Teknolojinin Etkisiyle Dönüşen İş İlişkisinde Giriş Kontrol Sistemleri, Yer Belirleme Sistemleri ve Sosyal Medya Vasıtasıyla İzleme

Selen UNCULAR[1]
ORCID: 0000-0001-5106-6489

Öz: Bilgi ve iletişim teknolojilerinin hızla ilerlemesi, kişisel verilerin iş ilişkisinde korunmasının önemini gittikçe arttırmaktadır. Zira iş ilişkisinde kişisel veri işlemeyi mümkün kılan bu teknolojiler artık eskisine göre çok daha müdahaleci şekilde ve az maliyetle kullanıldığı gibi, gerek iş başvurusunda bulunan adayların, gerekse işçilerin işyeri içinde ve dışında izlendiği uygulamaların yaygınlaşmasına yol açmıştır. Söz konusu izleme uygulamaları çok çeşitli şekillerde gerçekleştirilmekle beraber, bu makalede günümüzde ve gelecekte iş ilişkisi üzerindeki dönüştürücü etkileri ve ülkemizde az sayıda araştırmaya konu olmaları nedeniyle elektronik ve biyometrik giriş kontrol sistemlerine, elektronik yer belirleme sistemlerine ve sosyal medya kullanımına dayanan izleme uygulamaları ele alınmıştır. Bahsi geçen üç uygulama iş hukuku ve veri koruma hukuku mevzuatı kapsamında mahkeme kararları ve uluslararası düzenlemeler de dikkate alınarak incelenmiş olup hem adaylar ve işçiler, hem de işverenler açısından farkındalığı arttıracak adil, etkin ve kapsamlı öneriler sunmak amaçlanmıştır.
Anahtar kelimeler: Kişisel Veri, İş İlişkisi, Biyometrik, Yer Belirleme, Sosyal Medya, İzleme

Monitoring by Entrance Control Systems, Positioning Systems and Social Media in Employment Relationship Transforming with the Impact of Technology

Abstract: The rapid progress of information and communication technologies increases the importance of the protection of personal data in employment relationship. Furthermore, these technologies, which enable the processing of personal data in employment relationship, are now used in a much less costly yet more intrusive manner than before, and have led to the widespread monitoring of applicants and workers in and out of the workplace. Although these monitoring practices are carried out in a variety of ways, only the ones based on electronic and biometric entrance control systems, electronic positioning systems and social media usage are evaluated

[1] Avukat, LL.M.
Makale Geliş Tarihi: 26.12.2019, Makale Kabul Tarihi:10.05.2020

in this article due to their transformative effects on the employment relationship and the fact that they are subject to a small amount of research in Turkey. These three practices were examined within the scope of labour law and data protection law legislation by taking into account judicial and international instruments and it is aimed to present fair, effective and comprehensive proposals with the potential to raise awareness for both applicants and workers, and employers.
Keywords: Personal Data, Employment Relationship, Biometric, Positioning, Social Media, Monitoring

Giriş

Bilimin ve teknolojinin gelişmesiyle birlikte, işyerinde bilgisayarın, e-postanın, telefonun, internetin ve sosyal medya hesaplarının, işyerine, işyerindeki bazı bölümlere ve/veya katlara giriş-çıkışların ve işyeri dışındaki faaliyetlerin izlenmesine ilişkin uygulamalar son derece yaygınlaşmış ve kolaylaşmıştır. Uluslararası Çalışma Örgütü (International Labour Organization- UÇÖ)'nün İşçilerin Kişisel Verilerinin Korunması Hakkında Uygulama Kodu m.3/3'te bilgisayar, kamera, video ekipmanı, ses cihazı, telefon ve diğer iletişim araçlarının kullanılmasını, çeşitli kimlik ve konum belirleme yöntemlerini veya diğer her türlü gözetim yöntemini -bunlarla sınırlı olmadan- içerdiği ifade edilen izleme uygulamaları, doğrudan insan eliyle ya da teknolojik programlar ve/veya cihazlar vasıtasıyla gerçekleştirilebileceği gibi, kişisel veri elde edilmesini de sağlamaktadır. Ayrıca söz konusu uygulamalar, iş ilişkisi açısından 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) m.3/1(d) kapsamında iş başvurusunda bulunan adaya ve işçiye ilişkin her türlü bilgi şeklinde tanımlanabilen kişisel verilerin eskisine göre çok daha az maliyetle ve daha sistematik ve müdahaleci şekilde işlenmesine sebep olmaktadır. Böylece işverenin işyerini korumadaki ekonomik ve kişisel menfaatleri ile adayın ve işçinin özel hayatın gizliliği ve kişisel verilerin korunması hakları arasındaki dengeye yönelik güncel ihtimalleri dikkate alan değerlendirmeler yapmak gerektiği açıktır.

Bu çerçevede gerek günümüzde sıklıkla başvurulmaları ve gelecekte de artış göstererek çeşitli uyuşmazlıklara, tartışmalara ve değişikliklere gebe olmaları, gerekse Türk hukuku öğretisinde ve ülkemizdeki yargı kararlarında az sayıda incelemeye konu olmaları nedeniyle iş ilişkisinde gerçekleştirilen izleme uygulamalarından üç tanesine odaklanılmıştır. Bu uygulamalar ayrım yapılmaksızın 4857 sayılı İş Kanunu (İK), 854 sayılı Deniz İş Kanunu ve 5953 sayılı Basın İş Kanunu kapsamındaki ve İK m.4 uyarınca İK'nin kapsamı dışında kalan işlerde çalışan tüm özel sektör işçileri[2] ile uygun düştüğü hallerde adaylar açısından incelenmiştir. Üç bölümden oluşan bu makalede, ilk bölüm

[2] Kanımızca TBK m.393/3 ışığında; işçinin kişiliğinin korunmasını düzenleyen TBK m.417 ve iş ilişkisinde kişisel verilerin işlenmesini öngören TBK m.419, stajyerler ve 3308 sayılı Mesleki Eğitim Kanunu'na tabi olmayan çıraklar için de kıyas yoluyla uygulama alanı bulmaktadır.

işçinin elektronik ve biyometrik giriş kontrol sistemleri, ikinci bölüm işçinin işyeri dışında elektronik yer belirleme sistemleri ve son bölüm ise adayın ve işçinin sosyal medya vasıtasıyla izlenmesine ayrılmıştır. Söz konusu izleme uygulamaları UÇÖ, Avrupa Konseyi ve Avrupa Birliği düzenlemeleri de dikkate alınarak iş hukuku ve veri koruma hukuku kapsamında değerlendirilmeye çalışılmıştır.

İşçinin Elektronik ve Biyometrik Giriş Kontrol Sistemleri Vasıtasıyla İzlenmesi

İşverenler işçilerin işyerine giriş ve çıkış saatlerini, sıklığını ve güvenliğini kontrol etmek veya kaydetmek üzere kimlik tanımlaması, doğrulaması ve ayrıştırması yapan, gün içinde ziyaret ettikleri işyeri bölümlerini ve buralarda ne kadar süre bulunduklarını tespit eden elektronik ve biyometrik giriş kontrol sistemlerine başvurmaktadır. Söz konusu sistemler, işçinin kişisel verilerini işlemekte olup programlanmalarına bağlı olarak işyerinin belli alanlarına, bölümlerine ve/veya katlarına giriş ve çıkışı engelleyebilme özelliğine de sahip olurken, kişiye özel veya genel nitelikte tasarlanabilmektedir (Okur, 2013: 112).

Bu bağlamda elektronik giriş kontrol sistemleri, kişisel tanımlama numarası (Personal Identification Number- PIN) ya da manyetik veya çipli kart (akıllı kart) ile kontrolü gerçekleştirmektedir. İlk yönteme göre, her işçiye bireysel olarak verilen alfabetik veya rakamsal tanımlama numarasının/şifresinin işyerine giriş ve çıkışta merkezi bir sisteme ya da belirli sistemlere girilmesi üzerine giriş ve çıkış zamanları kayıt altına alınmaktadır. Manyetik veya çipli kart yönteminde ise, kişisel tanımlama numarasının bulunduğu bir bilgi taşıyıcısı içeren manyetik kartın veya kişisel bilgileri kayıt sistemine sahip bir çipli kartın işyerine giriş ve çıkışta turnikeye okutulması üzerine giriş ve çıkış zamanları kaydedilmektedir. Söz konusu sistemler işveren açısından imza defterinin veya klasik kart sisteminin aksine çok yönlü ve pratik olduğu gibi, işçiler de manyetik veya çipli kartlarını, kimlik kartı, kantinde ödeme aracı, yazıcı, fotokopi, otomat ve tarayıcı kartı olarak ve/veya işyerine giriş-çıkış zamanını belirlemek ve çalışma süresini kaydetmek için kullanabilmektedirler.

Öte yandan biyometrik giriş kontrol sistemlerinde, işçilerin biyometrik verilerini tanımaya veya taramaya ilişkin yöntemler bulunmakta ve işçinin fiziksel veya davranışsal özellikleri ölçülerek daha önce kaydedilmiş bilgiler (biyometrik numune veya şablon) ile karşılaştırma yapılması suretiyle kimlik tespiti sağlanmaktadır. KVKK m.6/1 ve 27 Nisan 2016 tarihli ve 2016/679 sayılı AB Genel Veri Koruma Tüzüğü (General Data Protection Regulation- GVKT) m.9/1 kapsamında özel nitelikli kişisel veri olan biyometrik veriler, GVKT m.4 gereğince "*yüz görüntüleri veya daktiloskopik (parmak izine dayanan) veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik ya da davranışsal özelliklerine yönelik belirli bir teknik işlemeden kaynaklanan kişisel veriler*" şeklinde tanımlanmakta olup biyometrik giriş kontrol sistemleri ile işçilerin parmak izi, avuç içi, el ve parmak geometrisi, yüz, iris, ses, retina,

DNA, ayak izi, yürüme, koku, ağırlık, deri ve vücut şekli gibi biyometrik verileri işlenmektedir[3].

İşyerinde, işyerindeki bazı bölümlerde ve/veya katlarda bulunan elektronik giriş kontrol sistemleri de işçilerin kişisel verilerine müdahale oluşturmakla birlikte, biyometrik giriş kontrol sistemleri, işçilere ait biyometrik verilerin kaydetme, depolama ve eşleştirme işlemleri doğrultusunda işlenmesine sebebiyet verdiğinden aşırı müdahaleci bulunmaktadır. Zira rozet, şifre veya kart gibi yöntemlerin aksine, biyometrik verilerin dayanağını teşkil eden biyolojik özellikleri değiştirmek ya da ortadan kaldırmak mümkün olmayıp kan, tükürük ve idrar gibi biyolojik örnekleri de içeren biyometrik verilerin kötüye kullanılması işçiler üzerinde daha ciddi ve tehlikeli sonuçlar doğuracaktır. Bu bağlamda Fransız hukukunda biyometrik verilerin taşıdığı öneme istinaden biyometrik giriş kontrol sistemlerinin Commission Nationale de l'Informatique et des Libertés (Ulusal Bilişim ve Özgürlükler Komisyonu- CNIL)'in özel denetimine tabi olduğu kabul edilmektedir[4]. Ne var ki özellikle yüksek düzeyde güvenlik gerektiren işyerlerinde ya da bir şirketin önemli projelerinin geliştirildiği ve/veya gizli bilgilerinin muhafaza edildiği bölümlerde, akıllı kartlar ile giriş-çıkış kontrolü de yetersiz kalabilmektedir. Bu yüzden kanımızca sadece kamu güvenliği açısından tehlike arz eden atom enerjisi veya kimyasal madde üreten, gizlilik gerektiren bilimsel ve/veya teknolojik çalışmaların yapıldığı ya da istihbarat faaliyetinde bulunan işyerlerinin veya bir bankanın kasa dairesi gibi yüksek güvenliğin zorunlu olduğu alanların girişleri ile sınırlı olarak biyometrik giriş kontrol sistemlerinin varlığı kabul edilebilir. Vurgulamak gerekir ki, bahsi geçen istisnai hallerde de veri koruma hukukunun temel ilkelerine ve kurallarına uygun hareket edilmesi gerektiği açıktır[5].

[3] Kullanılan ve geliştirilen diğer tanıma/tarama yöntemlerine dudak hareketlerinin, imzanın, avuç ve parmak damarlarının ve klavyeye harf yazımının incelenmesinin örnek olarak gösterilmesi mümkündür (Okur, 2013: 113; Article 29 Data Protection Working Party (WP), 2012: 18-27). Söz konusu yöntemler hakkında genel bilgi ve ABD'deki uygulama için bkz. Lane III, 2003: 65-76.

[4] CNIL tarafından 28 Mart 2019 tarihinde "İşyerlerinde Tesislere, Araçlara ve Bilişim Sistemlerine Biyometrik Kimlik Doğrulaması ile Erişim Kontrolünü Amaçlayan Cihazların Uygulanmasına Dair Model Yönetmelik" (Règlement Type Relatif à la Mise en Oeuvre de Dispositifs Ayant pour Finalité le Contrôle d'Accès par Authentification Biométrique aux Locaux, aux Appareils et aux Applications Informatiques sur les Lieux de Travail- CNIL Yönetmelik) yayımlanmış olup özel hukuk ve kamu hukuku işverenlerinin stajyerler, geçici işçiler ve gönüllüler gibi geniş anlamda işçilerin işyerine, bilişim sistemlerine ve mesleki araçlara erişimini kontrol etmek üzere kullandığı her türlü biyometrik veriye uygulanacak bu düzenleme bağlayıcı niteliktedir. Ayrıca CNIL kimlik kartlarının işçiler arasında hileli kullanımını engellemek için işyerinde dijital parmak izlerinin bulunduğu veri tabanlarının kurulmasının orantılı bir uygulama olmadığına karar vermiştir (Ayrıntılı bilgi için bkz. Andenas ve Zleptnig, 2003: 802).

[5] KVKK m.4/2'de yer alan temel ilkelere dair detaylı bilgi için bkz. Küzeci, 2018: 200-223; Ayözger Öngün, 2019: 134-160; Yücedağ, 2019: 47-63.

Ayrıca şimdiden bazı işyerlerinde uygulamaya konan ve yakın gelecekte artma ihtimali göz ardı edilemeyecek diğer bir izleme yöntemi ise radyo frekansıyla tanımlama (Radio Frequency Identification- RFID) çipleridir[6]. Söz konusu teknoloji bir nesnenin, hayvanın ya da insanın barkod etiketlerine benzer şekilde tarayıcı veya okuyucu ile tanımlanmasını sağlamaktadır. Üstelik işçilerin özellikle baş parmağı ile işaret parmağı arasına enjekte edilen pirinç tanesi büyüklüğündeki bu çipler, radyo dalgaları vasıtasıyla okuyucu ile iletişim kurduğu için okuyucudan uzak olsa bile fark edilebilmektedir. Ancak tıbbi müdahale olmaksızın çıkarılamadığından, işçinin iş saatleri içindeki ve dışındaki her hareketinin sürekli izlenmesine yol açmaktadır. Dolayısıyla işçinin kişisel verilerine ve özel hayatının gizliliğine yönelik aşırı derecede ve tehlikeli bir müdahale oluşturan bu tip uygulamaların yalnızca veri koruma hukukunun temel ilkeleriyle ve kurallarıyla değil, insan onuruyla da bağdaşmadığının ve özellikle iş ilişkisi bakımından kötüye kullanılmaya son derece müsait olduğunun altı çizilmelidir.

Bu itibarla KVKK m.6/3 kapsamında biyometrik verilerin işlenmesi işçinin açık rızasına veya kanunlarda öngörülen hallerin varlığına bağlı olsa da, gerek elektronik, gerekse biyometrik giriş kontrol sistemleri vasıtasıyla yapılan işlemeler öncelikle TBK m.419 uyarınca sözleşmenin ifası için zorunlu olduğu ölçüde gerçekleştirilmeli[7] ve bağımlılığa dayanan iş ilişkisinde işçinin açık rızasının tek başına hukuka uygunluğu sağlamayacağı unutulmamalıdır[8]. Nitekim işveren öncelikle veri koruma hukukunun ölçülülük, amaca bağlılık, şeffaflık, eşit işlem, veri güvenliği ve hesap verebilirlik gibi temel ilkelerini her veri işlemede harfiyen uygulamalı ve temel ilkelerin tamamlayıcısı niteliğindeki hukuka uygunluk nedenleri ise iş ilişkisinin işçinin korunması ve işçi lehine yorum gibi özgün nitelikleri doğrultusunda titizlikle değerlendirilmelidir. Üstelik kişisel verilerin korunması hakkını ihlal edebilecek nitelikteki giriş kontrol uygulamaları açısından işçinin rızasının sadakat borcunun bir gereği olduğu da kabul edilemez. Bu bağlamda ölçülülük ilkesi çerçevesinde aynı amaca ulaşmayı sağlayan ve işçinin kişisel verilerine daha az müdahale eden bir yöntemin varlığı halinde, biyometrik giriş kontrol sistemlerinin kullanılması hukuka aykırı olacaktır. İşyerinin güvenliğine dayanarak işçiye ilişkin biyometrik verilerin işlenmesi halinde dahi, işverenin menfaatleri ile işçinin kişilik değerleri arasındaki dengenin adil şekilde kurulması büyük önem arz etmektedir. Kaldı ki COVID-19 (Koronavirüs) gibi pandemilerde başvurulan elektronik ve biyometrik giriş kontrol sistemleri açısından da işçilerin kişisel verilerin korunması hakkı işverenlerin ekonomik menfaatlerine feda edilmemelidir. Ayrıca giriş

[6] Bahsi geçen uygulamanın Wisconsin'deki bir teknoloji şirketi olan Three Square Market tarafından hayata geçirildiği bilinmekte olup en düşündürücü yanı, başlamasından yalnızca birkaç gün sonra genel merkezdeki 80 işçiden 50'den fazlasının gönüllü olmasıdır (Custers ve Ursic, 2018: 326-327).

[7] TBK m.419 hakkında ayrıntılı bir değerlendirme için bkz. Süzek, 2017: 422-423; Mollamahmutoğlu, Astarlı ve Baysal, 2014: 719-720; Sevimli, 2011: 120-139; Manav, 2015: 104-105; Uncular, 2018: 88-94.

[8] Aynı yönde bkz. Sevimli, 2017: 10; Kişisel Verileri Koruma Kurumu, 2018: 6.

kontrol sistemleri vasıtasıyla elde edilen kişisel verilerin sadece toplanma amacıyla sınırlı olarak işlenmesi ve şeffaflık ilkesi gereğince işçilerin verilerin işlenmesinde izlenen amaç, hukuki dayanak, verilere erişimde yetkili kişiler, verilerin saklanma süresi ve verilere erişim, itiraz, verilerin düzeltilmesini, silinmesini, yok edilmesini veya anonim hale getirilmesini isteme ve zararın giderilmesini talep etme gibi haklar açısından yazılı olarak bilgilendirilmesi zorunludur[9].

Mevzuatımızda işçinin elektronik ve biyometrik giriş kontrol sistemleri vasıtasıyla izlenmesine yönelik özel bir düzenleme olmamakla birlikte, İstanbul Tabip Odası Hukuk Bürosu tarafından yapılan "Parmak İzi Uygulaması Hakkında Hukuki Değerlendirme"[10] başlıklı çalışma yol gösterici niteliktedir. Buna göre vücut bütünlüğünün ayrılmaz bir parçası olan ve bireyi fiziksel açıdan belirleyen parmak izi, kişisel bilgi niteliğinde olup parmak izi alma yetkisi CMK m.81 uyarınca Cumhuriyet savcısının emri üzerine yalnızca belirli sınırlar ve şartlar çerçevesinde kolluk kuvvetlerine tanınmıştır. Dolayısıyla işverenin herhangi bir yasal temele dayanmaksızın kendisini kolluk kuvvetlerinin yerine koyarak işçinin parmak izini alması kişisel verilerin korunması hakkının ihlali nedeniyle hukuka aykırıdır. Bahsi geçen çalışmada işyerine giriş ve çıkışlarda parmak izi uygulamasının Avrupa İnsan Hakları Sözleşmesi (AİHS) m.8'i ve Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin 95/46/EC sayılı mülga AB Yönergesi'ni açıkça ihlal ettiği de vurgulanmaktadır[11]. Kanımızca çalışmada değinilen hususların tamamı yerinde olup işyerine giriş ve çıkışlarda işçinin maruz kalabileceği biyometrik veri işlemeye müsait diğer tüm yöntemler için de geçerlidir.

[9] Ayrıntılı bilgi için bkz. CNIL, 2018a. Bu kapsamda CNIL tarafından elektronik ve biyometrik giriş kontrol sistemleri vasıtasıyla elde edilen kişisel verilere erişime yetkili kişilerin yalnızca insan kaynakları veya güvenlik bölümlerinde bilmesi gereken kişiler ile sınırlı olarak belirlenmesi ve erişimin mutlaka bir tanımlayıcı ve şifre ile gerçekleştirilmesi gerektiği ve işverenlerin bu verilerin güvenliğini sağlamakla ve yetkisiz kişilerin erişimini engellemek için en uygun önlemleri almakla yükümlü olduğu belirtilmiştir. Ayrıca erişime yönelik veriler için kayıttan itibaren 3 aylık ve izin kayıtları dahil çalışma süresinin izlenmesine ilişkin veriler için 5 yıllık saklama süresi öngörülmüştür.

[10] Çalışmanın tam metni için bkz. Eyüboğlu, 2010.

[11] Kaldı ki İl Sağlık Müdürlüğü bünyesinde görev yapan personelin mesai takibinde retina taraması yönteminin uygulanmasına ilişkin işlemin iptali istemiyle açılan bir davada, devlet hastanesinde mesai takibinin yüz tarama sistemi ile yapılmasına ilişkin uygulamanın kaldırılması talebinin reddi üzerine açılan işlemin iptali davasında ve uzman doktor olarak görev yapan davacıların, personel kart okuma sistemlerine kamera yerleştirilmek suretiyle görüntü kaydı alınarak mesai denetimi yapılması işleminin iptaline dayanan bir davada idare mahkemeleri tarafından davanın reddi şeklinde verilen kararlar, Danıştay'ın 12. ve 5. Dairelerince Avrupa İnsan Hakları Mahkemesi (AİHM)'nin ilgili kararları dikkate alınarak bozulmuştur (Ayrıntılı bilgi için bkz. Akgül, 2015: 215-217). Buna karşılık işçinin açık rızasının ve yeterli teknik donanımın olması halinde parmak iziyle giriş kontrolü yapılabileceği yönündeki görüş için bkz. Boydak, 2017: 334.

Öte yandan Avrupa Konseyi'nin CM/Rec (2015) 5 sayılı İş İlişkisinde Kişisel Verilerin İşlenmesi Hakkında Tavsiye Kararı (AKTK) m.18 uyarınca biyometrik verilerin işlenmesi, yalnızca uygun güvencelerle birlikte ve daha az müdahaleci başka bir yöntem mevcut olmaması halinde, işverenlerin, işçilerin veya üçüncü kişilerin meşru menfaatlerinin korunması için gerekliyse ve bilimsel olarak tanınmış yöntemlere dayanarak sıkı güvenlik ve orantılılık koşullarına tabi şekilde mümkün olabilecektir. Bahsi geçen meşru menfaat Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunması Hakkında Çalışma Grubu (Madde 29 Çalışma Grubu) tarafından hazırlanan 2/2017 sayılı İşyerinde Veri İşlenmesi Hakkında Görüş (2/2017 sayılı Görüş) çerçevesinde; işçilerin işleme faaliyeti hakkında bilgilendirilmiş olmaları kaydıyla işlemenin hem gerekli olması, hem de işçilerin özel hayatın gizliliği hakkından daha ağır basmaması halinde mevcuttur[12]. CNIL'e göre de biyometrik giriş kontrol sistemleri ölçüsüz nitelikte izleme oluşturduğundan, yalnızca elektronik giriş sistemleri yetersiz kaldığı veya işyerinin tamamı ya da belirli alanları ciddi güvenlik/hassasiyet gerektirdiği takdirde uygulanabilecektir (2018a). Biyometrik giriş kontrol sistemlerinin zorunlu olduğu tespit edildiğinde ise, biyometrik numunelerin/şablonların işçinin bireysel kontrolü, işçi ve işveren tarafından paylaşımlı kontrol veya işveren kontrolü altında saklanması uygun olacaktır[13]. Her halde biyometrik giriş kontrol sistemleri mutlaka veri koruma etki değerlendirmesine tabi olmalı, işveren yüksek seviye korumayı gerektiren durumu ve daha az müdahaleci başka sistemler yerine neden biyometrik sistemi kullandığını detaylarıyla kanıtlamalı (CNIL Yönetmelik m.3), hukuki düzenlemelere uymalı ve sendika temsilcilerine de danışmalıdır.

Bu doğrultuda gerek işyerine giriş-çıkışların takibinde, gerekse işyerinin güvenliğinin sağlanmasında işçilere ait sınırlı ve özel nitelikte olmayan verilerin yüklendiği manyetik veya çipli kart gibi elektronik sistemlerin kullanılması TBK m.419, AKTK ve 2/2017 sayılı Görüş ile veri koruma hukukunun temel ilkelerine daha uygun düşecektir çünkü yukarıda değinilen istisnai durumlar hariç biyometrik giriş kontrol sistemleri ile ulaşılmak istenen amaca elektronik giriş kontrol sistemleri ile rahatlıkla ulaşılabildiği ortadadır. Fakat vurgulamak isteriz ki, elektronik giriş kontrol sistemlerinde tutulan kayıtlarda da işçinin ay sonunda kaç sayfa belge bastığı ve belgelerin içerikleri veya çay tüketimi için yaptığı toplam ödeme gibi davranış profili belirlemeye yönelik bilgilerin yer almaması, bu sistemlerin işçinin mesai içindeki ve dışındaki davranışlarının takibi için kullanılmaması ve bu sistemler vasıtasıyla izlenen işçilere ait kişisel verilerin İK m.75/2 uyarınca hukuka ve dürüstlük kuralına uygun işlenmesi çok önemlidir.

[12] Ayrıntılı bilgi için bkz. WP, 2017: 19.

[13] Detaylı bilgi ve örnekler için bkz. CNIL Yönetmelik m.7.

İşçinin İşyeri Dışında Elektronik Yer Belirleme Sistemleri ile İzlenmesi

Atipik çalışma türlerinin giderek çoğaldığı günümüzde, pek çok işçi için işyeri kavramı değişime uğramakta ve işyerinden uzakta çalışma imkanları artmaktadır. Bu nedenle işverenler, işyerinden uzakta çalışan veya şoför ve kurye gibi işyeri dışında çalışmak zorunda olan işçilerin çalışma saatlerini kayıt altına alabilmek, iş aracının (taşıtının) kullanımı ile doğrudan bağlantılı olan malların, hizmetlerin veya kişilerin ulaşımını takip ve teyit edebilmek, yasal bir yükümlülüğü yerine getirmek, işçilerin, malların ve iş araçlarının güvenliğini sağlayabilmek ve acil durumlarda zamanı ve kaynakları daha etkili kullanabilmek için konum verilerine ihtiyaç duyabilmektedirler. İş araçlarını izlemeyi sağlayan teknolojiler özellikle ulaşım, sağlık, taşıt filoları ve eve teslim ile ilgili faaliyetlerde bulunan işverenler tarafından sıkça kullanılmaktadır. Kaldı ki pandemi sürecinde görüldüğü üzere, kuryelerin ve şoförlerin iş yükü fazlasıyla artarken işyerinde çalışmak zorunda olmayan pek çok işçi için uzaktan çalışmanın kaçınılmaz hale gelmesi, yer belirlemeye yönelik kullanılan sistemleri daha çok ön plana çıkarmıştır. Bunlar arasında oldukça yaygın olan ve düzenli olarak kodlanmış bilgi yollayan bir uydu ağından meydana gelen GPS (Global Positioning System- Küresel Yer Belirleme Sistemi) sisteminde, GPS alıcılarının uyduların yaydığı sinyaller üzerinden yer ve zaman bilgilerini elde etmesiyle Dünya üzerindeki kesin yer belirlenmektedir. Bu konum verileri, değerlendirilmek üzere bilgisayara yönlendirilebilmekte ve uygun bir bilgisayar programı ile hatasız olarak kişinin bulunduğu yeri ve hareketlerini gösterebilmektedir. Konum belirleme imkânı, cep telefonlarında bulunan GSM, GPRS ve UMTS teknolojileriyle de mümkün olup iş ilişkisinde elektronik yer belirleme sistemleri özellikle iş cep telefonu, iş aracı, iş bilgisayarı ve hareket edebilen diğer araçlar/cihazlar için söz konusu olmakta ve işveren işçinin ve aracın/cihazın konumunu ve hareketlerini sistemin özelliklerine göre eş zamanlı veya sonradan takip edebilmektedir (Uncular, 2018: 245; Goñi Sein, 2009: 21).

Bu bağlamda işveren işçinin iş aracını kullanım talimatlarına ve yol güzergahına uygun olarak kullanıp kullanmadığını, belirlenen ara dinlenmelerini yapıp yapmadığını, yalnızca iş amaçlı kullanım için tahsis edilen aracı özel amaçlı da kullanıp kullanmadığını ve aracın kaybolması ya da çalınması halinde yerini tespit edebilir (Okur, 2013: 136-137). Üstelik araç takip sistemi veya telematik[14] kullanan her işveren hem aracı kullanan işçi, hem de araç hakkında veriler toplayacak ve bu veriler sadece işçinin ve aracın konum bilgilerini değil, aynı zamanda kullanılan teknolojiye bağlı olarak sürücü davranışı dahil birçok başka bilgiyi de içerebilecektir[15]. Bu doğrultuda iş

[14] Telematik, gerçek zamanlı veri aktarma ve izleme teknolojileri kullanan sistemlere verilen genel ad olup bu sistemler, teknik güçlerine ve kapasitelerine bağlı olarak farklı imkanlar sağlasa da temel işlevleri, sisteme bağlı araçlara ait konum, sürüş analizi ve yakıt tüketimi gibi bilgileri belirlenen cihazlara aktarmak ve raporlamaktır.

[15] Detaylı bilgi için bkz. WP, 2017: 19.

aracına konulan olay kaydedici (event data recorder)[16] gibi bazı teknolojiler veya görüntü ve/veya ses kaydeden cihazlar aracın ve sürücünün sürekli izlenmesine de imkân tanıyabilmektedir.

Gerek KVKK'de, gerekse GVKT'de açıkça özel nitelikli kişisel veri olarak düzenlenmediğinden, konum verileri özel nitelikli kişisel verilere ilişkin korumaya tabi değildir. Ne var ki, konum verilerinin işlenmesinin işçiler açısından giderek daha da önemli sonuçlar doğurduğu açıktır. Zira kişinin konum verilerinin işlenmesi, alışkanlık, hobi ve karakter özellikleri gibi kişiliğin değişik görünümlerini de açığa çıkarması nedeniyle ayrımcılık tehlikesini meydana getirmekle kalmayıp ayrıca bu verilerin gasp, hırsızlık ve tehdit gibi çeşitli suçlarda kullanılması güvenlik sorunlarına da sebep olabilir. Bu nedenle kanımızca özel nitelikli kişisel veri olarak kabul edilmesi gereken konum verileri de sıkı, etkin ve kapsamlı bir korumayı hak etmektedir. Kaldı ki işveren elektronik yer belirleme sistemleriyle işçiyi izlerken yalnızca konum verilerini değil, işçiye ait diğer kişisel verileri de toplamakta ve başka işleme faaliyetlerinde de kullanabilmektedir. Dolayısıyla bu sistemler açısından da işçinin kişisel verilerin korunması hakkı ile işverenin yönetim hakkı arasında adil bir dengenin sağlanması zorunluluğu doğmaktadır.

Öte yandan işverenin işçi sağlığı ve iş güvenliği gibi hususlardan kaynaklanan yasal yükümlülükleri nedeniyle iş aracına elektronik yer belirleme sistemi yüklemek zorunda olması da mümkündür. Ayrıca somut olay çerçevesinde işverenin, özellikle acil veya pandemi gibi olağanüstü bir durumda, iş aracının konumunu bilmekte meşru menfaati de söz konusu olabilir. Ne var ki 2/2017 sayılı Görüş gereğince meşru menfaatin varlığı halinde dahi, öncelikle işlemenin gerekli ve orantılı olup olmadığının ve asgari müdahaleyi içerip içermediğinin değerlendirilmesi önem teşkil etmektedir. İşveren iş aracına izleme cihazının yerleştirildiğine ve aracın kullanılması esnasındaki hareketlerinin ve/veya sürüş davranışlarının kaydedildiğine ilişkin işçileri önceden açık ve detaylı olarak bilgilendirmekle de yükümlüdür[17]. Bu bilgilendirmenin hem sürücüye birebir yapılması, hem de sürücünün rahatlıkla göreceği ve anlayacağı şekilde her aracın içine yerleştirilmesi en uygun yöntem olacaktır.

[16] Olay kaydediciler işverene iş araçlarını süren işçiler hakkında önemli miktarda kişisel veri işlemek için teknik olanaklar sunmakta ve bu cihazlar kaza meydana geldiğinde sesli video kaydetme amacıyla iş araçlarına sıklıkla konmaktadır. Ani fren, yön değişimi veya kaza gibi belirli durumları kaydedebilme özelliğine sahip olan olay kaydediciler, sürekli izleme için de ayarlanabilmektedir. Elde edilen bilgiler işçinin sürüş davranışlarını -geliştirmek amacıyla- gözlemlemek ve denetlemek için kullanılabildiği gibi, -bu cihazların pek çoğu gerçek zamanlı olarak aracın konumunu ve sürüşe ilişkin araç hızı gibi diğer detayları izlemek için GPS içerdiğinden- sonraki işlemeler için de saklanabilmektedir. Fakat olay kaydedicinin kullanılmasının, yalnızca işçi hakkında elde edilen kişisel verilerin meşru bir amaçla işlenmek için gerekli olması ve işlemenin ölçülülük ve tamamlama ilkelerini ihlal etmemesi halinde hukuka uygun olduğu kabul edilmelidir (Bkz. WP, 2017: 21).

[17] Aynı yönde bkz. Wallach, 2011: 217; Özdemir, 2010: 247.

İş aracının ve iş cep telefonunun özel amaçlı kullanımına izin verildiği takdirde ise, işçinin mutlaka konum izlemeyi geçici olarak kapatma seçeneği olmalı ve işveren toplanan konum verilerinin işçilerin takibi veya değerlendirilmesi gibi meşru olmayan sonraki işlemelerde kullanılmamasını güvence altına almalıdır (WP, 2017: 20)[18]. Ayrıca 2/2017 sayılı Görüş uyarınca konum verilerinin özellikleri dikkate alındığında işverenin mesai saatleri dışında işçilerin konumlarını izlemeye yönelik meşru bir temele dayanması pek olası görünmemektedir. Ancak iş aracının ve/veya iş cep telefonunun mesai saatleri dışında izlenmesine ilişkin bir gereklilik ortaya çıktığı takdirde, risklere karşı orantılı bir uygulama söz konusu olmalıdır. Örneğin; hırsızlığı önlemek için önceden belirlenmiş bir bölge veya ülke gibi geniş bir alanın dışına araç çıkmadıkça mesai saatleri dışındaki konumun kaydedilmemesi veya işverenin iş aracının konumunun görünürlüğünü, sadece önceden belirlenmiş bir alanın dışına çıkılması halinde devreye sokması önemlidir (WP, 2017: 20).

Vurgulamak gerekir ki, Madde 29 Çalışma Grubu tarafından hazırlanan 13/2011 sayılı Akıllı Mobil Cihazlara İlişkin Konum Belirleme Hizmetleri Hakkında Görüş'te belirtildiği üzere; araç takip sistemleri personel takip sistemi olmayıp onların işlevleri sadece yüklendikleri araçların konumlarını takip etmek veya izlemektir. İşverenler bu sistemleri aracın hızına göre uyarı göndermek gibi sürücülerin veya diğer işçilerin davranışlarını ya da konumlarını takip etmek veya izlemek için kullanmamalıdır[19]. AKTK m.16'ya göre ise; işçilerin konumlarını ifşa eden cihazlar, işverenler tarafından izlenen meşru amaca ulaşmak için gerekli olduğunun ve onların kullanımının işçilerin sürekli izlenmesine yol açmadığının kanıtlanması durumunda kullanılabilir. İzleme ana amaç değil, yalnızca üretimi, sağlığı ve güvenliği korumak

[18] CNIL de işçilerin mesai saatleri dışında konum verilerinin toplanmasını veya iletilmesini devre dışı bırakabilmesinin ve kaydedilen verilere erişebilmesinin zorunlu olduğunu vurgulamaktadır (Bkz. 2018b).

[19] Ayrıntılı bilgi için bkz. WP, 2011: 14. Benzer şekilde CNIL, iş aracına yerleştirilen elektronik yer belirleme sisteminin; hız sınırlarına uygunluğu kontrol etmek, işçiyi sürekli izlemek, sendika temsilcilerinin hareketlerini takip etmek, mesai saatleri dışında konum verisi toplamak ve daha az müdahaleci yöntemler mevcut olmasına rağmen işçinin çalışma saatlerini hesaplamak amacıyla ve işçinin rotayı belirleme özgürlüğünün olduğu araçlarda kullanılamayacağını kabul etmektedir. Bu bağlamda iş aracının kullanılmaması gereken zamanlara ilişkin kilometreler, yapılan yolculuğun bilinmesine gerek kalmadan kötüye kullanımın ve ağırlığının belirlenmesi için yeterlidir (Bkz. 2018b). Öte yandan 5/2005 sayılı Katma Değer Hizmetler Sağlamak Amacıyla Konum Verilerinin Kullanılması Hakkında Görüş'e göre; konum verilerinin işlenmesi, insanların veya eşyaların ulaşımının izlenmesinin veya dağınık konumlardaki hizmetlere kaynak dağıtımının geliştirilmesinin bir parçası olarak yapılması ya da işçiyle veya görevinde kullandığı eşyalarla yahut araçlarla ilgili bir güvenlik amacı bulunması halinde hukuka uygundur. Konum verilerinin işlenmesi, işçilerin kendi seyahat planlarını istedikleri gibi yapmakta serbest olduklarında veya başka vasıtalarla izlenebilecekken gerçekleştirildiğinde ölçüsüz ve aşırı olacaktır (Bkz. 2005: 10).

veya işletmenin etkin faaliyet göstermesini güvence altına almak için gerekli olan eylemin dolaylı sonucu olmalıdır. Bu cihazların kullanımının işçilerin haklarını ve özgürlüklerini ihlal etme potansiyeli göz önüne alındığında, işverenler işçilerin özel hayatlarının gizliliğinin ve kişisel verilerinin korunması için tüm gerekli güvenceleri sağlamalı ve verilerin asgarileştirilmesi ve ölçülülük ilkelerine özellikle dikkat etmelidir.

Hukukumuzda işçinin elektronik yer belirleme sistemleri ile izlenmesine dair herhangi bir düzenleme öngörülmemiş olmakla birlikte[20], bu izleme uygulamalarına TBK m.419 kapsamında sadece sözleşmenin ifasının zorunlu kılması halinde başvurulmalı ve başvurulduğunda işçinin kişisel verileri İK m.75/2 uyarınca hukuka ve dürüstlük kuralına uygun şekilde işlenmelidir. Vurgulamak gerekir ki, elektronik yer belirleme sistemleri aracılığıyla izleme; Madde 29 Çalışma Grubu'nun ilgili görüşleri, AKTK ve veri koruma hukukunun temel ilkeleri ve kuralları uyarınca her şartta işçinin kişisel verilerin korunması hakkına en az müdahale edecek yöntemlerle gerçekleştirilmeli, asgari düzeyde veri toplamalı, ölçülü, meşru amaca bağlı ve şeffaf olmalı ve işçinin davranışlarının izlenmesine yol açmamalıdır. Başta işçinin rızası olmak üzere KVKK ve uluslararası kaynaklarda yer alan hukuka uygunluk nedenleri açısından iş ilişkisinin özgün niteliklerinin ihmal edilmemesi gerektiği de aşikardır. Ayrıca işveren gerek iş aracı, gerekse iş cep telefonu veya diğer cihazlar vasıtasıyla elde edilen konum verilerine yetkisiz kişilerin erişimini engellemek ve konum verilerinin işlenmesinde uygun güvenlik düzeyini sağlamaya yönelik gerekli her türlü teknik ve idari tedbiri almakla yükümlüdür.

Adayın ve İşçinin Sosyal Medya Kullanımının İzlenmesi

Hayatın her alanında oldukça yaygın olan bilgisayar ve internet kullanımı, birçok işyerinin de vazgeçilemez unsuru haline gelmiş ve iş görmeyi son derece kolaylaştırmıştır. Buna karşılık bahsi geçen kullanım işçide bazı sağlık sorunlarına neden olabildiği gibi, iş ilişkisini de olumsuz yönde etkileyebilmektedir. Zira söz konusu elektronik araçlar çalışma zamanının özel amaçlar doğrultusunda verimsiz geçirilmesine yol açabildiği gibi, işçilerin gizli ve sürekli olarak denetim altında tutulmalarına dahi imkân vermektedir. Böylece işçilerin kişisel verilerin korunması hakkı ile işverenin işe ve işyerine yönelik ekonomik menfaatleri arasında önemli çatışmalar ortaya çıkmaktadır.

[20] İşbu izleme uygulaması İspanyol Hukuku'nda Kişisel Verilerin Korunmasına ve Dijital Hakların Güvence Altına Alınmasına İlişkin 5 Aralık 2018 tarihli ve 3/2018 sayılı Organik Kanun (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Los Derechos Digitales)'un "İşyerinde Yer Belirleme Sistemlerinin Kullanılması Karşısında Özel Hayatın Gizliliği Hakkı" başlıklı 90. maddesinde düzenlenmiş olup işverenin işçileri -hukuka uygun olmak kaydıyla- denetlemek için yer belirleme sistemlerinden elde edilen verileri işleyebileceği ve işçilerin ve temsilcilerinin önceden bu sistemlerin varlığı, özellikleri ve veri koruma hukukundan doğan hakları ile ilgili açık, net ve doğru şekilde bilgilendirilmeleri gerektiği öngörülmüştür.

İşveren yönetim hakkı çerçevesinde işyerinde mesai saatleri içinde bilgisayar, internet bağlantısı, telefon, sosyal medya ve e-posta gibi elektronik araçların kullanılıp kullanılmayacağını belirleme ve kullanım kapsamı ile sınırlarına karar verme yetkisine sahiptir. Bu bağlamda işveren, söz konusu araçların işyerinde özel amaçlı kullanımını kısıtlayabileceği gibi, buna açık veya örtülü olarak izin de verebilir. Ne var ki işyerinde bilgisayar, telefon, internet, sosyal medya ve e-posta gibi elektronik araçların özel amaçlı kullanımının tamamen yasaklanması kanımızca işçinin kişiliğinin korunmasına, özel hayatına, manevi varlığını koruma ve geliştirme hakkına, haberleşme özgürlüğüne ve düşünce ve ifade özgürlüğüne ilişkin Anayasa m.13'ü ihlal eden aşırı bir müdahale oluşturmaktadır[21]. Nitekim CNIL'in 2002 tarihli raporu çerçevesinde; iletişim ve bilgi çağında bilgisayarın ve internetin özel amaçlı kullanılmasını tamamen yasaklamak gerçekçi olmayıp işçi ve işveren arasındaki menfaat dengesini de bozduğundan, mesleki üretkenliği engellemeyecek ölçüde makul bir kullanım imkânı tanınması sosyal açıdan daha kabul edilebilir olacaktır[22]. Kaldı ki 2/2017 sayılı Görüş'e göre; kişisel nedenlerle iletişimin tamamen yasaklanması pratik olmadığı gibi, ölçülü olmayan bir izlemeye de sebebiyet verebilecektir (2017: 23)[23].

Dolayısıyla işverenin bahsi geçen elektronik araçların işyerinde özel amaçlı kullanımını ancak işçinin özel hayatına ve haberleşme özgürlüğüne aşırı bir müdahale oluşturmamak kaydıyla sınırlayabileceği ve özel amaçlı kullanımın tamamen yasaklanmasının esasen işyerinde verimin düşmesine yol açarak işverenin menfaatlerine de hizmet etmeyeceği aşikardır[24]. Bu itibarla işyerinde elektronik araçların özel amaçlı kullanımını öğle arası ve/veya dinlenme araları dahil tamamen yasaklayan bir işverenin, özel amaçlı kullanımı gerekçe göstererek sözleşmeyi haklı veya geçerli nedenle feshetmesinin de hukuka uygun olmadığı kanaatindeyiz.

---

[21] Aynı yönde bkz. Özdemir, 2008: 19; Gürsel, 2016: 382-383; Wallach, 2011: 198; Barbulescu - Romanya, 05.09.2017 tarihli ve 61496/08 başvuru no.lu AİHM kararı (Barbulescu), para. 80. İşçinin onurunun korunması için işyerinde asgari düzeyde bile olsa özerk bir alanın sağlanması gerekliliği de savunulmaktadır (Calvo Gallego, 2012: 131 ve 140; Fernandez Villazon, 2003: 111). Genellikle elektronik iletişimin izlenmesi sorununun işyerinde özel amaçlı kullanımı yasaklayarak kolayca çözülebileceği iddia edilse de, tamamen yasaklama ölçüsüz ve gerçekdışı olacaktır (European Union Agency for Fundamental Rights and Council of Europe, 2018: 332).

[22] CNIL bu özgürlükçü yaklaşımını 2010 yılında hazırladığı rehberde de devam ettirmiş olup Fransa dışında Avusturya'da ve İtalya'da da bu konuda daha sosyal temelli bir bakış açısının benimsendiğine ilişkin bkz. Kuner, 2007: 263; Melzer, 2002: 19.

[23] Ayrıca Madde 29 Çalışma Grubu'nun İşyerinde Elektronik İletişimin Gözetlenmesi Hakkında Çalışma Belgesi (Elektronik İletişim Çalışma Belgesi)'nde de sıkça vurgulandığı üzere; elektronik iletişim araçlarının kişisel amaçlarla kullanımının tamamen yasaklanması hem makul, pratik ve gerçekçi değildir, hem de bu araçların işçilere günlük hayatlarında ne kadar yardımcı olabileceğini yok saymaktır (2002: 4, 17 ve 24).

[24] Kaldı ki işyerinde internetin ve e-postanın özel amaçlı kullanımını tamamen yasaklamanın işçiler üzerindeki olumsuz etkilerinin farkında olan bazı işverenler, işyerinde internet cafe gibi imkanlar sağlamaktadır (Tekergül, 2011: 69).

Zira tip iş sözleşmesindeki[25] ve/veya iç yönetmeliklerdeki böyle genel ve kapsamlı bir yasak aynı zamanda haksız şart oluşturacağından, TBK m.20-25 doğrultusunda da geçersizdir[26]. Ayrıca kanımızca işyerinde elektronik araçların işçiler tarafından özel amaçlı kullanımına dair herhangi bir düzenleme bulunmadığı takdirde, işçinin TBK m.396/2 ışığında mesai saatleri içinde işini aksatmadığı/yetiştirdiği, iş sözleşmesinden doğan haklarını ve yükümlülüklerini ihlal etmediği ve mesaisinin büyük bir bölümünü özel amaçlı kullanımla geçirmediği[27] sürece bu araçları kişisel nedenlerle kullanabileceği kabul edilmelidir[28]. Zira Köln Eyalet İş Mahkemesi bir kararında; bu yönde bir düzenleme yapılmaması ve kesin bir yasaklama kuralı bulunmaması halinde, işçinin telefonu ve interneti özel amaçlı kullanmasının kabul edilebilir sınırlar kapsamında mümkün olduğuna ve işverenin düzenleme yapmayarak bunu kabul etmiş olduğuna hükmetmiştir[29].

Öte yandan işyerinde özel amaçlı kullanıma tip iş sözleşmesine, iç yönetmeliklere ve/veya işyeri uygulamasına dayanılarak izin verilmesi, söz konusu iznin zaman, yer, şekil ve ücret açısından sınırlandırılmasına engel olmaz. Bu itibarla işyerinde elektronik araçların kullanımına ve gizliliğe yönelik ayrıntılı, net, anlaşılır ve adil işyeri politikalarının oluşturulması ve özel amaçlı kullanıma ilişkin kuralların iş sözleşmesinde, toplu iş sözleşmesinde veya personel yönetmeliği gibi belgelerde yazılı olarak net, adil, detaylı ve anlaşılır şekilde belirlenip işçinin, imzası ya da elektronik ortamdaki onayı alınmak suretiyle birebir bilgilendirilmesi şarttır[30]. Bu bilgilendirme kapsamında işyerindeki elektronik

[25] Tip iş sözleşmeleri, sanayileşmenin ve teknolojik gelişmelerin iş ilişkilerini bireysel planda düzenlenmekten uzaklaştırması üzerine işe alımlarda önceden işveren tarafından hazırlanmış veya hazırlatılmış ve içeriğinin tamamında ya da bir kısmında TBK m.20-25'te öngörülen genel işlem koşullarının iş ilişkisindeki yansıması olan genel iş koşullarının yer aldığı matbu metinlerden oluşan sözleşmelerdir. Böylelikle işçinin işe alınması bahsi geçen tip sözleşmeyi kabul etmesine bağlı olmakta ve çoğu zaman işçinin sözleşmenin tek bir maddesini bile sorgulaması işe alınmamasıyla sonuçlanabilmektedir (Detaylı bilgi için bkz. Ertürk, 2013: 90-91; Civan, 2015: 52-60).

[26] Aynı yönde bkz. Karademir, 2015: 59.

[27] Schleswig Holstein Eyalet İş Mahkemesi'nin 27.06.2006 tarihli ve 5 Sa 49/06 sayılı kararında; işçinin 3 gün içinde toplam 6 saat 45 dakika özel amaçlı internet kullanımı nedeniyle yükümlülüklerini yerine getirmemesi ve önemli sayılacak masrafların ortaya çıkması haklı bir fesih nedeni olarak kabul edilmiştir (Ayrıntılı bilgi için bkz. Hozar, 2007: 199-204). Buna karşılık Nürnberg Eyalet İş Mahkemesi'nin 26.10.2004 tarihli ve 6 Sa 348/03 sayılı kararına göre; işçinin bilgisayarının onarımı sırasında sık kullanılanlar bölümünde 26 adet özel nitelikli internet adresinin tespit edilmesi tek başına çalışma süresinin büyük bir kısmının internette geçirildiğini kanıtlayamaz (Bkz. Hekimler, 2005: 309-310).

[28] Buna karşılık herhangi bir düzenleme bulunmaması halinde, kural olarak işçinin mesai saatleri içinde özel amaçlı kullanım hakkına sahip olmadığı şeklindeki görüş için bkz. Okur, 2005: 53; Kuşku, 2008: 33.

[29] Bkz. Köln Eyalet İş Mahkemesi'nin 11.02.2005 tarihli ve 4 Sa 1018/04 sayılı kararı (Hekimler, 2006: 307-308).

[30] Aynı yönde bkz. Okur, 2006: 5; Kovach vd., 2002: 297. Ayrıca Hessen Bölge İş Mahkemesi'nin 04.07.2002 tarihli ve 5 Sa 987/01 sayılı kararında; işveren tarafından konulan

araçların iş amaçlı ve özel amaçlı kullanımı arasındaki fark açıklığa kavuşturularak özel amaçlı kullanımın süresi ve sınırları, buna ilişkin gerçekleştirilecek denetimin amaçları ve yöntemleri, teknik ve idari tedbirlerin kime, ne zaman, hangi istisnai durumlarda ve nasıl uygulanacağı ve işyeri politikasının ihlalinin tespitinde izlenecek usul ve uygulanacak yaptırımlar şeffaflık ilkesi uyarınca işçiye mutlaka iletilmelidir (Uncular, 2018: 253-254). Vurgulamak gerekir ki, sendikaya veya işçi temsilcilerine onay, görüş bildirme ve/veya toplu iş sözleşmesinde düzenleme yoluyla etki edebilme imkânı tanınması da önem arz etmektedir[31]. Elektronik İletişim Çalışma Belgesi'nde de yer verildiği üzere; elektronik iletişim araçlarının konumu ve mülkiyeti haberleşmenin ve yazışmaların gizliliği hakkına üstün gelemez (2002: 20).

Söz konusu elektronik araçlardan sosyal medyanın günlük hayatta giderek daha çok yaygınlaşması ile birlikte, adayların ve işçilerin yalnızca kişisel elektronik araçları ile değil, iş bilgisayarı ve/veya iş cep telefonu vasıtasıyla da internet üzerinden gerçekleştirdiği sosyal medya kullanımı ve bu kullanımın işverenler tarafından izlendiği uygulamalar artmaktadır. Sosyal medya genel olarak, kullanıcılar arasında çok çeşitli şekillerde iletişim kurmayı, belge, fotoğraf, video, ses, link veya metin yazma ve yorum yapma gibi kullanıcılar tarafından oluşturulan içerikler paylaşmayı ya da bunların dolaşımını -ve böylelikle çok büyük boyutlarda veri akışını ve işlenmesini- sağlayan ve internet üzerinden erişilebilen interaktif teknolojiler olarak ifade edilebilir. En popüler sosyal medya uygulamalarına ise Facebook, WhatsApp, Twitter, Instagram, Google+, Linkedln, YouTube, Xing, WeChat, Viber, Skype, Snapchat ve Telegram örnek olarak gösterilebilir. Bahsi geçen uygulamalar yalnızca bireylerin ve işletmelerin iletişim yöntemlerini değil, iş hayatının işleyişini de ciddi ölçüde etkilemektedir. Bu çerçevede işverenlerin ürünlerin ve hizmetlerin tanıtımı veya diğer mesleki hedeflere ulaşmak amacıyla işçilerin LinkedIn ve Xing gibi mesleki uygulamaları ve/veya Facebook, Twitter ya da benzeri kişisel uygulamaları kullanmalarını teşvik etmelerine veya zorunlu tutmalarına da sıklıkla rastlanmaktadır (Khan vd., 2011: 3). Üstelik işçilerin itibarının ve performansının müşteriler tarafından çevrimiçi değerleme yöntemleriyle belirlendiği yeni atipik çalışma türlerini doğuran Uber, Taskrabbit ve Deliveroo gibi dijital platformlarda sosyal medya kilit rol oynamaktadır.

Öte yandan işveren sosyal medya uygulamalarının tamamına ya da bir kısmına işyerinde girişi engelleyen ya da sınırlayan birtakım yöntemlere başvurabildiği gibi, adayın ve işçinin iş amaçlı ve/veya özel amaçlı sosyal medya kullanımını aday ve işçi hakkında daha detaylı, hızlı ve kolay bilgi toplamak için izlemesi de mümkün olabilmektedir (Uncular, 2018: 260)[32]. Zira adayların başvurularının sonuçlandırılmasında, işçilerin

mesai saatleri içinde özel amaçla e-posta kullanma yasağının, sözlü olarak değil, açık ve anlaşılır bir biçimde işçilere önceden yazılı olarak bildirilmiş olması gerektiği belirtilmektedir (Bkz. Hozar, 2007: 207).

[31] Aynı yönde bkz. Özdemir, 2008: 20.

[32] Veri koruma hukuku açısından işçi ve aday arasında hiçbir fark bulunmamaktadır. Zira gerek işe alınırken, gerekse iş sözleşmesi kapsamında çalışırken adayın ve işçinin zarara uğrayan

performanslarının değerlendirilmesinde ve iş ilişkisindeki yükümlülüklerin ihlalinin kanıtlanmasında[33] önemli bir kaynak haline gelen sosyal medya, adayların ve işçilerin işe ve işverene dair bakış açılarına ve özel hayatlarına yönelik ipuçları sunduğu ve işe alım, terfi, yaptırım ve hatta işten çıkarma kararlarına temel oluşturduğu için işverenlerce gerçekleştirilen izleme uygulamalarına yeni bir boyut katmaktadır. Bu itibarla sosyal medya iş geliştirme, yönetim ve çalışma performansının düzenlenmesi için yeni fırsatlar sunmakla birlikte, adayları ve işçileri gizlice ve sürekli izlenmeye maruz bırakmakta ve diğer bilgi ve iletişim teknolojilerinin silikleştirdiği özel hayat ve çalışma hayatı arasındaki sınırları giderek ortadan kaldırmaktadır[34]. Nitekim sosyal medya profillerinin varlığı ve yeni analitik teknolojilerin gelişmesi ile işverenler adayların ve işçilerin fikirleri, inançları, arkadaşları, alışkanlıkları, konumları, tavırları, ilgi alanları ve davranışları hakkında kolaylıkla bilgi toplamakta ve adayın ve işçinin özel nitelikli kişisel verileri dahil çok fazla veri elde etmektedir. Böylece işe alımda ve sözleşmenin devamında adayların ve işçilerin sosyal medya hesaplarındaki kişisel verilerinin işlenmesi olağan ve tartışmalı bir uygulama haline gelmiş olup işverenler işçilerin işyeri dışındaki davranışlarını bile sosyal medya aracılığıyla kontrol etmeye çalışmaktadırlar.

Bu kapsamda adayın ve işçinin kişisel verilerinin ve özel hayatının gizliliğinin korunması açısından en uygun yaklaşım, sosyal medyanın ne tamamen özel, ne de tamamen kamuya açık bir alan olarak kabul edilmesidir. Zira kimi kullanıcılar sosyal medya hesaplarının tamamını kamuya açık bırakırken, kimi kullanıcılar ise sosyal ağın türü ve gizlilik politikaları ile kendi gizlilik ayarları doğrultusunda pek çok farklı aşamalı erişime imkân tanıyan kısmen ya da tamamen kapalı/korumalı kullanımı tercih etmektedir[35]. Dolayısıyla kamuya açık olsun veya olmasın sosyal medyadaki içeriklerin esas olarak kullanıcının kişisel hesabının içinde yer aldığı ve kendi özerk alanına ait olduğu kabul edilmelidir (Alvarez Alonso, 2018: 313-314). Bu bağlamda adaya ve işçiye ait gerek sosyal medyada paylaşılan içerikler, gerekse sosyal medya hesapları işverenin mülkiyetinde olmayıp bu içeriklere gizlice veya zorla müdahale edilmesi adayın ve işçinin hem gizlilik beklentisine, hem de kişisel verilerin korunması hakkına aykırılık

menfaatleri aynı olup örneğin izleme uygulamalarını reddetmesi nedeniyle işçi işini kaybederken, aday da işe alınmamaktadır. Dolayısıyla iş görüşmeleri aşamasında iş sözleşmesi çerçevesindeki ekonomik bağımlılıktan söz edilemese de, adayın işe ekonomik gereksiniminin iş sözleşmesindekine benzer ve hatta daha zorlu bir dengesizlik ortaya çıkardığı yadsınamaz (Aynı yönde bkz. Sevimli, 2006: 146).

[33] Bu kapsamda İtalyan Temyiz Mahkemesi'nin 2017 yılındaki bir kararına konu dikkat çekici bir olaya göre; çok tehlikeli bir baskı makinesini kontrolsüz bırakarak çalışma alanını terk edip Facebook'ta sohbet eden bir erkek işçi hakkında kanıt toplayabilmek için işveren, mesai saati içinde işçiyi sohbete teşvik etmek amacıyla insan kaynakları müdürünü Facebook'ta kadın ismiyle sahte bir hesap açmaya ikna etmiştir. İşçinin tuzağa düşmesi üzerine ise, kanıt elde edildiğinde, iş sözleşmesi haklı nedenle feshedilmiştir (Topo ve Razzolini, 2018: 398).

[34] Aynı yönde bkz. Cervilla Garzon, 2017: 83.

[35] Aynı yönde bkz. Alvarez Alonso, 2018: 305-306.

teşkil edecektir. Sosyal medya içerikleri kural olarak iş sözleşmesinin kurulması veya ifası için de gerekli olmadığı gibi, işveren tesadüfen elde ettiği veya kullanıcının gönüllü olarak tamamen kamuya açtığı sosyal medya içeriklerindeki kişisel verileri işlerken de adayın ve işçinin haklarını ihlal edemez. Nitekim iş ilişkisi çerçevesinde adayın ve işçinin rızası, özgür iradeye dayanmaktan bir hayli uzak ve uygulamada çoğunlukla hukuka aykırılıkları meşrulaştırma aracı haline gelmiş olup gerek GVKT'de yer alan düzenlemeler ve Madde 29 Çalışma Grubu'nun ilgili görüşleri, gerekse TBK m.419 ve TMK m.24/2 doğrultusunda sosyal medya aracılığıyla gerçekleştirilen izlemeler açısından da tek başına meşru bir dayanak olarak değerlendirilmemelidir. Vurgulamak isteriz ki, işyerinde sosyal medya kullanımını, yeni yaklaşımlar gerektiren yepyeni bir olgu yerine, toplumdaki ve iş hayatındaki bireyselleşmenin ve öznelleşmenin revaçta olması, hayatın her alanının dijitalleşmesi ve metalaşması ve iş ilişkilerindeki kontrol düzeyinin sürekli artması şeklindeki uzun zamandır süregelen gelişmelerin bir devamı olarak görmek önemlidir (Risak, 2018: 442). Zira gelinen noktada çalışma yalnızca gerçek dünyada değil, sanal dünyada da söz konusu olup kişisel veriler ile sıkı bir etkileşim halindedir.

İşverenin adayın ve işçinin sosyal medyada paylaştığı bilgilere erişimini sağlayan pek çok yöntem bulunmakta olup işe alımda ve sözleşmenin devamında giderek artan şekilde başvurulan bu yöntemlerden bazıları;

- adayın ve işçinin adı internet arama motorlarına yazılarak herkese açık olan bilgilerinin incelenmesi yoluyla bilgi araştırma,
- adayın ve işçinin kamuya kapalı kişisel hesabında paylaştığı bilgilere, arkadaşlık, takip veya bağlantı kurma gibi talepler ya da diğer yollar vasıtasıyla erişme yahut adayın ve işçinin sosyal medya uygulamalarına ilişkin gizlilik ayarlarının işverenin erişimine açık olacak şekilde yeniden düzenlenmesini talep etme,
- aday ve işçi kişisel hesabına girdikten sonra işverenle birlikte hesabı inceleme ve içeriği gözlemleme,
- adaydan ve işçiden kişisel hesabının kullanıcı adı ve şifre gibi bilgilerini talep etmek suretiyle içeriğe herhangi bir kısıtlama olmaksızın doğrudan erişme

şeklinde en az müdahaleci olandan en çok müdahaleci olana doğru sıralanabilir (Kajtar ve Mestre, 2016: 25; Alvarez Alonso, 2018: 292).

İşverenlerin özellikle işe alımda internet arama motorları ve/veya kamuya açık sosyal medya uygulamaları üzerinden adayların eğitimi, yetenekleri, becerileri ve iş deneyimleri hakkında araştırma yapmaları kabul edilebilecekse de, kamuya kapalı sosyal medya profillerine gizlice veya zorla yetkisiz erişim hukuka aykırı olacaktır. Ayrıca kamuya açık olsa bile aday ve işçi tarafından paylaşılabilen aile ve arkadaşlık ilişkileri, alışkanlıklar, siyasi görüş, cinsel yönelim ve dini veya felsefi inanç gibi mesleki nitelikte olmayan kişisel veriler çeşitli önyargılar sebebiyle adayın ve işçinin aleyhine ayrımcılığa varan ciddi sonuçlara da yol açabilecektir (Sanchez Abril vd., 2012: 87). Üstelik aday ve işçi sosyal medyada hiçbir özel bilgi paylaşmamış olsa dahi, bu bilgilerin sosyal

medyadaki beğenme, kızma, üzülme, tebrik etme, etiketleme ve emoji koyma gibi tepkiler doğrultusunda veya diğer analiz yöntemleriyle tahmin edilmesi de günümüzde son derece kolaylaşmıştır (Custers ve Ursic, 2018: 324-325). ABD'de gerçekleştirilen farklı anketler işverenlerin %90'ından fazlasının işe alım sürecinde LinkedIn ve Facebook gibi sosyal medya uygulamalarını kullandıklarını ve %69'undan fazlasının sadece adayların kişisel profillerinde gördükleri bilgilere dayanarak adayları reddettiklerini ortaya koymaktadır (Alvarez Alonso, 2018: 291). Avrupa'da ise işletmelerin %30'undan fazlası işe alımda sosyal ağları kullanmaktadır[36]. Özellikle işe alım sürecinde adaylardan sosyal medya hesabının şifresinin veya erişim bilgilerinin işverenlerce talep edilmesi son derece yaygınlaşmış olup ABD'deki 18 eyalette bunu açıkça engelleyen yasal düzenlemeler kabul edilmiştir[37].

Bu çerçevede AKTK m.5/3 gereğince işverenin bir adayın veya işçinin sosyal ağlar başta olmak üzere çevrimiçi paylaştığı bilgilere erişimi zorunlu tutmaması ya da talep etmemesi gerekmektedir. Ayrıca ister özel, ister iş amaçlı kullanım olsun sosyal medyaya dair herhangi bir değerlendirme yapılırken önyargıdan uzak ve adil hareket edilerek her durumda adaya ve işçiye savunma hakkı tanınması esastır. İşverenin adayın sosyal medya profilini incelemesi ise, yalnızca kamuya açık sosyal medya hesabının mesleki amaçlara yönelik olması ve adayın becerileri ve kişilik özellikleri gibi iş teklifi ile yakından ilişkili mesleki bilgilerini içermesi halinde ve adayın sosyal medya profilinin inceleneceği hususunda önceden detaylı, anlaşılır ve net şekilde bilgilendirilmiş olmasına bağlıdır (WP, 2017: 11). İşyerinde sosyal medya kullanımına yönelik net, anlaşılır ve kapsamlı bir politika belirlenmesi de gerekli olmakla birlikte, önemli olan bu politikaların tutarlı ve adil bir şekilde uygulanması ve adayların ve işçilerin kişisel verilerinin etkin korunması bakımından işletmelerin işleyişinin ayrılmaz bir parçası haline gelmesidir[38].

İşyerinde özel amaçlı sosyal medya kullanımına izin verilmesi ve/veya işçinin bir ya da birden fazla sosyal medya uygulamasına sahip olması halinde, işverenin üye olmak, hesap/profil açmak, takipçi veya arkadaş olmak ve/veya iletişim kurmak yahut bunlara zorlamak gibi yollarla işçilerin davranışlarını izlemesi, gizlice ve sürekli kişisel verilerini toplaması ve diğer işleme faaliyetlerinde kullanması kabul edilemez (Uncular, 2018: 263). İşveren izlemenin rekabet yasağı gibi meşru menfaatlerinin korunması için gerekli olduğunu ve daha az müdahaleci bir yöntemin olmadığını ispat etmediği,

[36] Ayrıntılı bilgi için bkz. Eurostat, 2017.

[37] Detaylı bilgiler için bkz. De Stefano, 2018: 9; Levinson, 2013: 16-17.

[38] Aynı yönde bkz. Llorens Espada, 2014: 65. Nitekim ABD'deki bir anket sonuçlarına göre, katılımcıların %62'si işyerinde sosyal medyaya yönelik resmi politikaların olmadığını, %19'u işyerinde sosyal medyaya ilişkin bir politika uygulanıp uygulanmadığından haberdar olmadığını ve sadece beşte biri resmi bir sosyal medya politikasına tabi olduğunu belirtmiştir. Aynı ankette, sosyal medya politikası uygulayan bir işyerinde çalışan katılımcıların %32'si mesai saatleri içinde sosyal medya kullanımının yasaklandığını, %22'si ise bu politikaya uyulduğunu ifade etmiştir (Sanchez Abril vd., 2012: 105-106).

izlemeyi söz konusu meşru menfaatle, belirli bir süreyle ve ilgili işçiyle sınırlamadığı ve ilgili işçiyi izlemenin kapsamı hakkında açıkça, detaylı ve anlaşılır şekilde bilgilendirmediği sürece, işçinin sosyal medya hesabını veya sosyal medyadaki davranışlarını izlemesi hukuka aykırıdır (WP, 2017: 12). Öte yandan sosyal medyada özellikle iş ilişkisindeki bağımlılık unsuru nedeniyle işçinin geçerli olmayan rızasına dayanan izleme uygulamaları da hukuka ve dürüstlük kuralına aykırı olduğu gibi, işçiler işveren ile bağlantılı kurumsal/mesleki bir sosyal medya uygulaması kullanmaya da zorlanamaz. Kurumsal bir sosyal medya profilinin oluşturulması durumunda ise, işçiye her zaman kişisel sosyal medya profili kullanma imkânı da tanınmalı ve işçinin kişisel sosyal medya profilinden tamamen uzak durulmalı veya izleme yoluyla kişisel veri işlenmemelidir (WP, 2017: 12).

İşyerindeki sosyal medya kullanımını izleme uygulamaları açısından da hukukumuzda herhangi bir yasal düzenleme bulunmamakla birlikte, işverenin yönetim hakkı ve işçinin kişisel verilerin korunması hakkı arasında adil bir dengenin kurulması zorunludur[39]. Bu doğrultuda TBK m.419'a göre sözleşmenin kurulması ve ifası zorunlu kılmadığı sürece adayın ve işçinin sosyal medya kullanımı işverence izlenemez. Zorunluluğun varlığı halinde ise izlemenin, adayın ve işçinin kişisel verilerin korunması hakkına en az müdahale edecek yöntemlerle ve sosyal medyanın özel hayatın gizliliğini ve ifade özgürlüğünü de kapsayan çok boyutlu yapısı gereğince son çare olarak gerçekleştirilmesi şarttır. Önemle belirtmek isteriz ki, KVKK m.5/2(d) ve m.28/2(b) uyarınca adayın ve işçinin kamuya açık sosyal medya uygulamalarından kendisi tarafından gönüllü olarak alenileştirilmiş kişisel verileri açık rızası aranmaksızın işlenebilecek olup aday ve işçi bu işlemeye karşı sadece zararın giderilmesini talep hakkını kullanabilecektir. Bu yüzden kanımızca esas olan AKTK ve 2/2017 sayılı Görüş çerçevesinde hareket etmek olup en güvenli yol, adayların ve işçilerin -kamuya açık olanlar başta olmak üzere- tüm sosyal medya uygulamalarında yer alan kişisel verilerini titizlikle seçmeleri ve suistimallere yönelik giderek artan vakaları göz ardı etmeyerek gizlilik ayarlarına ve güvenlik önlemlerine azami özen göstermeleridir. Bu bağlamda veri sahiplerinin sosyal medya hesaplarını en azından tamamen kamuya açık hale getirmemeleri de kişisel verilerin korunması ve özel hayatın gizliliği haklarının ihlal edilme riskini en aza indirmek açısından uygun bir yöntem olarak düşünülebilecektir.

Böylelikle işverence gerek işyerindeki internetin, iş bilgisayarının ve iş cep telefonunun ve hatta kimi zaman kişisel elektronik araçların izlenmesi ile dolaylı, gerekse doğrudan gerçekleştirilen sosyal medya izleme uygulamaları bakımından da Anayasa m.90/5, TBK m.419 ve İK m.75/2 başta olmak üzere Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 sayılı Sözleşme, AİHS[40], AKTK ve diğer uluslararası kaynaklarda yer alan kurallar

[39] Aynı yönde bkz. Anton ve Ward, 1998: 904.

[40] İşçinin çevrimiçi bir hızlı mesajlaşma hizmeti olan Yahoo Messenger uygulamasındaki kişisel hesabında yer alan yazışmaların izlenmesi sonucunda işten çıkarılması üzerine AİHM'in önüne gelen ve Büyük Daire tarafından verilen 5 Eylül 2017 tarihli karar ile kesinleşen Barbulescu davasında; Yahoo

doğrultusunda hareket edilmesi büyük önem taşımaktadır. Nitekim sosyal medyada yer alan adaya ve işçiye ait kişisel verilerin hukuka, dürüstlük kuralına ve ölçülülük, şeffaflık ve eşit davranma ilkeleri başta olmak üzere veri koruma hukukunun temel ilkeleri ile iş ilişkisinin özgün niteliklerine uygun şekilde işlenmesi şarttır.

Öte yandan işverenin işçinin sosyal medya kullanımını izlemesi sonucunda başvurabileceği fesih son çare olmalı ve her halde işçinin savunmasının alınması ihmal edilmemelidir. Altını çizmek gerekir ki, ister geçerli nedenle, isterse haklı nedenle olsun feshin dayanağını oluşturan izleme uygulamasının hukuka uygun olması şarttır. Aksi takdirde, işveren haklı olsa bile haksız konuma düşecek ya da işçi sadece işinden olmakla kalmayıp insan hakkı olarak kabul edilen kişisel verilerin korunması hakkının yok sayılmasıyla da karşı karşıya kalacaktır. Kaldı ki işverenin işyerinde özel amaçlı bilgisayar, internet, telefon ve sosyal medya kullanımını tamamen yasaklaması gerek Anayasa m.13, gerekse TBK m.20-25 uyarınca geçersiz olduğundan, genel, kapsamlı ve haksız bir yasaklamaya dayanarak gerçekleştirilen İK m.18 ve İK m.25/II veya TBK m.435 doğrultusundaki fesihler de geçersiz veya haksız olacaktır. Üstelik işveren bu durumda fesih hakkını kötüye kullanmış olduğundan, İK m.18 kapsamında iş güvencesine tabi olmayan işçiler İK m.17/6'ya göre ve İK kapsamına girmeyen işçiler TBK m.434'e göre kötü niyet tazminatına da hak kazanabilecektir.

Bu itibarla Yargıtay 9. HD'nin 2017 yılındaki isabetli bir kararında[41]; WhatsApp uygulamasının, telefondan ve bilgisayardan internet vasıtasıyla iletişimi gerçekleştiren ücretsiz bir program olduğuna, burada diğer kullanıcılarla bireysel mesajlaşmak ve/veya sesli ya da görüntülü arama yapmak suretiyle iletişime geçilebildiği gibi, kurulan gruplar üzerinden iletişim sağlanmasının da mümkün olduğuna, grup içindeki iletişim grup dışındaki kişilere kapalı olduğundan işçilerin iş akışını bozmadıkları ve çalışmaları etkilemedikleri sürece bir WhatsApp grubu kurmalarının ve burada iletişim halinde olmalarının yasak olmadığına ve işçilerin bu kapsamdaki iletişimlerinin kişisel veri olarak da korunması gerektiğine hükmedilmiştir[42]. İşverenin WhatsApp grubunda gizli kalması gereken kişisel verileri aynı grup içinde yer alan diğer bir işçi vasıtasıyla hukuka aykırı şekilde elde ettiği de vurgulanmıştır. Ayrıca Yargıtay 7. HD'nin 2014 tarihli son derece yerinde bir kararına

Messenger uygulamasının bireylerin özel bir sosyal hayat sürmelerine olanak sağlayan iletişim çeşitlerinden sadece biri olduğu ve bu tip uygulamalar vasıtasıyla yapılan yazışmaların iş bilgisayarı kullanılsa dahi haberleşme kavramının içinde yer aldığı ortaya konmuş ve AİHS m.8'in uygulanabilirliğine karar verilmiştir (Bkz. para.74 ve 81).

[41] Bkz. Yargıtay 9. HD'nin 01.06.2017 tarihli ve 2016/14203E. ve 2017/9524K. sayılı kararı.

[42] Yargıtay 9. HD'nin benzer bir değerlendirmeye yer verdiği 2019 tarihli bir kararında; davacının ve bir kısım iş arkadaşının cep telefonu vasıtasıyla kullandığı WhatsApp uygulamasındaki yazışmaları gerekçe gösterilerek İK m.25/II kapsamında gerçekleştirilen fesih, salt gizlilik içeren kişisel veri niteliğindeki WhatsApp yazışmalarına dayandığından, haksız bulunmuştur (Bkz. Yargıtay 9. HD'nin 10.01.2019 tarihli ve 2018/10718E. ve 2019/559K. sayılı kararı).

göre; işçinin kişisel sosyal medya hesabında mesai saatleri dışında ve bizzat işveren tarafından verilen araç ve gereçler kullanılmadan yaptığı bazı paylaşımlar, iş sözleşmesine ve eklerine aykırı bir eylem meydana getirmemekte ve iş akdinin feshi için haklı veya geçerli bir neden oluşturmamaktadır[43].

Yargıtay 7. HD'nin 2015 tarihli oldukça önemli bir kararına[44] konu olayda ise; 07.08.2012 tarihinden beri Tek Gıda İş Sendikası'na üye olan davacının, Facebook'ta "işten atılan işçiler geri alınana kadar tüketimden gelen gücümüzü kullanalım lütfen ……. ürünleri almayalım, aldırmayalım" ifadelerini içeren bir pankarta ilişkin paylaşılan fotoğrafı ve "Anayasal hakkımızı kullandık, sendikaya üye olduk, ……. işvereni işten attı, …….. ürünleri tüketmiyoruz" ifadelerini içeren amblemin bulunduğu bir sendika sayfasını beğendiğinin tespit edilmesi üzerine hem kendi, hem de eşinin iş sözleşmesi İK m.25/II uyarınca haklı nedenle feshedilmiştir. Bu bağlamda Yargıtay 7. HD, davacının işverenin ürünlerinin tüketilmemesine ilişkin sosyal medyada yapacağı bir paylaşımın sadakat borcuna aykırılık teşkil edeceğine ve fakat somut olayda davacının beğendiği paylaşımların sendikaya üyelik nedeniyle işten çıkarılan işçilerin geri alınmasına yönelik ve sendikal faaliyetlerin engellenmeye çalışılmasına karşı baskı yaratmayı amaçlayan demokratik bir eylem oluşturduğuna, davacının işverenin marka imajını zedeleme, ürünlerini kötüleme veya şiddet çağrısında bulunma gibi bir niyetinin olmadığına ve sendikal faaliyet kapsamında kalan bu sosyal medya beğenileri ile davacının Anayasa'dan kaynaklanan sendikal hakkını kullandığına hükmetmiştir[45].

Buna karşılık Yargıtay 22. HD'nin 2016 yılındaki bir kararına[46] konu olaya göre; yaklaşık 8 yıl boyunca banka müfettişi olarak çalışan davacının dava dışı bir iş arkadaşı, güvenlik kamerası izleme odasında genel müdür ile yönetim kurulu başkanının odalarının bulunduğu koridoru izlerken genel müdürün -odasının önünde bulunan kutuları görünce- görevden ayrılacağı düşüncesiyle ekrandaki görüntüyü fotoğraflayıp cep telefonundaki WhatsApp uygulaması ile davacıya göndermiş ve davacı da bu fotoğrafı müfettiş arkadaşlarıyla iletişim kurduğu WhatsApp grubunda paylaşmıştır. Bunun üzerine iş

[43] Bkz. Yargıtay 7. HD'nin 03.06.2014 tarihli ve 2014/6519E. ve 2014/12285K. sayılı kararı.

[44] Bkz. Yargıtay 7. HD'nin 04.06.2015 tarihli ve 2015/21301E. ve 2015/11054K. sayılı kararı.

[45] Öte yandan benzer bir olaya dayanan başka bir davada; yerel mahkeme, davacının davranışının, sosyal paylaşım sitesinde sendikal faaliyet olarak yapılan boykota yönelik bir yazıyı beğenmekten ibaret olduğuna, bu davranışın tek başına sadakat ve özen yükümlülüğüne aykırılık teşkil etmeyeceğine ve davacının iş saatleri dışında sosyal paylaşım sitesinde yaptığı beğenme eyleminin haklı ve geçerli nedenle fesih gerekçesi oluşturmayacağına karar vermiştir. Ancak söz konusu karar Yargıtay 9. HD tarafından bozularak yalnızca işten çıkarılan işçilerin geri alınması konusunda yapılmış bir çağrının sosyal medya profilinde paylaşılmasının fesih nedeni olamayacağı belirtilmekle birlikte, boykot yönünde bir çağrıyı da içeren ilanın sosyal medyada beğenilmesinin sadakat borcunun ihlali niteliğinde olduğu ve haklı neden ağırlığında olmasa da, fesih için geçerli neden oluşturduğu kabul edilmiştir (Bkz. Yargıtay 9. HD'nin 17.09.2015 tarihli ve 2015/19277E. ve 2015/26072K. sayılı kararı).

[46] Bkz. Yargıtay 22. HD'nin 25.02.2016 tarihli ve 2016/2198E. ve 2016/5732K. sayılı kararı.

sözleşmesi geçerli nedenle feshedilen davacı işe iade davası açmış ve yerel mahkeme dava konusu olayın doğruluk ve bağlılığa aykırı olmaması nedeniyle davanın kabulüne karar vermiştir. Ne var ki Yargıtay 22. HD davalı bankanın genel müdürünün görevden alındığı izlenimini verecek nitelikteki bir görüntünün kurum dışına sızmasının özellikle basına yansıması halinde ekonomik açıdan sakıncalar doğuracağı gerekçesiyle davacının eyleminin İK m.25/II(e) gereğince doğruluk ve bağlılığa uymayan davranış teşkil ettiğini ve işyerine ait bir sırrın ifşası niteliği taşıdığını belirterek iş sözleşmesinin haklı sebeple feshedildiğine oyçokluğuyla hükmetmiştir. Karşı oy değerlendirmesinde ise; herkese açık olmayan bir WhatsApp grubu içinde fotoğraf paylaşma eyleminin, iş hukukunun en temel ilkelerinden biri olan işçi lehine yorum ilkesi gereğince ne haklı fesih, ne de geçerli fesih nedeni sayılabileceği vurgulanmış ve bir uyarı ile çözümlenebilecek hatalı bir davranışın birtakım farazi risklere dayanarak işçinin aleyhine an ağır sonuç olan işten çıkarma için gerekçe gösterilmesi isabetli bulunmamıştır.

Belirtmek gerekir ki, Yargıtay 9. HD'nin 01.06.2017 ve 10.01.2019 tarihli bahsi geçen iki kararı hariç Yargıtay kararlarında işçinin sosyal medya kullanımının izlenmesine yönelik veri koruma hukuku açısından herhangi bir değerlendirme veya tespit yer almamaktadır. Somut olay açısından isabetli kabul edilebilecek kararlarda dahi genellikle, işverence gerçekleştirilen izlemenin hukuka uygun olup olmadığının, sosyal medyanın ve iletişimin iş ilişkisindeki yerinin ve işçinin kişisel verilerin korunması hakkının ihlal edilip edilmediğinin incelenmesine rastlanmamaktadır. Bu durum işveren tarafından işçinin sosyal medya kullanımına dayanarak gerçekleştirilen fesihlerin, gerek iş hukuku, gerekse veri koruma hukuku mevzuatında öngörülen kişisel verilerin korunmasına dair temel ilkeler ve kurallar dikkate alınmadan veya ikinci planda bırakılarak çok boyutlu ve adil bir bakış açısından uzak bir karara varılmasına yol açabilmekte ve sosyal medya kullanımının, kişisel veriler ile yakından ilişkili olan doğasına da ters düşmektedir. Bu kapsamda vurgulamak gerekir ki, Barbulescu davasında; ulusal makamlar işçinin özel hayata ve haberleşmeye saygı haklarının uygun şekilde korunmasını sağlayamadıkları ve somut olayda adil bir menfaat dengesini kuramadıkları için AİHS m.8'in ihlal edildiğine hükmedilmiştir. Zira AİHM'e göre ulusal mahkemelerin, izleme tedbirlerinin uygulanmasına yönelik meşru nedenler olup olmadığını, işverenin işçinin özel hayatına ve haberleşmesine daha az müdahaleci tedbirlere başvurup başvuramayacağını ve izleme uygulamalarının işçinin haberi olmadan gerçekleştirilip gerçekleştirilemeyeceğini tespit etmeleri şarttır. Söz konusu kararda da ortaya konduğu üzere, feshin dayanağını oluşturan izlemenin ve delillerin hukuka uygunluğunun hem veri koruma hukuku, hem de iş hukuku çerçevesinde titizlikle değerlendirilmesi büyük önem taşımaktadır.

Öte yandan işverenin sosyal medya kullanımına yönelik hukuka aykırı izleme uygulamaları sonucunda sözleşmeyi haklı veya geçerli nedenle feshetmesi, işçinin kişisel verilerin korunması hakkı ile işverenin yönetim hakkı arasındaki dengenin işveren lehine bozulmasına yol açmaktadır. Nitekim sözleşmeyi ihlal etmesinin karşılığı olarak veya ihlal ettiği iddiasını kanıtlayabilmek adına (üstelik kimi durumlarda ihlal etmemiş olsa bile) işçinin kişisel verilerin korunması hakkı görmezden gelinmekte ve işverenin hukuka aykırı izleme

uygulamaları ile hukuka aykırı deliller yargı eliyle meşruluk kazanabilmektedir. Oysaki iş sözleşmesinin ihlalinin gerçekten varlığı dahi, işçinin insan haklarının çiğnenmesine zemin hazırlayamaz. Zira sözleşmenin ihlali ile işçinin kişisel verilerin korunması hakkının ihlali birbirinin karşılığını veya dengini değil, somut olayın farklı boyutlarını oluşturmakta olup esas olan iki tarafın da hukuka aykırı hareket etmemesidir. Dolayısıyla bilgi ve iletişim teknolojilerinin etkisiyle iş ilişkisinin dönüşümüne tanıklık ettiğimiz bu dijital çağda, ulusal ve uluslararası mahkeme kararlarının da adayın ve işçinin kişisel verilerinin korunmasına yönelik daha etkin, adil ve kapsamlı bir güvence oluşturması zaruridir.

Sonuç

Hayatın her alanı gibi iş ilişkisini de etkisi altına alan bilgi ve iletişim teknolojileri vasıtasıyla adayların ve işçilerin işyeri içinde ve dışında çeşitli şekillerde izlendiği uygulamalar oldukça yaygınlaşmıştır. Bu itibarla elektronik ve biyometrik giriş kontrol sistemleri, elektronik yer belirleme sistemleri ve sosyal medya vasıtasıyla gerçekleştirilen izleme uygulamaları da giderek iş hayatının olağan bir parçası haline gelmektedir. İş ilişkisinde yaşanan bu dönüşüm adayın ve işçinin kişisel verilerin korunması ve özel hayatın gizliliği hakları ile işverenin işyerini korumadaki ekonomik ve kişisel menfaatleri arasında adil bir dengenin kurulması için teknolojik gelişmelerin de dikkate alınmasını zorunlu kılmaktadır.

Bu çerçevede işyerine, işyerindeki bazı bölümlere ve/veya katlara girişi ve çıkışı denetlemek için işçilere ait sınırlı ve özel nitelikte olmayan verilerin yüklendiği çipli veya manyetik kart gibi elektronik giriş kontrol sistemlerinin kullanılması esas olup parmak izi, avuç içi veya retina taraması gibi biyometrik giriş kontrol sistemlerine başvurulabilmesi, biyometrik verilerin özel nitelikli kişisel veri olması da dikkate alındığında ancak olağanüstü güvenlik gerektiren çok istisnai görevler açısından mümkün olabilir. Öte yandan başta atipik çalışanlar olmak üzere işçinin iş cep telefonuna, iş aracına ve/veya hareket edebilen diğer araçlara/cihazlara yüklenecek elektronik yer belirleme sistemleri ile işyeri dışındaki her hareketinin ve davranışının izlenmesi işverenin yönetim hakkını kötüye kullanması nedeniyle hukuka aykırılık teşkil edecektir. Kaldı ki alışkanlık, hobi ve karakter özellikleri gibi kişiye özel bilgileri de ifşa etmesi ayrımcılığa ve hırsızlık, gasp ve tehdit gibi çeşitli suçlarda kullanılması güvenlik sorunlarına yol açabildiğinden, konum verilerinin de özel nitelikli kişisel veri olarak kabul edilmesi gerekmektedir. Ayrıca işveren işyerinde bilgisayar, internet, sosyal medya ve telefon gibi elektronik araçların kullanımını düzenleyebilme yetkisine sahip olsa da, adayın ve işçinin sosyal medya kullanımına yönelik izlemeleri kişisel verilerin korunması hakkını yok saymadan son çare olarak gerçekleştirmek zorundadır. Üç uygulama bakımından da unutulmamalıdır ki, adaya ve işçiye ait kişisel veriler başta TBK m.419 ve İK m.75/2 olmak üzere veri koruma hukukunun temel ilkelerine ve iş ilişkisinin özgün niteliklerine uygun olarak işlenmelidir. Aksi takdirde işverenin adayı ve işçiyi hukuka aykırı şekilde izlemesi hem uygulamayı geçersiz hale getirecek, hem de elde edilen

kişisel veriler olası bir uyuşmazlıkta hukuka aykırı delil oluşturacaktır. Kanımızca işverenin bahsi geçen izleme uygulamalarına karşı adayın ve işçinin kişisel verilerinin adil ve etkin şekilde korunmasının gerçekten sağlanabilmesinde önemli olan, iş ilişkisinde kişisel verilerin korunmasına yönelik sosyal adalet ve insan onuru temelinde bir bilinç oluşturulması ve ülkemizde bu bilinci sağlamlaştırmaya hizmet edecek yasal düzenlemelerin ve yargı kararlarının artmasıdır.

KAYNAKÇA:

Akgül, A. (2015) "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", **Türkiye Barolar Birliği Dergisi**, 118, 199-222.

Alvarez Alonso, D. (2018) "Social Media in the Employment Relationship Context: A Typology of Emerging Conflicts, and Notes for the Debate", **Comparative Labor Law&Policy Journal**, 39, 287-322.

Andenas, M. ve Zleptnig, S. (2003) "Surveillance and Data Protection: Regulation Approaches in the EU and Member States", **European Business Law Review**, Vol.14, Issue 6, 765-813.

Anton, G. ve Ward, J. J. (1998) *Every Breath You Take: Employee Privacy Rights in the Workplace- An Orwellian Prophecy Come True?*, Labor Law Journal, Vol.49, Issue 3. http://connection.ebscohost.com/c/articles/493912/every-breath-you-take-employee-privacy-rights-workplace-orwellian-prophecy-come-true (19.05.2020)

Article 29 Data Protection Working Party (2002) *Working Document on the Surveillance of Electronic Communications in the Workplace,* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (19.05.2020).

Article 29 Data Protection Working Party (2005) *Opinion on the Use of Location Data With a View to Providing Value-Added Services,* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf (19.05.2020).

Article 29 Data Protection Working Party (2011) *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices,* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf (19.05.2020).

Article 29 Data Protection Working Party (2012) *Opinion 3/2012 on Developments in Biometric Technologies*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (19.05.2020).

Article 29 Data Protection Working Party (2017) *Opinion 2/2017 on Data Processing at Work*, https://ec.europa.eu/newsroom/document.cfm?doc_id=45631 (19.05.2020).

Ayözger Öngün, A. Ç. (2019) **Kişisel Verilerin Korunması Hukuku- Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, İstanbul: Beta Yayınları.

Boydak, A. B. (2017) "İşyerlerinde Uygulanan Parmak İzli Giriş Kontrol Sistemine Hukuki Bakış", **TAAD**, Yıl: 7, S.30, 321-336.

Calvo Gallego, F. J. (2012) "TIC y Poder de Control Empresarial: Reglas Internas de Utilización y Otras Cuestiones Relativas al Uso de Facebook y Redes Sociales", **Aranzadi Social. Revista Doctrinal**, 4(9), 125-151.

Cervilla Garzon, M. J. (2017) "Efectos del Uso de La Aplicación 'Whatsapp' en el Marco de Las Relaciones Laborales", **Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social**, 136, 73-98.

Civan, O. E. (2015) **Genel İş Koşulları**, İstanbul: Beta Basım A.Ş.

CNIL (2018a) *L'Accès aux Locaux et le Contrôle des Horaires sur le Lieu de Travail*, https://www.cnil.fr/fr/lacces-aux-locaux-et-le-controle-des-horaires-sur-le-lieu-de-travail (19.05.2020).

CNIL (2018b) *La Géolocalisation des Véhicules des Salariés*, https://www.cnil.fr/fr/la-geolocalisation-des-vehicules-des-salaries (19.05.2020).

Custers, B. ve Ursic, H. (2018) "Worker Privacy in a Digitalized World under European Law", **Comparative Labor Law&Policy Journal**, 39, 323-344.

De Stefano, V. (2018) *'Negotiating the Algorithm': Automation, Artificial Intelligence and Labour Protection*, Employment Working Paper No.246, Employment Policy Department**,** International Labour Office, Geneva. https://www.ilo.org/wcmsp5/groups/public/---ed_emp/---emppolicy/documents/publication/wcms_634157.pdf (19.05.2020).

Ertürk, Ş. (2013) "Genel İş Koşulları ve Genel İş Koşullarının Denetlenmesi", **DEÜHFD,** Prof. Dr. M. Polat Soyer'e Armağan, C.15, Özel Sayı, 81-118.

European Union Agency for Fundamental Rights and Council of Europe (2018) *Handbook on European Data Protection Law- 2018 Edition*, Luxembourg. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (19.05.2020).

Eurostat (2017) *Social Media Statistics on the Use by Enterprises*. http://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_-_statistics_on_the_ use_by_enterprises (19.05.2020).

Eyüboğlu, M. (2010) *Parmak İzi Uygulaması Hakkında Hukuki Değerlendirme,* İstanbul Tabip Odası. https://www.istabip.org.tr/148-parmak-zi-uygulamas-hakknda-hukuki-deerlendirme--av-meric-eyuebolu-.html (19.05.2020).

Fernandez Villazon, L. A. (2003) **Las Facultades Empresariales de Control de La Actividad Laboral**, Aranzadi.

Goñi Sein, J. L. (2009) "Controles Empresariales: Geolocalización, Correo Electrónico, Internet, Videovigilancia y Controles Biométricos", **Justicia Laboral: Revista de Derecho del Trabajo y de la Seguridad Social**, 39, 11-58.

Gürsel, İ. (2016) **İşçinin Kişisel Verilerinin Korunması Hakkı**, Ankara: Adalet Yayınevi.

Hekimler, A. (2005) "Alman Federal Mahkeme Kararları", **Çalışma ve Toplum Ekonomi ve Hukuk Dergisi**, S.7, 2005/4, 301-312.

Hekimler, A. (2006) "Alman Federal Mahkeme Kararları", **Çalışma ve Toplum Ekonomi ve Hukuk Dergisi**, S.10, 2006/3, 305-314.

Hozar, N. N. (2007) "Özel Amaçla İnternet ve E-Posta Kullanımının İş İlişkisine Etkisi", **Sicil İş Hukuku Dergisi,** Yıl:2, S.7, 199-207.

Kajtar, E. ve Mestre, B. (2016) *Social Networks and Employees' Right to Privacy in the Pre-Employment Stage: Some Comparative Remarks and Interrogations*, Hungarian Labour Law E-Journal. http://hllj.hu/letolt/2016_1_a/A_02_Kajtar_Mestre_hllj_2016_1.pdf (19.05.2020).

Karademir, A. (2015) "İşyerinde İnternetin Özel Amaçla Kullanımı ve İşverence Gözetlenmesi", **Terazi Hukuk Dergisi**, 112, 56-74.

Khan, S., Moore, R. ve Weal, M. (2011) *Social Media on the Job: An Exploration of the Potential Legal Consequences of Employees' Social Media Activities During the Course of Employment*, WebSci'11 Proceedings of the 3rd International Web Science Conference Article No.19. https://eprints.soton.ac.uk/272348/1/Sarosh_paper.pdf (19.05.2020).

Kişisel Verileri Koruma Kurumu (2018) *Açık Rıza Rehberi,* https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096 fd7de.pdf (19.05.2020).

Kovach, K. A., Jordan, J., Tansey, K. ve Raminan, E. (2002) *The Balance Between Employee Privacy and Employer Interests*, Business and Society Review, Vol.105, Issue 2. https://onlinelibrary.wiley.com/doi/pdf/10.1111/0045-3609.00082 (19.05.2020).

Kuner, C. (2007) **European Data Protection Law, Corporate Compliance and Regulation**, UK: Oxford University Press.

Kuşku, Ç. (2008) **İşverenin İşçinin İnternet ve E-Posta Kullanımına Müdahalesi ve İşçinin Kişilik Hakları**, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Küzeci, E. (2018) **Kişisel Verilerin Korunması**, Ankara: Turhan Kitabevi Yayınları.

Lane, F. S. III (2003) **The Naked Employee- How Technology is Compromising Workplace Privacy**, New York: Amacom.

Levinson, A. R. (2013) *Social Media, Privacy, and the Employment Relationship: The American Experience*, Spanish Labour Law and Employment Relations Journal, Vol.2, No.1. https://e-revistas.uc3m.es/index.php/SLLERJ/article/view/1838/839 (19.05.2020).

Llorens Espada, J. (2014) "El Uso de Facebook en Los Procesos de Selección de Personal y La Protección de Los Derechos de Los Candidatos", **Revista de Derecho Social**, 68, 53-66.

Manav, A. E. (2015) "İş İlişkisinde İşçinin Kişisel Verilerinin Korunması", **GÜHFD**, C.XIX, S.2, 95-136.

Melzer, N. (2002) "Austria", **Employment Privacy Law in the European Union: Surveillance and Monitoring**, Frank Hendrickx (Ed.), Intersentia Publishers, 7-21.

Mollamahmutoğlu, H., Astarlı, M., Baysal, U. (2014) **İş Hukuku**, Ankara: Turhan Kitabevi Yayınları.

Okur, Z. (2005) "İşyerinde İşçinin Bilgisayar ve İnterneti Özel Amaçlı Kullanımının İş İlişkisine Etkisi", **Kamu-İş İş Hukuku ve İktisat Dergisi**, C.8, S.2, 47-75.

Okur, Z. (2006) "Yeni Teknoloji ve İş Hukuku", **Çimento İşveren Dergisi**, C.20, S.3, 4-19.

Okur, Z. (2013) **İş Hukuku'nda Elektronik Gözetleme**, İstanbul: Legal Kitapevi.

Özdemir, E. (2008) "İnternet ve İş Sözleşmesi: Yeni Teknolojilerin İş İlişkisine Etkileri Üzerine", **Sicil İş Hukuku Dergisi**, Yıl:3, S.10, 13-24.

Özdemir, H. (2010) "İşyerinde İşçilerin İzlenmesi ve İşçinin Kişilik Haklarının Korunması", **EÜHFD**, C.XIV, S.1-2, 231-270.

Risak, M. (2018) "Employer Acquisition and Use of the Contents of Employee Social Media: An Overview", **Comparative Labor Law&Policy Journal**, 39, 441-447.

Sanchez Abril, P., Levin, A. ve Del Riego, A. (2012) "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee", **American Business Law Journal,** Vol.49, Issue 1, 63-124.

Sevimli, K. A. (2006) **İşçinin Özel Yaşamına Müdahalenin Sınırları**, İstanbul: Legal Yayıncılık.

Sevimli, K. A. (2011) "Veri Koruma Hukuku İlkeleri Işığında Türk Borçlar Kanunu Madde 419", **Sicil İş Hukuku Dergisi**, Yıl:6, S.24, 120-141.

Sevimli, K. A. (2017) *İşçinin Kişisel Verilerinin İşlenmesi İçin Verdiği Rızanın Hukuki Değeri*, Toprak İşveren, S.116, http://dosya.toprakisveren.org.tr/dergi/2018-116.pdf (19.05.2020).

Süzek, S. (2017) **İş Hukuku**, İstanbul: Beta Basım A.Ş.

Tekergül, M. (2011) "İşyerinde Elektronik Gözetim Uygulamaları", **Sicil İş Hukuku Dergisi**, Yıl:6, S.23, 54-81.

Topo, A. ve Razzolini, O. (2018) "The Boundaries of the Employer's Power to Control Employees in the ICTs Age", **Comparative Labor Law&Policy Journal**, 39, 389-419.

Uncular, S. (2018) **Kişisel Verilerin Korunması Kanunu ve AB Genel Veri Koruma Tüzüğü Kapsamında İş İlişkisinde İşçinin Kişisel Verilerinin Korunması**, Ankara: Seçkin Yayıncılık.

Wallach, S. (2011) "The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy", **International Journal of Comparative Labour Law and Industrial Relations**, Vol.27, Issue 2, 189-219.

Yücedağ, N. (2019) "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler", **Kişisel Verileri Koruma Dergisi**, C.1, S.1, 47-63.