YAPAY ZEKA ÇAĞINDA HUKUK

İstanbul Barosu
Bilişim Hukuku Komisyonu
Yapay Zekâ Çalışma Grubu

2020

Danışmanlar

Prof. Dr. Burak **GEMALMAZ**, İstanbul Üniversitesi, Hukuk Fakültesi
Müh. M. Ayyüce **KIZRAK**, Yapay Zeka Araştırmacısı

Editörler

Av. Selin **ÇETİN**
Av. Elif **BABAN**
Stj. Av. Betül **ÇOLAK**

İstanbul Barosu

Bilişim Hukuku Komisyonu

Yapay Zeka Çalışma Grubu

2020


1878
İSTANBUL BAROSU
YAPAY ZEKA
ÇALIŞMA GRUBU
BİLİŞİM HUKUKU
KOMİSYONU

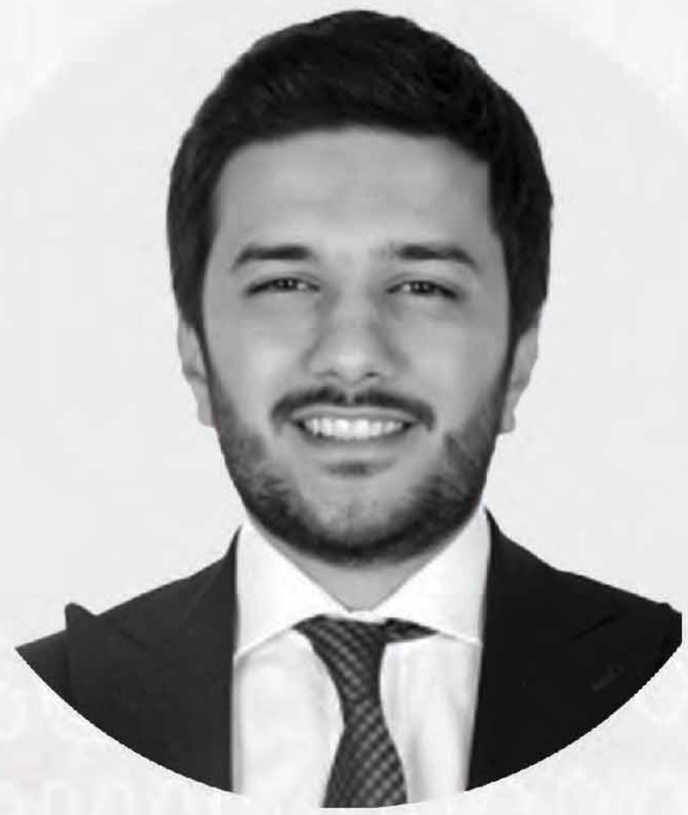
2020

YAZARLAR

Av. Can Sözer

Bilkent Üniversitesi Hukuk Fakültesi'nden 2008 yılında mezun olmuştur. 2010 yılında Viyana Üniversitesi'nde Avrupa ve Uluslararası Ticaret Hukuku dalında tezli yüksek lisansını, 2011 yılında İstanbul Bilgi Üniversitesi'nde İşletme Yönetimi dalında ikinci yüksek lisansını tamamlamıştır. 2010 yılından bu yana bünyesinde bulunduğu Esin Avukatlık Ortaklığı'nda halihazırda bilişim teknolojileri ve iletişim, uluslararası ticaret hukuku ve sağlık hukuku alanlarında kıdemli avukat ve ekip lideri olarak çalışmaktadır. İş dünyasının önemli sivil toplum kuruluşları bünyesinde çeşitli komitelerde görev almakta ve İstanbul Barosu'na kayıtlı olarak avukatlık mesleğini icra etmektedir.

Av. Yiğit Acar



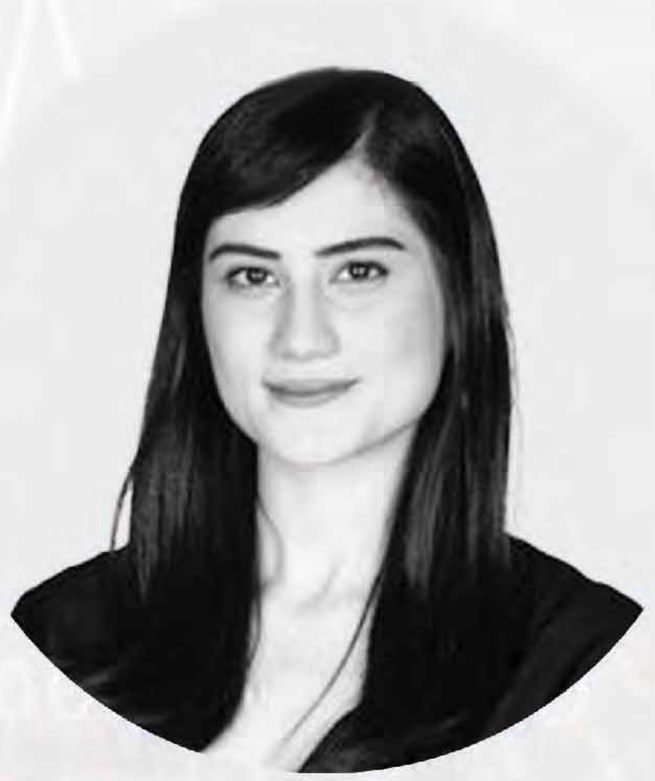
2014 yılında Kabataş Erkek Lisesi'nden, 2018 yılında İstanbul Üniversitesi Hukuk Fakültesi'nden mezun olmuştur. Meslek hayatına Esin Avukatlık Ortaklığı'nda devam eden Yiğit Acar, bilişim teknolojileri ve iletişim, uluslararası ticaret hukuku ve sağlık hukuku alanlarında çalışmaktadır ve İstanbul Barosu'na kayıtlı olarak avukatlık mesleğini icra etmektedir.

YAZARLAR

Av. Tuğrul Sevim

BTS&Partners ortağı olarak, ödeme sistemleri ve finansal sistemlerin yanı sıra kompleks BT ve telekomünikasyon sözleşmelerinde (geliştirme, lisanslama, entegrasyon, dış kaynak), e-ticaret ve internet ile ilgili yasal sorunlar ile kişisel verilerin korunması ve kompleks BT davalarında uzmanlaşmıştır. Av. Sevim, müvekkillere fikri mülkiyet portföylerinin yönetimi ve bu kapsamda gerekli sözleşmelerin hazırlanması ile ilgili hizmetleri sunmaktadır. Av. Sevim'in müvekkilleri arasında ödeme kuruluşları, yönetim danışmanlığı şirketleri, teknoloji ve dış kaynak hizmet şirketleri, telekom şirketleri, finans şirketleri, yazılım ve donanım sağlayıcıları ile diğer BT sektör oyuncuları yer almaktadır. Av. Sevim aktif olarak çeşitli önemli sivil toplum kuruluşlarında ve akademik enstitülerde teknoloji ve hukuki konularda danışmanlık hizmetleri sunmaktadır.

Av. Selen Zengin



İstanbul Bilgi Üniversitesi'nden mezun olmuş ve 2017 yılında BTS&Partners'da çalışmaya başlamıştır. Av. Zengin kişisel verilerin korunması, elektronik haberleşme, siber güvenlik, hukuk teknolojileri, e-ticaret, internet ve fikri mülkiyet hakları ile ilgili konularda hukuki danışmanlık çalışmalarını sürdürmektedir.
BTS & Partners'daki çalışmalarına Türkçe, İngilizce ve Fransızca olarak devam etmekte; ulusal ve uluslararası müvekkillerine hizmet sunmaktadır.

YAZARLAR

Av. Ceren Küpeli

Marmara Üniversitesi'nde Hukuk lisans eğitimi akabinde İstanbul Üniversitesi Hukuk Fakültesi'nde Kamu Hukuku yüksek lisansını tamamlamış, yüksek lisansı akabinde Johns Hopkins University Data Foundations nanodegree derecesini almıştır. EY Türkiye ve Turkcell hukuk müşavirliği akabinde Küpeli Hukuk ve Danışmanlık firmasını kurmuştur. Halihazırda İstanbul Üniversitesi-Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü'nde doktora eğitimine devam etmekte olan Küpeli, Marmara Üniversitesi ile Bahçeşehir Üniversite'sinde bilişim hukuku alanında misafir öğretim görevlisidir.

Av. Gülşah Deniz-Atalar

Lisans eğitimini Ankara Üniversitesi Hukuk Fakültesi'nde, yüksek lisansını Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Fikri Mülkiyet Hakları, Teknoloji Politikaları ve İnovasyon Yönetimi ana bilim dalında "İnovasyon ve Girişimcilik Kavramları Çerçevesinde Türkiye'de Sosyal İnovasyon ve Basvurulacak Hukuk" bitirme projesi ile tamamlamıştır. Ankara Barosu'na kayıtlı olarak avukatlık mesleğini sürdürmektedir. 2006 yılından beri dönem dönem Ankara Barosu Bilişim Kurullarında faaliyet göstermiştir. İnternette ifade özgürlüğü, erişim engellemeler ve online itibar yönetimi konularında dersler vermektedir. Özellikle yasama faaliyetleri kapsamında teknoloji politikaları alanında siyasi çalışmaları bulunmaktadır. Son dönemde çalışmaları dijital gözetim, yapay zeka ve etik konularında yoğunlaşmıştır. Ankara Barosu Bilişim, Teknoloji ve Hukuk Kurulu Başkan Yardımcısıdır.

GİRİŞ

Gülşah Deniz Atalar

"Quis custodiet ipsos custodes"[1]

(Gözetleyenleri kim gözetleyecek?)

Türkiye'nin ilk hukuk ve yapay zekâ kesişimini ele alan **Yapay Zekâ Çağında Hukuk** raporunu müteakiben kaleme alınan elinizdeki *İkinci Yıllık Rapor*, tüm dünyada etkileri hızla görülen Covid-19 pandemisi döneminde işçi-işveren ilişkilerinde gözetleme konusunu değerlendirmeyi hedeflemektedir. Teknolojinin gelişmesiyle beraber işyeri uygulamalarında yaşanan dönüşümler gözetim ve takip konularında sorunlar yaşatırken, bilfiil tecrübe ettiğimiz uzaktan çalışma modeli başka dönüşümleri zorunlu kıldığı gibi birçok soru ve sorunu da beraberinde getirmektedir. Bu nedenle İkinci Rapora, İlk Raporda yer alan ve **Av. Mehmet Ali Köksal** tarafından kaleme alınan "*Çalışanların Gözetlenmesi ve Yapay Zekâ*" başlıklı bölümün sonuç kısmı ile başlamanın, raporların birbirine olan bağlılığını ortaya koyma açısından faydalı olacağını düşünüyoruz.

"Bir iş ilişkisi kapsamında işverenin yönetim ve denetim yetkisi altına giren bir işçinin kendisine tanınan hak ve özgürlükleri işyeri sınırları içinde de varlığını sürdürmektedir. Ancak işçinin özel hayatının gizliliği ile kişiliğinin korunması gerekliliği, işçinin işyerinde bulunduğu sürece daralmaktadır. Bununla beraber işverenin bu haklar üzerinde mutlak bir yetkisi bulunmamaktadır. İşveren sadece işyerinin yönetimi açısından sınırlı olarak ve bazı koşulları yerine getirmek kaydıyla işçilerinin özel hayatları üzerinde denetim sağlayabilir. Bu noktada en önemli husus, işverenin işyerinde işçilerinden habersiz gizli izleme ve gözetleme yapamayacağıdır[2]."

Covid-19 pandemisinin yarattığı işyeri dönüşümleri, işverenlerin uzaktan çalışan işçileri hızla gelişen teknolojik aygıtlar yardımı ile gözetim altında tutmalarının önünü açmıştır. Önceden sadece işyeri olarak nitelendirilen mekanlarda mümkün olan bu gözetim, aynı anda özel hayattaki kişisel alanlara yayılmıştır. **Jeremy Bentham**'ın *Panoptikon gözün iktidarı* kitabında "(...) *Buna göre işin özü, iyi bilinen, etkili görünmeden gözetleme mekanizmasıyla birleşen gözetleyicinin konumunun merkeziliğinde yatmaktadır*(...)[3] " şeklinde mimarı olarak anlattığı etkili çalışan gözetimi, küreselleşen modern dünyada gelişen teknolojiler, internet iletişimi, araç ve uygulamaların erişebildiği verileri doğrultusunda gerçek bir görünmeden gözetlemeye dönüşmüştür. Ancak uzaktan çalışmanın gerçekleştiği alanların mahremiyet gerektiren alanlar olmasından hareketle bu gözetim mekanizmalarının denetlenmesi ve işverenin yönetim ve denetim yetkisini kötüye kullanmaması, işçinin ise uzaktan çalışma modeline adapte olabilmesi için üzerine düşen hak ve yükümlülüklerinin farkında olması gerekmektedir.

[1] *Detaylı bilgi için bkz. Quis Custodiet Ipsos Custodes? https://www.turkcebilgi.com/quis_custodiet_ipsos_custodes (Erişim Tarihi: 22.12.2020)*

[2] *KÖKSAL, Mehmet Ali, Yapay Zeka Çağında Hukuk, İstanbul Barosu, https://www.istanbulbarosu.org.tr/files/docs/Yapay_Zeka_Caginda_Hukuk2019.pdf, s.79. (Erişim Tarihi: 22.12.2020)*

[3] *BENTHAM, Jeremy, "Panoptikon Gözün İktidarı", (Çeviri: ÇOBAN, Barış &, ÖZARSLAN, Zeynep), 3.Baskı, Su Yayınları, İstanbul, 2019, s.*

A. DÖNÜŞEN İŞ YERİ UYGULAMALARI

Can Sözer & Yiğit Acar

Dönüşen iş yeri uygulamalarını irdelemek, öncelikle iş yeri kavramının tanımının yapılmasını gerektirir. İş yeri eskiden, dört duvarı ve çatısı bulunan, çalışanların haftanın beş günü mevcut bulunduğu, toplantıların fiziksel olarak yapıldığı gözle görülür bir yapıyı çağrıştırmaktaydı. Günümüzde iş yeri, telefon ve dizüstü bilgisayarımızın bulunduğu her yer olarak nitelendirilebilir durumdadır. Gerek iş için kullanılan teknolojilerin gelişmesi ve dijitalleşmenin önem kazanması gerekse dünyayı etkisi altına alan pandemi, iş yeri uygulamalarını değiştirdi ve dönüştürdü. İşveren ve çalışanların ayak uydurmaya çalıştıkları, birtakım fırsatlarla ve sorunlarla karşılaştıkları bu büyük dönüşüm, hukukçular için de yeni çalışma alanları yaratmaktadır.

1. İşe Alım Süreci

a. Başvuru

Çalışanın işverenle ilişkisi, işe alım sürecinden de önce, başvuru aşamasında başlamaktadır. Çalışan adaylarının iş ilanlarını gazete gibi geleneksel kanallar dışında elektronik ortamda bulunan farklı mecralar üzerinden görüntülediği ve incelediği günümüzde, başvurular da buna paralel olarak yalnızca fiziksel olarak kâğıt üzerine basılı formatta değil, bu elektronik mecralar üzerinden de yapılabilmektedir. Bu mecralar, *e-posta* gibi iletişim kanalları, kariyer temalı internet siteleri veya işverenlerin sosyal medya hesapları gibi mecralar olabilmektedir. Bu mecralardan bir ya da birden fazlasını tercih etmeyip kendi hazırladığı ve iş başvurularına özgülediği platformlar aracılığıyla iş ilanı ve başvuru süreçlerini yürüten işverenlerin sayısı da giderek artmaktadır. Söz konusu platformlar üzerinde işverenin detaylı soru formları ve testleri de bulunabilmektedir. Bu platformlar ile işverenler adeta bir çalışan adayı sadakati yaratmaya çalışmakta, çalışan adaylarının kabul edilmedikleri ilanlardan sonra çalışan adayları yine de iletişimde kalmak isterlerse güncel ilanlardan çalışan adaylarını haberdar edebilmektelerdir.

i. Başvuruların Değerlendirilmesi

Söz konusu platformlar veya diğer elektronik mecralar üzerinden toplanan başvuruları çoğunlukla işverenlerin İnsan Kaynakları alanında çalışan ilgili kişileri veya departmanları inceleyip eliyor olsa da bu elemede yapay zekâ teknolojilerinden yararlanan işverenler de mevcuttur. İşverenlerin kullandığı yapay zekâ teknolojileri, İnsan Kaynakları alanında çalışan kişiler için zaman ve efor tasarrufu sağlamaktadır. Bu yapay zekâ teknolojilerinin bazıları sohbet botlarını kullanarak çalışan adayı ile ilk görüşmeyi gerçekleştirmekte ve çalışan adayının açık olan pozisyona uygunluğunu değerlendirirken, bazıları işveren tarafından işe alındıkları takdirde en başarılı olacak çalışan adayının açık olan pozisyona uygunluğunu

değerlendirirken, bazıları işveren tarafından işe alındıkları takdirde en başarılı olacak çalışan adayını seçmeye çalışmakta, bazıları ise çalışan adayının diksiyonunu, konuşma tarzını ve yüz hareketlerini değerlendirip ideal aday olup olmadıklarına karar vermektedir[4]. Söz konusu yapay zekâ teknolojileri, işverenin kendisine öğrettiği kıstas ve kurallar üzerinden bir inceleme ve eleme gerçekleştirebilmekte veya bu inceleme ve elemeyi genel geçer istatistiki bilgiler üzerinden de yapabilmektedir. Bu durum bazı örneklerde yapay zekânın yaptığı seçimlerde belli etnik grupların, yaş gruplarının veya cinsiyetin diğerlerine tercih edildiği sonuçlar ortaya çıkarmış, işverenleri yapay zekânın önyargısı ile karşı karşıya bırakmış ve tartışma konusu olmuştur. Bu tür istenmeyen önyargılı sonuçlara ulaşan yapay zekâ teknolojilerinin önyargısını kırmaya ve objektif sonuçlara ulaşmasına yardım etmeye çalışan yazılımlar da üretilmektedir.

ii. İşe Alım Sürecinin Unsurları

Küçük ve orta ölçekli işletmeler ile yeni girişimler daha kısa süren ve daha hızlı sonuçlanan işe alım süreçlerini tercih ederken, büyük işletmeler, holdingler ve bilhassa çok uluslu şirketler daha uzun süren, daha yavaş sonuçlanan, içinde denemeye, sorgulamaya ve hatta pratiğe dönük öğeler içermekte olan birçok unsuru barındıran detaylı süreçleri tercih etmektedir. Süreçlerin uzunluğu çok uluslu şirketlerde bürokratik karar verme mekanizmalarının varlığı ve/veya işe alım kararlarının yurt dışında ve merkezi bir şekilde veriliyor olması gibi sebeplerden de kaynaklanabilmektedir. Çalışan adayıyla yalnızca tek bir görüşmenin yapıldığı hızlı işe alım süreçlerine artık neredeyse rastlanmamakta, çok aşamalı süreçlerin sayısının arttığı gözlemlenmektedir. Bu çok aşamalı süreçlerde çalışan adayları sözlü, yazılı, toplu, gruplar halinde ve bire bir pek çok mülakattan ve testten geçmekte, bilgi, beceri ve deneyimlerini işverene gösterebilmek için rekabetçi bir ortamda uğraş vermektedirler. Süreçteki bazı mülakat ve testler yüz yüze gerçekleştirilirken bazıları elektronik ortamdaki haberleşme araçları vasıtasıyla gerçekleştirilmektedir. Gerçekleştirilen bu testlerin bazı grup insanları dışladığına yönelik birtakım tartışmaların mevcut olduğu, örneğin *Amerika Birleşik Devletleri*'nde azınlık grupların testlerde genele göre daha başarısız olduklarının tespit edilmiş olduğu ve bunun işe alım sürecinde çalışan adaylarını teste tabi tutan işverenler nezdinde azınlık gruplara mensup çalışan adaylarını daha dezavantajlı konumda bıraktığı ileri sürülmektedir[5].

iii. İşe Alım Sürecinde Kişisel Veriler

Aşamaları sayıca artan ve sonuca ulaşma süresi gittikçe uzayan işe alım süreçleri işverenlerin çalışan adayı ile ilgili topladığı ve işlediği kişisel verilerin yoğunluğunu ve çeşidini de artırmaktadır. Geleneksel olarak nitelendirilebilecek bir işe alım sürecinde çalışan adayından toplanan veriler çoğunlukla özgeçmiş içerisinde yer alan bilgiler (*fotoğraf, kimlik bilgileri, mesleki geçmiş ve eğitim geçmişi gibi*), referans bilgisi ve adli sicil kaydı gibi bilgilerden ibarettir.

---

[4] *RAUB, McKenzie, Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices, Arkansas Law Review, 71(2), 2018, s.529-570, https://core.ac.uk/download/pdf/215462495.pdf, (Erişim Tarihi: 22.12.2020)*

[5] *AUTHOR, David & SCARBOROUGH, David, Does Job Testing Harm Minority Workers? Evidence from Retail Establishments, The Quarterly Journal of Economics, 2008, s.219-277, http://economics.mit.edu/files/599, (Erişim Tarihi: 22.12.2020).*

Günümüzde işe alım süreçlerinde toplanan veriler bunun ötesine geçmekte, kişilik veya davranış analizi, ses ve/veya görüntü kaydı içeren sunumlar ve hatta özel nitelikli kişisel veri niteliğinde olan sağlık verisi veya dernek üyeliği verisi gibi veriler de işverenler tarafından çalışan adaylarından toplanabilmektedir. Çalışan adayının çalışacağı işyeri ortamı (ofis, fabrika, saha gibi) çalışan adayı ile ilgili toplanacak verilerin yoğunluğunu ve çeşidini etkileyebilmekte, örneğin fabrikalarda veya tehlikeli iş veya üretim sahalarında çalışacak kişilerden daha farklı içerik ve yoğunlukta kişisel veriler toplanması gerekebilmektedir. Bilhassa gelişmekte olan iş sağlığı ve güvenliği uygulamaları ve ilgili mevzuat, bu tür yerlerde çalışacak kişilerden çok çeşitli sağlık bilgilerinin toplanmasını zorunlu kılmaktadır. Doğrudan çalışan adaylarından toplanmamakla birlikte, gerek iş başvurularının incelenmesi ve elenmesi aşamasında gerekse işe alım sürecinde çalışan adayına ilişkin, insan kaynakları ve/veya işe alımı yapan iş biriminin ilgili çalışan adayı hakkındaki gözlem, izlenim ve düşüncelerini yansıtan notları ve değerlendirmeleri de söz konusu çalışan adayı ile ilgili kişisel veri niteliğindedir.

iv. İşe Alım Sürecinde Kişisel Verilerin Yurtdışına Aktarılması

Çok uluslu şirketlerin bazılarının işe alım ile ilgili karar mekanizmalarının yurt dışında yerleşik üst veya kardeş şirketler olması, çalışan adayı ve sonraki aşamada çalışan verilerinin Türkiye'de yerleşik işveren tarafından yurt dışına aktarılmasını gerektirmektedir[6]. Kimi zaman kişisel veri Türkiye'de yerleşik bir işveren tarafından yurt dışına aktarılmamakta, doğrudan yurt dışındaki şirketin yönettiği iş başvuru platformu aracılığıyla yurt dışında toplanmaktadır. İşe başvuru ve alım prosedürlerine ek olarak, çalışanın işverenin bünyesinde çalıştığı süre boyunca deneyimlediği performans değerlendirmesi, terfi ve yan hakların tespiti gibi bazı İnsan Kaynakları uygulamaları da doğrudan yurt dışından yönetilebilmektedir. Yurtdışına aktarılan veya yurt dışında toplanan kişisel veriler, işverenlerin yurt dışında yerleşik üst veya kardeş şirketleri haricinde, üçüncü taraf hizmet sağlayıcıların sunucularında ve bulut sistemlerinde de saklanabilmekte ve işlenebilmektedir. Örneğin, işe alım sürecinde elektronik ortamdaki haberleşme araçları vasıtasıyla gerçekleştirilen mülakatların çoğunda çalışan adaylarının görüntü ve ses kayıtları yurt dışında toplanmaktadır. Çalışan adayı ve çalışan adaylarının kişisel verilerinin yurt dışına aktarılması, kişisel verilerin korunması hukuku anlamında aydınlatma ve açık rıza gibi birtakım aksiyonların alınması zorunluluğunu beraberinde getirmektedir.

v. İşe Alım Sürecinde Sözleşmelerin İmzalanması

İşe alım sürecinin sonunda işverenin çalışan adayını işe alma kararını vermesi üzerine işverenle çalışan adayı arasında iş sözleşmesi imzalanmakta ve çalışan adayı çalışan statüsünü kazanmaktadır. Geleneksel işe alım sürecinde yalnızca iş sözleşmesinin imzalanması yeterli iken günümüzde işveren tarafından çalışan adayına imzalatılmak istenen pek çok başka belge ile karşılaşılmaktadır. Bu belgelere işverenin kişisel verilerin korunması hukuku anlamında çalışana imzalatma gerekliliği ile karşı karşıya kaldığı belgeler, işverenin

[6] *Yurtdışına veri aktarımınına ilişkin detaylı bilgi için bkz. DÜLGER, M. Volkan, "Kişisel Verilerin Korunması Hukuku", 2. Baskı, Hukuk Akademisi, İstanbul, 2019, s.328.*

şirket politikaları doğrultusunda çalışana imzalatmak istediği, rüşvet karşıtı uygulamalara, şirket davranış kurallarına, çeşitlilik ve kapsayıcılık ile ilgili politikalar ve/veya cihaz/araç teslimine ilişkin belgeler örnek verilebilir. İmzalatılan belgelerin sayısı artarken, söz konusu belgelerin imzalanma yöntemi de değişiklik gösterebilmektedir. Geleneksel işe alım sürecinde iş sözleşmesi ve diğer belgeler ıslak imza ile imzalanırken günümüzde işverenler e-imza ve mobil imza gibi elektronik süreçleri de tercih edebilmektedirler. Söz konusu belgelerin onay ifadeleri ve/veya kutucuklar ile onaylanmasına özgülenmiş elektronik platformların kullanılması da mümkün olmaktadır. E-imza uygulamalarının işverenlerce daha sık kullanılmaya başlanması, hukukumuzdaki basit e-imza ve güvenli e-imza ayrımının işverenlerce dikkatlice incelenmesi gerekliliğine işaret etmektedir.

2. İş yerine Giriş Kontrolü

i. İş yerine Giriş Kontrolü Mekanizmaları

İş yerlerinde çalışan sayılarının artışı ve bilhassa plaza binalarında ve iş yeri komplekslerinde çok sayıda şirketin işyerinin bir arada bulunuyor olması, iş yeri ve çalışan güvenliği açısından işvereni yeni iş yerine giriş kontrolü mekanizmaları arayışına itmiştir. İş yerine giriş kontrolü geleneksel olarak çalışanı tespit ve teyit etme amaçlı kimlik ve/veya isim kontrolü, şifre ile giriş veya kartlı geçiş sisteminden ibaret iken günümüzde iş yerine giriş kontrolü denilince parmak izi, avuç içi izi, retina taraması ve yüz taraması gibi farklı uygulamalar da akla gelmektedir. Çalışanlar haricinde iş yerine girmesi gereken ziyaretçiler (tedarikçi çalışanı veya müşteri gibi) için ise daha ziyade isim kaydı, kimlik alıkonulması ve kart verilmesi gibi geleneksel yöntemler tercih edilmektedir. İş yerine giriş kontrolünde güvenlik görevlisi ve/veya resepsiyonist gibi kişilerin şahsen gerçekleştirdikleri kontrol uygulamalarına ek olarak yapay zekâyı kullanan algılama ve tanıma teknolojileri de sıklıkla kullanılmaya başlanmıştır.

ii. İş yerine Girişte Toplanan Kişisel Veriler

İş yerine giriş kontrolü mekanizmaları geleneksel olarak çalışanın veya ziyaretçinin ismi, soy ismi, ziyaret tarihi ve saati gibi bazı kişisel verilerin toplanmasını içerir. Ziyaretçiler için buna ek olarak ziyaretçinin çalıştığı kurum ve unvanı gibi kişisel veriler de toplanmaktadır. Birtakım güvenlik gerekçeleri ile T.C. kimlik numarası ve/veya imza toplayan iş yerlerine de rastlanmaktadır. Hatta üretim tesislerinde ve şirket merkezlerinde tedarikçi çalışanlarından iş yeri girişinde adli sicil kaydı toplanması yönünde yaygınlaşan bir uygulama da gözlemlenmektedir. Değişen uygulamalarla birlikte, parmak izi, avuç içi izi, retina taraması ve yüz taraması gibi biyometrik veri olarak sayılabilecek özel nitelikli kişisel veri niteliğindeki veriler de toplanmakta[7], bu veriler gerek yurt içinde gerekse yurt dışında sunucularda ve bulut hizmetleri üzerinde saklanmaktadır. Giderek yaygınlaşan başka bir uygulama da görüntü ve/veya ses kaydı alabilen güvenlik kameralarının iş yeri girişlerinde

[7]Özel nitelikli kişisel verilerin işlenme şartları ile ilgili detaylı bilgi için bkz. KÜZECİ, Elif, "Kişisel Verilerin Korunması", 3. Baskı, Turhan Kitabevi, Ankara, 2019, s. 246; AYÖZGER ÖNGÜN, Çiğdem, "Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil", 2. Baskı, Beta Yayınları, İstanbul, 2019, s.24.

konumlandırılması ve iş yeri giriş kontrolüne ilişkin düzenli olarak kayıt almasıdır. Tüm bu ve benzeri verilerin işveren tarafından toplanması ve işlenmesi, kişisel verilerin korunması hukuku anlamında işverenin birtakım yükümlülüklerini gözden geçirmesini gerektirmektedir.

iii. İş yerine Girişte Toplanan Kişisel Sağlık Verileri

Pandemi süreci, işverenler tarafından iş yeri girişlerinde çalışanların ve/veya ziyaretçilerin ateş ölçümlerinin yapılmasını gündeme getirmiştir ve bu uygulama kısa zamanda neredeyse her sektörde yaygınlaşmıştır. Söz konusu ateş ölçümleri ısı ölçen kameralar veya manuel olarak ateş ölçüm cihazlarıyla yapılmaktadır. Kimi işverenler ateş ölçümlerini isim, soy isim, ziyaret tarihi ve saati gibi başka kişisel verilerle birlikte kâğıt ortamında veya elektronik ortamda kayıt etmekte, kimi işverenler ise yalnızca anlık ölçümler ile yetinmekte ve herhangi bir kayıt faaliyeti gerçekleştirmemektedir. Ateş ölçümü neticesinde belli bir değerin üzerinde ateşi olduğu tespit edilen kişiler uyarılmakta, iş yerlerine alınmamakta ve/veya sağlık kuruluşlarına yönlendirilmektedirler. Ateş ölçümü, gerçekleştirilen uygulamanın kapsamına göre işverenleri aydınlatma yükümlülüğünün yerine getirilmesi ve/veya açık rıza alınması gibi bazı aksiyonlara itmiştir.

3. İş yeri İçerisinde Gözetim

i. Çalışanların Gözetimi

İş yeri içerisinde gözetim geleneksel olarak, iş yeri ve çalışan güvenliğinin sağlanması bakımından çalışanların fiziksel olarak şahsen izlenmesi ve görüntü ve/veya ses kaydı alabilen güvenlik kameralarının iş yerinin içerisinde muhtelif yerlere konumlandırılarak gözetim faaliyetinin bu kameralar tarafından gerçekleştirilmesinden ibarettir. Günümüzde çalışanların gözetimi yalnızca kameralar aracılığıyla görüntü alınmasına değil, aynı zamanda alınan görüntüleri irdeleyip anlamlandırabilen ve çalışanın performansı ve ruhsal durumu hakkında birtakım sonuçlara ulaşabilen yapay zekâ teknolojilerine de işaret etmektedir. Örneğin, bir çalışanın çalıştığı üretim tesisinde her gün ruhsal durumunun yüz mimikleri ve jestleri aracılığıyla tespit edilmesi, şirketin ilgili üretim tesisindeki çalışma verimini artırmak adına ilgili çalışanla ilgili birtakım aksiyonlar almasını elverişli kılmaktadır. Benzer bir şekilde alınan görüntüleri analiz eden yapay zekâ teknolojileri aracılığıyla çalışanın koruyucu donanım takıp takmadığı kolayca tespit edilebilmekte ve takmadığı takdirde uyarılabilmektedir[8]. Yapay zekâ teknolojileri ayrıca, çalışanın ihtiyaç molalarının sayısını ve sıklığını tespit etmek, çalışanların telefonla veya işyeri içerisinde birbirleriyle konuşurken kullandıkları seslerini analiz ederek o günkü stres düzeylerini tespit etmek ve çalışanın gönderdiği e-postaların içeriğini analiz ederek çalışma isteği ve motivasyonunu tespit etmek gibi başkaca alanlarda da kullanılmaya başlanmıştır.

Çalışanın e-postalarının izlenmesi ve analiz edilmesi yalnızca çalışma isteği ve motivasyonunu tespit etmek için değil, şirket içi soruşturmalar kapsamında bir veya birden fazla çalışan tarafından iddia edilmiş bulunan bir hukuka aykırılığın tespit edilmesi veya

[8] *ZUECO, Irine, Will AI Solve Your Workplace Safety Problems? Prosapien, 2020, (https://www.pro-sapien.com/blog/ai-solve-safety-problems/, (Erişim Tarihi: 22.12.2020)*

çalışanların birbirleriyle, işveren şirketin distribütörleriyle veya rakipleriyle rekabeti kısıtlayıcı ve önleyici yazışmalarda bulunup bulunmadıklarının tespiti için de gerçekleştiriliyor olabilir. Söz konusu izleme işverenin böyle bir izleme faaliyeti ile görevlendirdiği bir veya birden fazla çalışanı veya dışarıdan destek alınan bir şirket veya hukuk bürosu tarafından da gerçekleştirilebileceği gibi, yapay zekâ teknolojileri kullanılarak da gerçekleştirilebilir. Çalışanın e-postalarına ek olarak, işvereni tarafından profesyonel olarak kullanımı için kendisine verilmiş olan mobil cihaz ve dizüstü bilgisayar gibi aygıtlar üzerinde kaydettiği dosyalar ile mesajlaşma uygulamaları üzerinden de izleme faaliyetleri gerçekleştirilebilmektedir. Gerçekleştirilen bu izleme faaliyetleri doğrultusunda çalışan ile ilgili birtakım kapsamlı değerlendirmeler yapılabilmekte ve hatta İnsan Kaynakları anlamında birtakım aksiyonlar da alınabilmektedir.

İş yeri kavramının sınırlarının genişlediği günümüzde çalışanın gözetimi, fiziksel kameraların yanı sıra, işveren tarafından çalışanın iş amaçlı kullanımı için çalışana verilen cep telefonu ve tablet gibi mobil cihazlar aracılığıyla da gerçekleştirilebilmektedir. Günümüzde yaygınlaşan bir başka uygulama da mobil cihazlara uygulama olarak indirilebilen ve çalışanların afet gibi acil durumlarda tek tuşla yardım isteyebildiği veya yine tek tuşla güvende olduğunu bildirebildiği yazılımlardır. Bilhassa saha veya mağaza çalışanı fazla sayıda olan şirketlerin bu tür yazılımları, çalışan güvenliğini sağlamak ve veri akışını hızlandırmak adına, yaygın olarak kullanmaya başladığı gözlemlenmektedir.

İşverenler tarafından gerek çalışanlarının, sözleşmeli çalışanlarının ve stajyerlerinin gerekse taşeron firmaların bordrosunda bulunan ve işverenin bordrolu çalışanı konumunda olmayan kişilerin çalışma sıklıklarını ve sürelerini denetlemek için kullandıkları zaman ölçüm yazılım ve cihazlarının kullanımı da yaygınlaşmakta, bu kişilere yapılan ödemeler ve zaman olarak bu ödemelerin karşılığının alınıp alınmadığı hususu işverenler tarafından sıkı bir şekilde denetlenebilmektedir[9]. Buna ek olarak, çalışanın mesai saatleri içerisinde iş bilgisayarında veya mobil cihazında yüklü olan tarayıcı üzerinden ziyaret ettiği internet sitelerinin gerek çalışan verimliliğini yüksek bir seviyede tutmak gerekse hukuka ve/veya ahlaka aykırı içerik barındıran internet sitelerinin ziyaret edilmesini önlemek amacıyla izlenmesi ve kaydının tutulması da söz konusu olabilmektedir[10]. Ülkemizde de ilgili yüksek mahkeme kararları incelendiğinde, işverenlerin kendilerine ait çalışanlarca kullanılan bilgisayar ve elektronik e-posta adresleri inceleme yetkisi bulunduğu kabul edilmektedir. Bununla beraber, aşağıda detaylıca açıklanacağı üzere, bu yetkinin hukuka uygun ve ölçülü olarak kullanılması ile çalışanların temel hak ve özgürlüklerine riayet edilmesi gibi hususlara ayrıca dikkat edilmesi gerekmektedir[11].

[9]MATEESCO, Alexandra & NGUYEN, Aiha, Explainer: Workplace Monitoring & Surveillance, Data & Society, 2019, s.1-18, https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf, (Erişim Tarihi: 22.12.2020).
[10]SRHM, Managing Workplace Monitoring and Surveillance, SRHM, 2019, https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx, (Erişim Tarihi: 22.12.2020)
[11]Yargıtay, 22. HD. 1.9.2016, E. 2016/6321, K. 2016/13143.

Çalışanların artan bir şekilde yapay zekâ teknolojileri kullanılmak suretiyle izlenmelerinin çalışan üzerinde strese ve gerek fiziksel gerek psikolojik bazı stres kaynaklı sağlık sorunlarına yol açabileceği ileri sürülmüştür. Buna ek olarak, artan çalışan gözetimi uygulamalarının kişisel verilerin korunması ve özel hayatın gizliliği üzerindeki etkileri de akademisyenler ve yazarlar tarafından sıklıkla tartışılmaktadır. Bununla beraber, çalışanların izlemeye tabi tutulacakları yönündeki beklentilerinin teknolojinin gelişimi ve iş yaşamının evrimi ile doğru orantılı bir şekilde arttığı ve bu tür izlemeleri olağan karşılamaya başladıkları yönünde argümanlar da dile getirilmiştir. Güvenlik kameralarından e-posta izleme faaliyetlerine kadar geniş bir spektrumda karşılaşabildiğimiz söz konusu izleme faaliyetlerine ilişkin olarak birtakım hukuki düzenlemeler getiren veya yüksek mahkemeleri bu konuda çeşitli kararlar veren ülkeler mevcuttur.

Bu tür hukuki düzenlemelerde ve mahkeme kararlarında gerek işverenin hukuken korunabilir menfaatleri gerekse çalışanların gizliliği, özel hayata saygı ve kişisel verilerinin korunmasını isteme hakları dikkate alınabilmektedir [13] [14] [15] . **Avrupa İnsan Hakları Mahkemesi (AİHM)** mesleki hayatın özel hayat kavramı dışında tutulmaması gerektiğini ve bireylerin kimliğini oluşturmasının ve sosyalleşmesinin önemli bir aracı olan dış dünyayla ilişki kurma hakkını bireyin iş çevresini de kapsadığını ifade etmektedir[16]. İş yerinde gözetime ilişkin olarak **AİHM**, *Bărbulescu/Romanya* kararında çalışanın iletişiminin işveren tarafından denetlenmesinde dikkate alınacak hususları belirlemiş, bu kapsamda işverenin denetleme yöntemleri hakkında çalışanı önceden bilgilendirip bilgilendirmediği, yapılan incelemelerin kapsamı ile iletişimin denetlenmesi sürecinde çalışanın mahremiyetine ne ölçüde müdahale edildiği gibi hususların ayrıca gözetilmesi gerektiğini ifade etmiştir[17].

Anayasa Mahkemesi de konu ile ilgili yakın tarihli bir kararında, işyerinde gerçekleştirilen gözetim faaliyetleri bakımından benzer ilkelerin altını çizmiş, çalışanların bilgilendirilmesi, temel hak ve hürriyetler ile müdahalenin kişi üzerindeki sonuçları arasında bir denge gözetilmesi, bu anlamda amaçla bağlantılı, sınırlı ve ölçülü müdahalede bulunulması ve istenilen amaca başka yöntemlerle ulaşılıp ulaşılamayacağı gibi kriterlerin değerlendirilmesi gerektiğini belirtmiştir[18] .

---

[12]*BOEHMER, Robert G., Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise form the Modern Sweatshop, DePaul Law Review, 41(3), 1992, s.739-819, https://core.ac.uk/download/pdf/232967416.pdf, (Erişim Tarihi: 22.12.2020).*

[13]*PALLOT, Libby & KENNEDY, Russell, Australia, Debate over Use of Surveillance Shifts in Employers' Favor, SRHM, 2018, https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/global-australia-surveillance.aspx, (Erişim Tarihi: 22.12.2020)*

[14]*GARNER, E., Germany: Employee Monitoring Ruled Unlawful, SRHM, 2017, https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/germany-employee-monitoring-unlawful.aspx, (Erişim Tarihi: 22.12.2020)*

[15]*THOMPSON, Sarah & WOODS McGuire, EU Court: Employee E-mail Monitoring May Not Breach Privacy Rights, SRHM, 2016, https://www.shrm.org/resourcesandtools/legal-and-complance/employment-law/pages/germany-employee-monitoring-unlawful.aspx, (Erişim Tarihi: 22.12.2020)*

[16]*AİHM, Nietmiz/Almanya, B. No: 137/1088, 16/12/1992; Özpınar Türkiye, B. No: 20999/04, 19/10/2010; Campagnano/İtalya, B. No: 77955/01, 23/3/2006,)*

[17]*AİHM, Bărbulescu/Romanya [BD], B. No: 61496/08, 5/9/2017*

[18]*AYM, B. No 2016/13010, 17/9/2020*

ii. Çalışanların Araçlarda Gözetimi

Yukarıda anılan cihazlara ek olarak, yalnızca gözetim amacına özgülenmiş özel cihazlar da mevcuttur[19] ve bilhassa çalışana iş amacıyla veya yan hak olarak tesis edilmiş şirket araçlarında yaygın olarak kullanılmaktadır. Bu cihazlar güzergâh, konum, yakıt tüketimi, mola noktaları, mola süresi ve hatta sürüş tekniği gibi bilgileri kaydedebilmektedir[20]. Söz konusu araçların içine ve dışına yerleştirilen kameralar da aynı şekilde kayıt alabilmekte, araç süren çalışanın emniyet kemeri takıp takmama durumunu veya trafik kurallarına riayet edip etmiyor oluşunu tespit edebilmektedir. Araçlardan toplanan bilgiler çalışanlar ile ilgili İnsan Kaynakları süreçlerine konu edilebilmekte, bu bilgiler neticesinde çalışan hakkında olumlu veya olumsuz birtakım değerlendirmeler yapılabilmekte ve kararlar verilebilmektedir.

Sonuç olarak, yukarıda çeşitli uygulama örnekleri ile açıklandığı üzere, gelişen teknolojilerin işverenler tarafından işçiler üzerinde sürekli bir gözetim amacıyla tercih edilmesi, işçilerin mahremiyet hakkı ve buna bağlı olarak veri koruma hakkını sınırlayabilmektedir. Özellikle COVID-19 salgını sürecinde farklılaşan çalışma modellerinin bu gözetim eğilimini artırdığı görülmekte ve bu çerçevede iş yerinde gelişen teknoloji kullanımının yeniden gözden geçirilmesi ihtiyacı ortaya çıkmaktadır.

B. COVID-19 PANDEMİ SÜRECİNDE İŞ YERİ UYGULAMALARI VE TEKNOLOJİ KULLANIMINA ÖZGÜ RİSKLER VE TAVSİYELER

Tuğrul Sevim & Selen Zengin

COVID-19 salgını, kamu kurum ve kuruluşlarının yanı sıra özel sektör iş yerlerini de çalışanlarının ve iş ilişkisi içinde bulunduğu üçüncü tarafların sağlığının korunması amacıyla tedbirler uygulamaya yöneltmiştir. Kamu sağlığının korunması amacıyla alınan önlemler özel sektör iş yerlerinde, iş yerinde fiili çalışmaya tamamen veya kısmen ara verilmesini ve uzaktan çalışma modeline geçilmesini gerektirmiştir. Üretim ve operasyonel faaliyetlere mümkün olduğu ölçüde süreklilik kazandırılması adına iş yerinde farklı çalışma düzenlerini ve iş yeri uygulamalarını zorunlu hale getirmiştir. Önlemlerin temelinde iş yerinde veya işin gereği olarak iş yeri dışında yürütülen faaliyetlerde sosyal temasın azaltılması konumlandığından, işverenler olağan çalışma düzeninin yerini almaya veya mevcut çalışma düzeni içerisinde çalışan sağlığını korumaya elverişli teknoloji çözümlerine yönelmişlerdir.

Kullanım alanları özelinde bir ayrıma gidildiğinde bu teknoloji çözümlerini, uzaktan çalışma modeline özgü teknoloji çözümleri ve iş yerinde fiili çalışmaya devam edilmesi sebebiyle salgının önlenmesi için gerekli tedbirlere uyulmasını sağlamaya yardımcı çözümler olarak incelemek mümkün olabilecektir.

---

[19] *ARTICLE 29 DATA PROTECTION WORKING GROUP, Opinion 2/2017 on Data Processing at Work, Brüksel, 2017, s.12-13, https://ec.europa.eu/newsroom/document.cfm?doc_id=45631, (Erişim Tarihi: 22.12.2020)*

[20] *Boehmer, R. G., s.739-819.*

1. Uzaktan Çalışma Modeli Özelinde Dönüşen İş yeri Uygulamaları

10 Haziran 2003 tarih ve 25134 sayılı **Resmî Gazete'**de yayımlanarak yürürlüğe giren, 4857 sayılı İş Kanunu'nun 14'üncü maddesinde 2016 yılında yapılan değişiklikle[21] iş ve çalışma mevzuatına giren uzaktan çalışma kavramı, *işçinin, işveren tarafından oluşturulan iş organizasyonu kapsamında iş görme edimini evinde ya da teknolojik iletişim araçları ile iş yeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan iş ilişkisini* ifade edecek şekilde tanımlanmıştır. Bu tanım doğrultusunda, teknolojik araçların uzaktan çalışma ilişkisi anlamında iş görme ediminin yerine getirilmesine ilişkin unsurlarından biri olduğu sonucuna ulaşılmaktadır.

Uzaktan çalışma pratiğini mümkün kılan unsurlardan biri olmanın yanında, iş yerinde fiili çalışmadan uzaktan çalışmaya geçişi kolaylaştıran unsurların başında da dijitalleşmenin ve uygun teknolojik altyapı, cihaz ve araçların geldiği görülmektedir. Bu noktadan hareketle, küresel anlamda içinde bulunan olağan dışı çalışma koşullarına adaptasyonda halihazırda fiziksel ortamdaki iş süreçlerini dijital ortama taşımış ve operasyonel ihtiyaçlarına uygun teknoloji yatırımlarını gerçekleştirmiş olan iş yerlerinin stratejik bir avantaj kazandığı söylenebilecektir.

Uygun teknolojik araçlara sahip olmakla birlikte çalışanların bunların kullanımı için gerekli eğitimlere tabi tutulmadığı iş yerlerinde, yeni çalışma modelini uygulamaya geçişte, iş sürekliliğinin sağlanamamasının yanında, bilgi güvenliği ve kişisel verilerin korunması konularında da risklerle karşılaşılmıştır.

Bu risklerin tespiti ve uygulama önerilerinin değerlendirilmesi adına uzaktan çalışma ilişkisi çerçevesinde işverenlerce başvurulan teknolojik araçlar, kullanım amaç ve alanları özelinde bir ayrıma gidilerek ele alınmaktadır.

i. İletişim ve Haberleşme Odaklı Teknolojiler

Uzaktan çalışma modelini uygulayan iş yerleri bakımından en yaygın kullanım alanına sahip olan çözümlerin, çalışanların birbirleriyle ve iş ilişkisi içerisinde bulunulan üçüncü taraflarla haberleşme ve iletişiminin sürekliliğini sağlayan araçlar olduğu söylenebilecektir[22].

Söz konusu uygulamalar, kullanıcı gizliliğine ilişkin yüksek risk düzeyine sahip pratiklerinin yanı sıra, uygulama kullanıcısı konumunda olan iş yerleri özelinde ortaya çıkabilecek geniş ölçekli güvenlik risklerini de beraberinde getirebilecektir. Bilhassa uzaktan çalışma modeline geçen iş yerleri ile kullanıcı profilinde ciddi artış söz konusu olan bu uygulamaların, kullanıcı gizliliği ve güvenliğine ilişkin kurallarının titizlikle incelenmesi ve iş yeri organizasyonu için hassas nitelikteki bilgi ve belgelerin paylaşılmasında yeterli güvenlik seviyesini temin ettiğinden emin olunmaksızın, bu uygulamaların tercih edilmemesi tavsiye edilebilecektir[23].

[21] *İlgili değişiklik 20 Mayıs 2016 tarih ve 29717 sayılı Resmî Gazete'de yayımlanan 6715 sayılı İş Kanunu ile Türkiye İş Kurumu Kanununda Değişiklik Yapılmasına Dair Kanun'un 2'nci maddesi uyarınca yapılmıştır.*

[22] *LENONARDI, Paul. M., COVID and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work, Journal of Management Studies, 2020, s.1, https://onlinelibrary.wiley.com/doi/epdf/10.1111/joms.12648. (Erişim Tarihi: 02.02.2021)*

[23] *GOODYEAR, Michael, The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of U.S. Data Privacy Law, Houston Law Review, Vol. 10, No. 3, 2020, s.76- 97*

Nitekim, **Uluslararası Çalışma Örgütü'nün (ILO)** yayımlamış olduğu *COVID-19 Salgını Süreci ve Sonrasında Uzaktan Çalışmaya İlişkin Uygulama Rehberi*'nde video konferans, arama ve mesajlaşma uygulamalarının kullanım sıklığına dikkat çekilmiş; iş yeri organizasyonunda teknolojik çözümlerin ve araçların kullanıma ilişkin olarak, kurum içi teknoloji kaynağı ihtiyaçlarının belirlenmesi, çalışanların teknoloji yetkinlikleri doğrultusunda eğitimlerin verilmesi, kurum içi politikaların teknoloji araçlarını ve kullanıcı kişisel cihazlarını da kapsayacak şekilde belirlenmesi, çalışanlara gerekli teknik desteğin sağlanması, kişisel verilerin korunması konusunda eğitimlerin verilmesi ve kişisel verilerin korunmasına ilişkin düzenlemelere uyum sağlanması hususları vurgulanmıştır[24].

ii. Erişim Güvenliğine İlişkin Teknolojiler

İletişim ve haberleşme odaklı teknoloji çözümlerini ortak çalışma alanlarına ve kurumsal ağlara güvenli erişim sağlamaya elverişli teknolojilerin takip ettiği ifade edilebilecektir. Her ne kadar bilgi güvenliği yönetimine ilişkin kurumsal politika ve prosedürleri tatbik eden iş yerleri bakımından bu teknoloji çözümleri halihazırda kullanılıyor olsa da bilgi güvenliği, erişim yetki ve kontrolü, veri sınıflandırma, veri kaybı önleme, şifreleme ve anahtar yönetimi gibi konularda yerleşik güvenlik kuralları veya yeterli teknik altyapıya sahip olmayan şirketler bakımından da uygulama ihtiyacı gündeme gelmiştir.

Bu doğrultuda işverenlerin karşı karşıya kalabileceği güvenlik risklerinin, çalışanların kişisel cihazlarından belirli ortak alana, dizine, sisteme, uygulamaya vb. erişim sağlayabilmeleri adına geçici olarak yetki tanımlandığı durumlarda; çalışanların kurum içi güvenlik kuralları gereği yalnızca işverence tahsis edilen cihazlar vasıtasıyla erişim sağladığı durumlara kıyasla daha yüksek olacağını söylemek mümkündür[25]. Dolayısıyla, cihaz ve ağ güvenliğine ilişkin risklerin yönetilmesi amacıyla işverenler tarafından, kurum içi politika, prosedür ve kuralların oluşturulması ve bunların etkin bir şekilde yönetilmesine elverişli yapıların kurulması tavsiye edilebilecektir. Bunun yanında, kullanıcıların muhtemel güvenlik riskleri hakkında bilgilendirilmesi ve bu risklerin en aza indirgenmesini temin edecek tedbirlerin uygulanması konusunda düzenli eğitimlere tabi tutulması önem arz edecektir[26].

İşverenlerce ağ, uygulama ve kullanıcı cihazlarının güvenliğine ilişkin risklerin yönetilmesi amacıyla kurumsal politika ve prosedürlerin uygulamaya alınması ve mevcut güvenlik risklerine yönelik eğitim ve farkındalık artırıcı çalışmaların yapılmasına yönelik idari tedbirlerin alınmadığı durumlarda, 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("**6698 sayılı Kanun**") 12'nci maddesinde düzenlenen veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesine bağlı hukuki sonuçlar ile karşılaşılabilecektir. Nitekim, anılan madde

---

https://houstonlawreview.org/article/12850-the-dark-side-of-videoconferencing-the-privacy-tribulations-of-zoom-and-the-fragmented-state-of-u-s-data-privacy-law , (Erişim Tarihi: 02.02.2021)

[24] INTERNATIONAL LABOUR ORGANIZATION, Teleworking during the COVID-19 pandemic and beyond, A Practical Guide, 2020, s.15-37, https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_751232.pdf, (Erişim Tarihi: 22.12.2020)

[25] PRANGGONO, Bernardi & ARABO, Abdullahi, COVID-19 Pandemic Cybersecurity Issues, Internet Technology Letters, 2020, s.1-6, https://doi.org/10.1002/itl2.247, (Erişim Tarihi: 22.12.2020)

[26] Pranggono, B., & Arabo, A., s.4.

uyarınca veri sorumlularının kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almakla yükümlü oldukları düzenlenmiştir.

Uzaktan çalışma modeli gereği çalışanların kişisel cihazlarının iş amaçlı kullanılabileceği ve yeterli güvenlik standartlarını karşılamayan ağlar üzerinden kurum içi ortamlara erişim sağlanacağı göz önünde bulundurulduğunda, iş yeri dışındaki kişisel veri içeren elektronik ortam ve cihazlar bakımından da aynı güvenlik seviyesinin tesis edilmesi önem arz edecektir[27].

iii. Çalışanların Denetlenmesine Elverişli Teknolojiler

Uzaktan çalışma modeline geçişte işverenler tarafından, yönetim hakkı çerçevesinde işçinin fiilen çalışıp çalışmadığının veya kamu sağlığının korunması amacıyla alınan önlemlerin denetlenmesi gerekçeleriyle, özel hayatın gizliliğine müdahaleci yöntemlere de başvurulduğu görülmektedir. Çalışma saatleri içinde çalışan cihazlarındaki kameraların zorunlu olarak açık tutulmasına ve çalışanların cihazlarına yüklenen ve hatta doğrudan uzaktan erişim sağlanarak belirli aralıklarla fotoğraflarının çekilmesine ilişkin uygulamalar bu yöntemlere örnek olarak gösterilebilecektir[28].

Cihaz kameralarını açık tutma zorunluluğuna ilişkin uygulamalar bakımından çalışanların uygulamadan haberdar olması mümkünken; cihaz kameralarına uzaktan erişilmesi ve görüntü alınması ile gerçekleştirilen izleme faaliyetleri bakımından uygulamaya yönelik olarak bilgilendirilmesi söz konusu olmayacaktır. Nitekim uzak çalışma modeline geçişte, küresel çapta işverenlerin, çalışanların bilgisi dahilinde olmaksızın düzenli takip ve izleme fonksiyonları sunan elektronik gözetleme araçlarına da yöneldiği görülmektedir. Gelişen teknoloji ile bu elektronik gözetleme araçları işverenlere, konum takibi, çalışanlarca kullanılan cihazlardaki klavye hareketlerinin takibi ve ekran görüntülerinin kaydedilmesine ilişkin özellikler ve yapay zekâ yetkinlikleri kullanılarak performans analizi sonuçları sağlayabilmektedir[29].

İşverenler tarafından bu teknolojilerin kullanımı, uzaktan çalışma koşullarında iş faaliyetlerinin etkinliğinin ve verimliliğinin denetlenmesi gerekçesine dayandırılsa da COVID-19 salgını sürecinde iş yeri ve özel alan arasındaki sınırların belirsizleşmesi

---

[27] *KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), 2018, s.20, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, (Erişim Tarihi: 22.12.2020)*

[28] *VATCHA, Amy, Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees. The Information System Student Journal, 2020, s.4-5. https://www.lse.ac.uk/management/assets/documents/ischannel/Final-Print-iSChannel-Volume-15.pdf#page=4 , (Erişim Tarihi: 22.12.2020)*

[29] *KATSABIAN, Tammy, The Telework Virus: How the COVID-19 Pandemic Has Affected Telework and Exposed Its Implications for Privacy and Equality, 2020, s.17-19, SSRN 3684702, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3684702 , (Erişim Tarihi: 22.12.2020)*

sebebiyle, çalışanların özel hayatlarının gizliliği üzerindeki müdahaleci etkisinin, iş yerinin sınırlarını aşacağı hususunu dikkate almak gerekecektir[30].

İşçinin denetlenmesine ilişkin tüm teknolojik araçlar bakımından, işverenin yönetim hakkı ve işçinin anayasal koruma altına alınmış olan özel hayatın gizliliğine ilişkin hakkı arasındaki dengenin gözetilmesi şarttır[31]. Bu dengenin kurulması bakımından ise işçinin uygulanacak izleme faaliyetine ve bu faaliyetin sınırlarına ilişkin olarak açık bir şekilde bilgilendirilmiş ve 6698 sayılı Kanun'a uygun olarak aydınlatılmış olması şarttır.

Ancak, işçinin izleme faaliyeti hakkında bilgilendirilmiş olması ve hatta 6698 sayılı Kanun hükümlerine uygun olarak açık rızasının temin edilmiş olması, işverene gerçekleştirilecek izleme faaliyeti ile ilgili mutlak bir yetki tanımayacaktır. İşverenlerce yürütülecek elektronik izleme ve takip süreçleri kapsamında, iş faaliyetlerinin etkinlik ve verimliliğinin ölçülmesi amacıyla bağdaşmayacak ölçekte veri toplanmaması sağlanmalı; yürütülecek faaliyetlerin gereklilik ve ölçülülük yönünden değerlendirilmesi ve çalışanların özel hayatın gizliliğine ilişkin temel hakkı üzerindeki müdahaleci etkisinin analiz edilmesi gerekmektedir[32].

Bununla birlikte, işverenlere çalışanlarını "gizlice izleme" imkânı sağlayan teknoloji çözümlerinin kullanılmasının yönetim hakkı kapsamında değerlendirilmesi de mümkün olmayacaktır. Nitekim, Yargıtay 22. Hukuk Dairesi'nin 7 Mayıs 2019 tarihli Kararı'nda *işverence iş akdinin haklı nedenle feshine gerekçe oluşturacak bilgileri, işçinin bilgisayarına yerleştirdiği 'klavye yakalayıcısı' adı verilen özel bir takip programı kullanarak elde ettiği ve işçinin bu programdan haberdar olmadığı, işverence bu konuda bilgilendirilmediği, işçinin rızası hilafına tüm kayıtların özel yahut işe ilişkin bilgi ayrımı olmadan işverence günlük olarak elde edildiğinin anlaşılması karşısında, gizlice izleme neticesinde elde edilen bu bilgilerin fesih sebebi olarak ileri sürülmesinin mümkün olmadığına karar vermiştir*[33]. Anılan kararda Yargıtay, işverenin yönetim hakkının bir sonucu olarak işçiyi elektronik ortamda izlemesi ve takip etmesinin, işçinin bu izleme hakkında açıkça bilgilendirilmiş olması şartıyla mümkün olduğuna kanaat getirmiştir.

iv. İş yerinde Fiili Çalışmaya Geçişle Dönüşen İş yeri Uygulamaları

COVID-19 salgını sürecinde, ticari ve operasyonel faaliyetlerine süreklilik kazandırma ihtiyacı içinde bulunan işverenlerce sınırlı iş gücü ile iş yerinde fiili çalışmaya geçilmeye başlanmıştır. İş yerinde fiili çalışmaya geçişte salgının önlenmesi amacıyla gerekli tedbirlerin uygulanmasını, işverenin çalışanlarının sağlığını ve güvenliğini sağlama ve bu kapsamdaki

---

[30] *LI, Tiffany C, Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis, Loyola University Chicago Law Journal, 2020, s.82, SSRN 3690004, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3690004, (Erişim Tarihi: 22.12.2020)*

[31] *ALOISI, Antonio, & GRAMANO, Elene, Artificial intelligence is watching you at work. Digital surveillance, employee monitoring and regulatory issues in the EU context, Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection", edited by Valerio De Stefano, 41/1, 2019, s.95-121, SSRN 3399548, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3399548, (Erişim Tarihi: 22.12.2020)*

[32] *CATENACCI, Christina, Privacy and Surveillance in the Workplace: Closing the Electronic Surveillance Gap (Doktora tezi, The University of Western Ontario), 2020, https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=9347&context=etd, (Erişim Tarihi: 22.12.2020)*

[33] *Yargıtay, 22. HD., E.2017/21857, K.2019/9884, T.7.5.2019.*

risklerin en aza indirgenmesine ilişkin yükümlülüğü çerçevesinde değerlendirmek mümkündür. Bu özen yükümlülüğünün bir sonucu olarak işverenler, sağlık durumunun ve tedbirlerin uygulanıp uygulanmadığının kontrolü, iş yerinde sosyal temasın ve enfeksiyon riskinin azaltılması amacıyla çalışan hareketlerinin izlenmesine yönelik teknoloji çözümlerini hayata geçirmeye yönelmişlerdir.

v. İş yerinde Çalışanların Sağlık Durumunun Takibine İlişkin Uygulamalar

İş yerinde fiili çalışmaya devam edilmesi sebebiyle, COVID-19 salgınının iş yerinde bulunan çalışanlara bulaşma riskini en aza indirmek ve çalışanların sağlığının korunması adına işverenler, iş yerine girişlerde ateş ölçümü veya belirli durumlarda test yapılmasına ilişkin uygulamalara yaygın olarak başvurmaktadırlar[34]. Nitekim, 30 Haziran 2012 tarih ve 28339 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6331 sayılı İş Sağlığı ve Güvenliği Kanunu ("**6331 Sayılı Kanun**") uyarınca işveren, çalışanların işle ilgili sağlık ve güvenliğini sağlamakla ve bu anlamda çalışanlarının sağlığına ilişkin riskleri en aza indirmekle yükümlüdür.

Ancak COVID-19 salgınına ilişkin sağlık risklerinin mevcudiyetinin tek başına işverenlere çalışanlarının sağlık durumlarının düzenli kontrol ve takibi amacıyla mutlak bir yetki sağladığını söylemek uygun olmayacaktır. Gerek Avrupa Veri Koruma Kurulu[35] gerek Kişisel Verileri Koruma Kurumu[36] tarafından vurgulandığı üzere, çalışan sağlık verilerinin işlenmesine ilişkin olarak ölçülülük ve veri minimizasyonu ilkelerine uyum sağlanması gerekmektedir.

İşveren tarafından çalışanlarının sağlık durumuna ilişkin olarak elde edilen bu kayıtlar bakımından başta kişisel verilerin işlenmesinde uyulması zorunlu ilkeler olmak üzere, 6698 sayılı Kanun hükümlerine uygun hareket edilmesi gerekmekte; özel nitelikli kişisel verilerden olması sebebiyle, sağlık verilerinin işlenmesi, saklanması ve üçüncü taraflarla paylaşılmasına ilişkin veri güvenliği önlemlerinin[37] alınması gerekmektedir.

Bu doğrultuda, iş yerlerine girişte yaygın olarak tatbik edilen ateş ölçümlerine ilişkin olarak, uygulamanın doğrudan sır saklama yükümlülüğü altında bulunan sağlık meslek

---

[34] *BODIE, Matthew T., & McMAHON, Michael, Employee Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic, Washington University Journal of Law and Policy, Vol 64, 2020, s.3, http://law.wustl.edu/Journal/index.html , (Erişim Tarihi: 22.12.2020)*

[35] *EUROPEAN DATA PROTECTION BOARD, Statement on the processing of personal data in the context of the COVID-19 outbreak, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf , (Erişim Tarihi: 22.12.2020)*

[36] *KİŞİSEL VERİLERİ KORUMA KURULU, Kamuoyu Duyurusu COVID-19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler, 2020, https://kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler- , (Erişim Tarihi: 22.12.2020)*

[37] *KİŞİSEL VERİLERİ KORUMA KURULU, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kişisel Verileri Koruma Kurulu'nun 31/01/2018 tarih ve 2018/10 sayılı Kararı (https://www.kvkk.gov.tr/Icerik/4110/2018-10, (Erişim Tarihi: 22.12.2020)*

mensuplarınca yürütülmesi veya çalışanın yüksek ateş belirtisi göstermesi halinde işverenin ilgili çalışan özelinde kayıt oluşturmaksızın çalışanın test yaptırmasını talep etmesi tavsiye edilebilecektir[38] . Çalışanlardan test yaptırılmasının talep edildiği durumlarda, 6331 Sayılı Kanun'un 4'üncü maddesi gereği, iş sağlığı ve güvenliği tedbirlerinin maliyetinin çalışanlara yansıtılmaması hususu önem arz etmektedir.

Bunun yanında, çalışan sağlık verilerinin işlenmesine ilişkin hukuki risklerin en aza indirgenmesini teminen işverenlerce, çalışanların doğrudan kendi sağlık taramalarını yapmasına ve semptom gösterip göstermediği, COVID-19 teşhisi konulmuş kişilerle temas edip etmediği hususlarında beyanlarının toplanmasına elverişli uygulamaların değerlendirilmesi de tavsiye edilebilecektir[39] .

vi. İş yerinde Sosyal Mesafe Kurallarına Uyulmasının Takip ve Teşvik Edilmesine Yönelik Uygulamalar

İşverenlerce, yüksek oranda bulaşıcı olan COVID-19 salgınının işyerindeki diğer çalışanlara bulaşma riskini en aza indirgemek adına, iş yerinde sosyal mesafe kurallarına uyması zorunlu tutulmaktadır. İşverenin çalışanların işle ilgili sağlık ve güvenliğini sağlama ve bu anlamda çalışanlarının sağlığına ilişkin riskleri en aza indirme yükümlülüğü gereği, iş yerinde sosyal mesafe kurallarının oluşturulması ve bu kurallara uyulmasının takip ve teşvik edilmesine yönelik tedbirlerin, 6331 sayılı Kanun'a uygun önlemler olarak değerlendirilmesi mümkündür. Ancak işverenlerce sosyal mesafe kurallarına uyulmasının takibi amacıyla başvurulan teknolojik araçlar, iş yerinde salgının yayılma riskinin engellenmesi ve çalışan sağlığının korunması amacıyla sınırlı olarak uygulama alanı bulsa dahi, aktif ve sürekli olarak konum takibi yapılmasına olanak sağladığından, çalışanlar özelinde kişisel verilerinin korunmasına ilişkin endişeleri beraberinde getirebilecektir.

Çalışanların iş yerinde akıllı bileklikler takmasının zorunlu hale getirilmesi ve sosyal mesafe kurallarına uyulmaması halinde alarmlar üreten bu bileklikler vasıtasıyla çalışanlar arasındaki güvenli mesafenin devamlı olarak taranmasına yönelik uygulamalar bu amaçla kullanılan giyilebilir teknoloji araçlarına örnek gösterilebilecektir[40] . Bunun yanında üretim ve ortak çalışma alanlarına konumlandırılan kameralara entegre edilerek, sosyal mesafe ve koruyucu maske takılmasına ilişkin kurallarına uygun hareket edilip edilmediğinin denetlemesine olanak sağlayan yazılım çözümleri de mevcuttur[41].

---

[38] *Bodie & McMahon, M., s.11.*

[39] *GIDENGIL, Courtney A., FISCHER, Shira H., & BROTEN, Nicholas A., Framework for Evaluating Approaches to Symptom Screening in the Workplace During the COVID-19 Pandemic, Santa Moica: CA:RAND Corporation, 2020, s.13-15. https://www.rand.org/content/dam/rand/pubs/perspectives/PEA600/PEA653-1/RAND_PEA653-1.pdf, (Erişim Tarihi: 22.12.2020)*

[40] *PONCE, Aida, COVID-19 Contact-Tracing Apps: How to Prevent Privacy from Becoming the Next Victim, ETUI Research Paper-Policy Brief, 2020, s.4, SSRN 3593405, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3593405 , (Erişim Tarihi: 22.12.2020)*

[41] *RODRIGUEZ, Katitza, Workplace Surveillance in Times of Corona, Electronic Frontier Foundation, 2020, https://www.eff.org/tr/deeplinks/2020/09/workplace-surveillance-times-corona (Erişim Tarihi: 22.12.2020).*

Söz konusu uygulamalar vasıtasıyla çalışan kişisel verilerinin işlenmesine ilişkin risklerin en aza indirgenmesini teminen işverenler tarafından, (i) düzenli takip ve izleme amaçları başta olmak üzere, kişisel verilerin salgının yayılmasının önlenmesi ve çalışan sağlığının korunması haricinde amaçlarla işlenmemesi, (ii) çalışanlara kişisel verilerinin işlenmesine ilişkin açık ve anlaşılır bir şekilde bilgilendirme yapılması ve açık rızalarının alınması, (iii) kişisel verilerin saklanacağı sürenin mümkün olduğu ölçüde sınırlandırılması ve (iv) risk analizleri doğrultusunda gerekli teknik ve organizasyonel önlemlerin uygulanmasına yönelik faaliyetlerin yürütülmesi tavsiye edilebilecektir[42] .

C. SİBER GÜVENLİK TEHDİTLERİ

Ceren Küpeli

Günümüz dünyasında tüm sektörlerin ihtiyaç duyduğu, bu minvalde de korunması gerektiği noktasında açık bir konsensüs oluşan "veri", hukuki perspektifte de savunulması gereken temel kişilik haklarıyla bir bütün olarak, kişisel veri boyutuyla incelenmekte ve yasal mevzuatlarımızda karşılık bulmaktadır. Tüzel kişilikler yönünden de, tüzel kişiliğe ait verilerin hukuka aykırı olarak ifşası halinde tüzel kişiliklerin maddi ve manevi olarak zarar görebileceğinden bahisle[43] bu verilerin korunması gerektiği doktrinde kabul edilmektedir[44] . Aynı şekilde siber ihlaller, ülkesel düzeyde iç ve dış politika sorunlarına ve kurumlar arası koordinasyonlarda aksaklıklara sebep olmaktadır[45] . Başta kamusal işlemlerin yürütülmesini temin amacıyla Devlet tarafından olmak üzere, sivil toplum kuruluşları, özel kuruluşlar ve doktorluk, avukatlık gibi meslek kuruluşlarınca hizmetlerinin ifası için zorunlu olarak verilerin toplanması ve işlenmesi söz konusu olmaktadır[46] . Söz konusu veri işleyen kurum, kuruluş ve kişilerin siber güvenlik tehditlerinden haberdar olması, söz konusu tehditlerin önlenmesi noktasında şüphesiz ilk adım olacaktır. Nitekim dönüşen işyeri uygulamalarında da işbu perspektifte birçok siber tehdit karşımıza çıkmaktadır.

Bunun yanında, COVID-19 sürecinde, uzaktan erişim altyapılarının kullanımındaki artış, siber güvenliğe yönelik risk değerlendirmelerini tekrar gözden geçirme ihtiyacını doğurmuştur. Özellikle evden çalışmanın artması bireysel zafiyetlere dayalı riskleri daha da tetiklerken, COVID-19 ile ilgili kişilerin hassasiyetlerini kötüye kullanmak amacına yönelik siber saldırılarda da bir artış olduğu görülmektedir[47] .

---

[42]Ponce, s.4.

[43]GÖNEN, Doruk, Tüzel Kişilerde Kişilik Hakkı ve Korunması, 1. Baskı, İstanbul, On İki Levha Yayıncılık, 2011, s.90.

[44]KÜPELİ, Ceren, Tüzel Kişi Verilerinin Korunmasında İdarenin Sorumluluğu, 1. Baskı, Ankara, Adalet Yayınevi, 2020, s.44.

[45]GÜNTAY, Vahit, "21.Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk", Siyaset Bilimi ve Uluslararası İlişkiler Dergisi, s.2., 2019, s.96.

[46]AKILLIOĞLU, Tekin, İdari Usul ve Kişisel Verilerin Korunması, Türk İdare Hukuku Sitesi, 2004, http://www.idare.gen.tr/akillioglu-idariusul.htm , (Erişim Tarihi: 10.09.2020)

[47] DURGUN, Özgür Duygu, Covid-19 Döneminde Siber Saldırılar %542 Oranında Arttı; Çözüm Dijital İpekyolu, Boğaziçi Üniversitesi Haberler, 2020, https://haberler.boun.edu.tr/tr/haber/covid-19-doneminde-siber-saldirilar-542-oraninda-artti-cozum-dijital-ipek-yolu, (Erişim Tarihi:22.12.2020).

1. Siber Güvenlik Tehdit Türleri

i. Siber Saldırılar

Bilgi sistemlerine zarar vermek veya veri çalmak amaçlarıyla bilgi sistemlerine sızılması/saldırılması eylemlerine "siber saldırı" ismi verilmektedir. Gün geçtikçe komplike hale gelen arka kapı, Truva atı, solucan, casus yazılım, şifre kırma saldırıları siber saldırı örneklerinin başında gelmektedir[48] . Bilişim sistemlerine, sistem sahibi veya yetkilisinin rızası hilafına girilerek sisteme zarar verilmesi şeklinde tezahür eden eylem, Türk Ceza Kanunu'nun ("TCK") 244. maddesinde "sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu" olarak bir cezai karşılığı haizdir. Nitekim siber saldırılar uyarınca, fail tarafından bilişim sistemlerine yetkisiz erişim gerçekleştirilmesi ve sistemin işleyişinin bozulması söz konusudur. Gerek işe alım sürecinde toplanan veriler, gerekse işe alımı müteakiben barındırılan personel verileri, siber saldırıların doğrudan veya dolaylı hedefinde olabilmektedir. Çalışan adayları ile çalışanların özgeçmişlerinde yer alan kimlik bilgisi, referans ve adli sicil kaydı verileri ile işe alım sürecinde ayrıca birtakım görüntü/ses verileri alınıyorsa, tüm bu verilerin kişisel bilgilere erişmek isteyen siber saldırganların temel motivasyonu olabileceği değerlendirilmelidir. Özellikle bireyi doğrudan belirlemeye yarayan genom biyometrik verilerin ifşa olması ihtimalinde, kişinin telafi edilemez zararlar görmesine neden olunabilecektir.

Siber saldırı kapsamında siber saldırganlar tarafından, hedef sistemlere gönderilmek üzere virüs kullanılabilmektedir. Virüsler, verilerin silinmesi veya işlevsiz hale gelmesini hedeflemektedir[49] . Bu çerçevede, cihazlardaki virüsleri tespit edebilen güvenlik yazılımlarının kullanılması ve bu yazılımların sürekli olarak güncellenmesi önerilmektedir. Siber saldırı türlerinden olan solucanlar ise, girdikleri sistemlerde kendilerini çoğaltarak sistemlere zarar vermek üzere kodlanmış iken, Truva atı; zararlı yazılımlar barındırmasına rağmen kendisini zararsız bir yazılım olarak gösterebilmesi dolayısıyla tespiti güçlük yaratmaktadır. Casus yazılımlarda ise sistemlerdeki tüm verilerin izlenebilmesi sağlanmaktadır[50] . Cihazların bilinmeyen sebeplerle yavaşlaması halinde, söz konusu yazılımlar düşünülmelidir. Yavaşlayan ve sık sık hata veren cihazın, herhangi bir kötücül yazılım barındırıp barındırmadığının tespit edilmesine yönelik teknik bir destek alınması kritiktir. Teknik rapora istinaden cihazdaki yazılımların hangi aracı iletişim araçlarıyla sisteme indirildiği; bu noktadan yola çıkarak da, ileten faillerin kimlik ve IP adresine erişim sağlanmasına çalışılabilecektir.

Günümüzde oldukça sık başvurulan oltalama yönteminde ise, kişilerin sahte internet siteleri veya elektronik postalar aracılığıyla bir linke tıklatarak bilgilerine erişilmesi kurgusu söz

[48] *CANBERK, Gürol, SAĞIROĞLU, Şeref, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9. c., s. 3, 2006, s.169.*

[49] *ÇELİKKOL, Ömer, "Kamu Yönetiminde e-Devlet Yapılanması ve Türkiye için e- Devlet Model Önerisi", Yayınlanmamış Yüksek Lisans Tezi, Isparta, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, 2008, s..50*

[50] *GÜL, Ahmet, "Doğrudan-Dolaylı Bilişim Suçları", Ankara, Seçkin Yayıncılık, 2018, s. 41.*

konusudur[51] . Uygulamada söz konusu phishing linklerinin, verilerin elde edilmesi hedefindeki şirket personeline, kişilerin dalgınlıkla girebileceği formatta iletilerek kişilerin bu linke tıklanmasının sağlandığı görülmektedir. Bir çalışanın dalgınlığından yararlanılarak siber saldırganların sistemlere sızmayı başardığı düşünüldüğünde, bu saldırı türü karşısında, çalışanların bilinmeyen web sitesi veya linklere tıklamamaları, site isminin ve adresinin kontrol etmeleri, sahte olduğu izlenimi uyandıran sitelerde herhangi ödeme işlemi ve bilgi paylaşımı yapmamaları önem arz etmektedir. Cihazdaki eylemlerin kayıt altına alınmasını sağlayan log araçlarının kullanılması, kullanıcıların son eylemlerini göstermesi açısından önemli bir delil kaynağıdır. Siber saldırı muhatabı olan bir bilişim sistemlerine öncelikli olarak teknik müdahale akıllara gelmekle birlikte, somut olay bazında hukuki çarelerin de ivedilikle düşünülmesi ve koruyucu birtakım tedbirlerin alınması gerekmektedir. Keza, siber saldırı dolayısıyla veri ifşaları ve sistem güvenliğinin ihlali haricinde, bir saldırı ile sızılan bir bilişim sistemine hukuka aykırı içeriklerin yüklenmesi ile sistem sahibi/işleticilerinin söz konusu hukuka aykırı içerik barındırma eylemlerinden dolayı cezai sorumluluğunun gündeme gelmesi ihtimal dahilindedir. Bu nedenle siber saldırıya uğrayan sistemlerin, sistemde meydana gelecek aksaklık ve hukuka aykırılıklara ilişkin olarak müşterilerine ve tüm idari otoritelere bu durumu bildirmeleri, sorumluluklarının sınırının çizilebilmesi açısından da önem arz etmektedir.

ii. Mobil Uygulama Tehditleri

Günümüzde bankacılık işlemleri ile her türlü kişisel ve mali veri paylaşımının sürekli olarak mobil uygulamalar üzerinden gerçekleştiği değerlendirildiğinde, mobil uygulamalarının güvenliğinin sağlanmasının önemi ortaya çıkacaktır. Sıklıkla kullanılmayan bir uygulamanın, güncellemesinin gerçekleştirilmemiş olmasından bahisle uğradıkları bir siber saldırı akabinde cihaz için zararlı hale gelebilmesi mümkündür[52] . Söz konusu nedenlerle mobil cihazların kullanıcıları tarafından iyi tanınması ve cihazda güncelleştirmelerin yapılarak cihazın güncel tutulması, güvenilmeyen uygulamaların cihazlara yüklenmemesi ve kullanılmayan uygulamaların da silinmesi önerilmektedir.

Mobil uygulamaların cihazlara yüklenmesi aşamasında, uygulamanın kullanıcı kaydı oluşturmak üzere talep ettiği verilerin uygulamanın amaç ve hizmetiyle doğrudan bağlantılı olması; dolayısıyla kullanıcıların kullanıcı kaydı oluşturulması aşamasında paylaştığı kişisel verilerinin kapsam ve mahiyetini iyi analiz etmesi önemlidir.

İşverenler tarafından çalışanlarına iş amaçlı kullanılması için tesis edilen mobil cihazların güvenliğinin sağlanması noktasında, işverenlerin bu cihazdaki temel güvenlik kriterlerini sağlamış olmaları, cihaz kullanıcılarının da güvenli mobil kullanım konusunda gerekli özeni göstermeleri gerekmektedir. Keza, kurum içi cihazlarda olduğu gibi mobil cihazlara erişilerek hedef şirket ve şirket çalışanları verilerine erişilebilmektedir.

---

[51] *Gül, a.g.e., s. 41.*

[52] *ARSLAN, Bilgehan, SAĞIROĞLU, Şeref, DEMİRCİ, Sedef, "Güncel Mobil Tehditler ve Alınması Gereken Önlemler", International Symposium on Digital Forensics and Security, 2015, s.3.*

iii. Veri Sızıntıları

Veri işleyen kurum, kuruluş ve kişiler bünyesindeki verilerin; veriye temas eden kişilerin icrai veya ihmali davranışlarıyla bu verileri veya verilere erişim sağlayacak şifrelerin sızdırılması kurum içi veri sızıntısı kapsamındadır[53] . Çalışanların, çalışan özlük bilgilerini sızdırmaları, yetkisiz kişilere erişim izni vermeleri, kurum içi veri sızıntılarına verilebilecek örneklerdir.

Veri sızıntılarını önlemek üzere, verilere erişim yetkisi bulunan kişilerin yetki matrislerinin oluşturulması ve yetkili kişilerin cihaz ve sistemlerini, yetkisiz erişimlerden korumaları kritiktir. Aksi halde, şirketin ve çalışanların özel nitelikli kişisel verileri başta olmak üzere birçok verisinin ifşa olma riski mevcuttur. Veri sızıntılarının tespit edilmesi ve sızıntıların önlenmesi noktasında en önemli husus, kurumlarda yetki matrisinin oluşturulması ve erişimlere yönelik olarak log kayıtlarının tutulmasıdır. Söz konusu log kayıtları, yetkisiz erişim kaynaklı veri sızıntıları ile ifşa olan veriye en son hangi kullanıcının temas ettiğinin belirlenmesi açısından önemli bir delil mahiyetindedir.

iv. Kritik Altyapı Tehditleri

Kritik altyapı, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan Temmuz 2020 tarihli Bilgi ve İletişim Güvenliği Rehberi'nde ("*Rehber*"), "*işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar*" olarak tanımlanmıştır. Rehber kapsamında enerji ve elektronik haberleşme sektörü olarak detaylandırılan kritik altyapı sağlayıcısı kurum kuruluşların veri güvenliğine ilişkin almaları gereken tedbirler sayılmıştır. Cihaz-ağ erişim kontrolleri, veri iletimi ve kullanıcı erişimi gibi konularda somut olarak alınacak tüm önlemlerin Rehber kapsamında olması gerekmektedir. Söz konusu tedbirler ışığında, kurum kuruluş verileri ile çalışan verilerinin korunması sağlanmaktadır.

Ç. DEVLETİN YÜKÜMLÜLÜKLERİ

Gülşah Deniz-Atalar

"Fütürist gelenekten gelen tüm modernizmlerin asıl sorunu şuradadır: Önde gelen tüm roller pırıl pırıl makinalar ve mekanik sistemler tarafından üstlenildiğinde (...) modern insana fişi takmak dışında yapacak kayda değer bir şey kalmamaktadır."[54]

"Ben karanlık çağları hatırlıyorum. Adam başına sadece bir bilgisayar düşerdi, onu da kafatasımızın içinde taşırdık[55]*"* . Şimdi kişi başına gerçek anlamda düşen bilgisayar sayısı

[53] *Küpeli, a.g.e., s.126.*

[54] *BERMANN, Marshall, "Katı Olan Her Şey Buharlaşıyor", (Çeviren: ALTUĞ, Ümit & PAKER, Bülent), 9. Baskı, İletişim Yayınları, İstanbul, 2005, s.44.*

[55] *SAY, Cem, "Yeni Dünya Yeni Ağ", 1.Baskı, Destek Yayınları, İstanbul, 2020, s.9.*

kimilerine 1'den fazla düşerken kimileri ne yazık ki bu teknolojiye ulaşamamaktadır- dünya nüfusunun ¼ üne ulaşmış durumdadır[56]. Teknolojinin bu hızla gelişmesi ve aygıtların bu derecede yaygınlaşmasının dünya için ve dünyada yaşayanlar için iyi bir şey olup olmadığını gelecekte daha net göreceğiz ama ilerleyen sadece bilgisayar sayısı olmamış, bilgisayarların içindeki teknoloji de sürekli gelişip ilerlemiştir. Devletler ise kanun koyucu olma özelliği açısından değerlendirildiğinde bu teknolojiyi hep geriden takip etmiştir. Belki de teknolojik ilerlemenin önemli şartlarından birisi de regülasyonların gelişimi geriden takip etmesidir. Fakat söz konusu insan hakları olduğunda devletin yükümlülükleri mutlaka yerine getirilmesi gereken ve hiçbir gelişmeyi geriden takip etmemesi gereken bir hale bürünmektedir. Bu haklar tüm bireyler açısından devletlerin pozitif yükümlülüğü kapsamında korunması, teminat alınması ve negatif yükümlülüğü kapsamında ne kamusal makamlar ne de üçüncü kişiler tarafından ihlal edilmemesi gereken haklardır. Devletlerin yalnızca insan hakları ihlallerinden kaçınma yükümlülüğü içinde bulunmaları değil, aynı zamanda bireyleri, diğer bireylerin ihlallerinden koruma görevine de sahip oldukları açıktır[57]. Anayasa Mahkemesi'nin "Ömür Kara" ve "Onursal Özbek" kararına göre; Anayasa ve Türkiye'nin imzacısı olduğu Avrupa İnsan Hakları Sözleşmesi'nin ortak koruma alanı kapsamında kalan temel haklar, yalnızca kamusal gücün doğrudan uygulanmasıyla değil; kimi zaman da özel hukuk kişileri arasındaki uyuşmazlıklara konu olacak şekilde üçüncü kişilerin müdahaleleriyle zedelenebilmektedir. İlkinde söz konusu güvencelerin sağlanması adına kamusal makamlara yüklenen negatif ve pozitif tüm yükümlülüklerin doğrudan yerine getirilmesi konusunda tereddüt bulunmamakta ise de ikinci durumda devletin üçüncü kişilerin müdahalelerine karşı bireylere ne tür bir koruma imkânı sunması gerektiği ve hangi çerçevede yükümlülükler taşıdığı hususunda her olayın kendine özgü koşullarına göre değerlendirmelerde bulunuması gerekmektedir[58]. Avrupa İnsan Hakları Mahkemesi'nin ilgili içtihatlarının sistematik resmi, *Siliadin – Fransa*[59] davası gibi Mahkeme kararlarında bulunabilirken, bu kararlar pozitif yükümlülük kavramına bir tanım getirmemektedirler[60]. Avrupa Mahkemesinin görüşüne göre, pozitif yükümlülüklerin asıl karakteri şudur ki bu yükümlülükler uygulamada ulusal makamların bir hakkı güvence altına almak için gerekli tedbirleri almasını gerektirmektedir. Daha açık olarak ifade etmek gerekirse ulusal makamların makul ve uygun tedbirler alarak bireyin haklarını koruması gerekmektedir[61].

[56] *STATISTA, https://www.statista.com/statistics/610271/worldwide-personal-computers-installed-base/ (Erişim Tarihi: 22.12.2020); WORLDOMETER, https://www.worldometers.info/world-population/, (Erişim Tarihi: 22.12.2020)*

[57] *TEZCAN, Durmuş & ERDEM, M. Ruhan & SANCAKDAR, Oğuz & ÖNOK, Murat, "İnsan Hakları El Kitabı", 4.Baskı, Seçkin Yayıncılık, 2011, s.59; SUNAY, Reyhan, İnsan Haklarının Yatay Yetkisi ve Devletin Sorumluluğu, SÜHFD, Cilt 23, Sayı, 1, 2015, s. 12; İNCEOĞLU, Sibel, "İnsan Hakları Avrupa Sözleşmesi ve Anayasa", 3.Baskı, Beta Yayıncılık, 2013, s.56 vd; ÖZDEK, Yasemin, "Avrupa İnsan Hakları Hukuku ve Türkiye", TODAİ, İstanbul, 2004, s. 28 vd; Aybay, Rona: "İnsan Hakları Hukuku", İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2017, s. 156 vd.*

[58] *Anayasa Mahkemesi, Ömür Kara & Onursal Özbek Başvurusu, B. No2013/4825 24/3/2016, para.45.*

[59] *"Bu şartlar altında 4. madde ile uyum sağlanabilmesi için Devlet makamlarının yükümlülüklerinin sadece doğrudan eylemde bulunmamasıyla sınırlandırılması bu madde ile ilgili diğer uluslararası sözleşmelerle çelişkili olacağı gibi, maddeyi etkisiz hale getirecektir. Buna göre bu hükümden mutlaka, Sözleşmenin 3. maddesinde olduğu gibi, Devletlerin bu maddede yasaklanan muameleleri cezalandırmaları yönünde bir pozitif yükümlülükleri vardır" Siliadin/Fransa, BN. 73316/01, 26.7.2005, para. 89.*

[60] *JEAN-FRANÇOİS AKANDJİ-KOMBE, "Avrupa İnsan Hakları Sözleşmesi Kapsamında Pozitif Yükümlülükler", (Çeviri: ÇINAR, Özgür Heval & KAYA, Abdülcelil), Belçika, 2008*

[61] *Avrupa İnsan Hakları Mahkemesi, Hokkanen/Finlandiya, B.No:19823/92, 24/10/1994 para 58, López-Ostra/İspanya, B.No: 16798/90,9/10/1994, para 55.*

Bu noktada devlet özel hukuk kişileri arasındaki ilişkiler için de uygun ve makul önlemleri almakla yükümlüdür[62]. Devletin pozitif yükümlülüğü gerçek ve/veya tüzel kişilerin birbirleri ile olan ilişkilerinin uyuşmazlığa dönüşmesi halinde devreye girmekte ve bu uyuşmazlıkların çözüm mercilerinde ilgili kişilere temel haklara ilişkin anayasal güvencelerin sağlanması konusunda gerekli adımların atılmasını gerçekleştirmektedir[63]. Bu gereklilikler üçüncü kişilerin, bireylerin hak ve özgürlüklerine yaptığı haksız müdahalelere karşı kamusal makamlar tarafından müsamaha gösterilmemesi zorunluluğundan kaynaklanır. Zira derece mahkemeleri, özel hukuk ilişkisi kapsamındaki uyuşmazlıkların çözümlenmesinde bağlayıcı kararlar vererek güvencelerin korunup korunmamasında rol almaktadır. Bu noktada uyuşmazlıkların yargısal makamlar önüne taşınması ve hakkaniyete uygun bir yargılama yapılarak çözümlenmesi, kamusal makamların pozitif yükümlülüklerinin bir parçasını oluşturur[64].

Devletin pozitif yükümlülüğünün özel hukuk ilişkilerinde de devam ettiği yukarıdaki açıklamalardan da anlaşılmaktadır. İşçi işveren ilişkileri de bu kapsamda ele alınan ilişkilerdir. Raporun önceki bölümlerinde anlatıldığı gibi teknolojinin de etkisiyle dönüşüm geçiren işyeri uygulamaları, iş yapma modellerinin değişmesi, işçi ve işveren ilişkilerinin yeniden tanımlanmasına sebep olmuş ve tarafların hak ve yükümlülüklerinde de değişiklikler meydana getirmiştir. Bu değişiklikler devletin pozitif yükümlülüklerinin devreye girmesini, yasal alt yapıların hazırlanması ve bireylerin korunması için gerekli önlemlerin alınması hususunu da göz önüne sermiştir. Bu değişikliklerin bir kısmı regülasyon ihtiyacını doğurmakla beraber mevcut durum içerisinde Anayasa'da yer alan temel hakların korunması için ayrıca bir düzenleme ihtiyacı bulunmamakta, teknolojinin gelişmesi ve kullanılması ile devinim içerisinde olan içtihatlar aracılığı ile haklar korunmaya devam etmektedir. Anayasa Mahkemesi *E.Ü* kararına göre; İşveren ve çalışan arasındaki ilişkinin iki tarafı açısından da belirli hak ve yükümlülükler öngören ve esasen güven ilişkisi üzerine kurulu iş sözleşmesi ile şekillendirdiği unutulmamalıdır Somut uyuşmazlığın ilgili olduğu iş hukukunun dinamik bir niteliği olduğu, ayrıca iş ilişkilerinin genel kurallardan farklı kendine özgü bazı hukuki kurallar içerdiği de dikkate alınmalıdır[65]. İşçiler işyerlerinde her ne kadar mesleki bir hayat sürdürseler de bu özel hayattan ayrı bir hayat değildir ve Avrupa İnsan Hakları Mahkemesi de bu hususa kararlarında değinmiştir[66]. Bu durumda işçilerin hakları açısından yapılan değerlendirmelerin içerisine özel hayata saygı hakkı da girmektedir.

---

[62]*Avrupa İnsan Hakları Mahkemesi, Sorensen ve Rasmussen/Danimarka [BD], B. No: 52562/99, 52620/99, 11/1/2006, para.57; Palomo Sanchez ve diğerleri/İspanya [BD], B. No: 28955/06, 12/9/2011, para.59.*

[63]*""Uyuşmazlıkların özel hukuk kişileri arasında gerçekleştiği durumlarda temel hak ve özgürlüklerin sağladığı güvencelerin yerine getirilip getirilmediği denetlenirken Anayasa'nın kamusal makamlara yüklediği sorumluluklardan doğrudan özel hukuk kişileri sorumlu tutulamayacağından taşıdığı koşulların özelliklerine göre bu tür başvuruların devletin pozitif yükümlülükleri bağlamında ele alınması gerekebilir", Avrupa İnsan Hakları Mahkemesi, Barbulescu/Romanya, B.No:61496, 05.09.2017, (Çeviri: Anayasa Mahkemesi E.Ü B.No 16/13010 17/09/2020 para.65)*

[64]*Anayasa Mahkemesi, Ömür Kara & Onursal Özbek Başvurusu, B. No2013/4825, 24/3/2016, para.45.*

[65]*Anayasa Mahkemesi, E.Ü Başvurusu, B. No 16/13010, 17/09/2020 para.68.*

[66]*Avrupa İnsan Hakları Mahkemesi, Niemitz/Almanya, B.No:137/88.16.12.1992, para.29; Özpınar/Türkiye, B. No:20999/04 19/10/2010, para.45; Compagnano/İtalya B.No:77955/01, 23/03/2006 para.53.*

Anayasanın 20. Maddesinde koruma altına alınmış olan özel hayata saygı hakkı çerçevesinde devlet, kişilerin özel ve aile hayatına keyfî olarak müdahale etmemek ve üçüncü kişilerin haksız saldırılarını önlemekle yükümlüdür.

Teknolojideki gelişmelerle değişen ve dönüşen işyeri uygulamaları işçilerin kişisel verilerini[67] özel hayatlarını işverenlerin sonsuz bilgisine açmış durumdadır. Bu durum *Jeremy Bentham*'ın Panoptikon[68] fikrinin (ya da bu fikre eklemlenen sinoptikon ve polioptikon)[69] dijital çağa uyarlanmış elektronik bir mimari haline dönüşmeye başlamış ve işverenler çalışanlarını neredeyse distopik romanlarda anlatılanlar gibi denetimsiz bir şekilde gözetleyerek, Anayasada koruma altına alınmış olan özel hayatına saygı hakkını ihlal etmeye başlamış ve bu bir süreklilik halini almıştır. Önce televizyonun, sonrasında sosyal medya araçları ile çoğunluğun birbirini izlediği süreçlere geçiş yapılması da gözetim olgusunu normalleştirmiştir[70]. Normalleşme olgusuna rağmen Avrupa Konseyi üye ülkelerinde bu gözetimden rahatsız olan çalışanların yaptığı merci başvuruları sayesinde **AİHM** Barbelescu Romanya kararında çalışanın iletişiminin işveren tarafından denetlenmesi ile ilgili ilkeleri belirlemiştir[71]. Bu ilkeler aşağıda belirtilmiştir;

i) *İşverenin çalışanın haberleşmesini ve diğer iletişimini izlemeye yönelik tedbirler alabilme ihtimalinin, ve bu tip tedbirler alındıysa bunların uygulanıyor olduğunun çalışana bildirip bildirilmediği.*

ii) *(ii) İşverenin yürüttüğü izleme faaliyetinin kapsamı ve çalışanın mahremiyetine ne ölçüde girildiği.*

iii) *İşverenin iletişimin izlenmesi ve içeriğine erişilmesini haklılaştıran meşru gerekçeler gösterip göstermediği.*

iv) *Çalışanın özel yaşamına daha az müdahale eden yöntemlere ve çalışanın iletişiminin içeriğinin doğrudan erişilmesine yönelik tedbirler dışındaki tedbirlere dayanan hafif bir izleme sistemi kurulmasının mümkün olup olmadığı.*

v) *İletişimin izlenmesinin buna muhatap olan çalışan üzerindeki etkisi ve sonuçları; ve işverenin izleme aktivitesinin sonuçlarını nasıl kullandığı.*

---

[67] *Kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla-bir kişiye ilişkin bütün bilgileri ifade etmekte olup bireyin adı soyadı doğum tarihi ve doğum yeri gibi sadece kimliğini ortaya koyan bilgileri değil, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri sağlık bilgileri, genetik bilgiler IP adresi, e posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. (Anayasa Mahkemesi E.2014/74. K.2014/201, 25/12/2014; E.2014/180, K.2015/30,19/3/2015).*

[68] *BENTHAM, Jeremy, "Panoptikon Gözün İktidarı", (Çeviri: ÇOBAN, Barış &, ÖZARSLAN, Zeynep), 3.Baskı, Su Yayınları, İstanbul, 2019, s. 9*

[69] *BAUMAN, Zygmunt & LYON David, "Akışkan Gözetim", (Çeviri: YILMAZ, Elçin), 2.Baskı, Ayrıntı Yayınları, 2016, s.67.*

[70] *ARSLANTAŞ TOKTAŞ, Selma etl, "Türkiye'de Dijital Gözetim, T.C. Kimlik Numarasından E-kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi", Alternatif Bilişim Derneği, 2012, İstanbul, s.33.*

[71] *GEMALMAZ, Burak, Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır? Avrupa İnsan Hakları MahkemesiBüyük Dairenin 5 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: 22.12.2020)*

vi) *İşverenin izleme faaliyetinin çok müdahaleci olduğu haller başta olmak üzere, çalışana uygun güvenceler sağlanıp sağlanmadığı*[72].

Yukarıda açıklanan ilkeler, Türkiye'nin Avrupa Konseyi üyesi olmasından bahisle devletin yükümlülükleri bağlamında Türk hukukunu da bağlamaktadır. Bu kararda AİHM, iletişim alanındaki hızlı gelişmelere rağmen keyfiliğe karşı orantılılık incelemesinin ve usule ilişkin güvencelerin varlığının zorunlu olduğunu belirterek çalışanın iletişiminin incelenmesi bağlamında devletin pozitif yükümlülüklerine ilişkin esasları tespit edilmiştir. AİHM'e göre işveren iletişiminin incelenmesini haklı kılan meşru gerekçeleri ortaya koyabilmedir. Çalışana iletişimin denetlenmesi tedbiri karşısında yeterli güvencelerin sağlanması ve inceleme sonucunda elde edilen verilerin amaç doğrultusunda kullanılması gerektiğini belirtmiştir. Pozitif yükümlülüklere göre dair bu ilkelerin her somut olayın özelliğine göre ne ölçüde uygulandığının yetkili yargı organı tarafından tespit edilmesi gerekir[73]. Diğer yandan AİHM ulusal yargı makamlarının çalışanın özel yaşam hakkı ile işverenin işin yürütümündeki çıkarı arasındaki çatışmada hangi esaslar doğrultusunda muhakeme yapacağını da "dikte" etmektedir. Yani uyuşmazlığın esasına uygulanacak ilkeleri de oldukça ayrıntılı şekilde ortaya koymakta ve ulusal mahkemelerin bu esasları takip etmesini beklemektedir. Bu yönüyle kararın usuli yükümlülüklerin ulusal makamlarca yerine getirilip getirilmediğinin denetlenmesiyle yetinildiği pozitif yükümlülüklere ilişkin klasik kararlardan ayrıldığı düşünülebilir[74]. Derece mahkemeleri tarafından tarafların çıkarları dengelenirken ve müdahalenin ölçülülüğü irdelenirken 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, başvuruya konu olayda olduğu gibi sözleşmenin feshinin çalışanların eylem ya da eylemsizlikleri karşısında makul ve orantılı bir işlem olup olmadığı somut olayın koşullarına göre ele alınmalıdır. Ayrıca yargılamalar sırasında gerçekleştirilen işlemlerin ve neticede verilen kararın gerekçesinin bizatihi özel hayat alanına ilişkin bir müdahale oluşturmaması için derece mahkemelerince gereken özen gösterilmelidir[75]. Sonuç olarak, AİHM Büyük Daire tarafından verilen bu kararın işyerinde özel yaşam hakkının pozisyonuna dair meselelerde belirleyici olacağı söylenebilir. Örneğin hangi durumlarda işverenlerin çalışanların internet kullanımını izlemesinin zorunluluk olarak görüleceği, işverenlerin çalışanların internet aktivitesini otomatik olarak sürekli şekilde takip eden bir sistem kurup kuramayacağı gibi meselelere ışık tutacaktır. Ayrıca çalışanların kendi araç gereçleriyle çalışma saatleri içinde internet ve benzeri medyumları kişisel amaçları için kullanması durumunda yine Barbulescu kararındaki mülahazalar sonuca etkili olacaktır[76].

Teknolojinin gelişmesiyle birlikte iş sözleşmesi çerçevesinde çalışanların gözetlenmesi dışında karşılaşılan ve devletlerin pozitif yükümlülükleri çerçevesinde çözülmesi gereken sorunlardan birisi de ayrımcılıktır. İçinde yaşanılan otomasyon çağında yapay zekanın

[72] *Avrupa İnsan Hakları Mahkemesi, Barbelescu/Romanya, B.No:61496, 05.09.2017, para 121-122. (Çeviri: Gemalmaz)*

[73] *Avrupa İnsan Hakları Mahkemesi, Barbelescu/Romanya, B.No:61496, 05.09.2017, para 112-123. (Çeviri: Gemalmaz)*

[74] *Avrupa İnsan Hakları Mahkemesi, Barbelescu/Romanya, B.No:61496, 05.09.2017, para 121-122. (Çeviri: Gemalmaz)*

[75] *Anayasa Mahkemesi, Ömür Kara & Onursal Özbek Başvurusu, B. No2013/4825 24/3/2016, para.45.*

[76] *Avrupa İnsan Hakları Mahkemesi, Barbelescu/Romanya, B.No:61496, 05.09.2017, para 121-122. (Çeviri: Gemalmaz)*

makinelere entegrasyonu ile makine öğrenmesi denilen kavramın yapay zekalı varlıklarda ayrımcılık kapasitesini artırması ihtimalinin uzak olmadığı açıktır. Bu varlıkların ayrımcılık fikirlerine nasıl ulaştığı konusunda ise yapay zekalı varlıkları yaratanların fikirlerinde bilinçli olarak ya da bilinçaltlarında farkında olmadan barındırdıkları ayrımcılıktan kaynaklandığını söylemek yanlış olmayacaktır. Yapay zekanın yarattığı ayrımcılığın önlenmesi konusu sadece iş hukuku bağlamında değil genel olarak değerlendirilmesi ve etik ilkeler konusunda mutlaka önlemlerin alınmasını gerektirse de bu raporda işe kabul süreçlerinden, işyerinde devam eden ve işten ayrılma süreçlerine kadar her aşamada meydana gelebilecek teknoloji kaynaklı ayrımcılıklar açısından devletlerin yükümlülüklerinin neler olması gerektiği konusuna değinilmelidir. Türkiye'nin de üyesi olduğu Avrupa Konseyi Parlamenterler Konseyi, Eşitlik ve Ayrımcılık Yapmama Komitesi tarafından henüz 2020 yılı Ekim ayında yayınlanan yapay zeka kullanımından kaynaklanan ayrımcılığın önlenmesi raporunda devletlerin yükümlülükleri açık bir şekilde belirtilmiştir[77]. Raporun özet kısmında belirtildiği gibi yapay zeka, otomatik karar verme süreçlerinin büyük ölçüde kalitesini artırarak verimlilik açısından fırsatlar yaratmaktadır - ancak buna paralel olarak, ayrımcılığı devam ettirebilmekte ve şiddetlendirebilmektedir. Yapay zekanın kamu ve özel sektör kullanımlarının ayrımcı bir etkiye sahip olduğu zaten göz önündeyken, bilgi akışı aşırılıkları ön planda tutma ve nefreti teşvik etme eğilimindedir. Önyargılı veri kümelerinin kullanımı, insan haklarını koruma ihtiyacına entegre olamayan tasarım, algoritmaların şeffaf olmaması ve etkileri bakımından hesap verebilirlik eksikliği ve yapay zekâ ekiplerinde çeşitlilik eksikliği; hepsi bu olguya katkıda bulunmaktadır. Devletler, yapay zekânın toplumda ayrımcı bir etkiye sahip olmasını önlemek için harekete geçmeli ve bu alanda uluslararası standartlar geliştirmek için birlikte çalışmalıdır[78].

Birçok ülke ve üst birlik yapay zekâ kullanımına ilişkin olarak etik ilkeler konusunda çalışmalar yapmaktadır. Bu çalışmaların devletler tarafından internetin sınırları kaldırdığı düşüncesi ve uluslararası iş birlikleri göz ardı edilmeden yapılması elzemdir. Bu çalışmaların yasal altyapıya aktarılmasına henüz zaman vardır fakat yasal altyapıya aktarılmasa dahi belirlenen etik ilkelerin parlamentolar tarafından yasama süreçlerine dahil edilmesi ve şeffaflığın sağlanması denetleme mekanizmalarının işleyişine yardımcı olacaktır. Genel amaç, herkesin haklarının özellikle de yapay zeka kullanımının etkilerine daha çok maruz kalma ihtimali yüksek olan kadınlar, etnik, dilsel ve cinsel azınlıklar, işçiler, tüketiciler, çocuklar, yaşlılar engelliler veya dışlanma riski taşıyan diğer insanların haklarının garanti altına alınmasını sağlamaktır[79]. Avrupa Konseyi Parlamenter Asamblesi raporunda devamla, yapay zeka tabanlı sistemler üzerinde çalışan hem kamu hem de özel tüm kuruluşları, bu tür sistemlerin tasarımına en başından itibaren özellikle bu sistemlerin temel hakların kullanılması veya bunlara erişim üzerinde etkisi olabileceği yerlerde eşitlik ve ayrımcılık yapmama saygısının entegre edilmesini ve nerede olursa olsun yaygın kullanımına geçilmeden önce yeterince test edilmesini sağlaması gerektiğini belirtmiştir.

[77] *LACROIX, Christophe, Preventing discrimination caused by the use of artificial intelligence, Committee on Equality and Non-Discrimination, , 2020, s.3. https://pace.coe.int/en/files/28715, (Erişim Tarihi: 22.12.2020)*

[78] *Lacroix, s.1.*

[79] *Lacroix, s. 6.*

Bunun için hem kamu hem de özel sektörün bu İnsan Hakları Etki Değerlendirmesi çerçevesi oluşturulması ve tüm aşamalarda disiplinler arası ve çeşitli ekiplerin kullanılmasını teşvik etmektedir[80]. İnsan Hakları Etki Değerlendirmesi kavramı Birleşmiş Milletler İş ve İnsan Hakları Rehber İlkeleri çerçevesinde oluşturulmuştur[81]. Bu ilkeler işyerlerinde insan hakları ihlallerinin engellenmesi ve ihlal söz konusu olduğunda ihlalin giderilmesi için yapılması gerekenleri anlatan bir kılavuz niteliğindedir.

Her ne kadar bu raporun konusu olmasa da mutlaka değinilmesi gereken başka bir konu da devletlerin çalışma hayatını ve çalışanları korumak için yükümlülükleri çerçevesinde gerekli önlemleri almasını gerektiren makinelerin ve yapay zekanın yükselişi ve otomasyon süreçleri çerçevesinde emek piyasasında zaten yaşanmakta olan durgunlaşmanın artış gösterecek olmasıdır. Teknolojinin gelişmesi ve yaşamın her alanına dahil olması hayatın olağan akışlarını kolaylaştırdığı için coşkuyla karşılanıyor. Gelecekteki ilerlemenin daha da muhteşem olması bekleniyor ve birçok yorumcu bu teknolojilerin işleri dünya çapında dönüştüreceğini tahmin etmektedir[82]. Bir yanda yapay zekâ ve robotikte yaklaşmakta olan ilerlemelerin insanlar tarafından yerine getirilen işlerin sonunu getireceğine dair telaşlı argümanlar varken, diğer yanda birçok iktisatçı, geçmişteki teknolojik atılımların nihayetinde işgücü ve ücretleri yükselttiğini, bu sefer farklı olacağından endişelenmek için hiçbir neden olmadığını ileri sürmektedir[83].

Teknolojik gelişmeler yapay zekalı sistemlerin ve otomasyonların kullanılmasının önünü açmışken işçiler işlerini kaybetme riski ile karşı karşıya kalmaktadır. Devletlerin yükümlülüğü çalışanların makine ve teknoloji karşıtı olmalarını önlemek ve bu sistemlerle beraber çalışmanın gelişmesi için gerekli önlemleri almasıdır. Otomasyona karşı geliştirilebilecek stratejiler, yeni işlerde emeği eski haline getiren otomasyon etkisini dengelemek için emek artırıcı yöntemler bulmak ve yaratmak olmalıdır[84].

---

[80] *Lacroix, s. 4.*

[81] *BİRLEŞMİŞ MİLLETLER, Guiding Principles on Business and Human Rights, Cenevre-New York, 2011, https://www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/ (Erişim Tarihi: 22.12.2020)*

[82] *BRYNJOLFSSON, Erik, MCAFEE, Andrew, Big Data: The Management Revolution, HBR, 2012, https://hbr.org/2012/10/big-data-the-management-revolution, (Erişim Tarihi: 22.12.2020)*

[84] *ACEMOĞLU, Daron & RESTREPO, Pascual, Artificial Intelligence, Automation and Work, MIT, 2018 s.1. SSRN 3098384, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3098384, (Erişim Tarihi: 22.12.2020)*

[84] *Acemoğlu & Restrepo, s.2*

KAYNAKÇA

ACEMOĞLU, Daron & **RESTREPO**, Pascual, Artificial Intelligence, Automation and Work, MIT, 2018 s.1. SSRN 3098384, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3098384*, (Erişim Tarihi: 22.12.2020)

AKILLIOĞLU, Tekin, İdari Usul ve Kişisel Verilerin Korunması, 2004, *http://www.idare.gen.tr/akillioglu-idariusul.htm* , (Erişim Tarihi: 10.09.2020)

ALOISI, Antonio, & **GRAMANO**, Elene, Artificial intelligence is watching you at work. Digital surveillance, employee monitoring and regulatory issues in the EU context, Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection", edited by Valerio De Stefano, 41/1, 2019, s.95-121, SSRN 3399548, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3399548*, (Erişim Tarihi: 22.12.2020)

Anayasa Mahkemesi, E.2014/74. K.2014/201, 25/12/2014; E.2014/180, K.2015/30,19/3/2015.

Anayasa Mahkemesi, E.Ü Başvurusu, B. No 16/13010, 17/09/2020 para.68.

Anayasa Mahkemesi E.Ü Başvurusu, B.No 16/13010 17/09/2020 para.65.

Anayasa Mahkemesi, Ömür Kara & Onursal Özbek Başvurusu, B. No2013/4825 24/3/2016, para.45.

Anayasa Mahkemesi, B. No 2016/13010, 17/9/2020, *https://www.anayasa.gov.tr/tr/haberler/bireysel-basvuru-basin-duyurulari/calisanin-kurumsal-e-posta-hesabinin-incelenerek-is-akdinin-feshedilmesi-nedeniyle-kisisel-verilerin-korunmasini-isteme-hakkinin-ve-haberlesme-hurriyetinin-ihlal-edilmesi/*, Erişim Tarihi: 11.1.2021)

ARSLAN, Bilgehan, **SAĞIROĞLU**, Şeref, **DEMİRCİ**, Sedef, *"Güncel Mobil Tehditler ve Alınması Gereken Önlemler"*, International Symposium on Digital Forensics and Security, 2015, s.3.

ARSLANTAŞ TOKTAŞ, Selma etl, *"Türkiye'de Dijital Gözetim, T.C. Kimlik Numarasından E-kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi"*, Alternatif Bilişim Derneği, 2012, İstanbul, s.33.

ARTICLE 29 DATA PROTECTION WORKING GROUP, Opinion 2/2017 on Data Processing at Work, Brüksel, 2017, s.12-13, *https://ec.europa.eu/newsroom/document.cfm?doc_id=45631, (Erişim Tarihi: 22.12.2020)*

AUTHOR, David & **SCARBOROUGH**, David, Does Job Testing Harm Minority Workers? Evidence from Retail Establishments, The Quarterly Journal of Economics, 2008, s.219-277, *http://economics.mit.edu/files/599*, (Erişim Tarihi: 22.12.2020)

Avrupa İnsan Hakları Mahkemesi, Barbelescu/Romanya, B.No:61496, 05.09.2017, para 121-122.

Avrupa İnsan Hakları Mahkemesi, Campagnano/İtalya, B. No: 77955/01, 23/3/2006.

Avrupa İnsan Hakları Mahkemesi, Compagnano/İtalya B.No:77955/01, 23/03/2006 para.53.

Avrupa İnsan Hakları Mahkemesi, Hokkanen/Finlandiya, B.No:19823/92, 24/10/1994, López-Ostra/İspanya, B.No: 16798/90,9/10/1994, para 55.

Avrupa İnsan Hakları Mahkemesi, Niemitz/Almanya, B.No:137/88.16.12.1992, para.29.

Avrupa İnsan Hakları Mahkemesi, Özpınar/Türkiye, B. No:20999/04 19/10/2010, para.45.

Avrupa İnsan Hakları Mahkemesi, Palomo Sanchez ve diğerleri/İspanya [BD], B. No: 28955/06, 12/9/2011, para.59.

Avrupa İnsan Hakları Mahkemesi, Siliadin/Fransa, BN. 73316/01, 26.7.2005, para. 89.

Avrupa İnsan Hakları Mahkemesi, Sorensen ve Rasmussen/Danimarka [BD], B. No: 52562/99, 52620/99, 11/1/2006, para.57.

AYBAY, Rona: "İnsan Hakları Hukuku", İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2017, s. 156 vd.

AYÖZGER ÖNGÜN, Çiğdem, "Kişisel Verilerin Korunması Hukuku: Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil", 2. Baskı, Beta Yayınları, , İstanbul, 2019, s.24.

BENTHAM, Jeremy, "Panoptikon Gözün İktidarı", (Çeviri: **ÇOBAN**, Barış &, **ÖZARSLAN**, Zeynep), 2019, Su Yayınları, İstanbul, s. 23.

BERMANN, Marshall, "Katı Olan Her Şey Buharlaşıyor", (Çeviren: ALTUĞ, Ümit & PAKER, Bülent), İletişim Yayınları, İstanbul, 2005, s.44.

BİRLEŞMİŞ MİLLETLER, Guiding Principles on Business and Human Rights, Cenevre-New York, 2011, *https://www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/* (Erişim Tarihi: 22.12.2020)

BODIE, Matthew T., & **McMAHON**, Michael, Employee Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic, Washington University Journal of Law and Policy, Vol 64, 2020, s.3, *http://law.wustl.edu/Journal/index.html* , (Erişim Tarihi: 22.12.2020)

BOEHMER, Robert G., Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise form the Modern Sweatshop, DePaul Law Review, 41(3), 1992, s.739-819, *https://core.ac.uk/download/pdf/232967416.pdf*, (Erişim Tarihi: 22.12.2020)

BRYNJOLFSSON, Erik, **MCAFEE**, Andrew, Big Data: The Management Revolution, HBR, 2012, *https://hbr.org/2012/10/big-data-the-management-revolution*, (Erişim Tarihi: 22.12.2020)

CANBERK, Gürol, **SAĞIROĞLU**, Şeref, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9. c., s. 3, 2006, s.169.

CATENACCI, Christina, Privacy and Surveillance in the Workplace: Closing the Electronic Surveillance Gap (Doktora tezi, The University of Western Ontario), 2020, *https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=9347&context=etd*, (Erişim Tarihi: 22.12.2020)

ÇELİKKOL, Ömer, "Kamu Yönetiminde e-Devlet Yapılanması ve Türkiye için e- Devlet Model Önerisi", Yayınlanmamış Yüksek Lisans Tezi, Isparta, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, 2008, s..50.

ÇETİN, Selin, Yapay Zekanın Kullanımında Kaynaklı Ayrımcılığı Önleme, *https://robotic.legal/yapay-zeka-kullanimindan-kaynakli-ayrimciligi-onleme/* (Erişim Tarihi: 22.12.2020)

DURGUN, Özgür Duygu, Covid-19 Döneminde Siber Saldırılar %542 Oranında Arttı; Çözüm Dijital İpekyolu, 2020, *https://haberler.boun.edu.tr/tr/haber/covid-19-doneminde-siber-saldirilar-542-oraninda-artti-cozum-dijital-ipek-yolu*, (Erişim Tarihi:22.12.2020).

DÜLGER, M. Volkan, "Kişisel Verilerin Korunması Hukuku", Hukuk Akademisi, 2. Baskı, İstanbul, 2019, s.328.

EUROPEAN DATA PROTECTION BOARD, Statement on the processing of personal data in the context of the *COVID-19* outbreak, 2020, *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf* , (Erişim Tarihi: 22.12.2020)

GARNER, E., Germany: Employee Monitoring Ruled Unlawful, SRHM, 2017, *https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/germany-employee-monitoring-unlawful.aspx*, (Erişim Tarihi: 22.12.2020)

GEMALMAZ, Burak, Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır? AİHM Büyük Dairenin 5 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: 22.12.2020)

GIDENGIL, Courtney **A., FISCHER**, Shira H., & **BROTEN**, Nicholas A., Framework for Evaluating Approaches to Symptom Screening in the Workplace During the COVID-19 Pandemic, Santa Moica: CA:RAND Corporation, 2020, s.13-15. *https://www.rand.org/content/dam/rand/pubs/perspectives/PEA600/PEA653-1/RAND_PEA653-1.pdf*, (Erişim Tarihi: 22.12.2020)

GOODYEAR, Michael, The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of U.S. Data Privacy Law, Houston Law Review, Vol. 10, No. 3, 2020, s.76- 97, *https://houstonlawreview.org/article/12850-the-dark-side-of-videoconferencing-the-privacy-tribulations-of-zoom-and-the-fragmented-state-of-u-s-data-privacy-law* , (Erişim Tarihi: 02.02.2021)

GÖNEN, Doruk, Tüzel Kişilerde Kişilik Hakkı ve Korunması, İstanbul, On İki Levha Yayıncılık, 2011, s.90.

GÜL, Ahmet, Doğrudan-Dolaylı Bilişim Suçları, Ankara, Seçkin Yayıncılık, 2018, s. 41.

GÜNTAY, Vahit, "21.Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk", Siyaset Bilimi ve Uluslararası İlişkiler Dergisi, S.2., 2019, s.96.

INTERNATIONAL LABOUR ORGANIZATION, Teleworking during the COVID-19 pandemic and beyond, A Practical Guide, 2020, s.15-37, *https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_751232.pdf*, (Erişim Tarihi: 22.12.2020)

İNCEOĞLU, Sibel, "İnsan Hakları Avrupa Sözleşmesi", 3. Baskı, Beta Yayıncılık, s.56 vd.

JEAN-FRANÇOIS AKANDJI-KOMBE, "Avrupa İnsan Hakları Sözleşmesi Kapsamında Pozitif Yükümlülükler", (Çeviri: **ÇINAR**, Özgür Heval & **KAYA**, Abdülcelil), Belçika, 2008 *https://inhak.adalet.gov.tr/Resimler/Dokuman/1012201911281 1poizitif_yukumluluk.pdf* (Erişim Tarihi: 22.12.2020)

KATSABIAN, Tammy, The Telework Virus: How the COVID-19 Pandemic Has Affected Telework and Exposed Its Implications for Privacy and Equality, 2020, s.17-19, SSRN 3684702, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3684702* , (Erişim Tarihi: 22.12.2020)

KİŞİSEL VERİLERİ KORUMA KURULU, Kamuoyu Duyurusu COVID-19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler, 2020, *https://kvkk.gov-.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-* , (Erişim Tarihi: 22.12.2020).

KİŞİSEL VERİLERİ KORUMA KURULU, *"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlu-larınca Alınması Gereken Yeterli Önlemler"* ile ilgili Kişisel Verileri Koruma Kurulu'nun 31/01/2018 tarih ve 2018/10 sayılı Kararı *(https://www.kvkk.gov.tr/Icerik/4110/2018-10*, (Erişim Tarihi: 22.12.2020)

KİŞİSEL VERİLERİ KORUMA KURUMU, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), 2018, s.20, *https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf*, (Erişim Tarihi: 22.12.2020)

KÖKSAL, Mehmet Ali, Yapay Zeka Çağında Hukuk, İstanbul Barosu, *https://www.istanbulbarosu.org.tr/files/docs/Yapay_Zeka_Caginda_Hukuk2019.pdf*, s.79. (Erişim Tarihi: 22.12.2020)

KÜZECİ, Elif, *"Kişisel Verilerin Korunması"*, 3. Baskı, Turhan Kitabevi, Ankara, 2019, s. 246.

LACROIX, Christophe, Preventing discrimination caused by the use of artificial intelligence, Committee on Equality and Non-Discrimination, , 2020, s.3 *https://pace.coe.int/en/files/28715,* (Erişim Tarihi: 22.12.2020)

LENONARDI, Paul. M., COVID and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work, Journal of Management Studies, 2020, 1, *https://onlinelibrary.wiley.com/doi/epdf/10.1111/joms.12648*, (Erişim Tarihi: 02.02.2021)

LI, Tiffany C, Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis, Loyola University Chicago Law Journal, 2020, s.82, SSRN 3690004, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3690004*, (Erişim Tarihi: 22.12.2020)

KÜPELİ, Ceren, Tüzel Kişi Verilerinin Korunmasında İdarenin Sorumluluğu, Ankara, Adalet Yayıne-vi, 2020, s.44.

MATEESCO, Alexandra & **NGUYEN,** Aiha, Explainer: Workplace Monitoring & Surveillance, Data & Society, 2019, s.1-18, *https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf,* (Erişim Tarihi: 22.12.2020)

ÖZDEK, Yasemin, "Avrupa İnsan Hakları Hukuku ve Türkiye", TODAİ, İstanbul, 2004, s. 28 vd.

PALLOT, Libby & **KENNEDY**, Russell, Australia, Debate over Use of Surveillance Shifts in Employ-ers' Favor, SRHM, 2018, *https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/global-australia-surveillance.aspx*, (Erişim Tarihi: 22.12.2020)

PONCE, Aida, COVID-19 Contact-Tracing Apps: How to Prevent Privacy from Becoming the Next Victim, ETUI Research Paper-Policy Brief, 2020, s.4, SSRN 3593405, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3593405* , (Erişim Tarihi: 22.12.2020)

PRANGGONO, Bernardi & **ARABO**, Abdullahi, COVID-19 Pandemic Cybersecurity Issues, Internet Technology Letters, 2020, s.1-6, *https://doi.org/10.1002/itl2.247*, (Erişim Tarihi: 22.12.2020)

RAUB, McKenzie, Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices, Arkansas Law Review, 71(2), 2018, s.529-570, https://core.ac.uk/download/pdf/215462495.pdf, (Erişim Tarihi: 22.12.2020)

RODRIGUEZ, Katitza, Workplace Surveillance in Times of Corona, Electronic Frontier Foundation, 2020, *https://www.eff.org/tr/deeplinks/2020/09/workplace-surveillance-times-corona* (Erişim Tarihi: 22.12.2020)

SAY, Cem, "Yeni Dünya Yeni Ağ", 1. Baskı, Destek Yayınları, İstanbul, 2020, s.9.

SRHM, Managing Workplace Monitoring and Surveillance, SRHM, 2019, *https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx*, (Erişim Tarihi: 22.12.2020)

STATISTA, *https://www.statista.com/statistics/610271/worldwide-personal-computers-installed-base/* (Erişim Tarihi: 22.12.2020).

SUNAY, Reyhan, İnsan Haklarının Yatay Yetkisi ve Devletin Sorumluluğu, SÜHFD, Cilt 23, Sayı, 1, 2015, s. 12.

TEZCAN, Durmuş & **ERDEM**, M. Ruhan & **SANCAKDAR**, Oğuz & **ÖNOK**, Murat, "İnsan Hakları El Kitabı", 4. Baskı, Seçkin Yayıncılık, s.59.

THOMPSON, SARAH & **WOODS McGUIRE**, EU Court: Employee E-mail Monitoring May Not Breach Privacy Rights, SRHM, 2016, *https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/germany-employee-monitoring-unlawful.aspx*, (Erişim Tarihi: 22.12.2020)

TÜRKÇE BİLGİ, Quis Custodiet Ipsos Custodes? *https://www.turkcebilgi.com/quis_custodiet_ipsos_custodes* (Erişim Tarihi: 22.12.2020)

VATCHA, Amy, Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees, The Information System Student Journal, 2020, s.4-5. *https://www.lse.ac.uk/management/assets/documents/ischannel/Final-Print-iSChannel-Volume-15.pdf#page=4* , (Erişim Tarihi: 22.12.2020)

WORLDOMETER, *https://www.worldometers.info/world-population/*, (Erişim Tarihi: 22.12.2020)

YARGITAY 22. HD., E.2017/21857, K.2019/9884, T.7.5.2019.

YARGITAY 22. HD. 1.9.2016, E. 2016/6321, K. 2016/13143

ZUECO, Irine, Will AI Solve Your Workplace Safety Problems? Prosapien, 2020, *(https://www.pro-sapien.com/blog/ai-solve-safety-problems/*, (Erişim Tarihi: 22.12.2020)