integrity IN magazine

TEMMUZ-AĞUSTOS-EYLÜL 2016 SAYI:7

TEİD Etik ve İtibar Derneği Ethics & Reputation Society

Tüm Yolsuzlukla Mücadele Standartlarına Hükmedecek Standart

ISO 37001

Şirket İç Soruşturmalarında Çalışanların E-Mailleri Nasıl İncelenmeli?

Ahlâk Mirası Hangi Kasada Duruyor?

Aktivist mi O Uzaktaki?

Filler Neden Evcilleşmez

Yaşadığımız Güven Bunalımına Çözüm:

ACİL ETİK, ACİL UYUM...

İşverenlerin Aklındaki Soru:

ŞİRKET İÇ SORUŞTURMALARINDA ÇALIŞANLARIN E-MAİLLERİ NASIL İNCELENMELİ?

"İşverenler tarafından iç soruşturma süreci başlatıldığında e-maillerin okunmasına sıklıkla başvurulmaktadır. Ancak bu süreçte işverenin menfaatler dengesine göre hareket etmesi ve çalışanlarının kişilik haklarını koruma borcu altında olduğunu unutmaması gerekmektedir. Süreçte dikkat edilmesi gereken bir diğer husus ise şeffaflık ilkesidir. Bu kapsamda işverenin, çalışanlarını, e-maillerinin incelenebileceği konusunda iş sözleşmeleri ya da bilgi güvenliği gibi iç yönetmelikler aracılığı ile bilgilendirmesi uygun olacaktır."

Yazı: Av. Filiz TOPRAK ESİN, Av. Beril YAYLA, Av. Bensu AYDIN

Günümüzde şirket içi etik ve uyumluluk bilincinin artması oldukça sevindirici bir gelişme olarak karşımıza çıkıyor. Şirketler ihbar hatları kurarak, hem çalışanlarını bilinçlendirmekte hem de şirket içi uyumluluğun artmasına katkıda bulunuyor. Association of Certified Fraud Examiners (ACFE) 2016 Çalışan Suistimalleri ve İstismar Raporu (http://www.acfe.com/rttn2016.aspx), ihbar hattı olan şirketlerin yolsuzluğu yakalama oranının diğerlerine göre daha fazla olduğunu ve yolsuzluğun en yaygın tespit yönteminin ihbar olduğunu açık bir şekilde gösteriyor. Şirket iç mekanizması sayesinde bir uyumsuzluğun farkına varabileceği gibi, bir çalışanının veya üçüncü bir kişinin ihbarı ile de bir yolsuzluk iddiası ile karşı karşıya kalabilir. Böyle bir durumda, bu iddianın aslı olup olmadığını araştırırken şirket iç politikalarının olması hayat kurtarabilir. Yöneticiler serinkanlılıklarını kaybetmeden acil alarma basmalıdırlar. Genelde ilk reaksiyon olarak, uyum sorumlusu ve danışmanlarına başvurup acil bir yol haritası talep etmeleri gerekir. Bu noktada ilk akla gelen, yolsuzluğun mutlaka bir yerlerde iz bırakmış olduğudur. Bu izi takip etme yöntemlerinin başında ise yolsuzluğa dahil olduğu iddia edilen -şüphelenilen- çalışanın e-maillerinin incelenmesi gelir. Ancak bu süreç işverenler tarafından birçok tereddüde yol açmaktadır. Bu sürecin hukukun farklı yönleriyle değerlendirilmesi ve her aşamanın, bir sonraki aşama düşünülerek ele alınması çok önemlidir.

Bu çerçevede yazımızda disiplinlerarası bir yaklaşım ile kişisel verilerin korunması hukuku, iş hukuku ve ceza hukuku bakımından iç soruşturmalar kapsamında e-mail incelenmesi sürecinin nasıl yönetilmesi gerektiği değerlendirilecektir.

İŞ HUKUKU BAKIMINDAN DEĞERLENDİRMELER

İşverenler tarafından iç soruşturma süreci başlatıldığında e-maillerin okunmasına sıklıkla başvurulmaktadır. Ancak bu süreçte işverenin menfaatler dengesine göre hareket etmesi ve çalışanlarının kişilik haklarını koruma borcu altında olduğunu unutmaması gerekmektedir. Süreçte dikkat edilmesi gereken bir diğer husus ise şeffaflık ilkesidir. Bu kapsamda işverenin çalışanlarını e-maillerinin incelenebileceği konusunda iş sözleşmeleri ya da bilgi güvenliği gibi iç yönetmelikler aracılığı ile bilgilendirmesi uygun olacaktır.

İŞVERENLER TARAFINDAN İÇ SORUŞTURMA SÜRECİ BAŞLATILDIĞINDA, E-MAİLLERİN OKUNMASINA SIKLIKLA BAŞVURULUR. ANCAK BU SÜREÇTE İŞVERENİN MENFAATLER DENGESİNE GÖRE HAREKET ETMESİ VE ÇALIŞANLARININ KİŞİLİK HAKLARINI KORUMA BORCU ALTINDA OLDUĞUNU UNUTMAMASI GEREKİR.

Konu ile ilgili Yargıtay uygulamasına bakıldığında, Yargıtay'ın iş hukuku uyuşmazlıkları ile ilgilenen 9. Hukuk Dairesi'nin 13.12.2010 tarihli 2009/447 E. ve 2010/37516 K. sayılı kararı ile, *işverenin kendisine ait bilgisayar ve e-mail adresleri ile bu adreslere gelen e-postaları her zaman denetleme yetkisi bulunduğu* kabul edilmiştir. Yargıtay söz konusu kararında, çalışanların e-maillerinin incelenmesi durumunda işverenin yetkilerini son derece genişlettiği görülmektedir.

Diğer bir düzenleme ise 4 Şubat 2011 tarihli ve 27836 sayılı Türk Borçlar Kanunu'nun ("TBK") 419. maddesinde işçinin kişiliğinin korunması bölümünde yer alan "**İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir**." hükmüne ilişkindir. Söz konusu madde, geniş yorumlandığında şirket içi soruşturma sırasında şirket bilgisayarı üzerinden yapılan e-mail yazışmalarının, özel veya iş ile olup olmadığına bakılmaksızın incelenmesinin dahi mümkün olduğu söylenebilecektir.

Yargıtay'ın yaklaşımına karşı, uygulamada etik ve uyum bilincinin yüksek olduğu şirketlerin şeffaflık ilkesini benimsediği ve bu kapsamda iş sözleşmelerine ek olarak gizlilik politikaları, bilgi güvenliği politikaları gibi iç yönetmelikleri de çalışanlarına imzalattıkları görülmektedir. Ancak bu politikaların bağlayıcılığı ve e-mail incelemelerinin yapılmasının ne derece meş-

ru kıldığı da işverenlerce tereddüt oluşturan hususlardan birisidir. Zira çalışan e-mailleri kurumsal olsa da, bu e-mailler üzerinden kişisel yazışmalar da yapılabilmekte ve bu durum çalışanın özel hayatının gizliliğinin ihlal edilme riskini barındırmaktadır.

Bu konuda son derece yeni tarihli verilen Anayasa Mahkemesi'nin 10.05.2016 tarihli Resmi Gazete'de yayınlanan 24.03.2016 tarihli kararı bu konuya ışık tutmaktadır. Söz konusu kararda **Bilgi Güvenliği Taahhütnamesi ve İş Yeri Disiplin Yönetmeliği** gibi iş sözleşmelerinin parçası olarak kabul edilen iç yönetmelikleri imzalayan ve böylelikle işveren tarafından hazırlanmış kural ve kısıtlamaları içeren tüm genel düzenlemeler hakkında yeterli derecede bilgilendirilen çalışanların, kurumsal e-mail hesapları üzerinden gerçekleştirdikleri kişisel yazışmaların incelenmesinin mümkün olduğu sonucuna varılmıştır.

Buradan hareketle Anayasa Mahkemesi, çalışanların yazışmalarını inceleyen işverenin, meşru bir amaç taşıdığı ve işveren tarafından gerçekleştirilen müdahalenin söz konusu meşru amaçla ölçülü olduğu sonucuna vararak, çalışanların kurumsal e-mailleri üzerinden gerçekleştirilen kişisel yazışmalarının incelenmesinin özel hayatın gizliliğine dair haklarının ihlal edilmediğine hükmetmiştir.

Dolayısıyla, iş sözleşmelerinin yanı sıra işverence özellikle verilerin gizliliği ve kullanımı hakkında politikaların benimsenmesi ve bunların çalışanlar tarafınca kabul ettirilmesi, iç soruşturmalarda e-maillerin incelenmesi bakımından işverene ölçülü ve meşru olmak kaydıyla serbesti tanımaktadır. Söz konusu politikalarda ise kurumsal e-mailler üzerinden özel yazışmaların gerçekleştirilmesinin yasaklanması, işverene iç soruşturma sırasında e-maillerin incelenmesi konusunda karşılaştırılabilir düzeyde serbesti sağlayacaktır.

ASIL KURAL VERİ İŞLENMESİ İÇİN VERİ SAHİBİNDEN ONAY ALINMASI OLSA DA, BU ÖZELLİKLE İÇ SORUŞTURMALARDA HER ZAMAN MÜMKÜN OLMAZ BU NOKTADA, KİŞİSEL VERİ KANUNU'NDAKİ BİR TAKIM İSTİSNALAR DEVREYE GİRECEKTİR.

KİŞİSEL VERİLERİN KORUNMASI HUKUKU BAKIMINDAN DEĞERLENDİRMELER

Şirket çalışanlarının e-maillerinin incelenmesi ve bilgisayarın imajının alınması kişisel verilerin korunması bakımından da oldukça hassas bir konudur. **Özellikle 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete'de yayınlanarak kişisel verilerin korunmasına bambaşka bir boyut getiren Kişisel Verilerin Korunması Kanunu'nun ("Kişisel Veri Kanunu**") yürürlüğe girmesiyle birlikte iç soruşturmalarda atılacak her bir adımın bu açıdan da hukuka uygun olduğundan emin olunması gerekmektedir.

Peki, e-mail incelemesine başlanmadan önce veri sahiplerinden onay alınması gerekmekte midir?

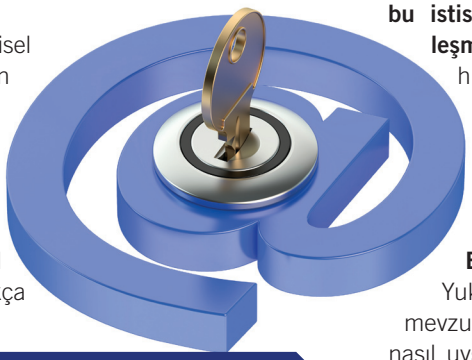
Kişisel Veri Kanunu açısından bakıldığında, ilgili kişilerin e-mailleri ve kurumsal bilgisayarları kapsamında kişisel veri niteliğindeki hususların barınması olasılığı bir hayli yüksek olduğundan, bu e-maillerin incelenmesi kişisel verilerin "işlenmesi" tanımı altında yer almaktadır. Asıl kural veri işlenmesi için veri sahibinden onay alınması olsa da, bu özellikle iç soruşturmalarda her zaman mümkün olmamaktadır. Bu noktada, **Kişisel Veri Kanunu**'ndaki bir takım istisnalar devreye girecektir. Bir başka deyişle, bu istisnaların varlığı halinde veri sahibinden (işçiden) açıkça onay alınmasına gerek kalmayacaktır. Bu istisnalar arasında hassas olmayan kişisel veriler bakımından Kişisel Veri Kanunu'nun Madde 5/2 hükmü uyarınca, "**İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması,"** kanunlarda açıkça öngörülmesi, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması sayılmaktadır.

Ancak bu istisnaların varlığında dahi veri işleme sırasında, Veri Koruması Kanunu Madde 4 hükmünde belirtildiği üzere, **amaçla bağlantılı olma, sınırlı ve ölçülü olma, gerektiği süre kadar muhafaza etme ile belirli açık ve meşru amaçlar için işleme** ilkelerine her zaman uyulması gerektiği unutulmamalıdır.

Örneğin sadece e-maillerin incelenmesini gerektiren bir ihbar var ise, bu e-maillerin arşivlerden incelenmesi için bir çalışma yapılması mümkündür, dolayısıyla daha da ileriye giderek **çalışanın** bilgisayarının imajının alınarak dosyalarına bakılmasına ihtiyaç bulunmamaktadır. Diğer bir ifadeyle, gerekli olmadığı halde detaylı bir inceleme yapılması **ölçülülük ilkesine aykırılık** teşkil edecektir. Benzer şekilde uygulamada çoğu zaman e-maillerin avukat veya danışman gibi üçüncü taraf konumundaki kişiler tarafından incelendiği görülmektedir. Bu halde, söz konusu e-mailler iç soruşturmanın kapatılması akabinde üçüncü taraf hizmet sağlayıcılar tarafından imha edilmelidir, zira veri koruması hukukunda gerektiği süre kadar muhafaza etme ilkesi geçerlidir.

Yukarıda açıklandığı gibi, TBK'nın kişisel verilerin kullanılmasına ilişkin TBK'nın 419. maddesinde yer alan, "**İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir hükmünün geniş uygulanması sonucunda çalışanın** e-mail yazışmalarının incelenmesi, "kanunda açıkça öngörülmesi" istisnası altında değerlendirilebilecektir.

ŞİRKET SORUŞTURMASINA PARALEL VEYA BU SORUŞTURMA ÖNCESİNDE VEYA SONRASINDA, SAVCININ DA KENDİ SORUŞTURMASINI YÜRÜTMESİ İHTİMAL DAHİLİNDEDİR.



Bunun yanı sıra şirket içinde yapılan soruşturmalar şirketin meşru menfaatleri çerçevesinde değerlendirilebilir, zira bu inceleme sayesinde **şirkette oluşacak telafisi mümkün olmayan zararların önüne geçilmeye çalışılacaktır.** Burada Kişisel Veri Kanunu'nun Madde 5/2'deki, "*ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla*" cümlesi önem kazanmaktadır, zira her bir olay için bu değerlendirmenin ayrı ayrı yapılması gerekmektedir.

Bununla birlikte son olarak **iş sözleşmesinin ifası kapsamında iç soruşturmada verilerin elde edilmesi halinde açık rıza alınmaksızın verilerin işlenebileceği düşünülebilir. Ancak bu istisnada önemli olan "doğrudan sözleşmenin ifasıyla ilgili olması**"dır. Bu hususun Veri Koruması Kanunu'nda **öngörülen,** Kişisel Verilerin Korunması Kurulu oluştuktan sonra daha da netleşeceği beklenmektedir.

AVRUPA BİRLİĞİ'NDE BENİMSENEN KRİTERLER

Yukarıdaki açıklamalar ile birlikte yeni mevzuatımıza giren Kişisel Veri Kanunu'nun nasıl uygulanacağına ilişkin henüz çıkarılan bir yönetmelik veya kılavuz olmaması nedeniyle, veri koruması alanında çok uzun bir geçmişe sahip olan Avrupa Birliği uygulamalarının da dikkate alınmasında fayda bulunmaktadır.

Avrupa Birliği uygulamalarına bakıldığında iç soruşturma sürecinde e-maillerin incelenmesine ilişkin **şeffaflığın benimsenmesi, meşru bir sebebin varlığı**, verilerin güvenliğinin sağlanması, işlenen verilere ilişkin veri sahiplerinin taleplerinin hukuka uygun şekilde **yönetilmesi** sayılmaktadır. Bu ilkelerin benimsenmesi ile hukuka uygun bir e-mail inceleme sürecinin yapıldığı söylenebilecektir.

CEZA HUKUKU BAKIMINDAN DEĞERLENDİRMELER

İç soruşturma sürecinde çalışanların kurumsal e-maillerinin ve diğer aygıtlarının hukuka uygun şekilde incelenmesi, ceza soruşturmaları **aşamasında da ayrı bir öneme sahip olmaktadır. Zira tüm bu incelemeler sonucunda elde edilen veri ve belgeler, soruşturma aşamasında delil niteliğini haiz olacaktır**. Ancak hukuka uygun olmayan delillerin değerlendirilmesi mümkün olmadığın-

ŞİRKETLERE TAVSİYELER

Bu yazıda yapılan **açıklamalar ışığında iç soruşturma sürecinde e-mail incelemelerinin yapılmasının neden birçok tereddüde** yol açtığı aslında açıktır. Dikkate alınması gereken birçok hukuki disiplin bulunmaktadır. Etik ve uyumluluğun tamamıyla yerleşmesine yönelik bu uzun yolculukta, özellikle e-mail incelemeleri konusunda şirketlere aşağıdaki yol haritasının izlenmesi tavsiye edilebilir:

- Veri koruma politikalarının işveren ve **çalışan** tarafından benimsenmesi; bunların zaman zaman gözden geçirilmesi,
- **İş sözleşmelerine** ve şirket iç yönetmeliklerine e-maillerin denetlenmesine ilişkin açık hükümler eklenmesi ve/veya **çalışandan** açık onay alınması,
- E-maillerin hukuka uygun, meşru amaçlarla, ölçülü şekilde incelenmesi ve bu sürecin güvenliliğinin sağlanması; **üçüncü taraf konumundaki danışmanlar ile çalışılıyorsa mutlaka bu kişilerle bir gizlilik sözleşmesi imzalanması,**
- **İç soruşturma sonrası e-maillerden elde edilen b**ulguların yargısal aşamalarda dikkate alınabilmesinin sağlanması, bu amaçla delillerin hukuka uygun şekilde toplanması.

Tüm bu hususların teker teker dikkate alınmasıyla birlikte, hukuka uygun bir inceleme süreci gerçekleştirilebilecek ve olası ihtilaflara karşı önlemler alınmış olacaktır.

dan, soruşturmaların yukarıda açıklanan şekillerde -Kişisel Veri Kanunu'na uygun şekilde- **yürütülmesi daha da önem kazanmaktadır. Buna ek olarak, ilgili çalışanın kurumsal bilgisayarı/aygıtı verdiğine ilişkin tutanağın bulunması, tüm hukuki sürecin bir avukat ile yürütülmesi ve bu şekilde ilgili kişinin anayasal haklarına ve özellikle özel hayatın gizliliğine zarar verilmemesi hukuka uygun delillerin toplanılması bakımından atlanmaması gereken noktalardır. Bu süreç öncesinde kişinin açık rızasının alınmış olması en sağlıklı ve güvenli yöntem olacaktır.**

İç soruşturma sırasında bilgisayardan veri toplanılmasına karar verilirse bu sürecin çok hassas olduğu ve profesyonel bir ekip tarafından yürütülmesi gerektiği bilinmelidir. Bilgisayar, eğer bir ağa bağlı ise, bu ağdan ayrılmalı ve güvenli bir bölgeye götürülerek muhafaza altına alınmalıdır. Veriler düzgün bir şekilde kopyalanarak, kopyalanan verilerin hash değeri (1) alınmalıdır. Böylelikle veriler zaman damgasıyla damgalanmış olacaktır. Hash değerinin ilgili çalışan huzurunda alınması veya bu mümkün değilse zaman damgası da olduğundan alınan hash değerinin ilgili kişiye iletilmesi şirketi ve ilgili kişiyi koruyacak bir adımdır. Tüm bu sürecin her adımının dokümante edilmesi ve tutanak tutulması tavsiye edilir.

Uygulamada şirketlerin iç soruşturmalarını yürüttükten sonra her zaman durumu yargıya intikal ettirmediklerini görüyoruz. Bu tecrübemiz ACFE 2016 Çalışan Suistimalleri ve İstismar Raporu'ndaki bulgular ile de teyit edilmiştir; örneğin şirketlerin %40.7'si ağırlıklı olarak repütasyonlarının etkilenmesinden korktuğu için yolsuzluğu yargı organlarına intikal ettirmemiştir. Ancak uygulamada, yargıya teslim edilmeyerek üstü örtülen usulsüzlüklerin ileride daha ciddi sorunlara yol açtığı görülmektedir.

Şirket soruşturmasına paralel veya bu soruşturma öncesinde veya sonrasında savcının da kendi soruşturmasını yürütmesi ihtimal dahilindedir. Bu süreçte savcılık makamı, diğer birçok aracın yanı sıra, şüpheli veya ilgili kişilerin e-maillerine ulaşmak ve bunları incelemek isteyebilir. Ceza Muhakemesi Kanunu'nun 134. maddesinde (*Bilgisayarlarda Arama ve El Koyma*), bilgisayarda önce yerince inceleme (arama) yapılması, bu şekilde delil elde edilmesi mümkün olmazsa, (*bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde*) bilgisayarlara el konulması öngörülmektedir. El konulan bilgisayarın (veya daha doğru bir ifadeyle *harddisk*'in) kopyası alınıp, orijinali derhal sahibine iade edilmelidir. Burada sadece "bilgisayar" dendiğine bakılmamalı, uygulamada her türlü elektronik araç üzerinde bu tedbir uygulanmaktadır. Ayrıca Adli ve Önleme Aramaları Yönetmeliği'nde de cloud gibi, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da bu hükmün uygulanması mümkündür. Soruşturmada her türlü delil elde etme yönteminin uygulanması, ancak artık başka surette delil elde etme imkanının bulunmaması gerekmektedir. Bir başka deyişle, bilgisayarlarda arama ve el koyma işleminin yapılması delil elde etme açısından son çare olmalıdır. Ne var ki uygulamada bu şart genelde atlanmakta ve bu konuda çok fazla hak ihlali olmaktadır. ✔

İÇ SORUŞTURMA SIRASINDA BİLGİSAYARDAN VERİ TOPLANILMASINA KARAR VERİLİRSE, BU SÜRECİN ÇOK HASSAS OLDUĞU VE PROFESYONEL BİR EKİP TARAFINDAN YÜRÜTÜLMESİ GEREKTİĞİ BİLİNMELİDİR.

Dipnotlar

(1) *Hash değeri: Dosyaların parmak izi de denilen ve dosya üzerinde en küçük bir değişiklik yapıldığında baştan sona değişen, dolayısıyla yedeklenen verilerin bütünlüğünü teminat almaya yarayan sayısal değerlerdir.*