Bilgi Çağında Bireysel Gizlilik

George Orwell'in Büyük Birader fantezisi gerçeğe mi dönüşüyor? Bilgi teknolojilerinin kullanımının hayatın her alanına girdiği bu yeni çağda en değerli varlığın "bilgi" olduğu artık toplumun her kesimi tarafından kabul edilen önemli bir gerçek; bilgi çağında herkesin "bilgisi kadar güçlü" olacağına kesin gözüyle bakılıyor. Ancak bu gelişmelere rağmen, sıkça göz ardı edilen ciddi bir toplumsal problem çok da uzak olmayan bir gelecekte hayatımızı tehdit edecek gibi görünüyor. Bireysel gizliliğin tehlikeye düşeceği, bir ya da daha fazla Büyük Birader'in her adımımızı gözleyebilir duruma geleceği, bu endişelerin temelini oluşturuyor ve bu endişeler artık dergilerin manşetlerine kadar taşınır oldu.

Bilgi teknolojilerinin hayatın içine artan biçimde girişi, her adımımızın birileri tarafından izlenebilir olması ile sonuçlanıyor. Kredi kartı şirketleri, kredi kartlarımız ile yaptığımız tüm alışverişleri takip ediyor; bu sayede bizler ile ya da alışveriş yaptığımız mağazalar ile kendileri için daha karlı anlaşmalar yapmayı hedefliyor. Kredi kartı şirketleri ile ilgili gizlilik problemlerimiz bu kadarla sınırlı kalmıyor. Şirket bize ait bilgileri, alışverişlerimize ilişkin olanlar dahil olmak üzere, istediği kişi ve kuruluşlara verme ve/veya satma hakkına da sahip. Kredi kartı başvuru formuna eşlik eden sözleşmenin bir maddesi bizleri bunu peşinen kabul etmeye zorluyor. Bu anlaşmalar, temel olarak kredi kartı sağlayıcısına sizin bilgilerinizi dilediği üçüncü şahıslarla paylaşma "hakkını" veriyor. Size hiç tanımadığınız firmalardan doğum günü ya da bayram tebrik kartları gelmiyor mu?

Mağazalar, indirim ve taksitlendirme gibi promosyonlar ile bizleri mağaza kartı sahibi olmaya teşvik ediyor. Mağaza kartları ile yaptığımız her türlü alışverişe ilişkin bilgiler mağazanın bilgisayar sistemlerinde depolanan bizimle ilgili kayda ekleniyor ve bu bilgiler mağazanın daha etkin satış teknikleri geliştirmesi için temel alınıyor. Ancak haftanın hangi günlerinde marketten kaç şişe alkollü içki aldığınızı ya da çocuğunuz olmadığı halde çocuk bezi aldığınızı (evlilik dışı bir ilişkiniz mi var?) birilerinin bilebiliyor olması fazlasıyla rahatsız edici değil mi?

Telefon şirketlerinin durumuna baktığımızda durumun pek de farklı olmadığını görüyoruz. Kullandığımız cep telefonları nedeniyle telefonumuzu açık tuttuğumuz sürece (en azından) hangi baz istasyonunun kapsama alanında olduğumuzun izlenmesi mümkün olabiliyor. Bugün kayıp ya da çalıntı cep telefonlarının bulunmasında kullanılan bu yöntemden faydalanarak, birisinin ne zaman nereye gittiğinin kayıtlarını tutmak olanaklı duruma geliyor. İşyeri ve evlerimizde kullandığımız telefonlar da dahil olmak üzere her telefon görüşmemiz arayan ve aranan numaralar ve zaman bilgisi ile birlikte saklanıyor. Hastanelerde saklanan tıbbi kayıtların durumu ise daha da düşündürücü. Daha önce geçirdiğimiz hastalıklara ve şu andaki sağlık durumumuza ilişkin her türlü bilgi hastane bilgisayarları üzerinde depolanıyor. Sağlık Bakanlığı'nın

Burak DAYIOĞLU
ODTÜ Bilgi İşlem Dairesi
Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü'nden 1998 yılında mezun oldu. Mezuniyetinden önce başlayan iş yaşantısı boyunca özellikle bilgi güvenliği ve ağ temelli uygulamalar konusunda çalıştı. Dizin hizmetleri, açık anahtar altyapıları, saldırı tespiti, e-posta hizmetleri gibi konularda çeşitli büyük ölçekli projelerde yer aldı ve danışmanlık hizmetleri sağladı. Halen ODTÜ Bilgi İslem Dairesi DNS Grubu'nda çalışan Dayıoğlu, ODTÜ Bilgisayar Mühendisliği Bölümü'nde sürdürdüğü yüksek lisans çalışmasını tamamlayarak aynı bölümde doktora çalışmasına başlama hazırlığındadır.

niyetleri çerçevesinde bir biçimde bu bilgilerin merkezileştirilmesi de yakında olmasa da ufukta görünüyor. Bu bilgiler arasında AIDS ya da kanser hastası olduğunuza (Allah korusun ama...) dair bilgilerin de yer alması mümkün ve böylesi bir bilginin gizliliği son derece önemli. Ne yazık ki çoğu hastanede bilgisayar ortamında saklanan hasta kayıtlarına ilişkin özelleşmiş erişim denetimi mekanizmaları bulunmuyor; kimin ne zaman hangi gerekçe ile tıbbi kayıtlarıma erişebileceği ve üzerinde ne gibi işlemler yapmaya yetkili olduğuna ilişkin bilgiler bu sistemlerin parçası olarak mevcut değiller. Herhangi bir doktor, sizin doktorunuz olmasa da, tıbbi kayıtlarınızı inceleyebiliyor ve belki de daha da önemlisi değiştirebiliyor. Doktorlarımızın iyi niyetinden hiç şüphemiz olmasa da yapılabileceklerin potansiyeli fazlası ile düşündürücü değil mi?

İnternet'te gezerken izlendiğinizi hiç düşündünüz mü? Web sitelerinin sizin web istemcinize gönderdiği çerezler aracılığı ile sitenin en son hangi kısmını ve ne zaman ziyaret ettiğinizi takip etmesi ve kayıt altına alması mümkün. Web' de bir çok belgeye ya da programa erişmeden web sunucu tarafından önce bir form doldurarak kişisel bilgilerinizi vermeniz isteniyor. Bu formlar aracılığı ile kişisel bilgilerinizi ne kadar sık açığa vurduğunuzun farkında mısınız? İnternet servis sağlayıcınız, hizmetlerini özelleştirmek ve kaynaklarını daha etkin kullanmak üzere internet üzerindeki her hareketinizi izliyor olabilir mi? İzlerse farkedebilir misiniz ya da engelleyebilir misiniz? Size hiç tanımadığınız firmalardan reklam içerikli e-posta mesajları gelmiyor mu? Sıradan bir iş gününde hiç görmek istemeyeceğim on kadar reklam mesajı alıyorum. Gelen reklamlar arasında bana tatil alternatiflerinden cinsel hayatımı renklendirmek için kullanabileceğim cinsel oyuncaklara varana değin hemen her seçenek var.

E-posta ile ilgili bir diğer problem, e-posta mesaj trafiğinin izlenmesidir. Büyük şirketlerin çoğunluğu, şirket sırlarının dışarı çıkmadığından emin olmak üzere e-posta trafiğini izliyorlar. Geçtiğimiz aylarda Amerika'da sonuçlanan davalarda mahkemeler, şirketlerin çalışanlarının e-posta trafiğini izlemesini makul bulmuş ve daha ötesinde e-posta mesajlarının tümünün şirketin mülkü sayılması gerektiğini ifade etmiştir. İnternet üzerinden bilgisayarınıza yüklenen bir truva atının gizliliğiniz açısından ne denli ciddi bir tehlike oluşturduğunu söylemeye bile gerek yok. Sayıları yüzün üzerinde olan farklı MS-Windows truva atları, tanımadığınız ve sizinle doğrudan ilgisi olmayan birilerinin bilgisayarınızdaki tüm verilere kolayca erişmesine neden olabiliyor. Bu truva atlarından sakınmak için gerekli önlemleri almadığınız taktirde bilgisayarınızın denetimini başkalarına kaptırabilirsiniz.

Bireysel bilgilerimizin depolandığı noktaları saymaya çalışırken, bilgisayar ortamında devlet tarafından saklanan nüfus ve vergi kayıtlarınızdan söz bile etmedim; eminim daha pek çoğunun adı bile geçmedi. Ama önemli olan nokta, bir biçimde izleniyor olduğumuzdur. Masum amaçları olsa da, toplanan bu bilgilerin bir

gün toplayan kuruluşlar ya da ele geçirebilecek bilgisayar korsanları tarafından kötü amaçlar ile kullanılması ihtimali son derece ürkütücüdür. Bunun bir basamak üzerinde, toplanan bilgilerin birleştirilmesi ve böylece yaşantımız ile ilgili her türlü detayın tek noktada incelenebilmesi ve değiştirilebilmesi var ki bu tehditin büyüklüğü beni her seferinde dehşete düşürüyor.

Bu yazıyı, benim hakkımda depolanan muhtelif bilgilere erişebilen ve bu bilgiler üzerinde tahrifat yapabilen bir saldırganın yaşantımı nasıl mahvedebileceği ile ilgili küçük bir fantezi ile sonlandırmak istiyorum. Tıbbi kayıtlarıma erişebilen bir saldırganın ne gibi sonuçlara vesile olabileceğine bir bakalım:
Çok da zor olmayan bir biçimde tıbbi kayıtlarıma erişen saldırgan, kayıtlarımı değiştirerek benim ölümcül bir kanser hastası olduğuma ilişkin bilgileri veri tabanındaki mevcut bilgilerim ile değiştirir. Daha sonra çalıştığım işyerine isimsiz ve imzasız bir mektup ile değiştirilmiş tıbbi kayıtlarımın bir dökümünü gönderir. Bu kayıtlarda yapılan tek tahrifat kanser olduğumun eklenmesinden ibaret olduğundan kayıtlar gerçekten inandırıcıdır; patronum eski rahatsızlıklarımdan bir kısmını da tanır ve belgede yazılanlara inanır. Benim psikolojik sorunlarımın başlayacağını ve zaten bir süre sonra bu hayata elveda diyeceğimi düşünerek -içi parçalansa da- beni kibarca kapı dışarı eder. Bu durumu sevinçle izleyen saldırgan deforme edilmiş tıbbi kayıtlarımı çalıştığım sektördeki tüm firmalara göndererek benim çalışamaz duruma gelmemi ya da en parlak ihtimal ile bir süre işsiz kalmamı sağlayabilir. Bu yazıda anlatılanların hayal ürünü olduğunu ve böylesi bir tehdidin söz konusu olmadığını düşünenler için Amerika Birleşik Devletleri, İngiltere, Kanada ve Yeni Zelanda devletlerinin ulusal istihbarat teşkilatlarının casus uydu sistemi Echelon'dan söz ederek yazıyı noktalamak istiyorum. Bu dört devletin bir araya gelerek oluşturdukları bir ulusal istihbarat birlikteliği, uluslararası her türlü veri iletişimi, faks ve ses trafiğini izleyerek anahtar kelime araması yapmakta ve ilgili iletişimlerin kaydını tutarak bir uzmanın incelemesi için saklamaktadır. Yıllar boyunca varlığı inkar edilen Echelon düzeneği, geçtiğimiz aylarda Avrupa Parlementosu'nun (AP) hazırlığına başladığı ve 18 Mayıs 2001'de taslağını yayınladığı 100 sayfalık bir raporla belgelenmiştir. Bu rapor ile Echelon'un varlığı ilk defa resmi bir kurum tarafından doğrulanmıştır.

Echelon ile ilintili AP raporunun en korkunç kısmı, düzeneğin ulusal güvenliğin korunması ve ulusal istihbarat amaçları için değil, ekonomik avantaj elde etmek üzere bir casus düzeneği olarak kullanıldığı saptamasıdır. Rapordan bir örnek vaka: Avrupalı Airbus Konsorsiyumu 1994 yılında Suudi Arabistan Ulusal Havayolları'na altı milyar dolarlık bir satış yapmak üzereyken, Echelon sayesinde faks ve telefon görüşmeleri dinlenmiş, toplanan bilgiler iki Amerikan firması olan Boeing ve McDonnell-Douglas'a verilmiş. Bu önemli bilgilere sahip olan Amerikan firmalarından birisi işi son anda Airbus Konsorsiyumu'nun elinden almayı başarmış ve altı milyar dolar ABD'ye gitmiş. Her türlü uluslararası ticari faaliyetinizi izleyen bir "grup" ile nasıl baş edilebilir?

Bu konu üzerinde biraz düşündüğünüzde tehditlerin çok ciddi ve sayı olarak çok da fazla olduğunu göreceksiniz. Will Smith'in "Enemy of the State" filminde canlandırdığı karakterin başına neler geldiğini ve hükümeti tarafından nasıl izlendiğini henüz görmediyseniz filmi mutlaka izleyin. Bilişim Çağı'nın bireysel gizliliğimizi önüne geçilemez biçimde nasıl tehlikelere sürüklediğini siz de görün.