınlatma yükümlülüğü, VERBİS kayıt yükümlülüğü ve kişisel verileri koruma yükümlülükleri bu başlıkta ele alınacaktır.

a) Aydınlatma Yükümlülüğü

KVK hukuku insanın doğuştan sahip olduğu ve insan hakkının en temel kavramı olan insan onurunu koruma amacı gütmektedir. Bunun bir gereği olarak bireyin dijital izleme uygulamalarıyla verilerinin işlenmesine rıza göstermesi, dahası sosyal medya uygulamalarında kişisel verilerini paylaşmış olması fark etmeksizin insan onurunun korunması amacının bir gereği olarak KVK hukuku kapsamında kişisel verileri korunur[891]. Yukarıda incelendiği üzere kişisel verilerin işlenmesinde şeffaflığın sağlanması ve ilgili kişinin işlenen verileriyle ilgili bilgi sahibi olması amacıyla genel ilkeler, açık rıza, veri işleme şartları ve aydınlatma yükümlülüğü gibi veri koruma enstrümanları geliştirilmiştir[892]. Bu enstrümanlardan

891) Gary T. Marx, Undercover: Palice Surveillance in America, Berkeley, University of California Press, [1988], s. 159 vd.

892) Aydınlatma metninde KVK Kurumu'nun hangi unsurları aradığına ilişkin KVK Kurul Kararı için bkz. "Aydınlatma ve açık rıza metinlerinin üyelere sunulan sözleşme metni içerisinde değil ayrıca düzenlenmesi, açık rızanın ilgili kişilere her bir faaliyet açısından onay verme ve vermeme seçeneklerini içerecek şekilde sunulması, aydınlatma metninin Kanun'un 10'uncu maddesinin yanı sıra Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in ilgili hükümlerine uygun şekilde düzenlenmesi ve yapılan işlemlerin sonucundan Kurulu bilgilendirmesi hususunda veri sorumlusunun talimatlandırılmasına" karar vermiştir. KVK Kurulu, "Spor salonu işletmecisi olan veri sorumlusunun, özel nitelikli kişisel veri niteliğini haiz kan grubu

anahtar niteliğine olanı ve kişisel verilerin korunmasının merkezini oluşturan, ilgili kişiye belirli içerikte sunulması zorunlu olan "aydınlatma yükümlülüğü" metinleridir. Aydınlatma yükümlülüğü metni kapsamında ilgili kişi veri işleme faaliyeti, işlenen verileri, veri işleme amacı ve hakları hakkında bilgi sahibi olmaktadır[893].

KVKK m. 10'da, GVKT m. 13 ve 14'te[894] düzenlenmiş olan aydınlatma yükümlülüğü, uluslararası düzenlemelerde BM'nin Rehber İlkeleri'nin 3. maddesinde ve 108 sayılı Sözleşme'nin 8. maddesinde düzenlenmiştir. Ayrıca KVK Kurumu aydınlatma yükümlülüğünün yerine getirilmesinde uyulacak esaslar için "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği" yayımladı[895]. Aydınlatma yükümlülüğünün içeriğinin, KVKK m. 4'te düzenlenen genel ilkelere ve Tebliğin 4. maddesine uygun olmasının yanında asgari olarak veri sorulusunun kimliğini, kişisel verilerin işlenme amacını, kişisel verilerin kimlere aktarılacağı ve aktarılma amacı, kişisel verilerin işlenme yöntemi ve hukuka uygunluk sebebi ile KVKK m. 11'de sayılmış olan ilgili kişinin haklarını kullanma yöntemlerini de içermesi gerekir[896].

GVKT m. 14 kişisel verilerin, veri sahibinden elde edilmediği durumlarda sağlanacak bilgileri düzenlemektedir. KVKK'da bu maddeyi karşılayan bir düzenleme bulunmamaktadır. KVK Kurumu yayımladığı Tebliğ'in 6. maddesinde

---

verisini ilgili kişinin açık rızasını almaksızın işlemesi hakkında Kişisel Verileri Koruma Kurulunun 23/12/2022 tarih ve 2022/1357 sayılı Karar Özeti" https://kvkk.gov.tr/Icerik/7594/2022-1357 (Erişim Tarihi: 14.11.2022).

893) Çekin, [2020], Kişisel Veriler, 119; Şehriban İpek Aşıkoğlu, Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-, Kişisel Verilerin Korunması Dergisi, C. 1, S. 2, [2019], s. 42; Küzeci, [2020], Kişisel Veriler, 219.

894) https://gdpr-info.eu/art-13-gdpr/ (Erişim Tarihi: 28.10.2022).

895) Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği, Resmi Gazete'nin 10.03.2018 tarih ve 30356 sayılı nüshası.

896) KVK Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, Nisan [2019], s. 9-11; Ayrıca bkz. Tebliğ m. 5.
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf (Erişim Tarihi: 28.10.2022).

bu hususu GVKT m. 14 ile benzer biçimde düzenlemiştir[897]. GVKT m. 14/3 fıkrası hükmüne göre veri sorumlusu m. 13'teki unsurları taşıyan bir bilgilendirmeyi kişisel verileri işlemeye başladıktan sonra makul bir sürede, her durumda en geç bir ay içinde ilgili kişiyi işlenen verileriyle ilgili aydınlatma yükümlülüğü kapsamında bilgilendirmekle yükümlüdür. İşlenen veriler iletişim amacıyla kullanılacaksa ilgili kişiyle ilk iletişim anında aydınlatma yükümlülüğü yerine getirilmelidir. Kişisel veriler bir başkasına aktarılacaksa bu durumda en geç ilk aktarılmaya konu edildiği zaman ilgili kişinin bilgilendirilmesi gerekir[898].

Açık rızanın alınmasında olduğu gibi aydınlatma yükümlülüğünün yerine getirilmesinde de bir şekil şartı öngörülmemiştir. Veri sorumlusu ispatlanabilir bir yöntemle bu yükümlülüğünü yerine getirdiğini ispatlamakla yükümlüdür. Bu husus Tebliğ'in 5. maddesinde; "veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle" biçiminde düzenlenmiştir. Örneğin işveren işyeri girişinde kamera gözetlemesi gerçekleştiriliyorsa kameranın bulunduğu yere kamera kaydı alındığına dair bir tabela asarak katmanlı aydınlatma[899] yapabilir ve yine girişte kolaylıkla görülen bir yerde pano asarak kamera gözetlemesinde işlenen görsel ve işitsel veriler için aydınlatma yükümlülüğünü yerine getirebilir. Aynı husus internet trafiğinin izlendiği durumda pop-up pencere açılması vasıtasıyla veya bir sekmeye eklenen metinlerle aydınlatma yükümlülüğü yerine getirilebilir[900].

Bu noktada belirtilmesi gereken diğer önemli bir husus aydınlatma yükümlülüğü verileri işlenen ilgili kişinin talebine bağlı olmadığıdır[901]. Dahası ilgili kişinin aydınlatma yükümlülüğü ile ilgilenmemesi, metindeki bilgilere ilgi

897) Detaylı bilgi için bkz. Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği, m. 6.
898) Detaylı bilgi için bkz. https://gdpr-info.eu/art-14-gdpr/ (Erişim Tarihi: 28.10.2022).
899) Katmanlı aydınlatma: "Kişisel verilerin elde edilmesi sırasında ilgili kişiye, kişisel verilerinin elde edildiği konusunda ön bilgilendirme yapılarak, ilgili kişinin KVKK m. 10 ve 11'e uygun aydınlatmaya yönlendirilmesini" sağlayan kısa görsel veya metinsel bir ifadelerdir.
900) KVK Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Ankara, Nisan 2019, s. 14.
901) EU, [2018], Handbook, s. 207.

gösterip göstermemesine bakılmaksızın veri sorumlusu tarafından ispatlanabilir bir yöntemle aydınlatma yükümlülüğü yerine getirilmelidir. Modernize edilmiş 108 sayılı Sözleşme'nin 8. maddesinde de bu yükümlülük veri sorumlusu açısından öngörülmüş ve bilgilendirmenin içeriğinde neler bulunması gerektiği düzenlenmiştir. Sözleşmenin 9. maddesinde ise ilgili kişinin haklarının nasıl kullanacaklarına ilişkinin bilginin de veri sorumlusu tarafından ilgili kişiyle paylaşılması ile adil ve şeffaf bir kişisel veri işleme faaliyetinin gerekliliği hüküm altına alınmıştır[902]. GDPR'ın 13 ve 14. maddelerinde de bu yönde düzenlemeler öngörülerek[903] ilgili kişinin talebine bağlı olmaksızın veri sorumlularına bu yükümlülük yüklenmiştir[904].

KVKK m. 10'da ve Tebliğ'de öngörülen unsurları taşıyan bir metin kapsamında veri sorumlusu işveren talebin bulunup bulunmadığına bakmaksızın dijital izleme uygulamalarında verileri işlenen ilgili işçileri aydınlatması gerekir[905]. Örneğin işçilerin kendi rızasıyla aydınlatma yükümlülüğü taleplerinin bulunmadığı yönündeki beyanları işvereni aydınlatma yükümlülüğünü yerine getirme yükümlülüğünden kurtaramaz. Aynı doğrultuda, işverenin işçilerden aldığı aydınlatma yükümlülüğü hakkından kendi rızasıyla vazgeçtiği yönündeki beyanlar da geçersiz olacaktır. Öte yandan aydınlatma yükümlülüğünün tam istisnası KVKK m. 28/1'de, kısmi istisnası ise KVKK m. 28/2'de düzenlenmiştir. Bu düzenlemelerin kapsamında bulunmayan her durumda ilgili kişinin, kişisel verileri işlenmeden önce aydınlatma yükümlülüğü kapsamında bilgilendirilmesi gerekir[906].

---

902) Explanatory Report of Modernised Convention 108, § 55-61. https://rm.coe.int/16800ca434 (Erişim Tarihi: 29.10.2022).
903) GVKT Gerekçe 39, https://gdpr-info.eu/recitals/no-39/ (Erişim Tarihi: 29.10.2022).
904) EU, [2018], Handbook, s. 207-208.
905) Aydınlatma yükümlülüğünün en az zorunlu unsurları KVKK m. 10'da ve Tebliğ'in "Aydınlatma yükümlülüğünün kapsamı" başlığında m. 4'te, "Usul ve esaslar" başlığında m. 5'te ve "Kişisel verilerin ilgili kişiden elde edilmemesi halinde aydınlatma yükümlülüğü" başlığında m. 6'da düzenlenmiştir.
906) KVK Kurulu bu hususu bir kararında; "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 5'inci maddesine göre ilgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmesi gerektiği, Kanun'un veri sorumlusunun aydınlatma yükümlülüğünü yalnızca 28'inci maddenin birinci fıkrasında düzenlenen tam istisna ve ikinci fıkrasında yer alan kısmi istisna hallerinin bulunduğu durumlarda kaldırdığı düşünülürse somut olay bakımından veri

İş ilişkisinde veri sorumlusu işveren öncelikli olarak kişisel verileri doğrundan işçiden elde edecek bir yöntemlere[907] öncelik vermesi gerekmektedir[908]. Bunun yapılması işçiden işlenen verileri hakkında doğrudan haberdar olma, işlenecek verileriyle ilgili bir hakimiyet alanının oluşması, kişisel verileri ve özel hayatının gizliliğinin korunduğu konusunda bir güvence hisseder[909]. Aynı doğrultuda işçilerle paylaşılacak aydınlatma metni açık olmalı, metinde anlaşılması güç teknik terimlere yer vermekten kaçınılmalıdır. Aynı zamanda şeffaflık ilkesinin gereği olarak ilgili kişi anlaşılır, sade bir dil kullanılmış, kolayca ulaşılabilir ve aydınlatma yükümlülüğünün unsurlarını taşıyan bir metin kapsamında aydınlatma yükümlülüğünün yerine getirilmiş olması gerekir[910]. Böylelikle ilgili kişi şüpheye mahal vermeyecek şekilde hangi verilerinin, hangi amaçla işleneceğini, işlemenin hukuki nedenlerini ve hakları konusunda bilgi sahibi olmalıdır[911].

İş ilişkisinde de KVK hukukunun temel yaklaşımı olan zorunlu olmadıkça kişisel verilerin işlenmemesi yaklaşımı kapsamında hareket edilmesi gerekir[912]. KVKK'da genel ilkelerin düzenlendiği m. 4/2-ç bendinde: "kişisel verilerin işlendikleri amaçla bağlantılı sınırlı ve ölçülü" olması gerekliliğinin temelinde işlenmesine ihtiyaç bulunmayan kişisel verileri işlememe ilkesine dayanmaktadır. Bu ilkenin önemi karakteristik özelliğinin bağımlılık unsuruyla şekillendiği bir hukuki ilişkide işçilerin kişisel verilerinin sözleşmenin ifası veya işin görülmesini

---

sorumlusunun aydınlatma yükümlülüğünün mevcut olduğu, Tebliğ'in aynı maddesinde aydınlatma yükümlülüğünün yerine getirildiğinin ispatının veri sorumlusuna ait olduğunun düzenlendiği, bu nedenle, somut olayda ilgili kişiye ait kişisel verilerin işlenmesi bakımından ilgili kişiye aydınlatma yapma yükümlülüğü bulunan veri sorumlusunun, bu yükümlülüğünü yerine getirmediği…" değerlendirmesini yaparak veri sorumlusuna idari para cezası uygulamıştır. Bkz. 01/06/2023 Tarihli ve 2023/924 Sayılı Karar Özeti, https://kvkk.gov.tr/Icerik/7763/2023-924 (Erişim Tarihi: 06.01.2024).

907) Bkz. § 9. II.

908) ILO, Protection of workers' personal data, m. 6/1, s. 2. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

909) ILO, Protection of workers' personal data (Commentary), s. 15.

910) Aşıkoğlu, [2019], Aydınlatma Yükümlülüğü, s. 44;

911) ILO, Protection of workers' personal data, m. 6/3, s. 2; KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi, s. 9; https://kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf (Erişim Tarihi: 22.03.2023).

912) KVK Kurumu, [2019], Uygulama Rehberi, s. 68.

aşacak biçimde işlenmesini sınırlandırmasında ortaya çıkar.

Ele alındığı üzere, KVK hukukunun temel ilkelerine uygun dijital izleme gerçekleştirmede ve işçilerin kişisel verilerinin işlendiği durumlarda hukuka uygunluk sebepleri ve ispatlanabilir bir yöntemle aydınlatma yükümlülüğünün yerine getirilmesi veri sorumlusu işverenin yükümlülüğündedir[913]. İş ilişkisi açısından veri işleme amaçlarını, işlenecek veriyi ve araçlarını belirlemede belirleyici olan gerçek veya tüzel kişi veri sorumlusu işveren, bu yükümlülüğünü gerçek veya tüzel kişi olabilecek veri işleyenlere bırakarak sorumluluktan kurtulmasına olanak bulunmamaktadır. KVKK m. 3/1-ı bendinde: veri sorumlusu; "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" biçiminde tanımlanmıştır. Örneğin, veri sorumlusu işverenin elektronik iletişimin izlenmesi için hizmet aldığı bir bilişim firması, bu işi ifa ettiği sürede işlediği işçi kişisel verilerinde, işveren adına kişisel veri işleyen statüsündedirler. Genel kabul veri işleyenlerin veri işleme sürecinde bir belirleyiciliği bulunmadığından bir yükümlülüğünün de bulunmadığı[914] şekilde olmakla birlikte, KVKK m. 12/4 fıkrasında veri işleyenlerin öğrendikleri kişisel verileri Kanun hükümlerine aykırı biçimde başkalarına açıklamayacağı düzenlenmiştir[915]. Aynı doğrultuda GVKT veri işleyenlere düzenlemeler kapsamındaki yükümlülüklerine uyduklarını göstermek için tüm işleme faaliyeti kategorilerinin bir kaydını tutma yükümlülüğü getirilmiştir[916].

İlgili başlıkta ele alındığı üzere aydınlatma yükümlülüğünün kişisel veri

913) KVK Kurumu, [2019], Uygulama Rehberi, s. 56.
914) Özellikle, sorumluluk açısından (hesap verebilirlik) açısından veri sorumlusunun yükümlülüğü bulunduğu, bu hususta veri işleyenin bir yükümlülüğü bulunmadığı kabul edilmektedir. Article 29 Working Party, Opinion 3/2010 on the principle of accountability, s. 7-8. https://www.dataprotection.ro/servlet/ViewDocument?id=654 (Erişim Tarihi: 30.10.2022).
915) KVKK m. 12/4. fıkra düzenlemesinde veri işleyenin yükümlülüğü: "Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder" biçiminde düzenlenmiştir.
916) EU, [2018], Handbook, s. 101.

işlemede hukuka uygunluk değerlendirmesindeki önemi AİHM Büyük Daire'nin Bărbulescu & Romanya[917] kararında ve AYM Genel Kurul E.Ü. kararında bariz biçimde görülmektedir. AİHM Büyük Daire, Bărbulescu & Romanya kararında işçinin elektronik iletişimin izlenmesi için tam bilgilendirme şartını aramıştır. AYM, E.Ü. kararında işverence dijital izleme uygulaması kullanılmasını yönetim hakkı kapsamında değerlendirmiş, fakat bunun hukuka uygun olması için işçinin önceden bilgilendirilmiş olası gerektiğine karar vermiştir. Kararda iletişimin denetlenebileceğine ve iletişim araçlarının kullanım koşullarına ilişkin olarak önceden tam ve açık bir bilgilendirme yapılmadığı hallerde temel hak ve özgürlüklerinin işyerinde de korunacağı yönündeki haklı beklentiyle çalışan kişinin kurumsal e-posta üzerinden kişisel yazışmalar yapabileceğinin işveren tarafından da öngörülebilecek bir durum olduğu vurgulanmıştır. Kararda bunun yapılmaması halinde işçilerden kişisel verilerinin ve özel hayatlarının işyerinde ve sağlanan iletişim araçlarında da korunacağına dair makbul bir beklentinin oluşabileceği belirtilmiştir[918].

b) Teknik ve İdari Tedbirleri Alma Yükümlülüğü

KVKK m. 12 hükmü kapsamında veri sorumlusu işveren kişisel verilerin hukuka aykırı biçimde işlenmesini önleme, kişisel verilere yetkisiz erişimleri önleme ve kişisel verilerin güvenliğini sağlama yükümlükleri bulunmaktadır[919]. Bu yükümlülükler kapsamında veri sorumlusu işveren dijital izleme uygulamaları vasıtasıyla işleyeceği kişisel verilerin hukuka uygun olarak işlenmesini temin etmek için tekniğin gerektirdiği her türlü teknik ve idari tedbirleri almakla yükümlüdür[920]. KVKK m. 12 düzenlemesinde, 95/46EC sayılı Direktif'in 17. maddesi esas

917) Bkz. § 7. IV. 3.
918) AYM Genel Kurul Kararı, E.Ü. Başvurusu, Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020, §75, R.G. Tarih ve Sayı: 14/10/2020-31274.
919) KVK Kurumu, [2019], Uygulama Rehberi, s. 97.
920) Veri Güvenliğine İlişkin Yükümlülükler, https://www.kvkk.gov.tr/Icerik/2040/Veri-Guvenligine-Iliskin-Yukumlulukler (Erişim Tarihi: 29.10.2022); Ayrıca KVK Kurumu teknik ve idari tedbirleri alma yükümlülüğünü somutlaştırmakta için "Kişisel Veri Güvenliği Rehberi"ni yayımlamıştır. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf (Erişim Tarihi: 29.10.2022).

alınmıştır. GVKT m. 32 vd. düzenlemelerinde kişisel verilerin işlenmesinde alınacak güvenlik tedbirleri detaylı bir şekilde düzenlenmiştir[921]. GVKT m. 32/1 düzenlemesinde veri sorumlularına diğer tedbirlerle birlikte kişisel verilerin işlenmesindeki riskle orantılı bir güvenlik seviyesini sağlamak için uygun teknik ve organizasyonel tedbirleri alma yükümlülüğü yüklenmiştir.

İdari tedbir olarak veri sorumlusu işveren işçilerine kişisel veri güvenliği ve farkındalığı için gerekli eğitimleri vermeli, veri tabanlarına yetkisiz erişimleri engellemeli, fiziki dosyalara yetkisiz erişimleri sınırlandırmalıdır. Aynı husus teknik tedbirler için de geçerli olduğundan yetkili olmayan işçilerin erişimine sistemlerin kapatılması, kişisel verilerden kopya alınmasını yasaklayan veya yetkiye göre sınırlandıran bir teknik sistemin oluşturulması bu açıdan önemlidir. Ayrıca oluşturulan prosedürlerin ve farkındalık metinlerinin kağıt üzerinde kalmamasına dikkat edilmeli ve alınan teknik ve idari tedbirlerin uygulamada işler sonuçlar verdiğini iç ve dış denetimlerle test etmelidir[922]. Örneğin bir saha satış personelinin müşteri ziyaretlerinin GPS verileriyle izlenmesi durumunda bu izleme verileri ilgili kişiler dışındakilerin erişimine kapalı olmalı ve doğrudan ilgili sınırlı sayıda kişi bu verileri ifşa etmeyecek şekilde işlemelidir.

Veri sorumlusunun alacağı teknik ve idari tedbirlere; verilere yetki matrisine uygun erişim sağlama, veri işleme sürecini analiz ederek belirli iyileştirmelerin sağlanması çalışmaları, işçilerin dijital güvenlik konusunda eğitilmesi, düzenli denetimler, teknik sızma testleri ve sürecin mevzuata uygun işleyişini denetleyecek testler örnek gösterilebilir. Örneğin, AİHM, I. & Finlandiya kararına konu olayda başvurucu, çalıştığı hastane tarafından veri koruma hakkının ihlal edildiğini, hastalığıyla ilgili kaydın başka personellerin erişimine açık olacak şekilde işlendiğini ve kişisel verilerine hukuka aykırı şekilde erişim sağlandığını iddia etmiştir, yerel mahkemeler bu iddia için yeterli kanıt bulunmadığından

921) EU, [2018], Handbook, s. 170.
922) EU, [2018], Handbook, s. 166.

davanın reddine karar vermiştir. AİHM, kişisel verilerin işlenmesinde kayıt sisteminin denetiminin ve hasta kayıtlarının kullanımını geriye doğru açıklığa kavuşturmak mümkün olmadığı, hastanenin bunun için etkin bir sistem oluşturmadığı gerekçesiyle AİHS m. 8'in ihlal edildiği sonucuna varmıştır[923].

KVKK m. 12/2'de veri sorumlusunun adına kişisel verilerin başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda birinci fıkrada belirlenen asgari tedbirlerin, veri işleyen sıfatına sahip olan bu kimselerce de alınmasında veri sorumlusu müştereken sorumlu tutulmuştur[924]. Örneğin, veri sorumlusu işveren adına işçilerin kullandığı araçların GPS takip sistemini veya internet trafik izleme uygulamasını veri işleyen statüsünde olan tedarikçi bir firmanın gerçekleştirilmesi durumunda olası bir veri ihlali durumunda veri sorumlusu ve veri işleyen oluşan zarardan ve KVK Kurulu'nun uygulayacağı idari yaptırımdan müştereken sorumlu olur[925].

İşyerinde kişisel verilerin korunmasına ilişkin etkin bir yapının oluşturulması sayılan teknik ve idari tedbirlerin alınmasına ve işçilere sorumluluklarının ve veri sorumlusu işverenin kişisel verilere ilişkin politika ve prosedürlerinin tebliğ edilmesiyle sağlanabilir. Dahası Yönetmelikte[926] vurgulandığı üzere kişisel verilere ilişkin politika ve prosedürlerin oluşturulması tek başına veri sorumlusunun KVKK yükümlülüklerini yerine getirdiği biçiminde yorumlanamaz. Bunun yapılması için işçilerde kişisel verilerin işlenmesi ve korunmasıyla ilgili bir farkındalık ve şirket kültürü oluşturulmasına bağlıdır. Ayrıca işçilerin kolay bir şekilde ulaşıp, kişisel veri işleme sürecinde karşılaştıkları

923) AİHM, I. v. Finland, No. 20511/03, 17 Temmuz 2008. https://www.hrlc.org.au/human-rights-case-summaries/i-v-finland-2008-echr-2051103-17-july-2008 (Erişim Tarihi: 29.10.2022).
924) KVK Kurumu, [2019], Uygulama Rehberi, s. 98.
925) KVK Kurulu Kararı, "Mağazacılık faaliyeti yürüten bir veri sorumlusunun veri ihlal bildirimi" hakkında Kişisel Verileri Koruma Kurulu'nun 07/10/2021 tarih ve 2021/1021 sayılı Kararı. https://www.kvkk.gov.tr/Icerik/7081/2021-1021 (Erişim Tarihi: 30.10.2022).
926) Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 5/2 düzenlemesinde bu husus şu şekilde hüküm altına alınmıştır: "Kişisel veri saklama ve imha politikası hazırlanmış olması; kişisel verilerin Kanuna ve Yönetmeliğe uygun biçimde saklandığı, silindiği, yok edildiği veya anonim hale getirildiği anlamına gelmez."

sorunları, veri işleme faaliyetinin hukuka uygunluğunu soracağı ve veri işleme faaliyetinin değerlendirmesinin yapılacağı bir komite oluşturulması faydalı olacaktır[927]. Eklemek gerekir ki, işçilerin verilerinin dijital izleme uygulamasıyla işlenmesi durumunda izlemenin her aşaması için gereklilik denetimi ile teknik tüm tedbirler alınmalı ve işçilerin bu verilerinin ifşa edilmesinin önüne geçecek teknik ve organizasyonel bir yapı oluşturulmalıdır[928].

Yukarıda ele alındığı üzere, özel nitelikli kişisel verilerin işlenmesi kural olarak yasaktır[929]. Fakat bazı faaliyetler niteliği gereği özel nitelikli kişisel veri işlenmesini gerekli kılar[930]. Özel nitelikli kişisel verilerin işlenmesi durumunda alınan teknik ve idari tedbirlerin asgari olarak KVK Kurumu'nun yayımladığı 2018/10 sayılı Kurul Kararına[931] uygun hale getirilmesi zorunludur. İşlenmesi halinde ilgili kişinin ayrımcılığa uğramasına sebebiyet verme olasılığı bulunan özel nitelikli kişisel verilerin işlenmesi ve korunması KVK hukukunda daha katı kurallara bağlanmıştır. AB 95/46 sayılı Direktif'in 8. maddesi, 108 sayılı Sözleşme'nin 6. maddesi ve GVKT'nin 9. maddesi buna örnek gösterilebilir. Aynı doğrultuda KVKK m. 6 özel nitelikli kişisel verileri sınırlı sayıda belirlemiş ve 6/3'te işlenme koşullarını daha sıkı kurallara bağlamıştır[932]. Örneğin işçinin işe girişte işverenle paylaştığı sağlık raporu, sağlık sigortası yaptırılan işçinin hastalık ve kullandığı ilaçlara ilişkin bilgileri, İSG yükümlülükleri kapsamında işçiyle ilgili işlenen kişisel sağlık verileri özel nitelikli kişisel veridir. Veri sorumlusu işverenin

927) ILO, Protection of workers' personal data, m. 11/13; Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m. 4 ve m. 5.
928) Article 29 WP, Employment context, s. 22; ILO, Personal Data Code, m. 7; CoE, Recommendation No. R (89) 2, m. 13/1.
929) GVKT m. 9/1, ayrıca m. 9 ve devamında bu nitelikteki verilerin işlenmesi ayrıntılı düzenlenmiş ve katı işlenme koşullarına (örneğin açık rıza gibi) bağlanmıştır.
930) Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brussels, 15 February 2007. Ayrıca bkz. GVKT m. 9/3 ve gerekçesi.
931) KVK Kurul Kararı, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı. https://www.kvkk.gov.tr/Icerik/4110/2018-10 (Erişim Tarihi: 30.10.2022).
932) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 145 vd.; Gürsel, [2016], İşçinin Kişisel Verileri, s. 117 vd.; Baysal, [2023], Kişisel Verilerin İşlenmesi, s. 528.

bu kişisel verileri işleyebilmesi için asgari olarak KVKK Kurulu'nun 2018/10 sayılı Kararına uygun teknik ve idari tedbirleri alması gerekir.

c) Denetlenebilir ve Şeffaf Bir Veri İşleme Süreci Oluşturma Yükümlülüğü

Kişisel verilerin işlenmesinde şeffaflık ilkesi verisi işlenen ilgili kişinin başvurularını ve bilgi taleplerini etkin bir şekilde cevaplamayı da içerir. Bundan dolayı aydınlatma yükümlülüğü metinlerinde ilgili kişinin haklarını veri sorumlusuna karşı ileri sürebileceği yöntemlerin bilgisinin de kişisel verileri işlenen ilgili kişiyle paylaşılması gerekir. KVKK m. 13'te ilgili kişinin başvurularına veri sorumlularının cevap vermelerinin usul ve esasları belirlenmiştir[933]. Ayrıca, KVK Kurumu yayımladığı "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[934]" ile ilgili kişilerin başvurularını hangi yöntemle veri sorumlularına ulaştıracakları açıklığa kavuşturulmuştur. Tebliğde veri sorumlularının ilgili kişilere başvurularını kolaylıkla gerçekleştirecek mekanizmaları oluşturma ve duyurma yükümlülüğü de yüklenmiştir.

Tebliğe göre kişisel verileri işlenen ilgili kişiler KVKK m. 11'de hüküm altına alınan haklarına ilişkin başvurularını Türkçe ve yazılı olarak veya kayıtlı elektronik posta ya da veri sorumlusunca başvurulara yönelik oluşturulmuş bir usul veya geliştirilmiş bir yazılımla veri sorumlusuna iletir. Başvuruda, Tebliğde belirtilen bilgilerin bulunması ve öngörülen usullere uyulması gerekmektedir (Tebliğ m. 5). Veri sorumlusu ise, usulüne uygun gerçekleşmiş başvuruyu etkin, hukuka ve dürüstlük kuralına uygun bir biçimde sonuçlandırmak ve gerekli cevabı en geç otuz gün içinde ilgili kişiye vermekle yükümlüdür (KVKK m. 13 ve Tebliğ m. 6).

933) KVK Kurumu, [2019], Uygulama Rehberi, s. 100.
934) Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, 10 Mart 2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlandı. Tebliğ'in 5. maddesinde "başvuru usulü", 6. maddesinde "başvuruya cevap" düzenlenmiştir.

GVKT m. 5/1-a bendinde kişisel verilerin adil ve şeffaf bir şekilde işeneceği temel ilke olarak düzenlenmiş, m. 12'de ise şeffaflığın sağlanmasının yöntemlerine açıklık getirilmiştir. AİHM kararlarında[935] kişisel veri işleme süreçlerinin veri sahibinin bilgisine açık olmasını ve verisi işlenen ilgili kişinin kişisel verilerinin ne olacağına anlamalarını sağlayacak bir süreç yönetiminin gerekli olduğu vurgulanmaktadır. Bu ancak kişisel veri işlenmeye başlanmadan önce ilgili kişinin işlenecek verileri hakkında bilgilendirilmesi, bilgilendirmede açık ve sade bir dil kullanılması ve kişisel verilere ilişkin haklarını kullanabileceği yöntemler ve usuller hakkında bilgilendirilmesiyle mümkündür[936].

d. Veri Sorumluları Siciline Kayıt Yükümlülüğü

KVKK m. 16 hükmü kapsamında veri sorumlusunun kişisel veri işleme faaliyetinde şeffaf olmasını denetleyen mekanizmalardan birisi, KVK Kurulu'nun yayımladığı istisnalar kapsamına girilmemesi halinde[937] Veri Sorumluları Bilgi Sistemi[938] (VERBİS) kaydının yapılması yükümlülüğüdür. KVKK m. 16/1 düzenlemesine göre, KVK Kurumu Başkanlığı tarafından kamuya açık biçimde tutulacak sicile (VERBİS) kişisel veri işleyen gerçek ve tüzel kişi veri sorumluları veri işlemeye başlamadan önce kaydolmak zorundadır[939].

935) AİHM, Haralambie v. Romanya, No. 21737/03, 27 Ekim 2009; AİHM, Guide on Article 8 of the European Convention on Human Right, 31 August 2019, s. 33 vd. https://inhak.adalet.gov.tr/Resimler/Dokuman/2432020134816Guide_Art_8_ENG.pdf (Erişim Tarihi: 02.11.2022).
936) EU, [2018], Handbook, s. 120; Article 29 Working Party, Opinion 2/2017 on data processing at work, s. 23.
937) KVK Kurumu, Sorularla VERBİS Rehberi, s. 9-10. KVKK m. 16/2 düzenlemesinde KVK Kurulu'na VERBİS kaydı hususunda istisna tanıma yetkisi verilmiştir. Buna göre KVK Kurulu 02.04.2018 tarih ve 2018/32 sayılı Kararı ile VERBİS'e kayıt olma yükümlülüğü bulunmayan veri sorumlularını belirlemiştir. Buna göre, noterler, avukatlar, dernekler, 6356 sayılı Kanuna göre kurulan sendikalar, siyasi partiler, mali müşavirler, yeminli mali müşavirler ile yıllık işçi sayısı 50'den az ve yıllık bilanço toplamı 25 Milyon Türk Lirası'ndan az olan gerçek veya tüzel kişi veri sorumlularının VERBİS kaydı yükümlülüğü bulunmamaktadır.
938) Veri Sorumluları Sicili Hakkında Yönetmelik, 30 Aralık 2017 tarih ve 30286 sayılı Resmi Gazete'de yayımlandı.
939) KVK Kurumu, [2019], Uygulama Rehberi, s. 102.

Ayrıca veri sorumlusu Kanun'da ve ikincil mevzuatta öngörülmüş olan VERBİS'le yakından ilişkili olan envanter, politika ve prosedürleri oluşturmakla yükümlüdür[940]. Bu aynı zamanda temel ilkelerden birisi olan "hukuka ve dürüstlük ilkesine uygun" kişisel veri işlemenin bir gereğidir. Böylelikle veri sorumlusu işveren dijital izleme gerçekleştirmede şeffaflığı gerçekleştirmek için gerekli özeni göstermesinin yanı sıra, işçilerin hangi dijital izlemede verilerinin işlendiğinin genel çerçevesini görebilmeleri açısından bir şeffaflık oluşturur ve işçilerin kişisel verileri üzerindeki haklarının korunmasına ilişkin makul beklentiler de karşılanmış olur[941].

7. Dijital İzlemede İşlenen İşçi Verilerinin Aktarılması

Dijital izleme uygulamaları bilişim teknolojileri ve veri tabanları üzerinde çalışan uygulamalar olduğundan bu teknolojilerin sunucularının ülke içinde olması veya bulut sistemler üzerinde bulunması gibi durumlar kişisel verilerin nereye aktarıldığı ve nerede yer alan sistemler üzerinde işlendiği sorularını gündeme getirir. KVK Kurulu yayımladığı "Gmail kararında" bu tür e-posta hizmeti sunan şirketlerin alt yapısının nerede olduğunun tam tespit edilemediğini, bunların dünyanın çeşitli yerlerinde olabileceğini, aynı hususun bulut sistemler (cloud) için geçerli olduğunu, bu vasıtalarla gerçekleştirilen veri işleme faaliyetlerini yurt dışına kişisel veri aktarımı olarak değerlendirdi[942]. Bu karar dijital izleme açısından önemlidir, zira kişisel veri işleyen dijital uygulamaların hangi veri tabanlarını kullandığı, sunucularının ve alt yapılarının nerede olduğunu her zaman tespit etmek zordur. Bu kapsamda dijital izleme uygulamalarında işlenen kişisel verilerin yurt içinde ve yurt dışına aktarılma koşulları bu başlıkta ele alınacaktır.

---

940) Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik m. 5 kişisel veri saklama ve imha politikasının esaslarını düzenlemektedir. Madde 6 kişisel veri saklama ve imha politikasının kapsamını düzenlemektedir.

941) Akgül, [2014], Kişisel Verilerin Korunması, s. 158.

942) KVK Kurulu, Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağı ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/157 Sayılı Karar; https://www.kvkk.gov.tr/Icerik/5493/2019-157 (Erişim Tarihi: 12.11.2022).

a) İşlenen Kişisel Verilerin Yurt İçinde Aktarılması

Kişisel verilerin yurt içinde aktarılması KVKK m. 8'de düzenlenmiştir. Maddenin ilk fıkrasında açık rıza bulunmaksızın kişisel verilerin yurt içinde aktarılmayacağı hüküm altına alınmıştır. İkinci fıkrada ise, Kanunun m. 5/2'de yer alan kişisel veri işleme şartlarının ve özel nitelikli kişisel veriler açısından ise yeterli önlemlerin alınması[943] şartı öngörülerek, m. 6/3 kapsamındaki veri işleme şartlarının bulunması durumunda açık rıza alınmaksızın kişisel verilerin aktarılabileceği düzenlenmiştir. Ayrıca aydınlatma yükümlülüğü metninde kişisel verilerin aktarılmasının hukuki şartı ve aktarıldığı yerlere ilişkin bilginin de ilgili kişiye bildirilmesi gerekir.

Bu düzenlemeler kapsamında veri sorumlusu işveren gerçekleştireceği dijital izlemede, örneğin işçinin davranışsal biyometrik verileri[944] olan araç kullanma biçimi, akıllı telefonu kullanma şekli, klavye kullanma ve tuşlara basış stili KVKK'da özel nitelikli kişisel veri olarak sayılan biyometrik veri olduğundan KVKK m. 8 düzenlemesinin atfı kapsamında aktarılması için m. 6/3'teki koşulların bulunması ve KVK Kurulu'nun 2018/10 sayılı Kurul Kararında öngörülen tedbirlerin alınması gerekmektedir.

Kişisel verilerin aktarılması özel hayatın gizliliğinin korunması hakkıyla yakından ilişkilidir. Nitekim, ABAD Rechnungshof - Österreichischer Rundfunk[945]

---

943) Özel Nitelikli Kişisel Veriler Açısından Yeterli Önemleri KVK Kurulu 2018/10 sayılı Kararında açıkladı. Kararın detayı için bkz. https://www.kvkk.gov.tr/Icerik/4110/2018-10# (Erişim Tarihi: 12.11.2022).

944) KVK Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, s. 4.

945) Karara konu olayda işveren belirli bir seviye üstü ücret alan işçinin ücrete ilişkin bilgilerini ismen işlemiş ve bu ismi içerecek biçimde kamu kurumuna (yasal düzenleme gereği) aktarmıştır. Başvurucu, kişisel verinin ismen gönderilmesinin gerekmediğini, anonim veri gönderilmesine olanak bulunmasına rağmen işverenin ismen veri aktarmasını özel hayatına müdahale olduğunu iddia etmiştir. Avusturya hükümeti iç mevzuatın bunu gerektirdiğini ve olayın 95/46 sayılı Direktif kapsamında kalmadığı yönünde savunma yapmıştır. ABAD, işverenin işçilerine ödediği ücretin tek başına işlenmesini özel hayata müdahale teşkil etmeyeceğini tespit ettikten sonra, söz konusu verilerin üçüncü taraflara aktarılmasını (davaya konu olayda bir kamu kuruluşu) kişisel verilerin aktarılması olarak nitelendirmiş ve bunun özel hayata müdahale olduğunu, ayrıca olayda 95/46 sayılı

kararında bir kişinin mesleki gelirine ilişkin verilerin isim bazlı işlenmesinin AİHS m. 8 kapsamında korunduğunu, AİHM kararlarında vurgulandığı üzere özel hayat kavramının kısıtlayıcı bir şekilde yorumlanmamasını, kişinin mesleki hayatı ile profesyonel anlamda yaptığı faaliyetlerin de bu kapsamda bulunduğunu tespit etmiştir. Kararda kişisel verilerin aktarımının AİHS'nin 8. maddesinde düzenlenen özel hayata saygı hakkına bir müdahale niteliğinde olduğuna ve olayda kişisel verilere ilişkin olan 95/46 sayılı Direktifin uygulama alanı bulacağına hükmedilmiştir[946].

Kişisel verilerin aktarılması ilgili kişinin verileri üzerindeki haklarını korumasını ve bir hakimiyet alanı oluşturmasını güçleştirir. ABAD kararında vurgulandığı üzere işverenin işçilerin ücrete ilişkin haklarının yer aldığı verileri isim bazlı işlemesinin iş ilişkisi kapsamında makul karşılanması gerekir[947]. Öte yandan bunların üçüncü bir tarafa aktarmasının ilgili kişinin bilgisi dışında gerçekleştirilmesi veya veri işleme amacı dışında aktarılması aktarma amacı ne olursa olsun ilgili işçinin kişisel verileri üzerindeki haklarını ihlal eder. Dahası aktarılan verilerin özel nitelikli kişisel veri olup olmadığı veya veri sahibini rahatsız edip etmediğine bakılmaksızın ihlalin gerçekleşmesi için bir kişinin verilerinin üçüncü bir kişiye bilgisi dışında aktarılması yeterlidir[948].

Direktifin 6(1)(c), 7(c) ve (e) maddeleri doğrudan uygulanabilir olduğuna karar vermiştir. § 3, § 75-75, § 100-101,
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62000CJ0465

946) ABAD, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others, 20 May 2003, § 25, § 73, § 74 ve § 75. https://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=en (Erişim Tarihi: 16.11.2022).

947) ABAD, C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and Others, 20 May 2003, § 75, (Erişim Tarihi: 16.11.2022).

948) Veri sorumlusu üniversitenin rektörü tarafından kişisel veri içeren Excel dokümanının e-posta ekinde üçüncü kişilerle paylaşılmasının herhangi bir veri işleme şartına dayanmadığı ve paylaşmanın da hukuki dayanağı bulunmadığını KVK Kurulu veri ihlali olarak nitelendirmiştir. Kararda özetle; "Veri sorumlusu üniversite rektörü tarafından ilgili kişilere ait kişisel ve özel nitelikli kişisel verilerin yer aldığı Excel dosyasının e-posta ekinde yer verilerek üçüncü kişilerle paylaşılmasının Kanun'un 5'inci ve 6'ncı maddelerinde belirtilen işleme şartlarına dayanılmaksızın gerçekleştirildiği, bu kapsamda Veri sorumlusunun Kanunun 12'nci maddesinin birinci fıkrasının (b) bendi çerçevesinde kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirleri yeterli düzeyde almadığı, şikâyete konu veri işleme faaliyetinin veri ihlali niteliği taşıdığı ancak veri sorumlusu tarafından Kurul'a bir

b) İşlenen Kişisel Verilerinin Yurt Dışına Aktarılması

Kişisel verilerin yurt dışına aktarılması KVKK m. 9'da düzenlenmiştir. Madde hükmünde kural olarak kişisel verilerin yurt dışına aktarılması ilgili kişinin aktarmaya ilişkin açık rızasının bulunması şartına bağlanmıştır. Ayrıca, KVK Kurulu tarafından yayımlanacak güvenli ülkeler listesi kapsamında yeterli korumanın bulunduğu ülkelere kişisel veri aktarılması ve yeterli korumanın bulunmadığı ülkelere aktarım yapılacaksa Kanun'un m. 5/2 ve 6/3 düzenlemelerindeki şartların bulunması ve yeterli önlemleri alacaklarını yazılı olarak taahhüt etmeleri ve KVK Kurulu'ndan izin almaları gerekir[949]. Belirtmek gerekir ki, güvenli ülkeler listesi KVK Kurumu tarafından henüz yayımlanmadı. Bu sebeple halihazırda kişisel verilerin yurt dışına aktarılmasında açık rıza ve veriyi aktaran veri sorumlusu ile verinin aktarıldığı veri sorumlusu veya veri işleyenin yeterli korumayı taahhüt ederek KVK Kurumu'ndan izin alınması dışında bir seçenek bulunmamaktadır[950].

Yukarıda belirtildiği üzere, KVK Kurulu'nun "Gmail" kararında bulut sistemleri (cloud) de kapsayacak şekilde konuyu değerlendirmesi ve bu tür sistemler üzerinde işlenen verileri yurt dışına aktarım olarak kabul etmesi[951] dijital izleme uygulamaları üzerinde tutulan ve sunucularının yurt dışında bulunduğu veya bulut sistem üzerinde işlendiği durumlarda yurt dışına kişisel veri aktarımı gündeme gelecektir.

---

veri ihlal bildiriminde bulunulmadığının tespit edildiği, bu durumun Kanun'un 12'nci maddesinin beşinci fıkrasında düzenlenen Kurul'a bildirimde bulunma yükümlülüğüne aykırılık teşkil ettiği" değerlendirmesi yapılmıştır. Bkz. KVK Kurulu, 01/06/2023 Tarihli ve 2023/928 Sayılı Karar Özeti, https://kvkk.gov.tr/Icerik/7764/2023-928 (Erişim Tarihi: 06.01.2024).

949) KVK Kurumu, Kişisel Verilerin Yurt Dışına Aktarılması Rehberi, s. 1-2. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9178818a-12c7-4d7f-a839-bdb8b6f358b1.pdf (Erişim Tarihi: 13.11.2022).

950) KVK Kurumu, Kişisel Verilerin Yurt Dışına Aktarılması Rehberi, s. 4.

951) KVK Kurulu, Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağı ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/157 Sayılı Kararı.

GVKT'de kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarılması 44-50 maddeleri arasında düzenlenmiştir. Madde 44'de ancak bu madde ve devamında düzenlenen koşulları sağlamaları ve üçüncü ülkede bulunan veri sorumlusunun bu koşullara uyması durumunda aktarılabileceği düzenlenmiştir[952]. Maddenin devamı düzenlemelerinde aktarmanın koşulları ve belirli durumlara özgü aktarmalarda alınacak tedbirler, bağlayıcı kurumsal kararları açısından düzenlemeler yapılmıştır. Ülkemiz veri koruma mevzuatının yurt dışına kişisel veri aktarmaya ilişkin normlarının bu detayda düzenlenmesi gerektiğini belirtmek gerekir.

8. Dijital İzlemede İşçinin İşlenen Kişisel Verileri Üzerindeki Hakları

Ele alındığı üzere, KVK hukukunun temel amaçlarından birisi veri işleme sürecini şeffaflık ilkesine uygun gerçekleştirmesini sağlamak ve ilgili kişiye (iş ilişkisi açısından işçi, işçi adayı ve eski işçi) kişisel verilerinin geleceğini belirleyecek bir hakimiyet alanı oluşturmaktır[953]. Bu amaçla hüküm altına alınmış düzenlemelerden birisi olan KVKK m. 11'de kişisel verileri işlenen ilgili kişinin işlenen kişisel verileriyle ilgili hangi haklara sahip olduğu açıklığa kavuşturulmuştur. İşçiler bu düzenleme kapsamında veri sorumlusu işverenleri tarafından işlenen kişisel verilerine erişim sağlayabilme ve kişisel verilerinin doğru ve güncel işlenip işlenmediğini öğrenebilme hakkına sahiptir. Kanunda herkesin veri sorumlusuna başvuruda bulunarak işlenen verileriyle ilgili bilgi talep etmesi herhangi bir sınırlamaya tabi tutulmadığından işçiler verileri üzerinde yeni bir veri işleme faaliyeti gerçekleştirilmesine gerek olmaksızın işlenen verileriyle ilgili bilgi talep edebilme ve bunların işleme amacına uygun kullanılıp kullanılmadığını öğrenebilme hakkına sahiptir[954]. Yukarıda ele alındığı üzere, veri işleme sürecinin şeffaflık ilkesine uygun olması için veri sorumlusunun (işveren) ilgili kişiyi işlenen

952) EU, [2018], Handbook, s. 249-252.
953) Küzeci, [2020], Kişisel Veriler, s. 95.
954) Nilgün Başalp, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, [2004], s. 48; KVK Kurumu, [2019], Uygulama Rehberi, s. 103-104.

verileri, işleme amacı, veri işlemenin hukuka uygunluk sebebi, saklama süresi, teknik ve idari tedbirler hususunda bilgilendirmesi zorunludur.

KVKK m. 11'de kişisel verileri işlenen ilgili kişinin hakları; kişisel verilerinin işlenip işlenmediğini öğrenme, işlenen verileriyle ilgili bilgi talep etme, kişisel verilerin hangi amaç kapsamında işlendiğini ve bu amaç doğrultusunda işlemeye konu edip etmediğini, kişisel verilerinin yurt içinde veya yurt dışında kimlere aktarıldığını, işlenen verilerinde hatalar ve eksikler varsa bunların düzeltilmesini, KVKK m. 7 kapsamındaki silme hakkı kapsamında şartlar oluşmuş ise verilerinin silinmesini veya yok edilmesini, düzeltilen veya silinen verileriyle ilgili olarak üçüncü kişilere bildirimde bulunmasını, münhasıran otomatik sistemler tarafından işlenen ve analize konu edilen verileri varsa bunlarda aleyhe çıkan sonuçlara itiraz etme ve hukuka aykırı veri işleme sebebiyle uğradığı zararların giderilmesini isteme hakları bulunmaktadır (KVKK m. 11). Eklemek gerekir ki, veri sorumlusu işveren bu maddede düzenleme yapılan hususları aydınlatma metninde işçiye bildirmekle yükümlüdür.

Veri koruma hukuklarında bu ve benzeri hükümlere (GVKT m. 13-14 ve ilgili kişinin erişim hakkını düzenleyen m. 15 gibi) yer verilmesinin amacı şeffaflık ilkesi kapsamında ilgili kişinin hakları hususunda bilgi sahibi olması, işlenen verilerini bilmesi, hangi haklarını ileri sürebileceğini bilmesi ve bu haklarını veri sorumlusuna karşı etkin kullanmasını kolaylaştırmaktır[955]. Eklemek gerekir ki, KVK hukukumuzda bir düzenleme bulunmamakla birlikte ilgili kişinin işlenen verileriyle ilgili bilgi talep etme hakkı dijital izleme uygulamaları açısından fikri mülkiyet hakları ve ticari sırları etkileyecek boyutlar içerebilir. GVKT Giriş 63. paragrafta ilgili kişinin veri işleme faaliyetinin hukuka uygunluğunu bilmek ve bunları doğrulamak için işlenen verilerine erişim hakkının önemi vurgulanmış fakat bu hakkın ticari sırlar, fikri mülkiyet hakları ve yazılımı koruyan telif hakları

955) Sandra Wachter/Brent Mittelstadt/Chris Russell, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", Harvard Journal of Law & Technology, Vol. 31, No. 2 Spring, [2018], s. 875-876.

üzerindeki başkalarının (örneğin dijital izleme uygulamasının yazılımını oluşturan firma) haklarını olumsuz yönde etkilememesi gerektiği belirtilmiştir. Öte yandan veri sorumlusunun bu tür haklarının bulunması, ilgili kişinin bilgi talebini tamamen reddetme hakkına sahip olduğu biçiminde yorumlanamaz (GVKT Giriş/Recitals §63).

İlgili kişinin veri sorumlusuna başvuru yöntemi KVKK m. 13'te, Kurula şikayet usul ve esasları ise KVKK m. 14 ve 15'te düzenlenmiştir. KVKK'da kademeli bir başvuru süreci öngörüldüğünden ilgili kişi öncelikli olarak veri sorumlusu işverene başvurarak bu haklarını talebe konu etmelidir. İşveren işçinin bu talebini otuz gün içinde cevaplamakla yükümlüdür. Bu usul tüketilmeden doğrudan KVK Kurulu'na şikayette bulunulması usulsüz olacağından Kurul tarafından başvuru dikkate alınmayacaktır[956].

III. Dijital İzlemeyi Sınırlandıran Genel Hukuk İlkeleri

KVKK'da genel ilkelerin düzenlendiği 4. maddesinin birinci fıkrasında kişisel verilerin ancak KVKK ve diğer kanunlarda öngörülen usul ve esaslar kapsamında işlenebileceği hüküm altına alınmıştır. Maddenin ikinci fıkrasında ise kişisel verilerin işlenmesinde m. 4/2 kapsamında düzenlenen bentlerdeki "ilkelere uyulması zorunlu" tutulmuştur. Anılan bentlerde dürüstlük ilkesine ve ölçülülük ilkesine doğrudan atıf yapılmıştır. KVK Kurumu yayımladığı Uygulama Rehberi'nde "hukuka uygunluk" kavramının kapsamının geniş olduğunu ve hukuk normlarına uygunluk ve evrensel ilkelere uygunluğun buna dahil olduğunu belirtmiştir[957]. Anılan düzenlemelerin de bir gereği olarak bu başlıkta dijital izlemeyi sınırlandıran eşitlik ilkesi, dürüstlük ilkesi, ölçülülük ilkesi, temel hak ve

956) KVK Kurumu, İlgili Kişinin Hak Arama Yöntemleri Rehberi, s. 2-3, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/353d85d5-87df-4c91-b08e-b4f0991a80f4.pdf
957) KVK Kurumu, [2019], Uygulama Rehberi, s. 64.

özgürlükler[958] ve işçi adayları açısından temelini dürüstlük ilkesi ve güven ilişkisinden alan culpa in contrahendo sorumluluğu ele alınacaktır.

1. Dijital İzlemenin Eşit Davranma Borcuna Uygun Uygulanması

Eşitlik ilkesi işçinin onurunun korunması ve adalet duygusunun zedelenmemesi gibi değerlerde işverenin sınırını belirleyerek yönetim hakkı kapsamında kullandığı hakları sınırlandırır[959]. Bu itibarla işveren yönetim hakkı kapsamında dijital izleme uygulamaları kullanılırken temelini dürüstlük ve hakkaniyet arayışından alan eşitlik ilkesini dikkate alması gerekmektedir[960]. Zira eşitlik ilkesi birçok hukuk ilişkisinde oluşturduğu gibi işverenin yönetim hakkı açısından genel bir sınırlandırma oluşturarak[961] iş sözleşmesinin taraflarının adalet duygularını besler ve işçinin adalet duygusunu tatmin ederek adaletin en temelde biçimsel olarak gerçekleşmesine zemin oluşturur[962]. Böylelikle işveren eşit davranma borcu kapsamında eşit durumdaki işçiler arasında eşitliği gözeten, dürüstlük ilkesi[963] ve hakkaniyet esasına dayanan bir çalışma düzeni ve uygulama birliği oluşturmak yükümlülüğü altına girmiş olur[964].

---

958) Detaylı bilgi için bkz. § 2. IV. 2.

959) Gaye Burcu Yıldız, İşverenin Eşit İşlem Yapma Borcu, Ankara, [2008], s. 31 vd.; Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 203.

960) A. Can Tunay, İş Hukukunda Eşit Davranma İlkesi, İstanbul, [1982], s. 32.

961) Yargıtay kararlarında eşit davranma borcunun, işverenin yönetim hakkını sınırlandırıcı etkisi tespit edilmektedir. Bkz. Yargıtay 9. HD, E. 2017/15337, K. 2020/1522, Karar Tarihi: 05.02.2020

962) Berna Öztürk, İşçinin Talimatlara Uyma Borcu, Onikilevha Yayıncılık, [2021], s. 226-227; Yasemin Işıktaç/Umut Koloş, Hukuk Sosyolojisi, İstanbul Bilgi Üniversitesi Yayınları, İstanbul [2022], s. 153.

963) Yargıtay eşitlik ilkesine aykırı talimat ve uygulamaları geliştirmeyeceğine karar vermektedir. "Bir başka açıdan ifade edilecek olursa, işverenin talimat verme hakkı, kanun, toplu iş sözleşmesi ile bireysel iş sözleşmesi hükümleri ile sınırlıdır. Bu itibarla, işveren, ceza ve kamu hukuku hükümlerine aykırı talimatlar veremeyeceğinden, işçi bu nevi talimatlara uymak zorunda değildir. Bunun dışında işveren, işçinin kişilik haklarını ihlal eden talimatlar veremez. Keza, Medeni Kanunu'nun 2'nci maddesinde düzenlenen hakkın kötüye kullanılması yasağı gereği, işveren dürüstlük kuralına aykırı talimatlar da veremez." Yargıtay 9. HD., E. 2013/12064, K. 2014/7256, T. 06.03.2014; Yargıtay 9. HD., E. 2018/5051, K. 2019/117, T. 07.01.2019; Yargıtay 22. HD., E. 2013/4534, K. 2013/5627 T. 19.03.2013.

964) Taşkent, [1981], Yönetim Hakkı, s. 10-11; Süzek, [1998], Yönetim Hakkı, s. 225 vd.; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 327; Süzek, [2019], İş Hukuku, s. 441; Tuncay, [1982], Eşit Davranma İlkesi, s. 24-25; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku s. 193; Mesut Gülmez, "İnsan Haklarında Ayrımcılık Yasaklı Eşitlik İlkesi: Aykırı Düşünceler", Çalışma ve Toplum Dergisi, 2010/2, [2010], s. 237; Rabia Sever, "İşverenin Eşit

Eşitlik ilkesi, KVKK m. 4/2-a beninde düzenlenen "hukuka ve dürüstlük kurallarına uygun olma" genel ilkesiyle birbirini destekleyen ilkelerdir. KVK Kurumu bu hükmün yorumunu: "Hukuka ve dürüstlük kuralına uygun olma ilkesi, diğer ilkeleri de kapsayıcı bir özelliğe sahiptir. Hukuka uygunluk, genel olarak hukuk normlarına ve evrensel hukuk ilkelerine uygunluktur. Hukuka uygunluğun kapsamı geniştir, mevzuata uygunluk da buna dahildir"[965] biçiminde yapmaktadır. Eşitlik ilkesi, dürüstlük kuralı ve adalet duygusunun zedelenmemesiyle ilişkili olduğundan veri sorumlusu işverence gerçekleştirilecek dijital izlemeyle kişisel veri işleme faaliyetinde eşitlik ilkesinin gözetilmesi gerekir.

İşverenin eşit davranma borcu İş Kanunu'nun 5. maddesinde "eşit davranma ilkesi" başlığında düzenlenmiştir. Ne var ki, hükmün içeriğinde eşit davranma borcu değil, iş ilişkisinde ayrımcılık yasakları düzenlenmiştir. İş Kanunu m. 5/1'de genel ayrımcılık yasakları: "dil, ırk, renk, cinsiyet, engellilik, siyasal düşünce, felsefî inanç, din ve mezhep ve benzeri sebeplerine" dayanılarak ayrım yapılamayacağı biçiminde düzenlenmiştir[966]. Fıkra düzenlemesi kapsamında örneğin işçinin cinsiyet, sendika üyeliği (benzeri sebeplere dayalı), siyasal düşüncesi esas alınarak dijital izleme gerçekleştirilmesi ayrımcılık olarak nitelendirilir. Farklı uygulamayı haklı gösterecek esaslı sebepler olmadıkça işveren dijital izlemeyi tam süreli ve kısmi süreli işçiler açısından farklılaştıramaz (İş Kanunu m. 5/2)[967].

Davranma Borcu", Legal İSGHD, C. 9, S. 34, [2012], s. 38, Kübra Doğan Yenisey, "İş Kanununda Eşitlik İlkesi ve Ayrımcılık Yasağı", Çalışma ve Toplum, 2006/4, [2006], s. 66-67; Sarper Süzek, "İşverenin İşçiyi Gözetme Borcu", Prof. Dr. Tunçer Karamustafaoğlu'na Armağan, Ankara, [2010], s. 829-848.

965) KVK Kurumu, [2019], Uygulama Rehberi, s. 64; KVK Kurumu, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular, KVKK Yayınları, Ankara, [2019], s. 42-43.

966) Kübra Doğan Yenisey, "Eşit Davranma İlkesinin Uygulamasında Metodoloji ve Orantılılık İlkesi", Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, S. 7, [2005], s. 974-975; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 327; Öztürk, [2021], Talimatlara Uyma, 228 vd.; Canan Ünal, İş Hukukunda Yaş Ayrımcılığı, On İki Levha Yayıncılık, [2018], s. 53-54; Süzek, [2019], İş Hukuku, s. 441.

967) Deniz Ugan Çatalkaya, "İş Hukukunda Eşitlik İlkesinin İki Bileşeni: İşverenin Dar Anlamda Eşit Davranma Borcu ve Ayrım Yasağı", Çalışma ve Toplum, 2021/2, [2021], s. 864-865.

İşverenin eşit davranma borcunun varlığını (dar anlamda) tespit etmek için bazı koşulların bulunması aranmaktadır[968]. Eşitlik ilkesinin uygulanabilmesi için öncelikli olarak bir iş ilişkisinin bulunması gerekmektedir. İkinci olarak işyerinde birlik ve zamanda birlik ilkesine uygun olarak aynı işyerinde ve aynı zaman diliminde çalışma gerçekleşmelidir. Son olarak eşitlik ilkesi açısından aralarında karşılaştırma yapma imkanını verecek iki veya daha fazla işçi topluluğunun bulunması gerekir[969].

Eşit davranma borcu, yönetim hakkı üzerinde sınırlamalar ortaya çıkardığından işveren dijital izleme uygulamalarında bu borca uygun bir veri işleme faaliyeti işletmekle yükümlüdür[970]. Zira eşitlik ilkesi, işverenin belirli ayrımları esas alarak ayrımcılık yapmasını ve haklı nedene dayanmayan (keyfi) ayrımcılık uygulanmasını yasaklamaktadır[971]. Bu itibarla işveren eşit işlem borcuna aykırı olacak şekilde dijital izleme uygulaması kullanması ve işçinin verilerini bir veri tabanında tutması kişilik hakkı ihlali de ortaya çıkarır[972]. Eşit davranma borcu, İş Kanunu m. 75/2 ile birlikte düşünüldüğünde işveren işyerinde işçilerin kişilik haklarıyla yakından ilişkili olan özel hayatının gizliliğini ve kişisel verilerin korunması için gerekli tedbirleri alma ve işlenen verileri bir amaç kapsamında en az müdahaleci yöntemle kaydetme ve koruma yükümlülüğü yüklemektedir[973].

Bu yönüyle eşitlik ilkesi işverenin dijital izleme uygulamalarına bir

968) Yargıtay kararlarında dar anlamda eşitlik ilkesinin koşullarını değerlendirmeye konu ederek karar vermektedir. Bkz. Yargıtay 9.HD., E. 2014/20115, K. 2015/32580 T. 17.11.2015; Yargıtay 22. HD., E. 2014/20050, K. 2014/36510 T. 23.12.2014; Yargıtay 9. HD., E. 2011/10207, K. 2011/8653 T. 24.03.2011; Yargıtay 22. HD., E. 2017/18906, K. 2019/14813 T. 2.7.2019; Yargıtay 9. HD., E. 2011/8547, K. 2011/8652 T. 24.03.2011.

969) Tuncay, [1982], Eşit Davranma İlkesi, s. 148-149; Yıldız, [2008], Eşit İşlem Yapma Borcu, s. 181, 188; Öztürk, [2021], Talimatlara Uyma, s. 250-251.

970) Yargıtay farklı konumda bulunan işçiler açısından eşit davranma yükümlülüğü yerine yönetim hakkı kapsamında işverenin farklı davranma hakkı bulunduğunu ifade etmiştir. Yargıtay 9. HD., E. 2020/9093, K. 2021/6337, T. 17.3.2021 kararı.

971) Öztürk, [2021], Talimatlara Uyma, s. 245-246.

972) Erbil Beytar, İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması. On İki Levha Yayınları, İstanbul, [2018], s. 46.

973) Süzek, [2019], İş Hukuku, s. 390-391; Okur, [2011], İşçinin Kişisel Verileri, s. 370, 399; Gürsel, [2016], İşçinin Kişisel Verileri, s. 40 vd.

sınırlama getirerek yönetme gücünün keyfi kullanımını sınırlandırır. Öte yandan hukukta eşitlik mutlak olmadığından belirli durumlarda uygulamanın bireyselleştirilmesi gerekebilir[974]. Bu aynı zamanda dijital izlemenin işçinin hakları üzerinde en az müdahale oluşturacak yöntemle gerçekleştirilmesi ilkesiyle de uyumludur. Örneğin suçun tespitine yönelik bir dijital izlemeyi sadece ilgili işçi veya işçilere uygulamak, kamera gözetlemesi üretim bandındaki işçilere yönelik kullanmak diğer işçileri izlemenin dışında tutmak daha az müdahaleci yöntemlerdir. Dolayısıyla dijital izlemenin bireyselleştirilme usulüne göre uygulanması eşit davranma borcuna aykırılık teşkil etmez[975]. Zira dijital izleme uygulamaları kullanılırken işçiler açısından izleme uygulamalarının kullanılmasını işin niteliği gereği (örneğin veznedar, yazılım geliştiren mühendis) haklı kılacak sebeplerin varlığı halinde işe veya işçiye özgü dijital izleme uygulamaları kullanması, bu kapsama girmeyen diğer işçiler için ise kullanılmaması bu ilkeye uygundur.

Dijital izlemenin bireyselleştirilmesi, eşitlik ilkesi açısından gruplandırmaların yapılması işverenin eşit davranma borcunda farklı uygulama gerçekleştirmenin hukuki temeli bulunduğundan eşitlik ilkesine aykırılıktan söz edilemez[976]. Örneğin bilişim yazılımları kodlayan ve yapay zeka yazılımları geliştiren bir teknoloji şirketinin kaynak kodlarının ve yazılım geliştirme sırlarının dışarı sızdırılmaması önem arz eder. Bu sebeple şirketin yazılım geliştirme birimde çalışan mühendislerin internet izlerinin izlenmesi, sadece bu kişilere yönelik oluşturulmuş bir odaya işçilerin biyometrik veri ile girmesi, odanın genel alanlarında kamera gözetlemesi gerçekleştirilmesi işverenin eşit işlem yapma borcuna aykırı değildir[977]. Bu örnekte işverenin kaynak yazılım kodlarının

974) Yıldız, [2008], Eşit İşlem Yapma Borcu, s. 31.
975) Yargıtay eşitlik ilkesinin işverenin yönetim hakkını sınırlandıran bir ilke olarak görmekte ve işverenin eşit davranma borcu kapsamında işçileri arasında keyfi ayrım yapmaması gerektiğine karar vermektedir. Yargıtay 9. HD., E. 2022/5442, K. 2022/7075 T. 6.6.2022; Yargıtay 9. HD., E. 2023/1603, K. 2023/7165 T. 16.5.2023.
976) Gürsel, [2016], İşçinin Kişisel Verileri, s. 374 vd.
977) Farklı örnekler ve "Finlandiya Çalışma Yaşamında Özel Hayatın Gizliliğinin Korunması Hakkında Kanun" m. 16/2'ye ilişkin açıklamalar için bkz. Gürsel, [2016], İşçinin Kişisel Verileri,

güvenliğinin sağlanması ve dışarı sızdırılmaması için belirli dijital izleme uygulamalarının kullanılması ve işçiler açısından farklılığa gidilmesi işin niteliğinden kaynaklanmaktadır.

İşveren dijital izleme uygulaması kullanırken dikkat etmesi gereken husus dijital izlemenin aynı durumdaki herkese eşit bir şekilde uygulanması gerekliliğidir[978]. Yazılım kodlayan mühendis örneğinden hareket ettiğimizde mühendislerden birisinin yazılımları rakip bir firmaya sızdırıldığı şüphesi söz konusu ise işveren bu durumda daha az müdahaleci bir yöntem yoksa, suçun tespitiyle ilgili sınırlı süreli, sınırlı bir alanda ve suçun tespit edilmesine yönelik olarak bu mühendisle ilgili gizli dijital izleme (örneğin e-postaların, bilgisayarın ve internet hareketlerinin izlenmesi) gerçekleştirebilir[979]. Bu durum ilgili işçi tarafından eşit davranma borcuna aykırılık olarak ileri sürülemez. Öte yandan, ilgili başlıkta detaylı incelendiği üzere, aydınlatma yükümlülüğünün unsurlarını taşımayan, sınırlı ve ölçülü olmayan, süresiz gizli izleme veya suçun önlenmesi için daha az müdahaleci bir yöntem söz konusuyken bunun gerçekleştirilmemesi dijital izleme uygulamasını hukuka aykırı hale getirir[980].

Eklemek gerekir ki, iş ilişkisinde işçi değişik kişisel değerlerini iş görme borcu kapsamında işverenin hakimiyet alanına açmaktadır. İş ilişkisinin bu özelliğinden kaynaklı işveren, işçinin kişisel değerlerinden fayda elde ettiğinden onun kişilik değerlerinin korunması için eşitlik ilkesinin de gözetildiği gerekli

---

s. 374; Kişisel verilerin işlenmesinde kişilik hakkı ve eşitlik ilkesi için bkz. Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 53.

978) Sevimli, [2006], Özel Yaşam, s. 146; Gürsel, [2016], İşçinin Kişisel Verileri, s. 245.

979) Bkz. AİHM Lopez Ribalda & Others v. Spain kararı, § 109-110; AİHM, Köpke v. Almanya Kararı, (Appl. No. 420/07), Judgment of ECHR of 05 October, [2010].

980) Bkz. Alman Federal İş Mahkemesi - BAG 2 AZR 681/16, § 33, https://www.bundesarbeitsgericht.de/entscheidung/2-azr-681-16/; İsviçre Federal Mahkemesi, 4A_518/2020, § 4.2.4, 25 Ağustos 2021 tarihli kararı. https://www.bger.ch/ext/eurospider/live/de/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F25-08-2021-4A_518-2020&lang=de&type=show_document&zoom=YES&

tedbirleri almakla yükümlüdür[981]. Bu yükümlülüğün bir gereği olarak işveren dijital izleme uygulamalarını kullanırken iş hukukunun işçinin kişilik değerlerini korumaya ve işçiyi gözetme borcuna ilişkin ilkelerini göz önüne alarak aynı durumdaki çalışanlar için benzer dijital izleme uygulamaları kullanması zorunludur.

2. Dijital İzlemenin Dürüstlük İlkesine Uygun Olması

Tüm borç ilişkileri için geçerli olan dürüstlük ilkesi işverenin yönetim hakkını sınırlandıran genel hukuk ilkelerinden birisidir[982]. Ayrıca iş ilişkisini ilgilendiren birçok hükümde dürüstlük ilkesine atıf yapılmıştır. Örneğin İş Kanunu m. 75/2 hükmünde: "işveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak…" düzenlemesi, KVKK'da ise m. 4/2-a'da genel ilke olarak "hukuka ve dürüstlük kurallarına uygun olma" hükmü öngörülmüştür. Dahası iş sözleşmesinin temelinde "güven ilişkisinin" bulunması dürüstlük ilkesine iş hukukunda geniş bir uygulama alanı bırakmaktadır. Örneğin TBK m. 398'de fazla mesai borcuna ilişkin düzenlemedeki atıf, işçinin "düzenlemelere ve talimatlara uyma borcunu" düzenleyen TBK m. 399'daki "işçiler, bunlara dürüstlük kurallarının gerektirdiği ölçüde uymak zorundadırlar" düzenlemesi ve işverenin gözetme borcunu düzenleyen TBK m. 417'deki işverenin "işyerinde dürüstlük ilkelerine uygun bir düzeni sağlamakla" yükümlü tutulması dürüstlük kuralının iş hukukundaki geniş uygulama alanın örnekleridir[983].

Dürüstlük ilkesi kanundan doğan hakların kullanılmasında, borçların sözleşmeye uygun ifasında, hukuki ilişkiden doğan hakların kullanılmasında ve

---

981) Emine Tuncay Kaplan, "İş Hukukunda Kişilik Haklarının Özellikle Bilgisayarda Toplanan Bilgilere Karşı Korunması", Ankara Üniversitesi Siyasi Bilgiler Fakültesi Dergisi, Prof. Dr. Cemal Mıhçıoğlu'na Armağan, Ankara Ocak-Aralık, [1997], C. 52, No. 1-4, s. 372.
982) Gülsevil Alpagut, "İşçinin Sadakat Borcu ve Türk Borçlar Kanunu ile Getirilen Düzenlemeler", Sicil, 25, Mart, [2012], s. 23; Güzel/Ugan Çatalkaya, [2014], Dürüstlük Kuralının İşlevi, s. 19-20, 41-42; Olgu Özdemir, İş Sözleşmesinin Feshinde Dürüstlük Kuralı ve Hakkın Kötüye Kullanılması Yasağı, On İki Levha Yayıncılık, [2022], s. 48 vd.
983) Dürüstlük kuralı ve hakkın kötüye kullanılması kişisel verilerin korunması ilişkisi için bkz. § 6. II. 3. a.

borçların yerine getirilmesinde uygulama alanı bulan bir ilkedir. Dürüstlük ilkesine hukuki ilişkilerin yorumlanması ve tamamlanmasında genel objektif bir kural olarak başvurulmaktadır[984]. Bu sebeple değinilen düzenlemelerdeki dürüstlük kuralına gerçekleştirilen atıflardan ve iş ilişkisinin güven temeline dayanmasından ortaya çıktığı üzere, işverenler dijital izleme uygulaması kullanırken dürüstlük ilkesini gözetmekle yükümlüdürler[985]. Zira dijital izleme yönetim hakkı, işçi verilerinin işlenmesi ve korunmasıyla ilgili olduğundan dürüstlük ilkesi uygulama alanı bulur.

Dürüstlük ilkesi, Medeni Kanun m. 2'nin birinci fıkrasında "dürüstlük ilkesi", ikinci fıkrasında ise "hakkın kötüye kullanılması yasağı" biçiminde düzenlenmiş olup, bu düzenlemeler iş hukukunda da uygulama alanı bulur[986]. Bu itibarla işveren işyerine ilişkin yönetim hakkı kapsamında kararlar alarak dijital

984) Oğuzman, M. Kemal/Barlas, Nami, Medeni Hukuk Giriş Kaynaklar Temel Kavramlar, Vedat Kitapçılık, İstanbul, 2020, s. 264; Aytekin Ataay, Medeni Hukukun Genel Teorisi, 3. Baskı, İstanbul, Fakülteler Matbaası, [1980], s. 147; Necla Giritlioğlu, Dürüstlük Kuralları, Hakkın Kötüye Kullanılması Yasağı, Özellikle Şekil Eksikliğinden Dolayı Geçersizliğin Hakkın Kötüye Kullanılması Yasağı ile Sınırlandırılması, İstanbul, [1989], s. 4; Selahattin Sulhi Tekinay, Medeni Hukukun Genel Esasları ve Gerçek Kişiler Hukuku, 6. Baskı, Filiz Kitabevi, İstanbul, [1992]; Yalçın Kavak, Medeni Hukukta Dürüstlük Kuralı ve İyiniyetin Korunması, İstanbul, Legal, [2019], s. 5; Eren, [2019], Borçlar Genel, s. 19; Mustafa Dural/Suat Sarı, Türk Özel Hukuku, C.1, 14. Baskı, Filiz Kitabevi, İstanbul, [2019], s. 244; Osman Gökhan Antalya/Murat Topuz, Medeni Hukuk, C.1, 3. Baskı, Seçkin Yayıncılık, Ankara, [2019], s. 495.

985) Yargıtay dürüstlük ilkesiyle ilgili; "Gerçekten de, her iki tarafın menfaatlerini korumak ve dengelemek için ileri sürülen güven ilkesine göre, bir irade beyanını anlamak ve değerlendirmek için, beyan muhatabınca bilinen ve bilinmesi gereken bütün hal ve şartları Medeni Kanun m.2'de düzenlenen dürüstlük ilkesi gereğince değerlendirmek gerekecektir. Böylece, beyana ne anlam verilmesi gerektiği ortaya çıkacaktır. Bu ilkeye göre, korunan karşı tarafın-beyan muhatabının- "haklı güven"idir. Beyan muhatabının gerekli dikkat ve özeni göstermeksizin, beyanı nasıl anladığına bakamayacaktır. Beyan muhatabı, kendisine ulaşan beyanı, dürüstlük ilkesi gereği, bildiği veya bilmesi gereken tüm unsurları dikkate alarak anlamalıdır. Yani, onun bu beyanı o şekilde anlaması MK. m.2 uyarınca haklı görünmelidir. İşte bu ilke, meydana gelen adaletsizliği ve taraflar arasında gerçekleşen sorunu çözmüş olmaktadır. Zira, güven ilkesi "karşılıklı birbirini gözetme" ve "bağlılık" esaslarına dayanmaktadır. Bu ilkeye göre, hem beyan sahibinin hem de beyan muhatabının menfaatleri dengede tutulmuş olmakladır. Bir yandan beyan muhatabının, dürüstlük kuralına (objektif iyiniyet) göre, bildiği ve bilebileceği bütün olguları değerlendirerek beyana vermesi gereken anlama olan haklı güveni korunmakta; diğer yandan ise, beyan sahibinin yaptığı beyanının, makul ve dürüst bir sözleşen insan tarafından anlaşılması olağan biçimde anlaşılacağına dair haklı güveni teminat altına alınmaktadır." biçiminde karar vermektedir. Yargıtay 9. HD., E. 2015/5593, K. 2016/20624 T. 22.11.2016; Yargıtay 9. HD., E. 2015/5614, K. 2016/20007 T. 15.11.2016;

986) Dural/Sarı, [2019], Türk Özel Hukuku, s. 241; Öztürk, [2021], Talimatlara Uyma, s. 206.

izleme uygulamaları kullanırken, yönetim hakkına göre daha üstte yer alan iş hukuku kaynaklarına uygun davranmakla yükümlüdür[987].

Önemle belirtmek gerekir ki, hukuki sorunları genel ilkelerle çözüme kavuşturmaya çalışmak ve her uygulamada genel ilkelere başvurmak diğer hukuki düzenlemeleri göz ardı etmek gibi keyfiliklere sebebiyet verir[988]. Dijital izleme açısından dürüstlük ilkesinin getirdiği sınırlama işverenin bu uygulamaları dürüst, namuslu, ortalama zekaya sahip ve ahlaklı bir kişi gibi hareket ederek kullanması ve işçilerde iş ilişkisi kapsamında oluşan güveni zedelemeyecek biçimde uygulaması gerekliliği biçiminde görünüm kazanır[989]. Ayrıca işverenin kanunun öngörmüş olduğu hükmü amacına aykırı düşecek biçimde başka bir ilişkide hükmü esas alarak uygulama gerçekleştirmesi kanuna karşı hile olarak değerlendirilmektedir.

Dürüstlük ilkesi aynı zamanda işverene kendi menfaatleriyle çatışan işçi menfaatlerini gözetmesi yükümlülüğü yüklemektedir. Örneğin gözetme borcu kapsamında işverenin, işçinin beden ve ruhsal sağlığını, kişilik haklarını, işçiyi çalışırken karşılaşacağı tehlikelerden korumak için gerekli teknolojik ve idari tedbirleri alma yükümlülüğü[990] bulunmaktadır. Evleviyet kuralının bir gereğe olarak işverenin de bu yükümlülüğe uygun davranması gerekir[991]. İşverenin veri işlemede en az veri ile faaliyetini sürdürmeye özen göstermesi, işlediği verilerin güvenliğini sağlaması ve işleme amacı kalmamış verileri imha etmesi aynı zamanda dürüstlük ilkesinin de bir gereğidir. KVK Kurumu yayımlandığı Uygulama Rehberi'nde "dürüstlük kuralına uygunluğu" kişisel veriler işlenirken korunması, ihlal edilmemesi ve veri sorumlusunun ilgili kişinin menfaatini gözetmesi

987) Öztürk, [2021], Talimatlara Uyma, s. 207.
988) Oğuzman/Barlas, [2020], Medeni Hukuk Giriş, s. 323-324.
989) Oğuzman/Barlas, [2020], Medeni Hukuk Giriş, s. 266.
990) Süzek, [2019], İş Hukuku, s. 388; Sevimli, [2013], İşçinin Kişiliğinin Korunması, s. 109-110;
991) Emine Tuncay Kaplan, "Yeni Türk Borçlar Kanunu Hükümlerine Göre İş İlişkisinde İşçinin Kişilik Haklarının Korunması", Sicil İş Hukuku Dergisi, Yıl:6, S.24, Aralık, [2011], s.41; Sevimli, [2013], İşçinin Kişiliğinin Korunması, s. 110.

gerekliliği olarak ifade etmiştir[992]. Dürüstlük kuralına uygun veri işleme veri sorumlusuna işlediği verilerle ilgili koruma yükümlülüklerini yerine getirmesi, ilgili kişinin makul beklentilerinin gözetilmesi ve verisi işlenen kişinin çıkarının gözetilmesini gerektirmektedir[993].

İşveren gözetme borcunun bir gereği olarak işçinin kişiliğini koruması, güvenliğini temin için gerekli tüm tedbirleri alması ve işlediği işçi verilerini onun haklı menfaatlerini koruyacak biçimde işlemesi[994] aynı zamanda dürüstlük ilkesinin bir gereğidir. Zira, işverenin kendisine bağımlı olarak çalışan işçiye yönelik çeşitli türde ve yoğunlukta dijital izleme uygulaması kullanma imkanının bulunması ve dijital izleme menfaati, işçinin temel hak ve özgürlükleriyle ilgili olan özel hayatının gizliğinin ve kişisel verilerinin korunması, haberleşme ve ifade özgürlüğü gibi haklarına aşırı müdahaleci sonuçlar ortaya çıkarmamalıdır. Özellikle dijital izleme uygulamalarında veri güvenliğinin sağlanmadığı ve veri minimizasyonun gerçekleştirilmediği[995] durumlarda bu uygulamalar işçinin özel hayatı ve kişisel verileri üzerinde ihlal edici sonuçlar ortaya çıkarır. Bu şekilde hareket etmek işverenin dürüstlük kuralına uygun bir çalışma düzeni kurarak işçinin kişilik haklarını koruyacak tedbirleri alması yükümlülüğüne aykırıdır[996].

Önemle eklemek gerekir ki, dijital izlemenin temel hak ve özgürlüklere[997] ilişkin düzenlemelere de uygun olması gerekir. Anayasa hükümleri iş hukukunda doğrudan uygulama bulduğundan, temel hak ve özgürlüklere ilişkin olan düzenlemeler işverenin yönetim hakkı kapsamında uygulayacağı dijital izleme

992) KVK Kurumu, [2019], Uygulama Rehberi, s. 64.
993) Yücedağ, [2019], Veri Koruma Genel İlkeleri, s. 50.
994) Süzek, [2019], İş Hukuku, s. 386; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 321; Ekonomi, [1987], Ferdi İş Hukuku, s. 154; Ulusan, [1990], İşçiyi Gözetme Borcu], s. 1 vd.; Demir, [2018], İş Hukuku ve Uygulaması, s. 212; Tunçomağ/Centel, [2018], İş Hukukunun Esasları, s. 135; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 182; Haluk Hadi Sümer, İş Hukuku, Seçkin Yayıncılık, 25. Baskı, Ankara, [2020], s. 89; Akyiğit, [2013], İş Hukuku, 207; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 290 vd.
995) Detaylı bilgi için bkz. § 6. II. 3. d.
996) Güzel/Ugan Çatalkaya, [2014], Dürüstlük Kuralının İşlevi, s. 19-20, 41-42; Özdemir, [2022], İş Sözleşmesinin Feshinde Dürüstlük Kuralı, s. 48-51.
997) Bkz. § 2. IV. 2.

uygulamaları üzerinde sınırlandırıcı bir etki ortaya çıkarır. Zira işçinin, işverenin otoritesi altında iş görme borcunu ifa etmesi onun temel hak ve özgürlüklerine müdahale hakkının işverene verdiği anlamına gelmez[998].

Günümüzde teknolojinin ortaya çıkardığı yoğun veri işleme olgusu kişinin kişilik değerinin ve insan onurunun korunması kişisel hak ve özgürlüklerin gelişmesi açısından daha önemli hale gelmiştir. Bu hususu AYM bir kararında şu şekilde tespit etmiştir[999]: "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı […]" amaçladığı belirtilerek "kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler" sebebiyle kişisel veriler daha fazla korunmayı gerektiren bir değere dönüşmüştür[1000].

3. Dijital İzlemede Ölçülülük Denetimi

Gücü sınırlandıran bir hukuk tekniği olan ölçülülük ilkesi, çatışan haklar ortaya çıktığında devreye girer ve hukuken korunan çatışan hakların adil bir dengede uzlaştırılmasında denetim olanağı sağlar. Bu özelliği gereği ölçülülük ilkesi karar verme süreçlerinde bir sonuca varma olanağı sağlar ve tarafların çatışan menfaatleri arasında bir denge oluşturur[1001]. Örneğin işverenin dijital izleme ihtiyacı ile işçinin özel hayatının gizliliğinin korunması ve kişisel verileri üzerindeki hakları arasında ortaya çıkan menfaat çatışmasında ölçülülük ilkesi

998) Ertürk, [2002], Temel Haklar, s. 49-50; Öztürk, [2021], Talimatlara Uyma, s. 288.
999) AYM, 9 Nisan 2014 tarih ve E:2013/122, K:2014/74 sayılı kararı. Bkz. https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-74-nrm.pdf
1000) KVK Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu Rehberi, s. 8. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/185c2130-8070-4b2b-a91e-1d48322ca352.pdf (Erişim Tarihi: 15.10.2022)
1001) Deniz Ugan Çatalkaya, İş Hukukunda Ölçülülük İlkesi, Beta, İstanbul, [2019], s. 30 vd.; Christian Rumpf, Ölçülülük İlkesi ve Anayasa Yargısındaki İşlevi ve Niteliği, Anayasa Yargısı Dergisi, C. 10, [1993], s. 45.

işverenin gücünü sınırlandırır ve kişilik hakkının özüne dokunulmasına izin vermez. Bu itibarla modern hukuk sistemlerindeki birçok normda, uluslararası sözleşme ve metinlerde, yüksek yargı kararlarında, kişisel verilerin işlenmesine ilişkin rehberlerde ve işçilerin dijital izleme uygulamalarıyla izlenmesinde dikkate alınacak AİHM ve AYM kararlarında "ölçülü" hareket edilmesi ölçütü ön plana çıkmaktadır.

a) Dijital İzlemenin Ölçülü Olması

Ölçülülük ilkesinin ortaya çıkışı ve asıl uygulama alanının idarenin keyfiliklerini sınırlandırması olmasına rağmen bu ilke özellikle güç asimetrisinin bulunduğu her iki tarafın özel hukuk kişisi olduğu olaylara da uygulama alanı bulacak şekilde bir yaygınlık kazanmıştır[1002]. Zira ölçülülük ilkesinde öngörülen denetimler temelde adaleti sağlama ve tarafların edimleri arasında adil bir dengeyi kurma düşüncesine dayanmaktadır[1003]. Böylelikle ölçülülük ilkesi sayesinde taraflar arasındaki güç dengesizliği giderilerek bireyin temel hak ve özgürlükleri müdahaleci uygulamalara karşı korunmuş olur ve kişi kendisini toplum içinde veya işyerinde özgürce ifade etme ve geliştirme imkanı yakalar.

Ölçülülük ilkesi demokratik hukuk devletinin temel görünümlerinden birisi olarak iktidarın, yasama organının ve kamu görevlilerinin gücü kötüye kullanılmasının ve insan haklarının ihlal edilmesinin önüne geçilmesi için tasarlanmış ve modern birçok hukuk sisteminin temel ve bağlayıcı bir ilkesi haline gelmiştir[1004]. Çatışan menfaatler arasında bir denge oluşturma işlevi üstlenen ölçülülük ilkesi, hukukun her alanında uygulanabilecek etik objektif ölçüt oluşturur

1002) Fazıl Sağlam, "Temel Hakların Sınırlanması ve Özü", Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, C. 506, S.B.F. İnsan Hakları Merkezi Yayınları, 4, Ankara, [1982], s. 117; Ugan Çatalkaya, [2019], Ölçülülük, s. 15 vd.
1003) Erhan Birben, "Yargı Kararları Işığında Toplu Eylem Hakkı Bakımından Ölçülülük Denetimi", İş Hukukunda Yeni Yaklaşımlar II, Ed. Kübra Doğan Yenisey/ Seda Ergüneş Emrağ, Beta Yayınevi, İstanbul, [2018], s.11.
1004) Pnina Alon Shenker/Guy Davidov, "Applying the Principle of Proportionality in Employment and Labour Law Contexts", McGill Law Journal, Vol. 59, Issue 2, [2013], s. 375.

ve hukuk devleti niteliğinin somutlaştırmada kilit bir rol üstlenir[1005]. Felsefi bir kavram da olan ölçülülük, "sana yapılmasını istemediğin şeyi başkasına yapma" diyen "altın kurala" kadar geri götürülebilmektedir[1006]. Bu yönüyle ölçülülük ilkesi kamu ve özel hukukun temel ilkelerinden birisi olarak toplumsal ilişkilerde ortaya çıkan sorunlarda gücün sınırlanmasında dengeleyici bir rol üstlenir[1007]. Bu bağlamda iş kanunları işverenin, görece olarak daha zayıf konumda bulunan işçiye karşı gücü kötüye kullanmasını sınırlamak için ortaya çıktığından, ölçülülük ilkesi iş hukukunda önemli bir uygulama alanı bulur[1008].

Ölçülülük ilkesi, AB mevzuatında birçok düzenlemeye konu edilmiştir. AİHS m. 18'de haklara getirilecek kısıtlamaların sınırlanmasında ölçülülük vurgusu; "bu Sözleşme hükümleri ile izin verilen kısıtlamalar öngörüldükleri amaç dışında uygulanamaz" ifadesiyle ve AB Lizbon Antlaşmasının 5. maddesinde, temel hak ve özgürlüklere getirilen sınırlandırmaların tespitinde ve yasama organının yetkilerinin kısıtlanmasında bir ölçüt ilke olarak ölçülülük (orantılı) vurgusu yapılmıştır[1009]. AB'nin 2000/43 sayılı Direktifinin 2/1-b ve 2000/78 sayılı Direktifinin 2. maddesinde dolaylı ayrımcılık tanımlanmış, meşru bir amaca ulaşmanın araçlarının uygun ve gerekli olması gerektiği düzenlenmiştir. Kullanılan araçların uygun ve gerekli olmaması halinde gerçekleştirilen düzenlemelerin dolaylı ayrımcılık olarak nitelendirilebileceği belirtilmiştir. Aynı doğrultuda 2000/C 364/01 sayılı AB Temel Haklar Şartı'nın 52. maddesinde hakların kullanılmasına ilişkin herhangi bir sınırlamanın kanunla yapılması, temel hak ve özgürlüklere ilişkin hakların özüne saygı gösterilmesi gerektiği, ölçülülük ilkesine uygun olarak, ancak gerekliyse ve Birlik tarafından tanınan genel çıkar hedeflerini veya başkalarının hak ve özgürlüklerini koruma ihtiyacını gerçekten karşılıyorsa

1005) Ekaterine Kardava, "Proportionality Principle as a Response Instrument to Challenges of Modern Labour Law", Journal of Law (TSU), Vol. 2017, No. 1, [2017], s. 174.
1006) Shenker/Davidov, [2013], Proportionality, s. 377; Aharon Barak, Proportionality: Constitutional Rights and Their Limitations, Cambridge University Press, [2012], s. 175.
1007) Kardava, [2017], Proportionality Principle, s. 173.
1008) Shenker/Davidov, [2013], Proportionality, s. 408-409; Kardava, [2017], Proportionality Principle, s. 176.
1009)http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0007.01/DOC_19, C 306/151, s. 151 (Erişim Tarihi: 02.05.2022).

yapılabileceği öngörülmüştür[1010].

Hukuk sistemimizde ölçülülük ilkesi en temel anlamda 1982 Anayasası'nın 13. maddesinde[1011] düzenlenmiş olup, gerekçesinde düzenlemenin Avrupa İnsan Hakları Sözleşmesi'nden alındığı belirtilmiştir. AİHM, ölçülülüğü; meşru amaçla, amaca ulaşmak için kullanılan araç arasındaki, yani müdahale ile elde edilecek yarar ile sınırlamadan doğan bireysel zarar arasındaki ölçüyü kaçırmamak, sınırlamanın demokratik bir toplumda ancak gerektiği ölçüde kullanılması[1012] olarak tanımlamaktadır.

İş ilişkisinde dijital izlemenin ölçülülüğü işverenin mülkiyeti korumak, uzaktan çalışmada denetim gerçekleştirmek, işyerinde alkol ve uyuşturucu kullanımının engellemek, çalışma sürelerini takip etmek ve verimliliği artırmak gibi meşru amaçlar için işçinin biyometrik verilerini işlemesi, işçiye çip takması[1013], tuvalette geçirdiği süreyi biyometrik verilerle izlemesi ve bilgisayar ekranı görülebilecek şekilde birçok yerden kamera ile gözetleme yapması; işçinin koltuğuna, masasına, bilgisayarına harekete duyarlı sistemler eklemesi[1014], kamera

1010) Hem AİHS, hem de AB Hukukunda ayrımcılığın, benzer durumdaki kişilere farklı muamele edilmesiyle olabileceği gibi, farklı durumlarda olan kişilere aynı şekilde muamele edilmesinden de ortaya çıkabileceği kabul edilmektedir. İkinci duruma 'dolaylı' ayrımcılık denilir, zira muamele farklı değildir, ama sonuçları farklıdır ve farklı özelliklere sahip insanlarca farklı şekilde hissedilecektir. Irk Eşitliği Yönergesinin 2(2)b maddesine göre 'tarafsız gibi görünen bir düzenleme, ölçüt veya uygulama belli bir ırktan veya etnik kökenden olan kişileri başkalarına kıyasla belirli bir dezavantaj içine sokuyorsa dolaylı ayrımcılık meydana geldiği kabul edilecektir. Avrupa Ayrımcılık Yasağı El Kitabı, Avrupa Birliği Temel Haklar Ajansı, 2010; Avrupa Konseyi, [2010], s. 29.

1011) Ölçülülük ilkesinin Anayasaya ilave ediliş formülüne ilişkin eleştiri için bkz. Kemal Gözler, "Anayasa Değişikliğinin Temel Hak ve Hürriyetlerin Sınırlandırılması Bakımından Getirdikleri ve Götürdükleri: Anayasanın 13'üncü Maddesinin Yeni Şekli Hakkında Bir İnceleme", Ankara Barosu Dergisi, Yıl 59, S. 2001/4, [2001], s. 53-67.

1012) AİHM, Handyside v. Birleşik Krallık Kararı, Karar Tarihi: 07.12.1976 Başvuru No: 5493/72. http://www.hrcr.org/safrica/access_information/ECHR/Handyside.html.; Şeref Gözübüyük, Anayasa Hukuku, 16. Baskı, Ankara, 2008, s. 178. Aynen aktarım Gaye Burcu Yıldız, "Türk İş Hukukunda Orantılılık İlkesi", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi C. 15, Özel Sayı-2013, [2014], s. 681; İbrahim Ö. Kaboğlu, "Hukukun Genel İlkeleri ve Anayasa Yargısı (Özgürlükler Hukuku Açısından Bir Yaklaşım)", Anayasa Yargısı Dergisi, Cilt 8, [1991], s. 303-304.

1013) İngiltere'de bazı şirketlerin işçilerine mikroçip takmasına ilişkin bir haber (Erişim 16.10.2021), https://tr.euronews.com/2018/11/12/calisanlara-takilan-mikrocipler-ingiltere-de-tartisma-konusu

1014) Ciocchetti, [2001], Monitoring Employee, s. 1.

gözetlemesindeki şüpheye dayalı olarak işçiyi diğer işçilerin yanında soyunmaya zorlaması ve üstünü araması gibi uygulamalarının varılmak istenen amaç açısından ne kadar ölçülü olduğunun değerlendirilmesi gerekmektedir.

Bu soruların cevaplanmasında işverenin, gerçekleştirdiği uygulamanın işçilerin üzerinde oluşturduğu etkiyi araştırıp araştırmadığı ve dijital izleme gerçekleştirmesindeki amacı için kullandığı aracın gerekli oranda kullanıp kullanmadığının göz önünde bulundurulması gerekmektedir[1015]. Bir amaca ulaşmak için kullanılan aracın varılmak istenen amaç açısından ölçülü olması gerektiğine vurgu yapan Braibant bu hususu; "Bir sineği ezmek için çekiç kullanmamak gerekir"[1016] benzetmesiyle somutlaştırmıştır. Bu niteliğinin bir sonucu olarak ölçülülük ilkesi denetimi, özellikle gücün işverende olduğu bir hukuki ilişkide, işverenin gücünün kendisine bağımlı çalışan işçi karşısında adil bir dengeye çekilmesine etki eder[1017].

Gerçekte sahada çalışan bir işçinin işyeri prosedürlerine uygun araç kullanımını ve iş tanımındaki yerleri ziyaret edip etmediğini tespit etmek isteyen işverenin, bu amacı GPS gibi bir izleme uygulamasıyla yerine getirebilmesi mümkünken, işçinin derisinin altına çip takarak[1018] sürüş hızını, sürücünün tepkilerini takip etmek istemesinin veya araç kabinine devamlı işçiyi gözetleme imkanı veren kamera yerleştirmesinin ölçülülük ilkesi kapsamında incelemeye tabi tutulması gerekmektedir. Örneğin tehlikeli madde taşıyan bir aracın trafik kullarına

---

1015) EDPB, Opinion 6/2018 on the draft list of the competent supervisory authority of Estonia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), https://edpb.europa.eu/sites/default/files/files/file1/2018-09-25-opinion_2018_art._64_ee_sas_dpia_list_en.pdf (Erişim Tarihi: 26.11.2022). Kararda WP 29 Kılavuz İlkeler WP 248'de belirlenmiş kriterlere atıf yaprak Kişisel Veri Etki Araştırmasının (DPIA) yapılmasını ve Kılavuz İlkelerde belirlenen iki koşulu karşılayan durumlarda etki araştırmasının yapılmasını önermiştir.

1016) Guy Braibant, Le principe de proportionnalité, Le juge et le droit public, Mélanges offerts à Marcel Waline, Tome II, Paris, LGDJ, 1974, 298; Aynen aktarım, Ugan Çatalkaya, [2019], Ölçülülük, s. 10.

1017) Ugan Çatalkaya, [2019], Ölçülülük, s. 10; Yüksel Metin, "Temel Hakların Sınırlandırılması Ölçülülük, Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?", SDÜHFD C. 7, S. 1, [2017], s. 17.

1018) İngiltere merkezli RFID çip üreticisi BioTeq'in şimdiye kadar 150 kişiye çip taktığına ilişkin bir haber, https://www.bbc.com/turkce/haberler-dunya-46177852 (Erişim Tarihi: 12.10.2021).

uygun hareket etmesini, kazaya karışmasını engellemek ve bu hususta iyileştirme yapmak isteyen bir işveren aracın yolda seyir halinde olduğu sürede yolu kamera ile takip etmesi amaç açısından ölçülü olarak nitelendirilebilirken, araç sürücüsünün her anını kayıt altına alan ve ona özel bir alan bırakmayan kamera sistemi amaç açısından ölçülü olarak nitelendirilmeyecektir.

Kişisel verilerin işlenmesinde genel ilkeleri belirleyen KVKK m. 4/2-ç bendinde de ölçülülük ilkesine atıf yapılmış ve kişisel verilerin; "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" gerekliliği düzenlenerek ölçülülük ilkesi denetiminin gerçekleştirilmesine olanak tanınmıştır. Böylelikle örneğin genel yerlerin dışında doğrudan işçileri hedef alan sürekli kamera gözetlemesi, başka türlü gerçekleştirilmesi mümkünken işçilerin parmak izi[1019] veya retina taramasıyla işyerine alınması, biyometrik verileri vasıtasıyla izlenmesi amaç açısından ölçülü kabul edilmeyecektir. Aynı doğrultuda uzaktan çalışmada keylogger gibi klavye vuruşlarını izleyen uygulamalarla devamlı biçimde izleme, web kameranın açılarak çalışılmasını zorunlu koşma gibi usullerle işçinin izlenmesi veya işçinin hareketlerine duyarlı uygulamalarla işyerinde sürekli takip edilmesi uygulamalarının istenen amaç açısından ölçülü olup olmadığının değerlendirilmesinde ölçülülük ilkesi önemli imkanlar sunar.

b) Dijital İzlemede Ölçülülük İlkesi Kapsamında Gerçekleştirilen Denetimler

Genel olarak ölçülülük ilkesinin "gereklilik", "elverişlilik" ve dar anlamda ölçülülük olarak ifade edilebilen "orantılılık" unsurlarının bulunduğu kabul edilmektedir[1020]. Anayasa Mahkemesi de ölçülülük ilkesini, "elverişlilik",

1019) Parmak izi kayıt sistemi ile işyerine girişin zorunlu tutulduğu bir işyerine ilişkin olarak, Anayasa Mahkemesi Genel Kurulu 10/3/2022 tarihli Ramazan Şahin (Başvuru Numarası: 2018/11988) kararında, Anayasa'nın 20. maddesinde güvence altına alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edildiğine karar vermiştir.
1020) Rumpf, [1993], Ölçülülük İlkesi, s. 29; Yıldız, [2014], İş Hukukunda Orantılılık, s. 682; Kaboğlu, [1991], Genel İlkeler, s. 303

"gereklilik" ve "orantılılık" olmak üzere üç alt ilke kapsamında değerlendirerek kararlar vermektedir. AYM kararlarında bu alt ilkeler; "elverişlilik, getirilen kuralın, ulaşılmak istenen amaç için elverişli olması; gereklilik, getirilen kuralın, ulaşılmak istenen amaç bakımından gerekli olması ve orantılılık ise getirilen kural ile ulaşılmak istenen amaç arasında olması gereken ölçü olarak açıklanmaktadır. Ölçülülük ilkesiyle devlet, cezalandırmanın sağladığı kamu yararı ile bireyin hak ve özgürlükleri arasında adil bir dengeyi sağlamakla yükümlüdür."[1021] şeklinde açılanmıştır.

aa) Gereklilik

Gereklilik ilkesi, bir amaca ulaşmak için birden çok yöntemle gerçekleştirilebilecek uygulamanın mutlaka gerekli olmasını ve bunlar içinden hakkı sınırlandıran en yumuşak yöntemin seçilmesini gerekli kılar[1022]. 1960'larda Alman Federal Anayasa Mahkemesi bu ilkeyi, "yasa koyucu aynı derecede etkili olup, ilgili temel hak üzerine sınırlayıcı etkisi daha az olan bir aracı bulamıyorsa, araç gereklidir"[1023] biçiminde tanımlamıştır. Örneğin uzaktan çalışmada, çalışma süresinin ne kadarının iş için geçirildiğini öğrenmek ve işçi üzerinde denetim oluşturmak isteyen işveren için dijital izleme gerçekleştirme gereklidir.

Bu kapsamda işverenin, işçinin bilgisayarda aktif geçirdiği süreyi ölçmek için bilgisayarın aktif süresini ve klavye vuruşlarını izlemesini olanaklı kılan bir denetim gerçekleştirmesi amaç açısından gerekli ve elverişli[1024] sayılabilirken, işverenin bu sürenin tamamında işçiyi ayrıca kamera açmaya zorlayacak bir uygulama gerçekleştirmesi ve bu sürenin tamamında işçinin tüm sosyal medya

1021) AYM, Esas Sayısı: 2013/99, Karar Sayısı: 2014/61, Karar Tarihi: 27.3.2014, Resmi Gazete Tarih-Sayı: 24.12.2014-29215.
1022) Sağlam, [1982], Temel Haklar, s. 115.
1023) Margherita Poto, "The Principle of Proportionality in Comparative Perspective", German Law Journal, Vol. 8, No: 9, September 1, [2007], s. 865; Rumpf, [1993], Ölçülülük İlkesi, s. 33; Sağlam, [1982], Temel Haklar, s. 115 vd.
1024) Gereklilik ile elverişlilik alt ilkeleri daha çok fiili imkanlarla ilgilidir ve bunların optimize edilmesiyle ilgilenir. Orantılılık alt ilkesi ise hukuki imkanların optimize edilerek taraflar açısından bir dengenin (ölçünün) sağlanmasını hedefler. Metin, [2017], Sınırlandırmada Ölçülülük, s. 7.

hareketlerini izlemesi temel hakları daha sınırlayıcı bir yöntem olduğundan gereklilik alt ilkesine takılabilecektir.

bb) Elverişlilik

Elverişlilik terimi sözlük anlamıyla "uygun olma, işe yarama"[1025] ve istenilen hedefe bir katkı sağlama durumunu ifade etmektedir. Elverişlilik alt ilkesi hedeflenen amaca uylaşmak için başvurulan vasıtaların amacı gerçekleştirmeye uygun olmasını gerekli kılar[1026]. Örneğin kamera gözetlemesinde amaç işyeri güvenliğini sağlamak ise, genel alanlara kamera konulması bu amacı gerçekleştirmek için elverişli kabul edilebilir, ne var ki işçinin bilgisayar ekranını da doğrudan gözetleyebilen bir kameranın yerleştirilmesinin, varılmak istenen işyeri güvenliğinin sağlanması amacı açısından uygun olmadığını belirtmek gerekir. Bu bağlamda dijital izlemede de elverişlilik ilkesinin en önemli özelliği, başlatılan uygulamanın diğer tarafın hukuk alanında gerçekleştirdiği etki değil; önemli olan söz konusu kararın amacı gerçekleştirmeye uygun olup olmadığı ve istenilen sonuca bir katkı sağlayıp sağlamadığıdır[1027].

cc) Orantılılık

Ölçülülük ilkesinin en önemli ve kritik aşamasını orantılılık denetimi oluşturur. Orantılılık alt ilkesiyle, ilgiliye ölçüsüz bir yükümlülük yükletilmemesi ve öngörülen düzenlemenin ilgili için beklenmedik nitelikte olmaması belirtilmektedir[1028]. Buna göre, gerekli ve elverişli olduğu iddia edilen bir dijital izleme uygulaması amaç-uygulama ilişkisi kapsamında değerlendirmeye tabi tutulmalı ve amaç ile uygulamanın işçi üzerinde oluşturduğu yükümlülük ölçüsüz

1025) TDK Güncel Türkçe Sözlük, https://sozluk.gov.tr/
1026) Ugan Çatalkaya, [2019], Ölçülülük, s. 65.
1027) Sağlam, [1982], Temel Haklar, s. 114; Ugan Çatalkaya, [2019], Ölçülülük, s. 65-66.
1028 Sağlam, [1982], Temel Haklar, s. 116, ve 360. dipnotta atıfta atıf yapılan Alman Anayasa Mahkemesi kararı.

bir oran içinde olmamasına dikkat edilmelidir[1029]. Bu ilke kapsamında işverenin bir amaç için öngördüğü dijital izleme uygulaması işçi açısından ölçüsüz bir yükümlülüğe sebebiyet vermemelidir. İşverenin gücüne karşı işçinin korunması iş hukukunun temel varlık sebeplerinden birisi olduğundan gerçekleştirilen dijital izlemenin amacı kapsamında orantılılık denetimi yapılarak gerçekleştirilen izlemeye ilişkin nitelendirme yapılmalıdır.

c. Uygulamada Ölçülülük Denetimi

Veri sorumlusu işveren dijital izleme uygulaması kullanmadan önce veri işleme amacı kapsamında ölçülülük denetimi yapması gerekmektedir. Bu aynı zamanda hukukumuzda ölçülülük ilkesini belirten ve kişisel verilerin işlenmesinde ölçülülük ilkesini arayan genel hüküm olan Kişisel Verilerin Korunması Kanunu'nun 4. maddesinin "ç" bendinin bir gereğidir. Anılan bende göre, kişisel veri işlenirken, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine uygun davranılmalıdır[1030].

Ölçülülük ilkesinin işyerinde uygulaması açısından AİHM'in Madsen & Danimarka[1031] ve Wretlund & İsveç[1032] kararları önemlidir. Davaya konu olayların

---

1029) Metin, [2017], Sınırlandırmada Ölçülülük, s. 7,13.

1030) Yargıtay fesihte işverenin ölçülülük ilkesini dikkate alması gerektiğine karar vermektedir. Yargıtay 9. HD., E. 2022/5442, K. 2022/7075 T. 6.6.2022 tarihli kararında "...İş sözleşmesine aykırı davranışta bulunan işçiye yaptığı eylemle orantılı bir yaptırım uygulamalıdır. Yapılan eylemle orantılı olmayan ve ölçüsüz olarak nitelendirilebilecek bir yaptırım mazur görülemez. Sonuç itibariyle fesihte bir cezadır. Ölçülülük ilkesi uyarınca, uygulanacak önlem, ulaşılmak istenen amacı gerçekleştirmeye elverişli olmalı bir başka anlatımla tedbir uygun olmalı, ulaşılmak istenen amaç açısından gerekli olmalı ve uygulanacak tedbirin sonucu olan müdahale ile ulaşılmak istenen amaç, ölçüsüz bir oran içerisinde bulunmamalıdır. Bu ilke uyarınca yargıç feshin geçerli olup olmadığını kararlaştırırken, işçinin davranışının ağırlığını dikkate alarak, her olayın özelliğine göre işçinin davranışı ile işverence uygulanan fesih türü arasında bir orantısızlık (ölçüsüzlük) olup olmadığını takdir edecektir. İşçinin davranışının haklı fesih olarak değerlendirilmesi ağır ve gerekli olmayan bir sonuç ise geçerli neden, işveren açısından iş ilişkisinin devamını önemli ölçüde çekilmez hale getirmeyecek ve işçiye fesih dışında başka bir disiplin cezası ile geçiştirilebilecek bir davranış ise, geçersiz neden kabul edilmelidir." biçiminde karar vermiştir.

1031) https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57509%22]} (Erişim Tarihi: 06.10.2022).

1032) AİHM, başvuranın itiraz ettiği hususların İsveç hukukunda yeterli bir temele sahip olduğunu ve dolayısıyla işyerinde uygulanan testin AİHS m. 8.2. anlamında "hukuka uygun" olduğunu tespit

benzer olduğu her iki başvuruda, işçiler işyerinde uygulanan zorunlu test sisteminin özel hayata saygı hakkını ihlal ettiğini ileri sürmüşlerdir. Madsen davasında, Danimarkalı bir denizcilik şirketinde yolcu asistanı olan başvuran, işverenin işçileri rastgele kontrol yöntemiyle teste tabi tutmasını ve testi geçme zorunluluğunun bulunmasını AİHS m. 8'de düzenlenen özel hayata saygı hakkı düzenlemesine aykırı olduğunu ileri sürmüştür. İsveç'te nükleer tesiste çalışan Wretlund işyerinde uygulanan alkol ve uyuşturucu testinin, AİHS m. 8'de korunan özel hayata saygı hakkını ihlal ettiğini iddia etmiştir. Her iki başvurucu da yaptıkları işlerin geminin ve nükleer tesisin güvenliğini doğrudan ilgilendiren işler olmadığını ileri sürmüşlerdir. Her iki davada da AİHM yapılan işin "kamu güvenliği" ve "başkalarının hak ve özgürlüklerinin korunması" açısından değerlendirmiş ve Madsen kararında AİHM, gemideki tüm mürettebatın güvenlik ekibinin bir parçası olduğunu ve herhangi bir zamanda gemide güvenlik ile ilgili işlevleri yerine getirebilme ihtimalinin bulunduğunu; Wredlund kararında ise, tesisin niteliğini ve güvenliğin önemini değerlendirerek testlerin bu meşru bir amaç kapsamında uygulandığına karar vermiştir. AİHM, özel hayata saygı hakkı ile güvenlik meşru menfaatini değerlendirirken işçilerin önceden bilgilendirilmesini, testlerin sıklığı, tüm işçilere eşit uygulanması, testlerde elde edilen verilerin herhangi bir şekilde kullanılmaması gibi olguları dikkate alarak karar vermiştir[1033].

WP 29 Çalışma Grubu iş ilişkisinde işçinin, işverene bağımlı olarak çalışması ve ekonomik bağımlılığı sebebiyle sözleşme tarafları arasında açık bir dengesizlik bulunduğunu ve ancak işçilerin olumsuz sonuçlardan çekinmeden iradelerini açıklamaları mümkün olmadıkça gerçek bir açık rızanın çok düşük bir ihtimal olduğunu belirtilmiştir[1034]. Bundan dolayı ölçülülük denetimi işçinin kişisel

---

etmiştir. https://www.eurofound.europa.eu/publications/article/2004/european-court-of-human-rights-rules-on-drug-testing (Erişim Tarihi: 06.08.2022).

1033) Elena Sychenko, "International Protection of Employee's Privacy under the European Convention on Human Rights", Zbornik Pravnog Fakulteta u Zagrebu, Vol. 67, No. 5, [2017], s. 771-772.

1034) The Art. 29 WP, Opinion 2/2017 kişisel verilerin iş ilişkisi kapsamında işlenmesine ilişkin WP 249, 8 Haziran 2017, s. 3; The Art. 29 WP, Opinion 03/2013 (n 66) s. 3; EU, [2018], Handbook, s. 144.

verilerinin korunmasında hukuka uygunluğun tespitinde etkin bir denetim olanağı vermektedir. Veri sorumlusu işveren ölçülü olmayı da öngören genel ilkeler denetimini gerçekleştirdikten sonra dijital izleme uygulaması kullanması dijital izlemenin işçi haklarını ihlal etme etkisini sınırlandıracaktır.

AYM'nin[1035] ve Yargıtay'ın[1036] iş ilişkisinde özel hayatın gizliliğinin korunması ve kişisel verilerin işlenmesine ilişkin kararlarına baktığımızda konunun aydınlatma yükümlülüğü ve işçinin rızasının alınması kapsamında değerlendirildiği görülmektedir. Bu anlamda rızanın bulunması kişisel verilerin işlenmesi için yeterli bir gerekçe kabul edilmiştir. Gerçekte WP 29 Çalışma Grubu görüşünde[1037] ve AİHM'in iş ilişkisinde kullanılan testlere ilişkin kararlarında[1038] rıza tek başına kişisel veri işlenmesi için yeterli görülmemiş, rızanın veri işlenmesi için bir hukuki zemin olduğunu, fakat işçinin iradesinin sakatlığa uğratılmadan rızasının alındığının ispat edilmesi yanında veri sorumlusu işverenin veri işleme faaliyetinin ölçülülük gibi veri koruma mevzuatının genel ilkelerine uygun olması da aranmıştır.

4. İşçi Adaylarının Dijital İzleme Uygulamalarıyla İzlenmesi: Culpa in Contrahendo Sorumluluğu

Veri koruma mevzuatlarının işçi verilerinin işlenmesi için öngördüğü

1035) AYM, 10/1/2018 tarih ve Başvuru No: 2014/14187 sayılı Nurcan Belin kararı § 37-39; AYM, E.2014/74, K.2014/201, 25/12/2014; AYM, E.2013/122, K.2014/74, 9/4/2014; AYM, E.2014/149, K.2014/151, 2/10/2014; AYM, E.2013/84, K.2014/183, 4/12/2014; AYM, E.2014/180, K.2015/30, 19/3/2015; AYM [GK], Bülent Kaya başvurusu, Başvuru No: 2013/2941, 11/5/2016, § 49; AYM [GK], Bülent Polat başvurusu, Başvuru No: 2013/7666, 10/12/2015, §62; AYM, Ata Türkeri başvurusu., Başvuru No: 2013/6057, 16/12/2015, § 31).

1036) Yargıtay 22. HD, E. 2017/21857 - K. 2019/9884, T. 07.05.2019; Yargıtay 9. HD, E. 2009/447 - K. 2010/37516, T. 13.12.2010; Yargıtay 22. HD, E. 2016/6321 - K. 2016/13143, T. 3.5.2016; Yargıtay 22. HD. E. 2013/36288 –K. 2015/9548, T. 10.03.2015.

1037) The Art. 29 WP, Opinion 2/2017 kişisel verilerin iş ilişkisi kapsamında işlenmesine ilişkin WP 249, 8 Haziran 2017, s. 3; The Art. 29 WP, Opinion 03/2013 (n.66) s. 3.

1038) AİHM, Wretlund v. Sweden, App. No. 46210/99, başvurusunda, nükleer santralde çalışan İsveçli ofis temizlikçisi işçinin işyerinde uyuşturucu testine tabi tutulmaması gerektiği, yaptığı işin dikkate alındığından bunun aşırı bir müdahale olduğunu, bunun özel hayata orantısız bir müdahale olduğunu, özel hayatının ihlal edildiğine ilişkin başvurusunu işyerinin niteliğine dikkat çekerek alınan tedbirin orantısız olmadığını ve başvurunun kabul edilemez olduğuna karar vermiştir.

sınırlamalar iş görüşmelerine katılan işçi adayları için de geçerlidir[1039]. Bu itibarla işçi adayından doğrudan veri işlendiği durumlarda, veri işlenmeden önce işçi adayının aydınlatma yükümlülüğüne uygun bilgilendirilmesi, kamera gözetlemesi söz konusu ise buna ilişkin katmanlı aydınlatma ve bilginin bulunması gerekir[1040].

İş sözleşmesinin kurulmasından önce işveren ve işçi adayı sözleşmenin içeriği, işin kapsamı, hak ve yükümlülüklerle ilgili birbirleriyle görüşmeler gerçekleştirirler. Bu sebeple iş sözleşmesinin kurulması öncesi görüşmelerde, tarafların sözleşmeden doğan bir sorumluluğunun (culpa in conrahendo) bulunduğu kabul edilmektedir[1041]. Zira iş görüşmelerinde sözleme tarafları tesadüfi bir şekilde bir araya gelmezler, iş görüşmelerinde ileride bir sözleşme kurma gayesi bulunur. Ayrıca işverenin işçi adayını görüşmeye davet etmesi, görüşme sürecinin devam etmesi işçide haklı bir beklenti oluşturur ve belirli bir süreye yayılan taraf teması güvene dayalı bir ilişki ortaya çıkarır. Bu itibarla sözleşme öncesi temasla taraflar arasında bir hukuki ilişkinin başladığı ve özen yükümlülüğü ile koruma borcu kapsamında yükümlülüklerin oluştuğu kabul edilmektedir[1042].

Culpa in contrahendo sorumluluğunda tarafların bir sözleşmenin kurulması

1039) İşçi adayının görüşme bilgilerini mevcut işvereniyle paylaşan işveren ile ilgili KVK Kurulu idari para cezası uygulamıştır; Kararda özetle; "Veri sorumlusu tarafından ilgili kişinin şirketleri ile iş görüşmesi yaptığı bilgisi ile iş görüşmesinde ilgili kişinin halihazırda çalışmakta olduğu iş yeri hakkında birçok söz beyan ettiği bilgisinin aktarılması faaliyetinin Kanun'un 8'nci maddesine uygun şekilde gerçekleştirilmediği değerlendirilmekte olup bu durumun Kanun'un 12'nci maddesinde yer verilen "veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır" hükmüne aykırılık teşkil etmesi nedeniyle, veri sorumlusunun 1997 yılından beri faaliyet gösterdiği, Türkiye genelinde 7 ofis, 1 depo ve 135 çalışan ile lojistik faaliyetlerini yürüttüğü ve ilgili kişinin başvurularına yasal süresi içerisinde yanıt vermediği de dikkate alınarak veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi kapsamında 100.000 TL idari para cezası uygulanmasına" hususları değerlendirilmiştir. Bkz. "İlgili kişinin bir şirket ile iş görüşmesi yaptığı bilgisi ile görüşmenin içeriği hakkındaki muhtelif bilgilerin iş görüşmesi yapılan şirket tarafından halihazırdaki iş yeri ile paylaşılması" hakkında Kişisel Verileri Koruma Kurulunun 04/08/2022 tarihli ve 2022/798 sayılı Karar Özeti, https://kvkk.gov.tr/Icerik/7575/2022-798 (Erişim Tarihi: 20.12.2023).

1040) Manav, [2015], Kişisel Veriler, s. 113-114.

1041) Eren, [2019], Borçlar Genel, s. 1265.

1042) Yargıtay 9. HD., E. 2016/20712, K. 2020/8343 T. 17/09/2020; Yargıtay 22. HD., E. 2017/20291 K. 2018/28025 T. 24.12.2018; Süleyman Yalman, Türk – İsviçre Hukukunda Sözleşme Görüşmelerinden Doğan Sorumluluk, Seçkin Yayıncılık, Ankara, [2005], s. 37 vd.

amacıyla görüşmelere başlamaları esnasında taraflardan birisinin kusurlu olarak dürüstlük ilkesine uygun davranmaması durumunda oluşan zararın tazmin edilmesini ifade etmektedir[1043]. İş sözleşmesini kurmak için bir araya gelen işveren ve işçi arasında dürüstlük ilkesi temelinde bir temas söz konusu olduğundan birtakım koruma ve bilgilendirme yükümlülükleri ortaya çıkmaktadır[1044]. Bu sebeple işverenin KVKK yükümlülükleri kapsamında aydınlatma yükümlülüğünü yerine getirmesi, aday işçi ile görüşmelerde işlediği veriyi ifşa etmemesi, üçüncü kişilerle paylaşması ve işçi adayının kişisel verileri üzerinde ihlal edici sonuçlar ortaya çıkaracak dijital izleme uygulamaları kullanmaması gerekir. Bunun aksi işveren uygulamaları culpa in contrahendo sorumluluğuna sebebiyet verir. Bu durumda işçi adayı uğramış olduğu zararları culpa in contrahendo sorumluğu kapsamda talebe konu edebilir[1045].

Sözleşme öncesi görüşmelerde iş ilişkisinin tarafı olacak işveren ile işçi arasında ortaya çıkan güven ilişkisinde, tarafların dürüstlük ilkesinden kaynaklanan davranış yükümlülüklerine uygun davranmayarak kusurları sebebiyle diğer tarafa zarar vermesi durumda bunun tazmin edilmesi sorumluluğu culpa in contrahendo

1043) M. Kemal Oğuzman/Turgut Öz, Borçlar Genel Hukuku, Vedat Kitapçılık, C. I, [2019], s. 38.
1044) Yargıtay 22. Hukuk Dairesi, çalışma izni bulunmayan yabancı uyruklu bir akademisyenle sözleşme görüşmeleri yapan ve bir buçuk ay akademisyeni çalıştırıp, çalışma izninin bulunmadığını bilmesine derslere girmesini sağlayan, sonrasında iş sözleşmesi akdetmeyen bir üniversite ile ilgili verdiği kararda bu sorumluluğu şu şekilde gerekçelendirmiştir: "borç doğurucu sorumluluk kaynakları yönünden somut olay değerlendirildiğinde; olaya "sözleşme görüşmelerinden doğan sorumluluk" kurallarıyla bakılması gerektiğinde kuşku ve duraksamaya yer olmamalıdır. Gerçekte de, sözleşme bir süreçtir. Bir anda kurulup meydana gelen hukuki bir işlem değildir. Sözleşme kurulmadan önce taraflar sözleşmenin muhtevası, şartları, içerdiği hak ve yükümlülükler üzerinde görüşmeler yaparlar; bu görüşmeler kısa veya uzun sürebilir. Görüşmelerin başlamasıyla görüşmeciler arasında hukuki bir ilişki kurulur. Bu ilişki sözleşme benzeri bir güven ilişkisidir. Güven ilişkisi MK. m. 2/1'de düzenlenmiş bulunan dürüstlük kuralına dayanır. Buna göre görüşmeler esnasında görüşmecilerin sözleşmenin muhtevası ve şartları hakkında birbirlerini aydınlatması, dürüstlük kuralına uygun davranması, birbirlerinin kişilik ve mal varlığı değerlerine zarar vermemek için gerekli özeni göstermesi, koruma yükümlülüklerine uyması gerekir. Görüşmeciler bu yükümlülüklere kusurlu olarak aykırı davranıp, görüşmelerin başlamasıyla aralarında kurulmuş bulunan güven ilişkisini ihlal ettikleri takdirde bundan doğan zarardan sorumludurlar." Yargıtay 22. HD., E. 2017/20291, K. 2018/28025 T. 24.12.2018.
1045) Dural/Sarı, [2019], Türk Özel Hukuku, s. 247; Oğuzman/Barlas, [2020], Medeni Hukuk Giriş, s. 311-312.

sorumluluğu olarak tanımlanmaktadır[1046]. Buna göre işverenin dürüstlük ilkesine aykırı olarak sözleşme görüşmelerinde çeşitli türde dijital izleme analiz ve raporlama uygulaması kullanması, bu hususta işçi adayına bilgi vermemesi adayın özel hayatı ve kişisel verileri üzerindeki haklarını ihlal eder. Örneğin işverenin işçi adayı hakkında gerçekleştirdiği arama motoru araştırması, sosyal medya taraması sonucu elde etmiş olduğu verileri işlemeye konu etmesi[1047], iş görüşmesi esnasında bu verilere dayanarak sorular sorması, bu verilerin ifşa edilmesi; iş görüşmesi esnasında gizli kamera gözetlemesi gerçekleştirildiğinin ortaya çıkması; işçi adayının duygu durumunu, davranışlarını analiz eden dijital izleme uygulamalarının kullanıldığının anlaşılması durumlardan işçi adayı diğer hakları yanında culpa in contrahendo hükümleri kapsamında tazminat talebinde bulunabilir[1048].

KVKK m. 5/2-c bendinde düzenlenen açık rıza dışında veri işleme hukuki şartlarından birisi olan sözleşmenin kurulmasıyla ilgili olan veri işlemeleri iş sözleşmesinin kurulması için bir araya gelen işveren ve işçi adayları için de geçerlidir. Aynı husus GVKT m. 6/1-(b) bendi düzenlemesinde de öngörülmüştür. Ayrıca işverenin bu süreçte veri işlemesi ve işçi adayları için belirli araştırmaları yapmasında bir meşru menfaati de söz konusudur. Bu sebeple kişisel verileri koruma düzenlemeleri bu durumlarda kişisel veri işlenmesini meşru amaç kapsamında kalması ve sınırlı ve ölçülü olması kaydı ile hukuka uygun kabul etmiştir. Ancak bu durumlarda dahi işçi adayı işlenen verileriyle ilgili ispatlanabilir bir yöntemle Tebliğ'e uygun bilgilendirilmeli ve hakları kendisine

1046) Eren, [2019], Borçlar Genel, s. 1264-1265; M. Kemal Oğuzman/Turgut Öz, Borçlar Hukuku Genel Hükümler, I. Cilt, Vedat Kitapçılık, 15. Baskı, İstanbul, [2019], s. 488 vd.
1047) Önemle belirtmek gerekir ki, işçi adayının sosyal medya hesaplarının herkese açık olması ve paylaşımların herkes tarafından görülebilmesi bu verilerin işlenmesinin hukuki dayanağı olamaz. Zira, herkese açık gerçekleştirilmiş sosyal medyada yer alan veri, ancak paylaşma iradesine uygun olarak işlendiğinde hukuka uygun veri işlemeden bahsedilebilir. KVKK Kurumu'nun yayımladığı rehberde bu husus şu şekilde vurgulanmıştır: "İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. "Örneğin, kişinin herkesin erişimine açık bir şekilde sosyal medya hesabında kişisel verisini paylaşması halinde verinin işlenmesi.) Bu hükmün uygulanabilmesi için kişisel verilerin ilgili kişi tarafından alenileştirme iradesinin ortaya konulması ve farklı amaçlar doğrultusunda kullanılmaması gerekir." Bkz. KVK Kurumu, [2019], Uygulama Rehberi, s. 44, 76.
1048) Sevimli, [2006], Özel Yaşam, s. 181; Gürsel, [2016], İşçinin Kişisel Verileri, s. 339.

hatırlatılmalıdır[1049]. Zira iş ilişkisinde olduğu gibi işçi adayı ile yapılan görüşme de eşit olmayan bir ilişki çerçevesinde gerçekleşir ve işe ihtiyacı olan adayın açık rıza beyanını özgür iradesiyle açıklamasını sınırlandırır. Bu itibarla işçi adayanın kişisel verilerinin işlenmesinde açık rızanın yasal bir dayanak olarak görülmemesi gerektiğini belirtmek gerekir[1050]. Aynı husus içi adayı için gerçekleştirecek dijital izleme, algoritmik analiz uygulamaları için de geçerlidir.

İşverenin, işçi adayı ile ilgili olarak gerçekleştireceği sosyal medya ve arama motoru taramasında elde edeceği veriler işçinin mesleki deneyimleri ve yeterlilikleriyle sınırlı değildir[1051]. İşverenin işçi adayı ile ilgili bu şekilde araştırma yaparak veri işlemesi veri işleme şartlarından birisine dayanmıyorsa KVK hukuku düzenlemelerine aykırıdır. Bu itibarla veri sorumlusu işverenin aday işçi ile ilgili kişisel veri işlemesinin KVKK m. 5'te düzenlenmiş veri işleme şartlarından birisine dayanması zorunludur. İşçi adayının sosyal medya veya internette paylaştığı verilerinin paylaşım amacı dışında işlemeye konu edilmesi KVK hukuku düzenlemelerine aykırı olduğu gibi bu verilerin aleni veri olarak kabul edilmesine olanak yoktur. Zira sosyal medyada, internette, blog veya web sitesinde paylaşılan verinin alenileştirilmiş olduğu tespitinde bulunabilmek için ilgili kişi tarafından alenileştirmeye ilişkin bir iradenin ortaya konmuş olması ve veri sorumlusu işverenin ise bu veriyi alenileştirme amacına uygun işlemesi gerekmektedir[1052]. Örneğin blogunda veya web sitesinde özgeçmişini paylaşan bir kişiye iş teklifinde bulunmak için telefon numarasını ve iletişim bilgilerini kullanmak alenileştirme iradesine uygun bir veri işlemedir. Öte yandan bir kişinin sosyal medyada paylaşmış olduğu bir yorum, görüntü veya eleştirinin işlenmesi ve iş görüşmesi esnasında işçi adayına bu hususta sorular sorulması alenileştirme iradesine uygun olmayan veri olduğundan, işverenin işçi adayına ilişkin veri işlemesinin hukuki

1049) WP29, Opinion 2/2017 on data processing at work – WP 249, 8 Haziran 2017, s. 11. http://ec.europa.eu/justice/data-protection/index_en.htm (Erişim Tarihi: 20.11.2022)
1050) WP29, [2017], Opinion 2/2017, s. 18.
1051) Yeliz Bozkurt Gümrükçüoğlu, "İşçinin Sosyal Medya Kullanımının İş Hukukundaki Etkileri", PressAcademia Procedia, V.7, [2018], s. 373.
1052) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 285; KVK Kurumu, [2019], Uygulama Rehberi, s. 44, 76.

dayanağının bulunmadığını belirtmek gerekmektedir.

İşverenin işçi adayının verisini işlemesi, iş ilişkisinde dijital izlemenin hukuka uygunluk ölçütleri kapsamında sınırlandırılmasının gerekliliği açısından yakın tarihli örneklerinden birisi New York'ta yaşanmıştır. New York'ta iş görüşmesine giden ve sosyal medya hesapları arkadaşları dışındaki kişilere sınırlı erişimli olan işçi adayından hesabındaki bilgilere ve paylaşımlara erişmek için Facebook şifresini istemiştir[1053]. İşveren ayrıca işçi adayı ile geniş kapsamlı bir sosyal medya taraması da gerçekleştirmiştir. İşverenin işçi adayı ile ilgili bu uygulamasının medyaya yansıması ve özel hayatın gizliliğinin ihlal edilmesi kapsamında tartışmalara konu edilmesi üzerine işverenlerin bu tür bilgileri istemesini yasaklayan yasal düzenlemeler yapılmıştır[1054]. Ülkemiz KVK hukukunda bu konuda doğrudan bir düzenleme bulunmamasına rağmen KVK hukukunun genel ilkelerinden hareketle işverenlerin işçi adaylarıyla ilgili olarak arama motoru veya sosyal medya mecralarında eriştiği verileri işlemesi veya ilgili işçi adayının kişisel verilerini alenileştirme amacı dışında işlemeye konu etmesi KVKK'nın veri işlemenin şartlarına ilişkin düzenlemelerine ve veri sorumlusunun aydınlatma yükümlülüğüne ilişkin düzenlemelerine aykırı olacaktır.

Eklemek gerekir ki, iş görüşmeleri aşamasında işe ihtiyacı olan işçi adayında oluşacak haklı beklenti aynı zamanda iradesini açıklamada özgürce hareket etme olanağını, iş ilişkisinde olduğu gibi güçleştirir. Bu sebeple işçi adaylarının kişisel verileri işlenirken açık rızaya dayalı veri işleme yerine diğer veri işleme şartlarının varlığı (örneğin, bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması veya kanunlarda açıkça öngörülme gibi) aranmalıdır. Ayrıca iş görüşmelerinde uygulanan testler işçi adayının yetkin olup

1053) Justin Basset isimli işçi adayı, 2012 yılında New York City'de bir iş görüşmesine gitmiştir. İş görüşmesinin klasik bir soru cevap görüşmesi olmasını beklerken kadın insan kaynakları çalışanı bilgisayarını açarak işçi adayından sadece belirli kişilerin erişimine açık olan Facebook hesabını şifresini istemiştir. Bu olay sonrası içi adayı başvurusunu geri çekmiş ve olayı medyaya ve yargıya taşımıştır. Susan Park, "Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy", American Business Law Journal 51, No. 4, [2014], s. 779
1054) Park, [2014], Employee Internet Privacy, s. 779-782.

olmadığı ve iş için uygun olup olmadığıyla sınırlandırılmalıdır.

İlgili başlıkta[1055] detaylı incelendiği üzere, iş görüşmesinde işçinin işe uygunluğunu tespit etmek için bazı sağlık raporlarını ve tıbbi muayeneye tabi tutabilir. Bu yapılırken KVKK m. 6/3'teki özel nitelikli kişisel verilerin işlenmesi kurallarına uygun davranılmalı, sır saklama yükümlülüğü bulunan ve koruyucu hekimlik kapsamında görevini icra eden işyeri hekimi üzerinden sürecin yürütülmesi gerekir. Diğer durumlarda işçi adayının açık rıza beyanını özgürce açıklayacağı koşulların sağlanması gerekmektedir. Bu yapılırken aydınlatma yükümlülüğü yerine getirilmeli ve özel nitelikli veri olan sağlık verisinin işlenmesi amaçla sınırlandırılmalıdır. Meşru amaç kapsamında sınırlı ve ölçülü işlenen bu tür kişisel veriler ilgili işçi adayının bilgisi olmadan üçüncü bir kişiye aktarılmamasına dikkat edilmelidir[1056]. Aksi durumda işverenin culpa in contrahendo sorumluluğu doğacağı gibi KVKK düzenlemeleri kapsamında idari ve TCK kapsamında cezai sorumluluğu doğabilecektir. Dahası KVKK m. 11/1-ğ düzenlemesi ve m. 14/3 fıkrası kapsamında kanuna aykırı olarak kişisel verileri işlenen işçi adayının ortaya çıkan zararını genel hükümlere göre (MK m. 25 ve TBK m. 58) isteme hakkının bulunduğunu da belirtmek gerekir[1057].

§ 7. DİJİTAL İZLEME YÖNTEMLERİNİN HUKUKEN DEĞERLENDİRİLMESİ

İş ilişkisinde kullanılan belli başlı dijital izleme uygulamalarının iş sözleşmesinin tarafları açısından ortaya çıkarmış olduğu sorunlar, çeşitli sistemler üzerindeki görünümleri ve yüksek yargının dijital izleme ihtilaflarına ilişkin vermiş olduğu kararlarda belirlediği ölçütler bu başlıkta ele alınacaktır.

1055) § 6. II. 4. i.
1056) EU, [2018], Handbook, s. 334; Avrupa Konseyi Bakanlar Komitesi'nin, CM/Rec.2015 Tavsiye Kararı'nın m. 3. https://rm.coe.int/cmrec-2015-5-on-the-processing-of-personal-data-in-the-context-of-empl/1680a43b68 (Erişim Tarihi: 01.11.2022).
1057) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 358.

I. İşçilerin İşyerine Giriş Sistemleri Vasıtasıyla İzlenmesi

İşverenler işyerine giriş ve çıkış saatlerini kontrol etmek, işçilerin işyerindeki izlerini takip etmek, bir işçinin başkasının adına veri girişini veya puantaj kayıtlarını imzalamasını engellemek amacıyla gerek işyeri girişinde gerekse çalışma mahallinde çeşitli dijital izleme uygulaması kullanmaktadır. Anayasa Mahkemesi'nin işyeri giriş sistemleri vasıtasıyla gerçekleştirilen dijital izlemeye ilişkin kararlarında[1058] ifade edildiği üzere; uygulamanın hukuki dayanağı, ölçülülüğü, izlemenin türü ve boyutuna ilişkin işçilerin bilgilendirilip bilgilendirilmediği veya özel nitelikli kişisel veriler için açık rızaya bağlı bir veri işleme söz konusu ise bu koşulun yerine getirilip getirilmediği gerçekleştirilen izlemenin hukuka uygunluğunu[1059] nitelendirmede önemli unsurlardır.

1. İşyeri Girişlerini İzleyen Dijital İzleme Uygulamaları

İşverenin işyerine giriş ve çıkışları takip etmede, işçilerin işe mesai saatlerinde geldiklerini ve mesai saatlerine uyarak işten ayrıldıklarını tespit etmede, işyerine yabancıların girişini engelleyerek işyeri güvenliğini sağlamada ve mülkiyeti korumada ekonomik menfaatleri ile iş sözleşmesinden doğan diğer menfaatleri bulunmaktadır[1060]. İşveren bu menfaatlerini korumak için işçinin kişilik hakları üzerinde en az müdahaleci sonuçlar ortaya çıkaracak bir yöntemle işyeri girişlerini denetleyebilir. Örneğin işyerine giriş ve çıkışlar ile işçinin işyerindeki hareketlerini kimlik bazlı giriş kartları ile denetlemek mümkünken bunun retina taraması veya diğer biyometrik veri esaslı özel nitelikli kişisel verilerle gerçekleştirmek işçinin kişisel verileri ve özel hayatı üzerinde müdahaleci sonuçlar ortaya çıkarır[1061].

1058) AYM Genel Kurul Kararı, Ramazan Şahin kararı, Başvuru Numarası: 2018/11988, Karar Tarihi 10.03.2022, Resmi Gazete 19 Nisan 2022, Sayı 31814.
1059) Hukuka uygunluk ölçütleri için bkz. § 6.
1060) Okur, [2013], Elektronik Gözetleme, s. 111.
1061) AYM Genel Kurul Kararı, Ramazan Şahin kararı, § 50-53.

a) Kimlik Bazlı Giriş Kartları

İşyerine girişte kullanılan kimlik bazlı giriş sistemleri işçiye özel atanan "personel tanıma numarası" (PIN) veya manyetik ve çipli kart sistemi esasına dayanan dijital izleme uygulamalarından oluşmaktadır. Bu sistemler işyerine girişte bulunan turnike sistemine bir şifrenin girilmesi veya benzer sistemle çalışan işçinin kimlik bilgileri esas alınarak tanıtılmış bir kartın sisteme okutulması suretiyle uygulanmaktadır. İşçi işyerine giriş yaparken bu sistemler turnikede bulunan entegre sistem tarafından kayıt edilmekte ve veri tabanında giriş saati ve kimlik bilgileri esaslı bir kayıt oluşturmaktadır. İşçinin işyerinden çıkması durumunda yine aynı sistem çalışmakta ve işçinin çıkış saati ve tarihi sistemde işlenmektedir[1062].

b) Biyometrik Veri Esaslı Giriş Sistemleri

İşyerine girişi sağlamak için retina veya parmak izi okuyucularının kullanılması özel nitelikli kişisel veri olan biyometrik verilerin işlenmesini, RFID etiketine işlenmiş işçiye ilişkin biyometrik verilerin giriş kartına entegre edilmesi kişisel veri ve özel nitelikli kişisel veri işlemesini gerektirir. Günümüzde işverenler işçilerinin biyometrik veya genetik verileri olan genetik haritalama, retina tarama ve mikroçipleme gibi yöntemler kullanarak dijital izleme gerçekleştirebilmektedir. Bu izleme yöntemlerinin bazıları yeni olsa da teknolojik gelişmelere bağlı olarak bu uygulamaların iş ilişkisinde yaygınlaşacağını öngörmek güç değildir[1063]. Teknoloji bu hızda gelişirken bu uygulamalara karşı işçinin özel hayatını ve kişisel verilerini koruyan yasal düzenlemeler ve yeni koruyucu yöntemler üzerinde düşünülmesi gerekmektedir[1064].

Kişisel veri koruma mevzuatımızda biyometrik veri özel nitelikli kişisel veri

1062) Okur, [2013], Elektronik Gözetleme, s. 112.
1063) Secunda, [2019], Right to Disconnect, s. 8.
1064) Bkz. § 9.

olarak düzenlenmiş (KVKK m. 6/1), fakat bu kavramlarla ilgili kapsayıcı bir tanım yapılmamıştır. Kişisel verilerin korunması açısından önemli yeni düzenlemeler getiren GVKT'nin 4. maddesinde biyometrik veri: "yüz görüntüleri veya daktiloskopi veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir" biçiminde tanımlamıştır[1065].

Tanımdan hareketle bir kişisel verinin biyometrik veri olarak nitelendirilebilmesi için veri işleme sonucunda kişinin fiziksel, fizyolojik veya davranışsal farklılıkları ve özellikleri ortaya çıkarılmış olmalı ve ortaya çıkarılan bu özellikler kişisel verileri işlenen kişinin kimliğini belirli veya belirlenebilir hale getiren kişisel veriler olması gerekmektedir[1066]. GVKT'da yer alan tanımdan ortaya çıktığı üzere biyometri kavramı ile insana ait fizyolojik ve davranışsal özgünlükler ifade edilmektedir. Biyometrik veri bu anlamda kişiye özgüdür, tektir ve benzersizdir. Bunların fizyolojik olanlarına kişinin parmak izi, retinası, avuç içi örnek gösterilebilirken; davranışsal olanları kişinin araç kullanma şekli, yürüyüş tarzı, klavyeye vuruş biçimi örnek gösterilebilir[1067].

İş ilişkisinde özel nitelikli kişisel veri olan biyometrik verilerin kullanımı yalnızca belirli durumlarda, işlenme amaçlarının meşru temele dayanması dikkate alınarak ve işyerindeki faaliyetin niteliği göz önünde bulundurularak "hassas alanlara" erişimi güvence altına almak için gerekçelendirilebilir. Örneğin, tehlikeli üretim süreçlerini veya işyerinde çeşitli sırların bulunduğu alanları veya belirli binaların, malların, gizli ya da saklı belgelerin veya değerli nesnelerin korunmasına

1065) KVK Kurulu, K. 2020/167, T. 27.2.2020 tarihli kararı; Anayasa Mahkemesi GK, E. 2014/180 K. 2015/30 T. 19.3.2015; İstanbul BİM, 3. İDD, E. 2017/1689 K. 2018/62 T. 18.1.2018.
1066) KVK Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, s. 4-5. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf (Erişim 24.4.2022).
1067) AYM Genel Kurul Kararı, Ramazan Şahin kararı, § 50-53; Danıştay 15. Dairesinin 2014/4562 Esas sayılı kararı, https://www.istabip.org.tr/icerik/biyometrikyurutmeyidurdurma.pdf (Erişim Tarihi: 24.4.2022).

yönelik biyometrik veri temelli giriş ve koruma sistemi oluşturulabilir[1068]. Bu örnekten hareketle dikkat edilmesi gereken asıl husus, gerçekleştirilecek biyometrik izlemenin meşru amaç kapsamında sınırlı ve ölçülü olması gerektiğidir. Önemle eklemek gerekir ki, işyerindeki bir faaliyetin biyometrik veri işlemeksizin gerçekleştirilmesi mümkünse bu durumda özel nitelikli veri olan biyometrik verilerin işlenmemesi gerekir. Zira, KVKK m. 6/1'de tahdidi olarak sayılan özel nitelikli kişisel verilerden birisi olan biyometrik veriler ya işçinin açık rızası kapsamında ya da kanunlarda öngörülmesi halinde (KVKK m. 6/3) açık rıza alınmaksızın ve fakat aydınlatma yükümlülüğü yerine getirilerek işlenebilir[1069].

2. Kişisel Veri Koruma Hukukunda Doğan İşveren Yükümlülükleri

İşveren işyeri giriş sistemleri kapsamında dijital izleme gerçekleştirirken öncelikli olarak KVKK m. 4'te düzenlenen genel ilkeleri dikkate almalı ve m. 5'teki veri işleme şartlarından birisine dayanarak kişisel veri işlemelidir. Ayrıca her durumda, KVKK m. 10 ve Tebliğ m. 4 ve 5'te öngörülen usul ve esaslar kapsamında aydınlatma yükümlülüğü yerine getirmelidir. İncelendiği üzere iş ilişkisi temelde iş sözleşmesine dayandığından ve KVKK m. 5/2-c bendinde bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olma açık rıza dışındaki hukuka uygunluk sebebi olarak düzenlendiğinden aydınlatama yükümlülüğü yerine getirilerek işyerine giriş sistemleri vasıtasıyla dijital izleme gerçekleştirilebilir.

Biyometrik verileri işleyen teknoloji, bir kişiyi tanımlamak için parmak izi, retina, avuç içi, kalp atış ritmi, damar dokusu veya ses gibi bireyin benzersiz fiziksel özelliklerini kullanır. Biyometrik izleme çoğu durumda fizyolojik veya davranışsal verinin taranması, dijital forma indirgenmesi ve karşılaştırma gerçekleştirebilme amacıyla kullanılabilecek şekilde bir sistemde saklanması sürecini içerir. Kişi

1068) Andrea Sitzia/Enrico Barraco, "Protection of Privacy in Labor Relations: The Italian Case within the European Dimension", Comparative Labor Law & Policy Journal, Vol. 31, No. 4, Summer [2010], s. 737.
1069) İşyerine biyometrik verilerle giriş yapılmasını isteyen işverene ilişkin AYM kararı için bkz. AYM Genel Kurul Kararı, Ramazan Şahin kararı, § 51.

tanımlanmış biyometrik teknoloji ile korunan yere veya sisteme erişmek istediğinde, fiziksel özellik tekrar taranır ve yeni tarama, saklanan örnekle karşılaştırılır. İkisi önceden belirlenmiş bir eşik dahilinde eşleşirse, bireye erişim izni verilir.

Bankacılık sistemlerinde[1070], 11 Eylül ABD saldırıları sonrası güvenlik ve istihbarat alanında[1071] yoğun olarak kullanılan biyometrik veriler iş ilişkisinde işçilerin çalışma saatlerini denetlemek işyerine giriş çıkışlarda veya sınırlandırılmış alanlara girişler için kapı kilitlerinde ve bilgisayar ve telefon sistemlerinde güvenlik amacıyla kullanılmaktadır. Bunun yapılması özel nitelikli kişisel verilerin işlenmesini gerektireceğinden bu veriler ancak KVKK m. 6/2 ve m. 6/3'teki işleme şartlarından olan açık rıza veya kanunlarda açıkça öngörülme veri kapsamında işlenebilir. Ayrıca işçinin temel hak ve özgürlükleri dikkate alınarak işverenin amacını gerçekleştirecek ve kişisel veriler ve özle hayat üzerinde daha az müdahaleci etkiler ortaya çıkaracak bir yöntemin olup olmadığına yönelik bir araştırma yapması, dijital izlemenin ve izlemede elde edilen verinin hukuka uygunluk değerlendirmesi açısından önemlidir.

Dahası biyometrik veri temelli izlemenin işyeriyle sınırlı kalmadığı, akıllı saat veya akıllı telefon gibi pek çok farklı yapay zeka temelli cihazla veri toplandığı örnekler iş ilişkisinde artmaktadır. Ayrıca bu sistemler internet üzerinden birbirine bağlı olduğundan işverenler, işyerindeki işçiyle ilgili veri toplayan (örneğin Fitbit) veya sosyal medya gönderilerinin ötesinde işçinin sağlık verileri, günlük rutinleri ve yaşam aktiviteleri dahil birçok katmanda yer alan veriyi işleyebilme olanağını elde etmiştir. Örneğin bir akıllı telefon GPS'inden alınan sürüş verileri, bir akıllı saatten alınan egzersiz, etkinlik ve kalp ritim verileri kişilik ve alışkanlıklarla ilgili çıkarımlara olanak verdiğinden, işçinin elektrik kullanımı, gece ne kadar geç

1070) Catherine Jasserand, "Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data", European Data Protection Law Review (EDPL), Vol. 2, No. 3, [2016], s. 298.
1071) Margaret Hu, "Biometric ID Cybersurveillance", Indiana Law Journal, Vol. 88, No. 4, Fall, [2013], s. 1478.

uyuduğu gibi yaşam tarzı özelliklerini ortaya çıkarabilir. Yine akıllı telefonlarda gerçekleştirilecek dijital izleme vasıtasıyla konuşmalarda geçen belirli kalıptaki kelimelerle işçinin genel durumu hakkında ve konuşma kalıplarındaki değişimlerden ruhsal durumuyla ilgili veriler dahi ortaya çıkarabilmektedir[1072].

Biyometrik verilerle işçileri izleme AİHM ve AYM kararlarına konu edilmektedir. Örneğin bir belediye kamu kuruluşunda çalışan Ramazan Şahin isimli memur, parmak izi biyometrik verisiyle kurumda mesai saati takibi gerçekleştirilmesinin özel hayata saygı kapsamında bulunan kişisel verilerinin korunması hakkının ihlal ettiği iddiasıyla Anayasa Mahkemesine bireysel başvuruda bulunmuştur. AYM, Ramazan Şahin kararında parmak izinin her kişide farklı olduğunu, bu verinin kişinin biyolojik olarak belirlenmesine imkan verdiğini, KVKK m. 6/1 gereği olarak biyometrik verilerin özel nitelikli kişisel veri olduğunu, özel nitelikli kişisel verilerin önemine binaen kanun koyucu tarafından daha katı işleme koşullarının öngörüldüğünü, özel nitelikli kişisel verilerin ise ancak kişinin açık rızası alınarak işlenebileceğini, bunun tek istisnasının kanunlarda açıkça öngörülmesi olduğunu, konu ile ilgili AİHM, Danıştay İdari Dava Daireleri kararı ile KVK Kurul kararlarına da değinerek mesai saatlerinin parmak izi ile takip edilmesinin ölçülülük ilkesine aykırı olduğunu tespit etmiştir. Ayrıca kararda işyeri giriş ve çıkışının biyometrik veriyle takip edilmesinin kanuni bir dayanağının da bulunmadığı tespit edilerek, gerçekleştirilen uygulama ile kamu işçisinin özel hayata saygı hakkı kapsamında bulunan kişisel verilerinin korunması hakkının ihlal edildiğine karar vermiştir[1073].

II. İşyerinde Kamera İzlemesi

İşyerinde kamera izlemesi ve seslerin kaydedilmesi işçilerin teknoloji

1072) Robert Sprague, "Survey of (Mostly Outdated and Often Ineffective) Laws Affecting Work-Related Monitoring", 93 Chicago Kent L. Rev., [2018], s. 252.
1073) AYM Genel Kurul, Ramazan Şahin kararı, Başvuru Numarası: 2018/11988, Karar Tarihi 10.03.2022, Resmi Gazete 19 Nisan 2022, Sayı 31814.

destekli araçlarla izlenmesinin en eski biçimlerindedir. Bu başlıkta aydınlatma yükümlülüğü bulunan kameralarla kişisel veri işleme faaliyeti, gizli kamera gözetlemesinin hukuka uygunluk ölçütleri ve yüksek mahkeme kararlarına konu olmuş kamera gözetlemesi örnek olayları analiz edilecektir.

1. İşverenin Kamera İzlemesindeki Menfaatleri

Kamera izlemesinden ne anlaşılması gerektiğine ilişkin hukukumuzda tanımlayıcı bir düzenleme mevcut değildir. İş hukuku açısından kamera gözetlemesi işyeri güvenliğini sağlamak ve işçinin işyerindeki çalışmasının denetlemek amacıyla görüntü ve bilgilerin her türlü teknolojik araçlarla elde edilmesi ve kaydedilmesi sürecidir[1074]. Kamera izlemesi özellikle 90'larda yapılan kimi araştırmalarda şirketlerin varlıklarını korumada etkili olduğu, üretkenliği artırdığı ve işyerinde sağlık ve güvenliği koruduğu yönünde yapılan araştırmalar[1075] işyerinde CCTV vasıtasıyla izlemede ciddi bir patlama yaşatmıştır[1076]. Günümüzde kamera teknolojisindeki gelişmeler sayesinde tespit edilmesi dahi zor küçüklükteki dijital ve hareketlere duyarlı kameralarla net, uzun süreli ve otomatik görüntü kaydetmek mümkündür.

Gelişen kamera teknolojilerine entegre yazılımlar işçilerin iş görme borçlarını ifa ederken dikkatlerini ve işe ayırdığı zamanı ölçebilmektedir. Web kamera veya işyerinde bulunan CCTV kameraları kişinin hareketlerine göre izleme ve odaklanma gerçekleştirebilirken, bazı işverenler işçilerin dikkatini izlemek için web kameralarından faydalanmaktadır. Kameraya veya web kamerasına yüklenen yazılımlar göz hareketleri, vücut hareketleri ve yüz ifadeleri gibi biyometrik verileri kullanarak, işçilerin verilen görevlere dikkat edip etmediği, müşterilerine hangi nitelikte cevap verdiği, verimlilik ve işe odaklanma düzeyini denetleyebilmektedir.

1074) Okur, [2013], Elektronik Gözetleme, s. 119.
1075) Topo/Orsola, [2018], Employer's Power, s. 391.
1076) Beck/Willis, [2005], Crime At Work, s. 193-195; McCahill/Norris, [1999], Watching the Workers, s. 208 vd.; Ciocchetti, [2001], Monitoring Employee, s. 3.

Bu itibarla işverenler; işyeri güvenliğinin sağlanması, işyerindeki mülkiyete konu hakların korunması, suçun önlenmesi, işçilerin tehlikelerden uzak tutulması, ruhsal ve bedensel sağlıklarının korunması, iş görme borcunun işyeri prosedürlerine ve iş sağlığı ve güvenliği yönetmeliklerine uygun iş yapılması hususlarını denetlemek gibi meşru menfaatler kapsamında kamera izlemesi gerçekleştirebilmektedirler.

2. Kamera İzlemesinin Sınırları

İşyeri güvenliğinin sağlanması, verimlilik denetimi ve mülkiyetin korunması gibi menfaatler kapsamında kamera izlemesi gerçekleştirilmesi makul karşılanmaktadır. İşveren kamera izlemesini özel hayatın gizliliğini ve kişisel verilerin korunmasını gözetecek biçimde uygulamakla yükümlüdür. Ayrıca kameraların kullanımının amaçla bağlantı ve sınırlılık ilkesi[1077] gözetilerek konumlandırılması, kameraların bulunduğu yerlere gerekli işaretlerin (katmanlı aydınlatma) ve yazılı uyarıların bulunması zorunludur.

a) Bilgilendirmenin Bulunduğu Kameralarla İzleme

Kamera izlemesi işçinin kişilik haklarından birisi olan kendi görüntüsü üzerindeki haklarının ihlaline sebebiyet verir. Dahası kamera ile izlemede ses kaydı da işleniyorsa bu işçinin hakları üzerindeki ihlalin ağırlığını artırır[1078]. Bu itibarla, işverenin veri işleme faaliyetinin KVK hukukunun genel ilkelerinde düzenleme bulan hukuka ve dürüstlük kuralına uygun olması ve TCK m. 135'da düzenlenen

1077) 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin 5. maddesinin "c" bendinde: kişisel verilerin kaydedilme amaçlarına uygun ve yerinde olacağı ve aşırı olamayacağı düzenlemiş, 6698 sayılı Kişisel Verilerin Korunması Kanununun 4/2-ç bendinde: kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine uygun işleneceğini ve 2016/679 sayılı Avrupa Veri Koruma Tüzüğünün 5/1-b bendinde: kişisel verilerin "belirtilen, açık ve meşru amaçlara yönelik olarak toplanır ve bu amaçlara uygun olmayan bir şekilde işlenmeyeceği" düzenlenmiştir.
1078) Okur, [2013], Elektronik Gözetleme, s. 121.

kişisel verilerin hukuka aykırı kaydedilmesi suçunun oluşmaması için işçilerin KVKK m. 10 ve aydınlatma yükümlülüğüne ilişkin Tebliğ'in[1079] m. 4 ve 5 düzenlemeleri kapsamında aydınlatılması gerekmektedir. Kameralara ilişkin aydınlatmada kameranın bulunduğu yerlere katmanlı aydınlatma niteliğindeki işaretler ve kısa metinlerle (kamera görseli veya bu işyerinde 7/24 kamera ile izlenmektedir gibi) gerçekleştirilebilir. Katmanlı aydınlatma sonrasında, işçinin tam olarak bilgilendirilmesi için izlemenin amacı, kapsamı, işlenen veriler, verileri işlenen işçinin hakları, haklarını kullanma yöntemleri ve işlenen verilerin saklanma süreleri hususunda bilgilerin bulunduğu bir metne yönlendirilerek tam olarak bilgilendirilmesi gerekir[1080].

Tebliğde öngörülen düzenlemeye uygun aydınlatma yükümlülüğünün yerine getirilmemesi gerçekleştirilen izlemeyi gizli izleme, başka bir ifadeyle hukuka aykırı izlemeye dönüştürebilir. Önemle eklemek gerekir ki, eğer kamera gözetlemesi özel nitelikli kişisel veri olan sağlık verisi ve cinsel yaşam verisi işleniyorsa ayrıca işçinin açık rızasının alınması gerekmektedir. Örneğin, işyeri mescidinde gerçekleştirilen bir kamera kaydını işveren, işçilik ihtilafının bulunduğu bir davaya delil olarak sunmuştur. Mescitte gerçekleştirilen kamera izlemesinde elde edilen özel nitelikli kişisel verisi mahkemeye bu şekilde delil olarak sunulan işçi bunu, KVK Kurumu nezdinde şikayete konu etmiştir. KVK Kurulu, güç dengesizliğinin bulunduğu durumlarda açık rızanın özgür iradeyle verilmesinin güç olduğunu, işçiye rıza göstermemeye yönelik etkin bir imkanın sunulmadığı durumlarda açık rızanın bulunduğundan bahsedilmeyeceğini tespit etmiştir. Ayrıca Kurul, işverenin mescitte gerçekleştirmiş olduğu kamera izlemesini genel ilkelere aykırı bulduğunu; "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerine uygun olması gerektiği, çalışanların; soyunma odaları, tuvaletler,

1079) KVK Kurumu tarafından yayımlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" 10 Mart 2018 tarih ve 30356 sayılı Resmi Gazete'de yayımlandı.

1080) Katmanlı aydınlatma ve aydınlatma yükümlülüğü için bkz. KVK Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, KVK Kurumu Yayınları, Ankara, [2019], s. 14, 19; WP 29, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, s. 25; Gürsel, [2016], İşçinin Kişisel Verileri, s. 376.

duşlar, mescit, dinlenme odaları ve emzirme odaları bakımından makul bir mahremiyet beklentisinde olduğu dikkate alındığında veri sorumlusu tarafından söz konusu alanlarda veri işleme faaliyeti gerçekleştirilmesinin çalışanların mahremiyet beklentilerini zedeler nitelikte ve özel alanlarının işgali niteliğinde sayılabileceği" biçiminde tespit etmiştir[1081]. Gerçekte işverenin izleme hakkının soyunma odaları, duşlar, dinlenme odaları ve dini amaçlarla ayrılmış yerlerde sınırlı olduğunu belirtmek gerekir. Ayrıca bu yerlerde gerçekleştirilecek izleme uygulamalarının, KVKK'nın genel ilkeleri denetimine tabi tutulması gerekir.

Kamera izlemesinde dikkate alınması gereken diğer bir husus da izlemenin işyeri giriş yerlerinde, genel çalışma alanlarında, işyerinde güvenlik riski bulunan alanlarında, iş sağlığı ve güvenliği prosedürlerine uygun iş yapılıp yapılmadığını denetlemede, tehlikeli sınıfta faaliyet gösteren işyerlerinde tehlikenin önlenmesinde, işçinin beden ve ruhsal bütünlüğünü korumda, üretim yerlerinin denetlenmesinde kullanılabileceğidir. Kamera izlemesi meşru amaç kapsamında ölçülü uygulanmalı ve işçinin kişisel verileri üzerinde en az müdahale gerçekleştirecek yöntemle gerçekleştirilmelidir[1082]. Başka bir söylemle kamera ve ses kaydı izleme sistemleriyle devamlı kayıt alınması çalışma alanlarında en son

1081) KVK Kurulu, söz konusu kararda veri sorumlusu işverene: "Veri sorumlusu tarafından mescitte kamera vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetine ilişkin ilgili kişinin açık rızasını özgür irade ile vermediği ve işten çıkarılma korkusu ile geriye dönük olarak kişisel verilerin işlenmesiyle ilgili diğer belgeleri de rızası olmadan imzalamak zorunda bırakıldığı kanaatine varıldığından Kanun'un 6'ncı maddesi kapsamında herhangi bir veri işleme şartına dayanılmaksızın veri işleme faaliyetinin gerçekleştirildiği, diğer taraftan açık rıza alınsa dahi söz konusu veri işleme faaliyetinin Kanun'un 4'üncü maddesinde yer alan genel ilkelerden "işlendikleri amaçla bağlı, sınırlı ve ölçülü olma" ilkesine aykırılık teşkil edeceği sonucuna varılmakta olup, bu hususların Kanun'un 12'nci maddesinin (1) numaralı fıkrasında yer verilen "Veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önlemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmüne aykırılık teşkil etmesi nedeniyle Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca veri sorumlusu hakkında 300.000 TL idari para cezası uygulanmasına, şikâyete konu kişisel veri işleme faaliyetinin Kanun'un 15'inci maddesinin (7) numaralı fıkrası kapsamında ivedilikle durdurulması ve sonucundan Kurula bilgi verilmesi yönünde veri sorumlusunun talimatlandırılmasına…" biçiminde gerekçesiyle idari yaptırım uygulanmasına karar vermiştir. KVK Kurulu, 10/08/2023 Tarihli ve 2023/1356 Sayılı Karar Özeti, "Bir işveren tarafından işe iade davasına, ilgili kişinin mescitte ibadet etme görüntülerinin ibraz edilmesi" hakkında karar için Bkz. https://kvkk.gov.tr/Icerik/7779/2023-1356 (Erişim Tarihi: 06.01.2024).

1082) Alpagut, [2019], Kamera Gözetlemesi, s. 295; Okur, [2013], Elektronik Gözetleme, s. 131.

başvurulacak yöntem olmalıdır[1083]. Örneğin üretim bandında güvenliği, bir acil durum sinyali gönderen düğme ile çözmek mümkünken işçilerin hareket noktalarının tamamının izlenmesi ve kayıt altına alınması onların özel hayatlarına saygı hakları ile kişisel verileri üzerinde orantısız bir müdahale ortaya çıkarabilir.

Kural olarak işçilerin dinlenme yerlerinin, giyinme yerlerinin, tuvaletlerin, duş yerlerinin izlenmesi işçinin kişilik hakları üzerinde ağır ihlaller ortaya çıkaracağından hukuka aykırıdır. Bu gibi alanlar ancak mahkeme kararının varlığı halinde suçun önlenmesi amacıyla izlenebilir[1084]. Eklemek gerekir ki, hukuka uygunluk ölçütlerini taşıyan kamera gözetlemesi gerçekleştirilmesi, izlemede elde edilen verilerin iş sözleşmesinin üzerinde etki oluşturacak biçimde kullanılmasını işveren açısından olanaklı hale getirir[1085].

1083) AİHM Lopez Ribalda & Others v. İspanya kararı, § 111-112, § 116; İdare mahkemesine taşınan bir olayda TRT Genel Müdürlüğü, Ankara'da bulunan stüdyolarının reji bölümlerinde devamlı izleme olanağı veren kameralı izleme sistemi kurmuştur. Haber-Sen bu uygulamanın özel hayata orantısız bir müdahale oluşturduğu gerekçesiyle Ankara 14. İdare Mahkemesi'nin 2023/808 E. ve 2023/2538 K. sayılı dosyasında davaya konu etmiştir. TRT, kamera izlemesindeki amacın canlı yayın kazalarını önlemek olduğunu, 360 derece kayıt alınmadığını ve ses kaydının bulunmadığını, kamera kaydının yapıldığına dair uyarı levhalarının asıldığını savunarak davanın reddini istemiştir. İdare mahkemesi, incelemeye konu ettiğimiz AİHM ve AYM kararlarına da atıf yaparak; "Avrupa İnsan Hakları Mahkemesi kararları da dikkate alındığında hakların korunması başka şekilde sağlanamıyorsa kamera sistemlerinin çalışanların çalışma alanlarını görecek şekilde kurulmasının mümkün olduğu ancak bunun bir son çare olarak değerlendirildiği ve bu düzenlemenin içeriğini ayrıntılı olarak ortaya koyan özel bir düzenleyici işlem olması gerektiği, kamera sistemlerinin çalışma alanlarını çekmesinin özel hayatın gizliliğini ihlal ettiği, sınırlı bir izleme sağlayacak şekilde güvenlik amacıyla giriş ve çıkışları izlemek üzere veya vatandaşlara da açık olan ortak alanlar ve iş sahiplerinin de giriş çıkışına açık, yoğun bir alış veriş trafiği olan alanlarda kurulabileceği ancak bu kameraların da çalışanların iş yapış şekillerini denetlemek veya sürekli olarak belli kişileri çekecek şekilde kurulmaması gerektiği, dava konusu uyuşmazlıkta kameralı takip sistemi ile kurumca belirlenen amacın gerçekleştirilmesinde elverişli sınırlı ve ölçülü olmadığı sonucuna ulaşılmıştır" biçiminde karar vermiştir. Karar için bkz. https://habersen.org.tr/2016/wp-content/uploads/2024/01/TRT-KAMERA.pdf (Erişim Tarihi: 06.01.2024).

1084) Okur, [2013], Elektronik Gözetleme, s. 128.

1085) Yargıtay işverenin yönetim hakkı kapsamında işçiyi her zaman izleyebileceği yönünde karar vermekte ve fakat bunun yapılabilmesi için işçinin önceden izleme konusunda bilgilendirilmiş olmasını aramaktadır. Örneğin bu hususta Yargıtay 22. Hukuk Dairesi, E. 2017/21857 K. 2019/9884 T. 7.5.2019 kararında şu şekilde karar vermiştir: "İşçinin izlendiğine dair bilgilendirilmemesi veya gizlice izlenmesi, bu izleme neticesinde elde edilen veriler, iş sözleşmesinin işçi tarafından ihlal edildiğini açıkça ortaya koysa dahi, hukuka aykırı olarak kabul edilmelidir."

b) Suçun Önlenmesi Amacıyla Gizli Kamera Gözetlemesi

Genel ilkelere uygun ve orantılı olmak kaydıyla, KVKK m. 28/2'de suçun önlemesi amacıyla kişisel veri işlenmesi aydınlatma yükümlülüğünün istisnası olarak düzenlenmiştir. Böylelikle aydınlatma yükümlülüğünün istisnası olarak sınırlı bir hareket alanı bırakılmış olmakla birlikte istisnaların dar yorumlanması esastır. Aksi durumda gizli izlemeyle elde edilen veri hukuka aykırı elde edilmiş bulgu ve delil olarak nitelendirilecektir[1086]. İşverenin gizli kamera gözetlemesi gerçekleştirmesi AİHM kararlarında değerlendirmeye konu edilmiş ve olaylar işverenin mülkiyet hakkı, yönetim hakkı, suçun önlenmesi, ispat; işçinin özel hayatının gizliliği, ölçülülük, başkaca bir vasıtayla gerçekleştirilememe başlıklarında değerlendirmeye konu edilmiştir.

aa) Avrupa İnsan Hakları Mahkemesi Kararlarında İşverenin Gizli Kamera Gözetlemesi

Köpke & Almanya kararına konu olan olayda[1087], Almanya Feldberg'de bir süper markette kasiyer olarak çalışan Köpke'nin işvereni, Eylül 2002'de içecek bölümünde usulsüz işlemler gerçekleştirildiğini fark etmiş ve Köpke ile diğer bir işçinin hesaplarda usulsüzlükler gerçekleştirdiğinden şüphe etmiştir. Bunun üzerine işveren, 7 Ekim 2002 ile 19 Ekim 2002 tarihleri arasında bir dedektiflik bürosunun da yardımıyla içecek bölümünde gizli kamera gözetlemesi gerçekleştirmiştir. Gizli kameralar kasiyer, kasa ve kasanın arkasını izleyecek biçimde konumlandırılmıştır. Dedektiflik bürosu bu sürede edindiği verileri işverene iki nüsha olarak teslim etmiştir. 5 Kasım 2002'de Köpke'nin iş akdi izleme süresinde 100 Euro'yu

---

1086) Süha Tanrıver, Türk Medeni Usul Hukuku Bağlamında Hukuka Aykırı Yollardan Elde Edilen Delillerin Durumunun İrdelenmesi, TBB Dergisi, S. 65, [2006], s. 371; Sümeyye Hilal Üçüncü, "Medeni Usul Hukuku Çerçevesinde Kişisel Verilerin Korunması", Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması, (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, [2023], s. 492 vd.

1087) Bkz. AİHM, Köpke v. Almanya Kararı, (Appl. No. 420/07), Judgment of ECHR of 05 October, [2010].
https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=002-782&filename=002-782.pdf&TID=ihgdqbxnfi (Erişim Tarihi: 18.12.2022);

kıyafetine saklayarak hırsızlık yapmak ve içecek bölümündeki hesaplarda usulsüzlük gerçekleştirmek sebebiyle derhal feshedilmiştir.

14 Kasım 2002 tarihinde olay Neubrandenburg İş Mahkemesi'nde yargılamaya konu edilmiş ve mahkeme içecek ve kasada meydana gelen usulsüzlüklerin gizli izleme için yeterli sebep olduğunu, işverenin mülkiyet hakkına ciddi bir saldırının bulunduğu ve bu hakkın daha az müdahaleci bir yolla açığa çıkarmanın mümkün olmadığı ve çatışan haklar gözetildiğinde mülkiyet hakkını korumak için gizli kamera gözetlemesinin gerçekleştirilebileceğine karar vermiştir. Mahkemenin kararı 18 Mayıs 2004 tarihinde istinaf mahkemesince onanmış ve kamera gözetlemesinin Alman Federal Veri Koruma Yasası'nın 6-b bölümüyle uyumlu olduğunu, kasa arkasının kamusal bir alan olmadığından kameranın görünür kılınmasının zorunlu olmadığını, başvurucunun isnatları kabul etmesi halinde bu tür bir izlemenin gerekmeyeceğine kararda yer vermiştir. 14 Kasım 2004 tarihinde karar Federal İş Mahkemesi'ne taşınmış ve karar federal mahkemece onanmıştır. 31 Ocak 2005 tarihinde Federal Anayasa Mahkemesi'ne özel hayatının gizliliği ve adil yargılanma haklarının ihlal edildiği gerekçelerine dayanarak başvuruda bulunulmuştur. Anayasa Mahkemesi 28 Haziran 2006 tarihli kararı ile derece mahkemelerinin verdiği kararlarda hak ihlali yönünde bir bulgu bulunmadığı gerekçesiyle başvuruyu reddetmiştir.

Başvurucu bunun üzerine, özel hayatının gizliliğinin ve adil yargılanma hakkının ihlal edildiği gerekçesiyle Almanya aleyhine AİHM nezdinde başvuruda bulunmuştur. AİHM özel yaşamın kişinin adı, resmi gibi kişisel kimliğine ilişkin verileri ve mesleki (profesyonel) hayatı, ev yaşamı gibi hususları kapsayabileceğini, bir kişinin eylemlerinin fotografik sistemler kullanılarak devamlı kayıt altına alınması halinde özel hayatın ihlaline ilişkin sorunlar ortaya çıkarabileceğini tespit ederek, bu durumda AİHS m. 8 kapsamındaki korumaların gündeme gelebileceği değerlendirmesinde bulunmuştur. AİHM işçinin işyerinde özel hayata saygı hakkının gözetilmesi gerektiğini, bu hakkın mesleki faaliyetleri de kapsadığını vurgulayarak, gizli kamera ile izlemenin özel hayata aşırı bir müdahale

oluşturduğunu fakat bir suç şüphesinin bulunması durumunda mülkiyet hakkını koruma kapsamında sadece suçun tespiti için sınırlı süreli, belirli alanda ve sadece suçun faillerini kapsayan gizli izleme gerçekleştirilebileceğini; ayrıca böyle bir durumda işverenin mülkiyeti korumak için daha az müdahaleci bir yöntemi bulunmadığını tespit ederek, Köpke'nin özel hayatına saygı hakkının ihlal edilmediğine karar vermiştir[1088].

İş ilişkisinde gizli kamera gözetlemesi gerçekleştirilmesine ilişkin olan yakın tarihli bir diğer AİHM kararına konu olay Lopez Ribalda ve Diğerleri & İspanya kararıdır. 17 Ekim 2019 tarihli AİHM Büyük Daire kararına konu olan Lopez Ribalda ve Diğerleri & İspanya kararında, başvuruculardan üçü kasiyer, ikisi ise tezgah arkasında çalışan satış personellerinden oluşmaktadır. Şubat 2009'da marketin yöneticisi stok seviyesi ile satış arasında dengesizlik bulunduğunu tespit etmiştir. Devam eden aylarda da stok kaybı oluşması ve zarar edilmesi üzerine mağaza yöneticisi stok kaybı ve zararın sebebini tespit etmek için başlattığı iç inceleme çerçevesinde 15 Haziran 2009'da mağaza giriş ve çıkışını izleyecek görünür, kasa ve etrafını ve üç kasayı görecek biçimde gizli CCTV kameraları kurmuştur. Gerçekleştirilen bir toplantıda market çalışanları görünür kameralar ve kamera gözetlemesiyle ilgili bilgilendirilmiş, fakat gizli kameralardan bahsedilmemiştir. 25 ve 29 Haziran 2009'da elde edilen veriler kapsamında hırsızlık yaptığı şüphesi bulunan işçilerle görüşme gerçekleştirilmiştir. Beşi başvurucu olmak üzere on dört işçi işten çıkarılmıştır. Toplantıda işçilerin bir kısmı hırsızlık olayını kabul etmiştir. Başvurucunun, müşterilerin kasaya getirdiği malları önce kasadan geçirdiği, sonrasında işlemi iptal ettiği, müşterilerin alarak gittiği mallar ile satış fişleri arasındaki farkın bundan kaynaklandığı, stok kaybının ve zararın bu durumdan kaynaklandığı tespit edilmiştir. Kasiyerlerden başka dördüncü ve beşinci başvurucunun ise kasiyerlerin yardımıyla mal çaldıkları kameralarla tespit edildiği kendilerine bildirilmiştir. İşveren bu durumu sadakat borcuna ve

1088) Dilek Dulay Yangın, "Avrupa İnsan Hakları Mahkemesi Büyük Daire'nin İşçilerin Gizli Kamera ile İzlenmesine İlişkin 17 Ekim 2019 Tarihli Lopez Ribalda ve Diğerleri Kararı'nın Değerlendirilmesi", Çalışma ve Toplum, 2020/3, [2020], s. 1709 vd.

iyiniyet ilkelerine aykırı bulduğunu, iş ilişkisinde bulunması gereken bu niteliklerin ciddi biçimde ihlal edildiğini, bunun iş ilişkisinin derhal sona erdirilmesini haklı sebepleri olduğunu belirtmiştir. Üçüncü, dördüncü ve beşinci başvurular şirketin yasal temsilcisiyle bir sulh sözleşmesi imzalayarak gelecekte açılabilecek davalarda ortaya çıkabilecek belirsizliklerin ortadan kaldırılması ve iş akdinin işveren tarafından feshedildiği hususlarından anlaşmaya vardıklarını belirtmişlerdir. Bu başvurucular işten çıkarma kararında belirtildiği şekliyle hırsızlığı kabul etmiş, buna karşılık işveren de ceza davası açmamayı taahhüt etmiştir.

İlk başvurucu 22 Temmuz 2009 tarihinde Granollers İş Mahkemesi'nde dava açmış, aynı gün diğer dört başvurucu da benzer davaları açmışlardır. 20 Ocak 2010'da iş mahkemesi işten çıkarmaların haklı olduğunu karara bağlayarak tüm başvuruları reddetmiştir. Mahkeme kararında gizli kamera gözetlemesinin ölçülü olduğunu, ciddi suistimal şüphesinin bulunmasının bu izlemeyi haklı kıldığını, kayıtların şüpheli durumun kayıtları olduğunu, yer ve amaç açısından da sınırlı tutulduğunu bunun orantılı bir uygulama olduğunu tespit etmiştir. Mahkeme sulh sözleşmelerinin geçersizliğine ilişkin iddiaları ise zorlama veya hileye yönelik bir emarenin bulunmamasını göz önüne almıştır. Catalonia Yüksek Mahkemesi'ne gerçekleştirilen temyiz başvuruları mahkeme tarafından önceki emsal içtihatlar, anayasa mahkemesi kararları, çalışma tüzüğü ve KVK hukuku kapsamında incelemiş, veri koruma hukuku açısından önceden işçiden rıza alınmasına gerek olmamakla birlikte uygulamanın ölçülü olması gerektiğini, olayda suç şüphesinin varlığı karşısında gerçekleştirilen gizli izlemenin orantılı olduğunu, gereklilik ve uygunluğu aşacak biçimde uygulanmadığına, diğer durumlarda suçun ispatının zor olacağını tespit ederek temyiz başvurularını reddetmiştir. Başvuruculların Anayasa Mahkemesi'ne gerçekleştirdikleri başvuru da temel bir hakkın ihlalinin söz konusu olmadığı gerekçesiyle reddedilmiştir.

Başvurucular, özel hayatlarının gizliliğini ihlal eden gizli kamera gözetlemesiyle elde edilen kayıtlara dayanılarak iş sözleşmelerinin feshedildiğini, mahkemelerin feshin geçersiz olduğuna karar vermeyerek bu hakkı korumakta

yetersiz kaldığını ileri sürerek AİHS m. 8'de doğan özel hayata ilişkin haklarının ve AİHS m. 6'dan doğan adil yargılanma haklarının ihlal edildiğini iddia etmişlerdir. AİHM Üçüncü Daire, 9 Ocak 2018 tarihli kararında[1089] gizli kamera gözetlemesinin makul süreyle sınırlı tutulmasına rağmen kapsamının geniş olduğunu, kasada çalışan tüm işçilerin zaman bakımından sınırlandırılmaksızın, tüm saatlerde izlendiğini, ulusal mevzuata uygun izlemenin amacı ve veri işlemeye ilişkin bilgi verilmediğini, bu ilkeler dikkate alındığından izlemenin ölçülü olmadığından hareketle özel hayatın gizliliğinin ihlal edildiğine, AİHS m. 6 kapsamındaki adil yargılanma hakkının ihlal edilmediğine karar vermiştir. Dairenin bu kararı talep üzerine AİHM Büyük Daire'ye gönderilmiştir. Büyük Daire, 17 Ekim 2019 tarihli kararında kamera gözetlemesine ilişkin ölçülülük denetiminin esaslarını inceledikten sonra, olayı AİHS m. 8 kapsamında değerlendirerek işverenin yönetim hakkı ile işçilerin özel hayatlarının gizliliği hakkı arasındaki çatışmanın dengelenmesi için devlete yükümlülüklere yüklendiğini ifade etmiştir.

Büyük Daire[1090], işverenin işyerini sorunsuz çalışması için belirli tedbirler almada, işyerindeki kayıpları tespit etmede ve mülkiyeti korumada meşru menfaatleri bulunduğunu bunun için kayıpların sebeplerini araştırma, sorumluları bulma ve cezalandırmaya yönelik önlemler almaya hakkı bulunduğunu tespit etmiştir. Başvuruya konu olayda kameraların sadece kayıpların meydana geldiği ödeme alanlarını kapsadığını, izlemenin süresinin de hırsızlık şüphesini doğrulamak için gerekli olan süre kadar olduğu yönündeki yerel mahkeme tespitini yerinde bulmuş; ayrıca işçilerin iş görme borçlarını müşterilerin olduğu bir alanda ifa ettiklerini, işyerinin kamuya açık bir alan olduğuna işaret ederek, işyerinde özel hayatın korunması için makul beklenti bulunduğuna işaret etmiştir. Mahkemeye göre izleme ile elde edilen veri başkalarına açıklanmamış, yetkili sınırlı kişilerce incelenmiş, ayrıca izleme ile elde edilen veri suçun ispatı dışında bir amaçla

1089) Karar metini için bkz. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-179881%22]} (Erişim Tarihi: 25.11.2022).
1090) AİHM Büyük Daire Kararı için bkz. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-197098%22]} (Erişim Tarihi: 25.11.2022).

kullanılmamış ve suçun gerçekleştiği yer ve şekli dikkate alındığında ispat için başkaca araçlar bulunmadığını tespit etmiştir.

AİHM Büyük Daire'nin Lopez Ribalda ve Diğerleri & İspanya kararında, devletin AİHS m. 8 kapsamında işçilerin özel hayata saygı hakkı ile işverenin mülkiyete ilişkin hakları arasında adil bir denge kurulup kurulmadığı, bu hakların korunmasında tarafların çıkarları açısından gerçekleştirilen müdahalenin ölçülülüğü değerlendirmeye konu edilmiştir[1091]. AİHM, İspanyol Hükümeti'nin, kamera gözetlemesi gerçekleştirenin özel bir işletme olduğu bu itibarla olayda AİHS'deki yükümlülüklerle ilişkisi bulunmadığına ilişkin savunmasını[1092] değerlendirmiş ve AİHS m. 8'in temel olarak bireyi kamu otoritelerinin keyfi müdahalelerinden korumayı amaçladığını fakat bireyin özel hayatına ve aile hayatına etkin saygının sağlanması amacıyla pozitif borçların da bulunabileceğini, devletin bireylerin kendi aralarındaki ilişkilerde bile özel hayata saygının sağlamak için önlemler almakla yükümlü olduğunu tespit ederek bu savunmaya itibar etmemiştir[1093].

AİHM'in bu kararında gizli kamera gözetlemesinde dikkate alınacak hususları önceki kararlarına atıflar yaparak şu şekilde belirlemiştir: i) kamera gözetlemesinin kapsamı ve uygulama şekliyle ilgili işverenin işçileri bilgilendirip bilgilendirmediği; ii) gerçekleştirilen kamera gözetlemesinin işçilerin mahremiyetlerine müdahale derecesi, bunun için izlenecek alanın mahremiyet düzeyi, zaman ve mekan sınırlamaları ve izlenecek kişi sayısı; iii) işverenlerce izlemeyi haklı çıkarmak için meşru nedenler sunulup sunulmadığı ve bunun kapsamı, izleme ne kadar müdahalesi olursa bunun gerekçelerinin de o kadar güçlü olması gerekir; iv) işverenin amacını gerçekleştirmek için daha az müdahaleci yöntemler var olup olmadığı hususunun tespit edilmesi ve işverenin ulaşmak

1091) Alpagut, [2019], Kamera Gözetlemesi, s. 301; AİHM Lopez Ribalda & Others v. İspanya kararı için bkz. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-197098%22]} (Erişim Tarihi: 19.12.2022).
1092) AİHM Lopez Ribalda & Others v. İspanya kararı, § 109-110.
1093) AİHM Lopez Ribalda & Others v. İspanya kararı, § 111-112.

istediği amaca, işçilerin özel hayatına daha az müdahale yöntemi varsa bu yöntem tercih edilmelidir. Bu koşul her olayın özelliğine göre değerlendirilmelidir; v) izlemenin sonuçları hakkında bilgi verilmesi ve izlemede elde edilen verilerin nasıl kullanıldığı, amaca ulaşmak için kullanılıp kullanılmadığını; vi) izlemenin özellikle müdahaleci olduğu (gizli kamera gibi) durumlarda, işverenin işçilerin yeterince güvence sağlayıp sağlamadığına dikkat edilir. Bu tür önlemler, diğerlerinin yanı sıra, ilgili işçilere veya personel temsilcilerine izlemenin kurulumu ve kapsamı hakkında bilgi verilmesi, böyle bir önlemin bağımsız bir kuruluşa bildirilmesi veya şikayette bulunma olasılığı şeklinde olabilir[1094].

AİHM Büyük Daire bu temel esaslar kapsamında olayı kendi özelinde değerlendirerek olayda kamera kayıtlarından başka delillerin bulunması, olayın bir süpermarkette gerçekleşmesi, iç hukuk düzenlemeleri ve yargılama sürecindeki delillerin değerlendirmesinde mahkemelerin incelemelerini de dikkate alarak AİHS m. 6 kapsamında adil yargılanma hakkının ihlal edildiği iddiasını oybirliğiyle, AİHS m. 8 kapsamındaki özel hayatın gizliliğinin ihlal edildiği iddiasını ise oy çokluğuyla reddetmiştir[1095].

Antović ve Mirković & Montenegro Kararı'nda ise Montenegro Üniversitesi Matematik Fakültesi Dekanı'nın amfi tiyatrolarının kamera ile gözetlemesine ilişkin gerçekleştirdiği uygulamalar değerlendirmeye konu edilmiştir. AİHM kararında Veri Koruma Otoritesi'nin ve iç hukukta verilen kararlar da değerlendirilerek özel hayat kavramının geniş bir kavram olduğu ve tüketilecek şekilde bir tanımının gerçekleştirmenin zor olduğunu, kişinin meslek hayatındaki verilerin, kişisel verilerin de bu kapsamda değerlendirileceğini ve olaya AİHS m. 8 düzenlemesini uygulanabileceğini tespit etmiştir. Ayrıca kişisel verilerin işlenmeden önce kanuna uygun aydınlatma yükümlülüğünün yerine getirilmesi

1094) AİHM Lopez Ribalda & Others v. Spain kararı, § 116.
1095) AİHM Lopez Ribalda & Others v. Spain kararının tamamı için bkz. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-197098%22]} (Erişim Tarihi: 20.12.2022).

gerektiğine, bunların yapılmamış olması ve kamera gözetlemesi sebebiyle özel hayata müdahale bulunduğu gerekçesiyle ihlal kararı vermiştir[1096].

bb) Gizli Gözetlemenin Hukuki Değerlendirmesi

Genel olarak hukuk davaları açısından HMK m. 189/2'de öngörülmüş olan; "hukuka aykırı olarak elde edilmiş olan deliller, mahkeme tarafından bir vakıanın ispatında dikkate alınamaz" düzenlemesi kapsamında hukuka aykırı biçimde elde edilmiş veriler dikkate alınmayacaktır[1097]. Zira medeni yargılama hukuku açısından bir delilin hukuken dikkate alınabilmesi için bunun hukuka uygun olması gereklidir. Bu kapsamda gizli kamera gözetlemesinde elde edilen delilin kendisi değil delilin elde ediliş biçimi hukuka uygun olmadığından hukuken dikkate alınmaz[1098]. Aynı husus ceza hukuku açısından CMK m. 206/2-a bendinde, kanuna aykırı elde edilmiş delillerin ortaya konmasının reddedileceği[1099] biçiminde hüküm altına alındığından gizli kamera kayıtları ceza yargılamasında delil olarak dikkate alınmaz[1100]. İşçinin

---

1096) https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-11757%22]} (Erişim Tarihi: 18.12.2022).

1097) Fevzi Şahlanan, "İşyerinde İşverence Sağlanan Bilgisayarı İşle İlgisi Olmayacak Şekilde Kullanma – Haklı Fesih (Karar İncelemesi), Tekstil İşveren Dergisi, S. 383, [2012], s. 2-6.

1098) Üçüncü, [2023], Medeni Usul Hukuku Çerçevesinde Kişisel Veri, s. 493.

1099) Ali Kemal Yıldız, Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi, Yayımlanmamış Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, [2002], s. 182 vd.; Erdener Yurtcan, "Yargıtay Kararlarının Işığında Hukuka Aykırı Delillere Dayanma Yasağı", Prof. Dr. Nurullah Kunter'e Armağan, İstanbul, [1998], s. 436.

1100) Yargıtay 22. HD., E. 2020/1482 K. 2020/5244 T. 1.6.2020 tarihli kararında gizli ses kaydına dayanılarak gerçekleştirilen feshin hukuka aykırı delile dayanıldığını şu şekilde değerlendirmiştir: "Akaryakıt konusunda faaliyet gösteren işyerinde işçilerin ses kayıtlarının alınmasını gerektiren haklı bir menfaatin varlığı da ortaya konulmadığına göre kişilik haklarına ve hukuka aykırı olarak elde edilen ses kayıtlarının delil olarak değerlendirilmesi mümkün değildir. Bu bağlamda, işçinin aleni bir şekilde işverene yöneltmek kastıyla kanunda düzenlenen şekilde işçinin işverene veya ailesine karşı şeref ve namusuna dokunacak sözler söylemesi eylemini gerçekleştirdiğinin kabul edilmesi dosya kapsamına uygun düşmemiştir. Bu nedenle mahkemece davacının kıdem ve ihbar tazminatı alacaklarının kabulüne karar verilmesi gerekirken yazılı şekilde karar verilmesi hatalı olup, bozmayı gerektirmiştir."
Yargıtay 4. CD., E. 2007/11957 K. 2009/21077 T. 22.12.2009 kararında hukuka aykırı delilleri özel hayatın gizliliği ve haberleşmenin gizliliği kapsamında şu şekilde değerlendirmiştir: "Kişilerin özel yaşamlarının ve haberleşmenin gizliliği ilkelerinin 20, 22. maddelerinde güvence altına alındığı Anayasa'nın 38/6. maddesinde, kanuna aykırı olarak elde edilen bulguların delil olarak kabul edilemeyeceği ifade edilmiş, tarafı olduğumuz Avrupa İnsan Hakları Sözleşmesi (İHAS)'nin 8. maddesinde özel yaşamın gizliliği korunmuş, 6. maddesinde ise adil yargılanma hakkı düzenlenmiş ve Avrupa İnsan Hakları Mahkemesi'nin içtihatlarında, özel yaşamın gizliliği ilkesine aykırı olarak elde edilen hukuka aykırı delillerin İHAS hükümlerine aykırılık teşkil edeceği kabul edilmiştir (bkz.

gizli kameralarla izlenmesi, internet trafiğinin, e-postalarının izlenmesi ve kayıt altına alınmasının gizli biçimde gerçekleştirilmesi halinde yine hukuka aykırı delil nitelendirmesi yapılabilir.

İşçinin özel hayatının gizliliği ve kişisel verileri üzerinde aşırı müdahaleci sonuçlar ortaya çıkardığından KVK hukuku ancak suçun önlenmesi amacının varlığı halinde gizli kamera gözetlemesine izin vermektedir (KVKK m. 28/2-a). İşverenlerin suçun önlenmesi amacıyla daha az müdahaleci bir yöntemin bulunmadığı durumlarda belirli, sınırlı ve ölçülü, belirli süreye dayanan ve bir gizli izleme gerçekleştirmeleri hukuka uygun kabul edilebilecekken bu koşulların bulunmaması halinde gerçekleştirilen gizli izleme hukuka aykırı olacaktır[1101].

---

6. madde yönünden 12.07.1988 tarihli Shenk-İsviçre kararı, prg. 30-48; Dr. Sibel İnceoğiu, Adil Yargılanma Hakkı, 3.B. 2008, s. 291; 8. madde yönünden 26.04.1985 tarihli Malone-İnglltere ve 24.04.1990 tarihli Fransa-Krusiin/Huoin kararı vd.; Durmuş Tezcan/Erdem Sancaktar, Türkiye'nin İnsan Hakları Sorunu, 2004, s. 38). S11\sayılı CYY'nin 206/2-a ve 217/2. maddelerinde ise yasa ve hukuka aykırı delillerin hükme esas alınamayacağı açıklanmıştır. 1412 sayılı CYY'nin 18.11.1992 tarihli ve 3842 sayılı Yasa ile değişik 254/2. maddesinde de soruşturma ve kovuşturma organlarının hukuka aykırı şekilde elde ettikleri delillerin hükme esas alınamayacağı belirtilmiştir."; Yargıtay CGK., E. 2009/160 K. 2009/264 T. 17.11.2009.

1101) Karara konu olayda sayaç okuyucusu işçinin iş akdi belediye alt işvereni tarafından hırsızlık, güveni kötüye kullanmak ve işverenin meslek sırlarını ortaya atmak gibi sebeplerle haklı nedenle SGK Kod 46 kapsamında feshedilmiştir. İşveren fesihte işçinin mağdur ile gerçekleştirdiği telefon kaydının mağdur tarafından kayıt altına alınması deliline dayanmıştır. İşçi işe iade davası açmış ayrıca KVK Kurumu'na verilerinin usulsüz işlendiği şikayetinde bulunmuştur. KVK Kurulu kararında HMK m. 189 kapsamında hukuka aykırı elde edilen delillerin, delil mahiyetinde olmayacağını, ayrıca TCK açısından bunun suç olduğunu tespitleri yapılarak, işçinin başvurusunu "Yargıtay CGK'nın 01/12/2020 tarihli ve 2020/485 sayılı Kararında da; 'Kişinin kendisine karşı işlenmekte olan bir suçla ilgili olarak, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkânının olmadığı ani gelişen durumlarda karşı tarafla yaptığı konuşmaları kayda alması halinin hukuka uygun olduğunun kabulü zorunludur. Aksi takdirde kanıtların kaybolması ve bir daha elde edilememesi söz konusudur.' değerlendirmesine yer verildiği, İşçi işveren uyuşmazlıklarında; işverenin iş sözleşmesini haklı nedenle feshettiğini başka türlü delil ile ispat etme imkânı yok ise ya da kaybolma ihtimali bulunan kanıtların kaybolmasının engellenmesi amacı var ise alınan ses kaydının hukuka uygun delil olarak kabul edilebileceği, bu kapsamda ilgili kişinin iş sözleşmesinin haklı sebeple feshedildiğini ispatlama aracı olarak kullanılan ses kaydının hukuka uygun delil olduğu, nitekim somut olayda ilgili kişinin ses kaydının veri sorumlusu tarafından da alınmadığı ve kullanıcı/müşteri tarafından veri sorumlusu ile paylaşılan ses kaydının delil mahiyeti taşıması sebebiyle veri sorumlusu tarafından muhafaza edildiği, Veri sorumlusu tarafından Kurum kayıtlarına intikal eden cevabi yazıda; ses kaydının herhangi bir personel ile paylaşılmadığının, şifreli diske aktarılarak ve gerekli idari ve teknik tedbirler alınarak güvensiz ortamdan silinmesinin sağlandığının ve yasal saklama süresi ile sınırlı, şifreli bir biçimde muhafaza edildiği" yönleriyle nitelendirmeye konu ederek "ilgili kişiye ait ses kaydının 8'inci maddenin (2) numaralı fıkrasının atfı ile Kanun'un 5'inci maddesinin (2) numaralı fıkrasının (e) bendinde yer alan "Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması" hükmü doğrultusunda mahkemeye aktarıldığı" yönünde karar vermiştir. KVK Kurulu, 07/09/2023 Tarihli

Önemle vurgulamak gerekir ki, suçun önlenmesi ve delillerin ortaya çıkarılması daha az müdahaleci bir yöntemle yerine getirilmesi mümkünse bu halde uygulanan gizli kamera gözetlemesinin ve gizli ses kaydının hukuka aykırı olduğu kabul edilmelidir[1102].

Öncelikli olarak bilgilendirmeye dayanan kamera gözetlemesi (kameralarda katmanlı aydınlatmanın bulunduğu) devamlı kayıt esasına dayandığından işçinin hakları üzerinde orantısız müdahaleler ortaya çıkarabilir. Bu itibarla bir üretim bandının izlenmesi ile dinlenme alanının izlenmesi farklı değerlendirmeye konu edilmelidir. Zira ilkinde işverenin kamera gözetlemesi meşru bir temele dayanmakta ikincisinde ise bu meşru temel zayıftır. Kamera gözetlemesi işçinin özel hayatı ve verileri üzerinde ihlal edici sonuçlar ortaya çıkarmaması için işverenin meşru menfaatleri ile işçinin hakları arasında bir adil denge gözetilmelidir. Örneğin işverenin iş sağlığı ve güvenliği tedbirleri, işyeri güvenliğini sağlama, mülkiyeti koruma kamera gözetlemesi için meşru sebep kabul edilebilir[1103]. Bu durumlarda kamera açıları işçiyi en az izleyecek biçimde konumlandırılması, işçinin verilerinin ve özel hayatının korunmasının göz önünde bulundurulması ve doğrudan işçiyi hedef alan kamera izlemelerinden uzak durulması gerekmektedir[1104].

Gizli kamera gözetlemesi ile işçinin izlenmesi ve kayıt altına alınması kural olarak yasaktır. Zira KVKK m. 5/1 hükmü: "kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez" biçimindedir. Maddenin ikinci fıkrasında ise veri işlemenin diğer şartları düzenlenmiştir. Öte yandan belirtildiği üzere KVKK m. 28/2-a bendinde suçun önlenmesi hali söz konusu ise veri işlemede KVKK'nın maddede

---

ve 2023/1548 Sayılı Karar Özeti, kararın tamamı için bkz. https://kvkk.gov.tr/Icerik/7777/2023-1548 (Erişim Tarihi: 06.02.2024).

1102) Okur, [2013], Elektronik Gözetleme, 133 ve dipnot 121, 122 ve 123'te atıf yapılan yazarlar; Alpagut, [2019], Kamera Gözetlemesi, s. 293.

1103) Okur, [2013], Elektronik Gözetleme, 133; Alpagut, [2019], Kamera Gözetlemesi, s. 293; Dulay Yangın, [2020], AİHM Kararı Değerlendirmesi, s. 1719.

1104) Okur, [2013], Elektronik Gözetleme, 133; Dulay Yangın, [2020], AİHM Kararı Değerlendirmesi, s. 1723.

sayılan maddeleri ile aydınlatma yükümlülüğüne ilişkin m. 10 uygulama alanı bulmaz. AİHM kararlarında tespit edildiği üzere işverenin mülkiyet hakkını koruması için başkaca bir daha az müdahaleci yöntem yoksa, belirli süreli, suçun tespitine yönelik olması, ölçülü ve sınırlı alanda olması kaydı ile dijital izleme gerçekleştirilebilecektir.

Doktrinde bir kısım yazar, gizli izlemenin ancak özel düzenleme bulunması halinde gerçekleştirilebileceğini aksi durumda izlemenin işçinin hakları üzerinde ciddi ihlalleri beraberinde getireceğinden, gizli izlemeyi kabul edilemez olarak nitelendirmişlerdir[1105]. Diğere yazarlar ise, KVKK m. 28/2-a bendi kapsamında değerlendirme yaparak "kişisel verilerin suç tespiti veya suç soruşturması için gerekli olması" durumlarında ölçülülük ilkesine uygun, ciddi suç şüphesine dayanmak, belirli süre ve alanla sınırlandırmak, suç şüphelilerine yönelik olması kaydı ile istisnai olarak gizli kamera kullanılabileceği görüşündedir[1106]. Kanaatimizce iş ilişkisinde ciddi suç şüphesinin bulunması, suçun tespiti veya soruşturması için başkaca daha az müdahaleci bir yöntemin bulunamaması durumunda belirli süreli, suç mahaliyle sınırlı olması, ölçülü olunması ve suç şüphelilerine yönelik olması kaydı ile gizli kamera gözetlemesi gerçekleştirilebilir. Yukarıda incelendiği üzere, KVKK m. 28/2-a düzenlemesi de buna izin vermektedir.

3. İşçilerin Duygu Durumunu, Vücut Isılarını, Seslerini İzleyen ve Analiz Eden Optik Sistemler

İşyerinde kullanılan belirli amaçlar için oluşturulmuş algoritma temelli optik sistemler işçilerin duygu durumunu, vücut ısılarını ve seslerinin değişimini izleyerek işçiler hakkında sağlık, stres ve psikolojik sonuçlar içeren algoritmik

1105) Sevimli, [2006], Özel Yaşam, s. 209; Okur, [2013], Elektronik Gözetleme, 125; Gürsel, [2016], İşçinin Kişisel Verileri, s. 375-376.
1106) Alpagut, [2019], Kamera Gözetlemesi, s. 313; Dulay Yangın, [2020], AİHM Kararı Değerlendirmesi, s. 1725.

analizler gerçekleştirmektedir. Algoritma bir sorunu çözmek veya belirli bir amaca ulaşmak için oluşturulmuş matematiksel süreçlere dayanan tasarım olarak tanımlanmaktadır[1107]. İş ilişkisinde kullanılan algoritmalar işçiyi diğer insanlardan ayıran fizyolojik, fiziksel veya davranışsal verileri işlemeyi de mümkün kıldığından KVKK'da özel nitelikli kişisel veri olarak sayılan biyometrik ve sağlık verilerinin işlenmesi söz konusu olabilir[1108].

Yukarıda ele alındığı[1109] üzere özel nitelikli kişisel veri olan biyometrik veriler ya kanunlarda öngörülen hallerde ya da işçiden açık rıza alınarak işlenebilir. Sağlık verileri ise koruyucu hekimlik, kamu sağlığının korunması için gerekli olma ve KVKK m. 6/3'te öngörülen koşullar kapsamında yetkili kurumlar ile sır saklama yükümlülüğü bulunan kişilerce açık rıza alınmaksızın diğer durumlarda ancak açık rıza alınarak işlenebilir. Örneğin Covid-19'un ortaya çıkardığı pandemi koşullarında işverenlerin kamu sağlığını ve diğer işçilerin sağlını korumak için işyeri girişine termal tarama yaparak işçilerin ateşini ve bağışıklık düzeyini ölçen optik sistemler yerleştirmesi KVKK m. 6/3 kapsamında ölçülü bir dijital izleme uygulaması olarak değerlendirilebilir. Bu örnekte işverenin ayrıca bu sistemlerde elde ettiği veriyi başkaca amaçlar için kullanması veya meşru amaç dışına taşacak şekilde veri işlemesi hukuka uygunluk durumunu ortandan kaldıracaktır.

Ayrıca biyometrik ve sağlık verisi işleyebilen optik sistemlerle gerçekleştirilen dijital izleme, KVKK m. 4'te düzenlenen genel ilkelere ve m. 10'da düzenlenmiş olan aydınlatma yükümlülüğünün kapsamına ilişkin düzenlemelerin dikkate alındığı bir yapı içinde uygulanması gerekmektedir. Aynı doğrultuda bu vasıtalarla işlenen özel nitelikli kişisel verilerin korunması için asgari koruma tedbirlerini öngören 2018/10 sayılı KVK Kurul Kararı'na uygun bir teknik ve idari

1107) John O. McGinnis/Steven Wasick, "Law's Algorithm", Florida Law Review, Vol. 66, No. 3, May, [2014], s. 1020-2022.
1108) KVK Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, s. 5.
1109) § 6. II. 4. i.

tedbir yapısı oluşturulmalıdır[1110]. Eğer veri sorumlusu işveren adına bu verileri bir veri işleyen tedarikçi gerçekleştiriyorsa veri sorumlusu için öngörülen asgari teknik ve idari tedbirleri almada KVKK m. 12/3 kapsamında her ikisi müştereken sorumludur[1111]. Aksi durumda gerçekleştirilen izleme hukuka aykırı olacağından KVKK m. 18 kapsamındaki idari yaptırımlar uygulanabilecek ve KVKK m. 17'deki TCK suçlarına gönderme kapsamında TCK'daki suçlar oluşabilecektir.

Belirtmek gerekir ki, optik sistemlerin gerçekleştirdiği dijital izlemede işlenen kişisel veriler algoritmik analiz sayesinde işçiler hakkında tahminler yapma, işçinin davranışlarını yönlendirebilme, işyeri planlamalarını yapma olanağını işverene verdiğinden işçinin hakları üzerinde gerçekleştirdikleri ihlalin boyutu da büyük olacaktır. Bu sebeple KVKK m. 4'te öngörülen genel ilkeler kapsamında biyometrik veri işleme süreci değerlendirmeye tabi tutulmalıdır. Bu değerlendirme sonucunda eğer meşru amaç için başkaca daha az müdahaleci bir yöntem varsa bunun benimsenmesi zorunludur. Zira algoritmik analiz temeline dayanan bu sistemler işledikleri yoğun ve özgün veri sayesinde işçi hakkında detaylı profilleme yapma imkanını işverene vermektedir. Bunun yapılması işçinin verilerinin iş sözleşmesinin amacıyla bağdaşmayacak şekilde işlenmesi ve özel hayatına saygı hakkına orantısız müdahale anlamına gelir. Bunun önüne geçilmesi için veri işleme etki araştırmasının yanında işyerinde algoritmik izlemenin işçi üzerindeki etkisini araştırmaya ve buna göre bu sistemlerin uygulanmasına yönelik hukuki mekanizmaların oluşturulması gereklidir[1112].

III. İş İlişkisinde Kullanılan Verimlilik ve İş Sağlığı Takip Uygulamaları

İşverenlerin işçilerin kullanımına vermiş olduğu cep telefonlarına ve akıllı

1110) Bkz. "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı kararın tamamına https://www.kvkk.gov.tr/Icerik/4110/2018-10
1111) § 6. II. 6. b.
1112) Emlyn Bottomley, "Data and Algorithms in the Workplace: An Overview of Current Public Policy Strategies", Center for Labor Research and Education University of California, Berkeley, Working Paper, Technology and Work Program, [2020], s. 3, 13-14.

giyilebilir sistemlere yüklenen Boomr, Track View, Hubstaff, StreetSmart, iş gücü yönetimi yazılımı gibi verimlilik takip uygulamaları işverenlere, işçilerin hareketlerini iş saatleri dışında dahi kolaylıkla takip imkanı vermektedir[1113]. Özellikle sahada çalışan işçilerin araçlarında ve mobil uygulamalarında yaygın kullanılan konum belirleme sistemleri olan GPS, Geofence ve RFID etiketleri gibi uydu bazlı izleme uygulamaları işçilerin günlük aktivitelerini konum bazlı işlemeye konu edebilir.

1. İşyerinde Verimlilik İzleme Uygulamalarının Kullanılması

Konum esaslı çalışan verimlilik izleme uygulamaları işçinin hareketlerini, bulunduğu yeri, fizyolojik ve davranışsal verilerini işleyen çeşitli dijital izleme uygulamasından oluşmaktadır. Bu dijital izleme uygulamaları genellikle işçinin iş görme borcunu ifa ediş biçimini tespit etmek, işçiler hakkında tahminlerde bulunmak, işçi verilerini analiz etmek veya kararlar almak, işçilerin davranışlarını yönlendirmek, işyerinin ihtiyaçlarını planlamak, işyerindeki belirli süreçleri otomatikleştirmek ve verimli kılmak amacıyla kullanılmaktadır. Bunun yapılması işçinin kişisel verilerinin işlenmesini gerektirdiğinden KVK hukuku açısından bu uygulamaların kullanılabilmesinin sınırları ve işverence yerine getirilmesi gereken yükümlülükleri bulunmaktadır.

a) İşçileri İzleyen Konum ve Hareket Bazlı Sistemler

Konum ve hareket algılama teknolojilerinin bilgisayarlara, akıllı telefonlara ve giyilebilir diğer teknolojilere entegre hale gelmesi işçilerin sürekli izlenmesi, hareket ve aktivitelerinin kayıt altına alınması açısından çok sayıda yeni olasılık ortaya çıkarmaktadır[1114]. Bilgisayar aktivite izleyicileri, klavye yakalayıcıları, GPS,

1113) Ifeoma Ajunwa, "Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law", Saint Louis University Law Journal, Vol. 63, No. 1, Fall, [2018], s. 23.
1114) Ajunwa, [2018], Algorithms at Work, s. 23-24.

ve Geofence konum ve hareket izlemede kullanılan yöntemlerden bazılarıdır. Ağ üzerinden veya uydu vasıtasıyla izleme olanağı veren bu sistemler işçinin konum ve hareket verilerini işlemeye konu edebilmektedir. Ayrıca bu sistemler çeşitli yapay zeka uygulamasıyla entegre hale getirilerek işçinin belirli anlardaki tanımlanmış verilerini işlemeye konu edebilir. RFID ise tek tek öğeleri otomatik olarak tanımlamak için radyo dalgalarını kullanan çeşitli teknolojiler için genel bir terimdir. RFID sistemlerinin etiket ve bir okuyucu olmak üzere iki ayrılmaz parçası bulunmaktadır. Okuyucular, etiket tarafından depolanan veya toplanan bilgileri yakalar[1115]. Böylelikle RFID sayesinde işyeri departman yöneticileri ve insan kaynakları yöneticileri işçilerle ilgili geniş kapsamlı veri elde edebilir[1116].

İş yaşamında RFID izleme özellikle lojistiği optimize etmek, kazaları önlemek ve kamyon şoförlerini takip etmek için kullanılmaktadır[1117]. Bazı işverenler ise RFID çiplerini işçilere takmayı denemiştir. ABD'de bazı eyaletler bu tür çiplerin işçilere zorla takılmasını yasaklayan yasal düzenlemeler gerçekleştirilmiştir[1118]. Ülkemizde işverenlerin işçilere çip takarak izleme örneği henüz bulunmamakla birlikte aslında teknolojik gelişmeler gelecekte nasıl uygulamaların ortaya çıkabileceği hakkında bir fikir vermektedir.

b) Giyilebilir Teknolojilerle İşçilerin İzlenmesi

İş ilişişinde giyilebilir teknolojilerle izleme dendiğinde işçinin faaliyetlerini, yaşam rutinlerini, sağlık durumunu, ateşini takip edebilen akıllı saatler, yapay zeka

1115) https://tr.wikipedia.org/wiki/RFID (Erişim Tarihi: 25.04.2022).
1116) Martin Abraham/Cornelia Niessen/Claus Schnabel/Kerstin Lorek/Veronika Grimm/Kathrin Möslein/Matthias Wrede, "Electronic Monitoring at Work: The Role of Attitudes, Functions, and Perceived Control For The Acceptance of Tracking Technologies", Human Resource Management Journal, C. 29, [2019], s. 658.
1117) Abraham/Niessen/Schnabel/Lorek/Grimm/Möslein/Wrede, [2019], Electronic Monitoring at Work, s. 658-659.
1118) Melanie R. Bueckert, "A Critical Review of the Law Regarding Electronic Employee Monitoring in Non-Unionized Workplaces in Canada", Master of Laws, Faculty of Law University of Manitoba Winnipeg, [2008], s. 20.

tabanlı çalışan gözlükler[1119], kulaklıklar[1120], sensörlü eldivenler[1121] ve yaka kartları ilk akla gelen dijital izleme uygulamalarıdır. Ayrıca bunların gelişen teknolojilerle çeşitli şekillere ve yapılara bürüneceğini ve yeni örneklerinin ortaya çıkacağını da belirtmek gerekir[1122]. Örneğin son olarak Amazon'un geliştirdiği dokunsal geri bildirimli bileklikler (2D Düzlemde Konum Tespiti ve Ultrasonik Bileklik ve Alıcılar) işçiler depolardaki ürünlerin yerini tespit ederken onlara zamanda tasarruf sağlamayı amaçlamaktadır. Bileklikler aynı zamanda dokunsal geri bildirim yoluyla işçilerin harekelerini, neye ne kadar zaman harcadıklarını da izleyebilmektedir. Sistem depo etrafına kurulan ultrasonik bilişim sistemlerini, depo işçilerinin taktıkları bilekliği ve bu faaliyeti denetleyebilen bir modülü içermektedir. İşçilerin tüm hareketlerini, duraklamalarını, tuvalette geçirdiği zamanı dahi izleyebilen bu giyilebilir dijital izleme uygulaması aynı zamanda belirli aralıklarla işçilere "hareketli olun", "kısa bir mola verin" gibi komutlar ve bildirimler de gönderebilmektedir[1123]. İşyerinde uygulanmak için geliştirilen bu ve benzeri giyilebilir dijital izleme uygulamaları gelecekte yeni giyilebilir izleme uygulamalarıyla işçilerin izleneceğini ve denetleneceğini göstermektedir.

Araştırmalarda giyilebilir teknolojilerin işyeri verimliliğini artırdığına, iş ilişkisinde riskleri minimize ettiğine, işçilerin birbiriyle uyumlu ve verimli çalışmasını sağladığına ilişkin bulgulara ulaşılmıştır[1124]. Öte yandan yapay zeka

---

1119) Alman asansör firması Tyssenkrupp, operatörlerinin bakım sorunlarını görebilmeleri ve tanımlayabilmeleri için asansör bakım operatörü işçisine HoloLens artırılmış gerçeklik gözlükleri kullandırmıştır. Detaylar için bkz. Mustafa Alp/Sevil Doğan, "Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", Çalışma ve Toplum, 2021/4, [2021], s. 2603 vd. (Alp/Doğan, [2021], Giyilebilir Teknolojiler).

1120) Lufthansa firması tarafından 2014 yılında geliştirilerek işçilerin kullanımına verilen "ses tabanlı akıllı kulaklıklar" vasıtasıyla, bakım kontrol listesi, bir teknisyenin kulaklıklarına iletilen sesli komutlara dönüştürmekte ve depolanan bu veriler belirli iyileştirmelerde kullanılmaktadır. Detaylar için bkz. Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2603 vd.

1121) BMW için 2016 yılında 'start-up' olarak üretilen "ProGlove" isimli sensörlü eldiven, elin arkasında yer alan barkod tarayıcı sayesinde veri işlemekte ve doğal el hareketlerini algılamakta ve işçilere geri bildirim verebilmektedir. Detaylar için bkz. Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2603 vd.

1122) Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2601; Ali Güzel/Deniz Ugan Çatalkaya/Hande Heper, "İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", Hukuk ve Adalet Eleştirel Hukuk Dergisi, C. 15, Özel Sayı, [2023], s. 59-60.

1123) Ajunwa, [2018], Algorithms at Work, s. 34-35.

1124) Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2600.

destekli bu tür giyilebilir teknolojilerin ortaya çıkardığı algoritmik yönetim ve analizin işçiler için psikososyal riskler ortaya çıkardığı, iş stresine sebebiyet verdiği verimlilik artışı ve uyumlu çalışma esaslı yaklaşımların bu riskleri görmezden geldiğine ilişkin çalışmalar da bulunmaktadır[1125].

Giyilebilir teknolojiler açısından özellikle teknoloji küçüldükçe çiplerin insana entegre edilmesine yönelik uygulamalar da artmaktadır[1126]. Gelecekte bu teknolojiler vasıtasıyla daha sofistike dijital izleme uygulamalarının kullanılacağını ve bireyin vücuduna entegre edilebilen dijital izleme sistemlerinin veya akıllı saat, akıllı telefon, sağlık izleyicileri, cilt sıkılığını takip eden veya kalp atışını izleyen uygulamalar vasıtasıyla kişinin yoğun olarak izlenmeye tabi tutulacağını varsayabiliriz. İş ilişkisini bu gelişmelerden ayrı düşünmek olanaksız olduğundan, işçileri giyilebilir veya vücuda eklenebilir teknolojilerle izlemenin ve denetlemenin yaygınlaşacağını belirtmek gerekir. Bunun en önemli göstergelerinden birisi giyilebilir teknoloji olarak tarif edilen bu aygıtlar veya benzerlerinin dünyadaki satış sayısında son yıllarda patlama yaşanmış olmasıdır. Büyük veri analizi, bulut bilişim, yapay zeka destekli akıllı fabrikalar, nesnelerin interneti[1127] ve giyilebilir

1125) Aude Cefaliello/Phoebe V. Moore/Robert Donoghue, "Making Algorithmic Management Safe and Healthy for Workers: Addressing Psychosocial Risks In New Legal Provisions", European Labour Law Journal, Vol. 14, No. 2, [2023], s. 192–210.

1126) İşverenlerin işçileri mikroçip implantlarla takip etmeye başlamalarına ilişin bir NewYork Post haberi için bkz. https://nypost.com/2017/04/03/bosses-are-already-tracking-employees-with-microchip-implants/ (Erişim Tarihi: 16.12.2022). Habere göre İsveç'te faaliyette bulunan Epicenter isimli firma yaklaşık 150 çalışanına mikroçip yerleştirerek tuvalet molalarını ve ne kadar süreyle çalıştıklarını tespit etmeyi hedeflemiştir. Ayrıca bu çip sayesinde çalışanların kredi kartı, anahtar, işyeri giriş kartı gibi birçok aygıttan kurtulacağı belirtilmiştir. Ayrıca haberde Epicenter'in iki yıl kadar önce birçok çalışanını çiplediği ve bu teknolojinin günlük yaşamda kullandığı belirtilmektedir.

1127) Nesnelerin İnterneti (IoT – Internet of Things), internet sayesinde kişinin günlük hayatta kullandığı nesnelerin birbiriyle iletişim kurması, veri alışverişinde bulunması, nesneleri kullananların yaşayışına dair veri toplamasıdır. Web özelliği bulunan bu cihazlar kişinin alışkanlıkları, yaşayışı, davranışları hakkında verileri analiz imkanı tanıyacak şekilde bulut sistemler üzerinde işler. Yapay zeka ve robot teknolojisiyle çalışabilme özelliği sayesinde işyerleri ve kişi için kolaylıklar ve zamanın verimli bir şekilde kullanılmasını sağlar. Bununla birlikte bu sistemlerin "insan bileşeni" de bulunduğundan işyerinde kullanılması durumunda işçinin yaşayışına ilişkin işlemeye konu ettiği tüm verileri işler ve analiz etme olanağını ortaya çıkarır. Avrupa Komisyonu 19.2.2020 tarihinde COM (2020) 64 "Yapay Zeka, Nesnelerin İnterneti ve Robot Biliminin güvenlik ve sorumluluk etkilerine ilişkin rapor" hazırlamış ve bu teknolojilerin ortaya çıkardığı büyük fırsatı, önemini ve oluşturabileceği potansiyeli kabul etmiş ve bu hedeflere ulaşmak için açık, öngörülebilir bir yasal çerçeveye ihtiyaç bulunduğunu tespit etmiştir.

teknolojiler Endüstri 4.0 olarak ifade edilen dönüşüm sürecinin bir parçası olarak iş yaşamında görünüm kazanmıştır[1128].

İşçiye entegre giyilebilir teknolojiler işitme cihazları, akıllı saatler, bileklikler, sensörlü eldivenler, gözlükler, kemerler, akıllı mont ve diğer izleme araçları biçiminde çeşitlenmiş olmakla birlikte bunlar akıllı saatler, konum takipçileri, sağlık ve hareket esaslı teknolojiler ve akıllı tekstil ürünleri şeklinde kategorileştirilmektedir[1129]. Örneğin cep telefonu, akıllı saat veya giyilebilir başka sistemler üzerinde çalışabilen StreetSmart İşgücü Yönetimi isimli yazılım mobil durumda olan her işçinin konumunu herhangi bir yere varış saatlerini, mola durumu, dinlenme arası, gittiği rota ve daha fazla programlanabilen başlıkta ayrıntılı bilgileri işverenlere Google Haritası üzerinde sağlayabilmektedir. Bu uygulamalar GPS, optik veri, kalp atım hızı ve işçinin hareketleri esaslı verileri işlediğinden 24 saat boyunca işçinin yaptıkları, yeme ve içme alışkanlıkları, uyku düzeni, yaşayış biçimi, boş zamanlarda yapılan işler ve iş saatlerinde işe ayrılan zaman gibi birçok veriyi işleyebilmektedir.

İş ilişkisini yakından ilgilendiren diğer izleme araçları olarak ifade edilen giyilebilir teknolojilere, dijital izleme gerçekleştirme olanağı sunan giyilebilir her şey girmektedir. Bu kategoride akıllı çoraplar, spor sutyenleri, akıllı gözlükler, çalışma tulumları, akıllı takımlar ve yoga pantolonları gibi çeşitli alanlara ayrılmış kişiye entegre teknolojiler yer almaktadır. Giyilebilir teknolojilerin asıl ortaya çıkaracağı sorun kişinin vücudunun işverenlere, şirketlere veya uygulama geliştiricilerine özel nitelikli kişisel verileri de içerecek şekilde geniş bir alanda önemli değere sahip verileri aktarma imkanı sağlamasıdır[1130].

Giyilebilir dijital izleme uygulamaları ilk bakışta zararsızmış, işyerinde iş

1128) Rachel Arrison, "You're Wearing That: Why Data Generated from Wearable Technology Should Be Protected under Privacy", Law Sports Lawyers Journal, 26, [2019], s.212.
1129) Ajunwa, [2018], Algorithms at Work, s. 26.
1130) Kenny Gutierrez, "Privacy in Wearables: Innovation, Regulation, or Neither", Hastings Science and Technology Law Journal, Vol. 13, No. 1, Winter, [2022], s. 26.

sağlığı ve güvenliği risklerini minimize etmede ve verimin artırmasında destek sağladığı izlenimi oluşturmaktadır. Ne var ki, bu uygulamaların işçiye ilişkin birden fazla veri kümesinde yer alan verileri işleme ihtimali bulunduğundan işçinin profili oluşturarak özel hayatlarının şeffaflaşmasına, özel nitelikli verileri de dahil olmak üzere birçok kişisel verisinin işlenmesine ve algılarını yönlendirebilmesine sebebiyet verebilir. Dijital izlemeyle işlenen bilgiler sayesinde işçinin olası davranışlarının ve sağlık durumunun tahmin edilebilmesi, elde edilen verilerin ve gerçekleştirilen analizlerin işçi aleyhine olacak şekilde kullanımlara konu edilmesi söz konusu olabilir[1131]. Bu sebeple giyilebilir teknolojilerde işlenen işçi verilerinin işçiyi belirli veya belirlenebilir hale getiren verilerden değil anonim verilerden oluşmasını sağlayacak uygulama ve analiz sistemlerinin geliştirilmesi hukuken zorunlu hale getirilmelidir[1132]. Bu noktada eklemek gerekir ki anonimleştirme, ilgili verinin herhangi bir veriyle ilişkilendirilse dahi işçinin belirlenebilir hale getirilmemesi biçimindeki veri ile kişi arasındaki bağın koparılmasıdır[1133]. Bu niteliği taşımayan veriler bir kişiyi belirlenebilir hale getireceğinden anonimleştirmeden bahsedilemez.

Kamera gözetlemesi, internet iletişiminin ve bilgisayarın izlenmesiyle ilgili oluşan içtihatlar ve doktrin görüşlerinde ele alındığı üzere verimlilik izleme uygulamaları ve işverenin gözetme borcu kapsamında kullandığı izleme sistemleri için aynı amacı gerçekleştirebilecek daha az müdahaleci yöntemler varsa bunların araştırılması ve uygulanması gerekir. Ayrıca izlemenin amaçla sınırlandırılması, sınırlı ve ölçülü olma ilkesi kapsamında değerlendirmeye konu edilmesi, elektronik iletişimin izlenmesine ve kamera gözetlemesine ilişkin AİHM ve AYM içtihatlarında belirlenen ölçütlerin bu izleme uygulamalarında aranması uygulamaların bireyin kişisel verileri üzerinde oluşturacağı ihlali

1131) Giovanni Ziccardi, "Wearable Technologies and Smart Clothes in the Fashion Business: Some Issues concerning Cybersecurity and Data Protection", Laws, Vol. 9, No. 2, June, [2020], s. 9.
1132) Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2622.
1133) KVK Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi, KVK Kurumu Yayınları, Ankara, [2018], s. 15 vd.

sınırlandıracaktır[1134].

2. İşyeri Dışında Konum Bazlı Dijital Sistemlerle İzleme

Günümüzde işçilerin konumlarının izlenmesi GPS, Coğrafi Bilgi Sistemi (GIS - Geographic Information System), baz istasyonları, Wi-Fi ağı veya RFID etiketi gibi konum bazlı çeşitli dijital uygulamanın mobil bilişim sistemlerine veya giyilebilir teknolojilere yüklenmesiyle gerçekleşmektedir. Baz istasyonları, uydu veya diğer radyo sinyali tabanlı sistemlerle desteklenen bu konumlandırma sistemleri sayesinde coğrafi etiketli görüntüler, video, ses ve metin belgeleri, uydu destekli görüntüler, IP adresine göre konum bilgileri kayıt altına alabilmektedir. Bu sistemler sayesinde işçinin mevcut veya geçmiş coğrafi konum verileri ve aktiviteleri işçinin bilgisi dahi olmaksızın işlemeye konu edilebilir[1135].

Yaygın kullanılan konum izleme sistemi GPS doğrudan kişinin konumsal, görsel ve davranışsal hayat alanını kapsamlı olarak takip etme ve kayıt altına alma imkanı veren bir dijital izleme yöntemidir. Zira, GPS teknolojik olarak farklı uydulardan gelen sinyallerin zaman farkını hesaplayarak ilgili kişinin bulunduğu yerin enlem ve boylamını belirleyebilen bir uydular, mobil sistemler, bilgisayarlar ve alıcılar sistemidir[1136]. Bu özelliğinden dolayı işçinin hangi zaman diliminde nerede, ne yaptığı gibi konularda işverene detaylı bilgi sunabilir. Eklemek gerekir ki, konum bazlı dijital izleme uygulamaları belirli durumlarda işverenin sözleşmeden doğan bir hakkı ve aynı zamanda belirli türde işler (Örneğin madencilik, araç filolarını verimli organize etme ve taşıt temelli işler) açısından kanunlardan doğan yükümlülüğüdür[1137].

1134) Aktaran, Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2623; Bkz. § 7.II.2.b.
1135) Erion Murati/Manjola Henkoja, "Location Data Privacy on MAAS under GDPR, European Journal of Privacy", Law & Technologies (EJPLT), Vol. 2019, No. 2, [2019], s. 122.
1136) https://tr.wikipedia.org/wiki/GPS (Erişim Tarihi: 22.04.2022).
1137) Kendra Rosenberg, "Location Surveillance by GPS: Balancing an Employer's Business Interest with Employee Privacy", Washington Journal of Law, Technology & Arts, Vol. 6, No. 2, Autumn, [2010], s. 145-146.

Günümüzde cep telefonlarındaki ve taşınabilir bilgisayarlardaki birçok uygulama işçilerin dijital izlerini kayıt altına alarak lokasyon bazlı davranış ve hareketlerini yönlendirecek denetimler oluşturabilmektedir. Öte yandan iş ilişkisinde işçilerin konumlarının izlenmesi işverenlerin bu izlemeyi işçinin yaptığı işle ilişkilendirdiği durumlarda gerçekleştirilebilmesi mümkündür (KVKK m. 4). Böyle bir ilişki örneğin insanların taşınması, mülkiyetin korunması[1138] ya da değerli malların transferi veya kuryelerin ve dağınık konumlardaki hizmetler için lojistik kaynakların dağılımının iyileştirilmesi gibi sebeplerden kaynaklanmış olabilir[1139]. Bu durumlarda konum izleme uygulamalarının kullanılması genel olarak kabul edilmektedir.

Ele alındığı üzere, konum izlemesi gerçekleştirilirken de özel hayat ve kişisel veriler üzerinde en az müdahaleci sonuçlar ortaya çıkaracak yöntem benimsenmelidir. Örneğin sürekli konum bazlı izleme uygulamalarının kullanılmasından kaçınılmalı ve işçi mesai saatleri dışında bu sistemleri kapatabilmelidir. Ayrıca çeşitli GPS ve lokasyon verilerini harmanlayarak işçileri yoğun izlemeye tabi tutmaya olanak tanıyan (Geofencing – coğrafi izleme) izlemeler de günümüzde yaygınlaşmaktadır[1140]. Bu sistemlerde coğrafi sınır, bir coğrafi alanı tanımlamak için GPS veya başka araçların ortaklaşa kullanılmasını sağlayan bir yazılım platformu tarafından oluşturulan sanal bir sınırdır[1141]. Böylelikle işverenler coğrafi sınırlama esaslı dijital izleme uygulamalarını

1138) EDPB, 04 Ekim 2022 tarihli GPS takibiyle çalışanların izlenmesini GVKT m. 5/1-c ve 6/1-f bendi kapsamında değerlendirmiş, mülkiyetin korunması için işverence GPS takibi yapılmasında meşru bir menfaatin bulunabileceğini, ancak gerçekleştirilecek izlemenin uygun ve gerekli olması gerektiğine karar vermiştir. Bu karar özelinde şantiyede gerçekleştirilen hırsızlık olayının bir daha yaşanmaması için çalışanların sürekli izlenme altında tutulmasının yasaya aykırı olacağı vurgulanmıştır. https://edpb.europa.eu/news/national-news/2022/safety-property-can-be-legitimate-interest-gps-tracking-measure-must-be_en (Erişim Tarihi: 11.11.2022).

1139) https://unece.org/wp29-introduction; 2130/05/EN, WP 115 Working Party 29 Opinion on the use of location data with a view to providing valueadded services, November 2005, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

1140) Michael Downey, "Legal Ethics and Geofencing, Litigation", Vol. 45, No. 4, Summer, [2019], s. 64.

1141) Jessica Pushka, "The Applicability of the Personal Information Protection and Electronic Documents Act to De-Indexing Internet Search Engine Results", Asper Review of International Business and Trade Law, 19, [2019], s. 193.

kullandıklarında işçi, işveren tarafından bir coğrafi sınır içinde dijital izlemeye tabi tutulur. Bu dijital izleme sayesinde işçiler belirlenen dijital sınıra girdiklerinde veya bu sınırdan çıktılarında geride bıraktıkları her türlü veri işverene aktarılır. Bu itibarla Geofencing, işyerine giriş – çıkış verisini işleyen sistemlerden daha fazlasını izlemeye konu ederek işverene, GPS konumlarına dayalı olarak işçilerin konumlarını gerçek zamanlı olarak izleme ve denetim olanağı verir. Bu özelliğinden dolayı işveren, işçilerini uzaktan izleme olanağını gerçek zamanlı konum belirleme sistemleri sayesinde elde etmekte ve işyeri verimini bu vasıtalarla artırmak amacıyla sanal sınırlayıcı dijital izleme uygulamalarını kullanmaktadır[1142].

Gerçek zamanlı konum takip sistemleri ve sanal sınırlama teknolojileri işçilerin işyeri prosedürlerine uygun iş yapmalarını sağladığı, ticari sırların ifşa edilmesini engellediği ve işyeri verimini artırdığına yönelik bulgular elde edilmiştir. Öte yandan konum izleme uygulamalarının işçinin özel hayat alanına taşacak şekilde kişisel verilerin işlenmesine sebebiyet verdiği, işçileri devamlı izlenme baskısı altında tuttuğu ve iş stresine sebebiyet verdiği de tespit edilmiştir[1143]. Bu sebeple bazı ülkelerde bu tür uygulamaları kullanmak sıkı şartlara ve ilgili kişinin rızasının alınması şartına bağlanmış aksi durum suç olarak hukuki düzenlemelere konu edilmiştir. Örneğin Kaliforniya'da, bir kişinin rızası olmadan konumunu veya hareketini belirlemek için dijital izleme uygulaması kullanmak suç olarak düzenlenmiştir. Aynı doğrultuda Connecticut'ta eyalet yasama organı işverenlerin, dijital izlemeden etkilenecek işçilere önceden bildirimde bulunmaksızın dijital izleme uygulaması kullanması yasaklanmıştır[1144]. Ülkemiz KVK hukuku açısından da bir kişiyi belirlenebilir hale getiren konum ve verimlilik izleme uygulamaları bir veri işleme şartına dayanmak zorundadır. Ayrıca bu uygulamalarla ilgili kişinin verisinin işlenebilmesi için aydınlatma yükümlülüğü kapsamında bilgilendirmenin yapılmış olması belirleyici bir hukuka uygunluk

1142) Benjamin Wong, "Data Protection Implications of Modern Employee Monitoring Software", Singapore Academy of Law Journal, Vol. 33, No. Special Issue, [2021], s. 107.
1143) Rosenberg, [2010], Location Surveillance, s. 145.
1144) Rosen Rosenberg, [2010], Location Surveillance, s. 149.

ölçütüdür[1145].

3. İşçinin Konum Belirleme Sistemleri ve Giyilebilir Teknolojilerle İzlenmesinin Sınırları

Konum belirleme ve giyilebilir dijital izleme uygulamaları vasıtasıyla izlemede elde edilen veri kişisel veri olabileceği gibi KVKK m. 6'da özel nitelikli kişisel veri olarak düzenlenen biyometrik (fizyolojik veya davranışsal) ve sağlık verisi de olabilir. Dahası bu sistemler kullanılmasa işverenin erişmesinin güç olduğu işçinin yaşam biçimi, alışkanlıkları, uyku düzeni, kalp atış hızı, stres ve terleme biçimi gibi birçok veri bu uygulamalar vasıtasıyla işlenebilmektedir[1146]. İşçiye özgü olan fiziksel veya davranışsal özellikler gibi ayırt edici ve kişiye özel verileri işlemeyi olanaklı kılan bu sistemler özel nitelikli kişisel veri de işlemektedir[1147]. Bu tür ayırt edici veriler özel nitelikli kişisel veri olarak düzenlenen biyometrik veri olduğundan işlenmesi ve korunması daha katı kurallara bağlanmıştır. Bu sebeple konum belirleme sistemleriyle dijital izleme gerçekleştirilmesi KVK hukukunun genel ilkeleri olan KVKK m. 4 ve iş ilişkisi açısından TBK m. 419/1'in ve aynı yönde düzenleme olan KVKK m. 5/2-c bendinin sunduğu ölçüt kapsamında gerçekleştirilecek uygulama değerlendirmeye tabi tutulmalıdır.

Bu değerlendirme sonrasında bu sistemler vasıtasıyla kişisel veri işlenmeden önce aydınlatma yükümlüğü kapsamında ilgili işçiler bilgilendirilmeli ve diğer teknik ve idari yükümlülükler yerine getirilmelidir. Ayrıca konum belirleme sistemleri veya giyilebilir teknolojilerle izlemenin işçinin bilgisi dışında gerçekleştirilmesi veya KVKK m. 10 ile Tebliğ'deki unsurları taşımayan bir aydınlatma metni kapsamında gerçekleştirilmesi işçinin özel hayatı ve kişisel

1145) Bkz. § 6. II. 4 ve 6.
1146) Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2615-2616.
1147) KVK Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber, s. 5.

verileri üzerinde ağır ihlal ortaya çıkarır. Dahası konum belirleme dijital izleme uygulamalarının gizli kullanılması işçinin işyerinde özel hayata saygı haklarına ilişkin makul beklentilerinde aldatılması anlamına gelecektir[1148].

Belirtmek gerekir ki işyeri dışında işçinin izlenmesine olanak veren konum belirleme sistemlerin iş ilişkisi için gerekli olduğu durumlarda işçinin mesai saatleri dışındaki verileri işlemesi hukuka aykırıdır[1149]. Aynı durum işçinin aktivitelerini kaydeden, klavye ve bilgisayar hareketlerini izleyen sistemler için de geçeleridir. Dahası KVK hukukunun genel ilkelerine uygun olmayan ve bilgilendirmenin de bulunmadığı izlemede bu sistemler vasıtasıyla elde edilen verilerin kullanılması hukuken mümkün değildir.

Yukarıda incelendiği üzere, KVKK m. 28/2-a bendi "kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması" durumunda işlenmesi KVKK m. 10'da düzenlenmiş olan aydınlatma yükümlülüğünün bir istisnasıdır. Bunun dışındaki dijital izlemelerde genel ilkelerin gözetilmemesi ve işçinin bilgilendirilmemesi izleme faaliyetini hukuka aykırı hale getirir. Ayrıca işçinin özel hayatı ve kişisel verileri üzerinde müdahaleci sonuçlar ortaya çıkaran bu izleme uygulamalarının işçinin mesai saatlerinin dışına taşacak şekilde veri işlemesi, hatta dinlenme, uyku anı verilerini giyilebilir teknolojilerle kayıt altına alması olanağı düşünüldüğünde işverenin kullanacağı bu uygulamaların kullanım alanını KVK hukukunun genel ilkeleri kapsamında değerlendirerek sınırlandırmak gerekmektedir.

Bu uygulamalar aynı zamanda büyük veri oluşturabilecek biçimde çalışabileceğinden işçinin birçok verisini işlemeye konu edebilir. Dahası iş ilişkisinde dijital izleme gerçekleştirebilen giyilebilir sistemler çeşitli yazılım ve sensörler içerdiğinden işlenen işçi verileri de çeşitli türde olabilmektedir. Örneğin

1148) Okur, [2013], Elektronik Gözetleme, s. 138.
1149) Okur, [2013], Elektronik Gözetleme, s. 137.

vücut ısısını kaydetme, stres düzeyini ölçme, atılan adım sayısını izleme, kalp atışını takip etme, işçinin fizyolojik bilgilerini izleme gibi veriler sağlık ve biyometrik verilerden oluştuğundan[1150] bunların işlenmesi özel nitelikli kişisel verilerin işlenme kurallarına tabidir. Dahası bu sistemlerin işlediği bu tür özel nitelikli kişisel veriler işçinin özel hayatına saygı hakkı ve kişisel verileri üzerinde ağır ihlaller ortaya çıkarabilir.

Yargıtay, işverenin GPS kayıtlarını esas alınarak fazla mesai hesaplaması yapma uygulaması kullanması sonucu elde etmiş olduğu veri ile işçinin GPS kayıtlarına aykırı düşecek şekilde fazla mesai girişi yapmasını dürüstlük kuralına aykırı bulmuş ve iş akdinin feshinin haklı nedene dayandığına karar vermiştir[1151]. İşverenin GPS takibi gerçekleştirmesi kişisel verilerin işlenmesini gerektirdiğinden bu hususta işçinin önceden tam olarak bilgilendirilmesi gerekmektedir. Bunun yapılmamış olması izlemede elde edilen veriler hukuka aykırı delil olarak nitelendirilmesine sebebiyet verebilir. Yargıtay'ın bilgisayar gibi elektronik cihazların izlenmesine ilişkin verdiği kararlarda bunu nazara almasına rağmen[1152] GPS izlemesinde elde edilen verilerde özellikle işçi aleyhine olan örneklerde bu hususta bir değerlendirme yapmaması eksikliktir. Zira bir verinin delil olarak kullanılabilmesi ancak bu verinin hukuka uygun olarak elde edilmiş olması ve bu hususta işçinin bilgilendirilmiş olmasına bağlıdır. Nitekim, HMK m. 189/2 hükmünde hukuka aykırı elde edilmiş delillerin ispatta dikkate alınması yasaklamıştır[1153].

IV. İşçinin Elektronik İletişiminin İzlenmesi

Günümüzde işçinin iş görme borcunun ifasının temel araçlarından olan

1150) Alp/Doğan, [2021], Giyilebilir Teknolojiler, s. 2602.
1151) Yargıtay 9. HD., E. 2016/17414 K. 2017/12165 T. 6.7.2017; Yargıtay 22. HD., E. 2014/6402 K. 2015/17560 T. 18.05.2015; Yargıtay 9. HD., E. 2016/35409 K. 2020/17378 T. 7.12.2020.
1152) Yargıtay 22. HD, E. 2017/21857, K. 2019/9884, T. 07.05.2019.
1153) Hakan Pekcanıtez/Oğuz Atay/Muhammed Özekes, Medeni Usul Hukuku, 14. Bası, Yetkin Yayınları, Ankara, [2013], s. 694.

bilgisayar, e-posta hesabı, internet, telefon, Skype, Zoom, Teams gibi elektronik iletişim araçları ve uygulamaları işverenler tarafından çeşitli amaçlarla dijital izlemeye tabi tutulmaktadır. İşverenin elektronik iletişimi izlemedeki menfaatleri ile işçinin iletişim hakkı, kişisel verileri üzerindeki hakları ve özel hayatına saygı hakkına ilişkin makul beklentisi hakları arasında bir çatışma ortaya çıkmaktadır.

1. Elektronik İletişimin İzlenmesinde İşverenin Menfaatleri

Bilgisayar teknolojisinin gelişmesi ağlar arası iletişimi hızlandırmış ve internet kullanımı, e-posta yazışmaları günümüz işyerlerinin tartışmasız bir gerçekliği haline gelmiştir. Öyle ki gün gittikçe daha fazla işçi bu uygulamaları kullanarak iş gördüğünden bunların oyun oynama, internette gezinme, sosyal medyada paylaşımlarda bulunma, pornografik içeriklere erişme ve farkında olmadan işyeri bilişim sistemlerini fidye saldırılarına, hacker sızmalarına açık hale getirme gibi kötüye kullanılması örneklerini de ortaya çıkmıştır. İşverenlerin bu olumsuzlukların önüne geçmek için iletişimi denetlemede mülkiyet hakkı ve sözleşme ilişkisine dayanan menfaatleri bulunmaktadır[1154]. Bu sebeple birçok işveren bilgisayarları, sunucuları, interneti ve e-postaları izleyen elektronik uygulamaları kullanmaya başlamıştır[1155].

İşverenlerin bilgisayarları, e-postaları ve interneti izlemesi devamlı veya rastgele denetime olanak veren sunucu tabanlı ve istemci tabanlı olarak gerçekleştirilebilmektedir[1156]. Sunucu tabanlı izleme işverenin internet ağları

1154) Okur, [2013], Elektronik Gözetleme, s. 163.
1155) Ciocchetti, [2001], Monitoring Employee, s. 4-5; Laurie Thomas Lee, "Watch Your E-mail - Employee E-Mail Monitoring and Privacy Law in the Age of the Electronic Sweatshop", John Marshall Law Review, Vol. 28, No. 1, Fall, [1994], s. 140-141.
1156) İstemci bilgisayar, sunucuda (server) depolanan bilgi, veri veya uygulamalara çalışan (kullanıcı) tarafından erişme olanağı olan daha az veri bulunan küçük bir bilgisayardır; sunucu bilgisayar ise veri tabanlarını, yüksek kapasiteli veri dosyalarını ve uygulamaları depolayan güçlü bir bilgisayardır. Sunucu bilgisayara birçok istemci bağlanarak veri dosyalarının tamamına veya kendilerine verilen yetki kapsamındaki sınırlı dosyalara erişim sağlayabilir.
http://www.differencebetween.info/difference-between-client-and-server (Erişim Tarihi: 19.04.2022).

üzerinde kurulur ve genellikle e-posta, internet trafiğini ve kullanımını izlemek için kullanılır. İstemci tabanlı uygulamalar ise birbirinden bağımsız olacak şekilde işçilerin kullandığı bilgisayar üzerine (örneğin klavye aktivitesi, vuruş bilgilerini kaydeden uygulamalar) kurulabilir. Bu sistemler üzerine kurulan dijital izleme yazılımlarının ortak özelliği işçilerin bilgisayarları nasıl, ne amaçla kullandıklarını, internet trafiğini ve e-posta yazışmalarını takip etme ve bunların ayarlanabilir amaçlar kapsamında raporlanabilir veri elde etme olanağını vermeleridir[1157].

İnternet trafiğini takip için kullanılan izleme yazılımı, işçilerin internet hareketlerini takip edip, yöneticilere raporlayabilecek şekilde uygulanabilir. Yine işçilerin internet gezinme bilgileri, ziyaret edilen siteler ve e-posta yazışmaları aktif olarak gerçek zamanlı izlenebilir ve dijital izleme belirli kavramları algılayacak şekilde işverene bilgi aktarabilir. Dahası kullanılan dijital izleme uygulaması vasıtasıyla, belirli aralıklarla bir işçinin bilgisayar ekranının fotoğrafını çekmesi, ekranın gerçek zamanlı kaydını alması ve bu uygulamayı takip eden işverene bu kayıtların gönderilmesi mümkündür. Ayrıca dijital izleme teknolojileri, işveren tarafından önceden belirlenen şüpheli anahtar kelimeleri tarayacak şekilde de ayarlanabilir. Özellikle işçilerin e-posta yazışmaları potansiyel riskli kavramlara ve uygunsuz mesajlara yönelik olacak biçimde taranabilir. Örneğin ticari sırlarını korumak veya işçilerin uygunsuz içerikleri e-postada paylaşmasını engellemek isteyen ya da işçilerin çalışma arkadaşlarını taciz etmesini önlemek isteyen bir işveren bu hususlara ilişkin belirli kavramları anahtar kelime olarak listeleyebilir ve bunları periyodik olarak tarayacak bir dijital izleme uygulaması kullanabilir. Eklemek gerekir ki, dijital izleme uygulamaları kayıt temelli kalıcı veri işlenmesine olanak sağladığından işverenler için güçlü bir yönetim aygıtına dönüşmektedir[1158].

İşverenlerin bilgisayar, e-posta ve internet kullanımını izlemek için gizli veya açık izleme yazılımları kullanması risklerin önlenmesi, mülkiyetin korunması

1157) Lasprogata/King/Pillay, [2004], Electronic Employee Monitoring, s. 8-9.
1158) Riedy/Wen, [2010], Electronic Surveillance, s. 88-89.

(fikri mülkiyet ve ticari sırlar gibi) ve verimliliğin artırılması gibi amaçlar kapsamında makul görülmekle birlikte bu sistemlerin kullanımının ölçülü olması ve izleme ile ilgili işçinin bilgilendirilmiş olması esastır[1159]. Özellikle bilgisayar, e-posta ve interneti izleme olanağı tanıyan dijital izleme uygulamaları işçinin özel hayat alanına müdahale olanağı tanıdığından, izlemenin her durumda genel ilkelere uygun olması ve bir veri işleme şartına dayanması zorunludur[1160]. Ayrıca e-posta ve internet kullanımının işyerinde izlenmesinin dışında işçilerin kişisel zamanlarında bu sistemler vasıtasıyla izlenmesinin[1161] işin niteliği objektif olarak bunu gerektirmiyorsa üretkenlik, ticari sırların ifşa edilmesinin önlenmesi gibi gerekçelerle meşrulaştırılmasına olanak bulunmamaktadır[1162].

2. İşverenin Elektronik İletişime İlişkin Talimatları ve Yükümlülükleri

İşçi asli borcu olan iş görme borcunu ifa ederken işverenin kullanımına verdiği bilişim cihazlarını, elektronik iletişimi ve interneti TBK m. 396'da düzenlenmiş olan özen ve sadakat borcuna uygun ve bu sistemleri işverenin haklı menfaatlerini gözeterek özenli kullanmakla yükümlüdür. Bu yükümlülük ve iş görme borcunu işverenin TBK m. 399 kapsamında oluşturduğu talimatlara uygun yerine getirme borcu işçiye telefon, internet ve e-posta gibi iletişim araçlarıyla ilgili oluşturulan prosedürlere uymasını gerektirmektedir[1163]. Örneğin işçinin mesai

1159) İşverenin yönetim hakkının bir sonucu olarak işçiyi elektronik ortamda izlemesi ve takip etmesi her zaman mümkündür. Ancak bunun için işçinin bu izleme hakkında bilgilendirilmiş olması şarttır. İşçinin izlendiğine dair bilgilendirilmemesi veya gizlice izlenmesi, bu izleme neticesinde elde edilen veriler, iş sözleşmesinin işçi tarafından ihlal edildiğini açıkça ortaya koysa dahi, hukuka aykırı olarak kabul edilmelidir. Yargıtay 22. HD., E. 2017/21857 K. 2019/9884 T. 7.5.2019.
1160) Sevimli, [2006], Özel Yaşam, s. 199 ve 399. dipnotta atıfta belirtilen yazarlar.
1161) Gartner'ın 2018'de yaptığı bir anket araştırmasına göre büyük şirketlerin yarısından fazlası çalışanlarını izlemek için e-posta metinlerini ve sosyal medya mesajlarını analiz etmek, GPS ile izleme, biyometrik verileri işlemek gibi yöntemler de dahil olmak üzere bazı dijital izleme tekniklerini kullandıklarını ortaya koymuştur. The Future of Employee Monitoring makalesi için bkz. https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring (Erişim Tarihi: 05.01.2023).
1162) Jill Yung, "Big Brother Is Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do about It", Seton Hall Law Review, Vol. 36, No. 1, [2005], s. 165.
1163) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 227; Süzek, İş Hukuku, s. 331; Okur, [2013], Elektronik Gözetleme, s. 147.

saatlerinde interneti oyun amaçlı kullanması, uzun süreli alışveriş sitelerinde zaman geçirmesi veya e-posta adresini özel amaçlarla kullanması özen borcuna aykırılık teşkil edeceği gibi işverenin elektronik iletişimi bu amaçlarla kullanılmasını yasaklamaya dair işyeri prosedürlerine de aykırılık teşkil eder[1164]. Eklemek gerekir ki, işverenin elektronik iletişimle ilgili oluşturduğu işyeri prosedürlerini eşitlik ilkesine uygun uygulandığının ve tüm işçilere bildirildiğinin ve işçilerinin bu prosedürlerden haberdar olduğunun ispatlanması gerekmektedir[1165].

Doktrinde bir görüş işverenin mülkiyetinde olan telefon, bilgisayar, e-posta hesabı ve internet gibi uygulamaların kullanımı hakkında serbestçe karar alma yetkisine sahip olduğu ve bunların özel amaçlarla kullanmasını tamamen yasaklayabileceğini savunmuştur[1166]. Bu görüşe göre özel amaçla kullanımın yasak olduğu durumlarda işçinin mesai saatleri içinde bu araçları özel amaçla kullanmasının asli borcu olan iş görme borcunun ihlaline sebebiyet vereceğini, bu borcun sözleşmeye uygun olarak verimli bir şekilde ifa edilmesinin zorunlu olduğunu, internetin özel amaçla kullanılmasının borcun ifasını olumsuz etkileyeceğini bu sebeple özel amaçla kullanımın yasak olduğu durumlarda aksi durumu kabul edilemez bulmuştur[1167].

1164) Yargıtay işverenin açık veya örtülü izninin olmaması halinde internetin özel amaçla kullanılmasının yasak olduğu yönünde karar vermiştir. Özel amaçla kullanıma iznin yasak olduğu durumda internetin özel amaçla kullanılması halinde iş akdinin ihtara gerek olmaksızın feshedileceğine pornografik resim ve videoların indirilmesi halinde de işvereni kamuoyu nezdinde zorda bırakacağından iş akdinin feshedilebileceğine kadar vermiştir. Yargıtay 9. HD., E. 2007/27583 K. 2008/5294 T. 17.3.2008.

1165) Süzek, [2019], İş Hukuku, s. 63; Okur, [2013], Elektronik Gözetleme, s. 152; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 32.

1166) Sezgi Öktem Songu, "İşçilerin İşyerinde Özel Amaçlı İnternet ve E-Posta Kullanımına İşverenin Müdahalesi Üzerine Bir Değerlendirme", Prof. Dr. Sarper Süzek'e Armağan, Cilt I, Beta Yayıncılık, İstanbul, [2011], s. 1068-1069, (Öktem Songu, [2011], İşyerinde Özel Amaçlı İnternet); Zeki Okur, "İşyerinde İşçinin Bilgisayar ve İnternet'i Özel Amaçlı Kullanımının İş İlişkisine Etkisi" Kamu-İş, İş Hukuku ve İktisat Dergisi, C. 8, S. 2, 2005, s. 54-55; Yiğit, [2013], İşyerinde İnternet, s. 51; Okur, [2013], Elektronik Gözetleme, s. 151-152; Doktrindeki bu görüş yaklaşımını Yargıtay 9. Hukuk Dairesi'nin: "İşverenin açıkça veya örtülü izni olmaksızın işyerinde internetin özel amaçlı olarak kullanımı yasaktır. Bir başka anlatımla, örtülü veya iş sözleşmesi ile açıkça internetin özel olarak kullanabileceğine dair izin yoksa işçi işyerinde özel amaçlı olarak internet kullanamaz. Ancak bu yasak istisnaen acil durumlarda ve işine ilişkin sebeplerden dolayı meşru bir şekilde delinebilir." kararına dayandırmaktadır. Yargıtay 9. HD., E. 2007/27583, K. 2008/5294, T. 17.03.2008.

1167) Okur, [2013], Elektronik Gözetleme, s. 151.

İşyerinde internet kullanımına ilişkin katıldığımız görüş ise, işverenin işyerinde interneti tamamen kullanmaya yasaklamasının çağın gereklerine uygun olmadığıdır[1168]. Dahası böyle bir yasağın temel haklardan birisi olan haberleşme hürriyeti ve özel hayat üzerinde ölçüsüz bir müdahaleye sebebiyet vereceğini belirtmek gerekir[1169]. Kanımızca işyerinin faaliyet konusu ve işin niteliği özellikle bir yasağı gerektirmiyorsa işyerinde elektronik iletişimin özel amaçlarla tamamen yasaklanması çağımızın gereklerine uymadığı gibi iletişim hakkı üzerinde ölçüsüz bir müdahale meydana getirir. Örneğin radyoaktivite tesisleri, çok tehlikeli sınıfta faaliyet gösteren işyerleri veya özel bir formülün, yazılım kodunun korunması gibi işyerinin niteliğinden kaynaklı zorunluluk bulunduğunda işverenin elektronik iletişimi tamamen yasaklaması makul görülmeli, diğer durumlarda elektronik iletişimi tamamen yasaklaması işçinin bu temel haklarına ölçüsüz bir müdahale olarak nitelendirilmelidir[1170].

Doktrinde işverenin özel amaçla internet ve e-posta kullanımını yasaklaması halinde bu yasaklamada aksi belirtilmedikçe işyerinin tamamında geçen tüm zamanları kapsayacağı, işverenin yönetim hakkı kapsamında tasarrufta bulunurken özel amaçla kullanımın belirli zamanlarla sınırlama hakkına sahip olduğu ileri sürülmüştür[1171]. Ayrıca işverenin internet ve e-posta kullanımını şahsi kullanıma sınırlandırması iş sözleşmesi veya konuya ilişkin çıkaracağı prosedürlerle gerçekleştirilebileceği ifade edilmiştir[1172].

Belirtmek gerekir ki, internetin ve kurumsal e-posta hesabının işyeri personel yönetmeliğinde veya internet, e-posta kullanım prosedürü gibi işyeri düzenlemelerinde özel kullanıma izin verilmemesi işverenin bu vasıtalarla işleyeceği kişisel verilerde işçiyi aydınlatma yükümlülüğünü ve dijital izlemenin

1168) Doğan Yenisey, [2017], Değerlendirme, s. 510; Dursun Ateş, [2019], Yönetim Hakkı, s. 575; Öztürk, [2021], Talimatlara Uyma, s. 364; Ugan Çatalkaya, [2019], Ölçülülük, s. 349-350.
1169) Öztürk, [2021], Talimatlara Uyma, s. 365; Ugan Çatalkaya, [2019], Ölçülülük, s. 349-350.
1170) Okur, [2013], Elektronik Gözetleme, s. 152.
1171) Nağme N. Hozar, "Özel Amaçla İnternet ve E-Posta Kullanımının İş İlişkisine Etkisi", Sicil İş Hukuku Dergisi, S. 7, [2007], s. 203.
1172) Öktem Songu, [2011], İşyerinde Özel Amaçlı İnternet, s. 1068-1069.

KVK hukuku hukuka uygunluk ölçütlerine uygun olması gerekliliğini ortadan kaldırmamaktadır. Aksi durum gizli izleme olarak nitelendirilebileceğinden hukuka aykırı veri işleme faaliyeti ortaya çıkacaktır. Kanaatimizce, AİHM Büyük Daire'nin gizli kamera gözetlemesine ilişkin oluşturduğu ilkeleri[1173] internet iletişiminin gizli izlenmesinde uygulanması mümkündür. Bu durumda bir suçun önlenmesi amacıyla başkaca daha az müdahaleci bir yöntemle gerçekleştirilmesine imkan bulunmadığı durumlarda, sınırlı bir süre, başka amaçlarla kullanmamak kaydıyla, suç şüphesiyle sınırlı olacak şekilde internet iletişim ve e-posta izlemesi gerçekleştirilebilir.

Elektronik iletişimin sınırlandırması ve dijital izleme ile izlenmesini KVK hukuku açısından değerlendirdiğimizde mülkiyetin işverene ait olması işverene elektronik iletişim araçlarını dilediği gibi izleyeceği ve yasaklayacağı sonucuna ulaşmak mümkün değildir. Zira KVKK m. 28/2-a'da yer alan "kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması" düzenlemesi dışında her durumda KVK hukuku, hukuka uygunluk ölçütlerine uygun (AİHM Büyük Daire, Bărbulescu & Romanya Kararı'nda "tam olarak bilgilendirme" ifadesi kullanılmıştır) bir veri işleme sürecinin oluşturulması zorunludur[1174]. Dahası işçinin internete erişiminin ve iletişim hakkının temel bir insan hakkı olduğu kabul edilmektedir[1175]. Eklemek gerekir ki, işveren tarafından işçinin kullanımına tahsis edilmiş kurumsal e-posta adresi de kişisel veridir[1176]. Zira, KVKK m. 3/d bendinde yer alan kişisel veri tanımı karşısında işçiyi belirli veya belirlenebilir hale getiren e-posta adresi, özel yazışmaları, dijital izleri gibi doğrudan veya dolaylı her veri kişisel veri niteliğine haizdir[1177].

1173) Bkz. § 7.II.2.b. aa.
1174) Elbir, [2020], İşçiye Ait Kişisel Veriler, s. 98.
1175) Melda Sur, "Çalışanın E-Postasına İşveren Tarafından Girilmesi", Sicil İş Hukuku Dergisi, Sayı 44, [2020], s. 59, (Sur, [2020], Çalışanın E-Postası); H. Burak Gemalmaz, "Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır?: AİHM Büyük Dairenin 05 Eylül 2017 Tarihli Barbulescu Kararı", [2017], https://blog.lexpera.com.tr/calisanlarin-internet-iletisiminin-isverence-izlenmesi-ozel-yasam-hakkina-aykiri-midir-aihm-buyuk-dairenin-05-eylul-2017-tarihli-barbulescu-karari/ (Erişim Tarihi: 16.12.2022)
1176) Bkz. Kişisel Verileri Koruma Kurulu'nun 25/11/2021 tarihli ve 2021/1187 sayılı Karar Özeti, Karar Tarihi: 25/11/2021, Karar No: 2021/1187.
1177) Bkz. Kişisel Verileri Koruma Kurulu'nun 25/11/2021 tarihli ve 2021/1187 sayılı Karar Özeti, Karar Tarihi: 25/11/2021, Karar No: 2021/1187.

İşveren işçilerin elektronik iletişim araçlarını ve uygulamalarını özel amaçlı kullanımına açık veya zımni olarak[1178] izin verebilir. Zira işveren mülkiyet hakkı kendisinde bulunan bu araçların özel amaçlarla kullanılmasına ilişkin hakkını kullanmaktadır[1179]. İşveren elektronik iletişim araçlarının özel amaçlarla kullanılmasına ilişkin izni iş sözleşmesinde, toplu iş sözleşmesinde veya işyeri prosedürlerinde ilan edebilir. Zımni izin ise bilgisi dahilinde bulunan özel

1178) Danıştay İdari Dava Daireleri Kurulu icra müdürlüklerine kurulan kamera sistemlerinin çalışanların özel hayatına müdahale oluşturduğu yönünde açılan davada davanın reddini AİHM Büyük Daire, Lopez Ribalda v. İspanya kararına atıf yaparak reddetmiştir. Kararda "Avrupa İnsan Hakları Mahkemesi içtihatlarında da ifade edildiği üzere, müdahalenin kamusal alanda vuku bulduğu hallerde dahi, bir kimsenin kamusal alanda "özel hayatın gizliliğine makul saygı beklentisi" söz konusu ise, özel hayatın gizliliğinin ihlalinden söz etmek mümkündür. (AİHM, Alpha Doryforiki Tileoraisi Anonymi Etairia/Yunanistan, Başvuru No: 72562/10, 22/02/2018, Paragraf No: 64; AİHM, Lopez Ribalda/İspanya, Başvuru No: 1874/13 ve 8567/13, 17/10/2019, Paragraf No: 89) Bununla birlikte, bu beklentiden söz edilemediği durumlarda, kamusal alandaki müdahalelerin özel hayatın gizliliğini sınırlandırdığı kabul edilmemelidir… Davaya konu kamera sisteminin kurulduğu icra daireleri, kamu hizmeti niteliğinde bulunan icra iş ve işlemlerinin yürütüldüğü yerler olup, bu dairelere iş takibi dolayısıyla alacaklı, borçlu ve tüm ilgililer giriş çıkış yapabilmektedir. Bu niteliği itibarıyla, kamu hizmetinin yürütüldüğü binalardan olan icra dairelerinin "kamuya açık", kamu binası niteliğinde olduğu hususunda tartışma bulunmamaktadır. Kamu hizmetlerinin yürütüldüğü ve kamu görevlilerinin kendilerine verilen görevleri ifa ettiği tüm kamu binalarında olduğu gibi, davalı idarenin anılan yerde gözetim ve denetimi sağlama görevi bulunduğu gözetildiğinde, icra dairelerinin buralarda görev yapan personel de dahil olmak üzere, herkes yönünden kamusal alan vasfında olduğu anlaşılmaktadır. Dolayısıyla, kural olarak bu alanlarda vuku bulan müdahaleler yönünden "özel hayatın gizliliğine makul saygı beklentisi" söz konusu değilse, özel hayatın gizliliğinin sınırlandırılmasından söz etmek hukuken mümkün değildir. Avrupa İnsan Hakları Mahkemesinin yukarıda değinilen kararında ortaya konulan temel yaklaşım doğrultusunda, somut olay bakımından icra dairesi personelinin özel hayatın gizliliğine makul saygı beklentisi irdelenirken, anılan alanların kamera ile izlenmesi tedbirinin meşru bir amaca dayanıp dayanmadığı önemli bir etken teşkil etmektedir. Bu çerçevede, dava dosyasında bulunan bilgi ve belgelere bakıldığında; Ankara İlinin nüfusunun fazla olması ve merkezde tek adliyenin bulunması, icra müdürlüklerine giriş çıkış sirkülasyonunun çok fazla olması, icra müdürlüklerinde çalışma ve işleyiş konusu itibarıyla icra personeli ve vatandaş arasında zaman zaman tartışma yaşanması, "rüşvet, görevi ihmal, görevi kötüye kullanma, alacaklı ile borçlu arasındaki tehdit, korku ve panik uyandıracak şekilde baskı yapma, iş takipçiliği" gibi konusu suç teşkil eden şikâyetlerin vuku bulması ve bu şikâyetlerin artmış olması gerekçelerine istinaden icra dairelerine kamera takip sistemi yerleştirildiği, muhtelif zamanlarda icra kasalarından para çalınması ve icra dosyalarındaki evrakın kaybedilmesi gibi eylemlerin meydana geldiği, bu eylemler nedeniyle icra personeli hakkında adli ve idari yaptırımların uygulandığı görüldüğünden, davalı idarenin meşru bir amaç doğrultusunda icra dairelerinde kamera ile izleme tedbirini uyguladığı sonucuna ulaşılmaktadır. Diğer yandan, davacı tarafından "makam odasının" kamera ile izlenmesinden bahsedilmekte ise de; dosyada yer alan bilgi ve belgeler incelendiğinde, icra müdürlerinin icra dairelerinde iş takibi dolayısıyla tüm ilgililerin giriş çıkış yapabildiği bölümde açık ofis şeklinde çalışma masalarının bulunduğu, bu alanın ayrı ve özel bir çalışma ofisi ya da makam odası olarak nitelendirilmeyeceği, dolayısıyla bu kısımlar yönünden de icra müdürlerinin veya ilgili personelin 'özel hayatın gizliliğine makul saygı beklentisi'nin yüksek olduğundan söz edilemeyeceği anlaşılmaktadır." Danıştay İDDK., E. 2021/1603, K. 2021/2631 T. 24.11.2021; Yargıtay yaklaşımı için bkz. Yargıtay 9. HD., E. 2007/27583 K. 2008/5294 T. 17.3.2008.

1179) Okur, [2013], Elektronik Gözetleme, s. 154.

kullanıma uzun bir süre ses çıkarmama şeklinde gerçekleşebilir[1180]. Her durumda işçi elektronik iletişim araçlarını özel amaçlarla kullanırken özen ve sadakat borcuna uygun davranmak, işverenin haklı menfaatlerini korumak ve işi aksatmamak, işyeri düzenini bozmamakla yükümlüdür. Aksi durumda gerçekleşen özel kullanım iş sözleşmesinin ortaya çıkardığı işçinin borçlarına aykırı olacaktır[1181]. Ayrıca belirtmek gerekir ki, işveren özel amaçlarla kullanımı zaman, uygulama, kullanım yeri, şekli gibi sınırlamalara tabi tutabilir[1182]. Örneğin işveren dinlenme aralarında interneti özel amaçlarla kullanıma izin verirken işçinin kullanımına verdiği e-posta hesabının kullanımını tamamen özel kullanıma kapatabilir.

İşverenin özel amaçla kullanıma izin vermesi halinde işçinin bilgisayar, e-posta, Teams, internet arama geçmişi, serbest zaman aktiviteleri, elektronik iletişim araçlarını kullanım alışkanlıkları gibi özel hayatının gizliliğini ilgilendiren ve iş ilişkisiyle de ilgisi bulunmayan kişisel veriler bu sistemlerde işlenebilecektir. Bu durumda işverenin aydınlatma yükümlülüğü ve açık rıza kapsamında işlediği verilerde ikili bir ayrıma gitmesi gerekir. İşle ilgili olanların izlenmesi, işlenmesi mümkünken işçinin özel alanında kalan verilerin işlenmesi hukuka aykırı olacaktır. Bu itibarla işveren elektronik iletişim araçlarını özel kullanım izni verdiğinde işçinin özel hayatına saygı duyulacağına ilişkin makul beklentisini karşılayacak bir yapı oluşturmakla yükümlüdür. Aksi durumda işçi aldatılmış olur ve özel hayatının gizliliği üzerinde orantısız bir müdahale gerçekleştirmiş olur[1183].

3. Elektronik İletişim Araçlarının İzlenmesine İlişkin AİHM ve AYM Yaklaşımı

İşverenin üstün özel yararı hukuka uygunluk sebebi açısından olaya

1180) Yargıtay 9. HD., E. 2007/27583 K. 2008/5294 T. 17.3.2008; Okur, [2013], Elektronik Gözetleme, s. 154-155.
1181) Okur, [2013], Elektronik Gözetleme, s. 155.
1182) Okur, [2013], Elektronik Gözetleme, s. 160.
1183) Okur, [2013], Elektronik Gözetleme, s. 163.

bakıldığında bu sistemleri kötüye kullanmasını önleme açısından işverenin haklı bir menfaatinin bulunduğu kabul edilse dahi telefon, bilgisayar, e-posta, Skype, Zoom ve interneti izleyen uygulamalardan elde edilen verilerin haklı fesih gibi durumlarda hukuken kullanılabilmesi için hukuka uygunluk ölçütlerinin bulunduğu bir kişisel veri işleme faaliyeti yürütmüş olması gerekir[1184].

Tez konusu açısından önemli bir örnek olan Alman Federal İş Mahkemesi'nin[1185] önüne gelen bir olayda, davalı işveren yeni ve hızlı bir internet bağlantısıyla ilgili tüm işçilere bir e-posta göndermiş Wi-Fi erişiminin ücretsiz olduğunu, yasadışı filmlerin indirilmesi vb. durumlarda işverenin sorumlu tutulması gerekçesiyle tüm internet trafik ve kayıtlarının izleneceğini, yasaya aykırılığın sorumluluğun ilgili işçiye yükletileceği bildirilmiştir. Daha sonra işyerinde gerçekleştirilen bir toplantıda hiçbir işçi internet erişiminin kötüye kullanılmasını engellemek için işverenin tüm internet trafiğinin kaydedilmesi kararına itiraz etmemiştir. İşveren sonrasında davacı işçinin bilgisayarına tüm klavye hareketlerini kaydeden ve düzenli olarak ekran görüntüleri alan bir yazılım (Keylogger) yüklemiştir. İşveren bu yazılımın gerçekleştirdiği kayıtları incelerken davacı işçinin babasının lojistik şirketi için bilgisayar yazılımı programladığı ve e-posta trafiğini yönettiği verisine ulaşmıştır. Davacı işçi bu veriden ortaya çıkan bilgileri kabul etmiştir. İşveren bu tespit sonrası işçinin iş akdini haklı sebeple feshetmiştir. Alman Federal İş Mahkemesi bir klavye yakalayıcısının zamanlama sınırlaması olmaksızın gizli kullanılmasını işçinin kişilik haklarına yönelik ihlalinin yoğunluğu açısından gizli video izlemesiyle karşılaştırılabilecek boyutta bir veri işlemeyi ve ihlali barındırdığını, bir klavye yakalayıcısı aracılığıyla veri toplanmasının, veri sahibinin işlenen verileriyle ilgili bilgi edinme hakkına büyük bir müdahale gerçekleştirdiğini tespit etmiştir. BAG'a göre, Keylogger yazılımının

1184) Bkz. § 6.

1185) Alman Federal İş Mahkemesi - BAG 2 AZR 681/16, § 32-33. Kararın tamamı için bkz. https://www.bundesarbeitsgericht.de/entscheidung/2-azr-681-16/ (Erişim Tarihi: 12.03.2023) Alman Federal İş Mahkemesi (BAG) 27 Temmuz 2017'de görülen bir davada Keylogger yazılımının işçilerin izlenmesi amacıyla gizli kullanımının veri koruma yasasını ihlal ettiğine ve bu tür izleme yoluyla elde edilen bulguların mahkeme işlemlerinde delil olarak kullanılamayacağına karar verdi (BAG 2 AZR 681/16).

bir iş ilişkisinde gizli kullanılması ancak izlemeye konu işçinin bir suç işlemesi veya başka bir ciddi görev ihlali yapmasına dair özel bir şüphenin bulunması halinde mümkündür[1186].

Anayasa Mahkemesi, sözleşmeli astsubay olarak çalışan bir kamu çalışanına ilişkin verdiği kararda, asker olan kamu görevlisinin kurum içi hizmette görevini ifa için kamunun tahsis ettiği interneti ve e-posta hesabını görev harici işlerde kullanması, sosyal amaçlı mesajlar göndermesi, e-posta hesabında tur ve gezi organizasyonları düzenlemesi amacıyla kullanması sebebiyle dokuzuncu yılın sonunda sözleşmesinin uzatılmamasını "özel hayata saygı hakkına ölçüsüz bir müdahale" olarak değerlendirmiştir. Kararda kurum içinde görevin ifası için tahsis edilen telefon, internet ve e-postanın izlenmesinin, belirli ölçülere göre kontrol edilmesinin temel hak ve özgürlüklerin ihlaline sebebiyet vermeyeceği tespit edildikten sonra, kişinin temel hak ve özgürlüklerine ölçüsüz müdahalenin de Anayasa m. 20'de güvenceye alınmış olan özel hayatın gizliliğinin ihlali anlamına geleceğine karar vermiştir[1187].

AYM'nin kararına konu olan bir diğer olayda gayrimenkul değerlendirme uzmanı olarak çalışan işçinin iş sözleşmesi; verilen işleri hatırlatılmasına rağmen süresinde yapılmaması, sık sık rapor alınması, savunma isteminin akabinde rapor almasına rağmen sosyal medya hesabından yapılan paylaşımlardan Bodrum'da tatilde olduğunun anlaşılması, bunun doğruluk, dürüstlük ve bağlılıkla bağdaşmadığı ileri sürülerek, İş Kanunu m. 25/II (h) ve (e) alt bentleri kapsamında haklı sebeple feshedilmiştir. Başvurucu 12.10.2017 tarihinde İstanbul Anadolu 3. İş Mahkemesinde işe iade istemiyle dava açmıştır. Dava dilekçesinde iş akdinin haklı sebebe dayanmaksızın feshedildiği ve feshe dayanak yapılan olguların gerçekle bağdaşmadığı, işverenin fesih hakkını kötüye kullandığı, kötü niyetli

1186) Alman Federal İş Mahkemesi - BAG 2 AZR 681/16, § 33.
1187) AYM, Genel Kurul, Tevfik Türkmen kararı Başvuru No: 2013/9704, 3/3/2016; Şen/Barın, [2021], Özel Hayata Saygı, s. 58-59; AYM, E.Ü. kararında (2016/13010 Başvuru No, 27.06.2020 karar tarihi, R.G. Tarih ve Sayı: 14/10/2020-31274); AYM. 21/1/2015 Tarih ve Başvuru No: 2013/9660 sayılı Serap Tortuk kararı.

hareket ederek psikolojik taciz uyguladığı ifade edilmiştir[1188].

İşveren cevap dilekçesinde, başvurucunun doğruluk ve bağlılığa uymayan davranışlarda bulunduğunu, işverenin güvenini kötüye kullandığını, sıkça rapor aldığını, rapor aldığı günlerde istirahat yerine şehir dışına tatile çıktığını, raporların gerçeğe aykırı alındığının başvurucu tarafından şirket mailinden gönderdiği 21.06.2017 tarihli e-postada ikrar edildiğini, raporlu olduğu dönemde tatil planları yaptığını, otel planı ve ödeme kayıtlarının aynı e-posta hesabı ile paylaşıldığını, işten ayrılmadan önce şirket raporlarını şirket dışına aktardığını, kendisine defalarca hatırlatılmasına rağmen işverenin zararına olacak biçimde hareket ettiğini, kasten görevlerini yapmamakta ısrar ettiğini, bunun şirketin itibarına ve müşterileri nezdindeki güvenine zarar verdiğini ileri sürmüştür[1189].

İş mahkemesi dosyada insan kaynakları uzmanı olan bilirkişiden rapor almıştır. Raporda, ağız ve diş sağlığı merkezinden alınan rapor tarihleriyle örtüşecek şekilde iş bilgisayarındaki tatil fotoğraflarının 20.02.20216 tarihine ait olduğu, 05.03.2017 tarihinde şirketin belgelerinin daha önce şirketten ayrılan bir müdüre yine şirket mail adresini kullanarak gönderdiği, başvurucunun imzasının taşıyan iş sözleşmesinin 9. maddesinde sır saklama yükümlülüğüne ilişkin düzenleme bulunduğu ve sözleşmenin ekinde ayrıca gizlilik sözleşmesinin bulunduğu, başvurucunun verilen sürelerde kendisine verilen görevleri yapmadığı, bu sebeple amirleriyle sorun yaşadığı, raporlar sebebiyle müşterilerden şikayetlerin arttığı tespit edilmiştir. Bu kapsamda mahkeme fesih gerekçesindeki hususların ispatlandığını ve İş Kanunu m. 25/II'deki koşulların oluştuğunu tespit ederek davanın reddine karar vermiştir. Karar, başvurucu tarafından istinaf incelemesine götürülmüş ve İstanbul Bölge Adliye Mahkemesi 25. Hukuk Dairesi 04.03.2020 tarihinde "ilk derece mahkemesi kararının objektif ve dosyadaki verilerle çelişmeyen tespitlerine, kararın dayandığı deliller, delillerin takdiri ve karar

1188) AYM, Esin Ağar kararı, Başvuru Numarası: 2022/23522, Karar Tarihi: 15.11.2023, § 2-3.
1189) AYM, Esin Ağar kararı, Başvuru Numarası: 2022/23522, Karar Tarihi: 15.11.2023, § 4.

gerekçesine göre istinaf başvurusunun esastan reddine" kesin olarak karar vermiştir. Başvurucu kararı 14.06.2020 tarihinde tebliğ aldıktan sonra 16.07.2020 tarihinde AYM nezdinde bireysel başvuru talebinde bulunmuştur[1190].

Başvurucu bireysel başvurusunda işyerinde kullandığı bilgisayarındaki resimlerin silinmesine izin verilmediğini, kişisel fotoğraflarının özel hayata saygı hakkını ihlal edecek biçimde işe iade davasına delil olarak sunulduğunu, özel hayata saygı hakkı kapsamındaki kişisel verilerinin korunmasını isteme hakkının ve adil yargılanma hakkının ihlal edildiğini ileri sürmüştür. AYM, başvuruyu işyeri bilgisayarında elde edilen fotoğrafların işe iade davasında delil olarak kullanılıp kullanılmayacağı temelinde ele almıştır. AYM, işveren tarafından tahsis edilen bilgisayarda bulunan fotoğrafların kişisel veri kapsamında bulunduğunu, bunlara "erişilmesinin, kullanılmasının ve işlenmesinin" özel hayata saygı hakkı kapsamında olduğunu tespit ederek, olayı özel hayata saygı temelinde, kişisel verilerin korunmasını isteme hakkı yönünden incelemiştir[1191].

AYM, işçinin özel hayata saygı hakkını ve kişisel verilerinin korunmasını daha önce vermiş olduğu kararlar kapsamında: "somut olayın koşullarına göre iş sözleşmelerinde kısıtlayıcı ve zorlayıcı düzenlemelerin ne şekilde belirlendiği, tarafların bu düzenlemeler hakkında bilgilendirilip bilgilendirilmediği, çalışanların temel haklarına yönelik müdahalede bulunulmasına neden olan meşru amacın müdahale ile ölçülü olup olmadığı, sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı hususlarının uyuşmazlığın çözümünde gözetilmesi" gerektiği biçiminde tespit edilmiştir (Ömür Kara ve Onursal Özbek, B. No: 2013/4825, 24/3/2016, § 50; E.Ü., [GK], B. No: 2016/13010, 17/9/2020, § 67; Samet Ayyıldız, B. No: 2018/34548, 28/12/2021, § 32). Kararda işverenin, işçinin kullanımına tahsis ettiği bilgisayarı, e-posta hesabı verilerini, WhatsApp içeriğinin izlenebilmesinin ölçütleri önceki kararlara atıf

1190) AYM, Esin Ağar kararı, Başvuru Numarası: 2022/23522, Karar Tarihi: 15.11.2023, § 6-7.
1191) AYM, Esin Ağar kararı, Başvuru Numarası: 2022/23522, Karar Tarihi: 15.11.2023, § 11.

yapılarak açıklanmıştır[1192].

Sonuç olarak AYM, Esin Ağar kararında, işyeri bilgisayarında yer alan başvurucuya ait tatil fotoğraflarının kişisel veri olduğunu, şirket mailinde yer alan özel yazışmaların kişisel veri olduğunu, yerel mahkemenin bu hususta bir değerlendirme yapmamasına rağmen iş sözleşmesinin feshine ilişkin temel sebebin başvurucuya tahsis edilen bilgisayardaki fotoğraflara dayanmadığını tespit etmiştir. Ayrıca başvurucunun talimatlara riayet etmemesi, savunma yazısının hemen sonrasında rapor alması, raporları süresinde teslim etmemesi, raporun hemen sonrasında işyerine gelmeyerek sosyal medya hesabı üzerinden Bodrum'dan fotoğraf paylaşımının bulunduğunun mahkeme tarafından tespit edildiği ifade edilmiştir. Bu bağlamda mahkemelerin gerekçelerinin yeterli olduğu, bütün deliller temin edilerek pozitif yükümlülüğünün yerine getirildiği ve olayda Anayasa m. 20'de güvenceye alınan özel hayata saygı hakkı kapsamındaki kişisel verilerin korunmasını isteme hakkının ihlal edilmediğine karar vermiştir[1193].

AİHM Büyük Daire, Bărbulescu & Romanya[1194] kararı işçilerin iş ilişkisinde bilgisayar, internet, e-posta ve anlık iletişim uygulamalarını kullanmalarının ve bunların izlenmesinin ilkeleri hususunda önemli tespitlerin yapıldığı bir karardır. Karara konu olayda Bărbulescu, Romanya'da özel bir şirkette satış mühendisi olarak çalışırken işverenin talebine uygun olarak, müşterilerin sorularını cevaplamak için bir Yahoo Messenger hesabı oluşturmuştur. Bărbulescu işyeri bilgisayarının özel işleri için kullanmayacağına ilişkin yasakları içeren işyeri iç prosedürlerini 2006 ve 2007'de imzalamıştır. Temmuz 2007'deki prosedür ve bildirimde ayrıca işverenin işçilerin çalışmalarını denetleme ve izleme hakkı bulunduğu yazılmıştır. 13 Temmuz 2007 tarihinde işveren, Bărbulescu'ya Yahoo Messenger iletişiminin izlendiğini ve internet

1192) AYM, Esin Ağar kararı, Başvuru Numarası: 2022/23522, Karar Tarihi: 15.11.2023, § 13-14.

1193) AYM, Esin Ağar kararı, Başvuru Numarası: 2022/23522, Karar Tarihi: 15.11.2023, § 17-19.

1194) AİHM, [GK], [2017], Bărbulescu v. Romanya, Başvuru no. 61496/08, 5 Eylül 2017 kararının detayları için bkz. https://hudoc.echr.coe.int/fre?i=001-177082 (Erişim Tarihi: 24.12.2022).

etkinliğinin arkadaşlarına kıyasla fazla olduğu ve bunu kişisel iletişim, kardeşi ve nişanlısı ile yazışmak için kullandığına dair kanıtların bulunduğu bildirilmiş ve iş akdi bu sebeple 1 Ağustos 2007 tarihinde feshedilmiştir[1195].

Bărbulescu, elektronik iletişiminin hukuka aykırı izlendiğini, kanunlara aykırı davranıldığını ileri sürerek dava açmış ve yerel mahkeme işverenin eylemlerinin ceza hukuku kapsamında yasa dışı olup olmadığının disiplin kovuşturmasının geçerliliğini belirlemede önemli olmadığına kanaat getirerek davayı reddetmiştir. Bărbulescu, işverenin çıkarlarının işçinin özel hayatının gizliliğinin korunması hakkından üstün tutulduğunu ileri sürerek istinafa gitmiş, istinaf ve temyizde farklı bir sonuç çıkmamıştır[1196].

Bărbulescu, Romanya'ya karşı AİHM'e, AİHS m. 8 kapsamında başvuruda bulunmuş AİHM 4. Daire 12 Ocak 2016 tarihli kararında işverenin yalnızca müşterilerle iletişim kurması için Yahoo Messenger hesabı açılmasını talep ettiği, işverenin işçinin bu amaçla açtığı hesabını incelemesinin AİHS m. 8'e aykırılık teşkil etmeyeceği yönünde karar ermiştir. Bu kararda Hakim Pinto de Albuquerque önemli tespitler içeren kısmi karşı oy kaleme almıştır. Karşı oyda özellikle işveren tarafından gereği gibi açıklanan ve uygulanan bir internet izleme politikasının bulunmadığını, işverenin erişim sağladığı ortamın kişisel olma ihtimali ve hassas yapısı gereği daha dikkatli davranılmasını, internete erişimin insan hakkı olduğunu ve işyerinde internetin izlenmesinin sadece işverenin takdir yetkisinde bulunamayacağını ileri sürmüştür.

AİHM Büyük Daire, anlık iletişimi yazışma olarak değerlendirmiş ve işçinin "makul bir mahremiyet beklentisinin" bulunduğuna vurgu yapmıştır[1197]. Büyük Daire, devletin AİHS m. 8 kapsamında pozitif yükümlülükleri bulunduğunu vurgulayarak özel hukuk kişileri arasında da kişisel verilerin ve özel hayatın

1195) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 16-23.
1196) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 24-30.
1197) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 80-81.

gizliliğinin korunması yönünde yükümlülükleri bulunduğu emsal AİHM kararları kapsamında değerlendirmiştir[1198].

Büyük Daire, devletlerin işçilerin dijital izlenmesine ilişkin olarak bir dizi faktörü dikkate almaları gerektiğini tespit etmiştir. Bunlar; işçinin iletişiminin işveren tarafından izlenebileceği olasılığı konusunda bilgilendirilip bilgilendirilmediği, izlemenin kapsamı ve işçinin özel hayatına müdahalenin derecesi, işverenin izlemeyi haklı çıkarmak için meşru sebepler sunup sunmadığı, daha az müdahaleci yöntemlere dayalı bir izleme sistemi kurmanın mümkün olup olmayacağı, dijital izlemeye tabi işçi için izlemenin sonuçlarının ve işçiye yeterli güvencelerin sağlanıp sağlanmadığının ortaya konması gerekir[1199].

Büyük Daire aynı zamanda devletlerin iletişimleri izlenen işçilere, ilgili kriterlerin yerine getirilip getirilmediğini ve söz konusu önlemlerin yasal olup olmadığını belirleme yetkisine sahip yargı organı önünde bir hukuk yoluna erişim sağlama yükümlülüğüne sahip olduğunu tespit etmiştir[1200]. Ayrıca yerel mahkemelerin tespit edilen ilkelere uygun yargılama gerçekleştirip gerçekleştirmediği de incelemeye konu edilmiş ve yerel mahkemelerde gerçekleştirilen incelemelerde iletişimin izlenmesini haklı gösterecek meşru sebeplerin olup olmadığına dair yeterli değerlendirme yapılmadığına ilişkin bazı bulgular tespit etmiştir[1201]. Büyük Daire bu nedenlerle, altıya karşı on bir oyla, Romanya'nın, AİHS m. 8'de düzenlenen özel hayatına ve haberleşmesine saygı gösterilmesi hakkına ilişkin olarak başvurucuya yeterli koruma sağlamadığı ve sonuç olarak söz konusu menfaatler arasında adil bir denge kurulmadığı sonucuna varmıştır[1202].

AİHM Büyük Daire bu kararda özetle işverenin işçinin işyerindeki

1198) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 114-115.
1199) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 121.
1200) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 121.
1201) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 135-140.
1202) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 141.

iletişimini denetleme hakkı bulunduğu, fakat iletişimin dijital izlemeye tabi tutulması için işçinin önceden izlemenin boyutu hakkında tam olarak bilgilendirilmesi gerektiğine karar vermiştir[1203]. KVK Kurulu da işçinin e-posta iletişiminin işveren tarafından izlenmesi ve denetlenmesine ilişkin verdiği 2023/86 sayılı kararında AİHM Büyük Daire'nin Bărbulescu & Romanya kararında işverenin işçinin iletişimini izleyebilmesi için ortaya koyduğu ölçütlere atıf yaparak bu yükümlülükleri yerine getiren işverenin işçinin iletişimini izleme ve denetleme hakkı bulunduğuna karar vermiştir[1204].

Doktrinde işverenin, işçilere tahsis ettiği kurumsal e-posta adresini şahsi kullanıma yasaklaması durumunda tüm e-postaların karine olarak iş e-postası olarak kabul edilmesinin bir gereği olarak işveren tarafından e-postaların içeriğinin denetlenebileceği görüşündedir[1205]. Bu durumda sadece özel olduğu belirtilen e-postaların içeriğinin denetlenemeyeceği işaret edilmiştir[1206]. Katıldığımız görüşe göre e-posta adresi ve internet işverene ait olsa dahi işverenin e-posta içeriklerine ulaşabilmesi için aydınlatma yükümlülüğüne uygun tam bilgilendirmenin yapılmış olması ve diğer veri işleme şartları yoksa işçinin açık rızalarının alınmış olması gerekir[1207]. Konu kısmına "özel" olduğu ifadesi yer alan e-postalar ise ancak suç şüphesinin bulunması ve daha az müdahaleci bir yöntemin bulunmaması durumunda açılıp okunması mümkündür. Belirtmek gerekir ki, aksi durumda işçi her e-postaya özel ifadesini ekleyerek bu durumu kötüye de kullanabilir.

Kanaatimizce işçinin işyerinde makul bir özel hayat beklentisi

---

1203) Gülay Arslan Öncü, Özel Yaşama ve Aile Yaşamına Saygı Hakkı, Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-8, Avrupa Konseyi Ankara Program Ofisi, 2019, s. 145; AİHM, [GK], [2017], Bărbulescu v. Romanya, § 124-141.
1204) Bkz. Kişisel Verileri Koruma Kurulu'nun 19/01/2023 tarihli ve 2023/86 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7593/2023-86 (Erişim Tarihi: 07.04.2023).
1205) Okur, [2013], Elektronik Gözetleme, s. 171.
1206) Okur, [2013], Elektronik Gözetleme, s. 171-172.
1207) Sur, [2020], Çalışanın E-Postası, s. 59; Sevimli, [2006], Özel Yaşam, s. 206-208; Gürsel, [2016], İşçinin Kişisel Verileri, s. 386-390.

bulunduğu[1208] kabul edilmeli, elektronik iletişimin izlenmesiyle gerçekleşen kişisel veri işleme faaliyeti özel hayata müdahaleye dönüştürülmemelidir. Dahası her durumda kişisel verilerinin işlenebilmesi için KVK hukukunda öngörülen hukuka uygunluk ölçütlerine uygun bir veri işleme faaliyetinin oluşturulması zorunludur[1209]. Örneğin suçun önlenmesi söz konusu değilken iletişimin gizli izlenmesi, işçinin tüm internet izlerinin kayıt altına alınması, özel iletişiminin dinlenmesi ve işlemeye konu edilmesi işçinin özel hayatı ve kişisel verileri üzerinde açık bir ihlal ortaya çıkaracaktır[1210].

1208) Gürsel, [2016], İşçinin Kişisel Verileri, s. 22-23; Kambellari, [2014], Employee Email Monitoring, s. 1-2.
1209) KVK Kurumu, [2019], Uygulama Rehberi, s. 74; KVK Kurumu, Kişisel Verilerin İşlenme Şartları Rehberi, s. 2-3, https://www.kvkk.gov.tr/Icerik/4190/Kisisel-Verilerin-Islenme-Sartlari (Erişim Tarihi: 22.12.2022).
1210) Ugan Çatalkaya, [2019], Ölçülülük, s. 349-350; Savaş, [2009], Siber Gözetim, s. 117.

ÜÇÜNCÜ BÖLÜM
DİJİTAL İZLEMENİN HUKUKİ SONUÇLARI

§ 8. DİJİTAL İZLEMENİN İŞ İLİŞKİSİNDEKİ SONUÇLARI

İşverenin dijital izleme uygulamalarıyla işçiyi izlemesi ve kişisel verilerini işleme faaliyetine konu etmesi izlemenin hukuka uygunluk ölçütlerine[1211] uygunluğu ile hukuka aykırılığı açısından taraflar yönünden iş sözleşmesinin feshi, kişiliği koruyan davalar, şikayet ve zararın tazmine konu edilmesi biçiminde sonuçlar ortaya çıkarmaktadır.

I. Hukuka Uygun Dijital İzlemenin Sonuçları

KVK hukuku açısından hukuka uygunluk değerlendirmesi yapılırken genel düzenlemelerden farklı olarak veri sorumlusu tarafından gerçekleştirilen kişisel veri işleme faaliyetinin verisi işlenen ilgili kişinin beklemediği ve beklenmesinin de kendisinden istenmeyeceği sonuçların ortaya çıkmasını engelleyecek biçimde hareket etme yükümlülüğü olduğu kabul edilmektedir[1212]. Bu yükümlülük veri sorumlusu işverene, KVKK düzenlemelerinde öngörülen usul ve esaslar uygun dijital izleme uygulaması kullanmasını zorunlu kılmaktadır. Bu başlıkta hukuka uygun dijital izlemenin iş ilişkisindeki sonuçları ele alınacaktır.

1. Hukuka Uygun Dijital İzlemeye İşçinin Uyma Yükümlülüğü

İşçi, işverenin hukuka uygun gerçekleştirdiği dijital izleme uygulamalarına uymakla yükümlüdür. Zira talimatlara uyma borcu işçinin iş sözleşmesinden doğan bir borcudur. İşveren yönetim hakkı kapsamında işçinin denetlenmesine, korunmasına ve risklerden uzaktan durmasını sağlamaya yönelik dijital izleme

1211) Bkz. § 6.
1212) KVK Kurumu, [2019], Uygulama Rehberi, s. 64-65.

uygulamaları kullanma hakkına sahiptir. İşçinin talimatlara uygun davranma borcu TBK m. 399 hükmünde "düzenlemelere ve talimatlara uyma borcu" başlığında düzenleme altına alınmıştır. Ayrıca talimatlara uyma borcu bağımsız bir borç olmayıp, iş görme borcu kapsamında bulunduğundan işçinin buna aykırı hareket etmesi iş görme borcunun ihlali olarak nitelendirilir[1213]. İşçinin talimatlara uyma borcu iş sözleşmesinin bağımlılık unsuruyla birlikte düşünüldüğünde, işçinin bu borcunun iş sözleşmesinin niteliğini belirlemede yardımcı dayanaklar sunduğu görülmektedir[1214].

Genel olarak işverenin çalışma koşulları, işçinin ücreti ile çalışma süresi üzerinde yönetim hakkına dayanarak talimatla düzenleme gerçekleştirme hakkı bulunmadığı, bunun dışındaki işin görülme biçimi, günlük çalışmanın başlangıç - bitişini, araç - gereç kullanımını, işin ifa edileceği yeri belirleme hakkına sahip olduğu kabul edilmektedir[1215]. İncelendiği üzere işverenin uyguladığı dijital izlemenin hukuka uygunluğu uygulamanın KVKK'daki usul ve esaslara, TBK m. 419/1'de öngörülmüş ölçütlere (KVKK'daki emsal ölçütlere), temel hak ve özgürlüklere uygun olmasına bağlıdır. Bu nitelikleri barındıran dijital izleme uygulamalarıyla işveren kişisel veri işleme faaliyeti yürütebilir, işçileri

1213) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 272; Süzek, [2019], İş Hukuku, s. 335; Eyrenci/Taşkent/Ulucan, [2020], Bireysel İş Hukuku, s. 22; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 253; Başbuğ, [2008], Yönetim Hakkı, s. 3; Balkır, [2008], Yönetim Hakkının Etik Sınırları, s. 73; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 91; Şen, [2005], Çalışma Koşulları, s. 51; Süzek, [1998], Yönetim Hakkı, s. 225-226.

1214) Öztürk, [2021], Talimatlara Uyma, s. 186; Süzek, [2019], İş Hukuku, s. 335; Yargıtay 9. HD, E. 2019/205, K. 2019/9469, T. 24.04.2019.

1215) Yargıtay işçinin talimatlara uyma borcu ile ilgili olarak: "İşçinin iş görme borcu, işverenin yönetim hakkı kapsamında vereceği talimatlarla somutlaştırılır. İşverenin yönetim hakkının karşıtını, işçinin işverenin talimatlarına uyma borcu teşkil eder. İşveren, talimat hakkına istinaden, iş sözleşmesinde ana hatlarıyla belirlenen iş görme ediminin, nerde, nasıl ve ne zaman yapılacağını düzenler. Günlük çalışma süresinin başlangıç ve bitiş saatlerini, ara dinlenmesinin nasıl uygulanacağını, işyerinde işin dağıtımına ilişkin ya da kullanılacak araç, gereç ve teknikler konusunda verilecek talimatlar bu türden talimatlar arasında kabul edilirler. İşverenin yönetim hakkı işyerinde düzenin sağlanmasına ve işçinin davranışlarına yönelik talimat vermeyi de kapsar. İşverenin yönetim hakkı kapsamında verdiği talimatlara işçi uymak zorundadır. İşçinin talimatlara uymaması, işverene duruma göre iş sözleşmesinin geçerli fesih hakkı verir." biçiminde karar vermektedir. Yargıtay 22. HD., E. 2016/30076, K. 2016/26815 T. 12.12.2016; Yargıtay 9. HD., E. 2016/13267, K. 2017/8370 T. 11.5.2017; Yargıtay 9. HD, E. 2019/6407, K. 2020/678, T. 20.01.2020; Yargıtay 9. HD., E. 2008/11542, K. 2009/867 T. 2.2.2009.

denetleyebilir ve işçinin kişisel verisini işleyebilir. İşçi hukuka uygunluk ölçütlerini barındıran dijital izleme uygulamalarına uygun iş görmekle yükümlüdür[1216].

İşverenin hukuka uygun dijital izleme uygulamasına işçinin uyması iş görme borcundan bağımsız nitelikte olmayıp, bu borcun kapsamında kalır ve onu tamamlar. Bundan dolayı işçinin, işverenin gerçekleştirdiği dijital izleme uygulamasına ve dijital denetim menfaatine uygun iş görme borcunu ifa etmemesi iş görme borcunun ihlali olarak değerlendirilmektedir[1217]. Örneğin işverenin hukuka uygunluk ölçütlerini yerine getirdiği GPS bazlı bir dijital izleme uygulamasıyla sahada çalışan satış personelini denetlemek istemesi, performanslarını ve ziyaret planlarını izlemesi ve analiz etmesi satış personelinin iş görme borcuyla ilişkilidir. Bu örnekten hareketle dijital izleme uygulamasını kapatan ve işverenin hukuka uygun talimatlarına uymayan mümessil iş görme borcuna aykırı davranmış olarak nitelendirilir. Dahası hukuka uygun bir dijital izleme uygulamasıyla izlenen satış personelinin gerçeğe aykırı ziyaret girişlerinde bulunduğu, ziyaretlerini gerçekleştirmediği ve iş görmesi için kendisine tahsis edilen araçla tatile gittiğinin tespit edilmesi durumunda elde edilen veri işçi aleyhinde farklı yaptırımlarda kullanılabilir[1218].

Sonuç olarak, hukuka uygunluk ölçütlerini taşıyan dijital izleme uygulamalarına işçinin uyma yükümlülüğü bulunmaktadır. Buna aykırı davranış

1216) Okur, [2013], Elektronik Gözetleme, s. 183.

1217) Süzek, [1998], Yönetim Hakkı, s. 225; Narmanlıoğlu, [2014], Ferdi İş İlişkileri, s. 253; Başbuğ, [2008], Yönetim Hakkı, s. 3; Balkır, [2008], Yönetim Hakkının Etik Sınırları, s. 73; Mollamahmutoğlu/Astarlı/Baysal, [2019], İş Hukuku, s. 181.

1218) Yargıtay ziyaret edilmeyen eczanenin sisteme ziyaret edilmiş gibi girilmesini geçerli fesih sebebi saymıştır. "Dosya içeriğine göre; tanıtım ve satış sorumlusu olarak davalı işyerinde çalışan davacının iş sözleşmesi, fiilen yapmadığı eczane ziyaretlerini yapmış gibi şirket kayıt sistemine girmek suretiyle yalan beyanda bulunduğu ve ayrıca her ayın 25'ine kadar bir sonraki ayın aylık çalışma programını şirket kayıt sistemine girmesi gerekirken fesih tarihi olan Eylül ayı itibariyle aylık çalışma ziyaretini siteme girmediği gerekçe gösterilerek 4857 sayılı Kanun'un 25/II maddesi uyarınca feshedildiği anlaşılmaktadır. Feshe konu davacının eylemleri, her ne kadar haklı fesih ağırlığında olmasa bile, iş akışını olumsuz etkileyen geçerli fesih ağırlığındadır. İşverence yapılan fesih geçerli sebebe dayanmakta olup davanın reddi gerekirken, yazılı şekilde kabulüne karar verilmesi hatalı olup, bozmayı gerektirmiştir." Yargıtay 22. HD., E. 2014/8887, K. 2014/8840, T. 21.04.2014.

işveren tarafından ihlalin boyutuna göre geçerli veya haklı sebeple fesih gerekçesi yapılabilir[1219]. Ayrıca işveren hukuka uygun dijital izlemede elde ettiği veride yer alan işçinin iş sözleşmesi yükümlülüklerine aykırılıklarına dayanarak iş akdini haklı nedenle feshedebilir. Bu durumlarda işçinin özel hayata saygı hakkı veya kişisel verilerine ilişkin haklarını ileri sürmesi sonucu değiştirmeyecektir.

2. Dijital İzlemede Elde Edilen Veri – Fesih İlişkisi

Sürekli borç ilişkisi doğuran iş sözleşmesinin feshi, bozucu yenilik doğuran bir sonlandırma irade beyanıyla gerçekleşir ve muhatabın hakimiyet alanına bu beyanın ulaşmasıyla sonuçlarını doğurur[1220]. İşveren dijital izleme uygulamasında elde ettiği veri iş sözleşmesinin devamını işverenden beklenmeyecek boyutta bir ihlali barındırıyorsa işveren açıklayacağı bir fesih beyanı ile iş akdini geçerli veya haklı sebeple feshedebilir.

a) Geçerli Nedenle Fesih

İş Kanunu m. 18/1 hükmünde belirsiz süreli iş sözleşmesinin süreli feshinde işverenin maddede sayılan nedenlerden birisine dayanmasını zorunlu tutmuştur[1221]. Düzenlemeye göre: "işveren, işçinin yeterliliğinden veya davranışlarından ya da işletmenin, işyerinin veya işin gereklerinden kaynaklanan geçerli bir sebebe dayanmak zorundadır." Özetle işveren tarafından geçerli nedenle iş sözleşmesinin süreli feshedilebilmesi için "işçiye ilişkin bir nedene" veya "işletme gereklerine" dayanılması gerekir.

1219) Okur, [2013], Elektronik Gözetleme, s. 183; Sevimli, [2006], Özel Yaşam, s. 265 vd.; Gürsel, [2016], İşçinin Kişisel Verileri, s. 371.
1220) Ali Güzel, "İş Sözleşmesinin 'Eylemli' Feshi ve Uygulama Sorunu, Çalışma ve Toplum, 2022/4, [2022], s. 2489-2490; Eren, [2019], Borçlar Genel, s. 64-65; Oğuzman/Öz, [2019], Borçlar Genel-II, s. 565; Oğuzman/Barlas, Oğuzman/Barlas, [2020], Medeni Hukuk Giriş, s. 166.
1221) Süzek, [2019], İş Hukuku, s. 552; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 418; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 634.

Dijital izlemede işlenen veride işçinin yetersizliğinin veya İş Kanunu m. 25/II'de düzenlenen "ahlak ve iyi niyet kurallarına uymayan haller" ölçüsünde haklı fesih nedeni sayılacak ağırlıkta olmayan fakat işyerinin düzenini ve işleyişini bozan, işyeri için olumsuzluklar ortaya çıkaran davranışlar[1222] tespit edilmesi geçerli fesih nedeni sayılabilir. İşçinin yetersizliğinden ne anlaşılması gerektiği İş Kanunu'nun gerekçesinde açıklığa kavuşturularak sayılmıştır. Madde gerekçesinde işçinin yetersizliği; "ortalama olarak benzer işi görenlerden daha az verimli çalışma; gösterdiği niteliklerden beklenenden daha düşük performansa sahip olma, işe yoğunlaşmasının giderek azalması; işe yatkın olmama; öğrenme ve kendini yetiştirme yetersizliği; sık sık hastalanma; çalışamaz duruma getirmemekle birlikte işini gerektiği şekilde yapmasını devamlı olarak etkileyen hastalık, uyum yetersizliği, işyerinden kaynaklanan sebeplerle yapılacak fesihlerde emeklilik yaşına gelmiş olma halleri" biçiminde sayılmıştır.

İşçinin fiziki yetersizliğinin bulunması halinde geçerli nedenle fesih hakkının doğması için işçinin kusurunun varlığı önem arz etmez[1223]. Öte yandan, işçinin davranışı sebebiyle geçerli nedenle iş akdinin feshedilmesi için işçinin kusurlu olması aranmaktadır[1224]. İşçinin yetersizliği fiziki yetersizliği hastalık veya yaşlılığı biçiminde görülebilir. Her ne kadar bunlar tek başına geçerli sebeple fesih gerekçesi yapılamaz olsa da hatta yaşlılığı baz alıp bir ayrım yapmak ayrımcılık

1222) Süzek, [2019], İş Hukuku, s. 553; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 419; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 636.
1223) Süzek, [2019], İş Hukuku, s. 553; Doğan Yenisey, [2017], Değerlendirme, s. 469.
1224) Yargıtay özen yükümlülüğünü ihmal eden ihmali davranışın da geçerli fesih nedeni yapılabileceğini, işçinin kusuruna dayanmayan davranışların ise fesih gerekçesi yapılamayacağına karar vermektedir: "İşçinin yükümlülüklerinin kapsamı bireysel ve toplu iş sözleşmesi ile yasal düzenlemelerde belirlenmiştir. İşçinin kusurlu olarak (kasden veya ihmalle) sebebiyet verdiği sözleşme ihlalleri, sözleşmenin feshi açısından önem kazanır. Geçerli fesih sebebinden bahsedilebilmesi için, işçinin sözleşmesel yükümlülüklerini mutlaka kasıtlı ihlal etmesi şart değildir. Göstermesi gereken özen yükümlülüğünün ihlal edilerek ihmali davranış ile ihlali yeterlidir. Buna karşılık, işçinin kusuruna dayanmayan davranışları, kural olarak işverene işçinin davranışlarına dayanarak sözleşmeyi feshetme hakkı vermez. Kusurun derecesi, iş sözleşmesinin feshinden sonra iş ilişkisinin arz edebileceği olumsuzluklara ilişkin yapılan tahminî teşhislerde ve menfaatlerin tartılıp dengelenmesinde rol oynayacaktır." Yargıtay 9. HD., E. 2017/12550, K. 2019/14617, T. 1.7.2019; Yargıtay 22. HD., E. 2015/24204, K. 2015/29383, T. 21.10.2015; Yargıtay 9. HD., E. 2016/24309, K. 2017/15326, T. 10.10.2017.

olarak nitelendirilse de yaşlılığın çalışma performansını olumsuz etkileyen fizyolojik bir durum olduğu genel olarak kabul edilmektedir[1225].

İşçinin yetersizliği mesleki yetersizlik biçiminde de görülebilir. İş Kanunu m. 18/1'de bu durum geçerli nedenle fesih sebebi olarak düzenlenmiştir. İşçiye bu yönde bir nitelendirmede bulunabilmek için işçinin ortalama, benzer durumdaki işçilerden daha az verimli ve düşük performansla çalışması[1226] ve işyerinde işçiye tebliğ edilmiş objektif performans değerlendirme ölçütlerinin bulunması gerekmektedir[1227]. Bu objektif ölçütle kapsamında değerlendiren işçinin ortalama benzer durumdaki işçilere göre daha az verimli çalışması işveren için geçerli fesih hakkını doğurur.

Hukuka uygun dijital izlemede elde edilen veride işverenin güvenini sarsan işçi davranışları da bulunabilir. Haklı nedenle fesih ağırlığında olmayan bu davranışlarda her zaman haklı fesih nedenlerindeki gibi açık şekilde esaslı bir ihlali tespit etmek mümkün olmayabilir. Bu durumda adil ve makul her işverence güçlü şüphe olarak değerlendirilen ve işçi tarafından gerçekleştirildiği yüksek olasılık

1225) Süzek, [2019], İş Hukuku, s. 554-555; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 465.
1226) Süzek, [2019], İş Hukuku, s. 557; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 470-471; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 637.
1227) Yargıtay objektif performans değerlendirme sisteminin oluşturulmasını ve işçiye önceden tebliğ edilmiş olmasını aramaktadır: "Yetersizlikten kaynaklanan sebepler; işçinin ortalama benzer işi görenlere göre daha az verimli çalışması, gösterdiği niteliklerden beklenenden daha düşük performansa sahip olması, işe yoğunlaşmasının giderek azalması, işe yatkın olmaması, öğrenme ve kendisini geliştirme konusunda yetersiz kalması, sık sık hastalanması, çalışamaz duruma getirmemekle birlikte işini gerektiği şekilde yapmasını devamlı olarak etkileyen hastalığa yakalanması ve uyum yeterliliğinin azalması gibi işyerinde işin görülmesini önemli ölçüde olumsuz etkileyen sebeplerdir. Objektif bir performans değerlendirmesi için, personelin görev tanımı ve performans değerlendirme kriterleri önceden saptanmalı ve işçiye tebliğ edilmelidir. Değerlendirme çalışanın görev tanımına, verimine, işverenin kurumsal ilkelerine, uyulması gereken işyeri kurallarına uygun olarak objektif ve somut olarak yapılmalı ve buna yönelik performans değerlendirme formları hazırlanmalıdır. İşyerine özgü çalışanların performanslarının değerlendirileceği, Performans Değerlendirme Sistemi geliştirilmeli ve uygulanmalıdır. Değerlendirmede işin gerektirdiği bilgi, beceri, deneyim gibi yetkinlikler, işyerine uygun davranışlar ve çalışandan gerçekleştirmesi beklenen ... ve kişisel gelişim hedefleri ile personelin bunları gerçekleştirme oranı esas alınmalıdır. Geçici nitelikte ve kısa süreli davranış ve sonuçlar değerlendirmede göz önünde bulundurulamaz." Yargıtay 22. HD., E. 2018/12201, K. 2018/21833, T. 11.10.2018; Yargıtay 9. HD., E. 2017/27643, K. 2018/14018, T. 27.6.2018.

dahilinde olan davranışların bulunması ve bunun iş sözleşmesinde bulunması gereken güven ilişkisini ortadan kaldırması halinde işveren, işçinin savunmasını da alarak bu verileri şüphe feshinde kullanabilir[1228]. Şüphe feshi işverene olası risklere karşı işletmesini ve kendisini koruyabilmesi ihtiyacı sebebiyle uygulama bulmuş istisnai bir geçerli fesih biçimi olduğundan[1229] her dijital izleme uygulamasında elde edilen veri ile bu fesih yoluna gidilmemesi gerekir. İstisnai bir geçerli fesih nedeni olduğundan şüphe feshinin fesih nedeni yapılabilmesi somut olayın haklı kıldığı ve işveren açısından giderilmeyen bir şüphenin bulunması ve güven esaslı bir ilişki olan iş ilişkisinde işveren açısından güven temelinin sarsılmış olması gerekir[1230].

Önemle belirtmek gerekir ki, işçinin davranışı veya verimi ile ilgili iş sözleşmesi geçerli sebeple feshedilecekse fesihten önce işçiden İş Kanunu m. 19/1'e uygun olarak savunma alınmış olması zorunludur. Kanun koyucu böylelikle işçiye hakkındaki iddialara ilişkin bir savunma imkanı tanımıştır. Ayrıca fesih gerekçesinde fesih sebebinin açık ve kesin bir biçimde işçiye bildirilmiş olması gereklidir[1231]. İşveren fesih hakkını, feshin son çare olması (ultima ratio) ilkesine uygun olarak iş ilişkisinin sürdürülmesinin kendisinden beklenmeyecek noktaya gelmiş olması ve son çare olarak feshe başvurulmuş olması gerekir. İşveren iş akdini feshine gerek duymayacak daha hafif bir yöntemle konuyu çözecekken iş akdinin feshi usulünü benimsemesi feshin son çare olması ilkesine aykırıdır. Gerçekten sözleşmeye bağlılık (pacta sund servanda) ilkesinin bir gereği olarak öncelikli olarak sözleşmenin ayakta tutulmasını amaçlayan bir anlayışla hareket edilmesi gerekir. Bu aynı zamanda iş güvencesi sisteminde feshin istisna olmasının da bir görünümü olduğundan feshe son çare olarak başvurulmalıdır[1232].

1228) Kübra Doğan Yenisey, "Şüphe Feshi", Sicil İş Hukuku Dergisi, Eylül [2008], s. 68.
1229) Doğan Yenisey, [2008], Şüphe Feshi, s. 71; Ulaş Baysal, "Şüphe Feshi Kavramı ve Şüphe Feshine İlişkin Yargıtay Kararlarının Değerlendirilmesi", Sicil İş Hukuku Dergisi, 2016/35, [2016], s. 89.
1230) Yargıtay 22. HD., E. 2017/40841 K. 2017/21915 T. 17.10.2017; Yargıtay 9. HD., E. 2012/31023 K. 2013/11390 T. 8.4.2013.
1231) Süzek, [2019], İş Hukuku, s. 587; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 655; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 494.
1232) Süzek, [2019], İş Hukuku, s. 587; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 657-658.

İşçinin, işvereni aleyhine sözler söylemesinin kamera gözetlemesinde tespit edilmesi; işverenin ailesine ve itibarına haklı nedenle fesih sebebi (İşK. m. 25/II-b) sayılacak düzeyde olmamakla birlikte sözler söylediğinin iletişimin izlenmesinde ortaya çıkması işveren için iş ilişkisini sürdürmesi objektif olarak olanaksız ise işverenin hukuka uygun dijital izlemde elde ettiği bu veriler kapsamında geçerli fesih hakkı doğar[1233]. Aynı husus kamera gözetlemesinde işçinin diğer işçilere sataşmasının görülmesi ve fakat haklı fesih nedeni ağırlığında bulunmaması, ancak bu davranışların işyeri düzenini bozması, işverenden iş sözleşmesinin devamının kendisinde beklenmeyeceği durumda, işveren tarafından iş sözleşmesinin dijital izleme vasıtasıyla elde edilen veri kapsamında geçerli nedenle feshedilmesi için de söylenebilir[1234].

İşçinin işe giriş – çıkış sistemlerinde işe geç gelmeyi alışkanlık haline getirdiğinin tespit edilmesi veya İş Kanunu m. 25/II-g koşullarını oluşturmayacak biçimde devamsızlıklar gerçekleştirdiğinin tespit edilmesi, arkadaşlarıyla devamlı gereksiz yere tartışmaya girişmesi ve geçimsizlik yapması bu hususların hukuka uygun elektronik iletişimin izlenmesinde ortaya çıkması, bu verilerin işçi şikayetleriyle örtüşmesi durumunda işçinin bu davranışları haklı nedenle fesih ağırlığında olmamakla birlikte, işveren için iş sözleşmesini geçerli nedenle fesih hakkı doğar.

İşçinin iş görme borcunu ifa etmesi için kendisine tahsis edilen eşyaya, işverenin malına zarar verdiğinin dijital izleme uygulamaları vasıtasıyla tespit edilmesi ve bu zararın İş Kanunu m. 25/II-ı bendi koşullarını karşılamadığı, 30 günlük ücreti düzeyinde olmadığı durumlarda (örneğin 15 günlük ücreti tutarında

1233) Süzek, [2019], İş Hukuku, s. 565.
1234) Yargıtay haklı fesih ağırlığında olmayan görüntülerde işçinin diğer işçilere sataşmasını geçerli fesih nedeni olarak kabul etmiştir. “Her ne kadar mahkemece davacının kavga ettiği, işyeri düzen ve kurallarına uymadığı, çalışma huzurunu bozduğu gerekçesiyle feshin haklı olduğu kabul edilmişse de, dosya içerisinde bulunan CD’den kamera kayıtları incelendiğinde, ses olmadığı, doğrudan davacının hareketinin görülmediği, diğer çalışana hakaret ettiğine dair delil olmadığı, haklı neden boyutunda bir sataşmanın olmadığı, ancak davalı tanıklarının anlatımlarına göre işyeri huzurunu bozduğu, dolayısıyla feshin geçerli nedenle yapıldığı anlaşılmıştır.” Yargıtay 22. HD., E. 2017/9463, K. 2018/325, T. 17/01/2018.

olması) işveren dijital izleme uygulamasında elde ettiği veriye dayanarak işçinin iş akdini geçerli nedenle feshe konu edebilir[1235].

b) Haklı Nedenle Fesih

Haklı nedenle fesih sebepleri, iş sözleşmesinin devamının dürüstlük kuralının bir gereği olarak bu hakkın doğduğu taraftan beklenemeyeceği durumlarda bu sebebin doğduğu tarafa tek taraflı irade beyanı ile iş sözleşmesini derhal feshetme hakkı vermektedir[1236]. Bu başlıkta örnekler bazında dijital izlemede hukuka uygun biçimde elde edilen veriler, haklı fesih nedenleri kapsamında değerlendirilecektir.

aa) Hukuka Uygun Biçimde Elde Edilme

İşverenin hukuka uygun dijital izleme uygulamalarında elde ettiği veriler haklı nedenle feshe dayanak oluşturur. Yargıtay dijital izleme için işçilerin önceden haberdar edilmesi veya bilgilendirilmesi koşulunu aramakta ve işverenin yönetim hakkı kapsamında oluşturduğu işyeri kurallarına ve talimatlarına işçinin uymak zorunda olduğuna karar vermektedir[1237]. Bu sebeple kurumsal e-posta hesaplarının

---

1235) Yargıtay işçinin verdiği zarar otuz günlük ücret düzeyinde değilse ve fakat işçinin davranışlarının işyerinde olumsuzluklara sebebiyet vermesi durumunda iş akdinin geçerli nedenle feshedilebileceğine karar vermiştir: "4857 sayılı Kanun'un 25 II- (ı) bendinde, işverenin malı olan veya eli altında bulunan makine, tesisat, başka eşya ya da maddelere otuz günlük ücreti tutarını aşacak şekilde zarar vermesi halinde işverenin haklı fesih imkânının bulunduğu hususu düzenlenmiştir. İşçinin kusursuz olduğunun ortaya çıkması halinde işverenin haklı ve geçerli fesih imkânı olmadığı gibi, işçinin kusuru belli bir yüzde ya da belli bir oran olarak saptanmışsa; zararın miktarı da bu kusur nispetinde azaltıldıktan sonra otuz günlük ücreti aşıp aşmadığına bakılmalıdır. Otuz günlük ücreti tutarında bir zarar yoksa, iş sözleşmesinin feshi haklı sebep olarak kabul edilmemelidir. Ancak otuz günlük ücretten az zarar sebebi ile işyerinde olumsuzluklara meydana gelmiş ve iş ilişkisinin sürdürülmesi işveren açısından önemli ölçüde beklenmez bir hal almış ise feshin geçerli sebebe dayandığının kabulü gerekir." Yargıtay 22. HD.; E. 2012/13192, K. 2012/16489, T. 10.07.2012.

1236) Süzek, [2019], İş Hukuku, s. 665; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 494; Yargıtay 22. HD., E. 2018/1227, K. 2018/7322, T. 21.03.2018; Yargıtay 9. HD., E. 2016/28800, K. 2021/6300, T. 17/03/2021.

1237) Yargıtay 22. HD, E. 2017/21857, K. 2019/9884, T. 07.05.2019, Kararda özetle: "Somut uyuşmazlıkta davacının şirkete ait gizli bilgileri şirket dışına çıkardığını, bu hususun davacıya ait usb cihazının bulunması ile ortaya çıktığını savunmuş ise de, yargılama sırasında dinlenilen davacı

veya internet trafiğinin izlenmesini isteyen bir işveren bu uygulamaların özel amaçlarla kullanılıp kullanılmayacağı, izlemenin amacı, biçimi, işçinin veri koruma hukukundan doğan hakları, haklarını kullanma yöntemleri ve getirilen yasağın sebepleri gibi hususlarda işçileri önceden bilgilendirmesi gerekir. Aynı durum sahada çalışan veya şirket aracı kullanan işçilerin lokasyon bazlı hareketlerinin GPS sistemiyle izlenmesi veya uzaktan çalışmada işçilerin aktif klavye süresinin klavye yakalayıcısıyla izlenmesi[1238] ve internet izlerinin takip edilmesi amacıyla gerçekleştirilen dijital izleme uygulamaları için de geçerlidir. Zira işçilere bilmedikleri bir konuda yükümlülük yüklemek veya böyle bir uygulamada elde

ve davalı tanıkları davacının zaman zaman işini evden de yürütebildiğini ve bilgisayarının da diz üstü bilgisayar olduğunu ifade etmiştir. Davalı taraf, davacının işyeri dışına çıkarmaması gereken iş sırrı niteliğindeki bilgileri işyeri dışına çıkardığına dair somut bir delil sunmamıştır. Diğer taraftan, dosya kapsamına göre davacının çalışma süresi içinde kariyer sitelerine girdiği, sohbet sitelerinde zaman geçirdiği, bir başka arkadaşını işverenine bazı bilgileri vermemesi konusunda yönlendirdiği, şirketin araç vermemesi üzerine işvereni kötülediği, fuarlara katılmama konusunda çeşitli bahaneler ürettiği, iş sözleşmesinin başlangıcında kendisinde bulunması gereken vasıflar konusunda hatalı bilgi verdiği sabit ise de, davalı işverenin bu bilgileri işçinin bilgisayarına yerleştirdiği özel bir takip programı ile elde ettiği anlaşılmaktadır. Davacı taraf, gerek haberleşme ve iletişiminin kayda alınması gerekse kaybolan USB'ye usulsüz olarak el konulduğu iddiası ile davalı işveren hakkında suç duyurusunda bulunduğunu belirterek, devam eden hazırlık soruşturmasının numarasını bildirmiştir. Davalı işveren ise işçinin bu izlemeden haberdar olduğu veya izlemenin yapılacağı konusunda bilgilendirilmediğine dair somut bir delil sunmamıştır. Şu halde davacı işçinin, bilgisayarında bulunan klavye yakalayıcısı adı verilen programdan haberinin olmadığı, işverence bu konuda bilgilendirilmediği, davacının rızası hilafına tüm kayıtların özel yahut işe ilişkin bilgi ayrımı olmadan işverence günlük olarak elde edildiğinin anlaşılması karşısında, elde edilen bu bilgilerin fesih sebebi olarak ileri sürülemeyeceği değerlendirilmelidir. İşverenin yönetim hakkının bir sonucu olarak işçiyi elektronik ortamda izlemesi ve takip etmesi her zaman mümkündür. Ancak bunun için işçinin bu izleme hakkında bilgilendirilmiş olması şarttır. İşçinin izlendiğine dair bilgilendirilmemesi veya gizlice izlenmesi, bu izleme neticesinde elde edilen veriler, iş sözleşmesinin işçi tarafından ihlal edildiğini açıkça ortaya koysa dahi, hukuka aykırı olarak kabul edilmelidir. Hal böyle iken, somut olayda işverence gizlice izleme neticesinde elde edilen bilgilerin haklı fesih sebebi olarak ileri sürülmesinin mümkün olmadığı kabul edilmelidir. Mahkemece feshin haklı bir sebebe dayanmadığı ve davacının ihbar tazminatına hak kazandığı sonucuna varılması gerekirken, yazılı gerekçe ile davanın reddine karar verilmesi hatalı olup, kararın bu sebeple bozulması gerekmiştir." biçiminde değerlendirme yapılmıştır.

1238) KVK Kurumu yayımladığı "Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi gereken Hususlara İlişkin Rehber'de" klavye "klavye basış biçimi" davranışsal biyometrik veri olarak kabul örneklendirilmiştir. Biyometrik veriler KVKK m. 6/1'de özel nitelikli kişisel veri olarak düzenlendiğinden veri sorumlusu işverenin bu verileri işleyebilmesi için özel nitelikli kişisel verilerin işlenmesi şartlarına uygun bir işleme faaliyeti oluşturması gerekmektedir. KVK Kurumu, Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi gereken Hususlara İlişkin Rehber, s. 5-6, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf (Erişim Tarihi: 02.07.2023).

edilen verilere hukuki bir sonuç bağlamak hukuken her durumda mümkün olmayacaktır[1239].

Önemle eklemek gerekir ki, derhal fesih hakkının, dijital izleme uygulamasıyla haklı fesih nedeninin öğrenildiği günden itibaren altı iş günü içinde kullanılması gerekmektedir[1240]. İş Kanunu m. 26/1 hükmünün bir gereği olarak haklı fesih nedenlerinin öğrenildiği günden başlayarak hakkın altı iş günü içinde kullanılması gerekmektedir. Altı iş günü geçtikten sonra ve her halükarda olayın üzerinden bir yıl geçtikten sonra fiil haklı fesih nedeni yapılamaz. Öte yandan işçinin maddi çıkar elde etmesi söz konusu ise bu bir yıllık süre uygulanmaz[1241].

bb) Dijital İzlemede İşverenin Şeref ve Namusuna Dokunacak Sözler ve Davranışların Tespiti

İş Kanunu m. 25/II-b bendine göre; "işçinin, işveren yahut bunların aile üyelerinden birinin şeref ve namusuna dokunacak sözler sarfetmesi veya davranışlarda bulunması yahut işveren hakkında şeref ve haysiyet kırıcı asılsız ihbar ve isnadlarda bulunması" haklı fesih nedeni olarak hüküm altına alınmıştır. İşçinin elektronik iletişimini izleyen uygulamalarında bu düzenleme hükmüne aykırı konuşma, yazışma ve fiillerinin tespit edilmesi durumunda işveren bu veriyi haklı fesih nedeni yapabilir. Öte yandan işçinin eleştiri hakkı kapsamında değerlendirilebilen davranışları ve beyanları ifade özgürlüğü kapsamında değerlendirilmeli ve bunlar haklı fesih nedeni olarak kullanılmamalıdır[1242].

1239) ILO Uygulama Kodu, m. 5-6; AİHM, [GK], [2017], Bărbulescu v. Romanya, § 77-78, § 133; AYM Ömür Kara ve Onursal Özbek, § 50; AYM E.Ü., § 67; AYM Fırat Gerçek § 21, § 29.
1240) Süzek, [2019], İş Hukuku, s. 690; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 574; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 771.
1241) Yargıtay feshe yetkili makamın öğrendiği tarihten itibaren altı iş günü içinde hakkın kullanılmasını aramaktadır. Yargıtay 9. HD., E. 2021/7569, K. 2021/12657 T. 23.9.2021; Yargıtay 9. HD., E. 2017/11316 K. 2019/15066 T. 4.7.2019; Yargıtay 22. HD., E. 2016/24606, K. 2020/1890 T. 6.2.2020; Yargıtay 9. HD., E. 2018/5432 K. 2018/11996 T. 29.5.2018; Yargıtay 22. HD., E. 2013/12067, K. 2014/13982 T. 21.05.2014.
1242) Süzek, [2019], İş Hukuku, s. 668; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 746; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 553.

Yargıtay işverene ait bilgisayarı ve e-mail adreslerini özel yazışmalarda kullanarak işverene hakaret niteliğinde sözler sarf etmenin, işveren açısından 4857 sayılı Yasa'nın 25 II-b maddesi uyarınca haklı fesih nedeni oluşturacağına karar verilmesi gerektiğine hükmetmiştir[1243]. Bir diğer kararda, davacı işçinin "dosyada bulunan tutanak ve telefon kayıtlarının çözümünden işverene ağır küfür ettiği ve işverenin altı günlük süresi içinde iş akdini haklı nedenle feshettiği anlaşıldığı" gerekçesiyle aksi yönde karar veren yerel mahkeme kararını bozmuştur[1244]. Bu itibarla dijital izleme uygulamasında tespit edilen işçinin, işverenin veya işverenin aile üyelerinden birisinin şeref ve onuruna dokunacak davranışlarda bulunmasını işveren için iş sözleşmesini haklı nedenle feshi hakkını doğurur.

cc) İşçinin İşverenin Diğer İşçisine Cinsel Tacizde Bulunması

İş Kanunu m. 25/II-c bendi hükmünde; "işçinin işverenin başka bir işçisine cinsel tacizde bulunması" işveren açısından iş sözleşmesinin haklı nedenle derhal fesih sebebi olarak hüküm altına alınmıştır. TBK m. 417'de işçinin kişiliğinin korunması açısından işveren, "özellikle işçileri psikolojik ve cinsel tacize uğramaları ve bu tür tacizlere uğramış olanların daha fazla zarar görmemeleri için gerekli önlemleri almakla" yükümlü tutulmuştur. Eklemek gerekir ki, cinsel tacizin işyeri veya işyeri dışında gerçekleşmiş olması haklı fesih kapsamında iş akdinin derhal feshi sonucunu değiştirmemektedir[1245].

İşçinin, işverenin bir çalışanına anlık mesajlaşma uygulaması üzerinde cinsel tacizde bulunduğunun dijital izlemeyle tespit edilmesi, cinsel taciz olarak nitelendirilebilecek e-posta gönderdiğinin dijital izlemeyle tespit edilmesi veya

---

1243) Yargıtay 9. HD., E. 2010/447, K. 2010/37516, T. 13.12.2010; Süzek, [2019], İş Hukuku, s. 669.

1244) Yargıtay 7. HD., E. 2015/4806 E., K. 2015/8302, T. 07.05.2015; Yargıtay 22. HD., E. 2014/30542, K. 2014/32185, T. 17.11.2014; Aynı yönde Yargıtay 22. HD., E. 2011/3997, K. 2011/7160, T. 09/12/2011 tarihli kararında işçinin elektronik posta üzerinde sataşması, işverene isnatlarda bulunması İş Kanunu m. 25/II-b kapsamında haklı fesih nedeni olarak değerlendirilmiştir.

1245) Süzek, [2019], İş Hukuku, s. 668; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 553; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 750; Yargıtay 9. HD., E. 2012/26702, K. 2013/3953, T. 04.02.2013.

kamera gözetlemesinde elde edilen verilerden tacizin görülmesi işveren açısından iş sözleşmesinin haklı nedenle derhal fesih sebebidir. Yargıtay bir kararında işçinin, işyerindeki bir kadın işçiyi mesajlarla evine çağırmasını, rahatsız etmesini ve taciz etmesini haklı fesih nedeni ağırlığında olduğunu ifade ederek işverenin bu mesajlara dayalı haklı feshini yerinde bulmuştur[1246]. Eklemek gerekir ki, cinsel tacize uğrayan işçinin tacizle ilgili olarak suç duyurusunda bulunmaması veya dijital izleme kaydında ortaya çıkan tacizin bir kısmını işverene raporlamaması işveren açısından iş akdinin haklı nedenle feshine engel değildir[1247].

Öte yandan bir kadın işçinin taciz şikayetiyle ilgili olarak işverenin gizli kamera gözetlemesi gerçekleştirmesi veya işçinin tacizi başka türlü ispat edemediği bir hal içindeyken gizli ses kaydı veya görüntü alınması durumlarının da değerlendirilmesi gerekmektedir. İlgili başlıkta detaylı ele alındığı üzere[1248], bir suç soruşturmasında suçun ortaya çıkarılması veya önlenmesi daha az müdahaleci bir yöntemle gerçekleştirilmesine olanak yoksa işveren gizli izleme uygulamaları kullanabilir. Bunun hukuka uygun kabul edilebilmesi için sınırlı süreli, suça yönelik, diğer kişiler üzerinde ihlale sebebiyet vermeyen, suç mahalini veya failini kapsayan gizli izleme gerçekleştirebilir (KVKK m. 28/2-a).

İşçinin kendisine yönelmiş bir tacizi anlık gelişmeye göre başka türlü belgelemesine olanak bulunmadığı durumlarda gizli ses kaydı alması[1249] veya gizli

---

1246) Yargıtay işçinin gönderdiği taciz mesajlarını şu şekilde değerlendirmiştir: "Her ne kadar mahkemece davacıya isnat edilen eylemlerin bayan iş arkadaşlarına cinsel tacizde bulunma boyutunda olmadığı, herhangi bir cinsel ifade içermeyen mesaj gönderme şeklinde olduğu, tüm iddiaların soyut düzeyde kaldığı gibi bir değerlendirme yapılmışsa da; dosya içerisinde mesaj kayıtlarının bulunduğu, söz konusu mesajlarda davacının bayan iş arkadaşını evine çağırdığı, rahatsız ettiği ve taciz ettiğinin sabit olduğu, diğer bayan personelleri de taciz ettiğine dair duyumlar olduğu, taciz eyleminin gerçekleşmesi için açıkça cinsel ifadeler içermesinin gerekmediği, dolayısıyla davacının eylemlerinin haklı neden ağırlığında olduğu anlaşılmıştır." Yargıtay 22. HD., E. 2017/21606, K. 2019/9567, T. 25.04.2019.
1247) Yargıtay 9HD., E. 2015/35411, K. 2019/3553, T. 13.02.2019.
1248) Bkz. § 7. II. 2. b.
1249) KVK Kurulu, 07/09/2023 Tarihli ve 2023/1548 Sayılı Kararı'nda işçinin bilgisi dışında ses kaydının alınmasını Yargıtay CGK'nın ortaya koymuş olduğu ölçütler kapsamında "izinsiz ses kaydı alınmasının, belli bazı durumlarda, Türk Ceza Kanunu kapsamında suç teşkil etmeyeceğinin ve hukuka uygun delil mahiyeti taşıyacağının Yargıtay içtihatları ile benimsendiği, Yargıtay Ceza Kurulu'nun 01/12/2020 tarihli ve 2020/485 sayılı Kararında da; 'Kişinin kendisine karşı işlenmekte

kamera kaydı gerçekleştirmesi durumunda gerçekte planlı bir durum söz konusu olmadığı örneklerde bu deliller hukuka uygun veri kabul edilmektedir. Örneğin bir özel bankanın inşaat birim müdürünün, banka çalışanı inşaat proje sorumlusuna performans değerlendirmesi toplantısında hakaret etmesi üzerine işçinin üzerindeki cep telefonu ile gizlice ses kaydı alınması ceza yargılamasına konu edilmiş ve Yargıtay eylemin başka türlü ispatına olanak bulunmadığı bir hal içindeyken kaydın gerçekleştiği değerlendirmesini yaparak olayda suç unsuru bulunmadığına karar vermiştir[1250]. Karara konu Yargıtay kararından hareketle eğer işçi kendisine yönelik tacizi o andaki duruma göre başka türlü belgelendirmesine olanak bulunmayan bir hal içindeyken gizli ses kaydı, kamera kaydı alması hukuka uygun kabul edilerek elde edilen deliller işçi aleyhine haklı nedenle fesih sebebi yapılabilir. Öte yandan tacize uğrayan işçinin planlı bir gizli ses ve görüntü kaydı oluşturması, bu yönde tacizi gerçekleştiren işçiyi yönlendirmesi hukuka aykırı delil olarak nitelendirecektir. Bununla birlikte iş ilişkisi güven temelli bir ilişki ortaya çıkardığından işveren tacize uğrayan işçinin beyanı ve gizli kaydı dikkate alarak işçinin davranışı sebebiyle iş akdini geçerli feshe konu edebilir.

olan bir suçla ilgili olarak, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkânının olmadığı ani gelişen durumlarda karşı tarafla yaptığı konuşmaları kayda alması halinin hukuka uygun olduğunun kabulü zorunludur. Aksi takdirde kanıtların kaybolması ve bir daha elde edilememesi söz konusudur.' değerlendirmesine yer verildiği, İşçi işveren uyuşmazlıklarında; işverenin iş sözleşmesini haklı nedenle feshettiğini başka türlü delil ile ispat etme imkânı yok ise ya da kaybolma ihtimali bulunan kanıtların kaybolmasının engellenmesi amacı var ise alınan ses kaydının hukuka uygun delil olarak kabul edilebileceği, bu kapsamda ilgili kişinin iş sözleşmesinin haklı sebeple feshedildiğini ispatlama aracı olarak kullanılan ses kaydının hukuka uygun delil olduğu…" biçiminde değerlendirmeye konu edilmiştir.

1250) Yargıtay 12. CD., E. 2013/26087 K. 2014/10205 T. 28.4.2014. Kararda özetle: "2009 yılında birim müdürü olarak çalışmaya başlayan müştekinin göreve başladığı günden bu yana kendisine karşı negatif bir tutum içerisinde olduğu, eski çalışan olması nedeniyle kendisini tasfiye etmek istediği, daha önce iş ortamında kendisine sözlü olarak hakaret ettiği, toplu ortamlarda kendisine karşı rencide edici ve küçük düşürücü tavırlar sergilediği, yaklaşık 1 ay önce hakkında haksız yere soruşturma başlattığı, olay günü de, performans değerlendirme toplantısında kendisine hakaret içerikli sözler söylemesi nedeniyle üzerindeki cep telefonu ile gizlice kayıt yaptığı, eylemi başka türlü ispat etmesinin mümkün olmadığı yönündeki savunması ile bu savunmayı doğrulayan bilirkişi raporuna göre, sanığın başkaca şekilde ispatlanması mümkün olmayan bir hal içerisinde iken toplantıda kendisine yönelik hakaret içerikli konuşmayı kayda aldığı, sanığın eyleminin hukuka aykırı olduğunu kabul etmenin mümkün olmadığı anlaşıldığından…" hususları değerlendirilmiştir.

dd) Dijital İzlemede İşçinin Sataşması ve İşyerinde Alkol, Uyuşturucu Kullanması Verisinin İşlenmesi

İşçinin işyeri düzenini bozacak sataşmalarda bulunması, işyerinde alkol ve uyuşturucu kullanması işveren için iş akdinin haklı nedenle derhal fesih hakkını doğurur. İş Kanunu m. 25/II-d bendinde bu husus; "işçinin işverene yahut onun ailesi üyelerinden birine yahut işverenin başka işçisine sataşması, işyerine sarhoş yahut uyuşturucu madde almış olarak gelmesi ya da işyerinde bu maddeleri kullanması" biçiminde hüküm altına alınmıştır. Bu düzenleme kapsamında işyeri kamera gözetlemesiyle tutulan kayıtlarda işçinin işyerinde alkol kullandığı, uyuşturucu kullandığının anlaşılması durumunda işveren bu veriye dayanarak iş akdini haklı nedenle feshedebilir. Yargıtay bu durumlarda kamera kayıtlarının bilirkişi marifetiyle incelenmesini ve olaydaki şüphelerin ortadan kaldırılarak elde edilen verinin nitelendirilmesi gerektiğine karar vermiştir[1251].

Kamera kayıtlarında elde edilen veride işçinin diğer işçilere sataşması, saldırması, hakaret etmesi, işçinin hakaretinin ve tehdidinin iletişimin izlenmesinde ortaya çıkması durumunda işveren bu verileri haklı fesih nedeni kapsamında kullanabilir. Öte yandan işveren kavgaya veya hakaret, tehdide karışmış işçiler arasında bir seçim yapar, sadece birisine yaptırım uygularsa bu durum eşit davranma borcuna aykırılık teşkil eder ve gerçekleştirilen feshi haksız fesih haline getirir[1252].

ee) Dijital İzlemede İşçinin Doğruluk ve Bağlılığa Uymayan Davranışlarının Tespit Edilmesi

Kuvvetli suç şüphesinin bulunması durumunda ve suçun önlenmesi amacıyla işverenin istisnai durumlarda gizli kamera gözetlemesi gerçekleştirmesi

1251) Yargıtay 9. HD., E. 2018/7697, K. 2021/656, T. 13.01.2021.
1252) Süzek, [2019], İş Hukuku, s. 671; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 746-747; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 552.

ve elektronik iletişimi gizli izlemesi hakkının bulunduğu ele alınmıştı[1253]. Bu şekilde olmayıp, fakat işverenin elektronik iletişimin izlenmesinde veya kamera gözetlemesinde elde ettiği veride ulaştığı işçinin doğruluk ve bağlılığa uymayan davranışları iş akdinin haklı nedenle feshine dayanak yapılabilir.

İş Kanunu m. 25/II-e bendinde işçinin doğruluk ve bağlılığa uymayan davranışı; "işçinin, işverenin güvenini kötüye kullanmak, hırsızlık yapmak, işverenin meslek sırlarını ortaya atmak gibi doğruluk ve bağlılığa uymayan davranışlarda bulunması" biçiminde düzenlenmiştir. Bu bentte sayılan örneklerle yetinilmemiş "gibi" sözcüğüne yer verilerek bu durumların sayılanlarla sınırlı olmadığı, benzer davranışların ortaya çıkması halinde de iş akdinin haklı sebeple derhal feshedilebileceği hüküm altına alınmıştır[1254].

Bu hüküm kapsamında örneğin gerçekleştirilen elektronik iletişimin izlenmesinde işçinin işverenin ticari sırlarını rakip firmalarla paylaştığı[1255], yazılım kaynak kodlarını dışarı sızdırdığı, yazılım kodlarını kendi faaliyeti için kullandığı[1256]; kamera gözetlemesinde[1257] işçinin depodaki bilgisayarlardan birisini

1253) § 7. II. 2. b.
1254) Süzek, [2019], İş Hukuku, s. 673; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 554; Ekmekçi/Yiğit, [2022], Bireysel İş, s. 755.
1255) Yargıtay işverenin meslek sırlarının sızdırılmasını haklı fesih nedeni olduğunu şu şekilde karara bağlamıştır: "Dosya içeriğinden, davacı işçinin davalı işveren ile aynı sektörde yer alan ve işi yapmakta olan rakip firmalara firma çalışanlarını yönlendirerek çalışmalarını sağladığı, bu işlerde firma çalışanı olan ve iş sözleşmesi aynı şekilde feshedilen E.. S.. ile birlikte hareket ettikleri anlaşılmaktadır. Somut olayda, davalı işveren, davacının doğruluk ve bağlılığa uymayan davranışlarda bulunduğunu ispatlamıştır." Yargıtay 22. HD., E. 2013/18003, K. 2014/28827, T. 23.10.2014.
1256) İşveren e-posta izlemesinde işçinin aynı iş kolunda faaliyette bulunduğunu tespit etmiş ve iş akdini haklı nedenle feshetmiştir. Yargıtay feshin haklı nedene dayandığına karar vermiştir. Kararda bu husus: "Dosyadaki bilgi ve belgelerden, davacının davalı şirketten ayrılmadan önce G. Bilişim adlı bir internet sitesi kurduğu, internet sitesinde davacının "genel müdür" olarak göründüğü, bu hususun davacı ile arkadaşı M.K.arasındaki elektronik posta yazışmalarından da sabit olduğu, davacının davalı işverenin bilgisi ve izni olmadan işçisi iken aynı iş kolunda benzer iş yapmaya başladığı bu eyleminin doğruluk ve bağlılığa uymayan davranış olup, işverenin feshinin haklı olduğu anlaşılmakla" biçiminde tespit edilmiştir. Yargıtay 9. HD., E. 2014/24194, K. 2015/35097, T. 10.12.2015.
1257) Yargıtay kamera izlemesinde işçinin doğruluk bağlılığa uymayan davranışlarını İş Kanunu m. 25/II-e kapsamında değerlendirmiştir. Kararda özetle; "Somut olayda davalı şirketin ibraz ettiği şikayet dilekçeleri, kamera görüntü çözümüne ilişkin tutanaklar, site içi kamera kayıtları, tanık beyanları ve özellikle davacının vermiş olduğu yazılı savunmasına göre davacının güvenlik görevlisi

götürdüğü verisine sonradan yapılan denetimde ulaşılması durumunda işveren bu veriyi haklı nedenle feshe dayanak oluşturarak işçinin iş akdini derhal feshedebilir. Dahası işçinin sadakat borcuna aykırı davranışlarının bulunması durumunda işverenin haklı nedenle fesih hakkını kullanabilmesi için işçinin fiillerinin mutlaka suç niteliğinde olması gerekli değildir. Ayrıca olayın ceza yargılamasına konu edilmesi ve beraat kararı alınması hukuk hakimini bağlamayacağını belirtmek gerekir[1258].

ff) İşçinin Yapmakla Ödevli Olduğu İşleri Hatırlatılmasına Rağmen Yapmadığı Verisine Ulaşılması

Hukuka uygunluk ölçütlerinin bulunduğu bir dijital izlemede işlenen veride işçinin işyeri talimatlarına uymadığı ve kendisine verilen işleri yapmadığı hususlarının tespit edilmesi ve bu hususta uyarılmasına rağmen bu davranışlarının yinelemesi İş Kanunu m. 25/II-h bendi kapsamında "yapmakla ödevli bulunduğu görevleri kendisine hatırlatıldığı halde yapmamakta ısrar etmesi" hükmü kapsamında iş sözleşmesi işveren tarafından haklı nedenle fesih gerekçesi yapılabilir[1259]. Zira, 6331 sayılı Kanun'un 19. maddesinde "çalışanların

olarak çalıştığı sitede görevli dava dışı kadın hizmetliye yönelik tedirgin edici, sıkıntı verici ve güvenliğinden kuşku duymasına yol açar nitelikte davranışlarda bulunduğu anlaşılmış olup işçinin sadakat borcu, işverenin işi ve işyeri ile ilgili hukuken haklı menfaatlerini korumayı, işverene zarar verecek ve risk altına sokabilecek davranışlardan kaçınmayı da gerektirdiği gözetildiğinde, davacının ispatlanan eylemlerinin, doğruluk ve bağlılığa uymayan davranışlar olduğu.." tespit edilmiştir. Yargıtay 22. HD., E. 2017/17966, K. 2018/25183, T. 22.11.2018.

1258) Süzek, [2019], İş Hukuku, s. 674; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 556-557; Yargıtay 9. HD., E. 2022/6276, K. 2022/7894, T. 15.06.2022; Yargıtay 9. HD., E. 2018/2956, K. 2018/20981, T. 20.11.2018.

1259) Yargıtay 9. HD., E. 2017/5618 K. 2017/13712 T. 20.9.2017 tarihli kararında iş sağlığı ve güvenliği tedbirlerine uygun hareket etmeyen işçinin iş akdinin haklı sebeple feshedilebileceğine karar vermiştir. Kararda: "Davacı işçinin uyarılara rağmen her hangi bir sağlık raporu sunmadığı ve çelik uçlu ayakkabıyı almamakta ısrar ettiği, iş güvenliği için gerekli çelik uçlu ayakkabıyı ısrarla teslim almayan ve giymeyen davacının iş güvenliği kapsamında kendi can güvenliğini ve buna bağlı olarak iş güvenliğini tehlikeye düşürdüğü, bu davranışında ısrarlı olduğu, " Kendi isteği veya savsaması yüzünden işin güvenliğini tehlikeye düşüren " davacının iş akdinin işveren tarafından 4857 sayılı Yasa'nın 25/II-ı maddesine göre feshinin yasaya uygun olduğu, davacının davranışlarının temadi etmesi karşısında İş Kanunu'nun 26. maddesindeki altı iş günlük hak düşürücü sürenin söz konusu olmayacağı anlaşıldığından, davacının kıdem tazminatı ve ihbar tazminatı taleplerinin reddi gerekirken yerinde olmayan gerekçeyle kabulü hatalı olup bozmayı gerektirmiştir." Yargıtay 9. HD., E. 2014/25783 K. 2015/11738 T. 24.3.2015; Yargıtay 9. HD.,

yükümlülükleri" düzenlenmiş olup, bu düzenleme kapsamında işçilerin işverence oluşturulmuş talimatlara ve alınmış iş sağlığı ve güvenliği eğitimlerine uygun davranma yükümlülüğü bulunmaktadır. Bu yükümlülüklere aykırı davranışlar, işçinin ve diğer işçilerin bedensel ve ruhsal sağlıkları için riskler ortaya çıkarırsa işverenin bunları dijital izleme uygulamalarıyla tespit etmesi durumunda bu ihlal de işveren tarafından haklı fesih sebebi yapılabilir[1260].

Sahada çalışan bir mümessilin doktor ve eczane ziyaretlerini haftalık planlara göre eksik gerçekleştirdiğinin GPS kayıtlarında ortaya çıkması, hatırlatılmasına rağmen aynı davranışlarda bulunulduğunun yine dijital izlemeyle ortaya çıkması, hatırlatılmasına rağmen aynı davranışları sürdürdüğünün tespit edilmesi durumunda işveren bu veri kapsamında iş akdini haklı nedenle feshetme hakkı doğar[1261]. Önemle eklemek gerekir ki, işçinin verilen görevin bir kısmını

2004/11687E., 2004/27978 K., Karar Tarihi: 15.12.2004; Okur, [2013], Elektronik Gözetleme, s. 184.

1260) Yargıtay dijital izlemeyle tespit edilmiş, işçinin işveren tarafından alınmış iş sağlığı ve güvenliği tedbirlerine uygun davranmamasını, işçinin işini savsamasını haklı fesih sebebi olarak kabul etmektedir. Bkz. Yargıtay 22. HD., E. 2017/20082, K. 2019/4651 T. 28.2.2019 tarihli kararı: "Somut olayda, davalı akaryakıt taşımacılığı yapan işyerinde 15/03/2010- 30/09/2011 tarihleri arası akaryakıt tanker şoförü olarak çalışan davacının iş sözleşmesi, akaryakıt sevkiyatı sırasında yüksek süratle araç kullandığı ve kırmızı ışık ihlali gerçekleştirdiği gerekçe gösterilerek haklı nedenle feshedildiği savunulmuş, Mahkemece davacının eyleminin haklı fesih ağırlığında olmadığı kabul edilerek davaya konu kıdem ve ihbar tazminatlarının kabulüne karar verilmiş ise de dosya içeriğinden, işverence davacıya yeteri kadar güvenli sürüş ve iş güvenliği eğitimi verildiği, davacının feshe konu eyleme ilişkin alınan yazılı savunmasında kırmızı ışıkta geçerek trafik kurallarını ihlal ettiğini kabul ettiği, iş sözleşmesinin 6.maddesinde, Trafik Yönetmeliği kurallarına aykırı davranma ve kuralları ihlal etmenin işten çıkarma sebebi olarak belirtildiği anlaşılmaktadır. Bu bağlamda feshe konu eylemin niteliğinden anlaşılacağı üzere davacının kullandığı araçta taşınan akaryakıtın yanıcı ve patlayıcı özelliği düşünüldüğünde meydana gelecek en basit bir kazanın dahi çok ağır sonuçlara yolaçacağı ve işyeri ve iş güvenliği bakımından tehlike oluşturacağı kabul edilmelidir. Tüm bu sebeplerle, somut olay bakımından, davalı işverenin davacı işçinin iş sözleşmesini 4857 sayılı İş Kanunu'nun 25. maddesinin II. bendinin (ı) alt bendinden yer alan "işçinin kendi isteği ve savsaması yüzünden işin güvenliğini tehlikeye düşürmesi..." sebebine dayanarak haklı sebeple feshettiğinin kabulü ile dava konusu kıdem ve ihbar tazminatı taleplerinin reddi gerekirken, yanılgılı değerlendirme ile yazılı şekilde karar verilmesi isabetli olmayıp bozmayı gerektirmiştir."

1261) Bu durumda haklı fesih ve geçerli fesih nitelendirmesini yaparken iş görme borcunun ifa ediliş biçimine göre bir değerlendirme yapılması gerekir. Yargıtay bu hususu: "İşçinin yapmakla ödevli bulunduğu görevleri, kendisine hatırlatıldığı halde yapmamakta ısrar etmesi, haklı fesih sebebi olarak kabul edilmesine karşılık, 4857 sayılı Kanun'un gerekçesine göre, işçinin "işini uyarılara rağmen eksik, kötü veya yetersiz olarak yerine getirmesi" geçerli fesih sebebidir. Somut olayda, temizlikçi olarak çalışan davacı işçinin, iş sözleşmesi işverence hatırlatıldığı halde görevlerini yapmamakta ısrar etmesi haklı fesih sebebine dayanılarak feshedilmiştir. Dosya kapsamındaki bilgi ve belgelerin birlikte değerlendirilmesinden, davacı işçinin görevini yapmakla birlikte uyarılara

yapması durumunda yapmakla görevli olduğu işi tam olarak neden yapmadığının nedenleri üzerinde durulması gerekir. Ancak görevin tam olarak bildirilmesi ve işçinin buna rağmen ısrar etmesi durumunda haklı nedenle fesih hakkı doğar[1262].

gg) Dijital İzlemede İSG Önlemlerine Uygun Davranılmadığının Tespit Edilmesi

İşverenin iş sağlığı ve güvenliği kapsamında oluşturduğu talimatlara işçinin uymadığı, işin güvenliğini tehlikeye attığının dijital izleme uygulamasıyla tespit edilmesi halinde işveren bu veriyi işçinin kastının veya ihmalinin varlığını da dikkate alarak İş Kanunu m. 25/II-ı bendi kapsamında işçinin "işin güvenliğini tehlikeye düşürmesi" hükmüne dayanılarak iş sözleşmesini haklı nedenle feshedebilir[1263].

Belirmek gerekir ki, iş akdinin iş güvenliğini tehlikeye düşürmek ve işyerinin İSG prosedürlerine uygun yerine getirmemesi sebebiyle haklı nedenle feshedilmesi için bir zararın ortaya çıkması gerekli değildir. Öte yandan iş sağlığı ve güvenliğinin tehlikeye düşürüldüğünün işçinin kastı veya savsaması (ihmali) sebebiyle ortaya çıkması zorunludur[1264]. Örneğin giyilebilir barette yer alan dijital

---

rağmen gereği gibi ifa etmediği, bu hususun iş ilişkisi sürecinde olumsuz etki yarattığı sabittir. Ancak, davacı işçinin 'işini uyarılara rağmen eksik, kötü veya yetersiz olarak yerine getirmesi' 4857 sayılı Kanun'un 18. maddesi uyarınca işçinin davranışlarından ve yeterliliğinden kaynaklanan geçerli fesih sebebidir" biçiminde değerlendirmiştir. Yargıtay 22. HD., E. 2013/1836, K. 2014/171, T. 14.01.2014.

1262) Süzek, [2019], İş Hukuku, s. 677.

1263) Sevimli, [2006], Özel Yaşam, s. 265 vd.; Okur, [2013], Elektronik Gözetleme, s. 183; Aydın, [2022], Kişilik Hakları, s. 129.

1264) Süzek, [2019], İş Hukuku, s. 678; "Somut olayda davacı, davalı bünyesinde toz boyama kabininde kaynakçı ustası olarak çalışmış ve iş sözleşmesi mola saatinde boya fırını içerisinde oturduğunun tespit edilmesi sebebi ile feshedilmiştir. Mahkemece, davacının boya fırını içerisinde oturması iş güvenliğini tehlikeye düşürdüğünden sözleşmenin davalı işveren tarafından haklı sebeple feshedildiğinin kabulü ile kıdem ve ihbar tazminatı alacaklarının reddine karar verilmiştir. Ancak, dosya içeriğine göre davacının eyleminin ne şekilde iş güvenliğini tehlikeye düşürdüğü açıklığa kavuşturulmamıştır. Bu durumda mahkemece, iş sağlığı ve güvenliği uzmanı eşliğinde işyerinde keşif yapılarak davacının eyleminin iş sağlığı ve güvenliğini ./..tehlikeye düşürüp düşürmediği, işveren açısından haklı fesih şartlarının oluşup oluşmadığı açıklığa kavuşturulmalı ve oluşacak sonuç dairesinde kıdem ve ihbar tazminatı istekleri hakkında bir karar verilmelidir." Yargıtay 22. HD., E. 2014/480, K. 2015/12127, T. 30.03.2015.

kamerada işçinin vinci salıncak olarak kullandığının tespit edilmesi, kamera gözetlemesinde işveren vekili olan işçinin İSG tedbirlerine uygun olmayacak biçimde şalteri kapatmadan makinelere, elektrik arızalarına müdahale ettirildiğinin, girilmesinin yasak olduğu cips kazanının içine girdiğinin tespit edilmesi iş sağlığı ve güvenliğini tehlikeye düşüren verilerdir. İşveren dijital izlemede elde ettiği bu veri kapsamında iş sözleşmesini haklı nedenle feshetme hakkını kullanabilir[1265].

II. Hukuka Aykırı Dijital İzlemenin Sonuçları

Hukuka aykırı dijital izleme uygulamalarıyla elde edilen veri iş sözleşmesinin feshinde kullanılamaz[1266]. Öte yandan iş sözleşmesi güven esaslı bir

1265) İşçinin iş sağlığı ve güvenliğini tehlikeye düşürmesini kamera kayıtlarında tespit eden işverenin haklı nedenle feshini Yargıtay 22. HD., E. 2011/12775, K. 2012/5476, T. 26.03.2012 tarihli kararında yerinde bulmuştur. Kararda özetle: "Kamera kayıtlarına dayanarak Somut olayda; mahkemece bilirkişiye çözümü yaptırılan işyeri güvenlik kamerası kayıtlarından davacının 08.08.2009 tarihinde meydana gelen yangın öncesinde makineye pamuk atarken bir yandan da arkadaşlarıyla sohbet ettiğinin görüldüğü, bunun akabinde çalıştığı makinede yangın çıktığı anlaşılmaktadır. Daha sonra alınan makine mühendisi bilirkişi raporunda olayın oluş şekli kamera görüntülerine göre değerlendirilerek yangının elektrik kontağından çıkma olasılığının bulunmadığı, işçilerin hatalı işlem yapmalarından kaynaklanmasının yüksek ihtimal olduğu belirtilmiştir. Daha önce de işyerinde aynı nitelikte yangınlar çıktığı belirtilmişse de davacının kullandığı makinede ilk kez yangın olduğu ve davacının işine gereken özeni göstermediğinin kamera kayıtlarıyla belirlendiği dikkate alındığında davranışlarının iş güvenliğini tehlikeye düşürücü nitelikte olduğu ve haklı neden oluşturduğu açıktır." tespitleri yapılmıştır. Aynı yönde, Yargıtay 9. HD., E. 2016/14055, K: 2016/10749, T. 28/04/2016.

1266) AYM, E.Ü. kararı Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020; Aynı doğrultuda AYM, Ömür Kara ve Onursal Özbek kararı § 50; AYM, Fırat Gerçek Kararı, Başvuru Numarası: 2019/25604, Karar Tarihi: 21.09.2022; Yargıtay 22. HD, E. 2017/21857 - K. 2019/9884, T. 07.05.2019. AYM, Fırat Gerçek Kararında bu hususu şu şekilde değerlendirmiştir (§ 29, § 30 ve § 31): "İstinaf merciinin gerekçelerinin başvurucuya özgü belge ve iletişim araçları üzerinden değil Ö.Ç. isimli işçi bağlamında Ö.Ç.nin kullanımına sunulan telefon üzerinden ortaya konulduğu anlaşılmıştır. Bu durumda başvurucuya/işçilere, işveren tarafından teslim edilen iletişim araçlarının kullanım sınırları, işverenin anılan araçları inceleme/denetleme yetkisi ve amaca aykırı kullanılmasına bağlanan yaptırım hususunu da içerecek şekilde aydınlatma yükümlülüğünün yerine getirildiği, Mahkemenin de başvurucu özelinde bu yönde bir bilgilendirmenin yapılıp yapılmadığına dair bir araştırma yaptığı söylenemez. Bunun yanında işveren, Ö.Ç.nin kullanımında olan telefonda amaçla uyumlu ve sınırlı bir inceleme yaptığını ortaya koyamamıştır. Zira işveren yargılama sürecinde müşteri iletişim bilgilerine ulaşmak adına telefonda inceleme yapıldığını savunsa da telefondan ele geçirilen ve feshe dayanak teşkil eden mesaj içerikleri bu durumu doğrulamamıştır. Kaldı ki mesajlaşma programlarının kişisel olarak da kullanılabileceği gözetildiğinde bir başkasına ait olan cep telefonunun denetlenmesinin ve başvurucuya ait mesajların ele geçirilmesinin başvurucunun özel hayatının ve haberleşmesinin gizliğinin korunması konusundaki makul beklentisine aykırı olduğu açıktır. Mahkemece de bir başkasına ait cep telefonunda yer alan yazışmaların ne suretle denetlendiğine, mesaj içeriklerinin feshe dayanak alınmasının gerekli olup olmadığına ve başvurucunun özel hayatı ile haberleşmesine olan etkisine yönelik herhangi bir

ilişki ortaya çıkardığından işçinin özel hayatı ve kişisel verileri üzerinde ağır müdahalelere sebebiyet veren dijital izleme uygulamalarına karşı işçinin iş akdini haklı nedenle feshetme veya çalışmama hakkının bulunup bulunmadığının incelenmesi gerekmektedir. İşçi işyerinde hukuka uygunluk ölçütleriyle uyuşmayan, gizli dijital izleme uygulamaları kullanıldığını öğrendiğinde izlemenin ihlal ettiği kişilik haklarını dikkate alarak iş sözleşmesini haklı nedenle feshetme hakkını kullanabilir. Ayrıca işçinin kişiliği koruyan koruyucu davaları açma veya uğradığı zararı tazmin etme hakları bulunmaktadır[1267].

1. İşçinin İş Akdini Haklı Nedenle Feshetmesi

İşverenin gerçekleştirdiği dijital izleme uygulaması işçinin özel hayatı ve kişisel verileri üzerinde ağır ihlallere sebebiyet verdiği durumlarda iş sözleşmesinin devamı işçi için çekilemez bir duruma gelebilir. Bu durumda işçi İş Kanunu m. 24/II kapsamında "ahlak ve iyiniyet kurallarına uymayan haller ve benzerleri" düzenlemesi kapsamında haklı nedenle fesih hakkını kullanabilir. Örneğin işyerinde soyunma odalarında gizli kamera gözetlemesinin gerçekleştirildiğinin öğrenilmesi, uzakta çalışan işçinin bilgisi bulunmaksızın tüm bilgisayar ekran aktivitelerinin kaydının gizli bir biçimde alındığı, işçinin kullanımına verilen cep telefonunun kişisel zamanı kapsayacak biçimde izlendiğinin ortaya çıkması İş Kanunu m. 24/II-b bendinde düzenlenen; "işveren işçinin veya ailesi üyelerinden birinin şeref ve namusuna dokunacak şekilde sözler söyler, davranışlarda bulunursa veya işçiye cinsel tacizde bulunursa" hükmü kapsamında iş akdinin haklı nedenle fesih hakkını işçiye verir.

---

değerlendirme yapılmamıştır (benzer değerlendirmeler için bkz. Samet Ayyıldız, B. No: 2018/34548, 28/12/2021, §§ 36-46). Nitekim Anayasa Mahkemesi başvuruya benzer olayları incelediği E.Ü. ve Samet Ayyıldız kararlarında, başvuruculara kurumsal e-posta ve kişisel Whatsapp hesabı içeriklerinin işveren tarafından denetlenmesi ve bu yazışmalar gerekçe gösterilerek iş akdinin feshedilmesi şeklindeki müdahalelerde ihlal kararları vermiştir. Somut olayda da yukarıda belirtilen gerekçelerle anılan kararlardaki ilkelerden ayrılmayı gerektirir bir durum bulunmadığı sonucuna ulaşılmıştır."

1267) Okur, [2013], Elektronik Gözetleme, s. 185.

Öte yandan işveren tarafından gerçekleştirilen hukuka uygunluk ölçütleri kapsamında bulunan bir dijital izlemede yer alan delile dayanarak işçinin iş sözleşmesini haklı nedenle feshetmesi de mümkündür. Örneğin bir toplantıda işverenin işçinin şeref ve haysiyetini kırıcı beyanlarda bulunması ve işçinin bunu sonradan izlemesi veya başka işçiler tarafından işçiye bildirilmesi ve delilin dijital izleme uygulamasında bulunması durumunda işçi, İş Kanunu m. 24/II-c bendinde düzenlenen, "işçi hakkında şeref ve haysiyet kırıcı asılsız ağır isnad veya ithamlarda bulunursa" hükmü kapsamında haklı fesih hakkını kullanabilir.

Belirtmek gerekir ki, işçi açısından "ahlak ve iyiniyet kurallarına uymayan haller ve benzerleri" ifadesi kapsamında haklı nedenle fesih hakkını düzenleyen İş Kanunu m. 24/II fıkrasında yer alan "benzerleri" sözcüğü fıkrada örneklendirilen durumların sınırlı sayıda olmadığını göstermektedir[1268]. Bu itibarla işçinin kişilik hakkı kapsamında korunan özel hayatı ve kişisel verileri üzerinde hukuka aykırı dijital izleme uygulamalarıyla gerçekleştirilen müdahaleler suç niteliği bulunmasa veya namusa ve şerefe dokunan bir durum olmasa dahi "benzerleri" sözcüğü kapsamda değerlendirilmeli ve işçinin özel hayatına hukuka aykırı müdahale "sataşma" (İş Kanunu m. 24/II-c) kapsamında kabul edilerek işçi açısından haklı fesih hakkının doğduğunu kabul etmek gerekir[1269].

İşverenin gizli dijital izleme uygulamalarıyla kişisel zamanlarının izlendiğini öğrenmesi veya işyerinde dinlenme alanlarında gizli kamera kullandığının tespit edilmesi işçinin kişilik hakları üzerinden ağır ihlaller ortaya çıkardığından işçi açısından, İş Kanunu m. 24/II-b kapsamında haklı fesih hakkı doğar. Benzer biçimde işverenin konum izleme uygulamalarıyla işçinin kişisel zamanını veya işçinin tüm konum hareketlerini gizlice izlediğinin öğrenen işçi, bilişim sistemleri ve internet izlerinin gizlice izlendiğini ve kayıt altına alındığını

1268) Sevimli, [2006], Özel Yaşam, s. 257; Okur, [2013], Elektronik Gözetleme, s. 187 vd.; Süzek, [2019], İş Hukuku, s. 665.
1269) Sevimli, [2006], Özel Yaşam, s. 259.

öğrenen işçi de iş akdini haklı nedenle feshedebilir[1270].

Eklemek gerekir ki, meslekleri gereği izlenmesi gereken meslek gruplarında işçinin izlendiğini bilmesi ve gerçekleşen dijital izlemenin hukuka uygun olması durumunda da işverenin dijital izleme uygulaması sonucu elde ettiği veriyi ifşa etmesi, başkalarıyla paylaşması işçi açısından haklı sebeple fesih gerekçesi olduğunu kabul etmek gerekir[1271]. Zira işverenin bu şekilde davranması gözetme borcuna aykırıdır.

Dijital izleme uygulamalarının işveren vekili tarafından uygulanması ve bu uygulamaların işçinin kişilik değerleri üzerinden ihlale sebebiyet vermesi de yukarıda yaptığımız değerlendirmeleri değiştirmeyecektir. İşçinin özel hayatı ve kişisel verilerine ilişkin hakları üzerinde gerçekleştirilen ihlalin işveren vekili tarafından gerçekleştirilmesi durumunda da işçi iş sözleşmesini haklı sebeple feshedebilir[1272]. Yukarıda ele alındığı üzere işçi haklı feshe ilişkin hakkını kullanırken İş Kanunu m. 26/1'de öngörülmüş olan sürelere uymalıdır[1273].

2. İşçinin Çalışmaktan Kaçınma Hakkı

İşçinin çalışmaktan kaçınma hakkı, işverenin iş sözleşmesinden doğan edimlerini yerine getirmemesi veya işçinin asli edimi olan iş görme edimini ifa etmesi için gereken hazırlık fiillerini gerçekleştirmemesi sebebiyle işçinin bu edimler yerine getirilinceye kadar iş görmeme olanağıdır[1274]. İş mevzuatında

1270) F. Burcu Savaş, "İş Hukukunda Siber Gözetim", Çalışma ve Toplum, 2009/3, [2009], s. 124; Okur, [2013], Elektronik Gözetleme, s. 188.
1271) Okur, [2013], Elektronik Gözetleme, s. 188-189; Yargıtay'a göre: "Kişinin gizli alanını oluşturan özel yaşamının gizliliğine dokunulamayacağından, sıfatı ve konumu ne olursa olsun, kişinin oluru bulunmadan özel yaşamına ve haberleşmesine ilişkin bilgiler kamuoyuna açıklanamaz." Yargıtay 4. HD., E. 2009/13627 K. 2010/10270 T. 14.10.2010.
1272) Okur, [2013], Elektronik Gözetleme, s. 188, Sevimli, [2006], Özel Yaşam, s. 259.
1273) Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersleri, s. 475.
1274) Betül Erkanlı Başbüyük, "İş Görmekten Kaçınma Sebebi Olarak İşyerinde Cinsel Taciz", İSGHD, C. 16, S. 61, [2019], s. 128-129; Öztürk, [2021], Talimatlara Uyma, s. 657 ve 2062. dipnotta atıf yapılan yazarlar.

çalışmaktan kaçınma hakkı iki farklı neden olan "ücretin gününden ödenmemesi" durumunda İş Kanunu m. 34/1 kapsamında çalışmaktan kaçınma olanağı[1275] ve İSGK m. 13/2. ve 3. bendinde[1276] düzenlenmiş olan "işyerinde ciddi ve yakın bir tehlikenin varlığı hali" kapsamında çalışanların çalışmaktan kaçınma hakkını kullanabileceği kabul görmektedir. Ayrıca işverenin, işçinin iş görme borcunu ifa edebilmesi için uygun hazırlık fiillerini yerine getirmemesi halinde işçinin "işveren temerrüdü" kapsamında çalışmaktan kaçınma hakkını kullanması gerekir.

Doktrinde işçinin çalışmaktan kaçınma hakkının hukuki niteliğiyle ilgili farklı görüşler ileri sürülmektedir[1277]. Görüş farklılıkları asıl olarak işçinin çalışmaktan kaçına hakkını dayandırdığı sebebe göre farklılaşmaktadır. Buna göre tartışma temelde karşılıklı sözleşmelerde ifada sırayı düzenleyen "ödemezlik def'ine" ilişkin olan TBK'nın 97 ve işçinin iş görme ediminin ifasını engelleyen durumlarda ücreti düzenleyen "işverenin temerrüdüne" ilişkin TBK m. 408 çerçevesinde gelişmektedir[1278].

1275) İş Kanunu m. 34/1 düzenlemesi: "Ücreti ödeme gününden itibaren yirmi gün içinde mücbir bir neden dışında ödenmeyen işçi, iş görme borcunu yerine getirmekten kaçınabilir. Bu nedenle kişisel kararlarına dayanarak iş görme borcunu yerine getirmemeleri sayısal olarak toplu bir nitelik kazansa dahi grev olarak nitelendirilemez. Gününde ödenmeyen ücretler için mevduata uygulanan en yüksek faiz oranı uygulanır."

1276) İSGK m. 13'ün 2. ve 3. Fıkrası: "(2) Kurul veya işverenin çalışanın talebi yönünde karar vermesi hâlinde çalışan, gerekli tedbirler alınıncaya kadar çalışmaktan kaçınabilir. Çalışanların çalışmaktan kaçındığı dönemdeki ücreti ile kanunlardan ve iş sözleşmesinden doğan diğer hakları saklıdır. (3) Çalışanlar ciddi ve yakın tehlikenin önlenemez olduğu durumlarda birinci fıkradaki usule uymak zorunda olmaksızın işyerini veya tehlikeli bölgeyi terk ederek belirlenen güvenli yere gider. Çalışanların bu hareketlerinden dolayı hakları kısıtlanamaz." biçimindedir.

1277) İşçinin çalışmaktan kaçınma hakkına yönelik detaylı görüşler için bkz. Betül Erkanlı Başbüyük, İşçinin İş Görmekten Kaçınma Hakkı, Seçkin Yayıncılık, Ankara, [2020], s. 63 vd.; Murat Engin, "Yeni İş Kanunu Tasarısı ve İşçinin İş Görmekten Kaçınma Hakkı", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 5, S. 1, [2003], s. 91; Ünal, [2018], Yaş Ayrımcılığı, s. 498; Sarper Süzek, İşçi Ücretlerinin Ödenmemesinin Hukuki Sonuçları, AÜHFD, C. 56, S. 4, [2007], s. 210-211; Arzu Arslan Ertürk, "İş Hukuku Boyutuyla Türkiye'de Psikolojik Taciz (Mobbing) ve Dünyadan Örnekler", MÜHFD, C. 20, S. 1, [2014], s. 308; İbrahim Aydınlı, "İşverenin İşyerinde "Çalışan" İşçilerin İş Görmekten Kaçınma Hakkı", Çimento İşveren Dergisi, Cilt: 19, Sayı: 4, Temmuz, [2005], s. 18 vd.; Seracettin Göktaş, Türk İş Hukukunda İşçinin Çalışmaktan Kaçınma Hakkı, Yetkin Yayınları, Ankara, [2008], s. 214.

1278) Ercan Akyiğit, "Ücreti Geciken İşçinin Çalışmaktan Kaçınması", Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Sayı: 5, [2005], s. 23; Erkanlı Başbüyük, [2020], İş Görmekten Kaçınma, 67-68.

Belirtmek gerekir ki, iki tarafa borç yükleyen iş sözleşmesinde işçinin iş görme borcunun karşılığını işverenin ücret ödeme borcu oluşturmaktadır. Ödemezlik def'i görüşüne göre işçinin ödemezlik def'ine başvurarak çalışmaktan kaçınması işvereni karşı edim olan ücreti ödemeye zorlayacaktır. Ödemezlik def'i görüşü karşılıklı edimler yönünde nitelendirme yapıldığında taraf edimleri örtüşmekte ve işçinin çalışmaktan kaçınması meşru bir temele dayandığından işçi açısından bir temerrüt durumu ortaya çıkarmamaktadır. Öte yandan ödemezlik def'i işçinin çalışmaktan kaçındığı sürede ücretinin ödenmemesi biçiminde işçi aleyhine bir sonuç ortaya çıkarmaktadır. Bu aleyhe sonuca sebebiyet vermemek için kanaatimizce işçinin ücretinin ödenmemesi, ciddi ve yakın bir tehlikenin bulunması veya işverenin işçinin iş görme borcunu ifa etmesi için ön hazırlık fiillerini yerine getirmemesi fark etmeksizin işçinin çalışmaktan kaçınma hakkının hukuki nitelendirmesini "işveren temerrüdü" çerçevesinde gerçekleştirmek iş hukukunun "işçi lehine yorum" genel yaklaşımına uygun olacaktır[1279].

İşverenin alacaklı temerrüdüne düştüğünü söyleyebilmek için öncelikli olarak "işçinin iş görme edimini ifaya hazır olması" ve "iş görme ediminin ifasının mümkün olması", işverenin ise bu ifayı "haklı veya objektif bir neden olmaksızın kabulden kaçınması veya işin yerine getirilebilmesi için gerekli hazırlık fiillerini yapmaması koşulu" aranmaktadır. İşverenin kullandığı dijital izleme uygulamaları açısından olaya bakıldığında işveren işyerinde TBK m. 417/1 hükümlerine uygun bir çalışma düzeni oluşturmak ve işçinin bedensel ve ruhsal sağlıklarını gözetmek zorundadır. Bu yükümlülük işçinin kişilik haklarını, özel hayatını ve kişisel verilerini koruyacak biçimde hareket etme yükümlülüğünü de içermektedir. İşçinin kişiliği, onuru, mesleki saygınlığı ve temel hak ve özgürlükleriyle ilgili olan bu yükümlülük, iş görme ediminin ifası için ön hazırlık fiillerini oluşturmaktadır. Dolayısıyla ön hazırlık fiillerine aykırı dijital izleme uygulamalarının bulunması durumunda işçi çalışmaktan kaçınma hakkını kullanabilir[1280].

1279) Görüşün detayları için bkzı. Erkanlı Başbüyük, [2020], İş Görmekten Kaçınma, s. 63 vd.
1280) Erkanlı Başbüyük, [2020], İş Görmekten Kaçınma, 74-78.

Sonuç olarak işverenin hukuka uygunluk ölçütlerini barındırmayan dijital izleme uygulamaları kullanması işçinin özel hayatı, kişisel verileri ve kişilik değerleri ile temel hak ve özgürlükleri üzerinde ihlal edici sonuçlar ortaya çıkarır. İşçi özel hayatı ve kişisel verileri üzerinde ihlal edici sonuçlar ortaya çıkaran dijital izleme uygulamalarının işyerinde kullanıldığını öğrendiğinde çalışmaktan kaçınma hakkını kullanabilir. Ayrıca eklemek gerekir ki, işverenin koruma borcu kapsamında işçinin zararına olabilecek dijital izleme uygulamalarından kaçınma yükümlülüğü de bulunmaktadır[1281]. Zira dijital izleme uygulamaları işçinin temel hak ve özgürlükleri üzerinde ihlal edici sonuçlar ortaya çıkardığından işverenin işçinin iş görme borcunu ifa edebileceği çalışma ortamından bahsedilemez. Bu sebeple işveren işçinin ifasını kabulde temerrüde düşeceğinden işçi çalışmaktan kaçınma hakkını kullanabilir[1282].

Önemle belirtmek gerekir ki, hukuka uygunluk ölçütlerine uymayan dijital izleme uygulamaları sebebiyle işçinin çalışmama hakkını kullanabilmesi için işverenin yükümlülükleri kapsamında gerçekleşen ihlal ile iş görme borcu arasında bir bağlantının bulunması gerekmektedir. Bu bağlantının olmaması örneğin işverenin işçiyi kişisel zamanında dijital izleme uygulamalarıyla takip etmesi başka hukuki yaptırımlar gerektirmesine rağmen iş görme borcu ile doğrudan ilgili olmadığından işçi çalışmayı reddetme hakkını kullanamayacaktır[1283]. İşyerinde işçilerin giyinme, spor, dinlenme odalarının gizli dijital izleme uygulamalarıyla izlendiğinin; bilgisayarların ekran aktivitelerinin tamamını kaydeden dijital izleme uygulamalarının kullanıldığının ortaya çıkması durumları iş görme borcuyla bağlantılı durumlardır.

1281) Süzek, [2019], İş Hukuku, s. 386.
1282) Okur, [2013], Elektronik Gözetleme, s. 186.
1283) Okur, [2013], Elektronik Gözetleme, s. 187 vd.

3. İşçinin Kişilik Haklarını Koruyan Davaları Açması

Kişilik hakkının korunması insanı insan yapan onuru, saygınlığı, ruhsal ve bedensel bütünlüğü, ismi, resmi, yaşam varoluş biçimi, özel hayatı, kişisel verileri gibi tüketilemeyecek ve para ile ölçülemeyecek değerlerle ilgili olduğundan Medeni Kanun'da kişiliği iç ve dış müdahalelere karşı koruyucu düzenlemeler öngörülmüştür[1284]. İşverenin işçiyi dijital izleme uygulamalarıyla izlemesi ve bu uygulamalarla işçinin kişisel verilerini işlemesi kişilik hakları üzerinde müdahaleci sonuçlar ortaya çıkardığından[1285] dijital izleme için KVK hukukunda öngörülmüş olan kişisel veri işleme usul ve esaslarının varlığı aranmalıdır[1286]. Aksi durumda işçi kişilik haklarına yönelen ihlal edici dijital izleme uygulamalarını kişiliği koruyucu davalara konu edebilir.

a) Kişilik Haklarına Saldırının Önlenmesi Davası

MK m. 24/1 hükmüne göre: "hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını" açacağı önleme davasıyla isteyebilir. MK m. 25 ise kişilik hakkına yönelik saldırı bulunması durumunda ilgili kişinin açabileceği davalar hüküm altına alınmıştır. Buna göre kişi "saldırı tehlikesinin önlenmesini", "sürmekte olan saldırıya son verilmesini", "sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini" açacağı davalarla talep edilebileceğini hüküm altına almıştır[1287]. Önleme davasının MK m.

1284) Serozan, [2013], Medeni Hukuk, s. 453; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 198-199; Oğuzman/Öz, [2019], Borçlar Genel, II. Cilt, s. 32; Eren, [2019], Borçlar Genel, s. 896; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 208-209; Dural/Öğüz, [2022], Kişiler Hukuku, s.139; Bilge Öztan, Şahsın Hukuku: Hakiki Şahıslar, Turhan Kitabevi, Ankara, 2000, s.148, (Öztan, [2000], Şahsın Hukuku); Öztan, [2021], Temel Kavramlar, s. 261; Hüseyin Hatemi, Medeni Hukuka Giriş, On İki Levha Yayınları, İstanbul, [2004], s. 92, (Hatemi, [2004], Medeni Hukuk); Serap Helvacı, Türk ve İsviçre Hukukunda Kişilik Hakkını Koruyucu Davalar, Beta Basım, İstanbul, [2001], s. 99-100.

1285) Yargıtay 22. HD., E. 2015/28830 K. 2018/15646 T. 25.6.2018.

1286) Okur, [2013], Elektronik Gözetleme, s. 36.

1287) Serozan, [2013], Medeni Hukuk, s. 475 vd.; Oğuzman/Seliçi/Oktay – Özdemir, [2016], Kişile Hukuku, s. 236 vd.; Sevimli, [2006], Özel Yaşam, s. 253; Okur, [2013], Elektronik Gözetleme, s. 193; Gürsel, [2016], İşçinin Kişisel Verileri, s. 412.

25'teki davalardan farkı kişilik haklarına henüz bir saldırı söz konusu olmasa ve fakat yakın bir zamanda saldırının gerçekleşeceğine dair ciddi bulguların bulunması halinde açılabilmesidir[1288].

İşçinin kişilik hakkına ciddi ve yakın bir saldırı tehlikesinin bulunması önlenme davasının açılma koşuludur, böyle bir durum söz konusu değilse önleme davası açılamaz. Örneğin işverenin dijital izleme uygulamasında işlediği işçi verisini, işçinin açık rızasını almadan yurt dışında bulunan bir analiz firmasına transfer etme kararı alması işçinin kişilik hakları için ciddi ve yakın bir saldırı tehlikesi ortaya çıkarır. İşverenin depoda çalışan işçilerin işyerinden çıkabilmelerini ancak kameraların bulunduğu bir odada soyunmaları ve çantalarını boşaltmaları koşuluna bağlayan bir karar alması ve bu uygulamanın kısa süre içinde başlayacağına yönelik duyuruda bulunması işçinin kişilik hakları üzerinde ciddi ve yakın bir saldırı tehlikesi ortaya çıkarmaktadır. Bu durumlarda işçi hakimden kişilik haklarına yönelen saldırının durdurulmasına yönelik bir karar vermesini isteyebilir.

Eklemek gerekir ki, işçinin önleme davasını açabilmesi için gerçekleştirilecek dijital izlemenin kişilik haklarına yönelik haksız nitelikte olması yeterlidir. Ayrıca işverenin kusurlu olması bu davanın açılmasında şart değildir. Bu durumda hakim işverenin kişilik hakkına saldırıya yönelik dijital izleme uygulamasını yasaklayan bir karar verir[1289].

b) Saldırının Durdurulması Davası

İşçinin kişilik haklarını ihlal eden bir saldırının durdurulmasını işçi, MK m. 25/1 kapsamında isteyebilir. Saldırının durdurulması davasında başlamış ve devam eden bir saldırının durdurulması isteme konu edilir. Önleme davasında olduğu gibi

1288) Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 243; Helvacı, [2012], Gerçek Kişiler, s. 128; Dural/Öğüz, [2022], Kişiler Hukuku, s. 144; Öztan, [2000], Şahsın Hukuku, s. 153; Gürsel, [2016], İşçinin Kişisel Verileri, s. 412.
1289) Serozan, [2013], Medeni Hukuk, s. 476; Oğuzman/Seliçi/Oktay – Özdemir, [2016], Kişiler Hukuku, s. 236.

durdurma davasında da saldırının hukuka aykırı olması yeterlidir, ayrıca gerçekleştirenin kusuru aranmaz[1290]. İşçi açacağı dava ile işverenin dijital izleme uygulamasını sona erdirilmesini veya çalışma süreleri içinde uygulanmasını, hukuka aykırılıklar varsa giderilmesini, işlenen kişisel verilerinin güvenliğinin sağlanması için gerekli teknik ve idari tedbirlerin alınmasını isteyebilir[1291].

İşverenin haklı bir nedeni bulunmaksızın işyeri giriş sistemini şifre veya kart bazlı olmaktan çıkarıp retina ve yüz taraması veya parmak izi taraması gibi işçinin biyometrik verileri esaslı hale getirmesi işçinin kişilik hakları üzerinde orantısız bir müdahale ortaya çıkarır. İşçi biyometrik verileri üzerinde gerçekleşen bu orantısız saldırının durdurulmasını MK m. 25/1 kapsamında hakimden isteyebilir. İlgili başlıkta[1292] biyometrik veri ve AYM kararı kapsamında ele alınan AYM, Ramazan Şahin kararına konu olayda Söke Belediye Başkanlığı parmak izi verisi işleyen sistemle mesai takibi yapmak istemiş, başvurucu ise bunu özel hayatına orantısız bir müdahale olduğunu belirterek dilekçeyle kuruma başvurmuştur. Başvurusunun reddedilmesi üzerine kurum işleminin iptali ve özel hayatı üzerinde gerçekleşen orantısız müdahalenin durdurulması için idare mahkemesine dava açmıştır. İdare mahkemesi AİHM kararlarına da atıf yaparak bu şekilde takip gerçekleştirilmesinin özel hayat üzerinde orantısız bir müdahale gerçekleştirdiğine karar vererek kurum işlemini iptal etmiştir. Bunun üzerine kurum istinaf başvurusu yapmış ve İzmir Bölge İdare Mahkemesi 2. İdari Dava Dairesi istinaf başvurusunu kabul ederek davayı kesin olarak reddetmiştir. Başvurucu konuyu AYM'de bireysel başvuruya konu etmiştir. AYM, kurumun uygulamasını özel hayat ve kişisel veriler üzerinde orantısız bir müdahale olduğuna karar vermiştir[1293]. Eklemek gerekir ki bu tür dijital izleme uygulamalarının gerçekleştirilmesine işçinin rızası bulunsa dahi rızanın geçerliliği, aynı amacı gerçekleştirecek daha az müdahaleci yöntemlerin

1290) Serozan, [2013], Medeni Hukuk, s. 463 vd.; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 243 vd.; Dural/Öğüz, [2022], Kişiler Hukuku, s. 146.
1291) Okur, [2013], Elektronik Gözetleme, s. 195.
1292) Bkz. § 7. 2.
1293) AYM, Ramazan Şahin kararı, Başvuru Numarası: 2018/26771, Karar Tarihi: 10.03.2022, Yayımlandığı Resmi Gazete: 14.04.2022 tarih ve 31809 sayı.

bulunup bulunmadığı ve izlemenin genel ilkelere uygunluğu kapsamında değerlendirmeye konu edilmesi gerekir.

c) Saldırının Hukuka Aykırılığının Tespiti Davası

Dijital izleme uygulamalarıyla kişilik haklarının saldırıya uğradığını düşünen işçi MK m. 25/1 hükmü kapsamında "sona ermiş olsa bile etkileri devam eden bu saldırının hukuka aykırılığını tespitini" talebe konu edebilir[1294]. Örneğin işverenin uzaktan çalışmada işçiyi denetlemek için işçinin kullanımına verdiği cep telefonuna yüklediği dijital izleme uygulamasıyla işçinin kişisel zamanını, aktivitelerini, uyku düzenini, internet trafiğini izlemesi durumu işçinin kişilik hakkı üzerinde ihlal edici sonuçlar ortaya çıkarır. İşçi kişilik hakkına yönelik bu saldırıyı fark etmesi üzerine işverenin ihlale son vermesini, ihlalin etkisini ve dijital izleme uygulaması kapsamında işlenen verileri, verilerinin aktarıldığı kişi ve yerler, özel hayatı üzerindeki ihlalin boyutunun veya saldırının hukuka aykırılığının tespiti için tespit davası açabilir.

Belirtmek gerekir ki, tespit davasını düzenleyen HMK m. 106 hükmü kapsamında tespit davası açabilmek için bir hukuki yararın bulunması gerekmektedir. Dijital izleme uygulamasının işçinin hakları üzerinde oluşturduğu hukuka aykırılık devam ettikçe veya saldırı etkisi sürdükçe işçinin bu davayı açmada hukuki yararı bulunduğu kabul edilmelidir[1295].

d) Kararın Üçüncü Kişilere Bildirimi ve İlanı

Dijital izleme uygulamasıyla içinin kişilik hakları üzerinde gerçekleşen ihlalin çok sayıda kişi tarafından bilinmesi veya dijital izlemedeki yanlış veriler ve sonuçlar sebebiyle işçinin kişilik hakkı üzerinde gerçekleşen ihlalin çok kişi

1294) Okur, [2013], Elektronik Gözetleme, s. 194-195; Oğuzman/Seliçi/Oktay-Özdemir, [2016], Kişiler Hukuku, s. 244-245; Dural/Öğüz, [2022], Kişiler Hukuku, s. 144.
1295) Helvacı, [2012], Gerçek Kişiler, s. 133; Gürsel, [2016], İşçinin Kişisel Verileri, s. 415.

tarafından bilinmesi durumunda işçi, MK m. 25/2'deki bildirim veya ilan talebini davada ileri sürerek mahkeme kararının ilan yolu ile üçüncü kişilere bildirilmesi için kararın ilanına karar verilmesini isteyebilir[1296]. Örneğin hukuka aykırı dijital izleme uygulamasında işlenen işçiye ilişkin doğru olmayan verilerin ifşa edilmesi durumunda, işçinin mahkeme kararı ile tespit ettirdiği hukuka aykırılığı ve doğru bilgiyi üçüncü kişilere ilan edilmesi talebini mahkeme yerine getirir.

Dijital izleme uygulamasında kişilik hakkı ihlal edilen işçi açtığı davanın kararının üçüncü kişilere bildirmesinde menfaati bulunabilir. İşçi bu durumda az yukarıda değinilen davalarla birlikte verilecek kararın üçüncü kişilere bildirilmesi isteminde bulunur (MK m. 25/1). Üçüncü kişilere bildirim kişilik hakkı üzerindeki ihlali gerçekleştiren taraf dışındaki ihlalden haberdar olanları ilgilendirmektedir. Zira kararın üçüncü kişilere bildirilmediği veya yayımlanmadığı durumlarda davanın tarafı olmayan üçüncü kişiler karardan haberdar olmayacağından işçinin bu kişilerin mahkeme kararını bilmelerinde menfaati bulunduğu durumda bu menfaat gerçekleşmemiş olacaktır[1297]. Eklemek gerekir ki, mahkeme kararının üçüncü kişilere bildirilmesi talebi ayrı bir dava ile ileri sürülmez. Bu talep ancak önleme, son verme veya hukuka aykırılığın tespiti gibi davalarda ileri sürülebilir[1298].

Hukuka aykırı dijital izlemede uygulamalarıyla işçinin kişilik hakkı üzerinde ihlale katılan üçüncü kişiler de olabilir. Bu kişiler işverenin müşterileri, alt işveren işçileri, tedarikçiler gibi kişilerden oluşur[1299]. Dijital izleme uygulamalarının işçinin kişilik hakları üzerinde oluşturduğu ihlalin haberdarı olan veya katılan bu kişiler açılacak davalarda taraf olmadıklarından mahkeme kararından haberdar olmayacaklardır. Bu sebeple işçinin mahkemeden talepte bulunarak örneğin hukuka aykırı dijital izleme uygulamasının sona erdirilmesi

1296) Helvacı, [2012], Gerçek Kişiler, 139; Öztan, [2000], Şahsın Hukuku, s. 155.
1297) Helvacı, [2012], Gerçek Kişiler, s. 142; Dural/Öğüz, [2022], Kişiler Hukuku, s. 147.
1298) Gürsel, [2016], İşçinin Kişisel Verileri, s. 416; Okur, [2013], Elektronik Gözetleme, s. 196; Helvacı, [2012], Gerçek Kişiler, 139; Öztan, [2000], Şahsın Hukuku, s. 155.
1299) Okur, [2013], Elektronik Gözetleme, s. 196.

davasının sonucunun üçüncü kişilere bildirilmesini istemesi gerekmektedir[1300].

III. Hukuka Aykırı Dijital İzleme: Kamusal Yaptırımlar

Bireyin kişisel verilerinin etkin korunabilmesi için KVK hukukunda suçlar ve kabahatler öngören hükümlere yer verilmiştir. KVKK m. 17'de "suçlar" başlığında TCK m. 135 ila 140'ıncı maddelerine atıf yapılmıştır. Kabahat halleri ise m. 18'de "kabahatler" başlığında hüküm haline getirilmiştir.

1. Hukuka Aykırı Dijital İzleme: İşverene Uygulanacak Ceza Yaptırımları

Kişisel verilerin işlenmesi açısından, KVKK m. 17'de "suçlar" başlığında TCK'nın 135 ila 140. maddelerine atıf yapılarak düzenleme gerçekleştirilmiştir. TCK'nın atıf yapılan hükümleri kişisel verilerin hukuka aykırı olarak ele geçirilmesi ve kaydedilmesi, ilgili kişinin rızası dışında aktarıma konu edilmesi ve yok edilmemesi suçlarına ilişkindir[1301].

Özel hayatın gizliliğine karşı suçlar ve kişisel verilerin hukuka aykırı olarak kaydedilmesine, elde edilmesine ve işlenen kişisel verilerin yok edilmemesine ilişkin olarak 5237 sayılı TCK'nın 132 vd. maddelerinde düzenlemeler yapılmıştır. TCK m. 132 maddesiyle başlayan Dokuzuncu Bölümü'nde "özel hayata ve hayatın gizli alanına karşı suçlar" başlığında özel hayatın gizliliğinin ihlaline neden olan

1300) Okur, [2013], Elektronik Gözetleme, s. 196; Gürsel, [2016], İşçinin Kişisel Verileri, s. 416-417.

1301) Yargıtay 5. CD., E.2014/10479, K.2018/4622 ve 21.6.2018 karar tarihli kararında kişisel verilerin hukuka aykırı biçimde kaydedilmesini: "kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği, belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi" olarak tanımlamıştır.

fiillerin vücut vereceği suçlar ve hükmedilecek cezalar belirlenmiştir[1302]. TCK m. 132'de "haberleşmenin gizliliğini ihlali", m. 133'te "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması", m. 134'te "özel hayatın gizliliğini ihlal suçu" suç olarak düzenlenmiştir. TCK'nın 135. maddesi ile 140 maddesi arasında ise kişisel verilerin kaydedilmesi (m. 135), verileri hukuka aykırı olarak verme veya ele geçirme (m. 136) ve verileri yok etmeme (m.138) biçimindeki kişisel verilere müdahale oluşturan eylemler de suç olarak düzenlenmiştir[1303].

TCK m. 135/1. fıkrası; "hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir" hükmüne haizdir. İkinci fıkrada ise kişisel verilerin hukuka aykırı kaydedilmesi suçunun nitelikli hali "kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır" biçiminde hüküm altına alınmıştır[1304]. İşverenin işçinin bilgisi bulunmaksızın kişisel zamanındaki kişisel verilerini dijital izleme uygulamasıyla kaydetmesi bu hüküm kapsamında değerlendirilir.

1302) 5237 sayılı Türk Ceza Kanunu 01.06.2006 tarihinde yürürlüğe girdi ve Kanun'un yürürlüğe girmesiyle 765 sayılı TCK yürürlükten kalktı. 756 sayılı mülga Kanun'da özel hayatın gizliliğini ve kişisel verileri suç olarak düzenleyen doğrudan bir hüküm yer almıyordu. Dolaylı bazı hükümler vasıtasıyla bu hak korunuyordu. M. Emin Artuk/Ahmet Gökçen/M. Emin Alşahin/Ü. Kerim Çakır, Ceza Hukuku Özel Hükümler, Adalet Yayınevi, 17. Baskı, Ankara [2018], s. 413-414.

1303) Artuk/Gökçen/Alşahin/Çakır, [2018], Ceza Özel, s. 413.

1304) Yargıtay Ceza Genel Kurulu, E. 2012/1514, K. 2014/312, T. 10.06.2014 tarihli kararında TCK m. 135'te yer alan kişisel verileri kaydetme suçunda korunan değeri şu şekilde tespit etmiştir: "TCK'nun 136. maddesinde tıpkı 135. maddesinde olduğu gibi korunan hukuki değer genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir. Bu düzenlemeler ile tüm kişisel veriler koruma altına alındığından kişisel verilerin mutlaka gizli olması zorunlu değildir. Gizli olmayan ve herkes tarafından bilinen kişisel veriler de hukuka aykırı eylemlere karşı korunmalıdır. Zira kişisel verilerin korunmasına ilişkin suçlarda korunan hukuki değer "sır" olmayıp, verinin ilgilisi olan kişinin kişilik haklarıdır… Türk Ceza Kanununun 135. maddesi, kişisel verilerin kaydedilmesi suçunu düzenlemektedir. Maddenin ilk fıkrasında kişisel verilerin kaydedilmesi, ikinci fıkrasında ise kişilerin, siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimseler cezalandırılmaktadır. Ancak madde de kişisel verilerin neler olduğu, kaydetmeden neyin anlaşılması gerektiğine dair bir açıklama bulunmadığı gibi TCK'nın 6. maddesindeki tanımlarda da herhangi bir açıklama bulunmamaktadır. Maddenin konuluş amacını açıklayan gerekçesinde gerçek kişiyle ilgili her türlü bilgi, kişisel veri kabul edilmelidir şeklinde bir açıklama vardır."

İşverenin dijital izleme uygulamasını işçinin sendika üyeliği veya sağlık ve cinsel tercihine ilişkin olması sebebiyle işlemesi ve kaydetmesi (işlemek) suçun nitelikli halini oluşturur. Örneğin işverenin, işçinin açık rızasını almadan ve aydınlatma yükümlülüğünü yerine getirmeksizin sendika üyesi olan (sendika üyeliği ayrıca KVKK açısından özel nitelikli kişisel veridir) işçileri, işyerine giriş için verdiği karta yüklediği bir RFID etiketiyle izlemesi, bu işçilerin işyerindeki ve işyeri dışındaki verilerini kayıt altına alması TCK m. 135/2'nin nitelikli halini oluşturur.

TCK m. 136'da kişisel verilerin hukuka aykırı olarak "verme, yayma veya ele geçirme" suçu düzenlenmiştir. Hükme göre; "kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır." Bu itibarla örneğin işverenin dijital izleme uygulamalarıyla sendikalı işçilere ilişkin işlediği kişisel verileri aynı sektördeki işverenlerle paylaşması kişisel verileri yayma suçunu oluşturur[1305].

İşverenin gizli kamera kullanması, işçinin ses ve görüntüsünü bilgisi dışında kaydetmesi, işçinin gizli görüntülerini yayması veya duşlara, soyunma odalarına, tuvaletlere koyacağı kameralarla denetim gerçekleştirmesi işçinin özel hayatının gizliliğine aşırı bir müdahale gerçekleştireceğinden, işçi "özel hayatın gizliliğinin ihlalini" düzenleyen TCK m. 134 kapsamında suç duyurusunda bulunabilir[1306]. Eklemek gerekir ki, işverenin TCK'nın özel hayatı ve kişisel verileri koruyan 132 ila 140 maddeleri arasındaki düzenlemelerin kapsamında bir ceza alması halinde bu karar hukuk mahkemeleri için de bağlayıcıdır[1307].

1305) Yargıtay Ceza Genel Kurulu "kişisel verileri yayma" suçunda geçen "yayma" sözcüğünü şu şekilde nitelendirmiştir: "Kişisel verileri yayma seçimlik hareketi de çeşitli şekillerde gerçekleştirilebilecektir; internet üzerindeki bir web sitesinde kişisel verileri yayınlamak, birçok kişiye elektronik posta ile ya da telefondan kısa mesajla göndermek, yazılı ya da görsel medyada yayınlamak gibi... Türk Dil Kurumu Büyük Türkçe Sözlüğünde "yaymak"; "birçok kimseye duyurmak, çevreye dağılmasına sebep olmak" olarak açıklanmıştır." Yargıtay Ceza Genel Kurulu E. 2012/1510, K. 2014/331, T. 17.06.2014.
1306) Gürsel, [2016], İşçinin Kişisel Verileri, s. 435.
1307) Cevdet İlhan Günay, İş Kanunu Şerhi, Yetkin Yayıncılık, Ankara, [2005], s. 956.

KVKK m. 17/2. fıkrası; "Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır" biçimindedir. Bu hüküm kapsamında dijital izleme uygulamalarıyla hukuka uygunluk ölçütü yerine getirilerek işlenmiş kişisel verilerin işleme amacı ortadan kalkmasına ve verilerin işlenmesi için belirlenmiş süreler dolmasına rağmen "yok edilmemesi" TCK m. 138'de düzenlenmiş olan "verileri yok etmeme" suçunu oluşturur. TCK m. 138/1. fıkra hükmünde bu suç; "kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir" biçiminde düzenlenmiştir. Bu hüküm kapsamında bir suçun oluşabilmesi için hukuka uygun işlenmiş kişisel verilerin bulunması, bunların yok edilmesi için görevlendirme yapılmış olması ve bu görevli kişilerin kişisel verilerin işlenmesi için belirlenen süreler geçmesine rağmen veriyi yok etmemesi gerekmektedir[1308]. TCK m. 139 hükmüne göre veriyi yok etmeme suçu şikayete bağlı bir suç değildir. Tüzel kişilerin bu suçu işlemesi halinde ise tüzel kişilere özgü öngörülmüş olan güvenlik tedbirleri uygulama alanı bulur[1309].

Sonuç olarak, işçinin kişisel verisinin ve özel hayatına ilişkin bilgilerin işveren tarafından işçi bilgilendirilmeksizin dijital izleme uygulamalarıyla kaydedilmesi, yayılması veya depolanması TCK m. 135 ve devamında hüküm altına alınmış suçların oluşmasına sebebiyet verir. Dijital izlemenin işçinin sendikal bağlantıları, cinsel tercihleri veya sağlığına ilişkin verileri işlemek amacıyla gerçekleştirilmesi TCK m. 135/2'de öngörülmüş olan suçun nitelikli halini oluşturur. Nitekim Yargıtay bir kararında kişisel verilerin "verilmesi, yayılması ya da ele geçirilmesi" suçunun oluşabilmesi için verinin kaydedilmiş halde bulunması gerektiğine karar vermiştir. Kararda bu husus; "belirli veya belirlenebilir" bir kişiye

1308) Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 6. Baskı, Seçkin Yayıncılık, Eylül, [2015], s. 720, (Dülger, [2015], Bilişim Suçları); Sinem Göçmen Uyarer, "6698 Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması", Galatasaray Üniversitesi SBE Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, [2019], s. 208-209.
1309) Dülger, [2015], Bilişim Suçları, s. 725.

ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi, TCK'nın 136/1. maddesinde "verileri hukuka aykırı olarak verme veya ele geçirme" başlığı altında suç olarak düzenlendiği vurgulanmıştır[1310].

2. İşçinin Verilerini Hukuka Aykırı İşleyen İşverene Uygulanacak İdari Yaptırımlar

Kanun koyucu kişisel verilere yönelik ihlallerin bazılarını (TCK m. 135-138 kaydetme, yayma, yok etmeme ve ele geçirme) daha ağır nitelikte görerek ceza hukuku kapsamında suç olarak hüküm altına almıştır. Kişisel verilere yönelen bazı ihlal biçimlerini ise ceza hukukunda uygulama alanı bulan ultima ratio (son çare/araç) ilkesinin bir gereği olarak suç olarak nitelendirmemiş, kabahat olarak hüküm altına almıştır. Böylelikle kişisel verilere yönelen ihlal edici fiillerin bir kısmı suç olarak, diğer bir kısmı ise kabahat olarak idari yaptırıma tabi tutulmuştur[1311].

1310) Yargıtay 18. CD., E. 2016/12443, K. 2019/2912, T. 13/02/2019 kararına özetle: "Bu suçun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir. Herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler de, yasal anlamda "kişisel veri" olarak kabul edilmekte ise de, anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçların doğmaması için, maddenin uygulamasında, somut olayın özellikleri dikkate alınarak titizlikle değerlendirme yapılması, olayda herhangi bir hukuk dalı tarafından kabul edilebilecek bir hukuka uygunluk nedeni veya bu kapsamda nazara alınabilecek bir hususun bulunup bulunmadığının saptanması ve sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir. TCK'nın 136/1. maddesinin, "Bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır." şeklindeki gerekçesinden de anlaşılacağı üzere, kişisel verilerin, verildiği, yayıldığı veya ele geçirildiğinin kabul edilebilmesi için, kişisel verilerin kaydedilmiş halde bulunması, kaydedilmiş haliyle başkalarına verilmesi, yayılması ya da ele geçirilmesi gerekir." hususları tespit edilmiştir.

1311) Zeynel T. Kangal, Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, On İki Levha Yayıncılık, İstanbul, [2019], s. 177.

Kabahatler Kanunu m. 2'de kabahat, idari yaptırımı gerektirir bir haksızlık olarak tanımlanmıştır. Aydınlatma yükümlülüğünün yerine getirilmemesinin ve kişisel verilerin işlenmesinde gerekli teknik ve idari tedbirlerin alınmamasının bir kabahat olarak hüküm altına alınmasıyla korunan hukuki değer bireyin özel hayatın gizliliği ve kişisel verilerine yönelecek ihlallere karşı onu etkin biçimde korumaktır[1312]. Böylelikle idari yaptırımlar vasıtasıyla veri sorumlusunun veri işleme faaliyetinde şeffaf olması ve veri güvenliğine ilişkin yükümlülüklerine uygun hareket etmesi sağlanmak istenmiştir. Veri güvenliğini sağlama yükümlülüğü, KVKK m. 12 kapsamında hukuka aykırı işlemeyi önleme, veriye hukuka aykırı erişimi engelleme ve veri muhafazasını belirlenmiş asgari önlemlerle sağlamayı içermektedir[1313].

KVKK m. 18'de "kabahatler" başlığında veri sorumlusunun hangi durumlarda idari yaptırıma tabi tutulacağı hüküm altına alınmıştır. Bunlar aydınlatma yükümlülüğünü yerine getirmeme[1314], kişisel veri güvenliğine ilişkin yükümlülükleri yerine getirmeme[1315], "kurul kararlarının gereklerini yerine

1312) Kangal, [2019], Kişisel Veri – Ceza ve Kabahatler, s. 198.
1313) KVK Kurumu, [2019], Uygulama Rehberi, s. 97.
1314) KVK Kurulu, veri sorumlusu işverenin aydınlatma yükümlülüğünü ve teknik ve idari tedbirleri alma yükümlülüğünü yerine getirmemeyi aynı kararda idari yaptırıma konu etmiştir. Kararda bu husus; "Aydınlatma yükümlülüğünü yerine getirmediği kanaatine varıldığından veri sorumlusu hakkında Kanunun 18 inci maddesinin birinci fıkrasının (a) bendi uyarınca 50.000 TL idari para cezası uygulanmasına, Veri sorumlusunun çalışanlarının ve yakınlarının açık rızaları olmaksızın kişisel verilerini ve özel nitelikli kişisel verilerini işlediği, işlediği özel nitelikli kişisel veriler bakımından Kanunun 4 üncü maddesinde yer alan genel ilkelerden ölçülülük ilkesine aykırı hareket ettiği ve bu verileri yine çalışanlarının açık rızası olmaksızın yurtiçi ve /veya yurtdışına aktardığı görüldüğünden, Kanunun 12 nci maddesinin birinci fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ile kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı hareket ettiği kanaatine varılan veri sorumlusu hakkında Kanunun 18 inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 200.000 TL idari para cezası uygulanmasına" biçiminde değerlendirilmiştir. Bkz. KVK Kurul Kararı, Karar Tarihi: 20/05/2020, Karar No: 2020/404, https://kvkk.gov.tr/Icerik/6913/2020-404 (Erişim Tarihi: 15.12.2023).
1315) KVK Kurul kararında "kişisel verilerin hukuka aykırı işlenmesini engellememe" her türlü teknik ve idari tedbirleri alma yükümlülüğü kapsamında değerlendirilmiş ve idari yaptırım uygulanmıştır. Kararda bu husus özetle; "Veri sorumlusu tarafından ilgili kişiye ve başka gerçek kişilere ait kişisel verileri barındıran Savcılık şikayet dilekçesinin olayla herhangi bir ilgisi olmadığı anlaşılan ve ilgili kişinin kardeşi olduğu belirtilen üçüncü bir kişiye e-posta yoluyla iletilmesi işleminin, Kanun'un 5'inci maddesinde yer alan kişisel verilerin işlenmesi şartlarından herhangi birine dayanmadığı ve bu kapsamda veri sorumlusunun Kanun'un 12'nci maddesinin (1) numaralı

getirmeme" ve "veri sorumluları siciline kaydolmama" olmak üzere dört kabahatten oluşmaktadır[1316]. Her yıl yeniden değerleme oranına göre yeniden belirlenen[1317] bu para cezaları için alt ve üst sınırları belirlenmiş, olayın özelliğine, ihlalin boyutuna ve veri sorumlusunun mali gücüne göre belirlenen aralıkta olmak üzere yaptırımı uygulama yetkisi KVK Kurulu'na bırakılmıştır. Örneğin veri sorumlusu işveren, aydınlatma yükümlülüğünü yerine getirmeden dijital izleme uygulamaları vasıtasıyla işçinin verilerini işlemesi KVKK m. 18/1-a kapsamında 5.000-TL'den 100.000-TL'ye kadar idari para cezası uygulanabilecektir. Bu idari para cezası aydınlatma yükümlülüğü yerine getirilmeyen her bir kişi bazında uygulanacağını belirtmek gerekir. İşverenin KVKK m. 12'de öngörülen teknik ve idari tedbirleri yerine getirmemesi 15.000-TL'den 1.000.000-TL'ye kadar idari para cezası sebebi olarak hüküm altına alınmıştır.

§ 9. DİJİTAL İZLEMENİN OLUMSUZ ETKİSİNİ SINIRLAMAYA YÖNELİK ÖNERİLER

Bu başlıkta kişisel verilerinin korunması, ilgili kişinin işlenen verileri hakkında bilgi sahibi olması ve verileri hakkında yeniden hakimiyeti ele geçirmesi fikri kapsamında gelişme göstermiş kişisel veri koruma hukuku enstrümanları olan açık rıza ve aydınlatma yükümlülüğünün sorunlu yönleri ile bilişim teknolojileri, giyilebilir sistemler, yapay zeka ve algoritmik analizler gibi yeni teknolojiler kapsamında gelişme gösteren dijital izleme uygulamalarında işçinin özel hayatının ve kişisel verilerinin etkin korunmasına yönelik öneriler ele alındı.

---

fıkrasında yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik gerekli her türlü teknik ve idari tedbirleri alma yükümlülüğüne aykırı hareket ettiği değerlendirildiğinden veri sorumlusu hakkında Kanun'un 18'inci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 150.000 TL idari para cezası uygulanmasına" biçiminde yer almıştır. Bkz. "Veri sorumlusu eski işveren tarafından ilgili kişinin kişisel verilerinin yer aldığı adli yazışma bilgilerinin kardeşi ile paylaşılması" hakkında Kişisel Verileri Koruma Kurulunun 02/09/2022 tarihli ve 2022/896 sayılı Karar Özeti, https://kvkk.gov.tr/Icerik/7584/2022-896 (Erişim Tarihi: 12.12.2023).

1316) Kangal, [2019], Kişisel Veri – Ceza ve Kabahatler, s. 177.

1317) Yeniden değerleme oranına göre belirlenmiş idari yaptırımlarının parasal sınırı için bkz. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/782832ef-892c-463d-a58d-a478b6f84586.pdf (Erişim Tarihi: 01.12.2023).

I. Açık Rıza ve Aydınlatma Yükümlülüğünün Veri Korumada Yetersizliği

KVK hukuku ilgili kişinin verilerinin korunmasını veri işlemede şeffaflık ve bireyin işlenen verileri üzerinde bir hakimiyet alanına sahip olmasını sağlamak amacıyla aydınlatma yükümlülüğü ve açık rıza gibi mekanizmalar çerçevesinde gelişmiştir. İş sözleşmesi otorite/bağımlılık ilişkisinin belirleyici olduğu bir ilişki ortaya çıkardığından bilgilendirmenin işçiyi koruyucu etkisi ve işçiden alınan açık rızanın geçerliliği kuşku uyandırıcıdır. Zira iş ilişkisinde işçinin serbestçe karar verebileceğinden bahsetmek güç olduğu gibi, kişisel verileri işlenen bireyler çoğunlukla uzun metinlerden oluşan aydınlatma yükümlülüğü ve açık rıza metinlerini okuma gereği duymazlar[1318]. Dahası gelinen aşamada her yerde aydınlatma metnine ve açık rıza bilgilendirmesine maruz kalan bireyin bu hususta bir yorgunluk yaşadığı belirtilmelidir.

1. Açık Rıza ve Aydınlatma Yükümlülüğünün Sorunlu Yönleri

Kişisel verileri işlenen ilgili kişinin verileri işlenmeye başlanmadan önce aydınlatma yükümlülüğü kapsamında bilgilendirilmesi, kişisel veri işleme faaliyetinin şeffaf olması ilkesi kapsamında yer alan önemli bir haktır. İlgili kişiye tanınan ve kişisel verileri işlenen bireyin talebine bağlı olmaksızın yerine getirilmesi zorunlu olan bu hak, veri sorumlusuna ilgili kişiyi tam bilgilendirme yükümlülüğü yükleyerek kişisel verileri işlemedeki keyfiliklerini engeller. Açık rıza beyanı ise veri işlemede ilgili kişiye bir hakimiyet alanı bırakması açısından önemlidir. Dahası, KVKK'nın ve GVKT'nin benimsediği ilke olan verisi işlenen ilgili kişinin eylemsizliğine bir sonuç bağlanmaması, unsurları bulunan açık rıza beyanının aranması veri korumada açık rızaya önemli bir rol yüklemektedir. Bu sebeple kişisel verilerin korunması hakkının bulunduğu çoğu durumda "açık rızayı" tamamen dışlamak bireysel özgür karar alabilme hakkını kısıtlar ve bireye ilişkin

1318) Solove, [2023], Murky Consent, s. 27-28; Adam S. Chilton/Omri Ben-Shahar, "Simplification of Privacy Disclosures: An Experimental Test", Coase Sandor Working Paper Series in Law and Economics No. 737, [2016], s. 41-42.

karaları devletin alması gibi sorunlu sonuçlar ortaya çıkarır[1319].

Açık rızanın koruyuculuğunun sorunlu yönleri bulunmakla birlikte bu hakkın bulunması bireysel özerklik ve özgürlükle ilgili olduğundan ve bazen de bireyin tasarruf edebildiği alanlarda aleyhine sonuçlara sebebiyet verse dahi ilgili kişinin açık rızasıyla karar verebilme hakkı hukuken korunmalıdır. Burada devletlerin yapması gereken bireyin kişisel verilerini korumak için etkin sınırlandırıcı enstrümanlar oluşturması ve bunu yaptıktan sonra bireye verileri veya kişisel verileri üzerinde açık rıza beyanını kullanacağı bir alan bırakmasıdır[1320].

Öte yandan, özellikle dezavantajlı (çocuklar, hastalar vb.) grupların bulunduğu durumlarda ve iş ilişkisi gibi bağımlı çalışmanın hiyerarşik bir ilişki ortaya çıkardığı ilişkilerde açık rıza ve aydınlatma yükümlülüğü kişisel verilerin işlenmesinin meşrulaştırıcı bir hukuki örtüsü işlevi görebilir[1321]. Nitekim kişisel veri işlenmesini iş ilişkisi açısından değerlendiren WP 29 Çalışma Grubu, bu ilişkide veri işlemenin yasal zemini olarak işçinin açık rızasının alınmasının oldukça tartışmalı olduğunu, işçilerin iradesini tam olarak açıklamayabileceğini, bunun açık rızanın unsurlarından birisi olan özgür iradeyle verilmiş olma açısından tartışmalı bir alan bıraktığını belirtmiştir[1322]. KVK Kurumu yayımlamış olduğu rehberlerde, işçi – işveren ilişkisinin bulunduğu[1323] eşit durumda olmayan kişiler arasında açılanan açık rızanın özgür iradeyle verilmiş olmasının güç olduğunu

1319) Solove, [2023], Murky Consent, s. 2.
1320) Solove, [2023], Murky Consent, s. 2-3.
1321) Heidi M. Hurd, "The Moral Magic of Consent, Legal Theory", Vol. 2, Issue 2, June 1996, s. 121.
1322) WP29 On the processing of personal data in the employement contex, Opinion 8/2001, 5062/1/EN/Final WP 48, [2001], s. 23.
1323) KVK Kurumu, [2019], Uygulama Rehberi, s. 50. Rehber'de işçi – rızanın özgür iradeyle verilip verilmediğinin denetiminde taraflar arasındaki dengesizlik ve birisinin diğeri üzerindeki etkisinin dikkate alınması gerektiğini KVK Kurumu Rehber'inde şu şekilde ifade etmiştir: "Tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerekir. Özellikle işçi-işveren ilişkisinde, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez."

belirtmektedir[1324].

İşverenin dijital izleme uygulamalarıyla ilgili olarak işçileri bilgilendirmesi, örneğin güvenlik amaçlı işyerinin ortak alanlarına yerleştirilen kameraların bulunduğu yerlere kamera ile izleme yapıldığına ilişkin simgelerle veya yazı ile işçilere bildirilmesi veya işin görülmesi için işçiye tahsis edilmiş telefonun, arabanın, e-posta hesabının, internetin kişisel amaçlarla kullanılıp kullanılamayacağı, bu araçların izlenmesine ilişkin KVK hukukunun ilkelerine uygun olarak işçileri bilgilendirilmesi dijital izlemenin hukuka uygunluğunu nitelendirmede yardımcı veriler sunar. Bununla birlikte, aydınlatma yükümlülüğünün yerine getirilmesi ve diğer veri işleme şartlarının bulunmadığı durumlarda işçilerden açık rızanın alınması gerçekleştirilen dijital izlemenin hukuka uygunluğunda tek ölçüt olarak değerlendirilmeye alınması işçinin kişisel verileri üzerindeki haklarını ihlal edebilir. Zira hukuka uygunluk sadece bilgilendirme ve açık rıza açısından değerlendirilirse, örneğin tele çalışan bir işçinin anlık olarak izlenmesi gibi işçinin özel hayatı ve kişisel verileri üzerinde müdahaleci etkiler oluşturan dijital izleme uygulamalarını ortaya çıkarır. Bunun önüne geçilmesi için, aydınlatma yükümlülüğü ve açık rızaya başvurmadan önce başkaca sınırlandırmalar geliştirilmelidir. Aksi durumda açık rızaya dayalı gerçekleştirilen dijital izleme uygulaması işçilerin rıza gösterdiği her durumda veri işlenmesi sonucunu ortaya çıkarır. Bunun işçinin özel hayatı ve kişisel verilerine ilişkin hakları üzerinde ihlal edici sonuçlar ortaya çıkaracağı açıktır[1325].

Belirtmek gerekir ki, işçiler ancak işverenleriyle herhangi bir sorun yaşamayacaklarına emin oldukları durumlarda açık rıza beyanından kaçınabilirler

1324) KVK Kurumu, [2019], Uygulama Rehberi, s. 49-50.
1325) KVK Kurumu, [2019], Uygulama Rehberi, s. 69.

ve bu yönlü talepleri reddedebilirler[1326]. Bu sebeple bildirim ve seçim[1327] uygulamasından daha koruyucu olmasına rağmen açık rıza bireyi korumada çoğu zaman yetersiz kalır. Zira açık rıza alınması sürecinde bireyin verdiği rızanın içeriğini, kişisel verileri üzerindeki etkilerini ve potansiyel risklerini bilmesi ve anlaması çoğunlukla olanaklı değildir. Ayrıca açık rıza ve aydınlatma yükümlülüğü yaklaşımı pratik de değildir ve bir süre sonra ilgili kişi üzerinde bilgilendirme ve "açık rıza yorgunluğu" ortaya çıkarır. İnsanların verdikleri rızanın konusu ve içeriğine ilişkin dikkatleri azaldığından zamanla neye rıza verdiği ve hangi hususlarda aydınlatıldığıyla ilgili bireysel hakimiyet yitimi gerçekleşir[1328]. Böylelikle açık rıza kişisel verileri korumada gerçek durumla bağını koparak "özgürce verilmiş" gibi algıya sebebiyet verir ve bireyi korumada etkili bir işlev olmaktan uzaklaşır. Dahası açık rızanın var olmasıyla yokluğu arasında gri alanlar da bulunduğunu belirtmek gerekir. Zira kişisel verilerin işlenmesine hukuki zemin oluşturan açık rıza bilgilendirmeleri ve unsurlarının varlığı muğlaklıklarla doludur. Öte yandan işçiye yönelik aydınlatma yükümlülüğü yerine getirilerek dijital izleme uygulamasını kullanılması dijital izlemeyi meşrulaştırmak dışında etkili bir güvence sunmamaktadır[1329].

İş ilişkisinde sadece güç dengesizliği işçinin iradesini olumsuz etkilemez veya onların seçimlerini baskılamaz. İşverenler, işçilerin iradesini etkileyecek küçük ödüllerle de onların karar verme süreçlerini yönlendirebilirler[1330]. KVK hukukunun düzenlemelerinin bu gibi açık alanlarda işçiyi ne kadar koruyabildiği tartışılmalıdır. Zira ilgili kişinin açık rızasını almak için teşvikler ve çeşitli

1326) GVKT m. 7'de açık rızanın koşulları düzenlenmiştir. Ayrıca WP29, Opinion 2/2017 çalışmasına çalışma ilişkisinde açık rızanın özgür irade ile verilme olasılığının düşük olduğunu, bu sebeple veri işleme amacı açısından daha az veri işlemeyi gerektiren, işçinin özel hayat alanına ve kişisel verilerine en az müdahaleyi gerçekleştirecek yöntemle bilgilendirmeye dayalı veri işleme sürecinin yürütülmesi gerektiğini vurgulamıştır Opinion 2/2017 s. 6 vd.
1327) Sloan/Warner, [2013] Norms, and Consent, s. 3; Bkz. § 6. 4. a). aa) Açık Rızanın Unsurları.
1328) Solove, [2023], Murky Consent, s. 5.
1329) Susser/Roessler/Nissenbaum, [2019], Digital World, s. 14 vd.; Solove, [2023], Murky Consent, s. 12 vd.
1330) Susser/Roessler/Nissenbaum, [2019], Digital World, s. 15; Solove, [2023], Murky Consent, s. 17.

argümanlar sunularak onların rızalarının bir amaç kapsamında kanalize edilmesi mümkündür. Örneğin satış biriminde çalışan işçileri sahada bir dijital izleme uygulamasıyla izlemeye ikna etmek isteyen bir satış müdürü onların rızalarını küçük bir prim ile kendi amacı doğrultusunda yönlendirebilir[1331]. Belirtmek gerekir ki, bu durumlar açık rızanın özgür iradeyle verilme unsuruna aykırılıklar barındırdığından işçilerin açık rızasının bulunmadığı kabul edilmelidir. Dahası bu örnekte diğer veri işleme şartları olan "sözleşme ilişkisi" ve veri sorumlusu işverenin "meşru menfaati" bulunduğundan bu dijital izleme gerekli ise bu kapsamda gerçekleştirilmesi mümkünken işçilerin açık rızasının alınması da dürüstlük ilkesine aykırı olacaktır[1332]. Ne var ki, kişisel veri koruma enstrümanlarının tüm bu sorunlu alanlarını/örneklerini çoğu zaman aydınlatma metinlerinde ve açık rıza beyanlarında tespit etmeye olanak bulunmamaktadır.

GVKT Giriş 43. Paragrafında özgürce verilen rızanın koşulları açıklanmış ve veri sorumlusu ile ilgili kişi arasında açık bir dengesizliğin bulunduğu durumlarda açık rızanın varlığından bahsedilmeyeceği vurgulanmıştır[1333]. KVKK'da işçi özelinde bir düzenleme bulunmamakla birlikte KVK Kurumu'nun yayımladığı rehberlerde bu esas benimsenmiştir[1334]. Özgürce açıklanan açık rıza beyanından ne anlaşılması gerektiğine GVKT Giriş 42. Paragrafında[1335] açıklık getirmektedir. Buna göre ilgili kişinin gerçek ve özgür bir seçimi yoksa veya zarar görmeden rızayı reddedemeyecek veya geri çeviremeyecek durumdaysa rızanın özgürce verilmiş olduğundan bahsedilmeyecektir[1336]. Bu sebeple dezavantajlı grupta bulunan kişilerin verdiği ve güç dengesizliğinin bulunduğu ilişkilerde verilen rızaya şüpheyle bakılmalıdır. Nitekim, European Data Protection Board (EDPB - Avrupa Veri Koruma Kurulu) yayımladığı rehberde ilgili kişinin açık rıza vermek zorunda hissetmesi veya onay vermemesi halinde olumsuz sonuçlarla

1331) Susser/Roessler/Nissenbaum, [2019], Digital World, s. 14.
1332) KVK Kurumu, [2019], Uygulama Rehberi, s. 72 vd.
1333) GDPR Recital 43, https://gdpr-info.eu/recitals/no-43/ (Erişim Tarihi: 15.11.2022).
1334) KVK Kurumu, Açık Rıza Rehberi, s. 6. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf
1335) GDPR Recital 42, https://gdpr-info.eu/recitals/no-43/ (Erişim Tarihi: 15.11.2022).
1336) Solove, [2023], Murky Consent, s. 21.

karşılaşacağını hissettiği durumlarda rızanın geçersiz olduğunu belirtmektedir[1337].

GVKT 42. Paragrafta yer alan gerekçe, WP 29 Çalışma Grubu'nun 2001 yılında kişisel verilerin işlenmesi iş ilişkisi açısından değerlendirdiği görüşüyle uyumludur[1338]. Örneğin uzakta çalışan bir insan kaynakları departmanı işçisinin internet trafik bilgilerinin, sosyal medya hesaplarındaki paylaşımlarının ve e-postalarının izlenmesini içeren bir açık rıza talebinin işçi tarafından işini kaybetmemek veya bu talebi reddetmenin olası kariyer gelişim sonuçlarından duyduğu kaygı sebebiyle kabul etmesi durumunda açık rızanın varlığından bahsedilmeyecektir. Bu sebeple açık rıza dijital izleme uygulamalarıyla işçileri izlemenin hukuka uygunluk sebebi olduğu durumlarda, izleme faaliyeti kendi özelinde değerlendirilmesi gerekmektedir.

Özellikli bir durum yoksa açık rıza dijital izlemenin ve kişisel verileri işlemenin hukuka uygunluk sebebi sayılmamalıdır[1339]. Örneğin uzaktan çalışan bir bilgisayar yazılımı uzmanının bilgisayardan hiçbir veriyi kopyalayamayacağı bir düzende çalıştırılması, internet trafik ve elektronik iletişiminin izlenmesi işverenin meşru menfaati kapsamında değerlendirilebilir. Bu durumda işveren bu işçiyi işlenecek verileriyle ilgili olarak aydınlatma yükümlülüğü kapsamında bilgilendirmesi veri işlemesi için yeterli olacaktır. Zira bu dijital izleme uygulamaları kişisel veri işlenme şartı olan "meşru menfaat" ve "iş sözleşmesinin ifasıyla doğrudan doğruya" ilgilidir. Bu örneği farklılaştırdığımızda çikolata üretimi yapan işverenin işyerine giriş ve çıkış için yüz tarama (biyometrik veri) esasına göre çalışan bir dijital izleme uygulaması kullanmayı aydınlatma yükümlülüğünü yerine getirerek unsurları bulunan bir açık rıza metni kapsamında gerçekleştirmek istemesi ve bu amaçla işçinin açık rıza beyanını alması, işçinin bu

1337) European Data Protection Board, Guidelines 5/2020 on Consent Under Regulation 2016-679, May 4, [2020], s. 13.
1338) WP29 On the processing of personal data in the employement contex, Opinion 8/2001, 5062/1/EN/Final WP 48, [2001], s. 23.
1339) WP29, Working document on the surveillance of electronic communications in the workplace, Adopted on 29 May 2002, 5401/01/EN/Final WP 55, [2002], s. 21.

uygulamaya açık rıza göstermesi veri işlemenin hukuka uygunluk sebebi sayılmamalıdır[1340].

Bazı özellikli işlerde gerçekten işveren bir riskle karşı karşıyadır ve risk sebebiyle dijital izleme uygulamasının kullanılması bir zorunluluk olabilir. Örneğin hastane hizmeti veren ve hastalara ilişkin birçok özel nitelikli kişisel veri işleyen, ayrıca bir hastalıkla ilgili önemli araştırmalar gerçekleştiren bir işyeri, hastalarının özel nitelikli kişisel verileri ile ticari sırlarını korumak için işçilerin kullanımına tahsis edilen e-posta hesaplarını ve internet trafik kayıtlarının detaylı bir şekilde izlenmesi, sistem güvenliği için ek tedbirler alması ve dijital izleme gerçekleştirmesi makul karşılanabilir. Öte yandan bu örnekte dahi işçilerin tam olarak bilgilendirilmesi, KVK hukukunun ilkeleri kapsamında bir değerlendirme yapılması ve izlemenin işçiler üzerindeki etkisinin tespit edilmesi gerekir.

2. Aydınlatma Yükümlülüğü ve Açık Rızadan Önce Yeni Denetimlerin Geliştirilmesi İhtiyacı

Dijital izleme uygulaması kapsamında kişisel veri işleme faaliyetine başlamadan önce, özellikle otomatik veri işleme sistemlerinde kişisel verilerin işlenmesinde meşrulaştırıcı bir dayanak olmaktan daha etkili bir işlevi olmayan aydınlatma yükümlülüğüne ve açık rızaya her durumda bir sonuç bağlamak yerine, işverenler genel ilkeler, kişisel veri etki değerlendirmesi kapsamında bir değerlendirme yapmakla zorunlu tutulmalıdır. Bu değerlendirme sonrasında işyeri için dijital izleme uygulamasının kullanılması zorunlu ise aydınlatma yükümlülüğünü yerine getirilip, diğer veri işleme şartları yoksa işçiden açık rıza alınarak dijital izleme uygulaması kapsamında veri işlenmesine başlanmalıdır[1341].

Ayrıca işçi verilerinin etkin korunabilmesi için KVKK'da iş ilişkisi özelinde

1340) Bkz. AYM Genel Kurul Kararı, Ramazan Şahin kararı, 2018/26771.
1341) Solove, [2023], Murky Consent, s. 6-7.

düzenlemeler gerçekleştirilmeli, ilgili başlıklarda incelenen kişisel veri etki değerlendirmesinin zorunlu hale getiren ve profil çıkarmanın sınırlandırılmasını öngören hükümlerin düzenlemeye kavuşturulması gerekmektedir. Özelikle dijital izleme gibi yoğun veri işlemenin söz konusu olduğu ve veri ifşasının önemli bir risk olarak ortaya çıktığı veri işleme faaliyetlerinde kişisel veri etki değerlemesinin yapılması, ilgili kişinin profil çıkarma ve otomatik veri işlenmesine konu edilmemesi hakkının düzenlemeye kavuşturulması gerekmektedir[1342]. Böylelikle işçilerin ve işçi adaylarının özel hayatları ile kişisel verilerine en az müdahaleyi gerçekleştirecek bir yöntemle meşru amaç için gerekli olan, ölçülü veri işlenmesi etkin bir şekilde sağlanmış olacaktır[1343].

İşverenler, bir amaç kapsamında dijital izleme uygulaması kullanmak yerine işçilerin kişisel verilerinin korunması ve temel haklarını daha az etkileyecek bir yöntem varsa bu yöntemin tercih etmeleri zorunlu hale getirilmelidir. Örneğin işçilerin devamlı biçimde kayıt altına alan ve denetleyen dijital izleme uygulamalarını kullanmak yerine aralıklı denetimleri anonim olarak gerçekleştiren ve sistem açıklarını gidermeyi hedefleyen bilişim uygulamalarının kullanılması gerekir. Aynı doğrultuda tüm e-posta içeriğini izleyen dijital izleme uygulamalarının ne kadar amaca uygun olduğu değerlendirilmelidir. Bunun yerine e-posta iletişiminin içeriğinden çok trafik verilerinin işlenmesi amaca daha uygun olabilir. İşveren bu değerlendirmeyi yaparak bir yanda kendi amacını gerçekleştiren, diğer yandan işçiler için en az müdahaleci olan ve onların özel

1342) Paola Grimaldi, "Robots, Unwearable Profiling and Protection of Vulnerable Users", European Journal of Privacy Law & Technologies (EJPLT), Vol. 2020, No. 2, [2020], s. 198-199.
1343) EDPB, İtalya'da Bozen/Bolzano Belediyesi'nin işçilere bilgi vermeden dijital izleme gerçekleştirmesini GVKT m. 5/1-a ve c, hukuka uygun olma, adil, şeffaf ve sınırlı ölçülü veri işleme; m. 6 yasal işleme koşullarının bulunması; m. 9 özel nitelikli kişisel verilerin işlenme koşulları; m. 13 aydınlatma yükümlülüğü ve m. 88 iş ilişkisi bağlamında kişisel veri işleme düzenlemeleri ve İtalyan DP m. 113 ve114 uzaktan izleme ve özel hayatın korunması için gereken önlemeler kapsamında incelemeye konu etmiş ve belediyenin bu düzenlemelere uygun bilgilendirme yapmaması, amaç kapsamıyla uyuşmayan şekilde izleme gerçekleştirmesini yasaya aykırı bulmuş ve belediyeye 80.000 Avro para cezası vermiştir.
https://edpb.europa.eu/news/news/2021/italian-sa-unfettered-employee-surveillance-be-banned_en (Erişim Tarihi: 26.11.2022).

hayatlarının gizliliğini de önemseyen bir yöntemi benimsemelidir[1344].

Yapay zeka temelli dijital izleme uygulamaları işçilerin profillerini çıkarmada, izlerini takip etmede veri sorumlusu işverene tamamen otomatikleştirilebilir ve algoritmik analize konu edilebilir veri açısından önemli imkanlar sunmaktadır. GVKT bunları sınırlandıran önemli normlar barındırmaktadır[1345]. KVKK'da benzer biçimde işçinin aydınlatma yükümlülüğü kapsamında bilgilendirilmesinden ve açık rızasının alınmasından önce kişisel verilerin işlenmesini sınırlandıran ön denetimlerin geliştirilmesi gerekmektedir.

Kanaatimizce dijital izleme uygulamasıyla işçinin verisini işlemek için aydınlatma yükümlülüğü ve açık rıza öncesinde; dijital izleme etki değerlendirmesinin gerçekleştirilmesi, başkaca daha az müdahaleci bir yöntemin varlığının araştırılması ve hukuka uygunluk ölçütlerinin dijital izleme faaliyetine uygulanması gibi kontrollerin gerçekleştirilmesi ve sonrasında kişisel verilerin işlenmesi gerekliyse aydınlatma yükümlülüğü yerine getirilerek dijital izleme uygulaması vasıtasıyla kişisel veri işlenmelidir. Zira her yerde birkaç sayfadan oluşan metinler kapsamında bilgilendirilmeye çalışılan gerçek kişilerin bilgilendirme metni yorgunu olduğunu, bu sebeple aydınlatma yükümlülüğünün verileri işlenen ilgili kişiyi/işçiyi korumaktan öte gerçekleştirilen dijital izlemenin meşrulaştırıcı aracına dönüşeceğini belirtmek gerekir[1346].

Öte yandan, KVKK etki araştırmasına ilişkin bir düzenleme bulunmamasına rağmen m. 4'te düzenlenen temel ilkelerden hareketle ve Anayasa m. 20 kapsamında bu sonuca ulaşmak mümkündür. Bununla birlikte kanun hükmünü zorlayacak yorumlar geliştirerek dolaylı yollarla sonuca ulaşmak yerine ülkemiz veri koruma mevzuatında bu denetimlerin zorunlu olarak arandığı düzenlemelerin

1344) WP29 On the processing of personal data in the employement contex, Opinion 8/2001, 5062/1/EN/Final WP 48, [2001], s. 17.
1345) Grimaldi, [2020], Unwearable Profiling, s. 198.
1346) Solove, [2023], Murky Consent, s. 5-6.

getirilmesi gerekmektedir.

II. Verilerin Doğrudan İşçiden Elde Edileceği Yöntemlerin Önceliklendirilmesi

Kişinin kendi verilerinin işlenme düzeyi ve geleceği üzerinde belirleyici olmada (verilerinin kaderini tayin etmede) özgür hareket etmesini ifade eden "informational self-determinism" kavramı ilk kez 1983'te Nüfus Sayımı Yasasına karşı açılan davada Alman Federal Anayasa Mahkemesi tarafından "Nüfus Sayımı Kararında" kullanılmıştır[1347]. Mahkeme bireyin kişisel verilerinin herhangi bir sınırlama olmaksızın işlenmesine, saklanmasına, kullanılmasına ve ifşa edilmesine karşı korunmasının Alman Anayasası'ndan doğan kişilik hakkının bir gereği olduğunu, bu temel hak aynı zamanda bireyin verileri üzerinde özgürce karar almasını ve verilerinin kimlerle paylaşacağını belirleme hakkını garanti altına aldığını ve kişilik hakkının ancak kamu çıkarlarına zarar vermesi durumunda sınırlanabileceğine karar vermiştir[1348].

Bu kararda yer verilen ilkeler sonraki yıllarda kişisel verilerin korunmasına ilişkin kanunlara ve 95/46 sayılı AB Direktifi gibi hukuki düzenlemelere etki etmiştir. Kişinin verileri ve verilerinin geleceği üzerinde belirleyici olması, ilgili kişiye kişisel verilerinin işlenip işlenmediği, kim tarafından hangi amaçlarla işleneceği ve kimlere aktarılacağı gibi hususlarda bilgi sahibi ve belirleyici olma hakkı tanımaktadır[1349]. Kişinin işlenen verileri üzerinde bir hakimiyet alanının bulunması ve verilerin doğrundan kendisinden elde edilmesi bireyin onuru ve kişiliğini özgürce geliştirme hakkının bir görünümüdür. Bu amaçla AYM çeşitli kararlarında bireyin bu hakkına yer verilmiş, ilgili kişinin herhangi bir verisinin

1347) Gerrit Hornung / Christoph Schnabel, Data Protection In Germany I: The Population Census Decision and The Right to Informational Self-Determination, Computer Law & Security Report, Volume 25, Issue 1, [2009], s. 84.
1348) Hornung/Schnabel, [2009], Data Protection In Germany, s. 85.
1349) Hornung/Schnabel, [2009], Data Protection In Germany, s. 87; Determann/ Sprague, [2011], Intrusive Monitoring, s. 1025.

bilgisi ve rızası olmaksızın işlenmemesi, paylaşılmaması, başkalarının erişimine açılmamasında menfaati bulunduğuna ve bunun bireyin kendi kişisel verilerinin kaderini belirleme hakkıyla ilişkili olduğuna karar verilmiştir[1350].

Bu itibarla iş ilişkisinde işçiye verileri üzerinde etkin bir belirleyici olmasını sağlayacak yöntemlerin geliştirilmesi gerekmektedir. Bu yöntemlerden birisi dolaylı yöntemlerle işçi hakkında veri işlemek yerine işin niteliği de dikkate alınarak doğrudan işçiden veri işlenmesini önceliklendiren mekanizmaların geliştirilmesidir. İş ilişkisinde işlenen kişisel verilerde şeffaflığı yakalamak ve işçilerin kişisel verileri üzerindeki menfaatlerinin korunması için Avrupa Konseyi CM/Rec.2015-5 sayılı Avrupa Konseyi Bakanlar Komitesi Kararı'nda işverenlerin, kişisel verileri dijital izleme uygulaması gibi vasıtasıyla dolaylı yollardan değil, doğrudan veri sahibi işçiden elde edilmesi (işlenmesi) tavsiye edilmektedir[1351].

Bakanlar Komitesi tavsiye kararları bağlayıcı olmamakla birlikte üye ülkelerin bu konudaki politikalarının belirlenmesinde etkileyicidir. Bakanlar Komitesi tavsiye kararının niteliği; "Avrupa Konseyi Statüsünün 15/B hükmüne dayanan, ulusal kanun koyuculara ve idarelere ölçütler getiren, üye devletlerin hükümetlerine yönelik uluslararası kararıdır. Bağlayıcı olmamakla birlikte, Komite, hükümetleri tavsiyeler doğrultusunda karar alıp almadıklarını bildirmeye davet eder" biçiminde düzenlenmiştir[1352].

Dijital izleme uygulamaları genel olarak işçilerin verisini dolaylı işlemeye

---

1350) AYM, Şengül Kayan kararı, Başvuru Numarası: 2013/1614, Karar Tarihi: 03.04.2014, § 32, https://www.resmigazete.gov.tr/eskiler/2014/05/20140522-28.pdf; AYM, E. 2009/1, K. 2011/82, Karar Tarihi: 18.05.2011; AYM, E. 1986/24, K. 1987/7, Karar Tarihi: 31.03.1987.

1351) CM/Rec.2015 Avrupa Komisyonu Bakanlar Komitesi Tavsiye Kararı'nın m. 5/1. fıkrası: "İşverenler, kişisel verileri doğrudan ilgili veri sahibinden elde edilmelidir. Örneğin, profesyonel referanslar elde etmek için üçüncü kişilerden toplanan verilerin işlenmesi gerekli ve yasal olduğunda, veri sahibi önceden usulüne uygun olarak bilgilendirilmelidir." tavsiyesini içermektedir. Tavsiye kararın tamamı için bkz. https://rm.coe.int/cmrec-2015-5-on-the-processing-of-personal-data-in-the-context-of-empl/1680a43b68 (Erişim Tarihi: 14.09.2023).

1352) Onur Karahanoğulları, İdari Takdir Yetkisinin Kullanılmasına İlişkin R(80)2 Sayılı Avrupa Konseyi Bakanlar Komitesi Tavsiye Kararı, AÜHFD, C. 34, S. 1-4, [1996], s. 325.

konu eden uygulamalardır. Örneğin iletişimin izlenmesinde elde edilen veri doğrudan işçiden elde edilen veriler değildir. İşçilerin kullanımına verilen cep telefonuna yüklenen uygulamalarla mesai saatleri dışındaki yaşam rutinlerinin dolaylı olarak izlenmesi, sosyal medya hesaplarında yaptıkları paylaşımların analizlere konu edilmesini yasaklayan düzenlemelerin yapılması gerekmektedir. WP 29 Çalışma Grubu'nun çevrimiçi işe alım bağlamında 2017/2 sayılı Görüşünde işçi veya işçi adayından dolaylı yöntemlerle, örneğin herkese açık sosyal medya hesabında paylaşılan verilerin işverenler tarafından kullanılmasının KVK hukukuna aykırı olduğuna dikkat çekilmiştir[1353].

Ayrıca belirtmek gerekir ki, işçi verilerinin dolaylı yöntemlerle işlemeye konu eden dijital izleme uygulamalarının görünmezlik ve belirlenemezlik özellikleri işçinin kişisel verileri üzerindeki hakları açısından bir risk ortaya çıkarmakta ve verilerin işlenmesinde şeffaflık ilkesine uygun hareket etmeyi güçleştirmektedir. İşverenler dijital izleme uygulamasıyla kişisel veri işleme faaliyetine başlamadan önce öncelikli olarak veri işlemedeki meşru amaçlarını belirlemesi ve bu amaç için işlenmesi gerekli olan kişisel verilerin işlenmesine dikkat edilmelidir. Ayrıca işçi açısından en az müdahaleci, mümkünse kişisel veriyi doğrudan işçiden elde edecek yöntemlerin önceliklendirmesi; bunun mümkün olmadığı durumlarda veri sahibi işçinin veri işleme faaliyetinin tüm detayları hakkında bilgilendirilmesi sonrasında veri işleme faaliyetine başlanması gerekmektedir.

Bakanlar Komitesi Tavsiye Kararı'nda önerildiği gibi işçilerin internet izlerinin, e-posta iletişiminin izlenmesi gerektiği durumlarda öncelikle önleyici tedbir olarak belirli işlemleri engelleyen filtreler kullanılmalı, izleme anonim veya rastgele kontroller biçiminde gerçekleştirilmelidir. Ayrıca işçinin iletişimin izlenmesinin zorunlu olması durumunda işçi üzerinde en az müdahaleci yöntem benimsenmeli ve verilerin doğrudan işçiden elde edileceği yöntemler

1353) WP 29, Opinion 2/2017 on data processing at work, 8 June 2017, s. 11.

önceliklendirilmelidir (CMRec. 2015-5/ m. 14). Özellikle işçilerin faaliyetlerini ve kişisel zamanlarındaki yaşayışlarını dolaylı yöntemlerle izleyen dijital izleme uygulamaları işçinin verileri ve özel hayatına saygı hakkı üzerinde ihlal edici sonuçlar ortaya çıkaracağından, bu tür dijital izleme uygulamalarının kullanılmasından kaçınılmalıdır (CMRec. 2015-5/ m. 15/2).

WP 29 Çalışma Grubu bu görüşünde işverenlerin işçi adayının veya işçinin sosyal medya profilinin kamuya açık olması nedeniyle bu verileri kendi amaçları doğrultusunda işlemesine izin verildiğini varsaymamaları gerektiğini ifade etmektedir. Bu sebeple veri işleme işverenin meşru bir menfaati kapsamında olsa dahi sosyal medya hesaplarında bulunan verileri esas alarak kişisel veri işlenmesi ancak ilgili işçinin veya işçi adayının sosyal medya hesabında yer alan verilerin belli amaçlar (örneğin kendisine iş teklifi gerçekleştirilmesi için işlemeye izin verme) kapsamında işlenmesine rıza gösterdiği durumlarda mümkün olmalıdır[1354].

İşverenlerin, iş başvurusunda bulunan kişinin sosyal medya profilinin kariyer, ticari veya özel amaçlarla ilgili olup olmadığını dikkate alması gerekmektedir. Avrupa Konseyi Bakanlar Komitesi Tavsiye Kararı'nda CM/Rec(2015)5 bu hususlar ele alınmış ve 5.3. başlıkta işverenlerin bir işçinin veya iş başvurusunda bulunan işçi adayının, özellikle sosyal ağlar aracılığıyla çevrimiçi olarak başkalarıyla paylaştığı bilgilere erişmeyi talep etmekten veya bilgileri talep etmekten kaçınması gerektiği vurgulanmıştır.

Belirtmek gerekir ki, işçinin özel hayatının gizliliği ve kişisel verilerinin korunmasına ilişkin hakkı anayasal temel bir hak olarak kişinin hakkı ve özgürlüğünün bir görünümü olduğundan dengenin işçilerin lehine olacak şekilde yasal düzenlemelerle sağlanması gereklidir[1355]. Bağımlılık ilişkisinin karakteristik

1354) Frank Hendrickx, "Privacy 4.0 at Work: Regulating Employment, Technology and Automation", Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall, [2019], s. 165.
1355) İşveren, işçiye işini görmesi için bilgisayar, cep telefonu veya başka bir eşya vermesi işçinin makul özel hayatın gizliliğinin korunması beklentisinin bulunması gerektiği yönünde karar veren Anayasa Mahkemesi kararı için bkz. AYM, Fırat Gerçek kararı, Başvuru Numarası: 2019/25604,

özelliği olduğu bir ilişkide bu denge ancak özel nitelikli kişisel verilerin işlenmesinin sınırlandırılması, verilerin doğrudan işçiden elde edileceği uygulamaların önceliklendirilmesi, sınırlı ve ölçülü veri işlenmesi, işçinin kendi verilerinin kaderini belirleme hakkı (informational self-determination) ve veri koruma etki analizi gibi enstrümanlarla sağlanabilir.

Fiili güç dengesizliğinin bulunduğu iş ilişkisinde işverenlere bu denetimler zorunlu hale getirildikten sonra, KVK hukukunun koruyucu mekanizmaları olan aydınlatma yükümlülüğünün ve diğer veri işleme şartları yoksa açık rızanın alınması gerekmektedir. Aksi durumda belirtildiği üzere, bu veri koruma enstrümanları işverenlerin, işçinin özel hayatı ve kişisel verileri üzerinde ihlal edici uygulamalarını meşrulaştırma aracına dönüşecektir. Zira işçi tarafından yılgınlıkla imzalanmış, birçok detayın bulunduğu, uzun sayfalardan oluşan aydınlatma yükümlülüğü metinlerinin koruyucu olmayacağı, ayrıca işçileri gerçek anlamda bilgilendirmek ve açık rızalarını almak için gereken bilgi miktarı düşünüldüğünde bunun pratik olmadığı da ortaya çıkmaktadır. Eklemek gerekir ki, işçilerin bunlara defalarca maruz kalması karşısında ortaya çıkacak yılgınlığın (belki duyarsızlaşmanın) işçilerin iradelerinin gerçek anlamda aydınlatma yükümlülüğüne ve açık rıza beyanına yansımamasına sebebiyet verecektir[1356]. Bu itibarla iş ilişkisinde öncelikli olarak verileri doğrudan işçiden elde edecek yöntemlerin önceliklendirilmesi gereklidir.

III. İşçinin Bilişim Sistem ve Uygulamalarıyla Bağlantıyı Kesme Hakkının Yasal Çerçeveye Kavuşturulması İhtiyacı

İşin teknoloji üzerinde, toplantıların dijital ortamda, yazışma ve karar almanın bilişim uygulamaları üzerinde gerçekleştiği günümüz iş yaşamında bu durum işçinin kişisel zamanını işgal edecek sonuçlar ortaya çıkarmaktadır. Bilişim

Karar Tarihi: 21.09.2022; AYM, E.Ü. kararı Başvuru Numarası: 2016/13010, Karar Tarihi: 17/9/2020; Aynı doğrultuda AYM, Ömür Kara ve Onursal Özbek kararı § 50.
1356) Solove, [2023], Murky Consent, s. 14.

sistemlerinin sunduğu bu olanakların bir sonucu olarak iş sözleşmesindeki bağımlılık unsuru bilişim sistemleri üzerinde dijital izleme ve denetleme uygulamalarıyla kişisel zamana yayılacak biçimde yeniden inşa edilmektedir[1357]. Bu sebeple uzaktan çalışmada işverenlerin, işçilerden beklediği her an ulaşılabilir olma beklentisi kişilik hakkı üzerinde ihlal edici sonuçlar ortaya çıkarmaktadır. Bunun önüne geçmek için "bağlantıyı kesme hakkı" (right to disconnect) kavramı taleplere konu edilmiş ve bu hak iş ilişkisi uygulamasına girmeye başlamıştır. İşçi haklarında duyarlı olduğunu iddia eden çeşitli işverenler işyerlerinde bu hakkı uygulayacak örnekler ortaya çıkarmaktadır. Örneğin 2011 yılı itibariyle Volkswagen çalışanlarının cep telefonlarına 18:00 ila 07:00 saatleri arasında e-posta gönderilmesini durduran politikalar benimsemiştir. Benzer bir uygulamayı Daimler şirketi hayata geçirmiş ve 2014 yılından itibaren çalışanlarının kullanımına sunduğu bir yazılım ile tatilde gelen e-postaların otomatik biçimde silinebilmesi olanağı tanınmıştır[1358].

"Ulaşılabilir olmama hakkı", "bağlantıyı koparma hakkı" kavramları kapsamında da incelemelere konu edilen[1359] bağlantıyı kesme hakkı; işçinin iş ilişkisinde ve kariyer gelişiminde olumsuz bir durumla karşılaşma kaygısı taşımadan bilişim sistemleriyle bağlantısını kesmesi ve iş dolayısıyla kişisel zamanında rahatsız edilmemesi hakkını ifade etmektedir. Eurofound'un (The European Foundation for the Improvement of Living and Working Conditions - Avrupa Yaşam ve Çalışma Koşullarını İyileştirme Vakfı) tanımına göre; işçilerin mesai saatleri dışındaki zamanlarında, ara dinlenmelerinde veya tatillerinde elektronik iletişim araçları olan e-posta, telekonferans, cep telefonu, bilgisayar, işçinin izlenmesine olanak veren teknolojik sistemlerle bağlantısını kesme hakkını

1357) Baycık/Doğan/Dulay Yangın/Yay, [2021], Pandemide Uzaktan Çalışma, s. 1705-1706; Kübra Doğan Yenisey, "Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri", Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı, On İki Levha Yayıcılık, (Editör, Kübra Doğan Yenisey / Seda Emrağ Ergüneş), İsanbul, [2021], s. 162.
1358) Levent Akın, "Türk Çalışma Yaşamında Pandemi Sürecinde Uzaktan/Evde Çalışma ve Olası Sonuçları", Festschrift für Otto Kaufmann Armağanı, Legal yayıncılık, İstanbul, [2021], s. 277-278.
1359) Ugan Çatalkaya, [2016], Ulaşılabilir Olmama, s. 733 vd.; Emre Ünal, İşçinin Ulaşılamama Hakkı, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, s. 3 vd.; Baycık/Doğan/Dulay Yangın/Yay, [2021], Pandemide Uzaktan Çalışma, s. 1706-1707.

ifade etmektedir[1360].

Eurofound bağlantıyı kesme hakkını temel haklar kapsamında değerlendirmekte ve devamlı çevrimiçi ve mobil iletişim için devamlı hazır halde olacağı beklentisinin işçilerin sağlığı için potansiyel bir tehlike olarak kabul etmektedir[1361]. Avrupa Parlamentosu bağlantıyı kesme hakkını temel bir işçi hakkı olarak ifade etmektedir[1362]. Bağlantıyı kesme hakkının kapsamına işçiye mesai saatleri dışında, tatilde, hafta sonları ve ara dinlenmelerinde ulaşılmaması ve işçinin kişisel zamanında bilişim sistem ve uygulamalarını kapatarak "ulaşılmama hakkını"[1363] kullanması girmektedir.

Belirtmek gerekir ki, bilişim teknolojilerinin ve internetin ortaya çıkardığı işçilerin her yerde, her an işini yapabilmesi olanağı ve bilgisayara veya cep telefonuna yüklenen bir uygulamayla işçinin kolaylıkla izlenmesi, denetlenmesi kişisel zamanlarında işçiye ulaşılabilme ve ondan iş istenmesine de sebebiyet vermektedir. İşçinin kişisel zamanı ve özel hayatı üzerinde işgal edici müdahaleler oluşturan bu olumsuzlukların engellenmesi için işçinin iş görme borcunun ifası için kendisine tahsis edilen bilişim sistem ve uygulamalarıyla bağlantıyı kesme hakkının düzenlemelere konu edilmesi gerekmektedir. Örneğin işçiden gece 23:00'da e-postayla veya cep telefonundan aranarak bir raporun hazırlanıp sabaha yetiştirilmesini istemek, işçinin bu talebe cevap vermezse işini savsaklamakla

---

1360) Tyler Jochman, "Effects on Employees' Compensation under the Right to Disconnect", Marquette Benefits & Social Welfare Law Review, Vol. 22, No. 2, Spring [2021], s. 210.

1361)https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/right-to-disconnect (Erişim Tarihi: 17.12.2022). AB'de doğrudan bir düzenleme bulunmamakta birlikte farklı Direktifler (Örneğin, Çalışma Süresi Direktifi - 2003/88/EC sayılı Direktif) kapsamında işçilerin bağlantıyı kesme hakkının bulunduğu kabul edilmektedir. Ayrıca 21 Ocak 2021'de Avrupa Parlamentosu, işçilerin bağlantıyı kesme hakkı lehine bir karar aldı ve Komisyon'u "dijital olarak işçilerin çalışma saatleri dışında bağlantılarını kesmelerini sağlayan" bir yönerge düzenlemeye çağırdı. Çağrı yapılan düzenlemenin ayrıca, "uzaktan çalışma için asgari gerekliliklerı belirlemeli ve uzakta çalışmanın koşullarını, saatlerini ve dinlenme sürelerini açıklığa kavuşturması" gerekliliği vurgulanmıştır. Avrupa Parlamentosu Üyeleri, işçilerin bağlantılarını kesme hakkının, fiziksel ve zihinsel sağlıklarını ve esenliklerini korumak ve onları psikolojik risklerden korumak için hayati önem taşıdığını öne çıkarmıştır.

1362)https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/679097/EPRS_BRI(2021)679097_EN.pdf (Erişim Tarihi: 12.07.2023).

1363) Ugan Çatalkaya, [2016], Ulaşılabilir Olmama, s. 734-751.

suçlanması kaygısı veya yöneticisinden takdir almak için bu tür taleplere hazır bir şekilde karşılık vermesi onun dinlenme hakkı ve kişisel hakları üzerinde yıkıcı etkiler ortaya çıkarabilir[1364]. Bu tür örneklerin artmasının işçinin özel hayatına saygı hakkını ihlal ettiği, işçinin verilerini yoğun işlemeye konu ederek bu haklar üzerinde müdahaleci sonuçlar ortaya çıkardığı kabul edilmektedir[1365].

Bu itibarla dijital izlemenin işçinin dinlenme hakkı ve verileri üzerindeki ihlal edici etkisini sınırlandıran haklardan birisi de iş görme borcunu ifa için işverenin işçinin kullanımına verdiği iletişim araçları, teknoloji ve bilişim uygulamalarıyla işçinin dinlenme aralarında ve kişisel zamanlarında bağlantıyı kesme hakkıdır[1366]. İşçinin mesai saatleri dışında ve dinlenme aralarında dijital izleme gerçekleştiren cihazları kapatması hakkının tanınması, bu sürelerde işçinin özel hayatı ve kişisel verileri üzerindeki ihlal edici uygulamaların etkisini KVK hukukunun öngördüğü bilgilendirme ve açık rıza gibi mekanizmalardan daha etkin koruyacaktır. Öte yandan işçinin bilişim sistem ve uygulamalarıyla bağlantıyı kesme hakkı keyfi ulaşılmama hakkı biçiminde yorumlanamaz. Bu kapsamda işçinin ara dinlenmesinde veya kişisel zamanı dışında bulunan mesai saatlerinde ulaşılabilir olması ve işverenin denetim, verimlilik beklentisi ile işçinin kişisel zamanı, özel hayatı ve kişisel verileri üzerindeki hakları arasında bir dengenin kurulması gerekmektedir[1367].

Covid-19'un etkisiyle yaygınlaşan uzaktan çalışmada işverenlerin uyguladığı dijital izlemeye dayanan denetim biçimleri işçinin özel hayatı ve verileri üzerinde müdahaleci sonuçlar ortaya çıkarması üzerine ILO Uzaktan Çalışma Uygulama Kılavuzu yayımladı. Kılavuzda uzaktan çalışmada iş-yaşam dengesinin

---

1364) Ugan Çatalkaya, [2016], Ulaşılabilir Olmama, s. 745.
1365) Giovanni Dosi/Maria Enrica Virgillito, "Whither the Evolution of the Contemporary Social Fabric: New Technologies and Old Socio-Economic Trends", International Labour Review, Vol. 158, No. 4, December, [2019], s. 617; Adams-Prassl, [2019], Artificial Intelligence at Work, s. 145-146.
1366) Paul M. Secunda, "The Employee Right to Disconnect", Notre Dame Journal of International & Comparative Law, Vol. 9, No. 1, [2019], s. 2-3, (Secunda, [2019], Right to Disconnect).
1367) Avogaro, [2018], Right to Disconnect, s. 123.

sağlanması için işverenlere işçilere kendi çalışma programını yönetme, ihtiyaçlarına göre bir çalışma düzeni oluşturma, işçilerin işlerini kaybetme kaygısı taşımadan dinlenme ve özel hayata ilişkin anlarında işle bağlantılarını kesmelerini, kullanımlarına verilmiş bilişim sistem ve uygulamalarıyla bağlantıyı kesme hakkının tanınmasını, bu hususta yöneticilerin gerekirse takvim ve çalışma programı oluşturmalarını önerilmektedir[1368].

Dijitalleşmenin dönüştürdüğü işveren denetimi bilişim sistemleri temelinde çeşitlenip gelişirken, iş hukuku normlarının bu denetim türünde işçinin özel hayatına saygı hakkını ve kişisel verilerini etkin koruyacak düzenlemeler barındırmadığını belirtmek gerekir[1369]. İş ilişkisinde teknolojinin ortaya çıkardığı menfaat çatışmasının işçinin özel hayatı ve kişisel verileri üzerinde ihlal edici etkiler ortaya çıkarmaması için işçinin işyeri bilişim sistemleriyle ve dijital izleme uygulamalarıyla bağlantısını kesme hakkı ve kişisel zamanında bu sistemler vasıtasıyla işçiye ulaşılmamasının yasal çerçeveye[1370] kavuşturulması gerekmektedir[1371]. Aksi durumda işçi işverenle sorun yaşamamak ve kariyer kaygıları sebebiyle kişisel zamanlarında iş ilişkisine ilişkin gelişmelere maruz kalmaya devam edecektir. Bu durumun işçinin anayasal dinlenme hakkını da ihlal ettiğini eklemek gerekir.

IV. Dijital İzleme Uygulamalarında Veri Koruma Etki Değerlendirmesinin Zorunlu Olması Gerekliliği

KVK hukukumuzda, GVKT m. 35'te düzenlenen veri koruma etki

1368) ILO, COVID-19 Ortamında ve Sonrasında Uzaktan Çalışma Uygulama Kılavuzu, [2020], s. 17-18,https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-ankara/documents/publication/wcms_759299.pdf (Erişim Tarihi: 07.09.2023).
1369) Adams-Prassl, [2019], Artificial Intelligence at Work, s. 134.
1370) Ulusal düzeyde, Fransa işçinin bağlantıyı kesme hakkını ilk kez 2013 tarihinde tanımış ve İş Kanunu'nun L.2242-17 maddesinde düzenleme gerçekleştirmiştir. Eurofound 2021 raporuna göre bugüne kadar Belçika, Fransa, İtalya ve İspanya'nın bağlantıyı kesme hakkını içeren mevzuatı bulunmaktadır. Almanya geleneği işyeri uygulaması çerçevesinde gelişmektedir. Secunda, [2019], Right to Disconnect, s. 27-29.
1371) Secunda, [2019], Right to Disconnect, s. 27-30.

değerlendirmesi ile m. 22'de yer alan profil çıkarmanın sınırlandırılmasına ilişkin düzenlemelerin öngörülmemesi önemli eksiklerdir. Özellikle yeni teknolojilerle devamlı dönüşen dijital izleme uygulamalarının işçinin kişisel verilerini iş ilişkisini aşacak yoğunlukta otomatik işlemeye konu edilebilme olasılığı dikkate alındığında bu denetimler işçi verisini korumada etkili bariyerler oluşturur. Kişisel veri etki değerlendirmesinde işlenecek kişisel verilerin kapsamı, amaçları, işleme bağlamı, işlenecek kişisel verilerin niteliği gibi denetimler sayesinde bunun işçiler üzerinde oluşturacağı etkinin ve ilgili kişinin hak ve özgürlüklerine müdahale boyutu ortaya çıkmış olur. Böylelikle iş ilişkisinde işlenmesi zorunlu olan kişisel veriler en az müdahaleyi gerektirecek yöntemle işlenmiş olur. Diğer yandan iş ilişkisi açısından GVTK m. 88'in üye ülkelere önemli bir uygulama esnekliği ve GVKT düzenlemelerinden daha ileri korumaları öngörme imkanı sağlaması dikkate alınarak müktesebata uyum açısından belirli uyumlandırmaların yapılması gerekmektedir[1372].

Aynı husus algoritmik profilleme ve algoritmik izleme için de geçerlidir. İşverenlerin işçi veya işçi adaylarının verilerini büyük veri sistemlerinde işlemesi, sonrasında bu verileri işçiler açısından çıkarım yapacak algoritmik analizlere tabi tutması işçinin temel hak ve özgürlükleri ile kişilik hakları üzerinde ihlal edici sonuçlar ortaya çıkaracaktır. Bundan dolayı öncelikli olarak iş ilişkisinde verilerin doğrudan işçilerden elde edilmesine ilişkin sınırlandırmalar öngören hükümler gerçekleştirilmeli ve yapay zeka uygulamaları ile algoritmik analizler için de algoritmik analiz etki değerlendirmesinin zorunlu hale getirmek gerekmektedir.

Öte yandan veri sorumlusu işverenden bağımsız olarak kullanılan bilgisayar yazılımlarının bu programı kullanan kişilerin kişisel verilerini gizlice izlediği ve kayıt altına aldığı tespit edilmiştir[1373]. İşverenin koruma borcu kapsamında işçilerin bu tür yazılımlar vasıtasıyla izlenmesini ve verilerini gizlice kayıt altına almasını

1372) Adams-Prassl, [2019], Artificial Intelligence at Work, s. 143.
1373) Sjoera Nas, "Data Protection Impact Assessment: Assessing the Risks of Using Microsoft Office ProPlus", European Data Protection Law Review (EDPL), Vol. 5, No. 1, [2019], s. 107.

engelleyecek bir çalışma ortamı kurması gerekir. Örneğin Microsoft'un Windows 10 işletim sistemi ve Office programları olan Word, Excel, PowerPoint, Outlook gibi uygulamalarda kişisel verilerin kullanıcıların bilgisi dışında işlendiği tespit edilmiştir. 2017 yılında Hollanda'da hükümet tarafından bu programlara ilişkin yapılan Veri Koruma Etki Değerlendirmesi Raporu'nda bu programların kişisel verileri kullanıcıların bilgisi dışında işlediği ve kullanıcılarına işlenen kişisel verileriyle ilgili herhangi bir seçenek sunmadığı ve ilgili kişilerin kişisel verilerinin işlenmesini kapatma seçeneğinin de bulunmadığı ortaya çıkmıştır. Bunun ortaya çıkmasının üzerine gösterilen tepkilerin bir sonucu olarak Microsoft, Office yazılımlarında 2019 yılından itibaren iyileştirmeler yaptığını duyurmuştur. Ne var ki örneğin Word yazılımında kullanıcı bilgileri ve yazım geçmişi, yazım hatalarını çevrim için düzeltme ve denetim gibi uygulamalarla kullanmaya devam etmektedir[1374].

İlk kez GVKT ile düzenlemeye kavuşan veri koruma etki değerlendirmesi (data protection impact assessment) veri sorumlusuna (iş ilişkisinde işveren) kişisel veri işleme sürecinde şeffaflığı sağlama ve hesap verebilir bir yapı oluşturma yükümlülüğü yüklemektedir. Zira dijital izleme uygulamalarının türlerinden olan nesnelerin interneti, giyilebilir yapay zeka sistemleri, algoritmik analize konu edilebilir büyük veri, internet izleri gibi işleme faaliyetleri işçinin kişilik hakları üzerinde büyük ihlallere sebebiyet verme ihtimalini barındırmaktadır. Bunun engellenmesi için dijital izleme uygulamasıyla veri işleme faaliyetine başlamadan önce işlenecek kişisel verilerle ilgili olarak veri koruma etki değerlendirmesinin yapılması bu riskleri minimize edecektir[1375].

GVKT m. 35/3 düzenlemesine göre özellikle gerçek kişinin verilerinin otomatik işlemeye konu edildiği durumlarda ve halkın kullanımında olan bir alanın

1374) Nas, [2019], Impact Assessment, s. 107-108.
1375) WP 29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 October [2017], s. 4; Kim T. Pauline, "Privacy Rights, Public Policy, and the Employment Relationship", Ohio State Law Journal, Vol. 57, No. 3, [1996], s. 671; Solove, [2023], Murky Consent, s. 18.

büyük çaplı ve sistematik olarak izlenmesi durumunda veri koruma etki değerlendirmesinin yapılması zorunludur[1376]. Etki değerlemesinin en az neleri içereceği GVKT m. 35/7'de düzenlenmiştir. Buna göre kişisel verilerin işlenmesindeki hukuka uygunluk sebepleri, veri sorumlusunun meşru menfaatleri ve veri işleme amaçlarına ilişkin sistematik açıklama, veri işleme faaliyetinin gerekliliği ve orantılılığına ilişkin değerlendirme, özel nitelikli kişisel veriler var ise bunların işlenmesine ilişkin gereklilik ve değerlendirme, veri sahibinin hakları ve özgürlüklerine gerçekleştirilecek müdahalenin riskler ve değerlendirmeler, başka bir yöntemle veri işlemeden sürecin yürütülüp yürütülemeyeceğine ilişkin değerlendirme ve kişisel verilerin korunmasına ilişkin alınan tedbir ve güvenceler yer alır[1377].

Veri koruma etki değerlendirmesinde öngörülen denetimler gerçekleştirilecek kişisel veri işleme faaliyetin en az kişisel veri işlenerek nasıl gerçekleştirileceği, daha az müdahaleci bir yöntemin bulunup bulunmadığı hususlarında gereklilik, sınırlı ve ölçülü olma, meşru amaç açısından bir araştırma gerçekleştirmeyi zorunlu kılmaktadır. Bu itibarla KVKK'da öngörülmemiş olan bu düzenlemenin iç mevzuatımıza aktarılması dijital izleme gibi yoğun veri işlenen faaliyetlerde kişisel verilerin işlenmesinin ve korunmasının ortaya çıkardığı riskleri minimize edecektir. Eklemek gerekir ki, kişisel veri işleme faaliyetinden önce veri koruma etki değerlendirme araştırması gerçekleştirilmesi aynı zamanda Avrupa Komisyonu'nun modernize ettiği 108 sayılı Sözleşme'nin 10/2. fırkasında da öngörülmüştür. Düzenleme, kişisel veri işlemenin kişisel veri sahibinin temel hak ve özgürlükleri üzerindeki olası etkilerinin kişisel veri işlenmeden önce ortaya konması amacıyla bir ön inceleme yapılmasını zorunlu kılmaktadır[1378].

WP 29 Çalışma Grubu kişisel veri etki değerlendirmesi için dokuz kriter geliştirmiş ve kriterlerden ikiden az olanını karşılayan veri işleme süreçlerinin az

1376) Nas, [2019], Impact Assessment, s. 108-109.
1377) General Data Protection Regulation, Preamble, Recital 75; EU, [2018], Handbook, s. 180.
1378) EU, [2018], Handbook, s. 180.

riskli olduğunu, iki ve daha fazla kriteri karşılayan süreçlerin ise riskli olduğunu ve etki değerlendirmesi yapılmasını önererek, bunun veri koruma mevzuatına uyum açısından yardımcı bir mekanizma olduğunu vurgulamaktadır[1379]. Ayrıca GVKT m. 35/1 veri işleme sürecinde yeni teknolojinin kullanılması, işleme bağlamı, kapsamı ve amacı açısından; m. 35/3 ise işleme türü açısından ölçütler sunarak veri işlemenin bireyin hakları ve özgürlükleri açısından ortaya çıkardığı yüksek riski minimize etmek için etki değerlendirmesini hüküm altına almaktadır[1380].

WP 29 Çalışma Grubu'nun belirlediği kılavuz ilkelerde belirli durumlarda veri koruma etki değerlemesinin gerekli olup olmadığını belirlemeye yardımcı olacak dokuz kriter belirlenmiştir[1381]. Buna göre, "1) veri işlemede ilgili kişiyle ilgili değerlendirme ve puanlamanın bulunması, 2) yasal veya benzeri önemli etkiye sahip otomatik karar alma, 3) sistematik izleme, 4) özel nitelikli kişisel veri işlenmesi, 5) büyük ölçekte işlenen veri söz konusu olduğunda, 6) eşleştirilen veya birleştirilen veri kümelerinin bulunması halinde, 7) iş ilişkisi gibi güç dengesizliğinin bulunduğu zayıf durumdaki kişilerin verilerinin işlendiği durumlarda, 8) yeni teknolojilerin kullanılması ve yeni teknolojik uygulamaların organizasyonel çözümler için kullanılması, 9) işlemenin kendi başına, veri sahibinin bir hakkını kullanmasını veya bir hizmeti veya sözleşmenin uygulanmasını engellemesi" durumunda, iki kriterden daha azını karşılayan veri işleme faaliyetlerinin daha düşük risk seviyesinde olduğunu ve bir veri koruma değerlemesinin yapılmasına gerek olmadığını, iki veya daha fazla kriteri karşılayan veri işleme faaliyetlerinde ise bir etki değerlendirmesinin yapılması gerektiğini

1379) Article WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 October, 2017; EU FRA, Handbook, s. 180.
1380) Raphael Gellert, "The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment", European Data Protection Law Review (EDPL), Vol. 3, No. 2, [2017], s. 212-213, (Gellert, [2017], Impact Assessment).
1381) Article WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679, WP 248 Rev.01, 2017, Brussels, 4 October 2017.

öngörmüştür[1382].

İş ilişkisinde kullanılan dijital izleme uygulamaları işçinin performansı, sağlığı, kişisel beğeni ve tercihleri, ilgi alanları, konumu, boş zaman aktiviteleri gibi birçok veriyi otomatik olarak işlemeye konu edebilir. Bu durum GVKT m. 35/1'de öngörülmüş olan ve işçinin özel hayatı ile kişisel verileri üzerinde ihlal edici yüksek riskler ortaya çıkarır. Bu durumda veri sorumlusu işverenin veri koruma etki değerlendirmesini yapması işçinin bu hakları üzerindeki müdahaleci etkiyi minimize edecektir[1383]. WP 29 Çalışma Grubu görüşünde etki değerlendirmesinin yapılmasının ölçütü olarak sayılan 9 kriterin 7. kriteri iş ilişkisi gibi hiyerarşik ilişkinin bulunduğu, güç dengesizliği sebebiyle iradesini açıkça ortaya koyamayacak veya dijital izleme uygulamasına karşı çıkamayacağı durumlarda veri koruma etki değerlendirilmesi yapılması önerilmektedir[1384].

Yukarıda ele alındığı üzere, yeni teknolojilerin işçilerin verilerini işleme biçimi ve gelecekte işlemeye konu edeceği veri boyutu düşünüldüğünde açık rıza ve aydınlatma yükümlülüğü gibi kişisel veri koruma mekanizmalarının bireyin verisini korumakta sorunlu alanlar bırakacaktır[1385]. Bu itibarla iş ilişkisinde dijital izleme uygulaması kullanılmadan önce veri koruma etki değerlendirmesinin gerçekleştirilmesi işçilerin hak ve özgürlüklerinin korunmasında ve kişisel verilerinin işlenmesinde koruyucu sonuçlar ortaya çıkaracaktır. Ancak etki değerlendirmesi yapıldıktan ve dijital izleme uygulamasının uygulanabilir olduğu sonucuna ulaşıldıktan sonra[1386] işçilerin işlenen kişisel verileri konusunda bilgilendirilmeleri ve diğer kişisel veri işleme şartlarının bulunmadığı durumlarda dijital izleme gerçekleştirmeden önce açık rızalarının alınması kişisel veriler üzerindeki ihlali sınırlandıracaktır.

1382) EU, [2018], Handbook, s. 181; Article WP29, Guidelines on Data Protection Impact Assessment, s. 9-11.
1383) Gellert, [2017], Impact Assessment, s. 213.
1384) Article WP29, Guidelines on Data Protection Impact Assessment, s. 11.
1385) Solove, [2023], Murky Consent, s. 29.
1386) Erion Murati/Manjola Henkoja, "Location Data Privacy on MAAS under GDPR", European Journal of Privacy Law & Technologies (EJPLT), Vol. 2019, No. 2, [2019], s. 132.

V. İş İlişkisinde Otomatik Profil Oluşturan Yapay Zeka Destekli Dijital İzleme Uygulamalarının Sınırlandırılması

İş yaşamında giderek yaygınlaşan giyilebilir sistemler ve biyometrik veri temelli teknolojilerin kullanılması işverenin, işçi üzerindeki kontrol düzeyini artıracak sonuçlar ortaya çıkarmaktadır. Yapay zeka teknolojisinin[1387] kullanıldığı bu sistemler işçinin kişisel özelliklerini hesaba katan veriler işleyebildiğinden işverene, işçi hakkında davranış temelli biyometrik veri sunmaktadır. İşçinin özlük verileri, performans ve iş ilişkisindeki diğer davranışlarıyla eşleştirilebilen bu kişisel veriler işçinin gelecekteki davranış ve tutumları hakkında çıkarımlarda bulunmak için kullanılabilir. Böylelikle dijital izleme, yapay zeka teknolojilerindeki hızlı gelişmelerin olanaklarıyla iş ilişkisinde "insan analitiği" olarak nitelendirilen kişisel verilerden elde edilen algoritmik çıkarımlara (profil oluşturma) dönüşmekte ve işçiyi dijital bir nesneye indirgeme riskini içinde barındırmaktadır[1388].

İşverenlerin kullanmaya başladığı duygu algılama teknolojisi gibi bazı teknolojiler, fizyonomi biliminin verilerini de kullanarak yüz hareketlerine veya boyutlarına dayalı olarak duyguları veya kişilik özelliklerini tanımlayarak dijital izlemeyi uzaktan ve her yerde gerçekleştirme olanağını bir adım daha ileri

---

1387) AB, dünyanın ilk "Yapay Zeka Yasası" üzerinde çalışmaya başladığını Aralık 2023'te duyurdu. Duyuruda yapay zekanın (AI) daha iyi sağlık hizmetleri, güvenli ve temiz ulaşım, daha verimli üretim ve ucuz sürdürülebilir enerji hususlarında önemli avantajlar sağlayabileceğini, fakat farklı uygulamalarda kullanılan yapay zeka sistemlerinin kullanıcılar için profilleme gibi riskler ortaya çıkardığını ifade etmiştir. Bunun önüne geçmek için AB'de kullanılan yapay zeka sistemlerinin güvenli, şeffaf, izlenebilir, ayrımcı olmayan ve çevre dostu olmasını sağlamanın önemli olduğu ve yapay zekanın zararlı sonuçları önlemek için yapay zeka sistemleri otomasyon yerine insanlar tarafından denetlenmesi önerilmiştir. Parlamento yapay zekanın kabul edilemez risklerini: "insanların veya belirli hassas grupların bilişsel davranışsal manipülasyonu, örneğin çocuklarda tehlikeli davranışları teşvik eden sesle etkinleştirilen oyuncaklar; sosyal puanlama: insanları davranışa, sosyo-ekonomik duruma veya kişisel özelliklere göre sınıflandırmak, insanların biyometrik tanımlanması ve sınıflandırılması, yüz tanıma gibi gerçek zamanlı ve uzaktan biyometrik tanımlama sistemleri" biçiminde tespit etmiştir.
https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (Erişim Tarihi: 24.12.2023).
1388) Sara Riso, "Monitoring and Surveillance of Workers in The Digital Age" https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age (Erişim Tarihi: 18.12.2023)

götürmektedir. Bu tür dijital izleme uygulamaları sayesinde bir işçinin yüzünün biyolojik özelliklerinden ve gün içindeki değişim ve tepkilerinden hareketle karakteri, yaşayışı, öncelikleri ve hayat yorumlayışı belirli bilgilerin ortaya çıkarılması ve bilgilerin işlenerek işçiye özgü algıların yönlendirilebilmesine olanak tanımaktadır[1389].

Tüm bu gelişmelerin bir sonucu olan ve bir veri izleme tekniği olan profil oluşturma (insan analitiği) belirli bir insan veya insan grubuna ait bir dizi özellik bu grubun geçmiş yaşam pratiğinden ortaya çıkan verilerden çıkarsanır ve daha sonra elde edilen sonuç bu karakter kümesine yakın uyum gösteren bireyler veya veri işlemeye konu edilen grup veya kişi için çıkarsamalara konu edilir[1390]. Profil oluşturma birey veya birey guruplarının otomatik dijital izleme uygulamaları vasıtasıyla verilerinin işlenmesi sonucu ortaya çıkan profille (özellik) daha sonra bu kişiye/varlığa veya diğer kişilere/varlıklara bu özelliklerin ışığında muamele edilmesidir. Özellikle işverenlerin kullanmaya başladığı duygu algılama teknolojisi gibi bazı teknolojiler, fizyonomi biliminin verilerini de kullanarak yüz hareketlerine veya boyutlarına dayalı olarak duyguları veya kişilik özelliklerini tanımlayarak dijital izlemeyi uzaktan ve her yerde gerçekleştirme olanağını bir adım daha ileri götürmektedir. Bu tür dijital izleme uygulamaları sayesinde bir işçinin yüzünün biyolojik özelliklerinden ve gün içindeki değişim ve tepkilerinden hareketle karakteri, yaşayışı, öncelikleri ve hayat yorumlayışı belirli bilgilerin ortaya çıkarılması ve bilgilerin işlenerek işçiye özgü algıların yönlendirilebilmesine olanak tanımaktadır[1391].

KVK hukukumuzda profil oluşturma ile ilgili bir düzenleme bulunmamasına rağmen, profil oluşturmada kullanılan veri bir gerçek kişiyi belirli veya belirlenebilir duruma getiriyorsa profil oluşturmada işlenen veri KVKK'nın

1389) Houwing, [2020], Biometric Surveillance, s. 175-176.
1390) Roger Clarke, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance", Journal of Law and Information Science, Vol. 4, No. 2, [1993], s. 404; Otto, [2019], Workforce Analytics, s. 390-391.
1391) Houwing, [2020], Biometric Surveillance, s. 175-176.

hükümleri kapsamında değerlendirilir. Bu sebeple profilleme sistemlerinin KVK hukukunun düzenlemelerine uygun veri işleme faaliyeti yürütmesi zorunludur[1392]. GVKT m. 4/4'te profil oluşturmanın tanımı gerçekleştirilmiş ve bir gerçek kişinin işteki performansı, kişisel tercihleri, davranışları, konumu veya işyerindeki hareketleri, rutinleri ve olay anlarında verdiği tepkilerin otomatik sistemler tarafından işlenmesi bu kapsamda değerlendirilmiştir[1393].

Profil oluşturma, tamamen otomatik sistemler vasıtasıyla gerçekleştirilir ve kişisel veri işleme tekniğinden farklı olarak doğrudan bir kişinin verisinin işlenmesi söz konusu değildir. Bunun yerine hakkında şüphe duyulan ve daha sonra izlemeye tabi tutulabilecek işçi gruplarının (kişilerin) davranışları gelecekte belirli çıkarımlarda (tahmin) bulunmak amacıyla bilişim sistemleri vasıtasıyla otomatik işlemeye konu edilir. İş ilişkisinde kullanılan profil oluşturan dijital izleme uygulamalarının işlediği veri bir işçinin daha sonra yapılacak bir incelemede belirlenebilmesi ihtimalini barındırdığı durumlarda profillemenin KVK hukukunun ilkelerine uygun olması gerekir.

Belirtmek gerekir ki, profillemede kitlesel veri işleme tekniklerinin tüm potansiyel olumsuz yönleri bulunmaktadır. KVK Kurulu, profilleme vasıtasıyla veri işlenmesini KVKK kapsamında değerlendirmiş ve profillemenin her zaman kötü bir uygulama olmadığını, bireyin temel hak ve özgürlüklerini, güvenliklerini tehdit etmeyecek noktaya kadar profillerin oluşturulmasının makul görülmesi gerektiğini ifade etmiştir. KVK Kurulu, profillemede bir kişinin belirli veya

1392) Alman Federal İş Mahkemesi, iş bilgisayarına kurulan bir klavye yakalayıcısı (Keylogger vb.) yazılımının kişinin iş ve özel hayatına ilişkin birçok veriyi işleyebileceğine, bu şekilde izlemenin veri sahibinin izlemenin etki alanına ilişkin haklarına ve bilgilendirilme hakkına ağır bir ihlal oluşturduğunu, işçinin bilgisayar ve klavye ile teması ile temasının kesilmesi arasındaki verilerin işlenme olanağı bulunduğunu, bunun işçi için geri dönülmez bir kayıt ve saklanma anlamına geldiğini, bu şekilde işlenen veriler, ilgili kişinin hem özel hem de iş kullanımına ilişkin neredeyse kapsamlı ve eksiksiz bir profil oluşturmayı mümkün kıldığını tespit ederek bu uygulamaların bu şekilde profil oluşturacak biçimde kullanılmasını veri koruma hukukuna aykırı bulmuştur. Bkz. BAG 2 AZR 681/16, § 33.

1393) Mireille Hildebrandt, Defining Profiling: A New Type of Knowledge, Profiling the European Citizen (Ed. Mireille Hildebrandt/Serge Gutwirth), Springer, [2008], s.17 vd.

belirlenebilir hale gelmesi durumda profillemenin KVKK kapsamında değerlendirileceğine karar vermiştir. Kararda profilleme: "Uluslararası uygulamada bireyin davranışlarının analiz edilerek bunu izleyen davranışları hakkında tahminlerde bulunmak adına bireyin kişisel verilerinin otomatik olarak işlenmesi 'profilleme' olarak adlandırılmaktadır. 'Tahmin' kelimesinin kullanılması aslında profil oluşturmanın bir kişi hakkında bir tür değerlendirme veya yargı içerdiğini göstermektedir" biçiminde tanımlamıştır[1394].

İşyerinde makine öğrenmesine, algoritmik analizlere ve üreten yapay zeka uygulamalarına kaynaklık eden profilleme esaslı otomatik karar sistemleri verilerden ve büyük oranda işçinin kişisel verilerinden beslenir. Bu veri madenciliği türünde iş süreçlerinin ve işçi gruplarının profilleri oluşturulabilir. Böylelikle örneğin işçinin hangi durumda nasıl davrandığı, hangi aralıklarla ne tür rutinlerde bulunduğu, işyeri izleri, yaşam tarzı ve alışkanlarıyla ilgili büyük miktarda veri işlenmekte ve bu veriler çeşitli kategorilerde analizlere konu edilebilmektedir. Bu sayede işçinin verimliliği ve gelecekte belirli olaylar karşısında nasıl davranacağına ilişkin bir profil ortaya çıkarılır. Ortaya çıkan profil işe alım, personel organizasyonu, işçileri belirli görevlerde optimizasyonu ve yönetimi, işçilerin hem doğrudan hem de dolaylı denetimi olanağını işverene vermektedir[1395].

Dijital izlemeyle oluşturulan profiller üretim stratejilerinde veya işçilere ilişkin çeşitli türde algoritmik analize tabi tutularak hedeflerin gerçekleştirilmesinde kullanılır[1396]. Örneğin satış biriminde çalışan işçilere ziyaret ettikleri müşteri sayısı ve hedef satış esas alınarak artırımlı prim verilmesinin saha ziyaretlerine ve işçilerin performansına etkisinin dijital izleme uygulamalarıyla takip edilmesi ve bir profilin ortaya çıkarılması, ortaya çıkan profilin gelecek

1394) Bkz. KVK Kurulu, "Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarihli ve 2021/1303 sayılı Karar Özeti" https://www.kvkk.gov.tr/Icerik/7288/2021-1303 (Erişim Tarihi: 30.03.2023).
1395) Otto, [2019], Workforce Analytics, s. 392.
1396) Otto, [2019], Workforce Analytics, s. 391.

hedeflerde kullanılması profilleme sayesinde gerçekleştirilebilir.

Profillemenin yapılması iş ilişkisinde önemli riskleri de beraberinden getirmektedir. Bu risklerden en büyüğü işçilerin özel hayatı, kişisel zamanı ve kişisel verileri ile ilgili işverenlerin büyük miktarda veri işlemesi ve bunun sonucu olarak işçilerin temel hak ve özgürlükleri ile verileri üzerindeki hakların ihlal edilebilme olasılığıdır. Bir diğer risk ise otomatik bireysel karar alma sistemleri olan profilleme algoritmik karar verme esaslı çalıştığından örneğin algoritmik seçilim daha önceki bireysel kararlara dayanıyorsa, bu durum karar almayı potansiyel olarak baltalayan aynı önyargıların algoritma tarafından çoğaltılmasa bile tekrarlanması olasılığını ortaya çıkarır[1397].

Ele alındığı üzere veri işleme faaliyetinin KVKK kapsamında değerlendirilebilmesi için tamamen veya kısmen otomatik olarak işlenmesi ya da bir veri kayıt sisteminin parçası olmak kaydı ile otomatik olmayan yöntemlerle işlenmesi gerekmektedir (KVKK m. 3/1-e, GVKT m. 4/2). KVKK m. 3/1-e'ye göre, kişisel verilerin elde edilmesi, kaydedilmesi veya depolanması da dahil olmak üzere, kişisel veriler üzerinde gerçekleştirilen herhangi bir işlem veya işlemler dizisi kişisel verilerin işlenmesidir[1398]. Bu itibarla profillemede işlenen işçi veri parçaları bir bütün olarak kişisel veri işleme faaliyetini oluşturur. Zira otomatik sistemler vasıtasıyla bir işçi esas alınmadan işlenen verilerden, işlenen verilerin hangi işçilere ait olduğunun "belirlenebilmesi" mümkündür. Bir gerçek kişinin belirlenebilir hale gelmesi ölçütü dikkate alındığında profillemede işlenen verileri kişisel veri haline getirmektedir[1399]. Nitekim, KVK Kurulu profillemeyle ilgili vermiş olduğu bir kararda profillemeyi kişisel veri işleme olarak değerlendirmeye konu etmiştir[1400].

1397) Clarke, [1993], Data Surveillance, s. 403-505; Otto, [2019], Workforce Analytics, s. 393 vd.
1398) KVK Kurumu, [2019], Uygulama Rehberi, s. 53-54.
1399) Hendrickx, [2019], Privacy 4.0 at Work, s. 165.
1400) Bkz. KVK Kurulu, "Araç kiralama programları yazılımcısı ve satıcısı firmalar tarafından, ilgili kişilerin verilerinin işlenmesi ve bu verilerin araç kiralama firmaları arasında paylaşılmasını sağlayan bir kara liste programı oluşturulması hakkında Kişisel Verileri Koruma Kurulunun

Dijital izlemede işçilerin işlenen verilerinden olan metadata veriler, çerezler ve profil oluşturma uygulamalarıyla ilgili KVKK'da bir tanım ve düzenleme yapılmamıştır. KVK Kurumu yayımladığı rehberle çerezleri[1401] KVKK kapsamında değerlendirmiş ve rehberde bu tür kişisel verilere ilişkin detaylı açıklamalar getirilmiştir. Aynı husus metadata verileri[1402] için çeşitli KVK Kurul kararlarda yapılmıştır. GVKT m. 4'te profil oluşturma tanımlanmış ve bir gerçek kişinin işteki performansının analiz edilmesi için veya kişisel özelliklerinin değerlendirilmesi ve kişiye ilişkin belirli çıkarımlar yapılması amacıyla otomatik her türlü kişisel veri işleme profil oluşturma kapsamında değerlendirilmiştir. GVKT m. 22/1'de ise profil oluşturma dahil olmak üzere tam otomatik bireysel karar alma süreçleri yasaklanmıştır. Devamı fıkralarda ise kuralın istisnaları düzenlenmiş ve bu durumlarda verisi işlenen ilgili kişilerin hakları, özgürlükleri ve meşru menfaatlerini koruyacak önlemlerin alınması yükümlülüğü düzenlenmiştir[1403].

Sonuç olarak, KVKK'da bireyin profilinin oluşturulmasıyla ilgili olarak GVKT m. 22 hükmüne benzer bir düzenleme gerçekleştirilmeli ve bireyin profilini oluşturabilen otomatik veri işleyen dijital izleme uygulamalarının yasaklanması ve kullanılmasının zorunlu olduğu durumlar istisnai olarak düzenleme altına alınması gereklidir. Aksi durumda gelişen teknoloji, bireyin internetle bağlantısı olan nesnelerle etkileşiminin artması (nesnelerin interneti) ve sensörler, giyilebilir teknoloji, e-ticaret gibi otomatik profil oluşturma esası üzerinde çalışan sistemlerin kişinin özel hayatı ve kişisel verileri üzerindeki ihlal edici etkisinin sınırlanması gittikçe güçleşecektir.

23/12/2021 tarihli ve 2021/1303 sayılı Karar Özeti" https://www.kvkk.gov.tr/Icerik/7288/2021-1303 (Erişim Tarihi: 30.03.2023).

1401) KVK Kurumu, Çerez Uygulamaları Hakkında Rehber, Haziran 2022. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf (Erişim Tarihi: 11.11.2022).

1402) KVK Kurulu, WhatsApp Kararı, https://www.kvkk.gov.tr/Icerik/7045/WHATSAPP-UYGULAMASI-HAKKINDA-YURUTULEN-RESEN-INCELEMEYE-ILISKIN-KAMUOYU-DUYURUSU (Erişim Tarihi: 12.11.2022).

1403) EU, [2018], Handbook, s. 234-235. Otto, [2019], Workforce Analytics, s. 394.

SONUÇ

Çalışmadaki amacımız işverenin işyerine ilişkin mülkiyet hakkı, yönetim hakkı, ticari itibarını koruma hakkı, meşru ekonomik çıkarlarının korunması hakkı gibi hakları ile idari yükümlülükleri ve işçileri gözetme borcu kapsamında gerçekleştirdiği dijital izleme uygulamalarında işçinin kişilik hakkı, özel hayatına saygı hakkı ve kişisel verileri üzerindeki hakları arasında nasıl bir adil denge oluşturulabileceğini ve bilişim sistem ve uygulamaları temelinde gerçekleştirilebilen dijital izlemenin işçinin kişilik hakları üzerindeki ihlal edici etkisinin nasıl sınırlandırılacağını incelemekti. Konuyu somutlaştırmak için girişte işverenlerin iş sözleşmesinden doğan anılan haklarının işçilerin temel hak ve özgürlüklerinden olan özel hayatları ve kişisel verileri üzerindeki haklarını ne düzeyde sınırlandırılabileceğine, iş ilişkisinde kullanılan dijital izleme uygulamalarının sınırlandırılmasında neleri esas alınacağını ve sınırın nasıl belirleneceğine ilişkin sorular sormuştuk.

İncelendiği üzere işçilerin özel hayatları ile kişisel verilerinin gizliliğinin korunması çeşitli uluslararası ve ulusal hukuk düzenlemesine konu edilmiş ve bunların nasıl korunacağı, kişisel verilerin hangi durumlarda işlenebileceği kurallara bağlanmıştır. Ayrıca işçilerin bu haklarının iş ilişkisi kapsamında da mevcut olduğu, meslek hayatının özel hayat ve kişisel verilerin dışında tutulamayacağı yargı kararlarında da teyit edilmiştir[1404]. Eklemek gerekir ki, işçinin iş görme borcunu ifası için kendisine tahsis edilmiş bilişim sistem ve uygulamalarını işin niteliği gereği yasağı gerektirdiği durumlar söz konusu olmadıkça kişisel amaçla veya iş görme borcunun ifası için kullanması gerçekleştirilen iletişimi özel hayat ve kişisel veri olmaktan çıkarmamaktadır[1405]. Zira özel hayat ve kişisel verilerin korunması aynı zamanda işçinin başkalarıyla

1404) ABAD, Österreichischer Rundfunk and Others v. Austria, § 25, § 73, § 74 ve § 75; AİHM, Copland v. United Kingdom, § 41, § 42, § 45; AİHM, [GK], [2017], Bărbulescu v. Romanya, § 25, § 69, § 71; AİHM, Niemietz v. Almanya, § 29.
1405) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 71.

sosyal temasta olması, sosyal kimliğini toplumda ifade edebilme ve geliştirmesi, ilişkiler geliştirmesi hakkı anlamına da gelmektedir[1406]. Öte yandan iş ilişkisinde işçilerin özel hayatları ve kişisel verilerinin korunması hakkı mutlak bir hak değildir. İşçinin bu hakları işverenin mülkiyet hakkı, ticari itibarı, ekonomik hakları ile gözetme borcu gibi hak ve yükümlülükler tarafından sınırlandırılır.

Bireyin kişilik haklarının kapsamında yer alan özel hayat kavramı tanımlanması güç ve kapsamının sınırlandırılması mümkün değildir. Teknolojiyle değişen yaşam tarzının ve dijital izleme uygulamaları gibi bilişim teknolojileri temelinde gerçekleşen veri işleme süreçlerinin özel hayat üzerinde ortaya çıkardığı etki dikkate alındığında bu kavramın bir tanım kapsamında sınırlandırılmasının gerekli olmadığını da göstermektedir. Uzun bir süre özel hayat kapsamında değerlendirilmiş kişisel veriler ise bir kişiyi belirli veya belirlenebilir hale getiren her türlü bilgi olduğundan bu bilginin özel hayat alanında, kamusal alanda veya kamuya açık paylaşılmış, kamusal alanda görülmüş olması arasında bir fark olmaksızın KVK hukukunun hükümleri kapsamında korunmaktadır. Eklemek gerekir ki, özel hayata saygı hakkından çıkmış bir hak olmasına rağmen kişisel verilerin korunması kendi dinamikleri çerçevesinde bağımsız olarak gelişmiştir. Ayrıca bu iki hakkın yarışan haklar olmadığını, birbirini destekleyen, bazı durumlarda birlikte korunan haklar olduğunu belirtmek gerekir[1407]. Kişisel verilerin teknolojik gelişmelerle işlenme biçimi, boyutu ve amacının değişmesi bireyin bu hakkının hangi boyutta ve hangi koşullar altında korunacağına ilişkin kuralların gelişmesini tetiklemiştir. Bu itibarla KVK hukuku özel, kamusal alan veya özel teşebbüs veya kamu kurumu ayrımı yapmadan kişisel verilerin korunmasını başlangıç noktası olarak kabul etmektedir[1408].

İş ilişkisinde kullanılan dijital izleme uygulamaları şüphesiz ki gelişecek yeni teknolojiler kapsamında çeşitlenecektir. Günümüzde işyerinde yoğun olarak

1406) AİHM, [GK], [2017], Bărbulescu v. Romanya, § 70; AİHM, Niemietz v. Almanya, § 29.
1407) Küzeci, [2023], Verilerin Korunması, s. 51.
1408) Alpagut, [2019], Kamera Gözetlemesi, s. 279.

dijital izleme kamera gözetlemesi, biyometrik veya kart, şifre esaslı işyeri giriş sistemleri, hareket ve konum belirleme sistemleri vasıtasıyla izleme, giyilebilir teknolojilerle işçilerin izlenmesi, işçinin internet, bilgisayar, e-posta gibi iletişiminin izlenmesi biçiminde gerçekleştirilmektedir. Bu sebeple ve işçinin iş sözleşmesinin zayıf tarafı konumunda olması da dikkate alınarak onun haklarının önceliklendiren yasal sınırlandırmaların oluşturulması gerekmektedir. Bu aynı zamanda iş sözleşmesinin tarafları arasındaki güç dengesizliğinin nispi emredici normlarla işçi lehine dengelemeye çalışan iş hukukunun temel yaklaşımının da bir gereğidir[1409].

Bir amaç kapsamında veya rastgele uygulanan dijital izleme uygulamaları işçilerin kişisel verilerini işlemektedir. İşçinin kişisel verisi işçiyi belirli veya belirlenebilir hale getiren her türlü bilgi olduğundan bu bilgilerin korunması için özel hukukun korumalarından başka özel veya kamusal ayrımı yapmayan KVK hukukunun kurallarına gereksinim bulunmaktadır. Özellikle hiyerarşik bir ilişkinin ortaya çıktığı iş sözleşmesinde açık rızaya kuşkuyla yaklaşmak ve sözleşme ilişkisiyle ilgili olma, kanunlarda öngörülme, hukuki yükümlülüğü yerine getirme gibi diğer veri işleme şartlarını önceliklendirmek gerekmektedir.

İşçiler çalışma saatlerinde iş görme borcuna uygun davranmaları ve işverenin de işçilerden bunu bekleme hakkı bulunmaktadır. Dijital izleme uygulamaları giyilebilir teknolojiler, harekete duyarlı sistemler, ekran ve klavye takipçileri, GPS, RFID gibi çeşitli formlarda işçi hakkında veri işleme ve işverene denetim gerçekleştirme imkanı vermektedir. Tezde işverenin mülkiyet hakkı, yönetim hakkı ve gözetme borcu kapsamında dijital izleme uygulamalarıyla kişisel veri işleme ve denetim hakkı ile bu hak ve yükümlülükleri veri işleme hukuka uygunluk ölçütleri kapsamında gerçekleştirilmesini zorunlu kılan düzenlemeler incelendi. İş sözleşmesinin ortaya çıkardığı otorite/bağımlılık ilişkisi taraflarının

1409) Süzek, [2019], İş Hukuku, s. 14 vd.; Çelik/Caniklioğlu/Canbolat, [2018], İş Hukuku Dersler, s. 22.

çatışan bu haklarında sözleşmenin güçlü tarafı olan işverenin yönetim hakkını sınırlandırarak gücü adil bir dengeye kavuşturabilecek iş hukuku düzenlemeleri bulunmamaktadır. İncelendiği üzere kişilik hakkını korumayı amaçlayan özel hukuk düzenlemeleri ise özel yasal düzenleme, sözleşme ilişkisi ve hukuka uygunluk sebepleri bulunduğunda veya olay kamusal alanda kaldığında işçinin kişisel verilerini korumada yetersiz kalmaktadır.

Bilişim sistem ve uygulamaları işverene daha önce olmadığı kadar işçinin kişisel zamanına işveren tarafından müdahale etme ve bu zamanların verilerini işleme imkanı vermektedir. Üstelik bu teknolojilerin kişisel zaman ile çalışma süresi, kişisel ile profesyonel hayat arasındaki sınırı da bulanıklaştırdığı bir gerçektir. Bu durumun ortaya çıkardığı zorluk işçinin verilerinin nasıl korunacağı ve işverenin dijital izleme imkanının etkin bir biçimde neyle sınırlandırılacağıdır. KVK hukukumuzda işçi verilerinin korunmasına ilişkin özel bir düzenleme bulunmamaktadır. TBK m. 419/1 ise, işçi verilerinin işlenmesine ilişkin bir ölçüt ortaya koyarak işçi verilerini işlemeyi ancak "işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olma" koşuluna bağladığından işçilerin verilerinin korunmasında etkili bir mekanizma sunmaktadır. Öte yandan TBK m. 419/1'de KVK hukukunun diğer ilke ve veri koruma mekanizmaları (aydınlatma yükümlülüğü, aktarma, veri koruma gibi) bulunmadığından bir gerçek kişi olan işçinin verilerinin korunmasında bu fıkra, TBK m. 419/2'nin de bir gereği olarak KVKK hükümleriyle birlikte uygulanmalıdır.

Dijital izlemenin bilişim teknolojileri ve internet temelli yapısı sadece işyerindeki işçi verilerini işlemekle sınırlı kalmaz. İşçinin kişisel zamanındaki verilerini, yaşam tarzı, alışkanlıkları ve zamanını geçirdiği yerlerle ilgili de veri işleme olanağını işverene verir. İşçinin özel hayatı üzerinde bu denli ihlal edici sonuçlar ortaya çıkaran dijital izlemeyi özel hayat kavramı çerçevesinde tartışmak ve kişilik hakkı kapsamında korumaya çalışmak işçinin bu haklarına orantısız müdahaleci sonuçlar ortaya çıkarabilir. Bu itibarla işçinin kişilik hakkı veya özel hayatı tartışmalarını yapılmadan onu belirli veya belirlenebilir hale getirecek her

türlü bilgisinin korunması gerekmektedir. KVK hukukunun yaklaşımı bu noktada özel hukuk düzenlemelerinden ayrılır ve işçinin bilgilerinin işlenmesini belirli koşullara bağlar.

Öte yandan KVK hukukunun öngördüğü mekanizmalar olan aydınlatma yükümlülüğü ve açık rıza iş ilişkisinde çoğu durumda işçinin verilerini korumaktan uzaktır. Zira otorite/bağımlı çalışma ilişkisi çerçevesinde somutlaşan iş ilişkisinde işçinin özgür iradesiyle açıkladığı açık rızasının varlığından bahsetmek güçtür[1410]. Eklemek gerekir ki, KVK hukukunun öngörmüş olduğu aydınlatma yükümlülüğü unsurlarını taşıyan metinleri uzun, teknik ve çoğunlukla bu tür metinlerin yorgunu olan birey/işçi tarafından anlaşılmayan, okunmayan metinlerden oluşmaktadır[1411]. Bu sebeple işveren dijital izleme uygulaması kullanmadan önce, KVK hukukunun bu mekanizmalarına gitmeden önce veri koruma etki değerlendirmesinin yapılması, verilerin doğrudan işçiden elde edildiği yöntemlerin önceliklendirilmesi, iş görme borcunun ifası için işçiye tahsis edilmiş bilişim sistemleriyle bağlantıyı kesme hakkının tanınması, profil oluşturan dijital izleme uygulamalarından kaçınılması ve KVK hukukunun genel ilkelerinin göz önünde bulundurulması gibi süreçlerin işletilmesi işçinin verilerini etkin koruyacak, dijital izlemenin işçi üzerindeki olumsuz etkisini minimize edecektir.

Bu süreçlerin işletilmesinden sonra KVK hukukunun öngördüğü hükümlere uygun işçinin bilgilendirilmesi, diğer veri işleme şartları (KVKK m. 5/2) yoksa işçinin açık rızası alınarak kişisel veri işlenmelidir. Sürecin anılan denetimler sonrasında bu şekilde gerçekleştirilmesi işverenin dijital izleme gerçekleştirme faaliyetlerini hukuka aykırılık tartışmalarının dışına çıkaracaktır. Üstelik işveren bu sayede dijital izleme uygulama kullanma hakkını daha etkin kullanabilecektir. Aksi durumda işçinin verileri üzerinde ihlal edici sonuçlar ortaya çıkaracağından işçi kişilik hakkının korunması hükümleri ile KVK hukukunun öngördüğü şikayet,

1410) KVK Kurumu, [2019], Uygulama Rehberi, s. 49-50.
1411) Chilton/ Ben-Shahar, [2016], Privacy Disclosures, s. 41-42; Solove, [2023], Murky Consent, s. 27.

tazminat ve idari yaptırım uygulanması talebi gibi haklarını da kullanabilecektir.

İncelendiği üzere KVK hukukumuzda iş ilişkisi özelinde düzenlemelerin bulunmaması büyük bir eksikliktir. Bu eksikliğin giderilmesi için iş ilişkisinde dijital izleme öncesi veri koruma etki değerlendirmesinin zorunlu olması (GVKT m. 35 düzenlemesi), işçiye bağlantıyı kesme hakkının tanınması, verilerin doğrudan işçiden temin edileceği yöntemlerin iş ilişkisinde önceliklendirilmesi, işçinin profilini oluşturabilecek dijital izleme uygulamalarının sert koşullara bağlanarak yasaklanması hususlarında kanun koyucu tarafından yasal düzenlemelerin yapılması gereklidir. Aksi durumda sadece aydınlatma yükümlülüğü ve açık rıza ile KVK hukukunun genel ilkelerine (KVKK m. 4) uygunluk kapsamında bir hukuka uygunluk değerlendirilmesi öngörülürse bu mekanizmalar işçinin verilerini dijital izleme uygulamaları karşısında etkin korumayacaktır. Bu durum işçi işveren arasındaki çatışmayı derinleştirecek, çalışma huzurunu bozacak ve işçinin devamlı izlendiği kaygısı sebebiyle kişiliğinin baskılandığı sonuçlar ortaya çıkabilecektir.

Eklemek gerekir ki, kişisel verileri koruma denetleme makamı olan KVK Kurumu'nun iş ilişkisi özelinde gerçekleştireceği yayınlar ve denetim işverenlerin dijital izleme uygulamalarında işçinin haklarını gözetmelerinde etkili olacaktır. Ayrıca Kurum'un yayın ve denetimleri işverenlerin dijital izleme süreçlerinde şeffaf olmaları, verileri amaca uygun sınırlı ve ölçülü işlemelerini sağlayacaktır. Bu itibarla KVK Kurumu dijital izleme uygulamaları özelinde işverenlerin uyması gereken yükümlülükleri, hangi durumların dijital izlemeyi hukuka aykırı hale getireceğini iş ilişkisi özelinde somutlaştırması işçilerin verilerinin korunmasında faydalı sonuçlar verecektir.

İncelendiği üzere işverenin özellikle uzaktan çalışmalarda işçileri denetlemekte haklı menfaatleri bulunmaktadır. İşverenler bu haklarını kullanırken eşit davranma ilkesine uygun davranması, şeffaf bir yapı oluşturması, iş süreçleri, bilişim sistemleri ve dijital izleme uygulamalarıyla ilgili olarak işyeri prosedürleri oluşturması işyerinde çalışma barışının sağlanması ve işçinin devamlı izlendiği

kaygısını minimize edecek, işçileri olumsuz davranışlardan uzak tutacaktır. Ayrıca işverenler kişisel veri, dijital izleme uygulamaları, işyerinde özel hayat ve sınırları, bilişim sistemlerini kullanma kuralları hususlarında işçilere farkındalık eğitimleri vermesi işçinin dijital izlemeye ilişkin kaygılarını minimize edecek, verimini artıracaktır.

Son olarak hukuka aykırı dijital izlemede elde edilen veriler hukuken kullanılamayacağı gibi işçi bu hukuka aykırılık giderilene kadar çalışmayı durdurabilir, iş sözleşmesini kişilik hakkı ihlali sebebiyle feshedebilir veya MK m. 25 kapsamında hukuka aykırılığın tespiti, önlenmesini, hukuka aykırılığa son verilmesi ve tazminat davaları açabilir. Ayrıca işçi idareye başvurarak ihlalle ilgili işverene idari yaptırım uygulanmasını isteyebilir veya TCK kapsamında suç duyurusunda da bulunabilir. Eklemek gerekir ki, işverenin hukuka aykırı dijital izleme uygulamalarına maruz kalmış işçi adayı da yasadan ve culpa in contrahendo sorumluluğundan doğan haklarını işverene karşı kullanabilir.

KAYNAKÇA

A. Cass, Ronald, Privacy and Legal Rights, Case Western Reserve Law Review, Vol. 41, No. 3, 1991

Abraham, Martin/Niessen, Cornelia/Schnabel, Claus/Lorek, Kerstin/Grimm, Veronika/Möslein, Kathrin/Wrede, Matthias, Electronic Monitoring at Work: The Role of Attitudes, Functions, and Perceived Control For The Acceptance of Tracking Technologies, Human Resource Management Journal, C. 29, 2019

Adams, Abi, Technology and the Labour Market: The Assessment, Oxford Review of Economic Policy, Volume 34, Issue 3, Autumn, 2018

Adams-Prassl, Abigail/Rauh, Christopher/Boneva, Teodora/Golin, Marta, Working from Home:The Polarising Workplace, VoxEU.org, https://voxeu.org/article/working-home-polarising-workplace

Adams-Prassl, Jeremias, What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work, Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall, 2019

Adorno, **Theodor W.**, Kültür Endüstrisi (1944-1960), (Çev. Nihat Ülner - Mustafa Tüzel - Elçin Gen), İletişim Yayınları, 6. Baskı, İstanbul, 2011

Ajunwa, Ifeoma, Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law, Saint Louis University Law Journal, Vol. 63, No. 1, Fall, 2018

Akgül, Aydın, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, Beta Basım Yayım, İstanbul, 2014

Akın, Levent, İş Sağlığı ve Güvenliği ve Alt İşverenlik, Yetkin Yayınları, Ankara, 2013 (İş Sağlığı ve Güvenliği)

Akın, Levent, Türk Çalışma Yaşamında Pandemi Sürecinde Uzaktan/Evde Çalışma ve Olası Sonuçları, Festschrift für Otto Kaufmann Armağanı, Legal yayıncılık, İstanbul, 2021 (Uzaktan Çalışma)

Akipek, Jale G./Akıntürk, Turgut/Ateş – Karaman, Derya, Kişiler Hukuku, I. Cilt, Beta Yayınevi, İstanbul, 2012

Aksoy Retornaz, Eylem/Güçlütürk, Osman Gazi, Yapay Zekada Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler, Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması, (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, 2023

Aksoy, Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara, 2010

Aktaş, Batuhan, Özel Hayatın Gizliliğini İhlal Suçu, Der Kitabevi, İstanbul, 2017

Akyiğit, Ercan, İş Hukuku, 9. Baskı, Seçkin Yayıncılık, Ankara 2013 (İş Hukuku)

Akyiğit, Ercan, Ücreti Geciken İşçinin Çalışmaktan Kaçınması, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Sayı: 5, 2005 (Çalışmaktan Kaçınma)

Akyürek, Güçlü, Özel Hayatın Gizliliğini İhlal Suçu, Seçkin Yayıncılık, 2. Baskı, Ankara, 2014

Aliefendioğlu, Yılmaz, Anayasa Mahkemesinin İşlevsel Yönü, Amme İdaresi Dergisi, Yıl. 1986, Cilt 19, Sayı 1, 1986.

Alli, Benjamin O., Fundamental Principles of Occupational Health and Safety, International Labour Office, Second Edition, Geneva, ILO, 2008

Aloisi Antonio/Gramano, Elena, Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context, Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall, 2019

Alp, Mustafa, Tele Çalışma (Uzaktan Çalışma), (Ed: Süleyman Başterzi), Prof. Dr. Sarper. Süzek'e Armağan, Beta Yayıncılık, C. I, İstanbul, 2011

Alp, Mustafa/Doğan, Sevil, Giyilebilir Teknolojiler ve İş İlişkisine Etkileri", Çalışma ve Toplum, 2021/4, 2021

Alp, Mustafa/Gürsel, İlke, Covid-19 Pandemisinde İşçilere Ait Sağlık Verilerinin İşlenmesi, Sicil İş Hukuku Dergisi, S. 44, 2020

Alpagut, Gülevil, 6331 Sayılı İş Sağlığı ve Güvenliği Kanununun Genel Esasları, İÜHFM, C.LXXII, S. 2, 2014 (İş Sağlığı ve Güvenliği)

Alpagut, Gülsevil, İşçinin Sadakat Borcu ve Türk Borçlar Kanunu ile Getirilen Düzenlemeler, Sicil İş Hukuku Dergisi, 25, Mart, 2012 (Sadakat Borcu)

Alpagut, Gülsevil, Dijitalleşen Çalışma Yaşamında İş Sözleşmesinin Unsurları, Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı, On İki Levha Yayıcılık, (Ed., Kübra Doğan Yenisey / Seda Emrağ Ergüneş), İsanbul, 2021 (Dijitalleşen Çalışma)

Alpagut, Gülsevil, İş Sağlığı ve Güvenliği Yasa Tasarısında İşverenlerin Yükümlülükleri ve Risk Değerlendirmesi, İşveren Dergisi, C. 50, S. 3, Ankara, Mayıs-Haziran, 2012 (Risk Değerlendirmesi)

Alpagut, Gülsevil, İş Sözleşmesinin Şartlarında Değişiklik ve Yargıtay'ın Konuya İlişkin Bir Kararının Düşündürdükleri, Çimento İşveren, C. 18, S. 5, Eylül, 2004 (Şartlarda Değişiklik)

Alpagut, Gülsevil, İşyerinde Kamera Gözetlemesi ve AİHM Kararları ile Tespit Edilen Esaslar, Savaş Taşkent'e Armağan, Ed. Kübra Doğan Yenisey, On İki Levha Yayıncılık, 2019 (Kamera Gözetlemesi)

Altıntepe, Ayşen, Türk İş Hukukunda İşverenin Yönetim Hakkı, İstanbul 2014

Amatuzzo, Allison, Wherever We Go, We Leave a Trail: Surveillance and Sousveillance in the United States and United Kingdom", Penn State Journal of Law and International Affairs, Vol. 7, Issue 2, 2019

Antalya, Osman Gökhan/Topuz, Murat, Medeni Hukuk, C.1, 3. Baskı, Seçkin Yayıncılık, Ankara, 2019

Araslı, Oya, Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi, Ankara, 1979, (Yayınlanmamış Doçentlik Tezi)

Archard, David, The Value of Privacy, Privacy and the Criminal Law, Antwerpen-Oxford, 2006

Arıkan, Engin, Kelsen'in Saf Hukuk Kuramı ve Ötesi", YUHFD Cilt. XVII No.2, 2020

Arpacı, Abdülkadir, Kişiler Hukuku, Gerçek Kişiler, Beta Yayınevi, 2. Baskı, İstanbul, 2000

Arrison, Rachel, You're Wearing That: Why Data Generated from Wearable Technology Should Be Protected under Privacy, Law Sports Lawyers Journal, 26,

2019

Arslan Durmuş, Seda, İşçinin Özel Yaşamının İş İlişkisine Etkisi, DÜHFD, C. 25, S. 42, 2020

Arslan Ertürk, Arzu, İş Hukuku Boyutuyla Türkiye'de Psikolojik Taciz (Mobbing) ve Dünyadan Örnekler", MÜHFD, C. 20, S. 1, 2014

Arslan Öncü, Gülay, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması, Beta Yayınları, İstanbul, 2011

Arslan Öncü, Gülay, Özel Yaşama ve Aile Yaşamına Saygı Hakkı, Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-8, Avrupa Konseyi Ankara Program Ofisi, 2019

Arslan, Gülay, Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı, Beta Yayınları, İstanbul 2011

Arslan, Ramazan/Ergün, Havanur, John Hicks'e Göre Tarım Merkantilizminden Sanayi Devrimine Emeğin Evrimi, Hak İş Uluslararası Emek ve Toplum Dergisi, C. 1 S. 1, Ankara, 2012

Arslan, Seda, İş Sağlığı ve Güvenliği Kanunu'na Göre İşverenin Genel Yükümlülükleri, Prof. Dr. Ali Rıza Okur'a Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 20, S. 1, 2014 (Genel Yükümlülükler)

Arslan, Seda, İşverenin Haklı Nedenle Fesih Hakkı, On İki Levha Yayıncılık, İstanbul, 2012 (Fesih Hakkı)

Artuk, M. Emin/Gökçen, Ahmet/Alşahin, M. Emin/Çakır, Ü. Kerim, Ceza Hukuku Özel Hükümler, Adalet Yayınevi, 17. Baskı, Ankara, 2018

Asta, Timothy A., Guardians of the Galaxy of Personal Data: Assessing the Threat of Big Data and Examining Potential Corporate and Governmental Solutions, Florida State University Law Review, Vol. 45, No. 1, Fall, 2017

Aşıkoğlu, Şehriban İpek, Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-, Kişisel Verilerin Korunması Dergisi, C. 1, S. 2, 2019

Atamer, Yeşim M., Sözleşme Özgürlüğünün Sınırlandırılması Sorunu Çerçevesinde Genel İşlem Şartlarının Denetlenmesi, Beta Yayınevi, 2001

Attila Özer, Gerekçeli ve 1961 Anayasası İle Mukayeseli 1982 Anayasası, Ankara, Kamu-İş Yay., 1996

Avogaro, Matteo, Right to Disconnect: French and Italian Proposals for a Global Issue", Law Journal of Social and Labor Relations, Vol. 4, No. 3, September/December, 2018

Aybay, Aydın/Aybay, Rona, Hukuka Giriş, İstanbul Bilgi Üniversitesi Yayınları, 4. Baskı, İstanbul, 2007

Aybay, Rona, Açıklamalı İnsan Hakları Evrensel Bildirgesi, Türkiye Barolar Birliği Yayını, Ankara, 2006 (Evrensel Bildirge)

Aybay, Rona, İnsan Hakları Hukuku, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2015 (İnsan Hakları)

Aydın, Ufuk, İş Hukukunda İşçinin Kişilik Hakları, Anadolu Üniversitesi Yayınları, Eskişehir, 2022

Aydınlı, İbrahim, İşverenin İşyerinde "Çalışan" İşçilerin İş Görmekten Kaçınma Hakkı", Çimento İşveren Dergisi, Cilt: 19, Sayı: 4, Temmuz, 2005

Aytekin, Ataay, Medeni Hukukun Genel Teorisi, 3. Baskı, İstanbul, Fakülteler Matbaası, 1980

Bachnakova Rozenfeldova, Laura/Dobrovicova, Gabriela, The Analysis of the Application of Personal Data Protection Norms by Collaborative Platforms, EU and Comparative Law Issues and Challenges Series, Vol. 6, [2022

Bak, Basak, Reviving a European Idea: Author's Right of Withdrawal and the Right to Be Forgotten under the EU's General Data Protection Regulation (GDPR), SCRIPTed: A Journal of Law, Technology and Society, Vol. 19, No. 1, February, 2022

Bakırcı, Kadriye, İş Hukuku Açısından İşyerinde Cinsel Taciz, İstanbul, Yasa Yayıncılık, 2000

Balboni, Paolo/Taborda, Martim Barata/Botsi, Anastasia/Francis, Kate, Accountability and Enforcement Aspects of the EU General Data Protection Regulation - Methodology for the Creation of an Effective Compliance Framework and a Review of Recent Case Law, Indian Journal of Law and Technology, Vol. 15, Issue 1, 2019

Balkır, Z. Gönül, İş Sağlığı ve Güvenliği Hakkının Korunması: İşverenin İş Sağlığı ve Güvenliği Organizasyonu, Sosyal Güvenlik Dergisi, C. 2, S. 1, Ocak, 2012 (İş Sağlığı)

Balkır, Z. Gönül, İşverenin Yönetim Hakkının Kullanılması ve Etik Sınırları", Sicil İHD, S. 12, İstanbul, 2008 (Yönetim Hakkı)

Ball, Kirstie, Electronic Monitoring and Surveillance in the Workplace. Literature review and policy recommendations, Publications Office of the European Union, Luxembourg, 2021

Bamberger, Kenneth A./Mulligan, Deirdre K., Privacy in Europe: Initial Data on Governance Choices and Corporate Practices, The George Washıngton Law Revıew, Vol. 81, No. 5, September, 2013

Barak, Aharon, Proportionality: Constitutional Rights and Their Limitations, Cambridge University Press, 2012

Başalp, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004

Başbuğ, Aydın, İşverenin Yönetim Hakkı ve Çalışma Şartlarında Değişiklik, Ankara, 2008

Başlar, Kemal, Türk Mahkeme Kararlarında Avrupa İnsan Hakları Sözleşmesi, Ankara, Avrupa Konseyi Türkiye Temsilciliği Yayını, 2008

Başterzi, Süleyman, Avukatla Bağıtlanan Sözleşmenin Hukuki Niteliği İş Sözleşmesinin Vekâlet ve Diğer İş Görme Sözleşmelerinden Ayrılması, MESS Sicil İş Hukuku Dergisi, Mart, 2010 (İş Görme Sözleşmeleri)

Başterzi, Süleyman, İş İlişkisinin Kurulması, Hükümleri ve İşin Düzenlenmesi Açısından Yargıtay'ın 2009 Yılı Kararlarının Değerlendirilmesi, İş Hukuku ve Sosyal Güvenlik Hukuku Derneği (Türk Milli Komitesi), Yargıtay'ın İş Hukuku ve Sosyal Güvenlik Hukuku Kararlarının Değerlendirilmesi 2009, Kamu İş Yayını, Ankara, 2011(Değerlendirme)

Battcock, Rupert, Data Protection: Where Next, International Journal of Law and Information Technology, Vol. 3, No. 2, 1995

Bauman, Zygmunt, Akışkan Modern Dünyadan 44 Mektup, (Çev. Pelin Siral), Habitus Yayıncılık, İstanbul, 2012 (Modern Dünya)

Bauman, Zygmunt/Lyon, David, Akışkan Gözetim (Çev. Elçin Yılmaz), 2. Basım, İstanbul, 2016 (Akışkan Gözetim)

Baycık, Gaye, Çalışanların İş Sağlığı ve Güvenliğine İlişkin Haklarında Yeni Düzenlemeler, Ankara Barosu Dergisi, 2013/3, 2013 (İş Sağlığı)

Baycık, Gaye, İş Hukukunda Yenilik Doğuran Haklar, Ankara Üniversitesi, Doktora Tezi, 2011 (Yenilik Doğuran Haklar)

Baycık, Gaye, İş ve Sosyal Güvenlik Hukuku Açısından Maden İşçileri, Yetkin Yayınları, 2006 (Maden İşçileri)

Baycık, Gaye/Doğan Sevil/Dulay Yangın, Dilek/Yay Oğuzhan, Covid 19 Pandemisinde Uzaktan Çalışma: Tespit ve Öneriler, Çalışma ve Toplum, 2021/3, 2021

Bayram, Fuat, Borçlar Kanunu Tasarısı Işığında İşverenin İşçinin Kişiliğini Koruma Borcu, İş Hukuku ve Sosyal Güvenlik Komitesi, 30. Yıl Armağanı, Ankara, 2016 (Fesih Hakkı)

Bayram, Fuat, İşverenin Fesih Hakkı Açısından İşçinin İşyerinde Özel Amaçlarla İnternet Kullanımı (Sanal Kaytarma – Cyberloafing), Prof. Dr. Ali Rıza Okur'a Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Özel Sayı, C. 20, S. 1, 2014 (İnternet Kullanımı)

Baysal, Ulaş, İş Hukukunda Kişisel Verilerin İşlenmesi, Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması, (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, 2023 (Kişisel Verilerin İşlenmesi)

Baysal, Ulaş, İşçiye Ait Taşınabilir İletişim Cihazlarının İş Amaçlı Kullanılması",

Sicil İş Hukuku, S. 40, 2018 (İletişim Cihazları)

Baysal, Ulaş, Şüphe Feshi Kavramı ve Şüphe Feshine İlişkin Yargıtay Kararlarının Değerlendirilmesi", Sicil İş Hukuku Dergisi, 2016/35, 2016 (Şüphe Feshi)

Beck, Adrian/Willis Andrew, Customer and Staff Perceptions of The Role of Closed Circuit Television in Retail Security, Crime At Work, (M. Gill, ed.), Macmillan Publishers Limited, 2005

Belling, Detlev W./İnce, Nurten, Türk-Alman Hukukunda Temel Hakların Özel Hukuk İlişkilerine Etkisi, Legal Hukuk Dergisi, C.12, S. 137, 2014

Beniger, James R., The Control Revolution Technological and Economic Origins of the Information Society, Harvard University Press, 1986

Bennett, Colin J., Regulating Privacy, Data Protection and Public Policy in Europe and the United States, Cornell University Press, 1992

Bennett, Colin J./Raab, Charles D., The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, 2013

Bentham, Jeremy, Panoptikon ya da Gözetim-Evi, XVIII. Mektup - Fabrikalar, (Ed. Barış Çoban/Zeynep Özarslan), Panoptikon: Gözün İktidarı, Su Yayınları 2. Baskı, İstanbul, 2016

Berber, Leyla Keser/Atabey, Ayça/Mert, Melis, E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler, Kişisel Verileri Koruma Dergisi, 2019

Berg ,Janine, Protecting Workers in the Digital Age: Technology, Outsourcing, and the Growing Precariousness of Work, Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall 2019

BeVier, Lillian R., Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection, William & Mary Bill of Rights Journal, Vol. 4, No. 2, Winter, 1995

Beydoğan, T. Ayhan, Mahremiyet Hakkı (Özel Hayatın Gizliliği ve Korunması) Basın Hürriyetine Karşı: İngiltere Örneği, DüGünen Siyaset, S. 10, Kasım, 1999

Beysan, Nazime, Hak Kavramının Hukuk Felsefesi Açısından Analizi, XII Levha Yayıncılık, 2015

Beytar, Erbil, İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması. On İki Levha Yayınları, İstanbul, 2018

Bilge, Selahattin Samet, Mobbing Terimi ve Türk Hukuk Düzeninde İncelenmesi, Ankara Üniversitesi Hukuk Fakültesi Dergisi, S. 65, C. 4, 2016

Birben, Erhan, İşçinin Özel Yaşamı Nedeniyle İş Sözleşmesinin Feshi, İş Hukukunda Genç Yaklaşımlar II, İstanbul, On İki Levha Yayıncılık, 2016 (Özel Yaşam)

Birben, Erhan, Yargı Kararları Işığında Toplu Eylem Hakkı Bakımından Ölçülülük Denetimi, İş Hukukunda Yeni Yaklaşımlar II, (Ed. Kübra Doğan Yenisey/Seda Ergüneş Emrağ), Beta Yayınevi, İstanbul, 2018

Blok, Peter, Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en het Amerikaanse recht, Boom Juridische Uitgevers, 2002

Bloustein, Edward J., Priacy As an Aspect of Human Dignity, Edited by, Ferdinand David Schoeman, Cambridge University Press, Second Edition, Cambridge, 2007

Blume, Peter E., Data Protection and Privacy – Basic Concepts in a Changing World, Scandinavian Studies in Law, Vol. 56, Stockholm: Jure Law Books, 2010

Blumenfeld, Stephen/Anderson, Gordon/Hooper, Val, Covid-19 and Employee Surveillance, New Zealand Journal of Employment Relations, Vol. 45, No. 2, 2020

Boehmer, Robert G., Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise form the Modern Sweatshop", DePaul Law Review, Vol. 41, Issue 3, 1992

Bostwick, Gary L., A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision, California Law Review, Vol. 64, No. 6, December, 1976

Botan, Carl, Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects", Communication Monographs, S. 63, C. 4, 1996

Bottomley, Emlyn, Data and Algorithms in the Workplace: An Overview of Current Public Policy Strategies, Center for Labor Research and Education University of California, Berkeley, Working Paper, Technology and Work Program, 2020

Bowie, Norman E./Duska, Ronald F., Business Ethics, Englewood Cliffs, N. J Prentice Hall, 1990

Bozkurt Gümrükçüoğlu, Yeliz, İş İlişkisinde İşçinin Kişisel Verilerinin Korunmasına İlişkin Sorunlar ve Kişisel Verilerin Korunması Kanunu, İş Hukukunda Yeni Yaklaşımlar (Ed. Kübra Doğan Yenisey, Seda Ergüneş Emrağ), İstanbul: Beta, 2017 (İşçinin Kişisel Verileri)

Bozkurt Gümrükçüoğlu, Yeliz, İşçinin Sosyal Medya Kullanımının İş Hukukundaki Etkileri, PressAcademia Procedia, V.7, 2018 (Sosyal Medya)

Bozlak, Ayhan, Avrupa İnsan Hakları Kararları Çerçevesinde Türk Ceza Hukukunda Özel Hayatın Korunması, Adalet Yayınevi, Ankara, 2013

Brookman, Justin, Protecting Privacy in an Era of Weakening Regulation, Harvard Law & Policy Review, Vol. 9, No. 2, Summer, 2015

Bruyer, Richard A., Privacy: A Review and Critique of the Literature, Alberta Law Review, Vol. 43, No. 3, 2006

Bueckert, Melanie R., A Critical Review of the Law Regarding Electronic Employee Monitoring in Non-Unionized Workplaces in Canada, Master of Laws, Faculty of Law University of Manitoba Winnipeg, 2008

Buitelaar, Jan C., Privacy: Back to the Roots", German Law Journal, Vol. 13, No: 3, 2019

Burke, Peter, Bilginin Toplumsal Tarihi, Tarih Vakfı Yurt Yayınları, (Çev. Mete Tunçay), İstanbul, 2001

Burkert, Herbert, Institutions of Data Protection - An Attempt at a Functional Explanation of European National Data Protection Laws, Computer/Law Journal, Vol. 3, Issue 1, 1981

Bygrave, Lee A., Data Protection Law, Approaching Its Rationale, Logic and Limits, Kluwer Law International, Holland, 2002 (Data Protection)

Bygrave, Lee A., The Place of Privacy in Data Protection Law, University of New South Wales Law Journal, Vol. 24, No. 1, April, 2001(Privacy)

Cabrelli, David/Zahn Rebecca, Theories of Domination and Labour Law: An Alternative Conception for Intervention? International Journal of Comparative

Labour Law and Industrial Relations, Vol. 33, Issue 3, 2017

Caniklioğlu Dikmen, Meltem, Anlamı, Kapsamı ve Sınırlarıyla Temel Haklar ve Anayasalarımız, Mahmut Tevfik Birsel'e Armağan, DEÜHFY, İzmir, 2001

Caniklioğlu, Nurşen, 6331 Sayılı İş Sağlığı ve Güvenliği Kanununda Öngörülen İşveren Yükümlülükleri, Türkiye Toprak, Seramik, Çimento ve Cam Sanayii İşverenleri Sendikası Çalışma Mevzuatı Seminer Notları, Antalya, 26-30 Eylül 2012 (İş Sağlığı)

Caniklioğlu, Nurşen, Kişisel Verilerin Korunması Açısından İşçilerin Hakları, Prof. Dr. Turhan Esener III. İş Hukuku Uluslararası Kongresi, Nisan, 2018 (Kişisel Veriler)

Carrillo David A., California Constitutional Law: Privacy, San Diego Law Review, Vol. 59, No. 1, February-March, 2022

Cefaliello, Aude/Moore, Phoebe V./Donoghue, Robert, Making Algorithmic Management Safe and Healthy for Workers: Addressing Psychosocial Risks In New Legal Provisions. European Labour Law Journal, Vol. 14, No. 2, 2023

Centel, Tankut, Hukuki Boyutlarıyla Mobbing, Çalışma Hayatında Psikolojik Taciz (Mobbing) Paneli Çalıştayı Bildiriler Kitabı, Yayınlanmış Tebliğ, Ankara, 2013 (Mobbing)

Centel, Tankut, Türk Borçlar Kanunu'nda Genel Olarak İşçinin Kişiliğinin Korunması, Sicil İş Hukuku Dergisi, S. 24, 2011 (Kişiliğin Korunması)

Chilton, Adam S./Ben-Shahar Omri, Simplification of Privacy Disclosures: An Experimental Test, Coase Sandor Working Paper Series in Law and Economics No. 737, 2016

Ciocchetti, Corey A., Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy", Duke Law & Technology Review, Vol.26, Issue 1, 2001

Civan, Orhan Ersun, Genel İş Koşulları, Beta Yayınları, İstanbul, 2015 (İş Koşulları)

Civan, Orhan Ersun, Genel İş Koşullarında Değişiklik Kayıtlarının Geçerliliği ve Denetimi, Prof. Dr. Turhan Esener'e Armağan, C. 1, Ankara, 2016 (Değişiklik Kayıtları)

Civan, Orhan Ersun, İş Hukukunda Uzaktan Çalışma (Evden Çalışma / Tele Çalışma), Legal İş ve Sosyal Güvenlik Hukuku Dergisi, S. 26, Temmuz, 2010 (Uzaktan Çalışma)

Clarke, Roger, Beyond the OECD Guidelines: Privacy Protection for the 21st Century, 2000, http://www.rogerclarke.com/DV/PP21C.html (Beyond the OECD)

Clarke, Roger, Privacy Protection for the 21st Century, http://www.rogerclarke.com/DV/PP21C.html (Privacy)

Clarke, Roger, Profiling: A Hidden Challenge to the Regulation of Data Surveillance, Journal of Law and Information Science, Vol. 4, No. 2, 1993 (Profiling)

Collins, Val, Privacy in the United Kingdom: A Right Conferred by Europe, International Journal of Law and Information Technology, Vol. 1, No. 3, Spring, 1994

Crayden, Andrew, A Modern-Day Gold-Rush: Applying Property Principles to Data Using Mineral Rights Concepts and the Rule of Capture, Vol 81, Issue 3, Louisiana Law Review, 2021

Cristolovean, Nicoleta Maria, Reflections on Personal Data Processing That Is Necessary for the Entering or Performance of a Contract, Jus et Civitas: A Journal of Social and Legal Studies, Vol. 8, No. 2, 2021

Cuijpers, Colette, A Private Law Approach to Privacy; Mandatory Law Obliged, SCRIPTed: A Journal of Law, Technology and Society, Vol. 4, No. 4, September, 2007

Çeçen, Anıl, Hukukta Norm ve Adalet, Ankara Üniversitesi Hukuk Fakültesi Dergisi S.32, 1975

Çekin, M. Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, On İki Levha Yayıncılık, İstanbul, 2020

Çelik, Aziz, Avrupa Sosyal Şartı ve Türkiye'nin Çekinceleri, Türk-İş Dergisi, S. 366, Mayıs-Haziran, 2005

Çelik, Nuri/Caniklioğlu, Nurşen/Canbolat, Talat, İş Hukuku Dersleri, Beta Yayınevi, 31. Baskı, İstanbul, 2018 (İş Hukuku Dersleri)

Çetin, Evra, İnsan Hakları Avrupa Sözleşmesi'nin 8-11. Maddeleri Bağlamında Çalışanların Hakları, İstanbul, 2015

Çetin, Muharrem/Asıl, Sermin, Günümüz Toplumunda Gözetim Olgusu, Üçüncü Sektör Sosyal Ekonomi, S. 52, C.1, 2017

Çiçekli, Bülent, Avrupa Sosyal Şartı-Temel Rehber, Seçkin Yayıncılık, Ankara, 2001

Davies, Paul/Freedland, Mark, (Edited by), Kahn-Freund's Labour and the Law, Third Edition, Stevens&Sons, London, 1983

De Stefano, Valerio/Stylogiannis, Charalampos/Wouters, Mathias/Durri, Ilda, System Needs Update: Upgrading Protection Against Cyberbullying And ICT-Enabled Violence And Harassment in The World Of Work, ILO Working Papers, 2020

Delbar, Catherine/Mormont, Marinette/Schots, Marie, New Technology and Respect for Privacy at the Workplace, Institut des Sciences du Travail, 2003

Demir, Fevzi, En Son Yargıtay Kararları Işığında İş Hukuku ve Uygulaması, Albi Yayıncılık, 11. Baskı, 2018

Demirkaya, Seher/Güler, Ceyhun, Çalışma Yaşamında İşçinin Kişilik Haklarının Korunması Bağlamında ILO'nun 190 sayılı Şiddet ve Taciz Sözleşmesinin değerlendirilmesi, Çalışma ve Toplum, 2021/4, 2021

Determann, Lothar/Sprague, Robert, Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States, Berkeley Technology Law Journal, Vol. 26, No. 2, Spring, 2011

Develioğlu, Murat, Avrupa Birliği Genel Veri Koruma Tüzüğü, On İki Levha Yayınları, İstanbul, 2017

Diffie, Whitfield/Landau, Susan, Privacy on the Line, The Politics of Wiretapping and Encryption, USA, MIT Press, 2007

Doğan Yenisey, Kübra Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri, Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı, On İki Levha Yayıcılık, (Ed. Kübra Doğan Yenisey/Seda Emrağ

Ergüneş), İsanbul, 2021 (Teknolojik Gelişmeler)

Doğan Yenisey, Kübra, Endüstri 4.0, Üretimin Değişen Yapısı ve İş Hukuku, Toprak İşveren Sendikası, 2019, S. 120, s. 1 vd. https://toprakisveren.org.tr/index.php/yayinlar/endustri-4-0-uretimin-degisen-yapisi-ve-is-hukuku/ (Erişim Tarihi: 16.06.2022), (Endüstri 4.0)

Doğan Yenisey, Kübra, Eşit Davranma İlkesinin Uygulamasında Metodoloji ve Orantılılık İlkesi, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, S. 7, 2005 (Eşit Davranma İlkesi)

Doğan Yenisey, Kübra, İş Hukukunda İşyeri ve İşletme, Alman ve Fransız Hukuklarıyla Karşılaştırmalı Bir İnceleme, Legal Yayıncılık, İstanbul, 2007 (İşyeri ve İşletme)

Doğan Yenisey, Kübra, İş Hukukunun Emredici Yapısı, Beta, İstanbul, 2014 (Emredici Yapı)

Doğan Yenisey, Kübra, İş İlişkisinin Kurulması, Hükümleri ve İşin Düzenlenmesi, Yargıtay'ın 2013 Yılı İş Hukuku ve Sosyal Güvenlik Hukuku Kararlarının Değerlendirilmesi Semineri, XII Levha Yayıncılık, 2017 (Değerlendirme)

Doğan Yenisey, Kübra, İş Kanununda Eşitlik İlkesi ve Ayrımcılık Yasağı, Çalışma ve Toplum, 2006/4, 2006 (Ayrımcılık Yasağı)

Doğan Yenisey, Kübra, Şüphe Feshi, Sicil İş Hukuku Dergisi, Eylül 2008 (Şüphe Feshi)

Doğan Yenisey, Kübra, Türk Borçlar Kanunu'nun Genel Hizmet Sözleşmesine İlişin Hükümleri ve İş Hukuku Açısından Önemi, İş Hukuku ve Sosyal Güvenlik

Hukuku Akademik Forumu, Legal Yayıncılık, 2014 (Genel Hizmet Sözleşmesi)

Doğan Yenisey, Kübra, Yargıtay'ın İş Hukuku ve Sosyal Güvenlik Hukuku Kararlarının Değerlendirilmesi 2016, On İki Levha Yayıncılık, Ankara 01-02 Aralık, 2017 (Değerlendirme)

Doğan, Sevil, İş Sözleşmesinde Bağımlılık Unsuru, İzmir, 2016

Dolgun, Uğur, Şeffaf Hapishane Yahut Gözetim Toplumu, Ötüken Yayınları, İstanbul, 2008

Dosi, Giovanni/Virgillito, Maria Enrica, Whither the Evolution of the Contemporary Social Fabric: New Technologies and Old Socio-Economic Trends, International Labour Review, Vol. 158, No. 4, December, 2019

Downey, Michael, Legal Ethics and Geofencing, Litigation" Vol. 45, No. 4, Summer, 2019

Dulay Yangın, Dilek, Avrupa İnsan Hakları Mahkemesi Büyük Daire'nin İşçilerin Gizli Kamera ile İzlenmesine İlişkin 17 Ekim 2019 Taraihli Lopez Ribalda ve Diğerleri Kararı'nın Değerlendirilmesi, Çalışma ve Toplum, 2020/3, 2020

Dumitru, Maria, Is There a Right of Option between the Processing of Personal Data Legal Bases Regarding General Data Protection Regulation 2016/679?, European Journal of Law and Public Administration, Vol. 6, No. 2, 2019

Dumortier, Jos, Evaluation and Review of the ePrivacy Directive, European Data Protection Law Review (EDPL), Vol. 2, No. 2, 2016

Dural, Mustafa/Öğüz, Tufan, Kişiler Hukuku, Filiz Kitabevi, 23. Baskı, İstanbul, 2022

Dural, Mustafa/Sarı, Suat, Türk Özel Hukuku, C.1, 14. Baskı, Filiz Kitabevi, İstanbul, 2019

Dursun Ateş, Sevgi, İşverenin Yönetim Hakkı, Seçkin Yayınları, Ankara, Mart 2019

Dutertre, Gilles, Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler, Avrupa Konseyi Yayınları, 2003

Duwell, F. Josef/Brınk, Stefan, Die EU Datenschutz-Grundverordnung und der Beschäftigtendatenschutz, Neue Zeitschrift für Arbeitsrecht, s. 666; Aktaran, Atila Erkal, Avrupa Genel Veri Koruma Düzenlemesi Bağlamında Memurların Kişisel Verilerinin Korunması Hakkı, Anayasa Yargısı, Cilt: 37, Sayı: 2, 2020

Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, 6. Baskı, Seçkin Yayıncılık, Eylül, 2015 (Bilişim Suçları)

Dülger, Murat Volkan, İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, S. 5, 2018 (Temel Hak ve Özgürlükler)

Dülger, Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi Yayınları, 3. Baskı, İstanbul, 2019 (Kişisel Veriler)

Ekmekçi, Ömer, Türk Borçlar Kanunu Tasarısının Genel Hizmet Sözleşmesine İlişkin Hükümleri Üzerine, Mercek, Temmuz 2005

Ekmekçi, Ömer/Gemalmaz, H. Burak/Aslan, Volkan/Yılmaz, H. Hilal, Anayasa Mahkemesine Bireysel Başvurunun Temel Esasları ve İş ve Sosyal Güvenlik Hukukuna İlişkin Kararlar; On İki Levha Yayıncılık, İstanbul, 2022

Ekmekçi, Ömer/Yiğit, **Esra**, Bireysel İş Hukuku, On İki Levha Yayıncılık, 4. Baskı, İstanbul, 2022

Ekonomi, Münir, İş Hukuku, C. I, Ferdi İş Hukuku, Üçüncü Bası, İstanbul, 1987 (Ferdi İş Hukuku)

Elbir, Nazlı, Kişiliğin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması, Doktora Tezi, Ankara, 2020

Ella, V. John, Employee Monitoring and Workplace Privacy Law, National Symposium on Technology in Labor & Employment Law, Washington, D.C., April 6, 7, and 8, 2016

Elliott, David/Soifer, Eldon, Privacy and Intimacy, Journal of Value Inquiry, Vol. 44, No. 4, December, 2010

Engin, E. Murat, Türk İş ve Sosyal Güvenlik Hukukunda İşveren, Banka Sigorta İşçileri Sendikası, 1993 (İşveren)

Engin, E. Murat, Yeni İş Kanunu Tasarısı ve İşçinin İş Görmekten Kaçınma Hakkı, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 5, S. 1, 2003 (İş Görmekten Kaçınma)

Engin, Murat E., Türk İş Hukukunda Evde Çalışma, Prof. Dr. Turhan Esener'e Armağan, Ankara, 2000 (Evde Çalışma)

Enqvist, Lena/Litins'ka, Yana, Employee Health Data in European Law: Privacy Is (Not) an Option?, Nordic Journal of European Law, 5(1), 2022 https://www.diva-portal.org/smash/get/diva2:1692131/FULLTEXT02.pdf

Entrikin, J. Lyn, The Right to Be Let Alone: The Kansas Right of Privacy, 53 Washburn L.J., 2012

Erdemir, M. Aymelek, İşverenin Yönetim Hakkı ve Sınırları, Seçkin, Ankara, Mayıs, 2015

Eren, Fikret, Borçlar Hukuku Genel Hükümler, Yetkin Yayınları, 24. Baskı, Ankara 2019

Ergin, Hediye, İşçinin İşyerinde Çalışan Diğer Bir İşçiye Sataşması Nedeniyle İş Sözleşmesinin İşveren Tarafından Feshi, Sicil İş Hukuku Dergisi, S. 34, 2015

Ergüneş Emrağ, Seda, 4857 Sayılı İş Kanununun Değişik 14. Maddesi Işığında Tele Çalışma, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, C. 13, S. 51, 2016

Erkanlı Başbüyük, Betül, İş Görmekten Kaçınma Sebebi Olarak İşyerinde Cinsel Taciz, İSGHD, C. 16, S. 61, 2019 (Cinsel Taciz)

Erkanlı Başbüyük, Betül, İşçinin İş Görmekten Kaçınma Hakkı, Seçkin Yayıncılık, Ankara, 2020 (İş Görmekten Kaçınma)

Ertürk, Şükran, İş İlişkisinde Temel Haklar, Seçkin Yayıncılık, Ankara, 2002

Eyrenci, Öner/Taşkent, Savaş/Ulucan, Devrim, Bireysel İş Hukuku, 7. Baskı, İstanbul, 2020

Fairclough, Bradyn, Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It, Journal of Corporation Law, Vol. 42, No. 2, Winter, 2016

Finkin, Matthew W., Privacy: Its Constitution and Vicissitudes - A Half-Century on, Canadian Labour and Employment Law Journal, Vol. 18, No. 2, 2015

Flanagan, Julie A., Restricting Electronic Monitoring in the Private Workplace, Duke Law Journal, Vol. 43, No. 6, April, 1994

Foucault, Michel, Hapishanenin Doğuşu, Çev. Mehmet Ali Kılıçbay, İmge Kitabevi, 1992

Foucault, Michel, İktidarın Gözü, Seçme Yazılar, (Çev. Mehmet Ali Kılıçbay), Yapı Kredi Yayınevi, İstanbul, 2007

Fried, Charles, Privacy [A moral analysis], Philosophical Dimensions of Privacy: An Anthology, Edited by: Ferdinand David Schoeman, Cambridge University Press, Second Edition, 2007

Fritsch, Clara, Reforming European Data Protection Law, (Serge Gutwirth / Ronald Leenes / Paul de Hert - Editors), Springer, 2015

Fulda, Joseph S., Data Mining and Privacy, Albany Law Journal of Science & Technology, Vol. 11, No. 1, 2000

Gaba, John Paul M./Estremadura, Joan Janneth M., Data Protection of Biometric Data and Genetic Data, Ateneo Law Journal, Vol. 64, No. 3, February, 2020

Galic, Maša/Tjerk, Timan/Koops, Bert-Jaap, Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation, Philosophy & Technology, Vol. 30, Issue 1, 2016

Garrie, Daniel B./Wong, Rebecca, Spyware Technologies: Limiting the Horizons

of Digital Privacy, Thomas M. Cooley Law Review, Vol. 23, No. 3, 2006

Gay, Darrell S./Kagan, Abigail M., Big Data and Employment Law: What Employers and Their Legal Counsel Need to Know, ABA Journal of Labor and Employment Law, Vol. 33, No. 2, Winter, 2018

Gellert, Raphael, The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment, European Data Protection Law Review (EDPL), Vol. 3, No. 2, 2017

Gellman, Robert, Fair Information Practices: A Basic History, Version 2.22, April 6, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020

Gemalmaz, H. Burak, Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır?: AİHM Büyük Dairenin 05 Eylül 2017 Tarihli Barbulescu Kararı, https://blog.lexpera.com.tr, 2017

Gemalmaz, Mehmet Semih, Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriş, 6. Baskı, Legal, 2007

Gerhart, Paul F., Employee Privacy Rights: Introduction and Overview, Comparative Labor Law Journal, Vol. 17, Issue 1, Fall, 1995

Gerstein, Robert S., Intimacy and Privacy, Edited by, Ferdinand David Schoeman, Cambridge University Press, Second Edition, Cambridge, 2007

Giddens, Anthony, Ulus – Devlet ve Şiddet, (Çev. Cumhur Atay), Kalkedon Yayınları, İstanbul 2008

Giritlioğlu, Necla, Dürüstlük Kuralları, Hakkın Kötüye Kullanılması Yasağı, Özellikle Şekil Eksikliğinden Dolayı Geçersizliğin Hakkın Kötüye Kullanılması Yasağı ile Sınırlandırılması, İstanbul, 1989

Glancy, Dorothy J., Privacy and the Other Miss M, Northern Illinois University Law Review, Vol. 10, No. 3, Summer, 1990, s. 401-490. http://law.scu.edu/wp-content/uploads/miss_m.pdf

Göçmen Uyarer, Sinem, 6698 Kişisel Verilerin Korunması Kanunu ve 5237 Sayılı Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Galatasaray Üniversitesi SBE Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, 2019

Göktaş, Seracettin, Türk İş Hukukunda İşçinin Çalışmaktan Kaçınma Hakkı, Yetkin Yayınları, Ankara, 2008

Gören, Zafer, Temel Hakların Düzenlenmesi ve Somutlaştırılması, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Yıl 19, S. 38, Yaz, 2020/2, 2020

Gören, Zafer, Temel Hak Genel Teorisi, 4. Baskı, DEÜHFY, İzmir, 2000

Gören, Zafer, Temel Hakların Sınırlanması - Sınırlamanın Sınırları, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Yıl 6, S. 12, Güz, 2007/2, 2007

Gözler, Kemal, Anayasa Değişikliğinin Temel Hak ve Hürriyetlerin Sınırlandırılması Bakımından Getirdikleri ve Götürdükleri: Anayasanın 13'üncü Maddesinin Yeni Şekli Hakkında Bir İnceleme, Ankara Barosu Dergisi, Yıl 59, S. 2001/4, 2001

Gözübüyük, Şeref, Anayasa Hukuku, 16. Baskı, Ankara, 2008

Gözübüyük, Şeref/Gölcüklü, Feyyaz, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 7. Baskı, Turhan Kitabevi, Ankara, 2007

Grimaldi, Paola, Robots, Unwearable Profiling and Protection of Vulnerable Users, European Journal of Privacy Law & Technologies (EJPLT), Vol. 2020, No. 2, 2020

Guerin, Lisa, Employment Law: The Essential HR Desk Reference, Berkeley, California, Nolo, 2011

Guillemette, Manon G./Fontaine, Isabelle/Caron, Claude, Hybrid RFID-GPS Real-Time Location System for Human Resources: Development, Impacts and Perspectives, Proceedings of the 41st Hawaii International Conference on System Sciences in Waikoloa, Hawaii, January, 2008

Gumzej, Nina, Data Protection For The Digital Age: Comprehensive Effects of The Evolving Law of Accountability, Juridical Tribune, Volume 2, Issue 2, December, 2012

Gutierrez, Kenny, Privacy in Wearables: Innovation, Regulation, or Neither, Hastings Science and Technology Law Journal, Vol. 13, No. 1, Winter, 2022

Gülmez, Mesut, İnsan Haklarında Ayrımcılık Yasaklı Eşitlik İlkesi: Aykırı Düşünceler", Çalışma ve Toplum, 2010/2, 2010

Gümüş, Tarık A., Devletin Pozitif Yükümlülükleri Ekseninde Özel Hayata Saygı Hakkı, AİHS Uygulaması Çerçevesinde Bir İnceleme, Adalet Yayınevi, Ankara, 2016

Günay, Cevdet İlhan, İş Kanunu Şerhi, Yetkin Yayıncılık, Ankara, 2005

Güriz, Adnan, Hukuk Felsefesi, 14. Baskı, Ankara, 2019

Gürkan, Ülker, Kişilik Kavramının Evrimi, Prof. Dr. Hâmide Topçuoğlu'na Armağan, Ankara Üniversitesi Basımevi, Ankara, 1995

Gürpınar, Damla, Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk, DEÜ Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı, 2017

Gürsel, İlke, İşçinin Kişisel Verilerinin Korunması Hakkı, Adalet Yayınevi, Ankara 2016

Güzel, Ali, Fabrikadan İnternete İşçi Kavramı ve Özellikle Hizmet Sözleşmesinin Bağımlılık Unsuru Üzerine Bir Deneme, Kamu-İş İş Hukuku ve İktisat dergisi, S. 2, Haziran 1997 (Güzel Fabrikadan İnternete)

Güzel, Ali, Ekonomik ve Teknolojik Gelişmelerin İş Hukuku ve Sosyal Güvenlik Hukukuna Etkileri, Prof. Dr. Münir Ekonomi 85. Doğum Günü Armağanı, (Ed. Kübra Doğan Yenisey), On İki Levha Yayıncılık, İstanbul, 2021(Teknolojik Gelişmeler)

Güzel, Ali, İş Sözleşmesinin "Eylemli" Feshi ve Uygulama Sorunu, Çalışma ve Toplum, 2022/4, 2022 (Eylemli Fesih)

Güzel, Ali, İş Hukukunda 'Yetki' ve 'Özgürlük', İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Turhan Esener'e Armağan, C. 15, S. 1, 2016 (Yetki ve Özgürlük)

Güzel, Ali/Heper, Hande, Sürekli İstihdamdan Geçici Atipik İstihdama! Mesleki Amaçlı Geçici İş İlişkisi, Çalışma ve Toplum, S.1, 2017

Güzel, Ali/Ugan, Çatalkaya Deniz, İş Sözleşmesinin Uygulanmasında ve İşverenin Yönetim Yetkisinin Sınırlanmasında Dürüstlük (Objektif İyiniyet) Kuralının İşlevi Üzerine, Prof. Dr. Ali Rıza Okur'a Armağan, İstanbul, 2014

Güzel, Ali/Ugan Çatalkaya, Deniz/Heper, Hande, İş Hukukunun Yapay Zeka İle Buluşması: İşverenin Algoritmik Yönetimi", Hukuk ve Adalet Eleştirel Hukuk Dergisi, C. 15, Özel Sayı, 2023

Hafızoğulları, Zeki, İnsan Hakkı Olarak Kişilik Hakları ve Kişilik Haklarının Korunması, AÜHF Dergisi, Yıl 1997, Cilt 46, Sayı 1, 1997

Han, Byung-Chul, Şeffaflık Toplumu, Metis Yayınları, (Çev. Haluk Barışcan), İkinci Baskı, İstanbul, 2017

Harris, David/O'Boyle, Michael/Bates, Ed/Buckley, Carla, Avrupa İnsan Hakları Sözleşmesi Hukuku, Çev. Mehveş Bingöllü Kılcı/Ulaş Karan), Ankara, Avrupa Konseyi, 2013

Hart, Herbert Lionel Adolphus, The Concept of Law, Oxford University Press, Third Edition, 2022

Hartman, Laura P., Technology and Ethics: Privacy in the Workplace, Business and Society Review, Vol. 106, Issue 1, December, 2002

Hatemi, Hüseyin, Medeni Hukuka Giriş, On İki Levha Yayınları, İstanbul, 2004

Hauck, Ronny, Personal Data in Insolvency Proceedings: The Interface between the New General Data Protection Regulation and (German) Insolvency Law, European Company and Financial Law Review (ECFR), Vol. 16, No. 6, December, 2019

Helvacı, Serap, Gerçek Kişiler, Legal Yayınevi, 4. Bası, İstanbul 2012 (Gerçek

Kişiler)

Helvacı, Serap, Türk ve İsviçre Hukukunda Kişilik Hakkını Koruyucu Davalar, Beta Basım, İstanbul, 2001 (Koruyucu Davalar)

Hendrickx, Frank, Privacy 4.0 at Work: Regulating Employment, Technology and Automation, Comparative Labor Law & Policy Journal, Vol. 41, No. 1, Fall, 2019 (Priacy 4.0 at Work)

Hendrickx, Frank, Protection of Workers Personal Data in The European Union, Two Studies, EC, Manuscript Completed in July, 2002 (Workers Personal Data)

Heper, Hande, İş İlişkisinde İşçinin İradesi, İstanbul, Eylül, 2021

Hert, Paul de/Gutwırth, Serge, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, Reinventing Data Protection, Serge Gutwırth, Yves Poullet, Cecile de Terwangne, Sjaak Nouwt, Springer, 2009

Hert, Paul De/Papakonstantinou, Vagelis, Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency, I/S: A Journal of Law and Policy for the Information Society, Vol. 9, No. 2, 2013

Hildebrandt, Mireille, Defining Profiling: A New Type of Knowledge, Profiling the European Citizen (Ed. Mireille Hildebrandt/Serge Gutwirth), Springer, 2008

Hornung, Gerrit/Schnabel, Christoph, Data Protection In Germany I: The Population Census Decision and The Right to Informational Self-Determination, Computer Law & Security Report, Volume 25, Issue 1, 2009

Houwing, Lotte, Stop the Creep of Biometric Surveillance Technology, European Data Protection Law Review (EDPL), Vol. 6, No. 2, 2020, s. 175-176, (Houwing, [2020], Biometric Surveillance); Aloisi/Gramano, 2019

Hozar, Nağme N., Özel Amaçla İnternet ve E-Posta Kullanımının İş İlişkisine Etkisi", Sicil İş Hukuku Dergisi, S. 7, 2007

Höld, Florian, Die Überwachung von Arbeitnehmern, Hamburg, 2006, https://law.shu.edu/online/students/assignments/docs/eu-data-protection-privacy-law-readings.pdf

Hu, Margaret, Biometric ID Cybersurveillance, Indiana Law Journal, Vol. 88, No. 4, Fall, 2013

Hurd, Heidi M., The Moral Magic of Consent, Legal Theory, Vol. 2, Issue 2, June 1996

Huxley, Aldous, Cesur Yeni Dünya, Çev. Ümit Tosun, İthaki Yayınları, 2021

Işık, Rüçhan, Toplu Şikayet Prosedürü, Anayasal Sosyal Haklar –Avrupa Sosyal Şartı, Karşılaştırmalı Hukuk ve Türkiye, Editör: İbrahim Özden Kaboğlu, Legal Yayınevi, Şubat, 2012

Işıktaç, Yasemin/Koloş, Umut, Hukuk Sosyolojisi, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2022

Işıktaç, Yasemin/Metin, Sevtap, Hukuk Metodolojisi, Filiz Kitapevi, 2021

İbrahim Ö. Kaboğlu, Özgürlükler Hukuku, 3. Baskı, Afa Yayınları, İstanbul, 1996

İçel, Kayıhan, Ceza Hukuku Açısından Kişisel Verilerin Korunmasında 'Kişisel

Veri ve Hukuka Aykırılık' Kavramları, İstanbul Barosu Dergisi, Mart – Nisan 2022, C. 94, S. 2022/2, 2022

İmre, Zahit, Medeni Hukuka Giriş, İÜHF Yayınları, İstanbul, 1980

İnceoğlu, Sibel, ABD Anayasa Hukukunda Mahremiyet Hakkı, İnsan Hakları Yıllığı 1997-1998, C. 19, S. 20, 1998

İzmir, Gökalp/Fazlıoğlu, Aygül, İşyerinde Psikolojik Taciz (Mobbing) ve Çözüm Önerileri, Kadın Erkek Fırsat Eşitliği, Komisyonu Yayınları, Ankara, 2010

Jasserand, Catherine, Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data", European Data Protection Law Review (EDPL), Vol. 2, No. 3, 2016

Jochman, Tyler, Effects on Employees' Compensation under the Right to Disconnect, Marquette Benefits & Social Welfare Law Review, Vol. 22, No. 2, Spring, 2021

Kabakcı, Mahmut, 6331 Sayılı Kanun'un İş Sağlığı ve Güvenliği Anlayışı ve Risklerden Korunma İlklerinin (m.5) İşlevi, Sicil İş Hukuku Dergisi, S. 29, 2013

Kaboğlu, İbrahim Ö., Anayasa'da Sosyal Haklar: Alanı ve Sınırları, Legal Yayıncılık, 2012 (Sosyal Haklar)

Kaboğlu, İbrahim Ö., Hukukun Genel İlkeleri ve Anayasa Yargısı (Özgürlükler Hukuku Açısından Bir Yaklaşım), Anayasa Yargısı Dergisi, Cilt 8, 1991, (Genel İlkeler)

Kalamatiev, Todor/Ristovski, Aleksandar, The Right to Privacy in Employment and Its Protection under the European Convention on Human Rights, Iustinianus Primus Law Review, Vol. 11, No. Special Issue, 2020

Kambellari, Evisa, Employee Email Monitoring and Workplace Privacy in the European Perspective, Iustinianus Primus Law Review, Vol. 5, No. 1, 2014

Kanbur, Aysun/Kanbur, Engin, İşyerinde Siber Zorbalık Ölçeği'nin Türkçeye Uyarlanması: Geçerlik ve Güvenirlik Sınama Çalışması, Psikoloji Çalışmaları - Studies in Psychology Cilt/Volume: 38, Sayı/Issue: 2, 2018

Kandemir, Murat, Evde Çalışma ve 6098 sayılı Türk Borçlar Kanunu'nun Evde Hizmet Sözleşmesine İlişkin Hükümleri, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LXXII, S. 2, Prof. Dr. Berin Ergin'e Armağan, 2014 (Evde Çalışma)

Kandemir, Murat, İş Hukuku ve Sosyal Güvenlik Hukuku Açısından Tele Çalışma, Legal Yayıncılık, İstanbul, 2011 (Tele Çalışma)

Kangal, Zeynel T., Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması, On İki Levha Yayıncılık, İstanbul, 2019

Kaplan, Emine Tuncay, İş Hukukunda Kişilik Haklarının Özellikle Bilgisayarda Toplanan Bilgilere Karşı Korunması, Ankara Üniversitesi Siyasi Bilgiler Fakültesi Dergisi, Prof. Dr. Cemal Mıhçıoğlu'na Armağan, Ankara Ocak-Aralık, 1997

Karahanoğulları, Onur, İdari Takdir Yetkisinin Kullanılmasına İlişkin R(80)2 Sayılı Avrupa Konseyi Bakanlar Komitesi Tavsiye Kararı, AÜHFD, C. 34, S. 1-4, 1996

Karayalçın, Yaşar, Türk Hukukunda Şeref ve Haysiyetin Korunması, 1962-1963 Öğretim Yılı Açılış Dersi, https://dergipark.org.tr/tr/download/article-file/638117

Kardava, Ekaterine, Proportionality Principle as a Response Instrument to Challenges of Modern Labour Law, Journal of Law (TSU), Vol. 2017, No. 1, 2017

Kaya, Cemil, İdare Hukukunda Bilgi Edinme Hakkı, Seckin, Ankara, 2005

Kaya, Mehmet Bedii/Taştan, Furkan Güven, Kişisel Veri Koruma Hukuku-Mevzuat-İçtihat-Bibliyografya, 2. Baskı, İstanbul, 2019

Kelsen, Hans, Saf Hukuk Kuramı: Hukuk Kuramının Sorunlarına Giriş (Çev. Ertuğrul Uzun), Nora Kitap, İstanbul, 2016

Kerr, Ian/Mann, Steve, Exporing Equiveillance, January 1, 2006

Kılıçoğlu, Ahmet M., Şeref Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk, 5. Baskı, Ankara, 2016

Klein, Kris/Gates, Vivian, Privacy in Employment: Control of Personal Information in the Workplace, Thomson Canada Limited, Toronto, 2005

Kokott, Juliane/Sobotta, Christoph, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No. 4, 2013

Konvitz, Milton R., Privacy and the Law: a Philosophical Prelude, Law and Contemporary Problems, Duke University School of Law, Vol.31, Issue 2, 1966

Koops, Bert-Jaap, Privacy Spaces, West Virginia Law Review, Vol. 121, No. 2, Winter, 2018, https://tretse.com/edward-t-hall-and-the-study-of-personal-space/

Kovac-Orlandic, Milica R., Employee's Right to Privacy: Where Is the Bound of the Employer's Right to Monitor Employees' Communications, Strani Pravni Zivot (Foreign Legal Life), Vol. 2020, No. 4, 2020

Kramer, Irwin R., The Birth of Privacy Law: A Century Since Warren and Brandeis, Catholic University Law Review, Vol. 39, Issue 3, Spring, 1990

Kuner, Christopher, European Data Protection Law, Corporate Compliance and Regulation, Second Edition, Oxford University Press, United Kingdom, 2007

Küzeci, Elif, Kişisel Verilerin Korunması Hakkı, Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, 2023 (Verilerin Korunması)

Küzeci, Elif, Kişisel Verilerin Korunması, On İki Levha Yayınları, 4. Baskı, İstanbul, 2020 (Kişisel Veriler)

Küzeci, Elif/Kılıç Şebnem, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Açısından Değerlendirilmesi, Legal İSGHD, C. 16 S. 63, 2019

Lasprogata, Gail/King, Nancy J./Pillay, Sukanya, Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada, Stanford. Tech. Law Review. 4, 2004

Lazar, Wendi S./Ruan, Nantiya. Is There a Future for Work, Georgetown Journal on Poverty Law and Policy, Vol. 25, No. 3, Spring, 2018

Lemmens, Koen, The Protection of Privacy between a Rights-Based and a Freedom-Based Approach: What the Swiss Example Can Teach Us, Tilburg Foreign Law Review, Vol. 11, No. 3, 2004

Levin, Avner, Dignity in The Workplace: An Enquiry Into the Conceptual Foundation of Workplace Privacy Protection Worldwide, ALSB Journal of Employment and Labor Law Vol. 11, No. 1, Winter, 2009

Levy, Karen E.C., Relational Big Data, Stanford Law Review Online, 66, 2013-2014

Leymann, Heinz, The Content and Development of Mobbing At Work, European Journal of Work and Organizational Psychology, C. 5, S. 2, 1996

Lockwood, Graeme, Workplace Monitoring and Surveillance: The British Context, Athens Journal of Law (AJL), Vol. 4, No. 3, July 2018

Lockwood, Graeme/Nath Vandana, The Monitoring of Tele-Homeworkers in The UK: Legal and Managerial Implications, International Journal of Law and Management Vol. 63, No. 4, 2021

Lukács, Adrienn, Employees' Right to Privacy and Right to Data Protection on Social Network Sites with Special Regard to France and Hungary, Iurisperitus Publishers, Szeged, 2021

Lyon, David, Elektronik Göz, (Çev. Dilek Hattatoğlu) Sarmal Yayınevi, İstanbul, 1997 (Elektronik Göz)

Lyon, David, Gözetlenen Toplum, (Çev. Gözde Soykan), Kalkedon Yayınevi, İstanbul, 2006 (Gözetlenen Toplum)

Mali, Prashant, GDPR Articles With Commentary & BU Case Laws, 2019

Manav, A. Eda, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XIX, S. 2, 2015

Manav Özdemir, A. Eda, İşçinin İzlenmesi ve Gözetlenmesi, Muhtelif Yönleriyle Kişisel Verilerin Korunması Hukuku, (Ed. Kemal Şenocak), Yetkin Yayınları,

Ankara, 2022

Manokha, Ivan, Covid-19: Teleworking, Surveillance and 24/7 Work. Some Reflexions on the Expected Growth of Remote Work After the Pandemic, Political Anthropological Research on International Social Sciences (PARISS), 2020

Llorens, Mariona Rosell, 9th International Conference on Internet, Law and Politics (IDP 2013) Big Data: Challenges and Opportunities Report, SCRIPTed: A Journal of Law, Technology and Society, Vol. 10, No. 2, August, 2013

Martin, Brian, Antisurveillance, Information Liberation, Freedom Press, London, 1998

Marx, Gary T., Surveillance and Society, Encyclopedia of Social Theory, 2005 http://web.mit.edu/gtmarx/www/surandsoc.html

Marx, Gary T., Undercover: Palice Surveillance in America, Berkeley, University of California Press, 1988

Mattelart, Armand, Gözetimin Küreselleşmesi Güvenlileştirme Düzeninin Kökeni, (Çev. Onur Gayretli/Su Elif Karacan), Kalkedon Yayınları, İstanbul, 2012

McCahill, Michael/Norris, Clive, Watching the Workers: Crime, CCTV and the Workplace, Macmillan Press, 1999]

McCrudden, Christopher, Human Dignity and Judicial Interpretation of Human Rights, EJIL, Vol. 19, No. 4, 2008

McGinnis, John O./Wasick, Steven, Law's Algorithm, Florida Law Review, Vol. 66, No. 3, May, 2014

Memiş, Emin, Anayasa Mahkemesi Kararlarının Bağlayıcılığı ve İptal Kararlarının Geriye Yürümezliği Kuralının Sorgulanması Anayasa ve İdari Yargı Kararları Örnekleri, Anayasa Mahkemesinin Kuruluşunun 60. Yılı Anısına 60 yıl 60 Makale, Anayasa Mahkemesi Yayınları, Cilt II, Ankara, 2022

Mensel, Robert E., Kodakers Lying in Wait Amateur Photography and the Right of Privacy in New York, 1885-1915 American Quarterly, Vol. 43, No. 1, March, 1991

Metin, Yüksel, Avrupa Birliği Temel Haklar Şartı, Ankara Üniversitesi SBF Dergisi, C. 57, S. 4, 2002 (Haklar Şartı)

Metin, Yüksel, Temel Hakların Sınırlandırılması Ölçülülük, Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?, SDÜHFD C. 7, S. 1, 2017 (Hakların Sınırlandırılması)

Meyer, Stephen, Adapting the Immigrant to the Line: Americanization in the Ford Factory, 1914-1921, Journal of Social History, Vol. 14, Issue 1, 1980

Michael D. Kirby, Transborder Data Flows and the Basic Rules of Data Privacy, Stanford Journal of International Law, 16, 1980

Michael, James, Privacy And Human Rights: An International and Comparative Study, with Special Reference to Development in Information Technology, Paris, 1994, https://www.legislation.gov.uk/aep/Edw3/34/1

Miller, Seumas/Weckert, John, Privacy, the Workplace and the Internet, Journal of Business Ethics, Vol. 28, ss. 255–265, 2000

Mollamahmutoğlu, Hamdi/Astarlı Muhittin/Baysal, Ulaş, İş Hukuku, Lykeon Yayınevi, Ankara, 2019

Moore, Adam D., Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy, Business Ethics Quarterly, Cambridge University Press, Jul., 2000, Vol. 10, No. 3, 2000

Moore, Barrington, Privacy, Studies in Social and Cultural History, New York, 1984

Muhonen, Tuija/Jönsson, Sandra/Bäckström, Martin, Consequences of Cyberbullying Behaviour in Working Life, International Journal of Workplace Health Management, Vol. 10, No. 5, 2017

Murati, Erion/Henkoja Manjola, Location Data Privacy on MAAS under GDPR, European Journal of Privacy, Law & Technologies (EJPLT), Vol. 2019, No. 2, 2019

Muratoğlu, Tahir, Avrupa İnsan Hakları Mahkemesinin Kuruluşu Görevleri ve Yargılama Usulü", TAAD, Yıl: 7, S. 27, Temmuz, 2016

Narmanlıoğlu, Ünal, İş Hukuku - Ferdi İş İlişkileri, Beta Yayınevi, 5. Baskı, İstanbul 2014

Narter, Sami, İş Kazası ve Meslek Hastalığında Hukuki ve Cezai Sorumluluk, Adalet Yayınevi, Ankara, 2014

O'Shea, Lizzie, Ada Lovelace, Tom Paine ve Paris Komünü Bize Dijital Teknoloji Hakkında Ne Öğretebilir?, (Çev. Ayşecan Ay), Metis Yayınları, İstanbul 2021

Odaman, Serkan, İşverenin Hizmet Sözleşmesini Ahlak ve İyiniyet Kuralları ve Benzerlerine Aykırılık Nedeniyle Fesih Hakkı, Ankara, 2003

Ogrıseg, Claudia, GDPR and Personal Data Protection in the Employment

Context, LLI, Vol. 3, No. 2, 2017

Oğuzman, M. Kemal/ Seliçi, Özer/Oktay-Özdemir, Saibe, Kişiler Hukuku (Gerçek ve Tüzel Kişiler), 16. Baskı, Filiz Kitabevi, İstanbul, 2016

Oğuzman, M. Kemal/Barlas, Nami, Medeni Hukuk Giriş Kaynaklar Temel Kavramlar, Vedat Kitapçılık, İstanbul, 2020

Oğuzman, M. Kemal/Öz, Turgut, Borçlar Hukuku Genel Hükümler, I. Cilt, Vedat Kitapçılık, 15. Baskı, İstanbul, 2019

Oğuzman, M. Kemal/Öz, Turgut, Borçlar Hukuku Genel Hükümler, II. Cilt, Vedat Kitapçılık, 15. Baskı, İstanbul, 2019

Okur, Zeki, İş Hukukunda Elektronik Gözetleme, Legal Yayıncılık, İstanbul, 2013, (Elektronik Gözetleme)

Okur, Zeki, İşyerinde İşçinin Bilgisayar ve İnternet'i Özel Amaçlı Kullanımının İş İlişkisine Etkisi, Kamu-İş, İş Hukuku ve İktisat Dergisi, C. 8, S. 2, 2005 (Özel Amaçlı Kullanım)

Okur, Zeki, Türk İş Hukukunda İşçinin Kişisel Verilerinin Korunması Hakkı, İş Dünyası ve Hukuk, Prof. Dr. Tankut Centel'e Armağan, İstanbul Üniversitesi Yayınları No. 5006, İstanbul, 2011, s. 370, 399 (İşçinin Kişisel Verileri)

Oliver, Hazel, Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out, Industrial Law Journal, Vol. 31, No. 4, December, 2002

Orwell, George, Bin Dokuz Yüz Seksen Dört, (Çev. Celal Üster), Can Yayınları, 2021

Otto, Marta, Workforce Analytics v. Fundamental Rights Protection in the EU in the Age of Big Data, Comparative Labor Law & Policy Journal, Vol. 40, No. 3, 2019

Öktem Songu, Sezgi, Bir Haklı Fesih Sebebi Olarak 'Sataşma', Sicil İş Hukuku Dergisi, S. 39, 2018 (Sataşma)

Öktem Songu, Sezgi, İşçilerin İşyerinde Özel Amaçlı İnternet ve E-Posta Kullanımına İşverenin Müdahalesi Üzerine Bir Değerlendirme, Prof. Dr. Sarper Süzek'e Armağan, Cilt I, Beta Yayıncılık, İstanbul, 2011 (Özel Amaçlı İnternet)

Özbudun, Ergun, Anaysa Hukuku Bakımından Özel Haberleşmenin Gizliliği, Ankara Üniversitesi Hukuk Fakültesi 50. Yıl Armağanı, Ankara Üniversitesi Hukuk Fakültesi Yayınları, No. 406, C. 1, Ankara, 1977

Özdemir, Erdem, İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkilerine Etkileri, Sicil İş Hukuku Dergisi, Haziran, 2008 (Yeni Teknolojiler)

Özdemir, Erdem, İş Hukukunda Mutlak Emredici Hükümlerin Yeri, AÜHFD, C. 54, S.3, Ankara, 2005 (Emredici Hükümler)

Özdemir, Erdem, İş Sağlığı ve Güvenliği Hukuku Dersleri, Vedat Kitapçılık, İstanbul, 2020 (İş Sağlığı ve Güvenliği)

Özdemir, Hayrunnisa, Haberleşmenin Gizliliği ve Kişisel Veriler, EÜHFD, C.13, S.1-2, 2009 (Haberleşmenin Gizliliği)

Özdemir, Hayrunnisa, İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması", EÜHFD, C. XIV, S. 1–2, 2010 (İşçilerin İzlenmesi)

Özdemir, Olgu, İş Sözleşmesinin Feshinde Dürüstlük Kuralı ve Hakkın Kötüye Kullanılması Yasağı, On İki Levha Yayıncılık, 2022

Özek, Çetin, Türk Basın Hukuku, İstanbul Üniversitesi Yayınları, İstanbul, 1978

Özer, Hatice Duygu, Pandemi Sürecinde Artan Tehlike: İşyerinde Siber Zorbalık, Selçuk Hukuk Kongresi 2020 Özel Hukuk Tebliğleri Tam Metin Kitabı, Nobel Akademi, 2020

Özsunay, Ergun, Gerçek Kişilerin Hukuki Durumu, İÜHF Yayınları, İstanbul, 1979

Öztan, Bilge, Medeni Hukukun Temel Kavramları, Yetkin Yayınları, 46. Baskı, Ankara 2021 (Temel Kavramlar)

Öztan, Bilge, Şahsın Hukuku: Hakiki Şahıslar, Turhan Kitabevi, Ankara, 2000 (Şahsın Hukuku)

Özyörük, Mukbil, Hukuka Giriş, Ege Yayınları, Ankara, 1959

Palm, Elin, The Ethics of Workspace Surveillance, Doctoral Thesis in Philosophy from the Royal Institute of Technology nr 26, 2017

Palmer, Vernon Valentine, Three Milestones in the History of Privacy in the United States, Tulane European and Civil Law Forum, 26, 2011

Park, Susan, Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy, American Business Law Journal 51, No. 4, 2014

Pauline, Kim T., Privacy Rights, Public Policy, and the Employment Relationship,

Ohio State Law Journal, Vol. 57, No. 3, 1996

Pease-Watkin, Catherine, Bentham'ın Panoptikon'u ve Dumont'un Panoptique'i, (Ed. Barış Çoban/Zeynep Özarslan), Panoptikon: Gözün İktidarı, Su Yayınları 2. Baskı, İstanbul, 2016

Pekcanıtez, Hakan/Atay, Oğuz/Özekes, Muhammed, Medeni Usul Hukuku, 14. Bası, Yetkin Yayınları, Ankara, 2013

Perumal, Vanessa, The Future of U.S. Data Privacy: Lessons from the GDPR and State Legislation, Notre Dame Journal of International & Comparative Law, Vol. 12, No. 1, 2022

Petrovıć, Dalibor, The Ethics of Employees' Surveillance in the Context of Rapid ICT Development, The 4th International Conference Mechanical Engineering in XXI Century, April 19-20 2018

Pogace, Enik, Employees' Data Protection in the Workplace and Its Legal Implications: A Comparative Overview of EU's Legal Framework, International In-House Counsel Journal, Vol. 10, No. 37, Autumn, 2016

Polater, Yusuf Ziya, Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması, Adalet Yayınevi, Ankara, 2010

Post, Antoine, Özel Hayatın Sınırları ve Alanları, (Ed. Philippe Aries/Georges Duby), Özel Hayatın Tarihi 5, Birinci Dünya Savaşı'ndan Günümüze, (Çev. Şehsuvar Aktaş), Yapı Kredi Yayınları, İstanbul 2010

Post, Robert C., Three Consept of Privacy, The Georgetown Law Journal, Vol. 89, 2001

Poto, Margherita, The Principle of Proportionality in Comparative Perspective,

German Law Journal, Vol. 8, No: 9, September 1, 2007

Price, David, The Emergence of a UK Data Protection Law, Yearbook of Law Computers and Technology, 1, 1984

Prins, Corien, Digital Diversity: Protecting Indentities Instead of Individual Data, Hetbinnenste Buiten, Leiden, 2010

Pushka, Jessica, The Applicability of the Personal Information Protection and Electronic Documents Act to De-Indexing Internet Search Engine Results, Asper Review of International Business and Trade Law, 19, 2019

Ray, David, Monitoring Privacy, Law Now, Vol. 25, No. 1, August/September, 2000

Regan, Priscilla M., Legislating Privacy: Technology, Social Values, and Public Policy, University of North Carolina Press, 1995

Richardson, Janice, Law and the Philosophy of Privacy, Routledge, London, 2016

Riedy, Marian K./Wen, Joseph H., Electronic Surveillance of Internet Access in the American Workplace: Implications for Management, Information & Communications Technology Law, Vol. 19, No. 1, March, 2010

Riso, Sara, Monitoring and Surveillance of Workers in The Digital Age https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age

Rosenberg, Kendra, Location Surveillance by GPS: Balancing an Employer's Business Interest with Employee Privacy, Washington Journal of Law, Technology & Arts, Vol. 6, No. 2, Autumn, 2010

Rouvroy, Antoinette/Poullet, Yves, The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, Reinventing Data Protection, Springer, 2009

Rubenfeld, Jed, The Right of Privacy, Harvard Law Review, Vol. 102, No. 4, February, 1989

Rule,James/Brantley, Peter, Computerized Surveillance in the Workplace: Forms and Distributions, Sociological Forum, 1992

Rumpf, Christian, Ölçülülük İlkesi ve Anayasa Yargısındaki İşlevi ve Niteliği, Anayasa Yargısı Dergisi, C. 10, 1993

Rustad, Michael/Paulsson, Sandra R, Monitoring Employee E-Mail And Internet Usage: Avoiding The Omniscient Electronic Sweatshops: Insights From Europe, Suffolk University Law School, The Berkeley Electronic Press, 2005

Sabuncu, M. Yavuz, Temel Hakların Anayasal Konumu Üzerine, İnsan Hakları Yıllığı, Yıl [1985-1986], Cilt 7, Sayı 1, s. 15-26; Anayasa Mahkemesi 60 Yıl 60 Makale, C. 1, 2022

Sağlam, Fazıl, Temel Hakların Sınırlanması ve Özü, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, C. 506, S.B.F. İnsan Hakları Merkezi Yayınları, 4, Ankara, 1982 (Temel Haklar)

Sağlam, Fazıl, Türk ve Alman Anayasa Hukukları Açısından Gizli Ses Kaydı, AÜSBFD, S. 1-4, Ankara, 1977 (Gizli Ses Kaydı)

Sarpong, Sam/Rees, Donna, Assessing The Effects Of 'Big Brother' in A Workplace: The case of WAST", European Management Journal, Volume 32, Issue 2, April, 2014

Savaş, F. Burcu, İş Hukukunda Siber Gözetim, Çalışma ve Toplum, 2009/3, 2009

Schabas, William A., The European Convention on Human Rights: a Commentary, Oxford University Press, Oxford, 2015

Schoeman, Ferdinand, Privacy Philosophical Dimensions of The Literature, Philosophical Dimensions of Privacy An Anthology, Edited by, Ferdinand David Schoeman, Cambridge University Press, Second Edition, Cambridge 2007

Secunda, Paul M., The Employee Right to Disconnect, Notre Dame Journal of International & Comparative Law, Vol. 9, No. 1, 2019 (Right to Disconnect)

Senyen Kaplan, Emine Tuncay, Bireysel İş Hukuku, Yetkin Yayınları, 9. Baskı, Ankara 2018

Senyen Kaplan, Emine Tuncay, İşverenin Koruma ve Gözetme Borcunun Kapsamı, Kamu-İş Dergisi, C: 7, S. 2, 2003

Senyen Kaplan, Emine Tuncay, Yeni Türk Borçlar Kanunu Hükümlerine Göre İş İlişkisinde İşçinin Kişilik Haklarının Korunması, Sicil İş Hukuku Dergisi, Yıl: 6, S. 24, Aralık, 2011

Seo, Sarah A., Charles Reich and the Legal History of Privacy, Touro Law Review, Vol. 36, No. 3, 2020

Serge Gutwirth, Privacy and The Information Age, Lanham: Rowman & Littlefield Publishers Inc. 2002

Serozan, Rona, Hukukta Yöntem, Vedat Kitapçılık, İstanbul 2015 (Hukukta Yöntem)

Serozan, Rona, Kişiye Sıkı Biçimde Bağlı Manevi Hakların Mirasçıya Geçebilirliği, Prof. Dr. Özer Seliçi'ye Armağan, Seçkin Yayıncılık, Ankara, 2006 (Manevi Haklar)

Serozan, Rona, Medeni Hukuk Genel Bölüm ve Kişiler Hukuku, Vedat Kitapçılık, İstanbul, 2013 (Medeni Hukuk)

Sever, Rabia, İşverenin Eşit Davranma Borcu, Legal İSGHD, C. 9, S. 34, 2012

Sevimli, K. Ahmet, İşçinin Özel Yaşamına Müdahalenin Sınırları, Legal Yayıncılık, İstanbul, 2006, (Özel Yaşam).

Sevimli, K. Ahmet, Türk Borçlar Kanunu m. 417 ve İş Sağlığı ve Güvenliği Kanunu Işığında Genel Olarak İşçinin Kişiliğinin Korunması, Çalışma ve Toplum, 2013/1, 36, 2013 (İşçinin Kişiliğinin Korunması)

Sevimli, K. Ahmet, Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419, Sicil İş Hukuku Dergisi, Yıl 6, s. 24, Aralık, 2011 (TBK Madde 419)

Sewell, Graham, The Discipline of Teams: The Control of Team-Based Industrial Work Through Electronic Surveillance, Administrative Science Quarterly, 1998

Shara, Monteleone, EPRS, European Parliamentary Research Service, Members Research Service PE 608.661, EU Legislation in Progress, September, 2017

Shenker, Pnina Alon/Davidov Guy, Applying the Principle of Proportionality in Employment and Labour Law Contexts, McGill Law Journal, Vol. 59, Issue 2, 2013

Sırabaşı, Volkan, İnternet ve Radyo- Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi), Ankara, 2007

Simic, Vladimir, Managing Modern Enterprises, International Journal of Economics and Law, Vol.3, 2013

Simitis, Spiros, Privacy - An Endless Debate, California Law Review, Vol. 98, No. 6, December, 2010

Simitis, Spiros, From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union, Comparative Labor Law and Policy Journal, Vol. 19, No. 3, Spring, 1998

Simitis, Spiros, The Case of the Employment Relationship: Elements of a Comparison in, Ed. Willibald Steinmetz, Private Law and Social Inequality in the Industrial Age: Comparing Legal Cultures in Britain, France, Germany, and the United States, Oxford University Press, London, 2000

Simon, Mark Reilly, The Use Of Electronic Surveillance And Performance Measures in The Workplace: A Qualitative Investigation, Durham Theses, Durham University. Available at Durham E-Theses Online: http://etheses.dur.ac.uk/429/

Sitzia, Andrea/Barraco, Enrico, Protection of Privacy in Labor Relations: The Italian Case within the European Dimension, Comparative Labor Law & Policy Journal, Vol. 31, No. 4, Summer, 2010

Sloan, Robert H./Warner, Richard, Beyond Notice and Choice: Privacy, Norms, and Consent, J. High Tech. Law, 2013

Solove Daniel J., Conceptualizing Privacy, California Law Review, Vol. 90, No. 4, July, 2002 (Conceptualizing Privacy)

Solove, Daniel J., A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3, January, 2006 (Taxonomy of Privacy)

Solove, Daniel J., Murky Consent: An Approach to the Fictions of Consent in Privacy Law, The George Washington Law Review, Vol .91, Issue 1, January 15, 2023 (Murky Consent)

Sprague, Robert D., From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace, The John Marshall Journal of Information Technology & Privacy Law, Vol. 25, Issue 1, Winter, 2007 (From Taylorism to the Omnipticon)

Sprague, Robert, Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees, John Marshall Law Review, Vol. 42, No. 1, Fall 2008 (Orwell Was an Optimist)

Sprague, Robert, Survey of (Mostly Outdated and Often Ineffective) Laws Affecting Work-Related Monitoring, Chicago-Kent Law Review, Vol. 93, Issue. 1, 2018 (Monitoring)

Steele, Jonathan, Data Protection: An Opening Door? The Relationship between Accessibility and Privacy in Sweden in an EU Perspective, Liverpool Law Review, Vol. 24, No. 1-2, January, 2002

Subaşı, İbrahim, Küresel Covid-19 Salgını'nın Türk Bireysel İş Hukukuna Etkisi, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Dergisi, S. 5, 2020

Sur, Melda, Çalışanın E-Postasına İşveren Tarafından Girilmesi, Sicil İş Hukuku

Dergisi, Sayı 44, 2020

Susser, Daniel/Roessler, Beate/Nissenbaum, Helen, Online Manipulation: Hidden Influences in Digital World, Georgetown Law Technology Review, Vol.4, Issue 1, 2019

Süzek, Sarper, İş Akdinin Türleri, Mercek İş Hukuku Dergisi, Nisan, 2001 (İş Akdi)

Süzek, Sarper, İş Güveliği Hukuku, Ankara, 1985 (İş Güvenliği)

Süzek, Sarper, İş Hukuku, Beta Yayınevi, 18. Baskı, İstanbul, 2019 (İş Hukuku)

Süzek, Sarper, İş Hukukunda Amaca Uygun Yorum, MESS Sicil, S. 34, 2015 (Amaca Uygun Yorum)

Süzek, Sarper, İş Hukukunda Yorum, İnan Kıraç'a Armağan, Galatasaray Üniversitesi, Ankara, 1994 (Yorum)

Süzek, Sarper, İşçi Ücretlerinin Ödenmemesinin Hukuki Sonuçları, AÜHFD, C. 56, S. 4, 2007 (Ücret)

Süzek, Sarper, İşverenin İşçiyi Gözetme Borcu, Prof. Dr. Tunçer Karamustafaoğlu'na Armağan, Ankara, 2010 (Gözetme Borcu)

Süzek, Sarper, İşverenin Yönetim Hakkı ve Sınırları, Prof. Dr. Metin Kutal'a Armağan, Ankara, 1998 (Yönetim Hakkı)

Sychenko, Elena, International Protection of Employee's Privacy under the European Convention on Human Rights, Zbornik Pravnog Fakulteta u Zagrebu, Vol. 67, No. 5, 2017

Szweda, Eric A., Applying the Personal Data (Privacy) Ordinance to Employee Monitoring, Hong Kong Law Journal, Vol. 43, No. 3, 2013

Şahin Ceylan, Şule, H.L.A. Hart'ın Yaklaşımıyla Hukuk Kavramı, Hukuk Felsefesi ve Sosyolojisi Arkivi 23. Kitap, Editörler: Hayrettin Ökçesiz, Gülriz Uygur ve Saim Üye, İstanbul Barosu Yayınları, 2012

Şahlanan, Fevzi, İşyerinde İşverence Sağlanan Bilgisayarı İşle İlgisi Olmayacak Şekilde Kullanma – Haklı Fesih (Karar İncelemesi), Tekstil İşveren Dergisi, S. 383, 2012

Şen, Ersan, Özel Hayatın Gizliliği ve Korunması, Kazancı Kitap, İstanbul, 1996

Şen, Murat, İş Hukukunda Çalışma Koşullarında Değişiklik, Ankara, 2005

Şen, Murat/Barın, Taylan, Özel Hayata ve Aile Hayatına Saygı Hakkı Karar Özetleri, Anayasa Mahkemesi Yayınları, 2021

Şenel, Leyla, Anayasalarda İnsan Hak ve Özgürlüklerinin Tanınması Sorunu, Oniki Levha, İstanbul, 2020

Tandoğan, Haluk, Şahsiyetin Akit Dışı İhlallere Karşı Korunmasının İşleyiş Tarzı ve Basın Yoluyla Olan İhlallere Karşı Özel Hayatın Korunması, 1962-1963 Öğretim Yılı Açılış Dersi, https://dergipark.org.tr/tr/download/article-

Tanrıver, Süha, Türk Medeni Usul Hukuku Bağlamında Hukuka Aykırı Yollardan Elde Edilen Delillerin Durumunun İrdelenmesi, TBB Dergisi, S. 65, 2006

Tarhanlı, Turgut, Birleşmiş Örgütü ve İnsan Haklarının Korunmasına İlişkin Başlıca Usuller, (Ed. Turgut Tarhanlı), İnsan Hakları, YKY, İstanbul 2000

Taşkent, Savaş, İşverenin Yönetim Hakkı, Doktora Tezi, İstanbul, 1981

Taşkın, Ahmet, Mobbingin Benzer Kavramlardan Farkı, Sicil İş Hukuku Dergisi, S. 28, 2012

Tekin, Nurullah, Adli ve Önleme Amaçlı İletişimin Denetlenmesi ve Bu Yolla Elde Edilen Bilgilerin Delil Olarak Değerlendirilmesi, Yargıtay Dergisi, C.35, S. 4, Ekim, 2019

Tekinay, Selahattin Sulhi, Medeni Hukukun Genel Esasları ve Gerçek Kişiler Hukuku, 6. Baskı, Filiz Kitabevi, İstanbul, 1992

Tezcan, Durmuş, Bilgisayar Karşısında Özel hayatın Korunması, Anayasa Yargısı Dergisi, C. 8, 1991 https://ayam.anayasa.gov.tr/media/4797/dtezcan.pdf

Thauberger, John J., Right to Privacy, Saskatchewan Bar Review, Vol. 30, No. 3, September, 1965

Thomas Lee, Laurie, Watch Your E-mail - Employee E-Mail Monitoring and Privacy Law in the Age of the Electronic Sweatshop, John Marshall Law Review, Vol. 28, No. 1, Fall, 1994

Tınaz, Pınar, Mobbing: İşyerinde Psikolojik Taciz, Çalışma ve Toplum Dergisi, S. 3, 2006

Tınaz, Pınar/Bayram, Fuat/Ergin, Hediye, Çalışma Psikolojisi ve Hukuki Boyutlarıyla İşyerinde Psikolojik Taciz Mobbing, Beta Yayınevi, İstanbul, 2008

Tokcan, Hüseyin, Bilginin Üretimi ve Kullanımı Açısından Bilgi Yönetimi: Üniversite'de Akademik Yöneticilerin Bilgi Yönetimi Algıları Üzerine Bir Uygulama, Doktora Tezi, Kırıkkale Üniversitesi, 2015

Topo, Adriana/Orsola, Razzolini, The Boundaries of the Employer's Power to Control Employees in the ICTs Age, Comparative Labor Law & Policy Journal, Vol. 39, No. 2, Winter, 2018

Troper, Michel, Hukuk Felsefesi, Dost Yayınlar, 2. Baskı, Ankara, 2019

Tunay, A. Can, İş Hukukunda Eşit Davranma İlkesi, İstanbul, 1982

Tunçomağ, Kenan/Centel, Tankut, İş Hukukunun Esasları, Beta Yayınları, 9. Baskı, İstanbul, 2018

Tzanou, Maria, European Union Regulation of Transatlantic Data Transfers and Online Surveillance, Human Rights Law Review, Vol. 17, No. 3, September, 2017

Ugan Çatalkaya, Deniz, İş Hukukunda Eşitlik İlkesinin İki Bileşeni: İşverenin Dar Anlamda Eşit Davranma Borcu ve Ayrım Yasağı", Çalışma ve Toplum, 2021/2, 2021 (Eşitlik İlkesi)

Ugan Çatalkaya, Deniz, İş Hukukunda Ölçülülük İlkesi, Beta, İstanbul, 2019 (Ölçülülük)

Ugan Çatalkaya, Deniz, Kişisel Yaşamı Kapsamında İşçinin, İşverence "Ulaşılabilir Olmama" Hakkı, İÜHFM, Prof. Dr. Fevzi Şahlanan'a Armağan Sayısı, C. 74, 2016 (Ulaşılabilir Olmama)

Ulusan, İlhan, Özellikle Borçlar Hukuku ve İş Hukuku Açısından İşverenin İşçiyi Gözetme Borcu, Kazancı Hukuk Yayınları, İstanbul, 1990

Uncular, Selen, Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Seçkin Yayıları, 2. Baskı, Ankara, 2018

Uncular, Selen, Teknolojinin Etkisiyle Dönüşen İş İlişkisinde Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme, Çalışma ve Toplum, C. 66, 2020/3, 2020

Urso, Scott D., Who's Watching Us at Work? Toward a Structural–Perceptual Model of Electronic Monitoring and Surveillance in Organizations, Communication Theory, Vol. 16, Issue 3, 2006

Üçüncü, Sümeyye Hilal, Medeni Usul Hukuku Çerçevesinde Kişisel Verilerin Korunması, Kişisel Verilerin Korunmasına Akademik Bakış – KVKK Akademi Derleme Çalışması, (Ed. Pınar Çağlayan Aksoy/Hüseyin Can Aksoy), Ütopya Grafik, Ankara, 2023

Ünal Adınır, Canan, Tele Çalışmada Verilerin Korunması, Mukayeseli Yönleriyle Kişisel Verilerin Korunması Hukuku, (Ed. Kemal Şenocak), Yetkin Yayınları, Ankara, 2022 (Verilerin Korunması)

Ünal, Canan, İş Hukukunda Yaş Ayrımcılığı, On İki Levha Yayıncılık, İstanbul, 2018 (Yaş Ayrımcılığı)

Ünal, Canan, İş Sözleşmesinin Kurulmasında Sağlığa İlişkin Veriler, İş Hukukunda Genç Yaklaşımlar III, (Ed. Prof. Dr. Tankut Centel), On İki Levha, 2018 (Sağlığa İlişkin Veriler)

Ünal, Şeref, Uluslararası Hukuk, Yetkin Yayınları, Ankara, 2005

Üye, Saim, Gündelik Dil Felsefesi Betimleyici Sosyoloji ve Eleştirellik, TBB

Dergisi, Eylül – Ekim, S.114, 2014

Üzeltürk, Sultan, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, Beta Yayınevi, İstanbul, 2004

Vigneau, Christophe, Information Technology and Workers' Privacy: Regulatory Techniques, Comparative Labor Law & Policy Journal, Vol. 23, No. 2, Winter, 2002

Vitak, Jessica/Zimmer, Michael, Surveillance and The Future of Work: Exploring Employees' Attitudes Toward Monitoring in a Post-COVID Workplace, Journal of Computer-Mediated Communication, 2023, Vol. 28/4, 2023

Vivarelli, Angela, The Crisis of the Right to Informational Self-Determination, Italian Law Journal, Vol. 6, No. 1, 2020

Vorvoreanu, Mihaela/Carl H. Botan, Examining Electronic Surveillance in the Workplace: A Review of Theoretical Perspectives and Research Findings, in Acapulco, Mexico, 2000

Voss, W. Gregory, Airline Commercial Use of EU Personal Data in the Context of the GDPR, British Airways and Schrems II, Colorado Technology Law Journal, Vol. 19, No. 2, 2021

Wachter, Sandra/Mittelstadt, Brent/Russell, Chris, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, Harvard Journal of Law & Technology, Vol. 31, No. 2 Spring, 2018

Wagner, Julian/Benecke, Alexander, National Legislation within the Framework of the GDPR, European Data Protection Law Review (EDPL), Vol. 2, No. 3, 2016

Warren, Samuel D./Brandeis, Louis D., The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, December 1890

Watkins Allen, Myria/Coopman, Stephanie, J./Hart, Joy L./L. Walker, Kasey, Workplace Surveillance And Managing Privacy Boundaries, Management Communication Quarterly, Vol. 21 No. 2, 2007

Westin, Alan F., Privacy and Freedom, New York, Atheneum, 1967

Westin, Alan F., The Origins of Modern Claims to Privacy, Philosophical Dimensions of Prvacy an Anthology, Ed. Ferdinand D. Schoeman, Cambridge University Press, 1984

Wieser, Luisa/Abraham, Martin, Employee Acceptance of Digital Monitoringsystems While Working From Home, New Technology Work Employment, 2023

Williams, Kara R., Protecting What You Thought Was Yours: Expanding Employee Privacy to Protect the Attorney-Client Privilege from Employer Computer Monitoring", Ohio State Law Journal, Vol. 69, No. 2, 2008

Wong, Benjamin, Data Protection Implications of Modern Employee Monitoring Software, Singapore Academy of Law Journal, Vol. 33, No. Special Issue, 2021

Wong, Rebecca, The Data Protection Directive 95/46/EC: Idealisms and Realisms, International Review of Law, Computers & Technology, Vol. 26, No. 2-3, July-November, 2012

Yalçın Kavak, Medeni Hukukta Dürüstlük Kuralı ve İyiniyetin Korunması, İstanbul, Legal, 2019

Yalman, Süleyman, Türk – İsviçre Hukukunda Sözleşme Görüşmelerinden Doğan

Sorumluluk, Seçkin Yayıncılık, Ankara, 2005

Yamakoğlu, Efe, Bilişim Teknolojilerinin Kullanımının İş Sözleşmesi Taraflarının Fesih Hakkına Etkisi, On İki Levha Yayıncılık, İstanbul, 2020

Yıldız, Ali Kemal, Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi, Yayımlanmamış Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2002

Yıldız, Gaye Burcu, İş Hukukunun Etkinliği ve Amacı Üzerine Yeniden Düşünmek, Çalışma ve Toplum, 2018/2, 2018

Yıldız, Gaye Burcu, İş İlişkisinin Kurulması, Hükümleri ve İşin Düzenlenmesi, Yargıtay'ın İş Hukuku ve Sosyal Güvenlik Hukuku Kararlarının Değerlendirilmesi 2015, XII Levha Yayıncılık, İstanbul 25-26 Kasım, 2016

Yıldız, Gaye Burcu, İşverenin Eşit İşlem Yapma Borcu, Ankara, 2008 (Eşit İşlem Yapma Borcu)

Yıldız, Gaye Burcu, Türk İş Hukukunda Orantılılık İlkesi, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi C. 15, Özel Sayı-2013, 2014 (İş Hukukunda Orantılılık)

Yiğit, Esra, İşyerinde İnternet ve E-posta Kullanımının İzlenmesi ve Gözetlenmesi, İÜ, Yüksek Lisans Tezi, 2013 (İşyerinde İnternet)

Yongalık, Aynur, İstisnalar Dar Yorumlanır Kuralı ve Değerlendirmesi, AÜHFD, C. 60, S. 1, Ankara 2011

Yung, Jill, Big Brother Is Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do about It, Seton Hall Law

Review, Vol. 36, No. 1, 2005

Yurtcan, Erdener, Yargıtay Kararlarının Işığında Hukuka Aykırı Delillere Dayanma Yasağı, Prof. Dr. Nurullah Kunter'e Armağan, İstanbul, 1998

Yücedağ, Nafiye, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, Kişisel Verileri Koruma Dergisi, C. 1, S. 1, 2019 (Veri Koruma Genel İlkeleri)

Yücedağ, Nafiye, Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İÜHFM C. LXXV, S. 2, 2017 (Genel Hukuka Uygunluk Sebepleri)

Yüksel, Saadet, Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale, Beta, İstanbul, 2012

Zafer, Hamide, Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK m.132-134)", Beta Yayınevi, İstanbul, 2010

Zevkliler, Aydın/Acabey, M. Beşir/Gökyayla, K. Emre, Medeni Hukuk, Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku, 5. Baskı, Ankara, 1997

Zevkliler, Aydın/Havutçu, Ayşe/Gürpınar, Damla, Medeni Hukuk, Temel Bilgiler, 6. Baskı, Ankara, 2008

Ziccardi, Giovanni, Wearable Technologies and Smart Clothes in the Fashion Business: Some Issues concerning Cybersecurity and Data Protection", Laws, Vol. 9, No. 2, June, 2020

Zuiderveen Borgesius, Frederik J./Kruikemeier, Sanne/Boerman, Sophie C./Helberger, Natali, Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, European Data Protection Law Review (EDPL), Vol. 3, No. 3, 2017

Zureik, Elia, Theorizing Surveillance: The Case of the Workplace, Surveillance as Social Sorting Privacy, Risk and Digital Discrimination, (Ed. David Lyon), Routledge, London, 2003

ÇEVRİMİÇİ KAYNAKLAR

http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

http://hudoc.echr.coe.int/eng?i=001-109029.

http://hudoc.echr.coe.int/eng?i=001-115871

http://www.ilo.org/

http://www.kazancı.com/

https://castle.eiu.edu/~alsb/Dignity%20in%20the%20Workplace%20final.pdf

https://customertimes.com/insights/data-is-the-new-oil/

https://dergipark.org.tr/tr/download/article-file/84746;

https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, s. 1-26,

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (

https://edpb.europa.eu/news/news/2021/italian-sa-unfettered-employee-surveillance-be-banned_en

https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

https://en.wikipedia.org/wiki/United_States_Bill_of_Rights

https://eur-lex.europa.eu/resource.html?uri=cellar:8275ac53-e4f0-4c82-82d7-15671106d69c.0002.06/DOC_1&format=PDF

https://fherehab.com/learning/public-exposure-and-mental-health/
https://home.heinonline.org/
https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001-45813&filename=HALFORD%20v.%20THE%20UNITED%20KINGDOM.pdf&logEvent=False
https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200344%22]}
https://ikmagazin.com/is-dunyasi/isverenin-evden-calisanlari-kamerayla-izlemesine-tepki-yukseliyor/
https://insanhaklarimerkezi.bilgi.edu.tr/tr/news/none-kisisel-verilere-dair-sozlesme-bakanlar-kurul/
https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/4825
https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf
https://sicil.mess.org.tr
https://sozluk.gov.tr
https://supreme.justia.com/cases/federal/us/429/589/
https://unece.org/wp29-introduction; 2130/05/EN
https://www.anayasa.gov.tr/media/3600/aihmkararlarindanornekler.pdf
https://www.archives.gov/founding-docs/bill-of-rights-transcript
https://www.calismatoplum.org/
https://www.coe.int/tr/web/impact-convention-human-rights/convention-on-human-rights-and-biomedicine#/
https://www.dailymail.co.uk/sciencetech/article-5673497/China-mining-data-directly-workers-brains-spot-emotional-depressed-employees.html
https://www.echr.coe.int/Documents/Guide_Art_8_TUR.pdf.
https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource
https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/monitoring-and-surveillance
https://www.goc.gov.tr/kurumlar/goc.gov.tr/yonetmelikler/Sozlesmeler/Avrupa-

Insan-Haklari-Sozlesmesi.pdf
https://www.icj.org/wp-content/uploads/2017/09/Ukraine-Denisov-v-Ukraine-Advocacy-legal-submission-2017-ENG.pdf
https://www.ilo.org/ankara/about-us/WCMS_372872/lang--tr/index.htm
https://www.ilo.org/public/libdoc/ilo/2005/105B09_8_engl.pdf
https://www.ilo.org/wcmsp5/groups/public/@ed_dialogue/@dialogue/documents/publication/wcms_209280.pdf
https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf
https://www.jdsupra.com/legalnews/data-privacy-laws-zeroing-in-on-7664079/
https://www.kvkk.gov.tr
https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/3a7934b6-406e-4911-a94d-795293aa0e3d.pdf
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/e3c6aa10-9de4-46f8-9b51-71bcf07c09b5.pdf
https://www.law.cornell.edu/wex/griswold_v_connecticut_(1965)
https://www.lexpera.com.tr
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7041862/
https://www.oecd.org/about/
https://www.oecd.org/general/organisationforeuropeaneconomicco-operation.htm
https://www.oecd.org/newsroom/oecd-welcomes-costa-rica-as-its-38th-member.htm
https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
https://www.oecd-ilibrary.org//sites/1686c758-en/1/3/2/index.html?itemId=/content/publication
https://www.oxfordlearnersdictionaries.com/definition/english/surveillance?q=surveillance

https://www.resmigazete.gov.tr/eskiler/2022/11/20221115-5.pdf
https://www.ssi.ens.fr/textes/a78-17-text.html#art31
https://www.un.org/youthenvoy/2013/08/ilo-international-labour-organization/?gclid
https://www.yargitay.gov.tr/documents/aihm2.pdf
www.eur-lex.europa.eu
www.lebibyalkin.com.tr