

# Panoptikon'un Elektronik Dirilişi: Etik Bir Sorun Olarak İşyeri İzleme

Köksal Büyük\*, Uğur Keskin\*\*

**Öz:** Çalışanların verimliliğini artırmak düşüncesiyle giderek yaygınlaşan bir elektronik izleme dünyasında yaşamaktayız. Bu konudaki yasal düzenlemelerin eksikliği, izlemenin iş hayatından özel hayata doğru kaymasına neden olmaktadır. Bu tür izlemelere sınır getirmemek, örgütsel etkinlikte kayıplar meydana getirdiği gibi çalışanların psikolojisi üzerinde de negatif etkiler ortaya çıkarmaktadır. Son yıllarda teknolojik alanlarda meydana gelen hızlı değişimler, elektronik takip sistemlerinin maliyetlerini büyük oranda düşürmüştür, bunun sonucu olarak da her geçen gün yeni elektronik izleme araçları çalışma hayatı içerisinde yer bulmaya başlamıştır. Bu çalışmanın problemi, "Bir organizasyonda etik bir sorun oluşturmayacak şekilde doğru bir izleme nasıl yapılır?" sorusuna yanıt verecek çözüm yollarını ortaya koymaktır. Bu amaçla kapsamlı bir yazın taraması gerçekleştirilmiş ve bulgular tartışılmıştır. Gerekli olmadığı hâlde kurulan bir izleme sistemi, hem işletme açısından bir maliyet hem de çalışanlara güvensizliğin göstergesidir. İşyerinde etik olmayan mahremiyet ihlallerinin önüne geçebilmek için çeşitli uluslararası örgütlerin belirlediği ilkeler doğrultusunda, izlemenin sınırlarının açıkça tüm çalışanlara beyan edilmesi gerekmektedir.

**Anahtar Kelimeler:** İşyerinde Gözetleme, Panoptikon, Elektronik İzleme, Çalışan Mahremiyeti, İş Etiği.

Enformasyon teknolojilerinin gelişimi, çalışma biçimlerini ve iş gücü yapısını önemli ölçüde etkilemiştir. Tarihin hiçbir döneminde çalışanlar, bugünkü kadar sıkı bir gözetim altında tutulmamışlardır. Bu durum sanayi toplumundan enformasyon toplumuna dönüşümün sonuçlarından birisidir. Enformasyon toplumu, 2. Dünya Savaşı esnasında askerî ve savunma amaçlarıyla kullanılan bilişim teknolojilerinin 1970'lerde iş dünyasına girmesiyle organizasyon yapılarında meydana getirdiği köklü değişimler sonucunda doğmuştur. 1980'lerden sonra bilginin stratejik bir rekabet

\* Sorumlu yazar, Dr., Eskişehir Osmangazi Üniversitesi İşletme Bölümünde yardımcı doçenttir. Çalışma alanları arasında stratejik performans yönetimi, yönetim felsefesi, yönetim ahlakı, kurumsal yönetim yer almaktadır.

*İletişim:* Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Eskişehir, Türkiye.  
Ş Elektronik posta: koksalsbuyuk@gmail.com Ş Tel.: +90 222 239 37 50/1038.

\*\* Dr., çalışma alanları arasında insan kaynakları yönetimi, yönetim felsefesi, performans yönetimi yer almaktadır.

*İletişim:* Hava Teknik Okulları Komutanlığı, Gaziemir, İzmir, Türkiye.  
Ş Elektronik posta: ugunkeskin08@gmail.com Ş Tel.: +90 232 251 1600 /4497.

unsuru hâline dönüşmesiyle bilgi toplumuna dönüşüm hızlanmıştır. Bu dönüşümün meydana getirdiği yeni ekonomiye ait mamul ve hizmetler, yönetim alanında enformasyonun bilgiye dönüşmesini ve bilginin yönetimini, işlenmesini ve dağıtımını ön plana çıkarmıştır. Bilişim teknolojilerinin hızlı gelişimi iş süreçlerinin, örgüt yapılarının, iş gücü profiline, ürün ve hizmetlerin yapısında hızlı değişiklikler yapılmasını zorunlu kılmıştır. Bu açıdan değerlendirildiğinde yeni ekonomi mikro ve makro birimlerde bir zihniyet ve anlayış değişikliğini ifade etmektedir (Söylemez, 2001). Castells'e (2005, s. 99) göre ise bu değişimin sonucu, enformasyona ve ağ örgütlenmesine dayanan küresel bir ekonomidir. Yaşanan bu dönüşüm örgütsel tasarımları da etkilemiştir. Dik ve sabit örgüt yapıları yerini esnek örgütlere, stratejik iş birimleri ve ürünlere odaklanan perspektif yerini İKY yeteneklerine odaklanan perspektife, pazarda kitlesel tüketim hedefi yerini niş tüketim ürünlerine, kitlesel seri üretim yerini bilişim teknolojileriyle desteklenen esnek üretime, sabit ve sınırlı yetenekler gerektiren işler yerini çok yönlü yetenekler gerektiren çeşitli işlere bırakmaktadır (Erdemir, 2007, s. 74).

1990'lı yılların özellikle ikinci yarısından itibaren gelişmiş ülkelerde olduğu gibi ülkemizde de bilgi toplumu olma yönündeki faaliyetlerin arttığı görülmektedir. Bu dönüşüm sürecinde mahremiyetin korunmasına yönelik tedbirler alınmadığı takdirde sıklıkla etik ihlallerle karşılaşılabilceği de görülmektedir.

Çalışmanın amacı, işyerindeki izleme faaliyetlerinin yaygınlaşmasının çalışan mahremiyeti açısından doğurduğu olumsuz sonuçların etik açıdan ne gibi sorunlar oluşturduğunun ortaya konmasıdır. Çalışmanın ilk bölümünde konuya dair kavramsal bir çerçeve oluşturmak amacıyla izleme faaliyetlerinin çalışan mahremiyeti üzerindeki olumsuz etkileri üzerinde durulmuş, ardından örgütsel açıdan izleme faaliyetlerinin meşruiyet kaynakları tartışılmıştır. İkinci bölümde ise modern hayatın oluşturduğu denetim mekanizması Panoptikon metaforuyla açıklanarak iş dünyasında elektronik olarak aynı anlayışın nasıl yeniden yükselişe geçtiği açıklanmaktadır. Sonuç bölümünde organizasyonların ve yöneticilerin işyeri izlemede benimsemesi gereken etik ilkeler üzerinde durularak, etik sorunların nasıl engellenebileceğiyle ilgili genel bir değerlendirme yapılmaktadır.

## İşyerinde Mahremiyetin Tükenişi: Örgütsel Gözetim

Mahremiyet, bireyin başkaları tarafından ne ölçüde tanınıp bilindiği, başkalarının fiziksel olarak bireye ne ölçüde ulaşabilir olduğu, bireyin başkalarının ilgisinin ve dikkatinin ne ölçüde nesnesi olduğu hususlarıyla açıklanabilecek bir kavramdır (Yüksel, 2009, s. 278). Organizasyon, çalışanlara yönelik temel bazı ahlaki sorumlulukları yerine getirmelidir. Bu sorumlulukların başında çalışanların fikirlerine, insanlık onuruna, özel yaşamlarının gizliliğine saygı duymak gelmektedir (Bowie ve Duska, 1990, s. 86). Mahremiyet kavramı üç farklı düzlemde değerlendirilebilir. Birincisi, kişiyi çevreleyen yakın fiziksel alanı korumayı kapsayan mekânsal mahremiyet; ikincisi, kişiyi haksız müdahalelere karşı korumayı kapsayan bireysel mahremiyet ve üçüncüsü de kişisel verilerin toplanma, saklanma, işlenme ve dağıtımının nasıl yapılacağını kapsayan bilgi mahremiyetidir (Eralp, 2013). Mahremiyet çalışma hayatı içerisinde değerlendirildiğinde işgören mahremiyeti ile ilgili tartışmalar genellikle üç ana başlık altında toplanmaktadır. Birincisi, telefon ve bilgisayar gibi teknolojik araçların kullanımının izlenmesidir. İkincisi çalışanların işyerindeki davranışlarının veya performanslarının kameralar aracılığıyla gözetlenmesidir. Üçüncü başlık ise çalışanlara ait kişisel bilgilere sahip olan işletmelerin bilgi güvenliğini sağlamalarıdır (Erdemir ve Çelikleş, 2006, s. 90).

İlgili literatür incelendiğinde izleme ve gözetleme/gözetim kavramlarının farklı anlamlarda kullanıldığı görülmektedir. İş dünyasında artan yoğun rekabet, insanın kapasitesinden en üst düzeyde yararlanabilmek için sıkı bir gözetim altında tutulmasını gündeme getirmektedir. İzleme (monitoring), amaca bağlı olmaksızın işyeri ve çalışanlarla ilgili olarak otomatik bir şekilde toplanan bilgileri ifade etmektedir. Diğer yandan gözetim (surveillance), bir otoriteyle davranışı kontrol edilmek istenen kişi arasındaki ilişki olarak tanımlanırken daha dar kapsamlıdır (Yılmaz, 2005, s. 3). İzleme, çalışanların performanslarının çeşitli yazılım ve elektronik donanımlar vasıtasıyla incelenerek raporlama sürecini kapsar (Alder ve Ambrose, 2005). İzleme, amaca bağlı olmaksızın çalışma hayatıyla ve işle ilgili olan enformasyonun sürekli ve düzenli olarak kayıt altına alınmasıdır (Botan, 1996, s. 294). İzleme ve teknoloji arasında sıkı bir ilişki söz konusudur. Teknolojinin, çalışanları ne kadar görünür kıldığı, gözetim yapan otoriteyi ne kadar görünmez kıldığı, ne kadar sürekli ve ayrıntılı kayıt tuttuğu, veri analizine ne kadar katkı sağladığı bu ilişkinin ana bileşenleridir (Yılmaz, 2005, s. 3).

E-gözetim teknolojisi üç farklı alana odaklanmaktadır: Performansa odaklanarak bilgisayar veya telefon kullanma sürelerini ölçme gibi faydalar

sağlamakta; işgören davranışına odaklanarak kaynak kullanımını ölçme, işgörenin konumunu takip etme gibi imkânlar sunmakta; işgören karakteristiklerine odaklanarak ise çalışan güvenilirliği, sağlık durumları gibi konularda bilgi vermektedir (Al-Rjoub, Zabian ve Qawasmeh, 2008, s. 190). İşverenler, daha fazla kâr dürtüsü ile çalışanlarını elektronik takip altında tutmak istemektedirler. Ancak bu durum çalışanların mahremiyeti açısından olumsuz sonuçlar doğurmaktadır. Günümüzde iş yerlerinde elektronik izleme donanımlarının sunduğu imkânlarla her şey kameralar aracılığıyla takip edilebilir, e-postalar kontrol altında tutulabilir, sabit diskteki belgeler ve ziyaret edilen siteler incelenebilir durumdadır. Akıllı cep telefonları ve bilgisayarlar yoluyla çalışanlar evdeyken bile işverenleriyle düzenli olarak iletişim hâlinindedirler. Amerika Birleşik Devletleri'nde yapılmış olan bir araştırma çalışanların %48'inin işverenlerin cep telefonlarını izlemesinden rahatsız olduklarını ortaya çıkarmıştır (Esen, 2005, s. 23). Ayrıca iş saatleri dışında gerçekleştirilen bu izlemelerin özel hayata müdahale olarak algılandığı ve tepkilere sebep olduğu diğer başka araştırmaların sonuçlarıyla da desteklenmiştir (Pearce ve Kuhn, 2003, s. 372).

Son zamanlarda yapılan araştırmalar, çalışanlar üzerindeki gözetimin her geçen gün artmakta olduğunu ortaya koymaktadır. Amerikan Yönetim Birliği tarafından yapılan bir araştırmada bir yıl içinde çalışanlarının telefonlarını, e-postalarını, sesli postalarını ve bilgisayar kullanımlarını izleyen şirketlerin sayısının %37'den %43'e çıktığı tespit edilmiştir (Lyon, 2006, s. 84). Amerika'da yapılan bir diğer araştırma ise işletmelerin %45'inin, çalışanlarının her türlü elektronik haberleşmesini izlediğini ortaya çıkarmıştır. Kullanılan izleme yazılımları çalışanların internet geçmişlerini ve e-postalarının her bir kelimesini kayıt altına almaktadır (Watson, 2001, s. 82).

Çalışanların izlenmesi hususunda en fazla mahremiyeti tehdit eden araç elbette ki video kameralardır. Bazı kameralar otopark ve merdivenlerde özel hayata müdahale etmeden güvenliği sağlarken işverenler, kameraları çoğunlukla kabul edilemez alanlara da yerleştirmeye başlamışlardır. Mahremiyet ihlaline en uç örnek çalışanların duşlarda ve soyunma odalarında da gözetlenmesidir. Bu gibi uygulamaların işle uzaktan yakından ilgisi olmadığı aşikârdır ve bu durum çok net olarak tacizdir. Çalışanların bu gibi mahrem alanlarda son derece yüksek bir gizlilik ve kişisel imtiyaz gereksinimi vardır (National Workrights Institute, t.y., s. 17-18). İnternet, kameralar, dinleme cihazları gibi araçların sağladığı teknik imkânlar sayesinde denetim artık toplumsal alandan bireysel alanların en uç noktalarına

kadar yaygınlaşmıştır. Örneğin İngiltere’de dört milyondan fazla kapalı devre kamera kayıt hâlinindedir ve bu sayı toplam nüfusla kıyaslandığında bu her 15 kişiye bir kamera düştüğünü göstermektedir (Dolgun, 2008, s. 253).

Örgütsel izlemenin yanında bilgi işlem çalışanları da kendi mesai arkadaşlarını bu sistemlerle takip edebilmektedir. İşverenler, bilgi işlem çalışanlarına verilere erişim konusunda tam yetki tanımaktadır. Oysaki bu verilere erişimin belirli resmî prosedürler çerçevesinde gerçekleşmesi gereklidir. Tüm bunların yanında en önemli hususlardan birisi de çalışanların ne zaman izlendikleri konusunda bilgi sahibi olamayışlarıdır. İşverenler firmaların her şeyi izlemeye hakkı olduklarını çalışanlarına bildirmektedirler. Çalışanlar takip altında olanların e-postaları mı, web sayfaları mı, yoksa sabit diskleri mi olduğunu maalesef bilememektedirler. Buna ilaveten takibin sürekli mi, rastgele mi ya da ihtiyaç duyulduğunda mı gerçekleşiyor olduğu da bilinmemektedir (National Workrights Institute, t.y., s. 3-4). Bu kayıt altına alma faaliyetlerinin çerçevesinin kayıt altına alanlara bildirilmesi önemli bir husustur. Bu uygulamanın en güzel örneği Lüksemburg’da Avrupa Komisyonunun Jean Monnet binasında kişilerin görebileceği şekilde yapılan bilgilendirme levhasıdır. Herkes tarafından kolayca görülebilen bilgilendirmede, “binada bulunan kameraların kaydettiği kişisel verilerin yalnızca Avrupa Komisyonu’nun 2001/45 sayılı tüzüğü uyarınca işlenebileceği ve bunun dışında kullanılmayacağı, bu verilerin sadece 30 günlük süre için saklanacağı ve gerekiyorsa suçların soruşturulması ve kovuşturulmasına ilişkin olarak adli mercilere iletilebileceği” ifadesine yer verilmektedir. Böylelikle kayıt altına alınan verilerin bahsedilen amaçlar dışında kullanılmayacağına güvencesi verilmektedir (Civelek, 2011, s. 42).

İşverenlerin çoğu, çalışanlar işletmenin kaynaklarını kullandıklarından onları izlemeyi kendilerinin bir hakkı olarak görebilmektedir. Çalışanlar ise izleme sonucunda aşağılandıkları ve küçük düşürüldükleri hissine kapılmaktadırlar (Ariss, 2002, s. 555). Elektronik izlemenin iş yerlerinde aşırı strese, iş memnuniyetinin düşmesine, kalitenin azalmasına sebep olduğu iddia edilmektedir (Watson, 2001, s. 82). Çalışanlar izlenmeyi özel hayatlarına müdahale olarak görmekte, bu uygulamanın etik olmadığını düşünmekte ve yasal olmadığına inanmaktadırlar (Lease ve Gordon, 2005, s. 4).

Massachusetts Coalition on New Office Technology tarafından gerçekleştirilen ve 49 işletmeden 700 çalışanın katıldığı bir araştırmaya göre katılanların %81’i gözetlenmenin işlerini daha stresli bir hâle getirdiğini ifade etmiştir. Benzer bir sonuç, Amerika’da iş sağlığı ve güvenliği ulusal enstitü-

sü NIOSH tarafından da elde edilerek doğrulanmıştır. Bu araştırmaya göre daha çok izlemeye maruz kalan çalışanların, izlenmeyen çalışanlara oranla yüksek derecede depresyon, gerilim ve kızgınlık yaşadığı tespit edilmiştir (Yılmaz, 2005, s. 33).

Ülkemizde de bilgisayar ve internet kullanımı hızla artmaktadır. Türkiye İstatistik Kurumu (TÜİK, 2012a) Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre Türkiye genelinde hanelerin %47,2'si evden internete erişim imkânına sahiptir. 2012 yılı Ocak ayında 10 ve daha fazla çalışanı olan girişimlerin %92,5'inin internet erişimine sahip olduğu görülmektedir. İnternet erişim oranı, 250 ve üzeri çalışanı olan girişimlerde %99,6 iken, 50-249 çalışanı olan girişimlerde %98,1, 10-49 çalışanı olan girişimlerde ise %91,2'dir (Türkiye İstatistik Kurumu [TÜİK], 2012b). Çalışanların çoğu evlerinde ve iş yerlerinde internet erişimine sahip olduklarından bilgisayar üzerinde yaptıkları işleri hem evlerinden hem de iş yerlerinden takip etme şansına sahiptirler. Bu yeni esnek çalışma biçimi, kişisel iletişimde de ev ve iş ayrımını ortadan kaldırarak kişisel iletişimin de çalışma hayatı içerisinde gerçekleşmesini sağlamaktadır. Bu koşullarda faaliyetlerini sürdüren çalışan, mesai saatleri dışında işyeriyle ilgili telefon, e-posta vb. görüşmeler yaptığından işyerinde kişisel iletişimi için zaman ayırmasını normal karşılamaktadır. Böyle bir durumda çalışan takip sistemleri, düzenli olarak kişisel iletişimi de kayıt altına almaktadır. Öğle arasında işyerinin kendisine verdiği tablet bilgisayarından eşine romantik bir evlilik yıl dönümü mesajı atan bir çalışanın bu özel bilgileri de takip sistemlerine takılabilmektedir.

Türkiye'de yapılan bir araştırmaya göre çalışanların büyük kısmı yönetimin iş yerlerini izlemeye hakkı olduğunu ve işyeri izlemenin çalışan verimliliğinin artması, işyerinde hırsızlık ve suiistimal olaylarının azalması gibi olumlu sonuçları olabileceğini düşünmektedirler. Buna karşın izlemenin çalışanların mahremiyetine zarar verebileceği, moral motivasyonunu bozarak verimliliği düşürebileceği ve çalışma barışını olumsuz etkileyebileceği de ortaya çıkmıştır (Erdemir ve Koç, 2006, s. 559-560). Çalışanlara yönelik izleme faaliyetlerine ilişkin Türkiye'deki mevcut durumu tespit etmeyi amaçlayan bir başka araştırmada ise internet, telefon, bilgisayar ve sohbet programlarının denetlenmesinin en sık başvurulan izleme faaliyetleri olduğu tespit edilmiştir. Bununla birlikte, masa ve ofislerin aranması, işgören takibine yönelik parmak izi, retina taraması, çalışanlara ait e-postaların ve kameralı cep telefonlarının denetlenmesi gibi yöntemlerin ise en az karşılaşılan yöntemler olduğu bulgusuna ulaşılmıştır (Erdemir, 2008).

## Çalışanları İzlemenin Meşruiyet Kaynağı: Üretkenlik ve Verimlilik

Sennett'e (1992, s. 57) göre toplumu oluşturan her bireyin otoriteye ihtiyacı vardır. Enformasyon toplumunun esnek çalışma biçimleri "otoritesiz iktidar"lar doğurmaktadır. Yeni kapitalizm, çalışma zamanının örgütlenmesinin yeni biçimlerini geliştirmiştir. Bireysel özgürlük vurgusunun öne çıkarılması, esnek emek piyasasında değişime açıklık ve koşullara ayak uydurabilmek savı, aslında birey üzerindeki denetimin kuvvetlendirilmesini sağlamaktadır. Bürokratik rutine karşı başkaldırı ve esneklik arayışı, çalışanları özgürleştirmek yerine onlar için yeni iktidar ve kontrol mekanizmaları üretmektedir. Örneğin esnek zaman kavramı, aslında çalışanı organizasyona tümüyle esir etmektedir. Esnek zamanlı çalışma türlerinden biri olan evden çalışma, işverenler için bir kaygı kaynağıdır. İşverenler, çalışanlar üzerindeki kontrolü kaybetme korkusuna kapılmakta ve evde çalışanların bu özgürlüğü istismar edeceklerini düşünmektedirler. Bu nedenle de işletmede olmayan kişiler üzerinde sıkı bir denetim mekanizması kurmak istemektedirler. Bu denetim mekanizmasını sağlayabilmek için bazı yöneticiler, çalışanlarının işletmeyi düzenli olarak telefonla aramasını ister, bazıları da çalışanını intranet üzerinden takip ederek e-postalarını denetmenlere kontrol ettirirler (Sennett, 2002, s. 48-61).

Örgütler güçlerini caydırıcılık, koşullandırıcılık ve ödüllendiricilik fonksiyonlarından sağlamaktadırlar. Berle ve Means'e (1991) göre enformasyon toplumunda örgütlerin iktidar kaynağı olmasının nedeni, yönetimin gücünün mülkiyet sahiplerinden yöneticilere devredilmiş olmasıdır. Bu iki bilim adamı, Amerika'da şirket yöneticilerinin şirket sermayesinde küçük bir hisseleri olmasına rağmen, şirketin karar mekanizmalarında büyük yetkilerinin olmasını incelemiştir (Galbraith, 2004). Modern şirket yöneticileri bugünün güçlü sınıflarıdır. Russell (1990, s. 45) da büyük örgütlerin gelişmesiyle "yönetici iktidarı" denilen yeni tip bir iktidar sahibi birey imajı oluştuğunu söylemektedir. Örgütler caydırıcılık, koşullandırıcılık ve ödüllendiricilik fonksiyonlarını pekiştirmek amacıyla elektronik izleme sistemlerini etkin olarak kullanmakta ve örtük bir sermaye ve mülkiyet egemenliğine zemin hazırlamaktadırlar.

Enformasyon teknolojilerinin gelişmesine bağlı olarak elektronik izleme sistemlerinin kullanımı da yaygınlaşmış, bilgi üzerindeki denetim artmıştır. Sanayi sonrası toplum tipi olarak da nitelendirilen bu dönemde bilgi, iktidarın ayrılmaz bir parçası ve "üretimin esas gücü" olmuştur (Lyotard, 1990, s. 11-12). Modernizmin en önemli hedeflerinden biri ilerlemedir. Bu

doğrultuda örgüt içindeki bütün unsurlar önceden belirlenmiş amaçlar doğrultusunda seferber edilmelidir (Erdemir, 2007, s. 82). Çalışanların verimliliğini denetleme üzerine kurulan izleme sistemleri organizasyon açısından bakıldığında, bilgi teknolojilerinin işle ilgili olmasını sağlamak, elektronik e-postaların ya da internet kullanımının işyeri politikasına uygun olmasını sağlamak, çalışanlara yönelik psikolojik şiddet, hırsızlık ve taciz olaylarını belirleyebilmek, ticari sırların ve özel bilgilerin dışarıya sızmasını engellemek, kötü niyetli kişilerin işverenin bilgisayar sistemine girmesini engellemek, bilgisayar ağının aşırı yüklenmesini engellemek, mahkemeye intikal etmiş davalarda işverene savunma hazırlamasına dair kaynak sağlamak, müşteri standartlarını izlemek gibi amaçlar taşımaktadırlar (Grey-Noble, 2008, s. 3; Lasprogata, King ve Pillay, 2004, s. 2-3).

İzlemenin çalışanlar açısından olumlu olduğunu iddia edenlerin başlıca argümanı, çalışanların performanslarına dair geri beslemenin ve bilgi toplamanın objektif verilere dayandırılmasıdır. Bu şekilde elde edilecek verilerle değerlendirmeler sürekli ve tarafsız olacak, bu sayede de çalışanlar kendilerini geliştirme imkânı elde edilecektir. Elektronik izleme sistemlerinin kullanımıyla, bireysel performansa ilişkin farkındalığın artmasının yanında değerlendirme belirsizliği nedeniyle oluşan gerilimin de azalacağı ifade edilmektedir (Yılmaz, 2005). İzleme sayesinde çalışanlar, bir kaydın dinlenmesi veya izlenmesi yoluyla tam olarak neyin yanlış ya da eksik yapıldığını görebilmektedirler. Bununla birlikte belirlenen objektif kurallar ve standartlar doğrultusunda performanslarını kendi kendilerine de belirleyebilmektedirler (Yılmaz, 2005, s. 3).

Yeni kapitalist dönemde, bir yandan insan “en değerli sermaye” olarak değerlendirilmekte bir yandan da klasik dönemdeki gibi, makinelerin cansız zihniyle birlikte aynı sisteme dâhil edilerek çalışma hayatında bir robota (cyborg) dönüştürülmekte, aynı anda sermaye, mal ve emek hâline dönüştürülerek tüm bütünlüğüyle üretim aracı hâline getirilmektedir. Üstelik bu sistem içinde bireyin üretimin bir parçası olmaması durumunda reddedilmesi, dışlanması ve var olmayan bir şey muamelesi görmesi kaçınılmaz hâle gelmektedir (Gorz, 2001, s. 16). Foucault (2007) bu hususu açıklarken “mümkün olduğunca verimli bir üretimle birlikte; işbölümünde kimilerinin şu işi, kimilerinin bu işi yapmasına ihtiyaç olduğunda, halkın direniş hareketlerinin, ataletin ya da isyanın, doğmakta olan tüm bu kapitalist düzeni altüst etmesinden korkulduğunda, o zaman, her bireyin somut ve kesin gözetlenmesi gerekli oldu” demektedir.



Daha fazla üreten daha fazla değerlidir anlayışıyla çalışanlar, bir üretim ve verimlilik baskısı altında tutulmaktadır. Küresel rekabet koşulları altında varlığını sürdürme telaşı içinde olan örgütler ise verimliliği ve üretkenliği denetim altında tutmak istemektedirler. Bu anlayış elektronik izleme sistemlerini işveren gözünde meşrulaştıran en önemli argümandır. Son zamanlarda Apple'ı dünyanın en değerli şirketi yapan iPhone'u üreten Foxconn'un fabrikaları isyanlar ve intiharlar ile anılmaya başlanmıştır. Çin Emek Bülteni isimli yayın organında çalışan G. Crothall durumu analiz ederken "İşçiler adaletsizliğe karşı çıkıyor ve haklarını arıyorlar ama sürekli üretim baskısı altındalar" ("Foxconn kilidi vurdu," 2012) ifadesi performans baskısının çalışanları nasıl etkilediğini açıklamaktadır. Bu durum Maier'in (2006, s. 31) ifade ettiği üzere iş dünyasında oynanan büyük oyunda, asıl oyuncunun firma olduğunu göstermektedir. Böyle bir sistemde çalışanlar sadece bir piyon görevi üstlenirler. Firmalar işgörenlere iş vermekle onlara çok büyük bir lütufta bulunduğu inancındadırlar. Eğer çalışanlar kibar ve itaatkâr davranır, rahatsız etmemek için seslerini yükseltmezlerse iş güvenceleri vardır. İşgörenlerden beklenen şey iş performanslarının yüksek olması ve sessizce ay sonunda maaşlarını almalarıdır.

Whalen ve Gates (2010, s. 14-22) özellikle hem işe almadan önce hem iş görme sırasında yoğun bir şekilde izlemeye tabi tutulan sekiz Amerikalı bilgi sektörü çalışanıyla mülakata dayalı olarak gerçekleştirdikleri nitel çalışmalarında iş yerlerinde gönüllü izlemenin (voluntary monitoring) pozitif boyutları üzerinde durmaktadırlar. Bu çalışma sonucunda çalışanların izlenmesinin dört faydası tespit edilmiştir: Kişisel güvenlik, hataları yakalama veya ikinci bir çift göze sahip olma, iş birliğini basitleştirme ve denetim kayıtları ve süreçleri. Ayrıca iş tatmininde artış ve kariyerin açık bir şekilde belirlenmesi de ikincil faydalar olarak belirlenmiştir. Farlee'in (2010, s. 204-206) çalışanların izlenmesi sırasında elde edilen bilgilerin ifşa edilmesi ve gizlenmesi konusunda bir model geliştirdikleri çalışmalarında bilgilerin gizlenmesinin risk paylaşma ve ifşa edilmesinin ise karar alma konusunda faydaları olduğundan söz edilmektedir. Bu çalışmada ifşa edilen bilgilerin üretim sisteminden ziyade izleme sistemi ile ilgili olduğu; ifşa edilen bilginin çalışan faaliyetleri ile çıktılar arasındaki ilişkiye bir etkisi olmadığı durumda ifşa etmenin tercih edilebileceği öne sürülmektedir. Smith ve Tabak (2009, s. 46) e-mail izleme sistemleri tasarımında örgütsel çevre, teknoloji, yapı ve kültür faktörlerinin dikkate alınması gerektiğini ifade etmektedirler. Yazarlar "güven" in yüksek performanslı çalışma ortamlarının merkezinde yer aldığını, gizliliğin de güven içeren ilişkiler kurmak

için gerekli bileşen olduğunu öne sürmektedir. Yöneticilerin bir yandan şirketlerini korurken, diğer yandan yetenekli iş gücünün kaotik ve yaratıcı katkılarını almak konusunda fayda-maliyet analizi yapmaları gerektiğini vurgulamaktadırlar.

İşgörenlerin organizasyon içerisinde zamanlarını nasıl harcadıkları, verimliliğe ne ölçüde katkı sağladıkları, organizasyona ait teknoloji ve araçları ne amaçla kullandıklarını takip etmek için izleme sistemleri etkin bir araç olarak kullanılmaktadır. İzlemeye yönelik tüm faaliyetler çalışma hayatında personelin güçlendirilmesi, yetki devri, takım çalışması ya da bilginin paylaşımının özendirilmesi gibi yaklaşımlarla çelişmektedir (Tafti, Mithas ve Krishnan, 2007). Al-Rjoub ve arkadaşları (2008, s. 194), çalışanlar açısından elektronik izlemeyi ele aldıkları çalışmalarında Ürdün'de özel ve kamu üniversitelerinde ve bankalarında bir anket gerçekleştirmişlerdir. Bu anket sonucunda çalışanların elektronik olarak izlendikleri zaman iş ve davranışlarını iyileştirdikleri tespit edilmiştir. Ancak çalışanlar bunun örgütün yararına olduğunu belirterek izlenmek istemediklerini ifade etmişlerdir. Örgütün verimliliğini arttırmanın kendilerinin değil, yöneticinin rolü olduğunu ifade eden katılımcıların %64'ü kişisel nedenlerle internette dolaştıklarını kabul etmekte ve bu kişilerin %97'si de bu durumun verimlilik üzerinde etkili olmadığını iddia etmektedirler. Örneğin Kanada'da çalışanlar haftada iki saatlerini kişisel nedenlerden ötürü internette geçirmektedirler.

Amerikalı Arthur Miller'in yazdığı *Satıcının Ölümü* adlı oyun, örgütlerin kendi çalışanlarını tüketip sömürmesini, ihtiyaç duyduğu şeyi alıp kullandıktan sonra geri kalanı bir tarafa atmasını anlatmaktadır. Elbette istisnalar vardır ama örgütün her kademesindeki birçok işgören ve yönetici, sağlığının ve kişisel hayatının, modern örgütlerce kurban edildiği bir durumla karşı karşıya kalmaktadır. Oyundaki kahramanın hikâyesi, sonucu bakımından aşırı bir örnek olmakla birlikte, özü bakımından durum böyle değildir. Günümüz dünyasında bireyler ve hatta bir bütün olarak topluluklar, hizmet ettikleri örgütler artık kendilerine ihtiyaç duymadığı zaman, bir tarafa atılma gerçeğiyle yüzleşmektedirler.

Üretkenlik ve verimlilik baskısı işletmelerin çalışanlarını iş ahlakına uygun hareket edip etmedikleri konusunda kontrol mekanizması kurmayı zorunluluk hâline getirmektedir. Gözetlemeyi meşrulaştırmak için kullanılan örgütlerin kâr güdüsü ve buna bağlı olarak da gerçekleşen üretim baskısının yanında bir diğer neden de işgörenlerin iş yerlerine ait kaynakları kullanırken yasalara veya etik ilkelere aykırı olabilecek davranışları gerçekleştire-

bilmeleridir. Yapılan araştırmalarda çalışanların işletmeye ait yazılımları evde de kullanmak için kopyaladığı, işletmenin sağladığı internet imkânını özel işleri ya da eğlence için kullandığı, işletmeye veya diğer çalışanlara ait bilgisayarlardan yetkileri olmadığı hâlde dosyalar aldığı, pornografik sitelerde vakit geçirdiği, işletmeye ait araç ve imkânları örgütsel amaçlar dışında kullandıkları, işyerine ait ya da iş arkadaşlarına ait verilere zarar verdiği, bazı çalışanların hatalarının gizlendiği ya da suçun başkalarına yüklendiği, işin standart süresinin veya molaların gereksiz yere uzatıldığı durumlar tespit edilmiştir (Erdemir ve Çelikaş, 2006, s. 91; Türkiye Genç İş Adamları Derneği [TÜGİAD], 1992, s. 48). Elbette ki organizasyon içerisinde tüm bu sayılanlara eklenebilecek birçok ahlak dışı davranışlar söz konusu olabilir. Tüm bu davranışlardan doğacak olumsuz sonuçların işletmenin üretkenliğini ve verimliliğini düşürmemesi isteği, etkin bir izleme sistemini gündeme getirmektedir.

## Panoptikon'un Elektronik Dirilişi

İletişimin gözetlenmesi ve kontrolü uluslararası alanda özellikle istihbarat sağlamak amacıyla çeşitli nedenlerle yapılabilmektedir. Bütün dünyada uydu tabanlı iletişimi izleyen beş devletin (ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda) gizli servislerinin ortaklaşa kurdukları ECHELON (Büyük Kulak) sistemi olduğuna dair bir komplo teorisi mevcuttur. İddialara göre bu sistem telefon görüşmeleri, faks, telsiz, internet, elektronik posta trafiği dâhil olmak üzere tüm iletişim araçlarını dünya çapında dinlemekte ve kaydetmektedir (Beceni, 2004, s. 14). Bu tür iddialar Foucault'nun iktidar kavramının anlaşılmasında ekonomiyi merkeze almak yerine iktidarı güç ilişkilerinin bir yansıması olarak gören yaklaşımını desteklemektedir. Bu yaklaşıma göre iktidar, temelde bireyleri, grupları ve sınıfları baskı altına alan, onlara hareket alanı bırakmayan, kontrol altında tutan bir mekanizma olarak karşımıza çıkar (Foucault, 2004, s. 31). Ancak Foucault (2004, s. 47) için iktidarın anlaşılmasında, bilgilerin üretimini, yayılımını, dağıtımını gerçekleştiren, onları kaydeden ve dolaşıma sokan bilgi aygıtlarının incelenmesi, iktidarın sahip olduğu ideolojinin analiz edilmesinden çok daha önemlidir. Foucault'ya göre, iktidar herhangi bir kurumla veya aygıtlarla bir görülemez. İktidarın nereden kaynaklandığına odaklanmak bizi sonu gelmez tartışmalara götürür. İktidarın etki etme tarzlarına ve bundan ne beklediğine yoğunlaşmak gerekir (Foucault, 2000, s. 308). Foucault'ya göre ikti-

dar yöneten-yönetilen rollerinden ziyade, belli bir tarihsel dönem içerisinde ortaya çıkan çeşitli kapatma kurumlarına dayanmaktadır. İktidarı monarşi kaynaklı analiz etmek kolaycı bir yaklaşımdır. Böyle bir açıklamaya başvururken bir hükümdarın insanların özel yaşamlarına bütünüyle müdahale edemeyeceğini gözden kaçırmamak gerekir. Asıl üzerinde durulması gereken şey, iktidarın görünür olması, izleme faaliyetlerinde bulunması değil, hedefini görünür ve izlenebilir kılmasıdır (Rouse, 1994, s. 95). Bu açıdan bakıldığında elektronik izleme sistemleri hedefini sürekli olarak görünür ve izlenilir kılmaktadır. Enformasyon toplumdaki iktidarın geçmişteki iktidarlara gibi insanları kapalı mekânlara hapsetmesi söz konusu değildir. Sanal mekânlar, insanları her an görünür ve izlenir kılmaktadır.

G. Morgan (1998, s. 383), yönetsel süreçleri çeşitli metaforlar kullanarak açıklamıştır. Ona göre örgütler, toplumsal olarak kurulan gerçeklikler olmalarına rağmen, kurgulayanlarının üzerinde bir ölçüde denetim kurma olanağı sağlayan bir varlık ve güç hâline dönüşmektedir. Örgütleri, ruhların hapisanesi olarak açıkladığı metafor, örgütlerin sonuçta bilinçli ve bilinç dışı süreçlerin ürünü olduğunu ve insanların ise bu süreçlerden kaynaklanan imge, fikir, düşünce ve eylemlerin tutsağı olabileceğini ifade etmektedir. Bu metafor örgüte başkalarına zarar verme pahasına olsa da belirli çıkarları gözetilen bir tahakküm aracı olarak bakılmaktadır.

Allen, Coopman, Hart ve Walker (2007, s. 174), örgütsel izlemenin yaygın ve ketum karakterini ortaya koymak için pek çok yazarın Panoptikon metaforunu kullandığını ifade etmektedir. Bentham (1995, s. 34) 1785 yılında kurguladığı Panoptikon tasarımıyla, iflah olmaz kişileri cezalandırmak, masum insanları gözetim altına almak, şüphelileri hapsetmek, işsizleri çalıştırmak için müebbet hapislerin, cezaevi atölyelerinin, imalathanelerin, tımarhanelerin, hastanelerin ya da okulların daha etkin ve verimli çalışacağını iddia etmiştir. Panoptikon kelimesi “görülen her alan -all seeing place” anlamına gelmektedir. Panoptikon; bütünü (pan-) gözlemlemek (-opticon) anlamına gelen bu tasarım birkaç katlık tek odalı hücrelerden oluşan bir halka üzerine kurulmuştur. Her hücre bu halkanın iç kısmına doğru açıktır ve halkanın dış cephesindeki duvarda birer pencere vardır. Halkanın ortasında mahkûmlardan tamamen saklanmış konumdaki gözlemcilerin kaldığı bir gözetleme kulesi yer almaktadır (Yılmaz, 2005, s. 14). Panoptikon’un temelinde yatan ilke, tek odalı hücrenin içindeki mahkûma, saklanacak hiçbir yer bırakmaması, buna karşılık dış cephedeki duvarın penceresinden gelen dış ışığın kuledeki nöbetçilere mahpusun her hareketinin gölgesini

izleme olanağını sağlamasıdır. Bentham'a göre, gözlemlenen her yanlış davranışının ceza getireceğini bilen, ama davranışlarının aslında ne zaman gözlemlendiğini bilmeyen mahkûmun, aklını başına alarak her zaman izleniyormuşçasına davranmaktan başka seçeneği yoktur. Böylece mahkûm dış baskılar sonucunda öz denetim sağlayacak, kendi hareketlerini kollamak durumunda kalacaktır.

Aslında Panoptikon, bir hapisshaneden öte, bir gözetim sistemidir ve Foucault bu mimari yapıyı modern gözetleme toplumunun bir metaforu olarak kullanmıştır. Foucault'ya göre iktidar, insanları özgürleştirme yanıl-samasıyla tahakküm altına alır ve inşa eder. Bu, iktidarın hilesidir, gerçekte her yeri çok daha fazla kaplar ve sinsi bir şekilde işler (Aktaş, 2012, s. 62-63). Otoriteyi temsil edenlere eleştirel bir yaklaşımda bulunan Bakunin'e göre, insan sürüsünün ayrıcalıklı gardiyanları olan yöneticiler güçlü, erdemli adanmışlıkları ve her şeyi bilen kafa yapılarıyla, onları kendi yararına güde-rek bu tür sistemleri icat ederler (2000, s. 114). Kontrol akıllıca ve kurnaz-ca, mahkûmların sürekli görünmeyen bir göz tarafından izlendiği duygusu tarafından sağlanmaktadır. Saklanacak hiç bir yer olmadığı gibi bu sistemde özel alan da bulunmamaktadır. İzlendiğini veya izlenmediğini bilmediği hâlde itaat mahkûmun tek rasyonel seçeneğidir.

Bentham'ın Panoptikon planı asimetrik gözetim felsefesini ifade etmektedir. Asimetrik gözetimde kişi ne zaman gözetlendiğini bilmemektedir. Bireyler tek başınadır, tamamen yalnızlaştırılmış ve sürekli görülebilir durumdadır. Görülmeden gözetim altında tutmaya olanak veren bu düzenleme, sürekli görmeye ve hemen tanımaya imkân sağlayan bir mekân tasarımıdır. Klasik hapisshanelerde hücrelerin üç ana fonksiyonu vardır. Bunlar; kapatmak, ışıktan yoksun bırakmak ve saklamaktır. Panoptikon tasarımında bunlardan yalnızca kapatma fonksiyonu korunmakta, diğer ikisi ise kaldırılmaktadır. Tam ışık ve bir gözetmen bakışı altında olma, aslında gizleyen karanlıktan daha fazla yakalayıcıdır. Görünürlük bir tuzaktır (Foucault, 2005, s. 251). Elektronik izleme sistemleri bir nevi Panoptikon anlayışının sanal simülasyonudur. Tüm video kayıtları, elektronik izler, GPS sinyalleri, ses kayıtları gündelik hayatımızda en küçük bir karanlık noktaya izin ver-meyerek elektronik bir hapisshane ortamı sağlamaktadır.

Sıkı kontrol ve izleme, ilk kez sistematik olarak Fordist dönemde Taylor'un bilimsel yönetim ilkeleriyle kendini göstermiştir. Klasik yönetim anlayışının hâkim olduğu dönemlerde Fayol da benzer biçimde üretimin verimliliğinin gözetim ve denetimle arttırılabileceğini vurguluyordu. Taylorizm

ve Fordizm emeği, emek süreciyle denetlemenin en keskin stratejileridir (Munck, 1995, s. 218). Klasik teori, örgütü tıpkı mahkûmların gözetlendiği bir hapisane gibi tasarlar ve bu tasarımın konsepti gözetlemeyi ön planda tutar. Fonksiyonel ustabaşılık sistemi işgörenin âdeta gölgesini bile takip eden bir yapı oluşturmaktadır. Taylor'un önerisine göre sekiz ustabaşından dördü planlama işleriyle görevlendirilecek ve bunlar planlama bölümünde çalışacaklardır. Bunlardan birincisi iş sıralama ve dağıtım ustabaşısı olarak, iş akışının sağlanması ve sıralama yapmakla görevlidir. İkincisi iş emri ustabaşısıdır. Onun görevi, teknik resimleri hazırlamak, parça başı ücreti hazırlamak, maliyetlerle ilgili bilgileri muhasebeye vermektir. Üçüncü ustabaşı, zaman ve maliyet ustabaşısıdır. Onun görevi ise zaman ve maliyetle ilgili çalışmalar yapmaktır. Dördüncüsü ise disiplin amiri olarak personelle ilgili işleri takip etmek ve işgörenlerin iyi ve kötü taraflarını ortaya çıkarmak ve iş barışı için çalışmak, ayrıca işe adam alma ve işten çıkarma işine bakmakla mükelleftir. Bu hâliyle örgüt büyük bir hapisaneye dönüşerek çalışanını, normalde ona dışarıdan dayatılması gereken performans kriterlerini kendi kendine dayatmaya teşvik etmektedir.

Foucault'ya göre, Panoptikon, örgütte ya da başka herhangi bir yerde, bugün kendini gösterdiği biçimiyle iktidar modelinin kendisidir. Fiziksel olarak böyle bir kontrol yapısı günümüzde mevcut değilse bile denetim daha dolaysız hâle gelerek dijital bir dönüşüm yaşamıştır. Aynı felsefeden hareketle içinde sahte bir özgürlüğün saklı olduğu daha sıkı bir gözetim ve denetim her yanımızı kuşatmış durumdadır. Yeni sistem, her şeyi kayıt altında tuttuğundan aylar ya da yıllar öncesine dönüp bir anı yeniden gözetleme imkânı da sunmaktadır. Sennett (2011, s.38) bu hususta bilişim teknolojilerinin kaynakların ve performansın gerçek zamanlı haritalarını sayısallaştırarak panoptik gözetlemeyi kolaylaştırdığını vurgulamaktadır.

E-izleme kavramı tıpkı Panoptikon tasarımında olduğu gibi 1960'ta Amerika, Kanada ve İngiltere'de hapisane yoğunluğunu azaltmak için ortaya çıkmış, daha sonra iş hayatında da kullanılmaya başlanmıştır (Al-Rjoub ve ark., 2008, s. 190). Kapitalist üretim biçiminde, işçinin etkinliği yerini yönetimin etkinliğine bırakmıştır. Artık yönetim, üretim sürecinde bir bütün hâlinde üretimin tüm öğelerini denetleme işlevini yürütmektedir. Böylece öznel bir üretim ögesi olan emek, üretim sürecinin dışına çıkarılarak nesnel bir öge hâline getirilmektedir (Braverman, 2008, s. 175-176).

## Sonuç Yerine

Foucault, aydınlanmacı düşüncenin temel varsayımlarından biri olan akıl ve özgürleşme birlikteliğini eleştirerek, modernitenin yeni baskı pratikleri geliştirdiğini ileri sürmektedir (Şaylan, 2002, s. 257). Günümüzde iş yaşamında var olan en önemli baskı araçlarından birisi de örgütsel gözetimdir. Böyle bir sonucun ortaya çıkmasında esnek çalışma biçimlerinin etkisinin olduğunu söylemek mümkündür. Sennett'in (2002) ifade ettiği gibi zaman bir çalışana ödül olarak verilse de onu âdeta organizasyonun avucunun içine yerleştirir, işverenler esnek biçimde çalışan işgörenlerin üzerindeki denetimi kaybetme kaygısıyla yeni kontrol mekanizmaları geliştirmeye çalışırlar. Bu durum denetleyicilere sürekli bilgi ve veri akışı sağlayan elektronik gözetim sistemlerine talebin niçin her geçen gün arttığını da açıklamaktadır. Buradaki kayıt altına alma ve veri akışındaki kontrolsüzlük çalışanların mahremiyetini zedeleyecek bir veri madenciliğine dönüşebilir. Avrupa Konseyi bu hususta adil bir izleme uygulayabilmek için temel bazı prensiplere uyulması gerektiğine vurgu yapmaktadır. Bu prensipler; gereklilik, kesinlik, ölçülülük, şeffaflık ve güvenlidir (Mitrou ve Karyda, 2006, s. 170).

İşverenlerin büyük bir kısmı doğrudan çalışanın performansıyla ilgili olmadığı sürece çalışanlarının kişisel bilgilerini öğrenme ihtiyacı hissetmezler. Ancak elektronik izleme pratiğinde yaşanan sorunlardan birisi işverenin gereksinimleri ile çalışanın mahremiyet kaygısı arasında bir denge kurulamamasıdır. Amerika Birleşik Devletleri'nde yapılan bir araştırma, işverenlerin %75'inin çalışanlarını herhangi bir neden olmaksızın izlediğini, %50'sinin çalışanlarını uyguladıkları takip programı hakkında bir eğitime tabi tutmadıklarını, %20'sinin yazılı bir takip politikası olmadığını, %25'inin takip uygulamasının suiistimal edilmesini önlemek için herhangi bir önlem almadığını göstermektedir (National Workrights Institute, t.y., s. 7-8). Böyle bir izleme biçimi âdeta sapkın bir davranış olan röntgencilik, örgütsel bir biçime dönüşmesi sorununu ortaya çıkarmaktadır.

Mahremiyetin evrensel etik ilkelerini belirleyebilmek oldukça güçtür. Bunun nedeni dünyadaki çeşitli kültürlerde mahremiyete dair etik algıların farklılığıdır. Toplumdan topluma, kültürden kültüre değişkenlik gösteren bir çeşitlilik içerisinde uluslararası geçerliliği olan etik ilkeler yerine yerel değerleri kapsayacak biçimde farklı etik ilkeler kabul edilebilir. Öte yandan bireylerin kendilerine ait bilgileri başkalarıyla paylaşma konusundaki hassasiyetleri aynı kültür içerisinde bile kişiden kişiye değişebilir. Aynı şekilde iş dünyası içerisinde işin doğası gereği bazı organizasyonlar daha ketum bir

kültüre sahip olabilirler. Bu açıdan mahremiyet kavramına, bireyin iletişiminin izni ve bilgisi olmaksızın denetlenmesi ve kişisel bilgilerinin yasal olmayan yollarla paylaşılması perspektifinden yaklaşılarak, insan hakları çerçevesinde etik ilkeler belirlemesi gerektiği tespiti yapılabilir.

Uluslararası örgütler bu konunun önemini kabul etmektedirler. Mahremiyetin ve kişisel verilerin korunmasına ilişkin kanunların uygulanmasında iş birliğinin gerekliliği OECD, Uluslararası Veri Koruma ve Mahremiyet Komiserleri Konferansı, Avrupa Konseyi, Asya Pasifik Ekonomik İşbirliği ve Avrupa Birliği nezdinde önemsenmektedir (The Organisation for Economic Co-operation and Development [OECD], 1997, s. 4). Türkiye'nin taraf olduğu BM İnsan Hakları Evrensel Bildirgesi'nin 12. maddesinde de özel hayatın gizliliği ve dokunulmazlığı kapsamında haberleşme özgürlüğü zikredilir. "Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz kalmaz. Herkesin bu karışma ve tecavüzlere karşı kanunla korunmaya hakkı vardır." Avrupa Konseyi, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'nin "Özel Hayatın ve Aile Hayatının Korunması" başlıklı 8. maddesi de mahremiyet ihlalinin ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmuş olmak koşulları altında söz konusu olabileceğini ifade etmektedir.

Uluslararası Çalışma Örgütü tarafından benimsenen ilkeler de mahremiyetin korunmasına dair önlemleri içermektedir. Bu ilkelere göre çalışan ve temsilciler bilgi toplama sürecinden, bu sürecin kurallarından ve haklarından haberdar edilmelidir; çalışanların özel hayatlarına dair bilgileri korumaya özen gösterilmeli ve izlemede kişisel bilgilere ilişkin bilgisayar kayıtları en aza indirgenmelidir; verileri kayıt altına almakla ve analiz etmekle görevli personelin, düzenli eğitimleri sağlanmalı ve işin ciddiyeti hususundaki bilinç düzeyleri geliştirilmelidir; çalışanların özel hayatına ilişkin bilgilerin korunması hususunda işverenler, çalışanlar ve onların temsilcileri iş birliği yapmalıdır; toplanan kişisel bilgiler herhangi bir ayrımcılık yapılmasına sebep olmamalıdır; işveren, çalışanların cinsel hayatı, siyasi, dinî ve diğer inançları konusunda bilgi toplamamalı ve işçinin suça eğilimini belirlemeye yönelik test yapmamalıdır; işgören hakkında toplanan bilgilere sadece ilgili ve yetkili olanlar erişebilir, bu bilgiler, üçüncü kişilere, çalışanın bilgisi ve onayı olmadan verilemez (Kaplan, 1997, s. 383).



Mitrou ve Karyda (2006, s. 176) çalışmalarında işgörenlerin gizlilik koruma hakları ile işverenlerin örgütsel kaynakları koruma ihtiyaçlarının çatışmasından yola çıkarak adil bir izleme uygulamak için uygulanması gereken temel prensiplere ilişkin bir liste sunmaktadır: İzleme politikasının amacı açıklanmalı, işgörenlerin e-mail, telefon, faks ve interneti nasıl kullanacakları veya kullanamayacaklarına ilişkin açık bir kılavuz içermeli, izlemenin hedefleri belirtilmeli, izleme sırasında kullanılacak yöntem ve araçlar tanımlanmalı, politika ihlal edildiğinde uygulanacak disiplin süreci tanımlanmalı, işgörenlerin iletişimlerinde güvenliklerini sağlama alternatifleri tanımlanmalı, e-mail tarama ve virüslere karşı koruma için otomatik araçlar ve sistemler kullanılmalı ve işgörenler bu politika gereği uygulamalarını kimin gözden geçireceği konusunda bilgilendirilmelidir.

Özel hayata dair hakların temel unsurları gizlilik ve bağımsızlıktır. İnsan hakları arasında özel yaşamına saygı hakkı da ele alınmaktadır. Bu alan üçüncü kişilerin giremediği bir yaşamı ve buradaki insan ilişkilerini içeren, hukuki olarak sınırları net çizilemeyen geniş bir alanı içermektedir. Özel hayata dair haklar, devlete bu alana müdahaleyi önleme ve gerektiğinde cezalandırma sorumluluğu da yükler. Devletin bireylerin kişisel alanına keyfi müdahaleleri ya da bu müdahalelere göz yumması demokratik toplumun oluşumuna zarar verecektir. Türk hukuk sisteminde etik olmayan gözetimle ilgili herhangi bir yasal düzenleme bulunmamaktadır. Ancak kişisel mahremiyetin korunmasıyla ilgili Anayasa, Medeni Kanun, Borçlar Kanunu, Türk Ceza Kanunu, CMUK ve Fikir ve Sanat Eserleri Kanunu'nda çeşitli hükümler bulunmaktadır. Ancak bu düzenlemelerin işyerindeki etik olmayan gözetlemeyi önleyebilecek bir yaptırım gücü yoktur. Erdemir ve Çelikaş'ın (2006, s. 99) çalışmalarında da belirttikleri gibi işgören mahremiyeti kavramının içinden çıkılmaz surette etrafının sarıldığı çağımızda, bu düzenlemelerin henüz yapılamamış olması büyük bir eksikliktir. Konunun, İş Kanunu'nda ek bir hükümlerle veya çıkartılabilecek "İşyeri Mahremiyeti Hakkında Kanun" ile düzenlenmesi gerekmektedir.

Etik olmayan davranışlar, etik olmayan metotlar kullanılarak önlenmeye çalışılmamalıdır. İş hayatında hırsızlıkları önlemek, fireleri azaltmak ve çalışanların iş dışında şeylerle vakit harcamasını engellemek amacıyla işletmeler, denetimleri elektronik izleme araçlarını kullanmaktadırlar. Bunun doğal sonucu olarak da iş ortamında mahremiyet ihlalleri oluşmaktadır. Bu izlemenin rencide edici hâle dönüşmesi çalışanlar üzerinde psikolojik baskıyı arttırmaktadır. Bir çeşit psikolojik yıldırma (mobbing) biçimi ola-

rak değerlendirilmesi gereken bu sıkı gözetim asla işverenin hakkı olamaz. Sosyal Güvenlik Kurumu'nun kendi bünyesinde hazırladığı "Mobbing'in Önlenmesine Dair Usul ve Esaslar" Yönetmeliği'nin 11. maddesinde "İşe gidiş geliş saatlerinin sürekli kontrol altında tutulması"nın bir mobbing çeşidi olduğu ifade edilmektedir. Kaldı ki her daim gözetim altında tutulan bir işgörene daha şiddetli bir mobbing uygulanmaktadır.

Gelişen teknoloji sadece yöneten ve yönetilen ilişkisini değiştirmekle kalmamış, insan ilişkilerinde farklı iletişim kanalları kurgulayarak yeni boyutlar eklemiştir. Bu boyutlardan birisi sanal ortamdaki sosyal paylaşımlardır. İşyerinde çalışanların birbiriyle sohbet etmeleri abartılmamak kaydıyla normal karşılanması gereken bir davranıştır. Bu sohbetin gerçek hayatta ya da sanal ortamda olması çalışanların sosyal ihtiyaçlarını karşılamaları açısından farklı değildir. O nedenle Facebook, Myspace, Twitter, LinkedIn gibi sosyal medya araçlarının kullanımının yasaklanması anlamlı değildir. Yöneticiler bazı sitelere erişimi teknik olarak engelleyebilirler ancak yasaklanan siteler erişime açık olmasına rağmen denetim yapıyorsa böyle bir durumda mutlaka mahremiyet ihlalleri doğmaktadır. Çalışanlar kendi aralarında aileleriyle, arkadaşlarıyla, sporla, televizyon programlarıyla ilgili birçok konuyu konuşurlar. Bu sohbetin makul süreler içerisinde kaldığında sanal ya da gerçek ortamda yapılması arasında bir fark yoktur. Bir işveren, çalışanlarının kişisel iletişimini takip etmeksizin işlerini etkili ve verimli bir şekilde idare edebilir.

İşyerinde etik açıdan mahremiyetin ihlalinin önüne geçebilmek için izlemenin sınırlarını açıkça tüm çalışanlara beyan etmek gerekir. Bu sınırlar içinde hangi amaçlara yönelik izleme yapıldığı açıklandıktan sonra çalışanlardan hangi tür davranışların beklendiği ve hangi tür davranışların istenmediği net biçimde ortaya konulmalıdır. Eğer herhangi bir çalışana yönelik elektronik takip gerçekleştirilecekse bu "vaka temelli" olmalıdır. Bu takibin sadece uygunsuz bir durum yaşandığında devreye girmesi ve ilgili olayla sınırlı kalması anlamına gelir. Örgüt herhangi bir takip programını uyguluyorsa çalışanlara bu konuda gerekli uyarılar ve açıklamalar yapılmalıdır. Ayrıca takip sırasında nelerin izlendiğinin ve izlemenin hangi zaman dilimlerinde gerçekleştiğinin bilgisi çalışanlarla paylaşılmalıdır (National Workrights Institute, t.y., s. 8).

Gerek araçlardaki GPS sistemleriyle gerekse tablet cihazlardan elde edilen konum bilgisi yoluyla çalışanları takip etmek çalışma saatleriyle sınırlanmalıdır. 24 saat çalışanların konum bilgilerini kayıt altına almak da

bir mahremiyet ihlalidir. İşveren, mahkûmların her hareketini izleyen bir gardiyan değildir. Üstelik Grey-Noble'nin (2008, s. 6-7) de belirttiği üzere işyerindeki izleme doğru biçimde uygulanmadığı takdirde çalışanlar ve yöneticiler arasında güvensizlik oluşacaktır. Bu ise çalışma ortamının örgüt kültürünü olumsuz yönde etkileyerek motivasyonu azaltacak bir unsur olarak karşımıza çıkabilir.

Özellikle bilgisayar üzerinde yapılan çalışmalarda kişisel bilgileri korumak amacıyla mahremiyeti artırıcı teknolojiler (MAT) kullanılabilir. Bu teknolojilerin amacı etik ilkelerin uygulanmasına yardımcı olmakla birlikte kullanıcılara ait verilerin çevrimiçi ortamda yayılması ve kullanılması risklerine karşı denetim imkânı sağlamaktadır. 1997 yılında OECD'nin yayımladığı rapor, küresel düzeyde kişisel verilerin korunabilmesini sağlayacak teknolojileri ve politikaları desteklenmektedir. 1998'de düzenlenen Ottawa Bakanlar Konferansında da OECD'nin "MAT"ların kullanımını desteklediği" ifade edilmiştir (OECD, 1997).

Petronio (2004, s. 174), iletişim güvenlik yönetimi (CPM: Communication Privacy Management) kuramını günlük hayat problemlerinin çözümüne yönelik pratik bir kuram olarak tanıtmaktadır. CPM, bu anlamda elektronik izlemeye çalışanların tepkilerini ortaya koymak konusunda yararlıdır. CPM, olaya bireysel bakış açısıyla yaklaştığı için izleme konusunda karar ve faaliyet açısından yaklaşan vekâlet kuramından (Agency Theory) farklılık göstermektedir. Örgütsel gözetim konusu kesinlikle yazılı iş etiği kuralları arasında belirtilmelidir. 1992 yılında ABD, Kanada, Meksika ve Avrupa'da faaliyet gösteren 1.900 firmanın iş etiğine yönelik tutumlarını belirlemek amaçlı yapılan bir araştırmaya göre ABD'deki şirketlerin %84'ünün diğer ülkelerdeki şirketlerin ise %58'inin yazılı iş etiği kuralları bulunmaktadır. Tüm bu şirketlerin %25'i son üç yıl içerisinde çalışanlarına etik ile ilgili eğitimler vermiş, etik komiteler ya da ombudsmanlar belirlemişlerdir (Kidder, 1995, s. 84-85).

Elektronik izlemenin örgüt için gerekli olup olmadığı çalışanlarla birlikte değerlendirilmelidir. Herhangi bir izleme sistemi kurulurken işverenlerin bazı hususlara dikkat etmesi gerekmektedir. İlk olarak uygulanması planlanan izlemenin verimliliğe katkısının olup olmayacağına, ikinci olarak izlemenin çalışanlar üzerinde oluşturacağı strese, üçüncü olarak çalışanların moraline ne yönde bir katkı sağlayacağına ve son olarak da artan verimliliğin artan stresi ve düşen morali dengeleyip dengelemediği hususlarına dikkatli biçimde bakılmalıdır (National Workrights Institute, t.y., s. 6).

İşveren ve işgören arasında güven tesis edilmesi, yüksek bir motivasyon elde etmek için gereklidir. Gerekli olmadığı hâlde kurulan bir izleme sistemi, hem işletme açısından bir maliyet hem de çalışanlara güvensizliğin göstergesidir. Elektronik izlemenin verimlilik üzerine katkılarıyla çalışanların motivasyon kayıpları arasında bir fayda-maliyet analizi yapılmalıdır. Çalışanların da katıldığı bu analiz sonucunda elektronik takip sisteminin kurulumu kararlaştırılırsa takibin sınırları belirlenmeli ve organizasyonda çalışan tüm taraflarca bilinmelidir.

İşgörenler elektronik olarak izlenmeleri konusundaki algılarını belirleme yönünde yapılan çalışmalarda yönetici ve yönetici olmayanların algılarında farklılıklar söz konusudur. Allen ve arkadaşlarının (2007, s. 183) yaptıkları araştırmaya göre yöneticilerin %74'ü, yönetici olmayanların %56'sı izlemenin yararlı ve gerekli olduğunu düşünmektedir. Yöneten açısından bakıldığında ise izleme faaliyetleri, çalışanların daha fazla üretebilmesi açısından gözetim altında tutulmasına ve verimlilik artışı sağlanmasına, böylelikle kârlılığın arttırılmasına katkı sağlamaktadır. Organizasyonlarda izleme; şüphe, itaatsizlik ve güvensizlik gibi olumsuz düşüncelerden hareketle gündeme gelmektedir. Takip edildiğini bilen veya hissedenen her çalışan, kendisine karşı bir güvensizliğin var olduğunu düşünerek bu durumdan rahatsız olacaktır. Öte yandan, örgüt tarafından hayata geçirilen personel güçlendirme, ekip çalışması gibi çalışanların rollerini güçlendirici yönetsel uygulamalar ise kurumsal bağlılık ve güven ortamı yaratacaktır. İşte bu iki farklı durum yöneten ve yönetilen ilişkisi açısından bir paradoksu ifade etmektedir. İşverenler ya da girişimciler açısından bakıldığında doğru ya da yanlışın ne olduğuna dair kesin hükümler verebilmek gerçekten de zordur. Örgütsel gözetimle ilgili sorun alanının basit bir evet ya da hayırla çözülemeyecek gri bir alan olduğu ifade edilebilir. Yöneticiler bazen etik dışı davranışları ussallaştırma tuzağına da düşebilirler.

# Panopticon's Electronic Resurrection: Workplace Monitoring as an Ethical Problem

Köksal Büyük\*, Uğur Keskin\*\*

**Abstract:** We live in a world of electronic monitoring with a view to improve the employees' efficiency. The lack of legal regulations in this area leads to shift from monitoring the employees' work lives towards their private lives. Failing to restrict such monitoring may cause losses in organizational efficiency and it negatively affects the psychology of employees. Rapid changes in technology in recent years have greatly reduced the costs of electronic monitoring systems, and as a result new electronic monitoring tools have emerged in work life. The purpose of this study is to find out the ethical ways for electronic monitoring in organizations. To this end a comprehensive literature review has been conducted and the findings have been discussed. An unnecessary monitoring system will cost financially to businesses and imply lack of trust in employees. In order to prevent violations of privacy in the workplace the boundaries of monitoring should be clearly stated to all employees in accordance with the principles set by various international organizations.

**Key Words:** Workplace Surveillance, Panopticon, Electronic Monitoring, Employee Privacy, Business Ethics.

Development of information technologies has significantly affected the forms of work and structure of labour. In no time in history have employees been under such close surveillance, which is one of the consequences of the transformation from industrialisation society into information society. Information technologies that were used in military and defense purposes during World War II were introduced into the business world in the 1970s and brought about radical changes in organizational structures. Information society was born as a result of such changes. The transformation into information society has accelerated since the 1980s with the

---

\* Ph.D., is an assistant professor Management. His research interests include strategic performance management, management philosophy, and corporate governance.  
*Correspondence:* Eskişehir Osmangazi Üniversitesi, İktisadi ve İdari Birimler Fakültesi, Eskişehir, Turkey.  
§ E-mail: koksalsbuyuk@gmail.com § Phone: +90 222 239 3750/1038.

\*\* Ph.D., his research interests include human resource management, management philosophy, performance management.  
*Correspondence:* Hava Teknik Okulları Komutanlığı, Gaziemir, İzmir, Turkey.  
§ E-mail: ugurkeskin08@gmail.com § Phone: +90 232 251 1600 /4497.

transformation of information into a strategic competitive factor. Products and services of the new economy have brought to foreground the conversion of information into knowledge, knowledge management, processing, and distribution. The rapid development of information technologies has necessitated rapid changes in business processes, organizational structures, and the structure of workforce profile, products and services. This new economy indicates a change in the mind set and understanding at micro and macro levels (Söylemez, 2001). Castells (2005, p. 99) suggests that the outcome of this change is the global economy that is based on information and network organization. This transformation has also affected the organizational designs: horizontal and rigid organizational structures have been replaced with flexible organizations, mass consumption with niche consumer products, mass production with flexible production supported by information technologies, fixed and limited capabilities with versatility and the focus has shifted from strategic business units and products towards HRM skills (Erdemir, 2007, p. 74).

### **Extinction of Privacy in the Workplace: Organizational Surveillance**

Privacy could be defined as to what extent the individual is recognized by others, he or she is physically accessible to others and is the object of others' interest and attention (Yüksel, 2009, p. 278). Organizations should fulfill some basic moral responsibilities towards their employees. The prime responsibility should be about respecting the employees' opinions, human dignity, and confidentiality of private life (Bowie & Duska, 1990, p. 86). Privacy could be identified in three different levels, the first is spatial privacy which involves the physical area surrounding the individual, the second is personal privacy which involves protection of the individual from unjustified interference and the third is information privacy which involves gathering, storage, processing and distribution of personal data (Eralp, 2013). The debate about employee privacy in work is usually grouped under three main headings; the first one is about monitoring the use of technological tools such as phone and computer; the second one is about surveillance of behaviour or performance of employees in the workplace through cameras; and the third one is the information security of companies who possess personal information about their employees (Erdemir & Çeliktaş, 2006, p. 90).

Monitoring refers to information that is collected in relation to the workplace and employees in an automated manner, regardless of purpose, while the concept surveillance has a narrower scope in that it refers to the relationship between an authority and the person that is under control (Yılmaz, 2005, p. 3). Monitoring involves examining the performance of employees through a variety of software and electronic equipment and reporting it (Alder & Ambrose, 2005). Monitoring involves continuously and regularly recording information related to working life and business, irrespective of the purpose (Botan, 1996, p. 294). There is a close relationship between monitoring and technology. The main components of this relationship could be listed as how much technology makes employees visible, how much it makes the surveillance authority invisible, how regularly and detailed records it keeps and, and how it contributes to data analysis (Yılmaz, 2005, p. 3).

E-surveillance technology focuses on three different areas: the focus on employee performance measures employees' computer or phone use, the focus on employee behaviour measures resource utilization and tracks employees' location, and the focus on employee characteristics provides information on topics such as health status and employee reliability (Al-Rjoub et al., 2008, p. 190). Employers want to keep their employees under electronic surveillance with an urge for higher profitability. However, this situation leads to negative consequences for employees' privacy. Thanks to the electronic monitoring equipment in today's workplaces, everything can be monitored through cameras, e-mails can be kept under control, documents and visited sites on the hard disk are traceable. Employers are in contact with their employees on a regular basis via smart mobile phones and computers, even at home. A survey that has been done in the United States revealed that 48% of employers are uncomfortable being monitored by mobile phones (Esen, 2005, p. 23). In addition, as supported by the results of some other studies, monitoring that takes place outside the working hours is not welcomed and perceived as interference with private life (Pearce & Kuhn, 2003, p. 372).

Recent research demonstrates that surveillance of employees is increasing with every passing day. A study conducted by the American Management Association has identified that the number of companies monitoring employees' phones, e-mails, voice mails, and computer use rose from 37% to 43% within a year (Lyon, 2006, p. 84). Another study conducted in

the USA has revealed 45% of the businesses monitor their employees' all kinds of electronic communications. Internet monitoring software records each and every word in e-mail messages and employees' search histories (Watson, 2001, p. 82).

Technical facilities provided by the internet, cameras, and listening devices have made surveillance more widespread than ever, both in communal and personal areas. For example, more than 4 million closed-circuit cameras are recording in the UK every day and when compared to the total population, there is a surveillance camera for every 15 people (Dolgun, 2008, p. 253).

Those who are under surveillance are unfortunately not aware whether it is their e-mails, web pages, or hard drives that are being monitored. In addition, it is not known whether the surveillance is continuous, random or as needed (National Work Rights Institute, n.d., p. 3-4). It is important that the employees be informed of the framework for recording activities. The board in Jean Monnet Building of the European Commission in Luxembourg which is easily visible by everyone, says "the personal data recorded by the cameras in the building will be processed in accordance with the European Commission's statute numbered 2001/45 and will not be used otherwise. The data will be stored for a period of 30 days only, and if necessary will be forwarded to the judicial authorities to be used in the investigation and prosecution of offenses when necessary". Thus, the individuals are assured that the data obtained from the records will not be used for purposes other than those mentioned (Civelek, 2011, p. 42).

Most employers think they are entitled to monitor their employees because they use company resource. Employees, on the other hand, feel humiliated and belittled as a result of monitoring (Ariss, 2002, p. 555). Electronic monitoring is said to cause extreme stress, a decline in job satisfaction and the quality of performance in workplaces (Watson, 2001, p. 82). Employees think of monitoring as an intervention in their private lives, also as an unethical and illegitimate practice (Lease & Gordon, 2005, p. 4).

According to a survey carried out by Massachusetts Coalition on New Office Technology with the participation of 49 enterprises and 700 employees, 81% of respondents stated that being monitored makes their work more stressful. A similar result was obtained by The National Institute for Occupational Safety and Health in America NIOSH, which confirms that employees who are exposed to more monitoring than their peers have been identified to experience a higher degree of depression, tension and frustration (Yilmaz, 2005, p. 33).



The use of computers and the internet is rapidly increasing in our country. According to TÜİK (2012a) Household ICT Usage Survey results, 47.2% of households in Turkey have internet access at home. As of January 2012, 92.5% of enterprises with 10 and more employees are reported to have internet access. Internet access rate is 99.6% for enterprises with 250 or more employees, 98.1% for enterprises with 50-249 employees, and 91.2% for enterprises with 10-49 employees (TÜİK, 2012b).

According to a study carried out in Turkey, the majority of employees tend to think the management has the right to monitor the workplace and it will bring positive results such as an increase in employee productivity and reduction of workplace incidents such as theft and abuse. However, the results also indicate that workplace monitoring may harm employees' privacy, demoralise and demotivate the employees and disturb the peaceful working environment (Erdemir & Koç, 2006, pp. 559-560). In another study analysing the current situation in Turkey, it has been found out that monitoring the internet, telephone, computer, and instant messaging programs is quite frequent. However, checking desks and offices, taking employee fingerprints, retinal scan, scanning e-mails and mobile camera phones were found to be the least encountered methods (Erdemir, 2008).

## **The Source of Legitimacy for Monitoring Employees: Productivity and Efficiency**

Sennett (1992, p. 57) suggests that each person in society needs an authority. Flexible work forms of information society leads to "authority without power". Employers are in fear of losing their authority over workers and tend to think that home office employees would abuse this freedom. For this reason, they wish to establish a strict control mechanism for people who are not in the company premises. This control mechanism is operated through asking employees to contact the enterprise by phone on a regular basis or inspecting their e-mails over an intranet (Sennett, 2002, pp. 48-61).

Organizations derive their authority from such functions as deterrence, conditioning and rewarding. According to Berle and Means (1991) the reason why organizations are so powerful in information-based society is because the authority has shifted from property owners to executives. These two scientists studied why U.S. company executives who have only some small shares of the company capital have such great decision-making powers (Galbraith,

2004). Modern corporate executives are today's powerful classes. Russell (1990, p. 45) asserts that with the development of large organizations, a new, powerful individual who possess "executive powers" has emerged

Along with the development of information technologies, there has been a widespread use of electronic monitoring systems allowing for increased control over information. During this period, which is also known as post-industrial society, information and knowledge has become an integral part of power, and also "the main force of production" (Lyotard, 1990, pp. 11-12). One of the most important goals of modernism is progress, and in this respect all the elements within the organization should be mobilized in accordance with pre-determined objectives (Erdemir, 2007, p. 82). Monitoring systems that are set up for controlling employee productivity are mainly used to ensure that information technologies, electronic e-mail or the internet are used appropriately and in a work related manner, to detect psychological mobbing, violence, theft and harassment incidents, to prevent leakage of trade secrets and proprietary information and to prevent malicious people from entering the employer's computer system, to prevent overloading in the computer network, to provide evidence for any legal cases that have gone to court, and to monitor customer satisfaction standards (Grey-Noble, 2008, p. 3; Lasprogata, King, & Pillay, 2004, pp. 2-3).

In the new capitalist period, on the one hand individuals are regarded as the "the most precious capital", on the other hand they are converted into robots or cyborgs being integrated into the same system as inanimate minds of machines, and turned into capital, goods and labour and eventually they have become a manufacturing tool as a whole. Moreover, in case the individual rejects being a part of this production process, he or she is inevitably isolated, excluded and mistreated (Gorz, 2001, p. 16). Foucault (2007) theorizes that the effectiveness of surveillance came about due to the rise of division of labour. With each person's task becoming more and more exact and differentiated from that of his or her co-workers, each person becomes more specialized and therefore individualized. This in fact allows individuals to be more easily documented, separated, and controlled in case of lethargy, resistance or threatening the capitalist system.

Foxconn factories which manufacture iPhones that have made Apple the world's most valuable company have recently shaken with riots and suicides. G. Crothall, a journalist in China Labour Bulletin analyses the situation as "workers are revolting against injustice and want their rights but they are under pressure for incessant production" ("Foxconn kilidi vurdu",

2012). This analysis reveals how performance pressure affects the employees. As Maier (2006, p. 31) puts forward, companies are the real actors of this big game in the business world, whereas employees act only as a pawn in such a system.

Whalen and Gates (2010, pp. 14-22), underline the positive aspects of voluntary monitoring in a qualitative study they conducted in America by interviewing eight IT employees who were monitored both before and during the hiring process. The study has suggested four benefits of employee monitoring, such as personal safety, identifying errors easily, facilitating collaboration, and ease of recording. In addition, increased job satisfaction and career identification have been suggested as secondary benefits. Farlee's (2010, pp. 204-206) model for disclosure and concealment of information obtained during monitoring employees shows that concealment of information may contribute to risk-sharing whereas disclosure may help in decision-making. In this study, it is found out that the information disclosed is related to the production system rather than the monitoring system, and if the disclosed information does not have a direct influence on the relationship between employee activities and outputs, the information may be disclosed. Smith and Tabak (2009, p. 46) express the organizational environment, technology, structure, and cultural factors should be taken into account in designing e-mail monitoring systems. According to the authors "trust" is at the heart of high-performance work environment, and confidentiality is a necessary component to build relationships that are based on trust.

All monitoring activities are in conflict with approaches such as empowering the employees, delegation, teamwork, or promoting information sharing (Taft, Mithas, & Krishnan, 2007). Al-Rjoub et al. (2008, p. 194) carried out a survey in private and public universities and banks in Jordan about the use of electronic monitoring. This survey has identified that employee behaviour improves when they are electronically monitored. However, the employees mentioned they would not like to be monitored.

However, various research has also revealed that employees copy corporate software for home use, use internet services provided by the company for personal or recreational purposes, access files that they are unauthorised to see, visit pornographic sites, use corporate tools and facilities outside organizational purposes, damage corporate and co-workers' data, hide some employees' faults and blame others for such faults, extend the standard processing time for a task or coffee breaks (Erdemir & Çeliktaş, 2006, p. 91; TÜGİAD, 1992, p. 48).

## Panopticon's Electronic Resurrection

Communication surveillance to provide intelligence is taking place in the international arena. There is even a conspiracy theory about the intelligence agencies of five states (U.S., UK, Canada, Australia and New Zealand) jointly establishing a surveillance system known as ECHELON (Big Ear). According to allegations, this system is capable of content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission, public switched telephone networks and microwave links (Beceni, 2004, p. 14). Such theories confirm Foucault's approach which regards authority as a reflection of power relations. According to this approach, authority is a mechanism which basically controls individuals, groups, and classes, puts pressure on them and does not leave room for manoeuvre (Foucault, 2004, p. 31). However, for Foucault (2004, p. 47) analysing power requires analysing the tools that produce, disseminate, distribute and record knowledge rather than analysing the ideology of power. According to Foucault, examining the source of power will only lead us to endless discussions, instead we should focus on ways the power influences us (Foucault, 2000, p. 308). Power is everywhere and 'comes from everywhere' so in this sense is neither an agency nor a structure. Power is not about who manages and who is managed, but it is about historical institutions such as prison, school and hospital. Relating the power to monarchy would be a simplistic approach, monarchy would not be able to intervene in the private lives of people. The essential thing to focus on is not the visibility or monitoring activities of power, it is how it makes its targets visible and traceable (Rouse, 1994, p. 95). From this perspective, electronic monitoring systems indeed continuously make their targets visible and traceable. In the information society, governments cannot confine people indoors, but virtual space makes people always visible and monitored. G. Morgan (1998, p. 383), uses metaphors to explain the administrative processes. According to him, even though organizations are social realities, they have turned into entities that enable a certain extent of monitoring on those who have established them.

Allen, Coopman, Hart, and Walker (2007, p. 174) suggest that many authors have used the metaphor of the Panopticon to express the secretive character of organizational monitoring. Bentham (1995, p. 34) devised an architectural device he called the *Panopticon*. The Panopticon was a universal institution based on the design for a Russian factory that minimised the

number of supervisors required, and proposed by Bentham for the design of prisons, workhouses, mental asylums and schools. The underlying principle of Panopticon order is the total and constant surveillance of inmates, workers, patients or pupils. But Bentham believed this approach could be successfully adopted in any environment which involved some level of supervision.

For Foucault, Bentham's Panopticon is a symbol for the modern disciplinary society. The Panopticon creates a consciousness of permanent visibility as a form of power, where no bars, chains, and heavy locks are necessary for domination any more. Foucault proposes that not only prisons but all hierarchical structures like the army, schools, hospitals and factories have evolved through history to resemble Bentham's Panopticon. This is the trick played by authority, and the authority actually covers much more than all the places and things in an insidious manner (Aktas, 2012, pp. 62-63). According to Bakunin those who represent authority invent such systems for their own benefit (2000, p. 114).

Bentham's Panopticon plan is an expression of asymmetrical surveillance. Each individual, in his place, is securely confined to a cell from which he is seen from the front by the supervisor; but the side walls prevent him from coming into contact with his companions. He is seen, but he does not see; he is the object of information, never a subject in communication. The panoptic mechanism arranges spatial unities that make it possible to see constantly and to recognize immediately. It reverses the principle of the dungeon; or rather of its three functions -to enclose, to deprive of light and to hide- it preserves only the first and eliminates the other two. Full lighting and the eye of a supervisor capture better than darkness, which ultimately protected. Visibility is a trap (Foucault, 2005, p. 251). Electronic monitoring systems are a kind of virtual simulation of the Panopticon. All video recordings, electronic monitors, GPS signals, sound recordings create a prison environment in our daily lives by not allowing a single dark spot. An illusionary freedom has surrounded us, because the new system keeps a record of everything you did, which gives you the chance to re-watch that moment that happened even months or years ago. Sennett (2011, p. 38) asserts that ICT facilitates panoptic surveillance by digitizing the highlights of real-time maps.

Tight control and monitoring manifested itself for the first time in the Fordist period with Taylor's scientific management principles. Fayol also

emphasized the efficiency of close monitoring and surveillance. Taylorism and Fordism are two prominent strategies for controlling the labour process (Munck, 1995, p. 218), and the organizational design in Classical theory resembles a prison where inmates are monitored. Functional foreperson system creates a structure that follows the personnel everywhere.

E-monitoring emerged in the 1960's in America, Canada and the UK to be used in prisons, then began to be used in business environment (Al-Rjoub et al., 2008, p. 190). In capitalist production forms, the efficiency of the worker has been replaced by the efficiency of management. Now management carried out all the functions of production, thus eliminating labour from the process of production (Braverman, 2008, pp. 175-176).

## Conclusion

One of the major repression tools in today's business environment is organizational surveillance, which is an outcome of flexible working conditions. As Sennett (2002) expresses, with flexible working hours, the organizations seem to give the time as an award to employees but then expose them to strict surveillance tools in fear of losing their authority.

The Council of Europe emphasizes some basic principles to be complied with for a fair surveillance. These principles are: necessity, certainty, proportionality, transparency and security (Mitrou & Karyda, 2006, p. 170). International Labour Organization has also adopted some principles regarding the protection of privacy, according to which, employees and representatives must be informed of the conditions of the data gathering process and their rights within this process. Also utmost care should be taken to protect the privacy of the employees and records of personal information must be kept to a minimum. Regular training should be provided for data recording and analysis officials to increase their awareness of the seriousness of the work they are doing. Employers, employees and their representatives should cooperate for the confidentiality of personal information and this information should not give rise to any discrimination. Employers should not gather any data about employee's sex life, political, religious and other beliefs and should not test employees' tendency for crime. The information collected should be accessed by authorized personnel only and this information should not be shared with third parties without the employee's knowledge and consent (Kaplan, 1997, p. 383).

Mitrou and Karyda (2006, p. 176) suggests a list of fundamental principles that should be complied with for a lawful monitoring to balance employers' security and employees' privacy. The purpose of the monitoring policy should be explained to the employees, the company e-mail, Internet, and telephone usage policies must be dynamic policies that are under constant review and posted in the workplace, on computer sign-on screens, and mentioned at weekly staff meetings, employees should be encouraged to submit ideas and become an integral component of the policy creation process. This would certainly help with compliance and could also improve employee morale since the employees would be invested in the process.

The location information obtained from GPS systems, and tablet devices to keep track of employees should be limited to work hours. Recording information about the location of employees 24 hours a day is a violation of privacy. The employer is not a guardian following every movement of prisoners. Grey-Noble (2008, p. 6-7) states that inappropriate monitoring in the workplace will cause insecurity between employees and managers, which will reduce the motivation of the work environment and negatively influence the organizational culture.

In order to protect the privacy of personal information, computer technologies such as privacy-enhancing technologies (PET) can be used. The purpose of these technologies is to assist in the implementation of ethical principles by controlling the spread of personal data online. Report published by the OECD in 1997 supports technologies and policies which provide protection to personal data. In 1998, the OECD Ministerial Conference held in Ottawa expressed they approve of the use of PET (OECD, 1997).

Petronio (2004, p. 174), introduces CPM: Communication Privacy Management theory to solve the everyday life problems in a practical way. According to CPM, organizational monitoring must be mentioned as a written rule of business ethics. According to a study that is conducted on 1900 companies operating in the United States, Canada, Mexico and Europe in 1992, 84% of the companies in the United States and 58% of the companies in the rest have written business ethics rules. 25% of these companies mentioned to have given training to their employees, assigned ethics committees or identified ombudsmen in the last three years (Kidder, 1995, pp. 84-85).

Organizational monitoring is on the agenda with negative thoughts such as doubt, disobedience and insecurity. Any employee who feels he or she is being monitored will be disturbed by this situation thinking that there is a

lack of confidence towards him or her. On the other hand, managerial practices such as personnel empowerment and teamwork will create an environment of trust and will boost institutional commitment. Here are two different situations that represent a paradox regarding employer and employee relations. It is not easy to tell right from wrong and manager also may fall into the trap of rationalizing unethical behaviour, because organizational surveillance is a grey area that cannot simply be solved with a yes or a no.

## References/Kaynakça

- Aktaş, Ü. (2012). *Anarşizm*. İstanbul: Metamorfoz Yayıncılık.
- Alder, G. S., & Ambrose, M. L. (2005). Towards understanding fairness judgments associated with computer task-specific monitoring: An integration of the feedback, justice, and monitoring research. *Human Resource Management Review*, 15, 43-67.
- Allen, M. W., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, 21 (2), 172-200.
- Al-Rjoub, H., Zabian, A., & Qawasmeh, S. (2008). Electronic monitoring: The employees point of view. *Journal of Social Sciences*, 4 (3), 189-195.
- Ariss, S. S. (2002). Computer monitoring: Benefits and pitfalls facing management. *Information and Management*, 39, 553-558.
- Bakunin, M. (2000). *Tanrı ve devlet* (çev. S. Ergün). Ankara: Öteki Yayınevi.
- Beceni, Y. (2004). *Siber uzayda mahremiyet*. İstanbul: II. Türkiye Bilişim Şurası Hukuk Çalışma Grubu.
- Bentham, J. (1995). *The panopticon writings* (Ed. M. Bozovic). London: Verso.
- Berle, A., & Means, G. C. (1991). *The modern corporation and private property*. New Brunswick, N.J.: Transaction Publishers.
- Botan, C. (1996). Communication work and electronic surveillance: A model for predicting panopticon effects. *Communication Monographs*, 63 (4), 293-313.
- Bowie, N., & Duska, E. R. F. (1990). *Business ethics*. Englewood Cliffs, N.J.: Prentice Hall.
- Braverman, H. (2008). *Emek ve teknelci sermaye: Yirminci yüzyılda çalışmanın değersizleşmesi*. İstanbul: Kalkedon Yayınları.
- Castells, M. (2005). *Enformasyon çağı: Ekonomi, toplum ve kültür. Ağ toplumunun yükselişi* (çev. E. Kılıç). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- Civelek, D. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi*. Yayımlanmamış uzmanlık tezi, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Ankara.
- Dolgun, U. (2008). *Şeffaf haphişane yahut gözetim toplumu*. İstanbul: Ötügen Neşriyat.
- Eralp, Ö. (2013). *KPS (Kimlik Paylaşım Sistemi), AKS (Adres Kayıt Sistemi) uygulamaları ışığında bireysel mahremiyet*. <http://www.ozgureralp.av.tr/makaleler/tckimliktdb.htm> adresinden 12.03.2013 tarihinde edinilmiştir.
- Erdemir, E. (2007). Adayış mı kaçış mı? Yönetimsel kontrol karşısında postmodern dönüşüm söylemi. *Yönetim Araştırmaları Dergisi*, 7 (1-2), 67-96.



Erdemir, E. (2008). Bilgi toplumunda çalışma ilişkilerinin yeni boyutu: İşyeri ve çalışanlara yönelik izleme faaliyetleri ve Türkiye'deki durum. *Sakarya Üniversitesi I. Ulusal Çalışma İlişkileri Kongresi bildiriler kitabı* içinde (s. 40-52). Sakarya.

Erdemir, E. ve Çelikaş, İ. (2006). Örgütsel ve hukuki açıdan işyeri izleme: Karşılaştırmalı bir inceleme. *Kazancı Hukuk Dergisi*, 19-20, 87-102.

Erdemir, E. ve Koç, U. (2006). İşyeri izleme faaliyetlerinin çalışanlar tarafından algılanışı: Eskişehir örneği. 14. *Ulusal Yönetim ve Organizasyon Kongresi bildiriler kitabı* içinde (s. 555-562). Erzurum: Atatürk Üniversitesi Yayınları.

Esen, E. (2005). Workplace privacy poll finding. *Society for Human Resource Management*, 1-47. Retrieved March 12, 2013, from <http://www.shrm.org/research/surveyfindings/documents/workplace%20privacy%20poll%20findings%20-%20a%20study%20by%20shrm%20and%20careerjournal.com.pdf>.

Farlee, M. A. (2010) Disclosure and secrecy in employee monitoring. *Journal of Management Accounting Research*, 22 (1), 187-208.

Foucault, M. (2000). *Hapishanenin doğuşu* (çev. M. A. Kılıçbay, 2. basım). Ankara: İmge Kitapevi Yayınları.

Foucault, M. (2004). *Toplumun savunmak gerekir* (çev. Ş. Aktaş, 3. basım). İstanbul: Yapı Kredi Yayınları.

Foucault, M. (2005). *Büyük kapatılma. Seçme yapıtlar: 3* (çev. F. Keskin ve I. Ergüden). İstanbul: Ayrıntı Yayınları.

Foucault, M. (2007). *İktidarın gözü seçme yazılar 4* (çev. I. Ergüden). İstanbul: Ayrıntı Yayınları.

Foxconn kilidi vurdu. (2012). *Radikal Gazetesi*. <http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1101561&CategoryID=80> adresinden 25/03/2013 tarihinde edinilmiştir.

Galbraith, J. K. (2004). *İktidarın anatomisi* (çev. R. Dikmen). Ankara: Hece Yayınları.

Goetz, A. (2001). *Yaşadığımız sefalet, kurtuluş çareleri* (çev. N. Tural). İstanbul: İletişim Yayınları.

Grey-Noble, B. (2008). *Workplace monitoring and the management of staff privacy: Issues and solutions*. Library 504- Individual Paper (pp. 1-11). University of British Columbia.

Kaplan, E. T. (1997). İş hukuku'nda kişilik haklarının özellikle bilgisayarda toplanan bilgilere karşı korunması. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* [Prof. Dr. Cemal Mıhçıoğlu'na Armağan], 52 (1-4), 383-386.

Kidder, R. M. (1995). *How good people make though choices*. New York: William Marrow Inc.

Lasprogata, G., King, N. J., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, 4, 1-46.

Lease, D. R., & Gordon, J. (2005). *Balancing productivity and privacy: Electronic monitoring of employees*. Retrieved December 11, 2012, from [http://www.drdaivlease.com/uploads/Balancing\\_Productivity\\_and\\_Privacy\\_David\\_Lease.pdf](http://www.drdaivlease.com/uploads/Balancing_Productivity_and_Privacy_David_Lease.pdf).

Lyon, D. (2006). *Gözetlenen toplum: Günlük hayatı kontrol etmek* (çev. G. Soykan). İstanbul: Kalkedon Yayınları.

Lyotard, J. F. (1990). *Postmodern durum* (çev. A. Çiğdem). İstanbul: Ara Yayıncılık.

Maier, C. (2006). *Merhaba tembellik: İşyerinde olabildiğince az çalışmanın yolları ve gerekliliği* (çev. R. Akman). İstanbul: Merkez Kitapçılık.

Mitrou, L., & Karyda, M. (2006). Employees privacy vs. employers security: Can they be balanced? *Telematics and Informatics*, 23, 164-178.

- Morgan, G. (1998). *Örgüt ve yönetim teorilerinde metafor* (çev. G. Bulut). İstanbul: MESS Yayınları.
- Munck, R. (1995). *Uluslararası emek araştırmaları*. Ankara: Öteki Yayınları.
- National Workrights Institute. (n.d.). *Privacy under siege: Electronic monitoring in the workplace*. Retrieved December 12, 2012 from <http://epic.org/privacy/workplace/e-monitoring.pdf>.
- The Organisation for Economic Co-operation and Development (OECD). (1997). *Implementing the OECD privacy guidelines in the electronic environment, focus on the Internet*. Retrieved January, 2, 2013, from <http://www.oecd.org/redirect/dataoecd/33/43/2096272.pdf>.
- Pearce, J. A., & Kuhn, D. R. (2003). The legal limits of employees off- duty privacy rights. *Organizational Dynamics*, 32 (4), 372-383.
- Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by. *Journal of Family Communication*, 4, 193-208.
- Rouse, J. (1994). *Power/knowledge*. In G. Gutting (Ed.), *The Cambridge companion to Foucault* (pp. 92-114). Cambridge: Cambridge University Press.
- Russell, B. (1990). *İktidar* (çev. M. Ergin). İstanbul: Cem Yayınevi.
- Sennett, R. (1992). *Otorite* (çev. K. Durand). İstanbul: Ayrıntı Yayınları.
- Sennett, R. (2002). *Karakter aşınması: Yeni kapitalizmde işin kişilik üzerindeki etkileri* (çev. B. Yıldırım). İstanbul: Ayrıntı Yay.
- Sennett, R. (2011). *Yeni kapitalizmin kültürü* (çev. A. Onocak, 2. baskı). İstanbul: Ayrıntı Yayınları.
- Smith, W. P., & Tabak, F. (2009). Monitoring employee emails: Is there any room for privacy? *Academy of Management Perspectives*, 23 (4), 33-48.
- Söylemez, S. A. (2001). Yeni ekonomi, rekabet ve rekabet politikaları. *Ekonomik Yaklaşım Dergisi*, 12 (40), 1-27.
- Şaylan, G. (2002). *Postmodernizm*. Ankara: İmge Kitabevi.
- Tafti, A., Mithas, S., & Krishnan, M. S. (2007). Information technology and autonomy-control duality: Toward a theory. *Information Technology and Management*, 8 (2), 147-166.
- Türkiye Genç İş Adamları Derneği (TÜGİAD). (1992). *İş ahlakı ve Türkiye’de iş ahlakına yönelik tutumlar*. İstanbul: Yazar.
- Türkiye İstatistik Kurumu (TÜİK). (2012a). Hanehalkı bilişim teknolojileri kullanım araştırması. *Haber Bülteni*, sayı: 10880. <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880> adresinden 16/01/2013 tarihinde edinilmiştir.
- Türkiye İstatistik Kurumu (TÜİK). (2012b). Girişimlerde bilişim teknolojileri kullanım anketi. *Haber Bülteni*, sayı: 10939. <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10939> adresinden 16/01/2013 tarihinde edinilmiştir.
- Watson, N. (2001). The private workplace and the proposed notice of electronic monitoring act: Is notice enough? *Federal Communications Law Journal*, 54, 79-102.
- Whalen, T., & Gates, C. (2010). Watching the watchers: “Voluntary monitoring” of infosec employees. *Information Management & Computer Security*, 18 (1), 14-25.
- Yılmaz, G. (2005). Elektronik performans izleme sistemlerinin çalışanlar ve işletmeler üzerindeki etkileri. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 4 (7), 1-19.
- Yüksel, M. (2009). Mahremiyet hakkına ve bireysel özgürlüklere felsefi yaklaşımlar. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi (AÜSBFD)*, LXIV (1), 275-298.