BİRİ BENİ DE Mİ GÖZETLİYOR?

İnternet hayatımıza girmeden önce de oldukça önemli bir konu olan "gizlilik" kavramı, içinde bulunduğumuz bilişim çağında daha da büyük bir sorun olarak gündeme oturdu. Aslında bilgisayarların ve İnternet'in bu alandaki işlevleri, diğer alanlardakinden pek de farklı değil: Hayatımızdaki çoğu eylemi daha pratik ve çabuk yoldan yapmamızı sağlayan bilgisayarlar, kişisel hak ve özgürlüklere yapılacak tecavüzlerin de daha hızlı ve etkin olmasını sağlıyor. Ancak yine de İnternet, bugünlerde kişisel gizliliğimizi savunduğumuz mahkeme salonunda suçlu koltuğuna oturturtulanların bir suç ortağı.

İnternet ortamı, gözetlemeye yönelik oldukça geniş ve zengin olanaklar sunan global bir oyun alanı haline gelmekte. İnternet'in yaygınlaşmasıyla birlikte, işverenlerin çalışanlarını, devletlerin vatandaşlarını ve ailelerin çocuklarını gözetlemek için açtığı elektronik gözlerin görüş alanı genişliyor. İnternet'te gezinti yapan kullanıcıları gözetlemeye yönelik olarak geliştirilmiş teknolojiler oldukça çeşitli. Kontrol amaçlı yazılımlar, bu örneklerden biri. Ebeveynlerin çocuklarının bilgisayar başında yaptıklarını gözetlemeleri için geliştirilmiş gibi görünen bu yazılımlar, günümüzde işverenlerin çalışanlarını kontrol etmesi ya da eşlerin birbirlerini kontrol etmesi gibi oldukça farklı amaçlara hizmet etmekte. İnternet'e bağlı bir bilgisayara bu yazılımı yüklediğinizde, o bilgisayar üzerinde Netscape, Internet Explorer, ICQ, YahooMail, Hotmail, Yahoo Messenger ve benzer araçlar kullanılarak yapılan tüm yazışmaları kaydedebiliyorsunuz. Ayrıca bilgisayar başındaki kullanıcının ziyaret ettiği tüm web sitelerini görmeniz de mümkün. Bu yazılımlar kullanıcının İnternet üzerinde gerçekleştirdiği iletişimin tümünü kaydetmek istemeyenler için, belli kritik sözcükler tanımlayıp yalnızca bu sözcüklerin geçtiği iletişimi kaydetmek gibi bir olanak da sağlıyor. Üstelik kaydedilen tüm bu sonuçları kontrol etmek için bilgisayar başında bulunmanız gerekmiyor. Yazılımın ayarlarında yapacağınız bir düzenlemeyle, kayıtların her 15 dakikada bir dilediğiniz bir e-posta adresine gönderilmesini de sağlayabiliyorsunuz. Bu yazılımlar kurulduğu bilgisayarın çalışmasını yavaşlatmayıp, başlangıç menüsünde yer almadığından ve Ctrl+Alt+Del komutunu verdiğinizde kapanacak programlar arasında görünmediğinden, farkedilmeleri oldukça

güç. Yalnızca Windows değil, Unix işletim sisteminde de çalışabilen bu yazılımları edinmek için ödemeniz gereken miktarsa yaklaşık 70-100 ABD doları. Yapılan istatistikler ABD'deki şirketlerin % 75'inin bu tür yazılımları kullanarak çalışanlarının bilgisayarlarını kontrol ettiğini, işten çıkarılmaların % 27'sinin de bu kayıtlar doğrultusunda gerçekleştiğini gösteriyor.

Bugünlerde oldukça ciddi tartışmalara yol açan bir başka yazılımsa IBM'in üzerinde çalıştığı BlueEyes (Mavi Gözler) yazılımı. Bilgisayar karşısındaki kullanıcıların göz hareketlerini ve yüz mimiklerini kaydedip sınıflandıran BlueEyes, bu kayıtları kullanarak kişilerin İnternet üzerindeki faaliyetlerini kontrol etmeyi amaçlıyor. Kişinin hangi web sitesinde ne kadar süreyle kaldığını, sitenin içinde hangi bölümleri ziyaret ettiğini ve ne tür ilanları incelediğini izleyerek kişinin ilgi alanını belirleyen yazılım, aynı kişinin bir sonraki İnternet ziyaretinde kayıtları kullanarak belli siteleri otomatik olarak karşısına çıkarmayı hedefliyor. Ancak, pazarlamacıların açılması için şimdiden sabırsızlandıkları bu mavi gözler, herkes için o kadar da sevimli değil. BlueEyes'ın kullanımına şiddetle karşı çıkan Amerika Sivil Özgürlükler Birliği (ACLU) yöneticilerinden Barry Steinhardt'a göre bu yazılım, kişilerin bir web sitesinde ne kadar zaman harcadığını belirlemekle kalmayıp, kim olduklarının da anlaşılmasını sağlayacakları için oldukça tehlikeli.

Bilgisayarların içinde bulunan işlemcilerin İnternet üzerindeki faaliyetleri izlemeye yardımcı olacağı konusundaki tartışmalar da henüz sonlanmış değil. 20 Ocak 2000'de Intel firması, piyasaya süreceği Pentium III işlemcilerinin herbirinin kendine özel ve tek bir İşlemci Seri Numarası (PSN) bulunduracağını açıkladığında, bu tartışmalar alevlenmişti. Intel yetkililerine göre bunun amacı, elektronik ticaret ve benzeri diğer web tabanlı uygulamalarda kullanıcıları tanımayı kolaylaştıracak olmasıydı. Ancak kolayca tanınabilecek bir PSN uygulaması, birçok web sitesi tarafından kaydedilip çeşitli veri tabanlarında kullanılabileceğinden, kişilerin gizlilik haklarına zarar vereceği iddialarına hedef oldu. Hep aynı kalan ve değiştirilmesi ya da silinmesi pek de kolay olmayan "işlemciye özel" bir PSN alt yapısı, reklam yapmak isteyen şirketlerce kısa sürede keşfedilebileceğinden, bilgisayarınızın bu şirketlerin bombardımanına uğramasına yol açabilirdi. İtirazların en şiddetlisiyse Çin Hükümetinden geldi. Ulusal güvenliği tehdit ettiğini söyleyerek ülke sınırları içinde Pentium III işlemcisinin satışını yasaklayan Çin, ayrıca tüm devlet kurumlarında bulunan Pentium III işlemcili bilgisayarlarla İnternet'e bağlanmayı da yasakladı. Aldığı bu itirazlar nedeniyle uzunca bir süre birçok gazete ve derginin manşet konusu olan Intel, sonunda yeni üretecekleri işlemcilerin üzerine "özel" bir PSN koymama kararı aldı.

Henüz hiç birimiz 24 saat gözetlenmiyorsak bile, yapılan tüm çalışmalar bunun çok da uzak bir olasılık olmadığını gösteriyor. Sun Microsystems şirketinden Scott McNealy'nin 1999 yılında söylediği "Şu anda sahip olduğunuz gizlilik oranı zaten sıfır, artık bu konuyla uğraşmayı bırakın" sözleri, oldukça ciddi yankılara neden olmuştu. Ancak her geçen gün yeni bir yöntemle karşımıza çıkan gözetleme teknolojisi geliştirme uzmanları, geliştirdikleri araçların tümünün olumlu sonuçlar doğuracağından emin. Örneğin, bilgisayar karşısındaki kişinin göz hareketlerini okuyan arayüzlerin öncelikli amacının Web'de gezinmemizi kolaylaştırmak olduğunu söyleyen araştırmacılar, bunların potansiyel suçluları da tanıyarak siber ortamdaki suç oranlarını azaltacağını savunuyor. Bu yöntemde öncelikle suçlulara ait mimikler uzmanlarca belirlenip, veri tabanına kaydediliyor. Daha sonra bu mimikler İnternet'te gezen kişilerinkiyle karşılaştırıldığında, siber ortamda suç işlemeye yeltenen bir kişi anında tespit edilebiliyor. Buna karşılık gizlilik savunucularının ortaya koyduğu resim oldukça bulanık. Gözetleme alanındaki teknolojinin ışık hızıyla geliştiğini söyleyen Steinhardt'a göre, bireyleri koruyacak gizlilik yasalarıysa halen Taş Devri'ni yaşıyor. Bu teknolojilerin doğru ve iyi niyetli kullanımlarının olumlu sonuçlar doğuracağına katılan gizlilik savunucularının sorunu, varolan yasaların bu araçların kötü niyetli kullanımlarına da olanak sağlayacak yapıda olması.

11 Eylül'ün Ardından

11 Eylül 2001 tarihinde Dünya Ticaret Merkezi ve Pentagon'a yapılan saldırıların hemen ardından, ABD içinde geçerli haberleşme mekanizmalarını kontrol eden anlaşmalar üzerinde değişiklik yapılmasına yönelik tartışmalar gündeme geldi. Eylemden üç gün sonra yapılan İnternet Güvenlik Hizmetleri Anlaşması toplantısında, oldukça önemli değişiklikler görüşüldü. Ancak tüm bu toplantılar, bireysel hak ve özgürlüklerle ilgilenen sivil toplum kuruluşlarından şiddetli bir tepki aldı. New York ve Washington'daki saldırılarda teknolojinin ne ölçüde kullanıldığı konusundaysa uzmanlar hâlâ tatmin edici bir sonuca ulaşabilmiş değil.

Siber Gözetleme Yelkenleri Açılıyor

Saldırıların ardından ABD Kongre'si, devletin kritik noktalardaki bilgisayarlarının, olası bir terörist saldırıya

en az bir havaalanı güvenlik sistemi kadar savunmasız olduğunun farkına vardı. Bunun üzerine gözlerini siber ortama çeviren Kongre, daha güçlü ve etkin siber gözetleme yöntemlerinin geliştirilmesi üzerinde durmaya başladı. Saldırılardan üç gün sonra, yasaların İnternet üzerindeki etkisini artırmak ve devletin bilim ve teknolojideki ilerlemeleri daha etkin olarak kullanmasını sağlamak amacıyla "Terörle Mücadele Yasası-2001" taslağı yeniden incelemeye alındı. Adalet Bakanlığı yetkilileri, saldırıların hemen ardından yeni bir teklif hazırlamaya başladılar. Adalet Bakanı John Ashcroft, terörle mücadele etmek için gerekli düzenlemeleri içeren yasayı kısa sürede yürürlüğe sokabilecekleri konusunda iyimser.

Yeni yasada terörizm, ileri teknolojiyle izlenmeyi gerektiren suçlar sınıfına yükseltiliyor. Tasarının en önemli özelliğiyse, herhangi bir tutuklama yetkisinin tüm telekomünikasyon türlerine uygulanabilmesini ve web üzerindeki faaliyetleri izlemek için de kullanılabilmesini sağlayacak olması. Buna göre arama izinleri yalnızca telefonların dinlenmesini sağlamakla kalmayıp, elektronik postaların okunmasını ve sesli elektronik postaların dinlenebilmesini de içerecek. Ashcroft yeni yasalarla ilgili olarak verdiği brifingde, yeni yasa uygulamasının, bir telefon numarasını dinlemek yerine bir bireyi tümüyle gizlice dinlemek olanağı sağlayacağı üzerinde durdu. Ashcroft'a göre otoritenin yalnızca cihazlar üzerine uygulanması, kişi kullandığı cihazı değiştirdiğinde gözetleme kapasitesinin de yitirilmesine yol açtığından, etkin bir yöntem değil.

Yeni tasarıyla birlikte köklü değişikliğe uğraması beklenen yasalar şunlar:

1. *1978 Dış İstihbarat Gözetleme Yasası.* Şu an yürürlükte olan yasaya göre, ancak söz konusu kişinin dış bir gücün ajanı olduğuna dair olası bir neden gösterildiğinde telefon dinleme yetkisi alınabiliyor. Yeni yasa tasarısıysa yalnızca dış güçlerin ajanları için değil, yasadışı herhangi bir araştırmaya yönelik bilgi toplanmasında da dinleme izninin verilmesini sağlamayı hedefliyor.

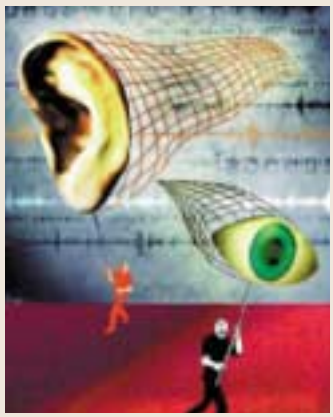
2. *1968 Federal Dinleme Yasası.* Bu yasa, polise iletişime müdahale yetkisinin, ancak iletişimin işlenmiş, işlenmekte olan ya da işleneceği sanılan suçla bir bağlantısı olduğuna bir kanıt gösterildiğinde verilmesini öngörüyor. Varolan yasaya göre polise bu yetki yalnızca bazı Kongre üyelerince verilebiliyorken, yeni tasarıya göre tüm temsilciler bu yetkiyi verme hakkına sahip olacak.

Tasarlanan paket, İnternet Servis Sağlayıcıları (ISP)'nın konumlarında da önemli değişiklikler öngörüyor. Yürürlüğe konması planlanan yeni yasalara göre, bir kişinin hayatının tehlikede olduğuna inanan bir servis sağlayı-

İnternet'i Korumak

İnternette'ki kişisel gizlilikle ilgili tartışmalar süredursun, bilgisayar korsanlarının gün geçtikçe daha yetenekli hale gelmesi, bilgisayarımızdaki dosyaların güvenliğine yönelik bir başka sorun olarak karşımıza çıkıyor. Her geçen gün yeni ve etkileri daha güçlü bir virüsün İnternet üzerinde yayılması, devlete ait önemli bilgisayarları olduğu kadar kişisel bilgisayarları da tehdit ediyor. Özellikle geçtiğimiz yaz yaşanan CodeRed virüsü saldırısı, siber ortama kırmızının en göz alıcı tonunda bir alarm saldı. Bu olayın ardından, İnternet'i olası saldırılara karşı korumak için alınması gereken önlemler de yeniden gündeme geldi.

İnternet'teki düşmanlarınımızı aramak için yola çıktığımızda, söz konusu alanın belirsizliği ve genişliği nedeniyle kendimizi sonu görülmeyen karanlık bir tünelin içinde bulmamız kaçınılmaz. Asıl şaşırtıcı olansa, tünelin sonundaki ışığa ulaştığımızda göreceğimiz yüzün yine kendimizinki olması. Yapılan araştırmalar İnternet'in korunmasındaki en zayıf noktanın, evlerdeki PC (kişisel bilgisayar) kullanıcıları olduğunu gösteriyor. Bugüne kadar alıştığımız bilgisayar virüslerinin yerini artık bilgisayar solucanlarının alıyor olması, oldukça ciddi bir tehlike. Çünkü bu ikisinin biyolojik adaşları arasındaki farklar, bilgisayar ortamında da geçerliliğini koruyor. Çalışmak ve kendini kopyalamak için bir başka programın varlığına ihtiyaç duyan bilgisayar virüslerinin aksine, bilgisayar solucanları kendi kendini kopyalayabilen ve bir başka programın varlığına ihtiyaç duymadan çalışabilen hacker yazılımlar. Özellikle evlerdeki PC'leri hedef alan bu sibernetik kurtçuklar, ulaştıkları bilgisayarları esir alarak diğer bilgisayarlardaki işlemlere zarar vermek amacıyla kullanıyor. Bilgisayar uzmanları, esir alınmış ev kullanıcılarının tespit edilebilmesi için yapılması gerekenler konusunda çalışmalarını sürdürüyor. Federal devletin bilgisayar servislerini sağlayan FC Business Systems şirketinden Gregory Peck'e göre İnternet'teki en korkunç kabusa neden olanlar, İnternet üzerinden alışveriş yapmak amacıyla DSL (sürekli bağlantıda olan geniş bant aralığı kapasiteli dijital abonelik hattı) kullanarak 24 saat İnternet'e bağlı kalan kişiler. Çünkü geniş bant aralığı, esir alınmış bir bilgisayarın İnternet'e sayısız pompalama yaparak hedeflenen web sitelerini çökertebilmesi anlamına geliyor.

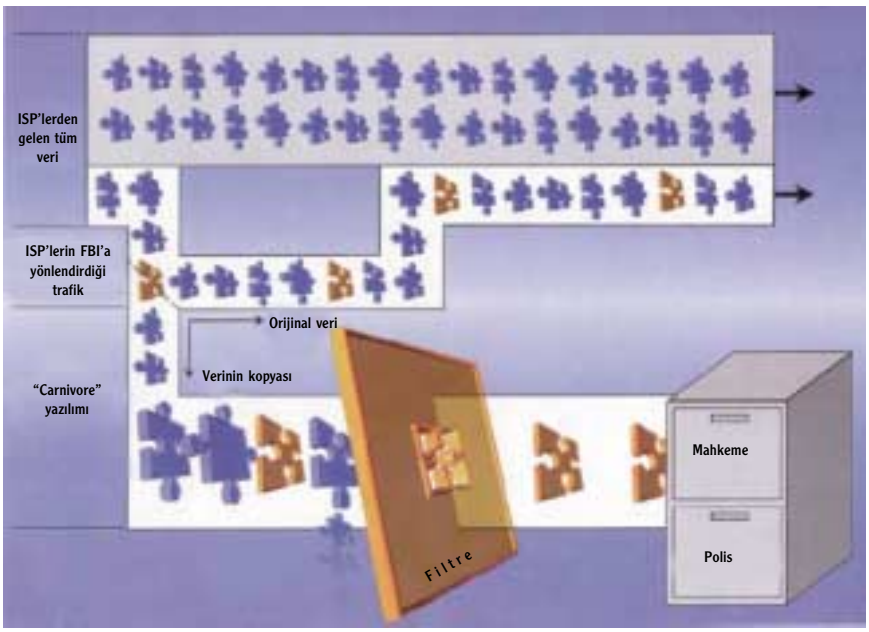


Virüs tarama programlarınızın otomatik olarak güncellenmesine, daima lisanslı yazılım kullanmanıza ya da satıcı firmalardan ürün güncellemeleriyle ilgili sürekli olarak elektronik posta alıyor olmanıza güvenerek, evinizdeki bilgisayarınızın bu saldırılardan uzak ve güvende olduğunu sanıyorsanız, bir kez daha düşünmenizi öneririz. Kullanıcılarını hacker saldırılarından koruma konusunda kendini sorumlu hisseden satıcı sayısı çok az olduğundan, ev kullanıcılarının da bilgisayarlarına koruma duvarı yüklemelerinde oldukça fayda var.

Çoğu yeni kişisel bilgisayar kullanıcısının yakında birçok acemi soketi mümkün kılan Windows XP® işletim sistemini kullanacak olması, güvenlik sorununu daha da karışık hale getiriyor. Soketler, bilginin ağ üzerinde transferini sağlayan paketleri (en küçük veri aktarım birimi) oluşturan yazılım yapıları. Acemi soketlerden oluşan bir teknolojiyle, paketler protokolleri koruyan kuralları ihlal eden herhangi bir mantıkla bile kurulabilir. Ayrıca acemi soketler, hackerların alıcı bir bilgisayarı çökertebilecek yanlış düzenlenmiş paketler oluşturmalarına da olanak sağlar.

Evlerdeki kişisel bilgisayarlara yönelik olarak alınacak tedbirlerin yanısıra, bir diğer yaklaşım da daha çok bilgisayar suçlusunu tutuklamak yolunda. Bugünlerde saldırganlar, içlerinde ulusal açıdan önem taşıyan bazı bilgisayarların da bulunduğu bir dizi bilgisayar üzerinde işlem yaparak tehlike oluşturabiliyor. Bu tür durumlarda sağlıklı kanıtların elde edebilmesi içinse, iki ya da daha fazla ülkenin adalet kurumlarının işbirliği yapması gerekiyor. Bilgisayar suçlarının uluslarası takibinin, bugünlerde aralarında ABD, Kanada ve Japonyanın da bulunduğu Avrupa Birliği üyesi 44 ülke tarafından incelenmekte olan "Siber Suç Anlaşması"nın kabulüyle birlikte daha da kolay hale gelmesi bekleniyor. Bu anlaşma ayrıca, bilgisayar suçu işlemeyi kolaylaştıracak yönerge ve programların, bir bilgisayar sisteminin test edilmesi ya da korunması süreçleri dışındaki aşamalarda üretilmesini ya da kullanılmasını da yasaklıyor. Bir diğer çözüm yolu da İnternet Servis Sağlayıcıları'nın güvenliğini arttırmaktan geçiyor. ABD Federal Ticaret Komisyonu'nun geçtiğimiz Temmuz ayında, finansal hizmet veren şirketlerin kendi ağ altyapılarını önceden tahmin edilen tehditlere karşı korumaları için sunduğu teklif, bu açıdan doğru yönde atılmış bir adımdı.

cı, konuyla ilgili olduğunu düşündüğü kişilerin elektronik iletişimine, beklemeksizin el koyabilecek. Ayrıca İnternet Servis Sağlayıcılar, izinli olmadığını düşündükleri herhangi bir kullanıcının izlenmesi için FBI'dan yardım talep edebilecekler. Tasarı, varlıklarına rağmen böylesine büyük bir terör eyleminin planlanabilmiş ve uygulanabilmiş olmasından ötürü mahçup duruma düşen Echelon, Carnivore ve buna benzer diğer yüksek teknolojili istihbarat sistemlerinin ISP'ler üzerinde kullanımlarının da artırılmasını kapsıyor. Aslında saldırının hemen ardından Carnivore'un çeşitli ISP'ler üzerinde kullanımının artırıldığı yolunda iddialar şimdiden yayılmış durumda. Worldcom ve Yahoo'nun da aralarında bulunduğu bazı önemli İnternet Servis Sağlayıcılar, bu söylentilere henüz karşılık vermedi. Yine yorum yapmayı reddeden Microsoft ve Earthlink'se, gerekli olduğunda yetkililerle işbirliği yaptıklarını kabul ediyor. American Online'ın tavrıysa diğerlerinden farklı: AOL temsilcisi Nicholas Graham, Carnivore'a yanaşmadıklarını, bu sistemi kullanmayı ya da gereklerine uymayı reddettiklerini belirtiyor.



Tepkiler

Devlet yetkilileri siber ortamdaki iletişimi gözetlemek için yapacağı değişikliklerin son halini henüz açıklamış değil. Ancak konuyla ilgili teknoloji uzmanları ve gizlilik savunucuları, yeni gözetleme tasarısının daha uzun vadeli bir bakış açısıyla hazırlanmasını sağlamak amacıyla Kongre'yi daha yavaş ve dikkatli davranması gerektiği yolunda uyarmaya şimdiden başladı. Yeni yasalara tepki olarak birçok sivil toplum kuruluşu biraraya geldi. Aralarında Amerika Sivil Özgürlükler Birliği ve Ulusal Avukatlar Birliği'nin de bulunduğu 150 grup, 300 hukuk profesörü ve 40 bilgisayar mühendisi, taslak üzerinde çalışılırken Amerikan yaşam tarzının çekirdeği olan hak ve özgürlükleri aşındırmamak için çok sakin ve düşünceli davranılması gerektiğini belirten bildiriyi meclise sundu.

Böyle bir kriz anında yapılacak değişikliklerin ABD vatandaşlarının gizlilik haklarına zarar vermemesi için ne yapılması gerektiği, gerçekten de önemli bir soru. Aldığı tepkilere karşılık olarak hükümet, terörle mücadele gücünü kişisel özgürlüklere müdahale etmeden artırmayı hedeflediğini söylüyor. Değişikliği hazırlayanların sözcüsü Kongre üyesi Viet Dinh'e göre, Terörle Mücadele Yasası kapsamında yapılan değişikliklerin tek amacı, devletin terörle başa çıkabilmek için ihtiyacı olanları sağlamak. Dinh ayrıca, gerekli yasa tasarısının gizlilik savunucusu çeşitli kurumların danışmanlığında hazırlandığını belirtiyor. Ancak halen sürmekte olan tepkiler, bu açıklamaların bireysel hak ve özgürlük savunucusu grupları yeteri derecede tatmin etmediğini gösteriyor.

Elektronik Gizlilik Bilgi Merkezi'nin yöneticisi Marc Rotenberg, ısrarcı tavrını sürdürenlerden. Rotenberg'e göre, devletin İnternet üzerinde kontrol mekanizması kurma ve gözetleme yetkisini genişletme talebine göz yumulmamalı. Elektronik Sınır Vakfı kurucularından John Perry Barlows da Amerikan halkının güvenliğinin, kişisel özgürlüklerinden daha önemli olamayacağını söyleyerek, yeni tasarının kişisel özgürlüklerin kaderine yapacağı değişikliklerden yakınıyor. Kontrol düşkünlerinin hayatlarının sonuna kadar 11 Eylül'ün tadını çıkaracağını düşünen Barlow, bunu engellemek için elinden geleni yapması konusunda kamuoyunu uyarıyor.

Yeni tasarının dinleme ve gözetleme konusunda getirdiklerine karşı çıkan grupların özellikle üzerinde durduğu nokta, konuşmaların içeriğiyle ilgili. Gizlilik savunucuları, şüpheliye gelen telefonların kaynaklarının kaydedilmesini makul buluyorlarsa da, bu konuşmaların içeriğinin dinlenmesini onaylamıyorlar. Ayrıca şüphelinin aradığı yerlerle ilgili olarak da bu koşulun geçerli olması gerektiğini savunuyorlar. Yeni tasarıya göreyse, her iki yöntem de herhangi bir arama yetkisi olmaksızın uygulanabilir durumda.

Korkulan diğer bir noktaysa, devletin 11 Eylül'deki saldırıyı kolaylaştırdığını düşünerek varolan şifreleme yasalarını tersine çevirmeye kalkışacak olması. Amerika Gizlilik Vakfı teknoloji yöneticilerinden Richard Smith'e göre bu durum, şifreleme konusundaki tartışmaların yeniden başlamasına neden olacak. Smith, ileri derecede şifreleme kullanılmasına engel olacak bazı tasarıların, iyi niyetli olsalar bile, dijital iletişim özgürlüğünü tehlikeye atacağını düşünüyor.

Yeni tasarının İnternet Servis Sağlayıcıları'nın yetkilerini arttırmayı planlıyor olması, tepki çeken bir diğer konu. Amerika Demokrasi ve Teknoloji Merkezi'nden James Dempsey, izinli olmayan kullanıcılar hakkında ISP'lerin karar verme yetkisine güvenmek yerine, bu tanımı yasanın kendisinin yapması gerektiğini söylüyor.

Tüm bu gruplar, yaşanan tarihi saldırının ardından gereken görevleri yapabilmesi için, devlete karşı biraz sabırlı davranmaları gerektiğini kabul ediyorlar. Ama tepki vermelerini gerektiren bir düzenleme yapıldığında gerekli karşılığı verebilmek için de hepsi hazırolda bekliyor. Adalet Bakanlığı ve

FBI'ın zaten çok geniş gözetleme yetkilerine sahip olduğunu ve hakimlerin gizlice dinleme taleplerini çok nadiren reddettiğini düşünen gizlilik gruplarının bu konudaki tavrı, oldukça kesin görünüyor. Gizlilik savunucuları, devletin güvenlik gereksinimleri ve sivil özgürlükler arasındaki dengeyi doğru ayarlayamaması halinde, bireysel özgürlüklere yapılacak tüm tehditleri yakından izlemede kararlı görünüyorlar.

Gerçekten Gerekli mi?

11 Eylül'de yaşanan saldırılarda teknolojinin ne derece etkin bir rol oynadığı henüz tam olarak anlaşılamadığından, sözü geçen tüm önlemlerin kişisel özgürlükleri sınırlaması bir yana, aslında gereksiz olduğunu düşünenler de var. Bunların en önemli dayanakları da, geçmişte yaşanmış bazı benzer olaylar. Örneğin Oklahoma'daki bombalama olayının hemen ardından, şifreleme teknolojisinin kullanımının sınırlandırılması yolunda çalışmalar başlatılmıştı. Ancak Elektronik Sınır Vakfı'nın resmi yöneticisi Cindy Cohn'a göre, bu saldırılarda şifreleme teknolojisi hiç kullanılmamıştı ve tüm bu girişimler gereksizdi. Dünya Ticaret Merkezi'nin 1993 yılındaki bombalanması olayı sonrasında da, Clinton hükümeti elektronik iletişimin kilitlenebilmesine olanak sağlayan bir şifreleme projesi başlatmıştı. Oysa ki çoğu uzmana göre bu olayda da teknoloji hiç kullanılmamıştı.

Birçok devlet kurumunda bilgisayar ve iletişim güvenliği uzmanlığı yapan Wayne Madsen, bu iddiaları daha da ileriye götürerek, varolan gözetleme teknolojisinin iki katına çıkarılmış olsa bile, 11 Eylül'deki saldırıyı önlemede yetersiz kalabileceğini söylüyor. Saldırıda düşük dereceli teknoloji olanaklarının bile kullanılmadığını düşünen Madsen'a göre, saldırganlar eylemi düzenlemek için teknolojiden ziyade küçük eylem hücreleri ve güvenli evler kullanmış görünüyorlar. Tüm bunlara karşın Madsen, Echelon, Carnivore ve benzer dinleme teknolojilerinin kullanımının artmasını bekliyor. Bu artış, geçmişteki gizlilik ve resmiyet ilkeleri doğrultusunda gerçekleşecek olsa da, bu kulaklar ülke içine çevrildiği andan itibaren, kimsenin gizlilik haklarına sahip olduğunu söylemesi mümkün olmayacak. FBI ve diğer ABD istihbarat servisleriyse, gözetlemenin artırılmasına gerek olup olmadığı konusunda yorum yapmayı reddediyor.

Ayşenur Topçuoğlu

Sizi Bir Yerden Tanıyor muyum?

Teknolojinin gözetleme alanında kullandığı tek silah, kuşkusuz İnternet değil. Kablosuz kameralar, insanları gözündeki iris tabakası, bacak boyu uzunluğu, derisinin yaydığı ışınlar ve hatta adımlarının şiddetinden tanımak amacıyla geliştirilen sistemler de gözetlemeyi her an ve her yerde gerçekleştirmek için çalışıyor. Kablosuz kameralar önceleri yalnızca casuslar, özel detektifler ve güvenlik alanındaki profesyonellerce kullanılırken, şimdilerde bazı şirketlerin Web üzerinde yaptığı yoğun pazarlama çalışmaları sonucunda daha geniş bir kitleye ulaşıyor. Günlük hayat içinde hepimizin uğradığı bankalar, mağazalar, oteller, metrolar ve caddeler bu kameralarla kuşatılmış durumda. Kaydettikleri görüntüleri herhangi bir kabloya ihtiyaç duymaksızın ana merkeze gönderen bu gizli gözler, olası tehlikeli bir durumu önceden tespit etmeyi amaçlıyor. Ailelere çocuklarını kontrol etme ya da posta kutusundaki mektupları kimin çaldığını bulmalarında bir çözüm önerisi olarak sunulan bu kameraların satışını yapan şirketler, reklamlarında kameraların röntgencilik amacıyla kullanılmamaları konusunda uyarıda bulunmayı da unutmuyor. Ancak kullanıcılar bu uyarılara pek kulak asmadığından olsa gerek, X10 kablosuz kamera fanlarının kurduğu sitelerde kameraların yerleştirilmesi için önerilen en ideal yer, genellikle banyolardaki deterjan kutuları.

Röntgencilik tehditini beraberinde getiren kablosuz gizli kameralar, üzerinde çalışılan son projeyle karşılaştırıldığında oldukça basit kalıyor. Şu anda var olan sistemin kamuya yönelik kullanımında, teknoloji yalnızca kapalı devre sistemlerin video sinyallerini alıp ana merkezdeki monitörlere gönderilmesi aşamasında kullanılıyor. Elde edilen görüntülerin izlenip değerlendirilmesiyse, 24 saat ana merkezde görevli kişilerce yapılıyor. Oysa üzerinde çalışılan yeni sistemler, şüpheli kişi ve davranışların belirlenmesi aşamasını da teknolojinin ellerine teslim etmeyi amaçlıyor. Sistemin çalışması için öncelikle psikologlarca suç belirtisi olarak tanımlanan davranış modellerinin ana veri tabanına yüklenmesi gerekiyor. Özel algoritmalar kullanılarak programlanmış bilgisayarlar, yüklenen bu modelleri kaydedilen görüntülerle karşılaştırarak davranışlar üzerinde anında yargıda bulunabiliyor.

Kişileri tanımak için geliştirilen bir diğer teknolojiyse, deriden yayılan renk spektrumunu ölçmek. Farklı insanların derisinin emdiği, yansıttığı ve yaydığı belirli renk modelleri imza yerine geçebilecek kadar belirgin ve birbirbirinden farklı. Ancak bu yöntem, yayılan yüzlerce dalgaboyunun bir alıcı tarafından taranabilmesi için kişinin yaklaşık beş dakika boyunca bir sandalyede oturmasını gerektirdiğinden, pek tercih edilmiyor.

Geliştirilmekte olan bir başka yaklaşım da, bir terziye gitiğinizde verdiğiniz bacak boyu uzunluğu ve bel çevresi kalınlığı gibi ölçülerinizi kullanarak tanınmanızı sağlamak. Bu yöntem üzerinde çalışan uzmanlara göre, bu ölçüler bireylerin tanınmasını sağlayacak bedensel imzalar şeklinde kullanılabilir.

Georgia Teknoloji Enstitüsü'ndeki uzmanlarsa kişileri yürürken attıkları adımların şiddettinden tanıyacak "akıllı zemin sistemi" üzerinde çalışıyor. Hazırlanan gelişmiş veri tabanı, binadaki tüm çalışanlara ve ziyaretçilere ait adımların kayıtlarını içeriyor. Bina içindeki tüm zeminler boyunca döşenen alıcılar, üzerlerinde atılan adımların şiddetini ölçüyor ve bunu veri tabanındaki kayıtlarla karşılaştırıyor. Karşılaştırma sonucunda adımların sistemde kayıtlı olmadığı görülürse, gerekli önlemler alınıyor.

Kişilerin güvenliğini artırmak amacıyla geliştirilmekte olan tüm bu teknolojiler, gizlilik savunucularının saldırılarından payını alıyor. Amerika Kişisel Hak ve Özgürlükler Kurumu'nun başını çektiği savunucular, tüm bu sistemler hayata geçerse toplum düzeninin, George Orwell'in bundan 53 yıl önce yazdığı "1984" adlı romanındakine benzeyeceği yolundaki uyarılarını sürdürüyor. Üstelik bu romanın kahramanı Winston'ın tele-ekrandan kaçabilme şansı varken, günümüz teknolojisinin sunduğu kızılötesi ya da termik kameralar, bizleri gözetlenmediğimiz ufacık bir yaşam alanından bile mahrum bırakabilir.

Kaynaklar

Meinel, C.; "Code for the Web"; Scientific American; Ekim 2001.
Amoto, I.; "Big Brother Logs On"; Technology Review, Eylül 2001.
Tristram, C.; "Behind Blue Eyes"; Technology Review; Mart 2001
Spring, T. ve Thorsberg, F.; "Will Attack Hurt Net Privacy?"; www.pcworld.com, 12 Eylül 2001.
Forno, R.; "What September 11th May Mean To Netizens"; www.securityfocus.com; 18 Eylül 2001
Harrison, A.; "Terror Attacks Revive Crypto Debate"; www.securityfocus.com; 20 Eylül 2001
Jones, J.; "Congress Considers Stronger Cybersurveillance"; www.infoworld.com; 21 Eylül 2001
Poulsen, K.; "Hackers Face Life Imprisonment Under Anti-Terrorism Act"; www.securityfocus.com; 24 Eylül 2001.
MacMillan, R.; "Lawmaker Sounds Computer Security Warning"; Newsbytes, 26 Eylül 2001.
Puzzanghera, J.; "Privacy Advocates Warn That Anti-Terrorism Plans Could Harm Free Society"; Washington Mercury News; 26 Eylül 2001
Phillips, E.; "Congress Debates Security vs. Civil Liberties"; Medill News Service; 2 Ekim 2001.
Poulsen, K.; "Alternative Anti-terror Bill Limits Life Sentence For Hackers"; www.securityfocus.com; 2 Ekim 2001.
Salkever, A.; "A Battle-Ready Net?"; Business Week; 2 Ekim 2001
McGuire, D.; "House Panel Approves Expanded Surveillance Powers"; Newsbytes; 3 Ekim 2001.
Hoffman, L.; "Lawmaker Proposes Creation of Cyber-National Guard"; Scripps Howard News Service; 3 Ekim 2001
"Is your computer being monitored?"; www.cnn.com; 19 Mart 2001
Garfinkel, S.; "The Net Effect"; www.techreview.com