

ENDÜSTRİYEL CASUSLUK VE BİLGİNİN ÇALINMASI

Dersin Adı: Bilişim Etiği ve Hukuk

Öğretim Üyesi: Doç.Dr.Özhan TINGÖY

Hazırlayan: Behlül ÇALIŞKAN

Tarih: 27.12.2006

1. ENDÜSTRİYEL CASUSLUK (SANAYİ CASUSLUĞU)

Endüstriyel casusluk, sanayi devrimi sonrası bir firmanın özel üretim teknolojisini, ürününü veya önemli bir bilgisini, rakip firmalara satılmasıdır. Günümüzde sanayi casusluğu “fuar uzmanlığı” adı altında fotografik hafıza ve çizim yeteneği çok yüksek olan insanlar tarafından da yapılmaktadır.¹

Endüstriyel casusluk, bilgilerin belirli milletler veya çıkar grupları için çalışan casuslar aracılığıyla ele geçirilmesinin hedeflenmesidir.

Burada, hem dost hem de karşı gruplar sürecin içine dahil olmuşlardır. Sık kullanılan endüstriyel casusluk teknikleri, USB hafıza kartları gibi sökülebilir saklama ortamlarındaki açık ve güvensiz USB portları aracılığıyla verilerin izinsiz kopyalanması, belgelerin, üretim tesislerinin, üretim tekniklerinin veya prototiplerin bugünkü yüksek çözünürlü kameralı cep telefonları aracılığıyla resmedilmesi, mektup ve e-postaların ele geçirilmesi, telefonların ve internet bağlantılarının izlenmesidir.

Amaç, bilgilerin önceden ele geçirilmesi ile çıkar sağlamak veya önceden tedbirler almaktır. Endüstriyel casusluğa karşı alınacak önlemlerden biri, USB bağlantılarını seçici olarak bloke eden yazılımların kullanılmasıdır.

Günümüzde Avrupa’da, Amerika Birleşik Devletleri’nin Echelon adlı casusluk sistemi ile Amerikan şirketlerinin yararına sistematik endüstriyel casusluk yürütmesinden korkuluyor.

Sanayi casusluğu son derece önemli sonuçları olan ve şirketlerin ağır ekonomik kayıplara uğramasına neden olan bir olgudur. Sınai araştırmalar uzun zaman ve geniş maddi kaynaklara ihtiyaç duymaktadır. Sınai haklar bu nedenle koruma altına alınmıştır. Eğer sınai haklar üzerinde var olan koruma söz konusu olmasa idi şirketlerin uzun ve pahalı ar-ge faaliyetlerine girişmek için bir motivleri olmazdı. Oysa sınai mülkiyet hakları şirketlere araştırmalarının sonuçlarını paraya tahvil etme imkanı tanımaktadır ve bu nedenle şirketler ar-ge faaliyetlerini bir yatırım olarak görmektedirler. Teknolojik

¹ <http://de.wikipedia.org/wiki/Wirtschaftsspionage>, 26.12.2006

gelişmenin sağlanması ortaya koyulan yeniliklerin, buluşların ve ürünlerin etkin korunması ve sahiplerine özel ayrıcalıklar tanınmasına bağlıdır. Doğal olarak kimi yapılanmalarda başta ekonomik nedenler -ve de askeri ve stratejik nedenler- dolayısıyla “sanayi casusluğu” adı verilen faaliyete yönelmekte ve haksız kazanç peşine düşmektedirler. Sanayi casusluğu şirketlerin ağır ekonomik sonuçlarla karşı karşıya kalmasına sebep olmaktadır. Özellikle genetik, tohum ve yeni bitki türleri geliştirme çalışmaları ve askeri projelere ilişkin faaliyetler (faaliyeti yürüten özel sektör dahi olsa) ulusal düzeyde stratejik önem kazanabilmektedir. Ceza kanunumuzun bu faaliyeti tanımlaması ve yaptırma bağlaması önemli ve yerinde bir gelişmedir. Ayrıca üçüncü bentte düzenlenen zorlama unsurunun üzerinde de durmak gerekmektedir.²

Örnek vaka: Dünyanın en büyük temizlik malzemeleri ve kozmetik devi Procter & Gamble, rakibi Unilever’in ‘endüstriyel casusluk’ suçlamalarından dolayı yasal yollara başvurma girişimini engelledi. Financial Times gazetesinde yer alan bir habere göre, kural dışı yollara başvurarak Unilever’in ürünleriyle ilgili bilgi toplayan Procter & Gamble, Unilever’e 10 milyon dolar ödeyerek davayı engellemeyi kabul etti. Rekabete dayalı bir “istihbarat hareketi” olarak adlandırılan olayda, Procter & Gamble dedektifler aracılığıyla, Unilever’in saç bakım birimi ile ilgili planlarının bulunduğu 80’den fazla dokümanı ele geçirmişti.³

2. BİLGİNİN ÇALINMASI

20 yıl öncesine kadar sanayi casusluğu çok büyük önem taşıyan, kuruluşun içinde büyük sıkıntılara ve kuruluşlar arasında ciddi yasal sorunlara neden olan bir olguydu. Bugün sanayi casusluğu yerini bilgi casusluğuna bıraktı. Artık şirketlerin bilgi birikimleri (know-how) büyük tehdit altında. Özellikle şirket içi ve şirketler arası ağların dışında, bir kurumun bilgilerinin internet vasıtasıyla tüm dünyaya açık hale gelmesi, bilgi casusluğunun sanayi casusluğundan çok daha geniş kapsamlı, tehditkar ve kolay yapılırlı olmasına neden olmaktadır.⁴

² <http://www.musatoprak.av.tr/?act=7&lang=1&textid=8>, 26.12.2006

³ <http://www.ntvmsnbc.com/news/104953.asp>, 09.01.2006

⁴ <http://www.tangram.com.tr/altyazi.htm>, 26.12.2006

Örnek vaka: ABD, bugüne kadar gerçekleşen en büyük mali bilgi hırsızlığını konuşuyor. Bankalar ve şirketler için hesap nakli yapan Arizona merkezli 'CardSystems Solutions' adlı şirketin güvenlik sistemini virüs yardımıyla delen hırsız veya hırsızlar, 40 milyon kişiye ait kredi kartı bilgilerini ele geçirdi. Durum, 'MasterCard International'ın güvenlik biriminin uyarısı üzerine anlaşıldı. Kredi kartlarıyla yapılan dolandırıcılıkları belirleyen uzmanların uyarısı üzerine başlatılan araştırmada 40 milyon kredi kartının risk altında olduğu, bu kartlardan 13.9 milyonunun MasterCard müşterilerine ait olduğu ortaya çıkarıldı.⁵

3. TEKNOLOJİ HIRSIZLIĞI

Teknoloji hırsızlığı, bir birey veya tüzel kişi tarafından geliştirilen, gizli veya korumalı bilgi, taslak, model veya prototip gibi teknolojik bilgilerin kendi kullanımı veya satışı için illegal yoldan elde edilmesidir. Teknoloji hırsızlığı askeri alanda ve özellikle bugün sivil alanda ortaya çıkmaktadır.

Teknoloji hırsızlığı ve endüstriyel casusluk arasındaki fark, teknoloji hırsızlığının yabancı teknolojilerin kullanımını kapsamaması, ama bunun endüstriyel casuslukta zorunlu olmamasıdır. Bu durumda endüstriyel casusluk rakip teknolojinin geliştirme durumu ve teknik imkânlarıyla ilgilenmiş oluyor. Yine teknolojik hırsızlık da casuslukla bağlantılı olmak zorunda değildir. Böyle düşünülürse, korunan bir teknolojinin kopyalanması ve satılması da teknolojik hırsızlık anlamına gelmektedir. Buna günümüzde daha çok korsancılık denir. Teknolojik hırsızlıktan korunmanın en önemli yolu, bilgilerin gizli tutulmasıdır.⁶

4. TASARIM HIRSIZLIĞI

Tasarım hırsızlığı kavramı ile; kendisine ait olmayan ya da harc-ı alem tasarımları kendisininmiş gibi göstererek Türk Patent Enstitüsünden (TPE) endüstriyel tasarım belgesi almayı kastediyoruz. TPE tarafından tasarımlar tescil edilirken şekli inceleme yapılır. Yani TPE, tasarım başvurularını sadece ücretin yatırılıp yatırılmadığı, gerekli

⁵ <http://www.radikal.com.tr/haber.php?haberno=156182>, 09.01.2006

⁶ <http://de.wikipedia.org/wiki/Technologiediebstahl>, 26.12.2006

evrakın verilip verilmediği gibi şekle ilişkin hususlara bakar ve bunlarda bir eksiklik yoksa başvuruyu Resmi Endüstriyel Tasarım Bülteni'nde yayımlar. Yayın tarihinden itibaren 6 aylık askı süresinde başvuruya herkes itiraz edebilir. İtiraz gelirse TPE bu kez, konuyu esas, yani yenilik ve ayırt edici nitelik açısından da inceler. Böylece özgün olmayan tasarımlara belge vermez. İtiraz edilmezse başvuru sahibine Endüstriyel Tasarım Belgesi verilir. Uygulamada Bültenler çok sınırlı bir kesim tarafından takip edildiği için, birçok tasarım başvurusuna haksız yere belge verilmektedir. Sorun da tam burada başlamaktadır.

Resmi Endüstriyel Tasarım Bülteni incelendiğinde yayımlanan (ve tabii belge ile ödüllendirilen) başvurulara konu tasarımların, çok büyük bir kısmı özgün değildir. Hatta herhangi bir sektörü tarihsel olarak incelemek isteyenlere Bültenleri takip etmelerini öneririm. Zira eski Mısır'dan kalma ürün tasarımları için dahi tasarım belgesi alınmaktadır. Oysa kanun koyucunun amacı, yeni ve ayırt edici nitelikte olan, yani özgün tasarımları hukuken koruma altına almaktır. ... 554 sayılı Endüstriyel Tasarımların Korunması Hakkında KHK'ya, 4128 sayılı Kanunla bir madde (m.48/A) ekleyerek şu ifadelerle yer vermiştir: "... kendisini haksız olarak tasarım başvurusu veya tasarım hakkı sahibi olarak gösterenler hakkında bir yıldan iki yıla kadar hapis cezasına ve üç yüz milyon liradan altı yüz milyon liraya kadar para cezasına... hükmolunur". Maddede geçen 300 milyon liradan 600 milyon liraya kadar olan para cezası her yıl artmaktadır. 2003 yılı için bu cezalar; 13 milyar 871 milyon ile 27 milyar 742 milyon TL. olarak uygulanmaktadır. Ayrıca bu kişilere karşı maddi ve manevi tazminat davaları da açılabilir.⁷

5. VERİ HIRSIZLIĞI

Veri hırsızlığı, siber dolandırıcılar tarafından gönderilen, tanınmış firmalardan (bankalar gibi) gönderilmiş gibi görünen, kredi kartı numarası veya şifre gibi gizli bilgileri elde etmeyi amaçlayan e-postalar aracılığıyla yapılır. Bu hileli mesajlar,

⁷ <http://www.etmk.org/haber267.html>, 08.01.2007

kullanıcıdan kurumun web sayfasına giderek kişisel bilgilerini güncellemesini ister. Ancak gidilen sayfa sahtekarların yarattığı resmi web sayfasını taklidir.⁸

Örnek vaka: 28,000 denizcinin ve aile üyelerinin kişisel bilgilerinin bulunduğu 5 adet spreadsheet dosyası bir web sitesinde görüldü. Kişisel bilgiler isim, doğum tarihi ve sosyal güvenlik numaralarını içeriyor.

Deniz Kuvvetleri 22 Haziran'da olaydan haberdar olduklarını ve etkilenenleri durumdan haberdar ettiklerini duyurdu: "Verilerin kanunsuz yollar için kullanıldığı hakkında henüz bir delil yok. Fakat bireyler banka hesaplarını ve kredi kartı verilerini dikkatli olarak monitör etmeli."

Bu durumdan etkilenenlerin kimlik hırsızlığı konusunda bilgilendirilmeleri için gerekenin yapılacağı da söylendi ve NPC (Navy Personnel Command) web sitesine şüpheli durumları nasıl gözlemleyeceklerini anlatan bilgiler eklendi.

Geçtiğimiz hafta Amerikan Ziraat Bakanlığı 26,000 çalışanın kişisel bilgilerinin çalındığını duyurmuştu. Mayıs ayında ise çalınan dizüstü bilgisayarda 26.5 milyon amerikan ordu görevlisinin verileri olduğu duyurulmuştu.⁹

4. İLGİLİ TCK MADDESİ

Endüstriyel casusluğa ve bilginin çalınmasına ilişkin Türk Ceza Kanunu'nda aşağıdaki madde yer almaktadır:

Meslek veya sanata ilişkin sırrın açıklanması

MADDE 241- (1) Sıfat veya görevi veya meslek veya sanatı gereği vakıf olduğu fennî keşif ve buluşları veya sınaî uygulamaya ilişkin bilgileri açıklayan kimseye, suçtan zarar görenin şikâyeti üzerine bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası verilir.

(2) Bu sırlar, Türkiye'de oturmayan bir yabancıya veya onun memurlarına açıklandığı takdirde, faile verilecek ceza üçte biri oranında artırılır. Bu hâlde şikâyet koşulu aranmaz.

⁸ http://www.pandasoftware.com/download/documents/help/pla/2007_nt/tu/915.htm, 08.01.2007

⁹ <http://www.e-hack.org/index.php?print=587>, 08.01.1982

(3) Cebir veya tehditle bir kimseyi sınaî veya ticarî bir sırrı açıklamaya mecbur kılan kişi üç yıldan yedi yıla kadar hapis cezasıyla cezalandırılır.