Doç. Dr. Mehmet Bedii KAYA

Çalışanların İletişim Araçlarının Takibi

www.mbkaya.com

İŞVERENİN ÇALIŞANIN İLETİŞİM ARAÇLARINI İZLEMESİNİN VE İNCELEMESİNİN HUKUKİ BOYUTLARI

Doç. Dr. Mehmet Bedii KAYA

Çalışan İletişiminin Takibi: Takip etmek kabahat, takip etmemek de! Peki ne yapsın veri sorumlusu?

İşverenlerin çalışanlarının iletişim araçlarını takip etmesinin sınırları tartışılmaya devam etmektedir.

İşveren çalışanın kurumsal e-postasını inceleyebilir mi? İşveren, çalışanın kurumsal mesajlaşma programını sürekli takip edebilir mi? Kurumsal e-posta ve iletişim sistemleri sınırsızca takip edilebilir mi?

İşverenlerin bir yandan mevzuata uyumu emredilmekte, bir yandan da mahremiyet ile dengeyi korumaları beklenmektedir. Ayrıca işverenlerin, çalışanlarının hukuka aykırı hareket etmesini önlemesi gerekmektedir. Uyumsuzluğun faturasını işveren ödemektedir.

İşveren, "Neden çalışanını takip etmedin ve denetlemedin?" sorusuyla karşı karşıya kalmaktadır. Çalışanını yoğun bir şekilde takip ettiği zaman da "Neden çalışanın mahremiyeti ihlal ettin?" sorusuyla karşı karşıya gelmektedir.

Kısaca, takip etmek de kabahat, takip etmemek de!

Kişisel Verileri Koruma Kurulu, 2026/2035 sayılı İlke Kararı ile konuyu yeni bir boyuta taşımıştır.[1]

Detaylara geçmeden evvel, KVK Kurulu'nun 2026/2035 sayılı kararında ilginç bir detay vardır.

[1] İşverenler Tarafından Çalışanlara Tahsis Edilen Kurumsal E-Posta Hesapları Başta Olmak Üzere, İşin Yürütülmesi Amacıyla Kullanılan İletişim Kanallarının Denetlenmesi Suretiyle Gerçekleştirilen Kişisel Veri İşleme Faaliyetlerinde Uyulması Gereken Usul ve Esaslar Hakkında İlke Kararı, Karar No: 2026/2035, Karar Tarihi: 16.09.2026, RG 08.10.2026/33394.

Bu karar oy çokluğuyla alınmıştır. Yani aslında Kurul üyelerinin tamamı bu konuda ikna olmamıştır. Oy birliği olmayan bir konuda ilke kararı alınması veya kararın ilke kararı olarak nitelendirilmesi ve tüm veri sorumlularından bu konuda yeknesak bir uygulama geliştirmelerinin beklenmesi de ayrı bir tartışma konusudur. Kararın oy çokluğuyla alınması, KVKK'yı uygulamaya yönelik karar verici Kurulun bu konuda hemfikir olmadığının teyidi niteliğindedir. Kurul hemfikir değilken, veri sorumlusu ne yapsın?

Kurul, işverenin genel denetim hakkının kapsamını alabildiğine daraltmış ve kısıtlamıştır.

Peki, işverenin iş amacıyla tahsis ettiği iletişim araçlarını kontrol etmesinde hakkaniyetli denge nasıl sağlanacaktır?

Şu bir gerçek ki, mevzuata uyum mazeret dinlememektedir. İş hukuku, siber güvenlik hukuku, kişisel verileri koruma hukuku, internet hukuku, rekabet hukuku, fikri mülkiyet hukuku ve yapay zeka hukuku kuralları çalışanların en ufak hatasını işverene fatura etmekte ve aykırılıkları çok ağır şekilde cezalandırmaktadır. Çalışanların tüm iletişim araçlarınn 7/24 denetimi bu bağlamda istisnai değil, genel bir kural hâline dönüşebilmektedir.

İş Kanunu, 7545 sayılı Siber Güvenlik Kanunu, KVKK m 12, 5651 sayılı Kanun, Rekabetin Korunması Hakkında Kanun, 6769 sayılı Sınai Mülkiyet Kanunu, 5846 sayılı Fikir ve Sanet Eserleri Kanunu ve daha nice düzenleme işverene gene bir takip ödevi getirmektedir. Ex-post değil ex-ante sorumluluk yüklemektedir.

Konuyu farklı mevzuatlar açısından ele alalım.

I. İş Hukuku Bağlamında Çalışanın Takibi

İşverenin, iş sözleşmesinin gereği gibi ifa edildiğini temin etmesi gerekmektedir. Müşterilere, iş ortaklarına ve yetkili kurumlara ne zaman dönüş yapıldığı, nasıl dönüş yapıldığı, hangi üslupla yazışıldığı, yazışmalarda standart şirket terminolojisinin takip edilip edilmediği, hangi tonun kullanıldığı ve nezaket kurallarına riayet edilip edilmediği gibi birçok konuyu sürekli denetlemesi gerekmektedir. Bu tür durumlarda iletişim araçlarının incelenmesi zaten sözleşmesel bir zorunluluktur. Kurumsal iletişim kuralları, şirketlerin ticari rekabetinde de belirleyici bir faktördür. İşverenin iletişim kanallarını denetlemesine bir sınır getirilirse, iş sözleşmesindeki denge haksız şekilde bozulmuş olur.

İşverenin bir çalışanının bir e-postayı saat kaçta yanıtladığı, nasıl hitap kullandığı, kopya veya gizli kopyaya kimi koyduğu, hatta yazışmada hangi emojiyi kullandığını bile bilmesinde meşru bir menfaati vardır.

Hatırlanacak olursa KVK Kurulu, bir e-postanın kopya (cc) kısmına eklenmemesi gereken bir kişinin eklenmesini KVKK'nın 12. maddesinin ihlali görerek idari para cezası uygulamıştır. Kurulun ilk ceza verdiği konulardan birisidir.

Nijhayetinde, iş amacıyla tahsis edilen bir aracın işin gereklilikleri sebebiyle proaktif şekilde takip edilmesi öngörülebilecek bir davranıştır. İş amaçlı iletişim kanallarında aslolan takiptir. Genel kanı da buna yöneliktir. Kurumsal olsun veya olmasın bir çalışan işe başladığı zaman kendisine böyle bir bilgi verilmemiş olsa bile en azından işin düzgün şekilde yerine getirildiğinin tespiti için yazışmalarının takip edileceğini öngörür. Bu tür işlemler iş tanımına mündemiç konulardır. Hayatın olağan akışı, ortalama bir çalışanın bu konuda bu yönde bir farkındalığının olmasını gerektirir.

İşverenin iletişim kanallarını ve içerğini incelemedeki menfaati, çalışanın işten ayrılmasından sonra da devam etmektedir. İşten ayrılmadan sonra birincil işleme amacıyla değil ikincil işleme amaçlarıyla işlenmeye devam edecektir. İşverenin, işten ayrılan çalışanının müşterilere nasıl taahahütler verdiğini, edimin ana veya tali unsurlarında bir değişiklik yapıp yapmadığını, termin ve teslim koşullarına ilişkin bir değişiklik yapıp yapmadığını öğrenme hakkı vardır. Sözleşmenin zamanaşımı süresi boyunca sözleşmeye muhatap olmuş çalışanın e-posta kayıtlarına delil amacıyla bakmak gerekebilmektedir. Örnekleri artırmak mümkündür.

Uzaktan çalışma durumunda işverenin çalışanının iletişim kanallarını denetimine yönelik hakkı daha da öne çıkmaktadır.

Esasında takip tek taraflı da değildir. Çalışan da işini düzgün yaptığını ispat amacıyla bu verileri kullanabilecektir. Bu takip sisteminin bilgi asimetrisini azaltıcı rolü vardır.

Kısaca, işveren iş hukuku kurallarına uyumun temini için iletişim kanallarını ve iletişim içeriklerini 7/24 kontrol etmek zorundadır. İş sürekliliğinin sağlanması, işverenin operasyonal güvenliğinin sağlanması gibi işverenin menfaatleri, çalışanın menfaatlerine üstün gelmektedir.

II. Siber Güvenlik Hukuku Bağlamında Çalışanın Takibi

İşverenin siber güvenliği sağlaması kanuni bir yükümlülüktür. Bilişim sistemlerini ve verileri siber saldırılardan korumak, bu ortamlarda işlenen verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına almak, saldırıları ve siber olayları tespit etmek, bu tespitlere karşı tepki ve alarm mekanizmalarını devreye almak ve sonrasında yaşanan siber olay öncesindeki duruma geri dönmek en temel yükümlülükler arasındadır. 7545 sayılı Siber Güvenlik Kanunu, koruma, güvence sağlama, tespit, tepki verme ve geri döndürme

yükümlülüklerinin yerine getirilmemesini hem idari para cezaları hem de hapis cezaları ile yaptırıma bağlamaktadır.

Veri sızıntılarında paradigma değişmiştir. Konu artık yalnızca para cezalarıyla değil, hapis cezalarıyla da disipline edilmektedir. Siber Güvenlik Kanunu uyarınca, kanundan kaynaklanan görev ve yetkilerini kötüye kullananlara veya kritik altyapıların siber saldırılara karşı korunması kapsamında görevinin gereklerine aykırı hareket etmek suretiyle veri ihlali yaşanmasına sebebiyet verenlere bir yıldan üç yıla kadar hapis cezası verilir. İşverenlerin kişisel veri dahil her türlü veri türüne yönelik suç işlenmesini önlenmesine yönelik yükümlülükleri doğmuştur.

Uçtan uca siber güvenliğin sağlanmasının yolu, tüm bilişim sistemlerinin uçtan uca ve sürekli takibinden geçmektedir. Sadece iletişim kanalının değil, içeriğin de sürekli kontrolü zorunludur. Bu amaçlar bakımından işverenin menfaatleri, çalışanın menfaatlerine üstün gelmektedir.

III. KVKK Bağlamında Çalışanın Takibi

İşverene, çalışanın iletişim kanallarını ve içeriklerini sürekli denetleme yönünde yükümlülük getiren temel düzenlemelerden biri aslında KVKK'nın kendisidir.

KVKK'ya göre işveren (= veri sorumlusu), kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak zorundadır. Uygun teknik tedbirleri almayan ve kişisel verilere yetkisiz erişime yol açan işveren, KVKK kapsamında idari para cezası ile karşı karşıya kalabilmektedir.

Konu yalnızca kişisel verilerin veri sorumlusu dışına çıkması değildir. Hukuka aykırı işlemeyi önleme yükümlülüğü, veri işleme faaliyetlerinin dayandığı hukuki işleme sebeplerinin de kontrol edilmesini kapsamaktadır. İşveren, iş birimlerinin doğru hukuki işleme sebeplerine dayanıp dayanmadığını dahi sürekli kontrol etmekle yükümlüdür.

KVKK'ya uyum açısından iletişim araçlarının ve içeriklerinin 7/24 takibi kanuni bir zorunluluktur. Aksi durum, KVKK bakımından bir çelişki oluşturacaktır. Hukuk, belirliliği zorunlu kılar. Bu konuda en ufak bir tereddüt yaşanması hâlinde, ortaya çıkacak bir kişisel veri ihlalinde ihlal mazur görülebilecek midir?

Keza, kişisel veri yalnızca kimliği belirli olan kişilere ilişkin verileri değil, kimliği belirlenebilir kişilere ilişkin verileri de kapsamaktadır. Kişisel veri, belirli durumlarda bağlamsal nitelik taşıyabilmektedir. Bu nedenle kişisel veri ihlalleri, basit bir formülle takip edilebilecek bir formattan ibaret değildir.

Kısaca, KVKK'ya uyumun temini için iletişim kanallarının ve içeriklerinin sürekli denetlenmesi ve incelenmesi KVKK'nın 12. maddesinde somutlaşmış bir hukuki zorunluluktur.

IV. İnternet Hukuku Bağlamında Çalışanın Takibi

Türk bilişim hukukunun en temel düzenlemesi İnternet Kanunu olarak da anılan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dur.

İşverenler, çalışanlara internet altyapısı sunmakla 5651 sayılı Kanun bağlamında ticari amaçlı olmayan toplu kullanım sağlayıcısı statüsüne geçmektedir. 5651 sayılı Kanun'un 7. maddesinin ikinci fıkrası uyarınca ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür.

İşverenler, internet ağlarında suç işlenmesinin önlenmesi için tedbir almakla ve internet ağındaki aktiviteleri takip etmekle yükümlüdür. 5651 sayılı Kanuna uyumun temini için iletişim kanallarının ve içeriklerinin sürekli denetlenmesi ve incelenmesi 5651 sayılı Kanun kapsamında hukuki bir zorunluluktur.

V. Yapay Zeka Hukuku Bağlamında Çalışanın Takibi

Yapay zeka, siber güvenlik açısından ciddi bir risk oluşturmaya başlamıştır. Eskiden bir şirkete yönelik siber saldırı gerçekleştirmek için ileri düzey teknik bilgi gerekirken, artık yapay zekâ araçlarıyla karmaşık saldırılar çok daha kolay şekilde gerçekleştirilebilmektedir. Çocuklar bile bu tür saldırıların faili olabilmektedir.

Deepfake yöntemleriyle yalnızca ses ve görüntü taklidi değil, kişilerin yazım tarzları da taklit edilebilmektedir. El yazısı nasıl kişiye özgü bir örüntü içeriyorsa, dijital ortamda yazılan metinlerden de kişiye özgü örüntülerin çıkarılması mümkündür.

Bunlar teorik düzeyde kalan tehditler değildir. Oltalama saldırılarının ötesinde, nokta atışı niteliğinde zıpkınlama saldırılarının gerçekleştirildiği bir dönemdeyiz.

Risk durumuna göre tedbirlerin daha da ileri seviyeye taşınması zaruridri. Kimlik taklidi tehditlerinin önlenmesi amacıyla kritik konumdaki çalışanların görüntü, ses ve yazım gibi biyometrik verilerinin işlenmesi, bunların parmak izlerinin çıkartılması belirli durumlarda kişisel verilerin korunması ve veri sorumlusunun operasyonel güvenliğinin sağlanması açısından kaçınılmaz hâle gelebilmektedir.

Çalışan, gerçek bir kişiyle mi yoksa başkasının kimliğini taklit eden biriyle mi muhataptır? Bu konuda proaktif tedbirlerin alınması zorunlu hâle gelmektedir. Önleyici bir yaklaşımla gerekli tedbirler alınmazsa, telafisi mümkün olmayan zararların ortaya çıkması mümkündür.

Yakın zamanda, CEO'dan gelmiş gibi görünen sahte bir e-postaya teyit almaksızın yanıt verilmesi sonucunda bir üye listesinin saldırgana gönderildiği ve bu ihlal nedeniyle Kurulun 1 milyon TL idari para cezası kestiğine ilişkin bir haber paylaşılmıştı. Basit bir kimlik taklidiyle çok büyük ölçekli bir kişisel veri ihlali mümkündür.

Benzer şekilde, işverenin gölge yapay zeka (shadow AI) gibi kullanımları tespit etme ve önlemeye yönelik meşru menfaati bulunmaktadır. Gölge yapay zekayı tespit için de kurumsal e-postayla hangi platforma üye olunduğunu sürekli takip etmesi zorunludur.

Yapay zekâ çağında her bir çalışana yönelik her türlü siber aktivitenin 7/24 incelenmesi, çalışanların profillenmesi, iletişim içeriklerinin değerlendirilmesi, kontrol edilmesi, uzmanlara aktarılması, şirket içinde analiz edilmesi ve bu amaçlarla yapay zekâ araçlarının kullanılması bir zorunluluktur.

VI. Rekabet Hukuku Bağlamında Çalışanın Takibi

Çalışanların iletişimlerinin en ince ayrıntısına kadar denetlenmesini gerektirdiği bir diğer düzenleme, 4054 sayılı Rekabetin Korunması Hakkında Kanun'dur.

Rekabet Kurumu, 2020 yılında yayımladığı Yerinde İncelemelerde Dijital Verilerin İncelenmesine İlişkin Kılavuz hükümlerini uygulamaktadır.

Rekabet Kurumu; teşebbüslere ait sunucular, masaüstü ve dizüstü bilgisayarlar, taşınabilir elektronik cihazlar, CD'ler, DVD'ler, USB bellekler, harici diskler ve bulut servisleri gibi bilişim sistemleri üzerinde inceleme yapmaya yetkilidir. Ayrıca, tümüyle şahsi kullanıma özgülendiği tespit edilen taşınabilir iletişim cihazları hariç olmak üzere, cep telefonu ve tablet gibi taşınabilir iletişim cihazları üzerinde hızlı gözden geçirme yöntemiyle teşebbüse ait veriler üzerinde kontrol gerçekleştirebilir.

İşverenler, iş amaçlı tahsis edilen cihazlarda kurumsal rekabet politikalarının etkin şekilde uygulandığını tespit etmek, Rekabetin Korunması Hakkında Kanun'u ihlal edebilecek nitelikte herhangi bir içerik bulunmadığını temin etmek ve bunun için süreklilik arz eden bir denetim mekanizması kurmakla yükümlüdür.

Kısaca, Rekabetin Korunması Hakkında Kanun'a uyumun temini için iletişim kanallarının ve içeriklerinin denetlenmesi kanuni bir zorunluluktur.

VII. Fikri Mülkiyet Hukuku

İşeveren, işe özgülediği bilişim sistemlerinde fikri mülkiyet ihlallerini önlemekle yükümlüdür. Kişisel kullanımı freeware olan ancak ticari amaçlı kullanımı lisansa tabii olan bir yazılım çalışan tarafından kurumsal e-postasıyla kayıt yapılarak kullanılabilmektedir. Bu tür kullanımlar şahsi değil ticari kullanım olarak nitelendirilmektedir ve bu tür kullanımlar hem mali hem de cezai sorumluluk doğurmaktadır. Cezai sorumluluğun şahsiliği itibariyle ilgili çalışan sorumlulukla muhatap olsa da tüm süreçte işveren de hesap vermek durumunda kalabilmektedir. Mali kısımda ise sorumluluk işverene yüklenmektedir. İşveren, çalışanın kurumsal e-postasıyla hangi hizmetlere abone olduğunu periyodik olarak takip etmek zorundadır. Önleyici fikri mülkiyet hukuku uyumu için proaktif ve etkin bir mekanizma kurulması zorunludur.

VIII. Aktif Denetim Ödevi Getiren Diğer Özel Düzenlemeler

İşverenlerin aktif denetim ödevi altında olduğu düzenlemeler bunlarla sınırlı değildir. Bankacılıktan sağlığa gümrükten elektronik haberleşmeye kadar birçok alanda, çalışanların gerçekleştirdiği işlemlerin tamamının, çoğu zaman önceden haber verilmeksizin denetlenmesine dayanak oluşturan düzenlemeler bulunmaktadır. Keza, gizli bilgilerin ve ticari sırların korunması için de işverenin sürekli bir takip mekanizması kurması gerekmektedir. Örnekleri artırmak mümkündür.

Sonuç ve Değerlendirme

İşverenlerin denetim ödevinin genel değil de dar bir çerçeveye oturtulması hukuk sisteminin bütünlüğü ilkesiyle bir çelişki oluşturmaktadır.

İşverenin genel bir denetim ödevine sahip olması, KVKK'nın 4. maddesindeki ilkelere uymayacağı anlamına gelmemektedir. İşveren elbette bu işlemeleri meşru bir amaç doğrultusunda gerçekleştirecektir. İletişimin denetlenmesinin istisnalara hapsedilmesi ve işverenlerin takdir yetkisinin kısıtlanması, işverenin diğer hukuki yükümlülükleriyle çelişki oluşturmaktadır. Ayrıca bu durum, büyük ihlallerin ve güvenlik sorunlarının

ortaya çıkmasına yol açma riskini de bünyesinde barındırmaktadır. Mahremiyete daha az müdahaleci yöntemlerin tercih edilmesi, daha büyük güvenlik risklerinin ortaya çıkmasına neden olabilecektir.

Öte yandan, işverene genel aydınlatma yükümlülüğünün dışında ilave bir aydınlatma ödevi yüklenmesi, KVKK'nın 10. maddesinin lafzına da aykırı olacaktır.

Kişisel verilerin korunmasında işveren hesap verebilir olduğu sürece, tercih edeceği araçlara ilişkin otonomisi ortadan kaldırılmamalıdır.

Yukarıda izah edildiği üzere, yapay zekâ ile birlikte güvenlik riskleri farklı bir seviyeye taşınmıştır. Proaktif bir denetim mekanizmasının kurulması, çalışanların hem iç hem de dış paydaşlarla iletişiminin aktif olarak denetlenmesi, önleyici mekanizmaların oluşturulması, iletişim kurulan tarafa ilişkin hem üst verilerin hem de iletişim içeriğinin denetlenmesi, KVKK'nın hem lafzına hem de ruhuna uygun bir yorumdur.

İşverenlerin tabi olduğu mevzuatın çeşitlenmesi, meşru müdahale amaçlarının da çeşitlenmesine yol açmıştır.

KVKK 2016 yılında kabul edilmiştir. KVKK'nın zamanın ruhuna ve güncel risklere göre yorumlanması gerekmektedir. Amaçsal yorum ve hakkaniyet bunu gerektirmektedir. Yapay zekâ kaynaklı tehditler, siber güvenliği sağlama yükümlülüğü, yurt içi ve yurt dışı düzenlemelerden kaynaklanan çok katmanlı hesap verebilirlik rejimleri dikkate alındığında, daha hakkaniyetli bir yorum geliştirilmesi gerekmektedir.

İşveren aydınlatma ödevini yerine getirdiyse, bilgi güvenliği sözleşmesiyle çalışandan bilişim sistemlerinin iş amacıyla kullanacağına dair taahhüdü alındıysa, eğitim verilerek bilişim sistemlerinin iş amacıyla kullanması gerektiğine dair farkındalığı sağlandıysa, kısaca bir işyeri kuralı oluşturulmuşsa ve bunun için açık iş akışları oluşturulmuşsa ve aykırılıklara ait disiplin hükümleri oluşturmuşsa, mevzuatın öngördüğü meşru amaçlarla işverenin genel denetim denetim hakkı vardır denilebilecektir. İşveren, çalışanına iş amacıyla tahsis ettiği tüm iletişim araçlarını önceden haber vermeksizin ve süreklilik esasına göre hem takip edebilecek hem de inceleyebilecektir.

Veri sorumlusuna hem sorumlu ilan edip hem yetkilerini elinden almak KVKK'nın hem lafzına hem de ruhuna aykırıdır.

Tekrar vurgulamak gerekir ki, işverenin çalışanı genel takip etme hakkı hesap vermeyeceği ve bu süreçte elde ettiği verileri anlamına gelmemektedir. KVKK'nın temel ilkeleri her bir bit veri veya üst-veri için hukukiliğin belirlenmesinde yol gösterici olmaya devam edecektir.