KRİPTO YÖNETMELİĞİ Mİ? KORKU TOPLUMUNA GİRİŞ Mİ?

Burak OĞUZ
Bilgisayar Mühendisi
burakoguzs@yahoo.com

İnternet'in ve mahremiyetin her geçen gün daha çok tartışılmaya başlanıldığı günümüzde BTK tarafından hazırlanan ve yayınlanan bütün yönetmelikler, yanında büyük tartışmaları da yanında getiriyor. Bu tartışmaların en sonuncusu ve belki de bugüne kadar yayınlanmış yönetmelikler içerisinde teknik açıdan en çok tartışma koparanı ise Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti içinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Yönetmeliği.

Kripto, kabaca, mesajların önceden belirlenmiş bir kodlama ile gizlenmesidir. Kriptoloji ise şifre bilimidir. Çeşitli iletilerin, yazıların belli bir sisteme göre şifrelenmesi, bu mesajların güvenlikli bir ortamda alıcıya iletilmesi ve iletilmiş mesajın deşifresiyle uğraşır. (Wikipedia)

Özellikle günümüzde işlem gücünün ve iletişim hızının inanılmaz boyutlara ulaşmasıyla birlikte, kişilerin ve kurumların Internet ve benzeri iletişim kanalları üzerinden yetkisiz kişiler tarafından bilgilerinin alınması, dinlenmesi veya değiştirilmesi gibi riskler de oluşmaya başladı. Bu risklerden korunmanın yolu ise en basit ve genel olarak kullanılan kripto altyapılarının oluşmasına neden oldu. Ancak her zaman bu konudaki tartışma mahremiyet üzerinden yapıldı. Gerek kişilerin gerekse de kurumların mahremiyeti buradaki tetikleyici faktör oldu.

Ancak yayınlanan yönetmelik ile MİT, Emniyet, Jandarma gibi asayiş ve istihbarat kurumlarının kendi içlerindeki iletişimlerindeki kripto kullanımının karışılamaz durumu korunurken, vatandaşın iletişimi güvenlik vb. nedenlerle denetim altına alınmak isteniyor.

Bu yönetmelik ile ilgili ilk uygulama bir cep telefonu üreticisinin özel şifreli mesaj haberleşme altyapısı üzerinde yapıldı. Toplumun ve özel sektörün konu ile ilgili tepkileri gözlendi. Bazı kişiler yönetmeliğin getirmiş olduğu hem teknik açıdan hem de mahremiyet açısından sorunların farkına varmasına rağmen bir çoğunluk oluşturamadı. Çoğu teknik ve akademik çevreden de hiçbir tepki oluşmadı.

Teknik Açıdan Yetersiz

Yapılan yönetmelik ile şifreli haberleşme yapılmak istenildiği zaman, bu haberleşmenin sadece BTK tarafından onaylanan cihazlar üzerinden yapılması gerekliliğini getiriyor. Bunun yanında yapılan bütün şifreleme ile ilgili deşifre anahtarlarının da kurula teslimini şart koşuyor.

Ancak günümüzde çok yoğun olarak kullanılan Açık Anahtar Altyapısına (PKI – Public Key Infrastructure) dayanan teknolojilerin bu yönetmelik ile haberleşmede kullanılamayacak duruma getirilmesi, oluşturulan yönetmeliğin teknik açıdan ne kadar yetersiz olduğunu ortaya koyuyor. Örnek olarak Açık Anahtar Altyapısına dayanan en önemli teknolojilerden birisi olan SSL'in açık hale getirilebilmesi için sadece o tekil zaman için oluşturulan ve tek seferlik kullanılan şifreleme anahtarlarının da kurul tarafından saklanabilmesi gerekiyor. İkinci bir yöntem olarak da Türkiye'deki bütün Internet trafiğini BTK içerisinden geçmesi gerekiyor. Ne yazık ki iki yöntem de şu an için teknik açıdan uygulanabilir değildir. Ayrıca bu yönetmeliğin gerçek anlamda uygulanmak istenmesi durumunda ülkemizin dış ağlarla iletişimi de bir soru işareti oluşturmaktadır.

Diğer önemli bir nokta ise şifreleme cihazlarının ve anahtarlarının BTK'ya teslim edilmesi durumunda bunların saklanması ve kullanım koşulları ile ilgili bir bilgi verilmemesidir. Bu cihazların ya da anahtarların kaybolması veya çalınması durumunda ülke çapında çok büyük bilgi güvenliği sıkıntıları oluşabileceği ve bunun sorumluluğunun alınması gerektiği unutulmamalıdır.

Diğer önemli bir konu ise BTK'nın şu an için iletişim güvenliği ile ilgili çalışan kurumlar için bir denetçi durumunda olmasıdır. Ancak bu yönetmelik içerisinde ortaya çıkan bir diğer sorun, BTK'yı bu derece önemli cihaz ve bilgileri saklarken denetleyecek bir kurumun belirlenmemiş olmasıdır.

Korku Toplumuna Neden Olabilir Mi?

Bu yönetmeliğin akıllara getridiği en önemli örnek panoptikon tarzı denetleme mekanizmasıdır. Yine Wikipedia'dan küçük bir alıntı yapmak gerekirse,

" Panoptikon'un temelinde yatan ilke, tek odalı hücrenin içindeki sakine saklanacak hiçbir yer bırakmaması, buna karşılık dış cephedeki duvarın penceresinden gelen dış ışığın kuledeki nöbetçilere mahpusun her hareketinin bir silüetini izleme olanağını sağlamasıydı. Bentham'ın (bu hapishaneyi tasarlayan mimar) yaklaşımına göre, gözlemlenen her yanlış davranışının ceza getireceğini bilen, ama davranışlarının aslında ne zaman gözlemlendiğini bilmeyen mahpusun, aklını başına toplayarak her zaman izleniyormuşçasına davranmaktan başka seçeneği yoktu. Böylece mahkûm bizzat kendi hareketlerini kollamak durumunda kalacaktı."

Bu yönetmlikten anlaşılan da kabaca bu yaklaşıma benzemektedir. Denetlenmeyen bir güç tarafından toplumda bulunan herkesin gizli iletişimini izleyebilme yetkisi, demokrasilerde olması gerekenden çok daha büyük bir güçtür. Bu yaklaşım toplum içerisinde insanların sürekli takip edildiği duygusunun oluşması ile zamanla bireylerin otosansür uygulamasına zemin sağlayabilir.

Eğer amaç "güvenlik" ise Avrupa ve Amerika'da uygulanan sadece şüpheli şahısların takip edilmesine dayalı yöntemlerin kullanılması daha yerinde olacaktır.