Kişisel Bilgilerin Korunması

Elk.Elo.Müh. E: Önder Köktürk
onder@kokturk.com

Ülkemizde kişisel verilerin işlenmesinde yeterli ve açık bir yasal düzenlemenin olmaması ve kişisel verilerin işlenmesi süreçlerini denetleyecek bir kurum bulunmaması, bilgi teknolojilerini bilinçli kullanma konusundaki eksiklikler, verilerin kontrolsüz şekilde işlenmesi, bazı temel hakların ihlal edilmesine sebep olmaktadır.

Günümüzde bilgi ve iletişim teknolojilerinin gelişimine bağlı olarak verileri oluşturmak, erişmek, iletmek ve saklamak günden güne kolaylaşırken, güvenliğini sağlamak ise bir o kadar zorlaşmaya başlamıştır. 5237 nolu Türk Ceza Kanunu'nun "Özel hayat ve gizliliğe" yönelik dokuzuncu bölümünde yer alan 135. madde de kişisel bilgiler için "Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri.." gibi genel bir tanım yapılsa da "Ad ve soyaddan başlayarak, tanımlanmış ya da doğrudan veya dolaylı olarak kişiyle ilişkili her türlü fotoğraf, mesaj, telefon, banka hesap numarası, adres bilgisi, soy ağacı, çalıştığı veya üyesi olduğu kurum, maaş, sicil, sağlık, değerlendirme, mal varlığı ve benzeri ilişkili diğer tüm bilgiler" kişinin "Kişisel bilgileri" olarak değerlendirilir.

Kişisel bilgiler, bireylerin doğumundan ölümüne kadar hayatın her alanında gerek kamu ve gerekse özel sektör (hastane, okul, devlet birimleri..) tarafından yaygın olarak kaydedilmekte, başkalarına aktarılmakta ve paylaşılmaktadır. Bilgisayarlar ve internet sayesinde verilere erişmek bundan 5-10 yıl öncesine göre oldukça kolaylaşmış ve yaşam kalitesini olumlu yönde etkilemesine rağmen, ülkemizde kişisel verileri işlenmesinde yeterli ve açık bir yasal düzenlemenin olmaması ve kişisel verilerin işlenmesi süreçlerini denetleyecek bir kurum bulunmaması, bilgi teknolojilerini bilinçli kullanma konusundaki eksiklikler, verilerin kontrolsüz şekilde işlenmesi, bazı temel hakların ihlal edilmesine sebep olmaktadır. "Türk Ceza Kanunu'nun Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" kapsamında 134, 135 ve 136. maddelerinde kişisel verilerin hukuka aykırı olarak işlenmesi suç sayılmış, ancak hangi hallerde hukuka aykırı veya hangi hallerde hukuka uygun olduğuna dair düzenleme yapılmamıştır.

Kişisel Verilerin Korunması Kanunu Tasarısı ile ilgili ilk çalışmalar 1989 yılında başlamış fakat, 2004 yılına kadar çeşitli tasarılar hazırlansa da sonuçlandırılamamıştır. 2004 yılında Adalet Bakanı'nın oluru ile yeni bir komisyon oluşturularak kamu kurumları, üniversiteler ve sivil toplum örgütleri de dahil olmak üzere 50'den fazla kuruluştan görüş alınarak tasarı düzenlenmiş ve 2006 yılında başbakanlığa gönderilmiştir. Başbakanlık, tasarıyı 2008 yılında Türkiye Büyük Millet Meclisi'ne sevk etmiş ve oradan da sırası ile Adalet ve Adalet Alt Komisyonu'na yönlendirilmiştir. Alt komisyon araya TBMM Seçimleri'nin girmesi nedeniyle çalışmalarına ara vermiş ve süreci yasal sürede tamamlayamadığı için iç tüzük gereğince tasarı hükümsüz sayılmıştır. Kişisel verilerin korunması 2010 yılı anayasa değişikliği ile ilk kez anayasal güvence altına alınmıştır. Bu kapsamda, güncellenmiş Kişisel Verilerin Korunması Kanunu Tasarısı 2012 yılı Haziran ayında başbakanlığa iletilmiştir. İlgili tüm kurumların katkısıyla çalışmalar sürmekte olup, 2013 yılında Bakanlar Kurulu toplantısın-

da gündeme gelen Kişisel Verilerin Saklanması Yasa Tasarısı'nın, bütün özel ve kamu kuruluşlarına kişisel verilerin paylaşımında yeni düzenlemeler getirmesi beklenmektedir. OECD ve Avrupa mevzatına uyum nedeniyle de hazırlanan kişisel veri düzenlemesi, kişisisel verilerin depolanmasını daha kolaylaştırıcı ancak paylaşımını kısıtlayıcıdır.

Basında yer alan taslak tasarıya göre;

- Kişisel Verileri Koruma Kurulu oluşturulacaktır. Bütün kamu ve özel kurumlar kişisel verileri bu kurum izniyle toplayabileceklerdir.

- Bağımsız veri denetim kuruluşları oluşturulacaktır. Bu kuruluşlar kişisel verilerin yanlış kullanımını denetleyecek ve kişilerin isteği üzerine kendileri hakkında yanlış veri toplanıp toplanılmadığını, başka kurumlara aktarılıp aktarılmadığını da araştırabileceklerdir.

- İsim, telefon numarası, araç plakası, pasaport numarası, sosyal güvenlik numarası, TC kimlik no, özgeçmiş, resim, görüntü, parmak izleri, genetik bilgiler, cinsiyet, adres bilgileri tasarıdaki düzenlemelere göre arşivlenebilecek, akli, fiziki, psikolojik özellikler, siyasi düşünce, din, ırk, mezhep bilgileri saklanamayacaktır.

Tasarının yasallaşması sonrası, ilgili tüm kurumların hızlı bir şekilde veri koruma çalışması başlatmak zorunda olacakları belirtilmektedir.

Tasarı ile ilgili çalışmaların ilerlemesi umut ve memnuniyet verici olmakla beraber bilgi güvenliğini sadece yasal ve teknoloji sorunu olarak görmek yanlış olacaktır. Çünkü araştırma ve istatistikler, bilgi güvenliği sürecindeki en zayıf noktanın "İnsan" olduğunu göstermektedir. Kişisel bilgilerin kullanılması, sınıflandırılması ve saklanması esnasındaki tüm süreçlerde bireylerin eğitimi ve bilinçlendirilmesi bilgi güvenliği konusunda olgunluk seviyesinin artmasına ve olası olumsuzlukların azalmasına doğrudan etki edecektir. Yürürlükte olan veya geliştirilecek yeni kanunlar olsa da olumsuz hallerde meydana gelebilecek maddi veya manevi zararların telafi edilemeyeceği asla unutulmamalıdır.

İlk olarak Parola yönetiminden başlayın!

Bilgiler genellikle, bilgisayar ve internet kullanılarak toplanmakta, saklanmakta ve iletilmekte olduğu için öncelikle kimlik yönetimi olarak isimlendirilen kullanıcı adı ve parola kullanımı konusuna dikkat edilmesi gerekmektedir. Pareto İlkesi[1] kapsamına % 20 lik bir etki veya iyileşmenin, % 80 oranında etki veya sonuç vereceği savunulmaktadır. Bu prensipten yola çıkarak Parola seçimlerinde "güçlü" olarak nitelendirilen ve zor tahmin edilen diziler seçerek bilgi güvenliğine önemli katkılar sağlanabilir. Yakın zamanda basında da yer alan hatta içinde Emniyet Genel Müdürlüğü gibi bazı kamu kurumlarındaki kullanıcıların dahil olduğu üzere, "123456" şeklinde kısa ve basit bir parola kullanmanın olumsuz sonuçları bilinmelidir. Dünya genelinde yapılan bilgi güvenliği incelemelerinde bölgesel kültürel farklar olmakla beraber, doğum günü, isim, telefon numarası, doğum tarihi, ev hayvan ismi gibi bilgilerin yüksek oranda parola olarak kullanılması söz konusudur. Gerek sosyal mühendislik[2] çalışmaları gerekse basit parolalar için kırma ve çözme yazılımları sonucu parolalar çözülerek kişisel bilgiler ele geçirilmektedir. Paylaşımlı bilgisayar kullanıcıları, çalışmaları bittiğinde parola ve diğer bilgilerinin makina üzerinde veya internet tarayıcısı içinde saklanmadığına emin olmalıdırlar. Özellikle kurulum gerektirmeyen yaygın web uygulamaları ile işi bittiğinde, uygulamanın menüsünde yer alan güvenli sonlandırma seçeneği ile oturumlarını sonlandırmaları gerekmektedir. Ayrıca web uygulamalarının güvenli bağlantı sağlayan güvenilir sertifika kullanarak https:// ile olması iletişimi güvenli kılacaktır. Küçük harf, büyük harf, sayılar ve diğer sembollerle birlikte en az 9 karakter uzunluğundaki dizilerden oluşturulmuş parolalar, güvenli (kırılması, tahmin etmesi zor anlamında) olarak nitelendirilmektedir. Güvenli parolaların ekran, klavye üstüne yapıştırılmış küçük kağıtlarda veya herkesin ulaşabileceği dosyalarda yer almaması ve sosyal mühendislik kapsamında üçüncü şahıslar tarafından ele geçirilebilir olmamasına dikkat edilmesi gerekmektedir. Bunlara ilaveten bilgisayarlarda (cep telefonlarında) bu bilgileri kullanırken istenmeyen (solucanlar, tuş kaydedidici...) zararlı yazılımlara karşı da korunmak gerekmektedir.

Zararlı yazılımlardan nasıl korunabiliriz?

Genellikle (windows, android, linux.. gibi) platformlara özel olarak üretilmiş Antivirüs veya Endpoint Internet Güvenliği adı altında ücretli veya ücretsiz yazılımlar vardır. Bu yazılımların mutlaka kullanılması ve işletim sistemleri ile birlikte güncel sürümlerinin bulunması ön şarttır. Antivirüs yazılımlarının % 100 bir koruma sağlayamayacağı asla unutulmamalıdır. Çünkü zararlı yazılımlar büyük oranda uygulamaların veya işletim sistemlerinin yazılım açıklarını veya zayıflıklarını kullanarak bulaşmaya çalışırlar. Yama adı verilen güvenlik açıklarını tamir eden güncellemelerin düzenli olarak yapılması büyük önem taşımaktadır. Hayatı kolaylaştırsa da taşınabilir bellekler bir makinadan başka bir makinaya zararlı yazılım bulaştırmak için sık kullanılan birimlerdir. Ayrıca bu belleklerin küçük ve kolay taşınabilir olmaları nedeniyle çalınması sonucunda da bilgi sızıntısı veya kaybı yaşanması ile sık karşılaşılmaktadır. Zararlı yazılımların bir diğer önemli bulaşma nedeni, korsan indirme veya P2P4 olarak adlandırılan dosya paylaşım siteleri üzerinden dağıtılan içine zararlı kod zerk edilmiş lisansız yazılımlardır. İndirilen yazılımların büyük bir bölümü yapısal değişiklik ve gizleme yöntemleri ile antivirüs ve güvenlik yazılımlarını devre dışı bırakmakta veya tespit edilememektedir. İşletim sistemi seviyesinde kendini gizleyerek çalışabilen bu tip çok zararlı yazılımlar, arka planda bilgisayarı kötü niyetli şahısların kontrölüne teslim etmektedir. Bu durumda bilgisayar sizin bilginiz ve kontrolunuz dışında kötü amaçlara hizmet edecek "BotNet"olarak isimlendirilen köleleştirilmiş ordunun bir üyesi olacaktır. Siber yeraltı dünyasında onlarca bilgisayardan üretilen binlerce hatta onbinlerce köle bilgisayar ordusu, çok düşük fiyatlara satılmakta veya kiralanmaktadır. Bu kapsamda kişisel bilgiler risk altında olduğu gibi, bir başkası sistem üzerinden bir siber suç işliyor olabilir. Tespit durumunda bilgisayarınız, internet hattınız ve IP adresiniz[3] servis sağlayıcı üzerinden sizi adreslediği için olası bir hukusal süreçte sorumluluk size ait olabilir.

Hayatımızı oldukça kolaylaştıran ve kullanım konforunu arttıran kablosuz bağlantı teknolojilerinde riskler yüksek olduğu unutulmamalıdır. Güvenlik ayarları iyi yapılmamış veya yeterince güçlü parola ve kriptolama teknikleri kullanılmamış bir erişim noktası saatli bombadan farksızdır. Özellikle Ortadaki adam (Man-in-the-Middle) olarak adlandırılan araya girme atağı sonucu, başka bir şahıs, trafiği kendi üzerinden geçirerek bilgilere ulaşabilir, değişiklik yapabilir. Otel, açık alan gibi ortak alanlardaki kablosuz erişimleri sorgusuz sualsiz kullanmadan önce biraz düşünmek fayda sağlayacaktır.

Bir yanda tehditlerin çeşitliliği diğer yanda bu sistemleri kullanmak durumunda olmak, içinden çıkılması zor bir bilmece gibi de olsa, yazıda anlatılan ana noktalara dikkat etmek, bilinçli bir kullanıcı olmak, bizleri ve kişisel bilgilerimizi korumada önemli farkındalık ve avantajlar sağlayacaktır.

[1]. Pareto ilkesi, iş yönetimi düşünürü Joseph Juran'ın öne sürdüğü "çoğu olay için, etkilerin kabaca % 80'nin etkenlerin % 20'sinden kaynaklandığına ait" tezidir. Bu ilke aynı zamanda 80/20 veya 20/80 oranı olarakta bilinir. http://tr.wikipedia.org/wiki/Pareto_%C4%B0lkesi

[2]. Sosyal mühendislik genellikle bilgi toplama, dolandırıcılık yada bilgisayar sistemlerine erişmek amacı ile hile ve aldatma yolu ile bilgi toplama sanatı olarak ifade edilir. http://en.wikipedia.org/wiki/Social_engineering_(security)

[3]. IP adresi: Internet üzerinde TCP/IP protokolü üzerinden haberleşmeyi sağlayan x.y.z.t olarak Versiyon 4 notasyonunda 0 ile 255 arasındaki sayılardan oluşturulmuş sayı dizileridir.

4. P2P Peer-to-Peer olarak adlandırılan kişisel sistemlerin internet üzerinden birbirleri ile dosya alış verişi yapmasına imkan veren yazılımlardır. Bittorent, gnutella, dDonkey ve Emule yaygın olarak bilinmektedir.