

İŞLETMELERDE E-MAİL KULLANIMININ KİŞİSEL ÖZGÜRLÜKLER AÇISINDAN DEĞERLENDİRİLMESİ

Yard.Doç.Dr. Figen Dalyan
Anadolu Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
İşletme Bölümü
Yönetim ve Organizasyon Anabilim Dalı
fdalyan@anadolu.edu.tr

ÖZET

Çalışanların e-mail mesajları nasıl kişiseldir? Cevap açık değildir. Açık olmaması, çalışanlarının e-mail mesajlarının korunması gelecek yüzyılda da öncelikle tartışılan konuların başında gelmesine neden olacak gibi görünmektedir. Kişiselliği ve kişisel özgürlükleri koruma yeni bir konu değildir ve çalışanların özeli; alkol testi, çalışanlarla ve yaptığı işle ilgili araştırmalar yapmak, psikolojik testler, telefon, bilgisayar ve elektronik gözlemeleme ve diğer çalışanlara haber vermeksizin denetleme biçimleri gibi konuları içermektedir.

Bu alanların tartışmaya açık olma özelliği, işverenler, yöneticiler ve çalışanlar olduğu kadar onların etkileşim halinde olduğu danışmanlar, bilgi hizmet ve destek personeli, tedarikçiler ve müşterilerin kişisellekle ilgili beklentilerinin karşılanmasını talep etmelerinden kaynaklanmaktadır. Kullanıcılar ve organizasyonlar etik yönetimle ilgili hala deneyimsizdir ve e-mailin kişiye özel olmasıyla ilgili yasal düzenlemeler, zorla içeriğine ulaşılabilmesi nedeniyle zedelenebilmektedir. Bu çalışma, e-maile iletişimde kişisel özgürlüğe saldırının yasal ve etik yönlerini işverenler ve çalışanlar açısından inceleyerek, potansiyel sorunları ortaya koymaktadır. Aynı zamanda ABD ve Türkiye'nin yasal sistemi incelenerek, e-mailin kişiselliğini korumadaki uygulamaları irdelenmektedir.

Anahtar Kelimeler: E-mail, kişisel özgürlük, etik, yasalar

ABSTRACT

How private are employees' e-mail messages? The answer is unclear. This lack of clarity means that protection of employee e-mail will be at the forefront of legal controversy for at least the rest of the decade. Privacy protection is not a new issue, and employee privacy encompasses a spectrum of issues, including: Drug testing, searches of employees and their work areas, psychological testing, telephone, computer and electronic monitoring and other types of employee surveillance.

The controversial nature of these areas demands that employers and employees, as well as those with whom they interact (consultants, information service support personnel, suppliers and customers) be aware of and responsive to, expectations of and concerns about privacy. Users and organizations naive about ethical conduct by intrusions. This article examines the potentially conflicting expectations of employers and employees regarding the ethical and legal aspects of privacy invasions in e-mail communications. It also examines the U.S. and Turkish legal system to determine sources in protecting e-mail privacy.

Keywords: E-mail, privacy, ethics, legal system

1. GİRİŞ

Elektronik iletişim kaynakları ve cihazlarındaki çoğalma ile birlikte, birbirini etkileyen ve tetikleyen bu modayla ilgili etik standartlar her geçen gün daha fazla üzerinde durulan bir konu haline gelmiştir. Pek çok organizasyon bugün ilgili faaliyetlerde bir iletişim yolu olarak çalışanlara e-mail olanağı sağlamaktadır. Elektronik posta gönderme ve alma bugün belki de en çok kullanılan İnternet teknolojisidir. ABD'de yapılan bir

araştırmaya göre her gün 130 milyon çalışan 2.8 milyar elektronik posta göndermekte ve almaktadır (Wakefield, 2004: 52). İşyerlerinde elektronik posta kullanımı iki şekilde olabilir; ya her çalışanın kendine ait elektronik posta adresleri vardır ya da işyerinin aldığı uzantıyla işverenin çalışanlarına verdiği elektronik posta adresleri vardır. E-mail aynı organizasyonda gönderilip alınabildiği gibi, işletme dışından da (müşteriler, tedarikçiler, çeşitli düzenleyici kurumlar gibi) olabilir.

İlk bakışta, rutin e-maillere uygulanabilecek etik standartların, bu yeni yapıda uygulanma gerekliliği, doğal bir sonuç gibi görünmektedir. Eğer bir bireyin mailini okumak, etiğe uygun değilse, benzer şekilde bir işverenin ya da yöneticinin çalışanların e-mailini okuması da yanlış olacaktır (Greenwald, 2004: 2). Eğer bir çalışana bilgisi dışında okunmaması için belgelerini bir dolaba kilitlemesine izin veriliyorsa, bilgisayardaki dosyalarda benzer şekilde korunmalıdır. Bugün pek çok işletme, kurumun Internet olanaklarını kişisel mektupları için kullanan çalışanlara tepki göstermektedir, benzer şekilde Internet de arkadaşlarla iletişim ya da Net'te sörf için değil, sadece işletmenin amaçları için kullanılmaktadır.

Ancak belgelerle, elektronik dokümanlar arasında önemli farklılıklar vardır. İyi bir bilgisayar uzmanından yardım alarak, çalışanların bilgisayardaki dosyalarına ulaşımı denetim altına almak, hiç te zor değildir. Hatta bu, çalışanların haberi olmadan da gerçekleştirilebilir. Dosyaların dolaplara kilitletlenmesinin aksine, bu yöntemde çalışanlardan anahtar istemek de gerekli değildir. Çalışanlar doğal olarak şaşıracaktır ve patronlarının e-maillerini okuyabildiğini keşfettiklerinde dehşete düşeceklerdir.

2. BİLGİSAYAR SUÇLARINA İLİŞKİN BAZI TABLOLAR VE İSTATİSTİKLER

Aşağıdaki bazı tablo ve istatistikler bilgisayar suçlarının ciddiyeti konusunda önemli ip uçları vermektedir:

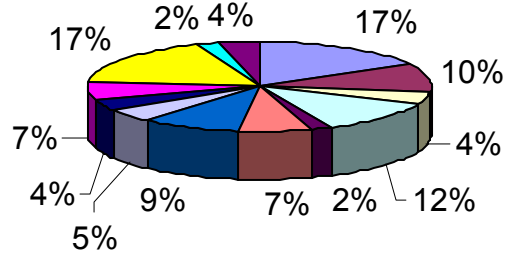
Tablo 1: ABD'de Bilgisayar Suçlarından Doğan Ekonomik Kayıplar

Suç Tipleri	Ne kadar para kayboldu?			
	Yıllık Kayıplar			
Bilgi Hırsızlığı	1997	1998	1999	2000
	20,048,000 \$	33,545,000 \$	42,496,000 \$	66,708,000 \$
Sabotaj	4,285,850 \$	2,142,000	4,421,000 \$	27,148,000 \$
Telekom Dinlemeleri	1,181,000 \$	562,000 \$	765,000 \$	991,200 \$
Dışarıdakilerin Sisteme Girişleri	2,911,700 \$	1,637,000 \$	2,885,000 \$	7,104,000 \$
İçeridekilerin Internet Erişimini Suiistimal Etmeleri	1,006,750\$	3,720,000 \$	7,576,000 \$	27,984,740 \$
Dolandırıcılık	24,982,000 \$	11,239,000 \$	39,706,000 \$	55,996,000 \$
Servisin Yok Sayılması	-	2,787,000 \$	3,255,000 \$	8,247,000 \$
Spoofing	512,000 \$	-	-	-
Virüs	12,498,150 \$	7,874,000 \$	5,274,000 \$	29,171,700
İçeridekilerin Yetkisiz Girişleri	3,991,605 \$	50,565,000 \$	3,567,000 \$	22,554,500 \$
Telekom Dolandırıcılığı	22,660,300 \$	17,256,000 \$	773,000 \$	4,028,000 \$
Aktif Hat Dinlemeleri	-	245,000 \$	20,000 \$	5,000,000 \$
Laptop Hırsızlığı	6,132,200 \$	5,250,000 \$	13,038,000 \$	10,404,300 \$
Toplam Yıllık Kayıplar	100,119,555	136,822,000 \$	123,779,000 \$	265,568,240 \$
Toplam Kayıp	626,306,795 \$			

Kaynak: http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm

Tabloda görüldüğü gibi bilgi hırsızlığı nedeniyle katlanılan zarar ve kayıplar en büyük miktarı oluşturmaktadır. Bunu dolandırıcılık izlemektedir. Ancak çalışmanın konusuyla ilgili olarak telekom dinlemeleri, içerdekilerin Internet erişimini suiistimal etmeleri, içerdekilerin yetkisiz girişleri ve aktif hat dinlemelerinin toplamı dikkate alındığında maliyet olarak bilgi hırsızlığından sonraki en büyük tutarı, 56.530.440 \$'ı bulduğu görülmektedir.

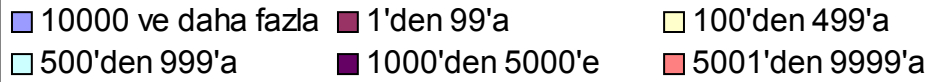
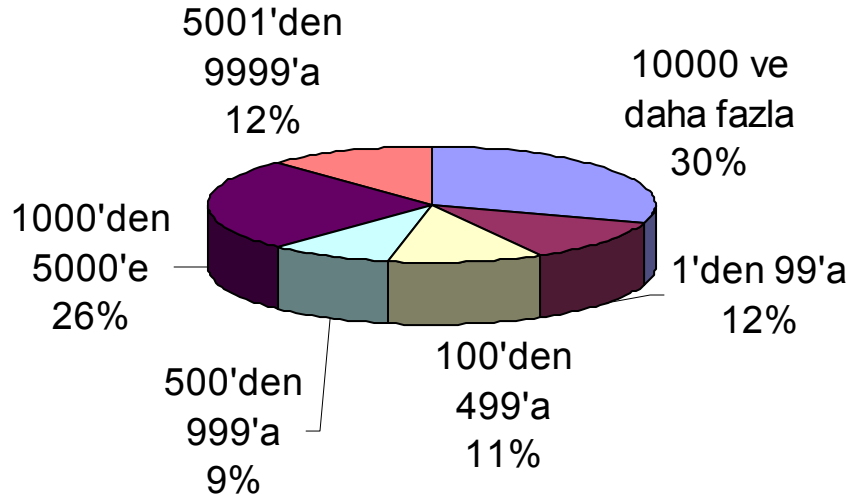
Kime Soruldu?



Şekil 1: Soruları Cevaplayan Kurumlar

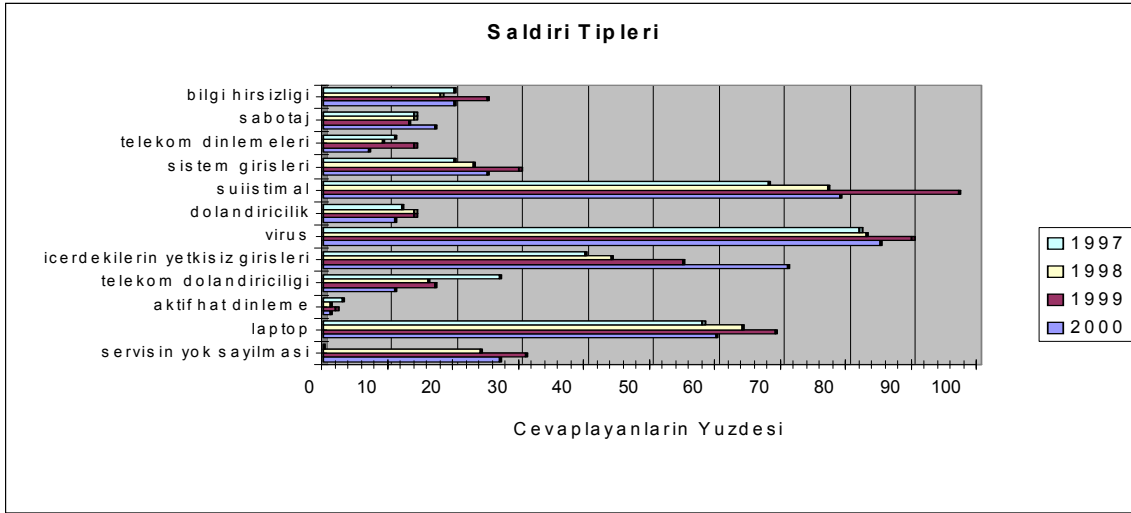
Kaynak: http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm

Cevaplayanların Çalışan Sayısı



Şekil 2: Soruları Cevaplayan Kurumların Çalışan Sayıları

Kaynak: http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm



Şekil 3: Saldırı veya Kötüye Kullanma Tipleri

Kaynak: http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm

3. E-MAIL VE ETİK

Organizasyonlar, çalışanlarına, iş ortaklarına, müşterilerine ve topluma olduğu kadar kendine de etik davranmak zorundadır. Ancak etik davranışın başarılması genellikle zordur. Buradaki öncelikli konu, bireyler ve gruplar üzerindeki mevcut ya da potansiyel olumsuz etkidir. Ne etikdir ve ne etiğe uygun değildir? Cevaplar doğru ve dürüst değildir. “iyi”, “doğru” ve “ahlak” ile ilgili sosyal standartlar, davranışlarımıza yön vermeye yardım eder ancak tüm durumlar için belirli ve kesin cevaplar vermez. Bireyler ve iş yerlerinin kişiselliği ile ilgili politik tartışmalar, etiğe ve kişisel özgürlüklere saygı ile ilgili görüşlerde bir fikir birliğinin yoksunluğunu göstermektedir. Yasalara ve mahkemelere, alkol testleri, bireylerin ve mekanların fiziksel incelemesi, haber vermeksizin gizli yapılan gözlemler ve diğer bireylerin özeliyle ilgili meselelerden kaynaklanan yasal ve etik sorunların çözümü için başvurulmaktadır (Kladko, 2004: 1). Bu çalışmada, e-mailin kişiselliğinin zedelenebilme olasılığını tanımlamak ve çalışanların ve işverenlerin, e-mail kullanımında kişisel beklentileriyle ilgili etik meseleler konusundaki farkındalığını geliştirmeye dikkat çekmek amaçlanmaktadır.

Bilgisayar kullanıcılarının, uygulamaların ve sistemlerin karşılıklı bağlılığının sayısındaki artışın yanında teknik kapasitenin üzerinde artan karmaşıklık, e-mail'in kişiye özel olmasıyla ilgili büyük değişimde uzlaşılması gerektiği anlamına gelmektedir. E-mailin kişiselliği önündeki engeller iki boyutta özetlenebilir: Engelin kaynakları ve engelin tipleri. E-maile iletişim, hem organizasyonun iç kaynakları hem de dış kaynaklar tarafından durdurulma riski altındadır. İç kaynaklar, işletmeler tarafından istihdam edilen çalışanlardır ve yöneticileri ve üst yönetimi de içerir. Dış kaynaklar, organizasyonla formal ya da informal ilişkilerle etkileşim halinde olan bireyler ya da kurumlardır (Wagstaff, 2004: 41). Formal ilişkiler, hizmet sağlayıcılar, danışmanlar, tedarikçiler ve müşterilerle ilgilidir. Karşılıklı etkileşim bazen de rakipler ve “hekırlarla” olan formallığın olmadığı ilişkilerde de ortaya çıkabilir.

Buradaki tehlike, e-mailin gözlemlenmesi uygun görülmemiş olabileceği gibi izin verilmemiş de olabilir bu, yönetici gibi bir iç yetkili, bir yasa koyucu kurum gibi bir dış yetkili tarafından göz yumulabileceği gibi, tamamen yetkisiz birinin özelinin ihlali de olabilir. Bu kombinasyonlar dört bölüm altında yapılandırılabilir (Hayes, 2004: 46). Bu çalışmada, e-mail mesajlarının kişiselliği, yetkilendirilmiş iç yasaklar açısından değerlendirilmektedir.

4. ÜST YÖNETİMİN E-MAIL'İN KİŞİSELLİĞİNE BAKIŞ AÇISI

Organizasyonlarda e-mailin gözlemlenmesi, üst yönetim tarafından bir gereklilik olduğu kadar, doğru bir hareket olarak da görülebilir. İşletme kaynaklarının sahipleri olarak işverenler, e-maillerin gözlemlenmesini doğru olarak algılayabilirler. Böylesi bir gözlem, etik açıdan doğru ya da yasal açıdan yapılabilir olarak kabul edilebilir de edilmeyebilir de. Ancak çalışanlara bu eylemi gerçekleştirmeye ilgili sunulan nedenler, etiğe uygun ve yasal görülebilir: İşletme kaynaklarını kötüye kullanma ya da kişisel kullanımı engelleme, hırsızlık ya da işletme casusluğunu araştırma ya da engelleme, araştırmada yasa koyucu kurumlarla işbirliği, teknik sorunların çözümü ya da diğer belli koşullar gibi (Precision Marketing, 2004: 17).

Buradaki gri alan, e-mailin iç gözleminin, çalışanların performansı için kullanılmasıdır. E-mail mesajları gözlenenler için, gözlem iki taraflı bir yetki olabilir. Verimli ve başarılı çalışanlar kadar verimsiz çalışanlar, işletme tarafından bu yolla tespit edilebilir (Cohan, 2000: 81). Çok çalışan bir işletme personeli, işini zamanında bitirmek ya da satış yapmada e-mail kullanabilir, eğer mektuplaşmak için kullanıyorsa, verimlilikleri ve başarıları göz ardı edilebilir. Dış çevreye gönderilen e-mail mesajlarını inceleyerek, performansı gözlemlenmede başarısız olan bir işletme, ticari bilgileri ve hissedarlarla ilgili bilgileri korumada da başarısız olabilir.

Bu örneklerde olumlu sonuçlar elde etmek için, çalışanlar tarafında gönderilen ve alınan tüm mesajlar incelenecektir. Bazıları bunu çalışanların kişisel özgürlüğüne saygısızlık ya da etik olmayan bir davranış olarak değerlendirebilir. İşverenlere ve yöneticilere göre çalışanların kendilerine saklama eğiliminde oldukları bilgi incelenmelidir. Ancak bir işveren, eğer bir e-mail sistemi bir işverene ait ise ve işverenin ve işletmenin amaçları için kullanılması gerektiğini, çalışanların kendi özel amaçları için kullanmasının beklenemeyeceğini belirtmektedir (Boutin ve Udell, 2004: 42). Bu nedenle işverenlere ve yöneticilere göre e-mailin gözlenmesi etiğe uygundur, çünkü çalışanların işverenin e-mail sistemine saygı gösterildiğinde zaten kendi özeliyle ilgili beklentileri için bir neden olmayacaktır.

5. KİŞİSEL ÖZGÜRLÜKLER AÇISINDAN ÇALIŞANLARIN E-MAIL'E BAKIŞI

E-mail mesajlarıyla ilgili çalışanların görüşü, mahrem, gönderen ve alan arasında olan, cevapların kişiye özel olduğu biçimindedir. Bu görüşten hareketle hemen hemen her çalışan e-mail hesabına bir şifre koyarak güvenilirlik sağlamaya çalışmaktadır. değerlendirme mantıklı görünmektedir, e-mail bir şifre koyarak denetim altına alınabilir böylece güvenilir

İş performansını, ürün kalitesini ve verimliliği geliştirmek amacıyla uygulanan elektronik gözleme, pek çok farklı biçimde gerçekleştirilebilir. Örneğin, e-mail mesajları genellikle doğrudan okunaklı yaygın alfabetik biçimde, hemen okunabilmesi amacıyla gönderilir ve alınır. Çalışanların bilgisayarlarını ya da mesajlarını koruması, çalışanların bilgisi ya da rızası dışında engellenebilir ya da görülebilir, e-mail mesajları, üst yönetim tarafından incelenebilir. Pek çok kullanıcı, bilgisayarlarındaki "delete" tuşuna bastığında, bir e-mail mesajının gerçekten silinmesini beklemektedir. Ancak kullanıcının mesajı silmesi sıklıkla klavyede gerçekleşmekte, e-mail mesajları yıllarca saklanabilmektedir. 1990'lı yılların başında peş peşe pek çok ABD işletmesinin e-mail sistem yöneticilerini protesto edilmesine, çalışanların e-maillerinin rutin denetimi ve yazıldığı açıklamalarına şahit olmuştur. Kamuoyuna yansıyan bu uygulamalarda, işletmelerin e-mail sistemlerini yönetme hakkı, yasal anlamda incelenmeye başlamıştır ve ülke genelinde şu soru tartışılmaya başlamıştır "işletmelerin bu uygulamaları etiğe uygun mudur?" (Leizerov, 2004: 59)

Hangi tip ve özellikteki e-mail sistemi kullanılırsa kullanılsın buradaki önemli soru şudur: Eğer bir çalışan iletişim aracı olarak kullandığı bir e-mail hesabına sahipse, kişisel ya da kişiye özel olan nedir ve nasıl korunmalıdır? E-mail yoluyla iletişim bugün çalışanların tanıtımında ya da çalışanlara yaptıkları işle ilgili emirleri iletmede, çalışanların kullandığı araç-gereç ve ekipmanlarla ilgili bilgilendirmelerde, çalışanların çalışma zamanlarıyla ilgili bilgilendirmelerde ve hatta çalışanlara işletme amaçlarıyla ilgili hatırlatmalarda kullanılmaktadır. Bunun yanında e-mail mesajları çalışanların işverenlerin emirlerine uyup uymadıkları, araç-gereç ve ekipmanları standartlara uygun kullanıp kullanmadıklarını, çalışma saatlerine uyulup uyulmadığını ve buna bağlı olarak maaş ve yan ödemelerin belirlenmesinde ve hatta çalışanların işletme amaçlarına göre faaliyet gösterip göstermediğini tespit etmede, kısaca çalışanları tanımda kullanılabilir (Cappel, 1995: 821). Böylesi önemli ve maliyetli bir yatırım ile, çalışanlar e-mailin kişiselliği konusunda yasal beklentilere sahip midir?

İşverenlerin önemli ve özel çıkarlarına karşılık çalışanlar "kişisellik" ilgili haklara sahip midir? Kişiselliğe saldırı ya da kişiye özel olanın işgali ile sonuçlanabilen, e-mailin kişiselliğini işverenlerle çalışanların farklı algılamaları göz önüne alındığında, öncelikle bu konudaki yasal düzenlemelerin gerçekleştirilmesi ve hem işverenlerin hem de çalışanların kişiye özeli korumanın önemini anlamalarının gerekliliği ortadadır (Greenwald, 2004: 2) Etik değerler ve yasalar aynı olmamasına rağmen aralarında çok yakın bir ilişki vardır. Yasalar, resmi uygulamalar için bir araçtır, etik ise sosyal bir rehber ve prosedürdür.

6. ELEKTRONİK İLETİŞİMDE KİŞİSELLİĞİ GÖZETEN UYGULAMALAR

The Congressional Office of Teknological Assessment (OTA) 1985'de yaptığı bir araştırmada ABD nüfusunun %50'si, bilgisayarların kişisel hakları tehdit ettiğine ve bu hakların korunması için daha fazla şeylerin yapılması gerektiğine inandıklarını tespit etmiştir. Bu çalışma Elektronik İletişim Kişiselliğini Koruma (Electronic Communications Privacy Act (ECPA)'nın 1986'da kanunlaşmasında referans olmuştur (Sipior ve Ward, 1998: 629). Amerika gibi gelişmiş ülkelerde kişiselliğe değer verilmektedir. Kişinin özeli gibi sosyal bir değer eğer yasalarla korunmuyorsa, bu bir hak mıdır? Bugün ABD'de çalışanlar bu haklarının yasalarla

korunduğunu bilmektedirler ve bu hakka malikdirler. OTA'nın tespitlerine göre e-mail'e saygı anlamında "mevcut koruma faaliyetleri zayıftır, belirsizdir ya da mevcut değildir. Bu korumadan yoksunluk önemlidir çünkü, e-mail gözlemlenmeye, izinsiz incelenmeye ve hiçbir iz bırakmadan takip edilmeye müsaittir. OTA'ya göre "e-mailin kişiselliği" beş biçimde ihlal edilebilmektedir (Sipior ve Ward, 1995: 37):

- Gönderilen kişinin terminal ya da elektronik hesabından
- Bir başkasına nakledeken
- Alıcının mail kutusuna girdiğinde
- Mesaj yazıcıdan yazdırıldığında ve
- E-mail hizmeti veren sistem ya da kuruluşun hesabında tutulduğunda ya da saklandığında

OTA'nın 1985'de yaptığı bu çalışmada, işletmelerin kendi e-mail sistemlerinin yasalarla denetlenip korunamayacağı sonucuna varmıştır. Kongre ECPA'nın kararını, elektronik iletişimde gizli dinlemeleri ve gözlemlere karşı korumaya yönelik mevcut federal yasada değişiklikler yapmada kullanmıştır. Buradaki amaç, e-mail, cep telefonu ve veri gönderme gibi yeni elektronik iletişim biçimlerinde uygun olmayan engellemeler ya da gizli dinlemelere karşı kişiselliği ve kişiye özel olanı koruma yönünde genişletmek olmuştur (Halpert, 1998: 625)..

Geniş bir şekilde ECPA telgraf, telefon ve elektronik iletişimin durdurulması yanında açma ya da ifşa etme ya da iletişimi sınırlayıcı yönde kullanmayı yasaklamıştır. Ve ilk defa elektronik iletişimin tanımı genişletilerek, e-mail'de tanım içine sokulmuştur. Hatta ECPA'nın 2. maddesinde, elektronik iletişimdeki mesajların ifşa edilmesini ve ulaşılmaya çalışılmasını, önemli istisnalar dışında yasak getirilmiştir. Özel sektördeki işverenlerin ve yöneticilerin e-mailleri takip etmesini kapsayıp kapsamadığı, gizli gözlemlemeyi önlemeye yönelik önceki federal yasanın bir parçası da olan ECPA'nın iki istisnası nedeniyle açık değildir. Bu istisnalar ise şunlardır (Sipior ve Ward, 1998: 630):

İşletmede Kullanımı Ya Da İşletmeleri Kapsaması: Bu istisna ECPA'nın ortaya koyduğu pek çok örneğin temelidir. Çalışanların e-mailinin kişiselliğine saldırılara yönelik taleplerini etkin bir şekilde karşılamak için işverenler, elektronik iletişimi sınırlama ve haber vermeden gözlemlemenin nedenini, işletmenin rutin yönetiminin bir parçası olduğunu göstermek zorundadır. 1983'de tespit edilen bir olayda bir çalışan, patronunun satıcılarla yaptığı telefon görüşmelerini dinlediğini ve bazılarını engellediğini fark etmiştir. Mahkemeye yansıyan bu olaya, iletişime getirilen belli sınırlama ve gözlemlerin, işletmelerin rutin faaliyetlerinin bir gereği olduğu yorumu getirilmiştir. Bir işletmenin amacı ise, telefonla iletişim kişisel olduğunda sona erer. Telefonla iletişim için söz konusu olan bu istisna, e-maile de uygulanabilir. Eğer bir işveren ya da yönetici, işletmesindeki e-mail sisteminin büyük oranda işle ilgili kullanıldığını emin olmak istiyorsa, e-mail mesajlarının içeriğinin rutin bir şekilde gözlemlenmesi bu istisnayı kapsayabilir.

Önceden Rıza Gösterme Ve Uygun Bulma: Bu istisna telefon ve e-mail mesajlarının gözlemlenmesine izin vermektedir. Buna göre işveren, çalışanlarına e-maillerinin incelenebileceğini bildirerek, çeşitli olası risklere karşı kendi sorumluluğunu koruyabilir. Böylesi bir rıza gösterme ya da uygun bulma benimsenebilir ya da uygulanabilir ancak gözleme getirilen bu rıza sınırlandırılmıştır. Daha önce de değinilen 1983'deki olayda, rıza gösterme ya da uygun bulma sadece işle ilgili aramaların gözlemlenmesiyle sınırlandırılmıştır. Mahkeme uygun bulmanın genişletilerek çalışanların tüm telefon görüşmelerini kapsamasını reddetmiştir.

ECPA'nın e-mail'in kişiselliğini koruma konusundaki tespitleri açık değildir ve hala da üzerinde tartışılan bir konudur. Ve son yıllarda yapılan gerek yasal ve gerekse bilimsel araştırmalar, ECPA'nın çalışanların e-mailleri iletişimlerinde kişiselliklerini korumaya yönelik ciddi çaba harcamadığını göstermektedir (Verton, 2004: 1).

7. TÜRKİYE'DEKİ DURUM

İş Kanunu'nun 9. maddesine göre belirli süreli iş akidleri bir yıl veya daha fazla süre için yapılmışsa bunların yazılı olması zorunludur. Bu sözleşmelerde genellikle, işin ne olduğu, nasıl ifa edileceği, ücret, çalışma saatleri vs. gibi birçok hususun yanında bir de "gizlilik" başlıklı bir madde bulunur. Bu maddede genel olarak işçinin işiyle ve işyeri ile ilgili olarak elde ettiği bilgileri sözlü veya yazılı olarak, basın-yayın araçları, mektup, röportaj, İnternet vs. gibi yollarla açıklaması yasaklanır. Bu şarta uyulmaması halinde bu durumun işveren açısından haklı fesih sebebi olacağı ve işverenin bu durumdan bir zararı olmuşsa bunun işçi tarafından tazmin edileceği düzenlenmektedir.

Bugün Türkiye'de de birçok orta ölçekli ve büyük işyerlerinde bilgisayar kullanımı yaygınlaşmıştır. Özellikle de birçok işyerinin İnternet bağlantısının olması çalışanların bilişim teknolojilerinden faydalanmalarını mümkün kılmıştır. Bu durum beraberinde bazı yasal problemleri de getirmektedir. Bu problemlerden bugün en çok tartışılan işverenin çalışanın e-mail trafiğini izleyip izleyemeyeceği yani çalışanın kişisel bilgilerinin gizliliğinin korunması problemidir. Bunun dışında yasal olmayan "downloadlar" sebebiyle işverenin karşı karşıya kalabileceği telif haklarına ve marka haklarına tecavüz iddiaları, işyeri bilgisayarlarının konusu suç teşkil

eden eylemlerde kullanılması gibi problemler de ortaya çıkmakta ve tartışılmaktadır. Bu konu daha çok “gizlilik” başlıklı madde içinde değerlendirilmektedir.

Bir çalışanın kullanmakla, hizmet akdindeki gizlilik maddesini ihlal edebileceği teknolojiler öncelikle şunlar olabilir:

- Elektronik posta alma ve gönderme
- Eş zamanlı sohbet programları (IRC,ICQ, Net Meeting gibi)
- USENET, Haber Gruplarına ve Posta Listelerine üye olma.
- Çeşitli web sitelerindeki forumlara yazma.

- Truva atı, casus programlar, keyword logger’lar gibi bilgi sızdırmaya yarayabilecek programları yüklemek veya yüklenmesine sebep olmak.

Bu sınıflamada en yaygın olarak kullanılan ve tartışılan çalışanın e-mail göndermesi ve almasıdır.

Eğer işveren ile işçi arasında bir hizmet akdi varsa ve bu akitte gizlilik maddesi varsa işçi buna uymakla yükümlüdür. Burada bu maddenin işçi tarafından ihlal edilip edilmediği hangi kriterlere göre tespit edilmelidir? Bu soruyu cevaplamak için öncelikle bakılacak husus sözleşmedir. Sözleşmede hangi durumların gizlilik maddesini ihlal edeceği açıkça belirlenmiş olabilir. Bunlara örnek olarak şu durumlar verilebilir (Özdilek, 2003: 2):

- İşyerinin imajını ve ismini zedeleyebilecek bilgilerin elektronik posta yoluyla üçüncü şahıslara aktarılması.

- İşyeri ve işçi verimliliği hakkındaki bilgilerin aktarılması.

- İşyerinin ticari sırlarının ve diğer gizli bilgilerinin açıklanması (örneğin alınan bir know-how’un açıklanması)

Bunlar ve bunlara benzeyen durumlar sözleşmede açıkça öngörülmüşse sözleşme hükümleri uygulanacak ve bu durum işveren için haklı bir fesih sebebi oluşturacaktır. Eğer sözleşmede bir açıklık yoksa ve sözleşmenin yorumu yoluyla da bir sonuca varılamıyorsa İş Kanunu hükümlerine bakılacaktır. İş Kanunu’nda hizmet akitlerinde gizlilik maddesine ilişkin açık bir hüküm yoktur. Fakat kanunun 17/II/d maddesinde şöyle bir ifade bulunmaktadır :

“ İşçinin, işverenin güvenini kötüye kullanmak, hırsızlık yapmak, işverenin meslek sırlarını ortaya atmak gibi doğruluk ve bağlılığa uymayan davranışlarda bulunması, ”

Buradaki *“işverenin meslek sırlarını ortaya atmak”* ibaresi böyle bir problemin çözümünde yardımcı olabilir. Kanunun 17. maddesi işveren açısından haklı fesih sebeplerini düzenlemektedir. İşçinin *“işverenin meslek sırlarını ortaya atması”* ahlak ve iyi niyet kurallarına uymayan davranışlardan biri olarak düzenlenmiştir. Eğer çalışanın gönderdiği elektronik posta yoluyla işverenin işine ilişkin olarak sır niteliğindeki bir bilgi üçüncü bir kişiye aktarılmışsa kanunun 17. maddesinin II/d maddesi uygulanabilecektir. Bu uygulama mutlak mı olmalıdır bazı sınırlayıcı kriterler getirilebilir mi? Her somut olayın şartlarına göre değişmekle birlikte burada şu kriterler sınırlayıcı olarak ortaya konulabilir (Özdilek, 2003: 3):

- Açıklanan bilgi sebebiyle işverenin zarar uğramış olması veya zarara uğrama ihtimalinin güçlü olması.

- Bilginin açıklandığı kişinin ticari rakip olması.

- Bilginin açıklandığı kişi ticari rakip olmamakla birlikte bu bilgiyi geniş kitlelere ve özellikle o sektöre yayabilecek kişilerden olması ve bu açıklama sebebiyle işverenin zarara uğraması veya uğrayabilme ihtimalinin bulunması.

E-mail ile “gizlilik” maddesinin ihlal edilip edilmediğini tespit etmenin çeşitli yolları olabilir. Bilginin açıklandığı kişinin bir açıklamasıyla, basın-yayın yoluyla veya herhangi bir şekilde duyumla bu durum öğrenilebilir. İşveren ayrıca çalışanlarının elektronik posta trafiğini izleyen yazılımlar kullanarak da bu durumu tespit edebilir. Bugün piyasada bu tür izlemeye imkan veren çok sayıda program bulunmaktadır. Bu programlarla işveren çalışanın elektronik postaları hakkında şunları öğrenebilir (Özdilek, 2003: 5):

- Elektronik postanın alıcısı
- Elektronik postanın göndericisi
- Elektronik postadaki kelime sayısı
- Çalışanın elektronik postayı okumak için harcadığı zamanı
- Çalışanın elektronik posta yazmak için harcadığı zamanı
- Elektronik posta eklerinin sayısını ve türünü
- Elektronik postanın işle bağlantılı olup olmadığını
- Bazı anahtar kelimelere göre içeriğin tespiti

İşveren böyle bir programla çalışanın gizlilik maddesini ihlal ettiğini tespit eder ve buna dayanarak çalışanın hizmet akdini feshederse bu fesih kişisel bilgilerin gizliliği ilkesi karşısında geçerli olacak mıdır? İşçi haksız fesih nedeniyle ihbar ve kıdem tazminatları talebinde bulunursa, mahkemede kişisel bilgilerin gizliliğinin ihlal edilmesinin haklı fesih sebebi oluşturmadığını ileri sürebilecek midir? Bu soru bugün çok tartışılan bir

konudur. Mesele Türkiye'deki yasalar açısından ele alındığında öncelikle Anayasa'nın kişisel bilgilerin korunmasını garanti ettiği görülmektedir. Anayasa'nın 20. maddesine göre :

“Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Adli soruşturma ve kovuşturmanın gerektirdiği istisnalar saklıdır.

Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hakim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça, kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz.”

Konuyu doğrudan ilgilendiren Anayasa'nın 22. maddesinde ise:

“Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.

Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hakim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.”

Görüldüğü gibi haberleşmenin gizliliği mutlak bir hak olarak tanınmıştır. Ancak hakim kararıyla haberleşmenin gizliliğine dokunulabilir. Bazı kamu kurum ve kuruluşlarında ise istisnaların olabileceği belirtilmiştir. Anayasanın bu düzenlemesi karşısında hizmet akidlerine konulan gizlilik maddesinin ne anlam ifade edeceği düşünülebilir. İşveren hiçbir şekilde haberleşme gizliliğine dokunamayacağına göre çalışanların elektronik posta yoluyla işverene ve işletmeye ait sırlarını açıklaması durumunda işveren bu maddeye dayanarak hizmet akidini feshedemeyecek midir?

Burada hukuki ilişkilerin iyi tespit edilmesi gereklidir. Öncelikle ortada bir sözleşme ilişkisi vardır ve sözleşmenin içeriğini tespit etmekte taraflar serbesttir. Bu sebeple öncelikle sözleşme hükümlerine bakılacaktır. Sözleşmede işçinin gizlilik maddesini ihlal ettiğinin nasıl öğrenildiği önemsiz ise işveren iş akdini haklı sebeple feshedebilecektir. Bu fesih haklı bir fesih olmadığını iddia ederken davacı tarafın ileri süreceği gerekçeler fesih haksızlığını ortaya koyabilecek gerekçeler olmalıdır. Bu konudaki haklı sebep çalışanın işletmedeki çalışması dolayısıyla, başkalarına açıklandığı takdirde işverenin zarar görebileceği işveren ve işletmeye ait bilgilerin üçüncü kişilere açıklanmasıdır. Bu noktadan hareket edildiğinde kişisel bilgilerin gizliliğinin ihlal edildiği iddiası haklı sebep kavramını tartışmakta kullanılamayacak bir argüman olarak görülmektedir. Kısaca işveren hizmet akidindeki gizlilik maddesinin ihlali sebebiyle iş akdini haklı nedenle feshedebilir. İşçi Anayasa'nın kişisel bilgilerin ve haberleşme hürriyetinin korunduğuna ilişkin maddelerini ileri sürerek fesih haklı bir fesih olmadığını ileri süremez. Böyle bir iddia kıdem-ihbar tazminatı ve diğer işçilik haklarının talep edildiği bir davada değil, tazminat talebine dayalı veya ceza hukukunu ilgilendiren diğer davalarda ileri sürülebilir. Burada zayıf durumda olan işçinin suiistimallere karşı korunabilmesi için sözleşme hükümlerinin çok iyi yorumlanması ve somut olayın şartlarına göre durumun değerlendirilmesi gerekir. Örneğin işçi e-mail gönderdiği bir arkadaşına işyerinin çok güzel bir yer olduğunu, rahat bir çalışma ortamında olduğunu söyleyebilir. İşveren böyle bir açıklamayı gizlilik maddesinin ihlali olarak yorumlayamaz (Özdilek, 2003: 8).

İşveren Anayasa'nın düzenlemesi ile işçinin gizlilik maddesini ihlal ettiğini elektronik posta izleme araçlarıyla öğrenmesi arasındaki çatışmayı giderebilecek bazı önlemler alabilir ve bu sayede hizmet akitlerine koyduğu gizlilik maddesinin yürürlüğünü sağlayabilir. Bunu yapabilmeyen en kolay yolu sözleşmedeki düzenlemelerden başka işyerinde bir e-mail veya bilişim teknolojileri kullanımına ilişkin kurallar yayınlaması ve bunu çalışanlara bildirmesidir. Açıkça izleme yapılacağı ve bunun sonuçlarının belirtilmesine rağmen gizlilik maddesinin ihlaline yönelik eylemler tespit edilirse çalışanın izlemeye rızasının olduğu kabul edilerek haklı sebeple iş akdi feshedilebilir.

8. SONUÇ

Çeşitli bilimsel çevreler ve yasal sistem bugün gelişmiş ülkelerde hala, çalışanların kişisel özgürlükleriyle ilgili beklentileriyle işverenlerin çıkar ve beklentileri arasında denge kurmaya çalışmaktadır. Yönetimsel açıdan, çalışanların verimliliğine önemli katkılar sağladığı bilimsel çalışmalarla tespit edilmiş olan ve organizasyonel bir kaynak olarak her geçen gün önemi artan e-mail, bir etik ve yasal anlayışla kullanılmalıdır. Yasal sistemin açık ve net bir kurallar bütünü sunamaması nedeniyle işletmeler, kendilerine ait iç e-mail sisteminin kullanımı ve kişisel özgürlüklerin nerede başlayıp nerede bittiğini netleştiren politikalar geliştirilmelidir. Böylesi politikaların yoksunluğu, çalışanların, kişisel özgürlükleriyle ilgili beklentileriyle, işverenlerin bu olaya bakış açısında farklılıklara neden olabilir. Bunun yanında net bir politika ile bu dengenin sağlanması, bilgi teknolojilerinin kapasitesinin dinamik doğası nedeniyle zordur. Teknolojik gelişmelerdeki tahmin edilemeyen bu hız, daha önce örneği olmayan pek çok soruna, yasal sistemin çözüm getirmesini gerekli kılmaktadır.

Türkiye'deki durum açısından e-mail'in kişiselliğine bakıldığında hizmet akitlerindeki “gizlilik” maddesi işverenin elinde çalışana karşı kullanılabileceği çok güçlü bir silah haline gelebilir. Yine aynı şekilde kişisel bilgilerin gizliliği ve haberleşme hürriyetinin gizliliği işçi tarafından kötüye kullanılabilecek silahlar haline

gelebilir. Mahkemelerde çözümlenmesi uzun zaman alabilecek bu sorunun bu aşamaya getirilmeden çözümlenebilmesi için bazı yollar izlenebilir.

Bunlardan ilki sözleşmede bu hususun tereddüde yer vermeyecek biçimde düzenlenmesidir. Sözleşme ile hangi hareketlerin “gizlilik” maddesini ihlal edeceğinin çok açık bir şekilde tanımlanması, kast veya ihmali hallerinin neler olduğunun ve bunlara bağlanacak sonucun ne olacağının açıklanması, hareketlerin sonucunun açıkça ne olacağı (akdin feshi, disiplin cezası, maaş kesimi gibi) belirtilmelidir. Buna ek olarak işyerinde bir e-mail veya bilişim teknolojileri kullanımına ilişkin kurallar oluşturmak ve tüm çalışanlara bu kuralları anlatmak, açıklamak ve ilgililere bu kuralları (imza karşılığı veya başka bir şekilde) bildirmek sorunun çözümünde yardımcı ve yol gösterici olacaktır.

İşveren de çalışanlarıyla ilgili elde ettiği kişisel bilgileri kesinlikle ifşa etmemeli, ağın güvenliğini sağlamak için gerekli önlemleri almalıdır. Bu yükümlülük hem işin niteliğinden hem de İş Kanunu'nun iş güvenliğine ilişkin maddelerinden çıkarılabilir. Bilgi çağında artık çalışanların e-mail kullanmalarını engellenmemek gerekir. Buna karşın çalışanlar da işyeri kurallarına ve sözleşme hükümlerine uygun hareket etmelidirler.

KAYNAKÇA

Boutin, Paul; Udell, Jon (2004), “Can E-Mail Be Saved?”, InfoWorld, V.26, I.16, p.40-50.

Cappel, James J. (1995), “A Study of Individuals’ Ethical Beliefs and Perceptions of Electronic Mail Privacy”, Journal of Business Ethics, V.14, I.10, p. 819-828.

Cohan, John Alan (2000), “Privacy in Workplace”, The Secured Lender, V.56, I.3, p.80-83.

Greenwald, Judy (2004), “Privacy Issues Creating Dilemma For Employers”, Business Insurance, V.38, I. 7, p.1-2.

Halpert, Jane (1998), “Ethical E-Mail Issues”, Business Ethics (Editor: Laura Pincus Hartman), New York: McGraw-Hill International Editions, p. 624-625.

Hayes, Frank (2004), “Mail Mishap”, Computerworld, V.38, I.28, p.46-48.

Kladko, Brian (2004), “Cambridge, Mass., Firm Devises Way to Confirm Whether E-Mail Has Been Read”, Knight Ridder Tribune Business News, p.1-3.

Leizerov, Sagi (2004), “E-Mail and The Law”, Journal of Accountancy, V.198, I.2, p.58-61.

Özdilek, Ali Osman (2003), “Hizmet Akitlerinde Gizlilik Maddesinin Bilişim Teknolojileri Kullanımı Açısından Değerlendirilmesi”
<http://www.bilismhukuku.net/index.php?option=content&task=view&id=322&Itemid=40>, s.1-11. İndiriliş tarihi: 16.08.2004.

Özdilek, Ali Osman (2002), “Bilgisayar Suçları Ne Kadar Ciddi?”, s.1-12.
http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm, İndiriliş tarihi: 16.08.2004.

Özel, Cevat (2002), “Bilişim-İnternet Suçları”, s.1-15.,
http://www.hukukcu.com/bilimsel/kitaplar/bilism_internet_suclari.htm, İndiriliş tarihi: 16.08.2004.

Precision Marketing (2004), p.17-19.

Sipior, Janice C. Ve Ward, Burke T. (1995), “The Ethical and Legal Quandary of E-Mail Privacy”, Communications of the ACM, V.38, N.12

Sipior, Janice C. Ve Ward, Burke T. (1998), “The Ethical and Legal Quandary of E-Mail Privacy”, Business Ethics (Editor: Laura Pincus Hartman), New York: McGraw-Hill International Editions, p. 626-631.

Verton, Dan (2004), “E-mail Glitch Exposes Flaw In Privacy Law”, Computerworld, V.38, I.28, p.1

Wagstaff, Jeremy (2004), “What Price Privacy?”, Far Eastern Economic Review, V.167, I.19, p.40-43.

Wakefield, Robin L. (2004), “Computer Monitoring and Surveillance”, The CPA Journal, V.74, I.7, p.57-65.