İletişim Özgürlüğüne Müdahale Raporu (2009)
ELEKTRONİK GÖZALTI DÜNYASI: e-Göz@ltı

ÖZET

İnternet'in dünya genelinde yaygınlık kazanması ile mekan kavramı bir anlamda ortadan kalkmış, kıtalararası iletişim ve bilgi transferi bir tuşa basmaktan ibaret hale gelmiştir. Teknolojideki bu gelişmelerden toplumlar pozitif anlamda yararlandıkları gibi, baskı, korku ve sindirme yöntemlerini olağan bir politikaya dönüştüren, özgür ve demokratik yaşam biçimini içselleştirememiş ülkelerde ise; teknolojik sistem ve cihazlarla temel hak ve hürriyetlere müdahale yaşam kültürü haline dönüştürülmeye çalışılmaktadır. Bununla birlikte; suç örgütleri de, gelişen bu teknolojiyi yakından takip ederek, hem kazançlarını arttırmakta, hem de geleneksel suç tiplerinin dışında yeni suç tiplerini de geliştirmektedirler. Küreselleşmenin kirli ve karanlık yüzü olarak tanımlayabileceğimiz bu gelişmeler toplumsal huzuru, barışı ve güvenliğimizi ciddi bir şekilde tehdit etmektedir.

Bugün cep telefonları, İnternet üzerinden elektronik posta haberleşmesi, anlık ileti gönderimini sağlayan servisler, sanal iletişim grupları gibi çeşitli sosyalleşme ağları, insanların kişisel ve toplumsal iletişiminde temel araçlar haline gelmişlerdir. Bu iletişim araçlarının gün geçtikçe artan kullanımı; insanların teknolojinin gelişimine paralel olarak iş ve ev yaşamlarında görülen değişikliklerin toplumsal iletişim ortamına bir yansıması olarak değerlendirilebilir. Elbette bu gelişmelerin insanların iletişim olanaklarını kolaylaştırdığı söylenebilir. İnsanların toplumsallaşma süreci açısından ayrıca sorgulanabilir olan bu araçların yarattığı olanakların yanında önemli ölçüde kısıtlayıcı etkileri bulunmaktadır. Kişilerin telefon konuşmalarında, anlık ileti ve e-posta yazışmalarında kendilerine otosansür uyguladıkları, bazı konularda konuşmaktan ve yazmaktan çekindikleri, dolayısıyla iletişim ortamı içerisinde iletişimsizlik denilebilecek bir sürecin yaşandığı görülmektedir.

Dünya'da ve ülkemizde teröre karşı önlem ve güvenlik gerekçesiyle iletişim özgürlüğü başta olmak üzere çeşitli haklar ve özgürlükler kapsamında ciddi sınırlamalara başvurulduğu bir dönem yaşanmaktadır. Bu sınırlandırmalar kapitalist sistem içerisinde kar artırma yöntemleriyle birleştiğinde daha da genişlemektedir. Örneğin sokakları gözetleyen kamera sistemleri kurulmaktadır. Son olarak 1 Mayıs öncesinde DİSK Genel Merkez binasını gözetlemek üzere İstanbul Emniyet Müdürlüğü'nce mobil elektronik sistem entegrasyonu (mobese) kamerası yerleştirilmesi kamuoyunda tepki çeken uygulamalardan biri olmuştur. Okullar, toplu taşıma alanları, büyük alışveriş merkezleri başta olmak üzere pek çok kamusal mekan devasa gözetim sistemi içerisinde yer almaktadır. Alışveriş ve bankacılık işlemleri gibi günlük yaşama ilişkin faaliyetler sırasında elde edilen kişiye özel bilgiler, bu kişilerin isteği ya da bilgisi olup olmadığına bakılmaksızın yine ticari amaçlı olarak kullanıma açılmaktadır. Büyük alışveriş marketlerinin dağıttıkları kartlar, kredi kartlarıyla yapılan harcamalar üzerinden şirketler pazar araştırması ve yönlendirmesi yapabilmektedirler. İnternet'te hizmet veren arama motorları başta olmak üzere bazı siteler kişinin elektronik ortamdaki gezintilerini kaydedip analiz ederek, o kişilerin ilgi alanlarına uygun yönlendirmelerde bulunabilmektedirler. Böylece modern dünyanın insanları tüketim alışkanlıklarından, hobilerine, okudukları kitaplara, gittikleri yerlere, katıldıkları etkinlik ya da grupların takibine kadar uzanan geniş bir izleme ağı içerisinde bulunmaktadırlar. İzleme dünyası küçük yaş gruplarına kadar yayılmakta, kreşlerdeki kamera sistemlerinden çocukların okuduğu kitapların kayıtlara geçirilmesine varıncaya dek uzanmaktadır. Artık kapitalist sistem içerisinde "fişlemenin" adı "performans ölçümü" olmuştur.

Denetim-gözetim paradigmasına göre modern iktidarlar, bireyi sistem içerisinde en verimli şekilde kullanabilmeyi amaçlarlar. Bireyi en verimli şekilde kullanabilmenin yolu ise onu; bedeni, ruhu ve tüm faaliyetleri ile bilinebilir, hesaplanabilir (istatistik verisi olarak) bir

nesne haline getirmekten geçer. Zira modern çağda devlet tarafından künyesi tutulan birey, yeni kurum ve teknikler yoluyla gözetime tabi tutulmuş, sicil kayıtları yaratılarak fişlenip güncellenmiş, merkezileşmiş bilgi matrislerine (arşivleme) sürekli aktarılarak depolanmış ve depolanmaktadır.

Türkiye'de 2006 yılında 2 bin 699, 2007 yılında 4 bin 947, 2008 yılında ise 5 bin 212 kişinin telefon görüşmelerinin gereksiz yere dinlendiği ve bu dinleme kayıtlarının imha edildiği açıklanmıştır. Dinleme ve izleme olaylarını günümüzdeki teknolojik gelişmeleri de dikkate alarak 3'e ayırabiliriz:

1- Trafik takibi (Kim, kiminle, ne zaman iletişim kuruyor?): İzleme kapsamında değerlendirilen bu uygulama temel olarak, sabit telefonla yapılan görüşmelerde, cep telefonlarıyla yapılan görüşmelerde, İnternet üzerinden yapılan elektronik haberleşmelerde (e-posta, anlık ileti, İnternet sitelerine yapılan ziyaretler) kimin, kiminle, ne zaman ve ne kadar süre iletişim kurduğunun saptanması şeklinde özetlenebilir.

2- Konum belirleme (Kim nerede bulunuyor, kiminle beraber bulunuyor?/Yer tespiti): İzleme kapsamında kimin, ne zaman, nerede bulunduğunun tespiti için ayrıca başvurulan yöntemler bulunmaktadır. Tarihsel olarak hafiyecilik, dedektiflik gibi yöntemlerle yapılan kimin nerede bulunduğuna ilişkin tespit, günümüzde elektronik cihazlara kaymıştır. Küresel konum belirleme (GPS) aletleri, baz istasyonları, İnternet'e çıkışı sağlayan numara (İnternet Protokolü-IP), uydu ve uçaklar konum belirleme amacıyla kullanılmaktadır.

3- İçerik takibi (Kim kime ne diyor?): Yazılı, sözlü ve elektronik ortamda gerçekleştirilen iletişim kapsamında içeriksel takip yapılmasına yönelik olarak değişik uygulamalar bulunmaktadır. Bu tür içerik takipleri yasal talepler dışında günümüzde teknolojinin hızla gelişmesi, İnternet'ten içerik takibi yapabilecek cihazlara erişim kolaylığı, düzenleme ve denetim yetersizliği nedeniyle kişilerin rahatlıkla gerçekleştirebileceği uygulamalara dönüşmüşlerdir. Teknolojik aletlerin gelişmişliğine paralel olarak içerik takibi teknolojileri de giderek karmaşıklaşmış, uzman olmayan kişilerin fark etmesinin mümkün olamayacağı bir noktaya ulaşmıştır. Fark edilmesi giderek zorlaşırken, uygulaması da ters orantılı olarak giderek kolaylaşmakta ve ucuzlamaktadır. Yasadışı dinlemeler santraldan, panodan, apartman girişinden, anten ve uydu aracılığıyla havadan yapılabildiği gibi lazer dinleme, casus yazılımlar, monitör dinleme, kablo dinleme, vakumlama, casus klavye gibi araç ve yöntemlerle de gerçekleştirilmektedir.

İletişim özgürlüğü açısından ülkemizin sahip olduğu hukuksal düzenlemelere bakıldığında ise mevzuatın son derece yetersiz olduğu görülmektedir. Son yıllarda kimi yeni yasal düzenlemeler yapılmış olmakla birlikte, iletişim güvenliğinin sağlanamadığı, bu alandaki toplumsal kaygıların en üst safhaya ulaştığı bir süreç yaşanmaktadır. Gerek ülkemizin de taraf olduğu Avrupa İnsan Hakları Sözleşmesi'nde, gerekse Anayasamızda özel hayatın ve haberleşmenin gizliliğine vurgu yapılmış ve hangi durumlarda, hangi organlar eliyle, nasıl istisnaların uygulanacağı da kesin bir şekilde belirlenmiştir. Ancak gizliliği korumaya yönelik tedbirler almakla görevli resmi makamların ortaya koyduğu kimi uygulamalar, bizzat kamu görevlilerince gizliliğin ihlal edildiği kuşkularını doğurmakta ve toplumda bir otosansür mekanizmasının işlemesine neden olmaktadır.

İletişimin hukuk dışı dinlenmesinin önlenmesiyle ilgili olarak, suçtan mağdur olan kimselerin yapabilecekleri son derece sınırlıdır. Nitekim iletişimin dinlenmesi de gizli yapılmaktadır ve genellikle mağdurun suçtan haberdar olması söz konusu değildir. Ancak iletişim kayıtlarının yayınlanmasıyla suçtan haberdar olunabilmektedir. Bu aşamada ise failin suçtan beklediği yarar gerçekleşmiş olacağından, uygulanacak bir yaptırımın da önemi kalmayabilmektedir. Özellikle ticari ya da mesleki sırların elde edilmesi gibi gizlilik ihlallerinde kayıtların yayınlanması söz konusu olmadığından, mağdurun da suçu öğrenme olanağı bulunmayacaktır.

Kamunun özgürce kullanabileceği güvenli haberleşme hakkı; yasal güvence altına alınmalıdır. Bu konudaki hak ihlallerinin önüne geçilmesi ve güvenlik açıklarını giderecek düzenlemelerin ivedi olarak hayata geçirilmesine ihtiyaç bulunmaktadır. Teknoloji okuryazarlığıyla birlikte teknoloji kullanımı etiğinin geliştirilmesi ise ayrıca üzerinde durulması gereken bir konudur.

NASIL VE NELER YAPILMALI?

1. Teknolojik gelişmelerin yararlar yanında yarattığı sıkıntıların çözümünde öncelikle özgürlükleri kısıtlayıcı değil, genişletici bir bakış açısıyla hareket edilmesi gerekir.
2. Anayasal güvenceye sahip iletişim özgürlüğünün korunması temel prensip olmalıdır.
3. İletişim özgürlüğüne zarar veren yasadışı dinleme ve izleme olaylarına karşı denetim yükümlülüğü öncelikle kamuya aittir. Buna yönelik denetim mekanizması ve altyapı sağlanmalıdır.
4. İletişim hizmetini sağlayan şirket ve kurumlara da iletişim özgürlüğünün korunmasına yönelik olarak sorumluluklar yüklenmeli ve gerekli denetim mekanizması kurulmalıdır.
5. Teknoloji kullanımı konusunda kamunun bilinçlendirilmesi gerekmektedir. Türkiye'de teknoloji okuryazarlığı yükseltilmelidir.
6. Dinleme ve izleme cihazlarının satışı, yurda girişi denetim altına alınmalı, kontrollü yapılmalıdır. Kaçak girişler önlenmeye çalışılmalıdır.
7. Casus yazılımlara karşı yasaklayıcı bir zihniyetin İnternet dünyasında geçerliliği yoktur. Bu nedenle bu tür yazılım kullanımlarına karşı öncelikle toplumda teknoloji etiğinin yerleştirilmesi önemlidir.
8. Casus yazılım gönderimini engelleyebilecek yazılımlar da cep telefonu satan şirketler, cep telefonu hizmeti veren şirketler ve kamunun ortak sorumluluğuyla yaygınlaştırılabilir.
9. Cep telefonlarına yüklenebilecek yazılımların kimliklendirilmesi ve insanların onay listesinde olmayan yazılımların o kullanıcıya gönderimini engelleyecek bir sistem kurulabilir.
10. Casus yazılımın var olup olmadığına ilişkin telefon kontrol hizmeti ve casus yazılımlara karşı anticasus program kurulum hizmeti verilmelidir. Yurttaşlara bu tür hizmetleri verecek kamusal birimler oluşturulmalıdır.
11. Anticasus yazılımların geliştirilmesi, casus programların indirilmesini engelleyici güvenlik duvarları yerleştirilmesi konusunda TÜBİTAK kamu adına sorumluluk üstlenebilir.
12. Bedava cep telefonları ve bilgisayar alınmamalıdır.
13. İzleme ve dinlemeye karşı pasif odalar, frekans önleyici cihazlar kullanılabilir.
14. Anlık ileti gönderiminde ve İnternet üzerinde sesli görüşmelerde şifreleyerek konuşma ve mesaj iletimi gerçekleştiren sistemler tercih edilmelidir.
15. Cep telefonlarında da şifreleme yazılımları kullanılarak, dinlemeye karşı kişiler kendileri önlem alabilirler.
16. Ortam dinlemesi yapan cihazlar olduğundan şüpheleniyorsanız vericileri bulmak için geliştirilmiş aygıtlar edinebilirsiniz.
17. Bilgisayar kullanımında kişisel güvenliğiniz için almanız gereken temel önlemleri mutlaka sağlayın. Antivirüs yazılımları, güvenlik duvarları, şifreleme, yedekleme, geriye dönük izleme yapmayı engelleyecek şekilde güvenli silme yazılımları kullanın ve bu yazılımların güncellemelerini takip edin.

ELEKTRİK MÜHENDİSLERİ ODASI