KİŞİSEL VERİLERİN KORUNMASI

Oldouz Karimi[1], Adem KORKMAZ[2]

[1] İstanbul Üniversitesi, Enformatik Bölümü, İstanbul

[2] Kilis 7 Aralık Üniversitesi, Enformatik Bölümü, Kilis

oldooz_karimi@yahoo.com, adem@kilis.edu.tr

Özet: Bilgi teknolojisinin ve iletişimin hızla geliştiği günümüz dünyasında, kişilik hakları zarar görebilmektedir. Özellikle kişilik haklarının bir parçası olan kişisel verilerin elektronik ortamda işlenmesi, işleniş şekli ve bu bilgilerin paylaşımı noktasında son dönemde meydana gelen ilerlemeler gerek uluslararası gerekse ulusal alanlarda birçok hukuki düzenlemenin yapılmasına sebep olmuştur. 21. Yüzyılda her türlü bilgi serbest dolaşabilmeli, ancak kişiye bağlı temel haklar da korunmalıdır. Belirtilen çerçeve doğrultusunda hazırlanan bu çalışma, giriş ve kişisel veri, kişi ve kişisel verilerin saklanması ve kişisel verilerin korunmasında oluşmaktadır

Anahtar Sözcükler: kişisel veri, kişi, Güvenlik, Kişisel Bilgilerin Gizliliği

Abstract:

In this study it has been emphasized the protection of persons, respect their fundamental rights and freedoms, notably the right to privacy and the protection of personal data and the processing of such data, which is one of the main principle for a democratic and modern state. The progress made in information technology is making the processing and exchange of such personal data considerably easier, therefore the protection of personal data is getting even harder day by day. In the 21st century every kind of data should be able to flow freely, but also the fundamental rights of individuals should be safeguarded. Because of that, a lot of countries especially in Europe which are also the member of EU accepted new rules and regulations on this issue.

The study consists of an introduction and the terms of the personal data, person and the protection of such data are studied.

1. Giriş

Teknolojinin hızla geliştiği, kişilerin, toplumların ve ülkelerin ekonomik, sosyal, kültürel olarak birbirine iyice yaklaştığı günümüz dünyasında, birey kendi kişisel alanını ve haklarını korumakta daha da zorlanır hale gelmiştir.

Modern hukuk düzenleri en yüksek değer olarak kişiyi kabul etmişlerdir. İkinci Dünya Savaşı ile baskıcı rejimlerin tarih sahnesinden silinmesi sonucu kişiliğin, devlet karşısında yüceltilmesi gereken bir değer olduğu bilincine varan modern yasa koyucular, bu amaç çerçevesinde hukuk düzenlerini hem ulusal hem de uluslararası alanda inşa etmişlerdir(1)(2).

Gelişen teknoloji karşısında daha önce sadece tozlu dosyalarda ve arşivlerde hapsedilen ve sınırlı sayıda insanın ulaşabildiği bazı kişisel veriler günümüzde sadece birkaç bilgisayar tuşu mesafesi kadar yaklaşmıştır. Bu doğrultuda, günümüz dünyasında hak sahibinin rızası dışında bir başkasının eline geçebilecek bu tür bilgilerin muhafazası ve kimlerin hangi koşullarda bu bilgileri toplayabileceği ve bir başka kişi ya da kuruma aktarabileceği önemli bir konu haline gelmiştir.(2)

Son yıllardaki teknolojik ilerleme, kişiye teknik yönden hem kolaylıklar sağlayarak hem de zorluklar yükleyerek kişiliğin korunmasındaki tartışmaları disiplinler arası bir alana çekmiştir. Bu tartışmaların yürütülmesinde itici ivme teknik ilerleme ile şeffaflaşan hayat alanlarımızın korunması kaygısı olmuştur. Zira kişilik hakkı, ister gerçekleşmiş ister gerçekleşmemiş bulunsun her saldırı karşısında korunmak istenmiştir. Bu sebeple, modern yasa koyucular özel hukukun sunduğu olanakları yeni teknolojilerin yarattığı muhtemel saldırılar karşısında saldırı öncesi koruma bakımından güçlendirmişlerdir(1)(2).

2. KİŞİSEL VERİ KAVRAMI

Haberleşme araçlarının akıl almaz boyutlarda gelişmesi, kişisel veri ve bilgilerin korunması sorununu da gündeme getirmiştir. Bu doğrultuda ulusal ve Uluslararası kuruluşlar konunun üzerinde durmaya başlamışlardır. Bilgi toplumunda kişisel bilgiler, ilgili kişilere zarar vermeyecek doğrultuda kullanılmalıdır. Kişisel bilgilerin korunması sorunu, bunların açıklanmasının kişiye verebileceği zarardan kaynaklanmaktadır(3)

Birey ve kurumlara özgü, hangi bilgilerin korunması gerektiğini belirtmeden önce, bireysel bilgilerin neler olabileceği ve bu bilgiler kullanılarak neler yapılabileceği konusu üzerinde durmakta yarar vardır. Kişilerin kendilerinin konu oldukları bilgilere, "isme bağlı veriler" veya "bireysel veriler" denilmektedir. İsme bağlı veriler, örgütler tarafından depo edilmekte, işlenerek bilgi haline getirilmekte, talep halinde üçüncü kişilere devredilmektedir. Bu dolaşım bazen sınır ötesine de uzanmaktadır. Toplumsal örgütler ve bazı serbest meslekler grupları kişisel veri toplayıcısıdır. Toplumsal örgütler kapsamına ise en başta devlet olmak üzere çeşitli kamu kuruluşları, özel hukuk kesiminde kâr amaçlı kuruluşlar, sivil toplum kuruluşları girmektedir.(2)

Meslekler kapsamında ise günlük hayatımızdan bildiğimiz doktorluk, avukatlık, noterlik, bankacılık gibi meslekler bu kapsamda sayılabilir. Kısacası, toplumda hemen herkes bilgi toplamakta değerlendirmekte ve bunları değişime tabi tutmaktadır.(4)

Bu tür bilgilerin, günümüzde yoğun olarak kullanıldığı alanlardan bazı somut örnekler aşağıda sıralanmıştır. Kimlik Bilgileri, Adres Bilgileri, Kredi Kartı Bilgileri, Telefon Bilgileri, Telefon Rehberi Bilgileri, Elektronik Posta Bilgileri (İnternet Bilgileri) , Emniyet ve Jandarma Birimlerindeki Bilgiler.

3. KİŞİ KAVRAMI

Kişi, haklardan yararlanan, hak sahibi olan varlık demektir. Hukuk, kişi olma özelliğini önce insana tanımıştır. Kanun koyucu, insanların yanında toplum ihtiyaçlarına cevap verebilmek için, hak ve yükümlülükleri diğer

bazı insan veya mal topluluklarına da yöneltmiştir(5).
Hukukta gerçek kişi dediğimiz insanın yanı sıra tüzel kişi olarak tanımlanan Bazı insan ve mal topluluklarına da hak sahibi olabilme ve borçlanabilme yetisinin verildiğine yukarıda değinmiştik. Tüzel kişi, fiziki varlığı bulunmayıp, varsayıma dayanan ve belli bir amacın gerçekleştirilmesi için organize olmuş insan veya mal topluluklarıdır. Sanal kişi de denen tüzel kişiler, hak ve sorumluluk sahibi olma bakımından aynen insan gibi kabul edilmektedir(6).
Kişisel verilerin korunması kapsamında kişi kavramının içeriğine kimlerin gireceğine ilişkin olarak uluslararası doktrin ve mevzuatta bir görüş birliği bulunmamaktadır (7)(2). Nitekim, bir görüşe göre, veri koruma yasalarının kapsamına, yalnızca gerçek kişilere ilişkin bilgiler girebilirken, diğer bir görüş ise tüzel kişilere ait bilgilerin de kişisel veri niteliği taşıyabileceğini savunmaktadır (8).

4. Günümüzde kişisel verilerin korunması

Günümüzde, modern iletişim araçları vasıtasıyla bilginin toplanıp depolanarak, kişiler, kurumlar ve hatta ülkeler arasında paylaşılması kolaylaşmıştır. Bu durum, kişisel
verileri elinde bulunduran kimseler ile bu verilerin ilgili oldukları kimseler arasındaki menfaat dengesini veri sahipleri aleyhine bozmuştur. Nitekim, bu tür bilgilere erişim kolaylaştıkça, veri sahiplerinin maddi ve manevi varlıkları aynı oranda zarar görmeye başlamış ve menfaatlerinin korunması ihtiyacı ortaya çıkmıştır. Ayrıca, çağdaş toplumlarda insan haklarına verilen önem de, kişilik hakkı çerçevesinde değerlendirilen kişisel verilerin korunması ihtiyacını perçinlemiştir. Bu bağlamda, kişisel verilerin korunması meselesi, çağdaş toplumlarda çeşitli ulusal ve uluslararası düzenlemelere konu edilmiştir.(9)

5. İnternette İletişim Türleri

Kişilerin duygu, düşünce yada bilgilerini herhangi bir yolla başkasına transferine iletişim denir.İletişimde kişinin konuşma şekli , kullandığı kelimeler , beden dili , jest ve mimikleri, ses vurgusu önem taşır.Mesela: Elektronik posta; İngilizce ismi olan "e-mail" de çok kullanılır. “Haber grupları bir çeşit ileti saklama alanı olarak çalışan iletişim ortamlarıdır. Her ne kadar haber grubu ismi sınırlayıcı bir tanım olsa da gerçekte haber grupları kalıcı tartışma platformları olarak kullanılmaktadırlar. Dosya aktarım iletişim kuralı, (İngilizce: File Transfer Protocol; FTP), bir veri yığınının - ASCII, EBCDIC, ve binary- bir uç aygıttan diğerine iletimi için kullanılmaktadır. Telnet, Internet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir. Web patlamasından kısa bir süre öncesine kadar Gopher internete girmek için kullanılan grafik arayüze sahip tek yöntemdi. World Wide Web (kısaca WWW veya web):Web’in temeli İnternettir. Web İnternet üzerinde kurulmuştur ve İnternetin sunduğu mekanizmalardan çoğunun kullanılmasını sağlar.

6. Siber Uzay

Yeni milenyum ile internet hayatımızın çok önemli bir parçası olmuştur. E-ticaret, e-posta, e-devlet gibi "E-"(elektronik) önekine sahip kavramlar ile İnternet ile beraber hayatımıza bir anda giren kavramlardır. İnternet’i etkin olarak kullandığımız 10-15 sene gibi bir süre zarfında içerisinde "Siber" kelimesi geçen birçok yeni kavram daha ortaya çıkmıştır. Siber uzay, siber silah, siber güvenlik, siber casusluk siber savaş gibi. Bu kavramlar ve ifade ediliş biçimleri şu şekildedir. Amerikan Savunma bakanlığınca: “İnternet’in bulunduğu, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan” olarak tanımlanmıştır. Diğer bir tanımlama da ise şu şekilde geçmektedir: “insanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma

durumudur" (10)

7. Siber Suçlar

Türk yazınında kavramsal olarak henüz görüş birliğine varılamayan ve"bilgisayar suçları", "internet suçları", "siber suç" veya "bilişim suçları" olarak adlandırılan suçlar için, Dünya'daki tek düzenleme olan Avrupa Konseyi Siber Suç Sözleşmesi'nin adına uygun olması ve uluslararası hukukta yaygın olarak kullanılması nedeniyle bu çalışmada kavramsal olarak "siber suç" ifadesi tercih edilmiştir(11).

Siber suç, bir bilgisayar, ağ veya donanım cihazı kullanılmak suretiyle,elektronik ortamda hukuka aykırı olarak gerçekleştirilen her tür fiil olarak tanımlanabilir. 1980'li yıllardan sonra bilgisayar ve İnternet kullanımının yaygınlaşması ile birlikte, siber suçların sadece ekonomik boyutlarının olmadığı ve bu tür suçların en az ekonomi kadar önemli, diğer bazı değerler aleyhine de işlenebileceği anlaşılmıştır. Bunun sonucu olarak da bu suçların ayrı bir disiplin altında incelenmesi gereği ortaya çıkmıştır.

Bir kişiye ait isim, adres, telefon veya sosyal güvenlik numarası veya aile hayatına ilişkin kişisel veriler çoğu kez veri sahibinin bilgisi ve isteği dışında yayılabilmektedir. Böyle durumlarda, bilgilerin milyonlarca sayıda iletilmesi ya da çoğaltılması saniyelerle ifade edilmektedir. Klasik ceza hukukunda suç aracı olan herhangi bir vasıta gibi kişisel verilerin de, üçüncü kişilerin tasarrufuna girdiği anda suç aracı olarak kullanılma riski doğmuş olmaktadır. Klasik suça göre daha hızlı ve kolay işlenebilen siber suçun tespit edilmesi ve bu suç tespit edilse bile failin yakalanması her zaman mümkün olamamaktadır.

Siber suçları, geleneksel anlamdaki suçlardan ayıran özelliklerden en önemlisi, bu suçların işleniş şekillerinin (modus operandi) tespitinin zorluğudur. Söz konusu suçlar, yepyeni ve çok farklı yollarla işlenebilmektedirler(11).Çoğu kez ilk etapta kişisel verilerin çalınması, ikinci etapta ise bu verilerin kullanılması suretiyle suç işlendiğinden siber suçlar genellikle zincirleme şekilde gelişmektedir.Kişisel verilerin elde edilmesi için işlenen hırsızlık suçu sanal veya fiziki ortamda gerçekleşebilmektedir.

8.Kişisel Verileri Edinme Yöntemleri ve Siber Suç Türleri

Kimlik hırsızlığı

Kimlik hırsızlığı, gerçek veya tüzel kişilere ait kişisel bilgilerin yetkisiz kişilerce, dolandırıcılık veya diğer suçların işlenmesinde kullanılmak üzere ele geçirilmesi, iletilmesi (transferi), muhafaza edilmesi veya kullanılması olarak tanımlanabilir(9). Son yıllarda sıkça rastlanmaya başlayan veri kayıpları, dikkatleri kamu ve özel sektörde teknolojik gelişmelerle artan kimlik hırsızlığı ve kişisel verilerin korunması kavramına çevirmiştir.Kimlik hırsızlığı konusunda farkındalık arttıkça, şüphesiz tüketicilerin de kişisel bilgilerini paylaşırken tereddütleri artmaktadır.Avrupa Komisyonu, bu nedenle Veri Koruma Direktifini yeniden gözden geçirme çalışmalarını başlattığını açıklamıştır.Kimlik hırsızlığı, klasik veya çevrimiçi olmak üzere iki farklı ortamda işlenebilmektedir.(12) **Klasik (off-line) kimlik hırsızlığı:**Kimlik hırsızları veri elde etmek için her tür yola başvurmaktadırlar. Bu yollardan biri de insanlar arasındaki iletişim ve insan davranışındaki açıklardan faydalanarak güvenlik süreçlerini atlatma olarak adlandırılan *sosyal mühendisliktir***.** Bu kavram, kişileri gizli bilgilerini vermeleri için aldatmak olarak da tanımlanabilir. Etkileme, zorlama, aldatıcı ilişkiler geliştirme, sosyal mühendislik saldırı araçlarındandır. Kimlik hırsızlığında bu yöntemler sıkça kullanılmaktadır.

Klasik kimlik hırsızlığı yöntemleri:

i-Çöp karıştırma (dumpster diving): Çöpe atılmış her tür çek yaprağı, kredi kartı, banka sözleşmesi, fatura veya kişisel veri içeren ve elektronik ya da diğer araçlarda yer alan kayıtları elde etmek için bu kayıtları incelemeye çöp karıştırma denilmektedir. Hırsızlar bu iş için çöp toplayıcılarla menfaat karşılığı işbirliği yapmaktadır.ABD'de bu

konuda hazırlanmış 1997 tarihli bir Kanun bulunmaktadır.

ii-Bahane yaratma (pretexting): Bir banka, telefon şirketi veya diğer bir bilgi kaynağını arayarak, belli bir müşteri gibi davranıp herhangi bir şifre ya da başka bir bilgiyi elde etmek için kullanılan sosyal mühendislik yöntemidir.

iii- Omuz üstünden seyir (shoulder surfing): ATM cihazı veya diğer şifre girilen ekranları gizlice izleyerek şifre çalma yöntemidir.

iv-Tarama (Skimming): Kredi kartlarının arkasındaki manyetik verileri elde ederek sahte kartlara ekleme şeklinde yapılmaktadır.

v- İş kayıtları hırsızlığı: İşyerlerindeki bilgisayar veya dosyaların çalınması veya bu bilgilerin elde edilmesidir.Bu hırsızlık yönteminde, çalışanlara rüşvet vs. menfaat sağlayarak bilgi edinilebilmektedir.

Çevrimiçi (on-line) kimlik hırsızlığı:Çevrimiçi ortamda kullanılan kimlik hırsızlığı yöntemleri, belirli sayıyla sınırlı değildir.Zira bu yöntemler günden güne değişebilmektedir.Bu çalışmada örnekleyici olmak üzere çeşitli çevrimiçi kimlik hırsızlığı yöntemleri hakkında bilgi verilmektedir.Suç unsuru taşıyan yöntemlerle elde edilen bu veriler, elde edildikten sonra başka suçların işlenmesinde de kullanılabilmektedir.Bu tür kimlik hırsızlığı, eticaret faaliyetleri sırasında tüketicilerin güvenlerinin sarsılmasına neden olmaktadır.Günümüzde, çevrimiçi ortamda kişisel verileri elde etmek için;

i. Kötü niyetli yazılım veya programlar (malware)

Yaygın olarak virüs, truva atı, bukalemun, çerezler olarak karşılaşılan kimlik hırsızlığı yöntemlerinden cep telefonu, sabit telefon veya bilgisayarlara yüklenen yazılım veya programlar aşağıda incelenmektedir.

ii. Aldatıcı nitelikte e-posta veya İnternet siteleri

1) Oltalama (Phishing):

Phishing, bir işletme, banka ya da devlet kurumundan geliyormuş izlenimi yaratılan bir e-posta ya da aslını kopya eden bir İnternet sitesi (mirror web site) aracılığıyla, kişilere ait kredi kartı bilgisi, şifre, diğer hesap bilgileri vb. çalmayı amaçlayan bir İnternet dolandırıcılığıdır. Oltalama saldırılarının 2007'de ABD'de tüketici ve işletmelere maliyetinin 2,1 milyar dolar olduğu tahmin edilmektedir .

2) İstenmeyen elektronik posta (spam):

Genellikle zararlı bir içeriğe sahip olan ve istenmeyen, alıcıya iradesi dışında gönderilen elektronik mesajlardır. Bu mesajlar, BİT'in gelişimine ve yayılımına paralel olarak tüm dünyada giderek büyüyen sorunların başında gelmektedir.

iii. Sistem veya yazılımların açıkları (hacking) kullanılmaktadır.

"Korsan saldırı" olarak da Türkçe'ye çevrilebilecek "hacking" kavramı, elektronik sistemler veya bilgisayar açıklarından yararlanmak suretiyle kişisel verileri çalmak için kullanılan en yaygın yöntemlerden biridir. İzinsiz ve hukuka aykırı bir şekilde kişisel verilerin çalınmasını sağlayan bir diğer yöntem de kırma (cracking)80 yöntemidir. Kişisel veri elde etmenin yanısıra, sistemin ücretsizkullanılmasını da sağlayan bu yöntemler, bilgisayar korsanlarını (hacker) bilgisayarla ilgili sahtecilik gibi daha tehlikeli suçlara teşvik edebilir(11)(12).

Kişisel verilerin suistimali: Ticari ya da meslek sırları, ya da diğer değerli kişisel bilgilerin kişinin kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek amacıyla kullanılması, satılması ve dağıtılmasına *kişisel verilerin suistimali* denilmektedir.

Banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan büyük miktardaki kişisel bilgilerin ticari değeri ile ilgili suistimaller önemli siber suçların işlenmesinde basamak görevi görürler.

İletişimin gözetlenmesi ve denetlenmesi:

Ulusal güvenliğin sağlanması, suçun önceden tespit edilebilmesi ve yargılama esnasında delil olarak kullanılabilmesi amacıyla kovuşturma organları tarafından genellikle gizli izleme sistemleri kullanılmaktadır. İletişimin bu şekilde gözetlenmesi ve denetlenmesi, ilgili hukuki usul ve esaslara ve zorunluluk unsuruna uygun olarak yapılmalı

ve elde edilen veriler gerekirse anonimleştirilmelidir.

İletişimin gözetlenmesi ve denetlenmesi uluslararası alanda da başta istihbarat olmak üzere çeşitli nedenlerle yapılabilmektedir.Bütün dünya üzerindeki uydu tabanlı iletişimi izleyen beş devletin[1]gizli servislerinin ortaklaşa kurdukları ECHELON sistemi (Büyük Kulak) telefon görüşmeleri, faks, telsiz, İnternet, elektronik posta trafiği dahil olmak üzere tüm iletişim araçlarını dünya çapında dinleme ve kaydetme kapasitesine sahip bir sistemdir. Sistem sayesinde elde edilen ham veriler özel bir mekanizma sayesinde çözümlenmekte ve iletişimin içeriği bu şekilde öğrenilmektedir.Temel amacı ulusal güvenliği sağlamak olmasına rağmen ticari ve diğer sırların, sistem içinde yer alan devletler tarafından haksız olarak kullanıldığı ve diğer devletlere ait stratejik bilgilerin de elde edildiği bilinmektedir.ECHELON sisteminin dünya İnternet trafiğinin yüzde 90'ını kontrol ettiği de verilen istatistikler arasındadır(14).

Günümüzde, istasyonlar, parklar, kamusal yollar, caddeler gibi herkesin ulaşabileceği kamusal alanlarda optik ve elektronik donanımlar vasıtasıyla gözetleme yapılabilmektedir.Bu alanların video ile gözetlenmesi bütün yurttaşların temel haklarını ilgilendirdiğinden sıkı hukuksal koşullara bağlanması gerekmektedir(13).

Veri madenciliği (data mining):

Veri madenciliği, veri yığınları arasından istatistik ve matematik teknikleri kullanılarak verilerdeki gizli örüntüleri çözmeye yarayan, fark edilmesi güç ilişkileri açığa çıkaran, ileriye yönelik tahminler yapılmasını sağlayan ve bu alanda kurallar üreten veri tabanı teknolojisi ve tekniklerinin uygulamasını ifade etmektedir. Kısaca veri madenciliği, veri tabanlarından elde edilen bilgiyi yapılandırarak, bilgi keşfedilmesini sağlayan araçlar ve teknikler olarak nitelendirilebilir.

Günümüzde kurumlara ait veritabanlarında milyonlarca kişiye ait bilgi depolanmaktadır. Bu verilerle birtakım analizlerin otomatikleştirilmiş sistemler vasıtasıyla yapılması gerekliliği, veriye erişimi, en az verinin kendisi kadar önemli hale getirmiş ve veri madenciliği uygulamaları gündeme gelmiştir. Veri madenciliği iyi niyetlerle kullanılabileceği gibi, kişisel verilerin elde edilerek çeşitli şekillerde kötüye kullanılmasına da sebep olabilmektedir.(12)

Sahte kişilik oluşturma ve kişilik taklidi: Kişilik taklidi, gerçek kişilere ait bilgilerin kullanılarak suç işlenmesi ve o kişinin bu suçun faili durumuna düşmesi ile sonuçlanan eylemdir. Kredi kartı numara oluşturucu programlar gibi araçlar kullanılarak elde edilecek gerçek bilgiler, bazen de hayali kişiler oluşturulmasında kullanılmakta, böylece haksız menfaat sağlanarak kişilere zarar verilmektedir.

Sahte internet sitesi (Pharming):Türkçe'de bilinen bir karşılığı olmayan pharming ifadesi "sahte İnternet sitesi" olarak kullanılabilir. Sanal dünyanın dolandırıcıları tarafından tasarlanan ve bir İnternet sitesinin çevrimiçi hesap ödeme sayfasıymış gibi görünen sahte İnternet sayfası ile kişilerin bilgilerinin çalınmasına "pharming" denilmektedir.

Hesap ve aboneliklerin kötüye kullanılması: Veri hırsızları, kurbanlarının kredi kartı, çek, yatırım, telefon (sabit ve mobil), İnternet ödeme, e-posta ve diğer İnternet hesaplarını, sosyal sigorta numaralarıyla sağlık güvencelerini kullanmak suretiyle istismar edebilmektedirler. Bununla birlikte, elde edilen bilgiler telefon, kredi kartı, kredi, çek ve yatırım, İnternet ödeme, otomobil sigortası ile ilgili yeni hesapların açılmasında da kullanılabilmektedir. Bir suça ilişkin soruşturma ve kovuşturma evrelerinde, tıbbi tedavi için, ev veya işyeri kiralarken, işe girerken vb. durumlarda da başkalarına ait kişisel veriler kullanılabilmektedir.(12)

9.Kişisel Verilerin Kötüye Kullanılmasında ve Siber Suçla Mücadelede Alınacak Tedbirler

Veri hırsızlıkları, fiziksel ve bilgi işlem güvenliğine yeterince önem

[1] Bu beş devlet ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda'dır

verilmemesi,dizüstü bilgisayar hırsızlıkları, korsan faaliyetler, şirket çalışanlarının veri sızdırması gibi farklı şekillerde gerçekleşebilmektedir.

Siber suç ve veri hırsızlıklarında farkındalığı artırmaya yönelik olarak son yıllarda önleyici, caydırıcılığı artırıcı ve koruyucu birtakım önlemler alınmaktadır.Bu tedbirlerden *önleyici* nitelikte olanların başarısı, yalnızca bilgi teknolojileri okuryazarlığının artırılması ile mümkün değildir.Bireyin farklı ortamlardaki davranışlarının mahremiyete yönelik etkilerinin farkında olabilmesi ve tehlikeleri öngörebilmesi oldukça önemlidir.Bu sebeple, kişilerin mağduriyete uğramadan önce neler yapmaları gerektiği konusunda bilgilendirilmeleri ve bilinçlendirilmeleri faaliyetleri önleyici niteliktedir.

Mahremiyet artıcı teknolojiler, kimlik doğrulamada sağladığı avantaj nedeniyle mahremiyetin korunmasında *elektronik imza* ve güvenlik ve veri gizliliğinin sağlanmasında *akıllı kartlar* koruma ve özellikle maddi zararın azaltılmasında günümüzde yaygınlaşmaya başlayan tedbirlerdendir. Koruyucu nitelikteki bu tedbirler aşağıda incelenmektedir.

Mahremiyet artırıcı teknolojiler: Temel amacı; mahremiyet kanunlarının ya da ilkelerinin uygulanmasına yardımcı olmak, kişiyi belirlenebilir kılan verilerin toplanması veya bu verilerin daha ileri düzeylerde işlenmesini mümkün olduğunca aza indirgemek olan teknolojik çözüm araçlarına mahremiyet artırıcı teknolojiler[2] (MAT) denilmektedir.Bu teknolojiler, kullanıcıya verilerinin çevrimiçi ortamda ifşa edilmesi, yayılması ve kullanılması riskine karşı kontrol imkanı sağlamaktadır. Bu kontrol, herhangi bir ağ üzerindeki tarayıcılarda veya e-postalarda kişisel verilerin belirli durum ve şartlarda anonim hale getirilmesi, çerezlerin veya diğer izleme teknolojilerinin filtrelenmesi, verinin yayılması şartlarının belirlenmesi, verilerin şifrelenmesi vb. seçenekler ile gerçekleşmektedir.

"Güvenlik teknolojileri" ve "mahremiyet artırıcı teknolojiler" olarak ifade edilen araçlar arasında sıkı bir ilişki bulunmaktadır. Mahremiyetin korunabilmesi için güvenliğin de iyi sağlanması gerekmektedir.MAT'lar, kişisel verilerin küresel alanda çevrimiçi akışında (e-ticaret faaliyetleri gibi) kullanıcıların kişisel verilerini verirken duydukları endişeyi kısmen azaltmaktadır.Genellikle tüketiciler için tasarlanan MAT'ların bazı türleri ise, kurumlar ve işletmelerin mahremiyet politika ve uygulamalarına yardımcı olmak için tasarlanmaktadır.

Elektronik imza (e-İmza):Kimlik doğrulama, neredeyse bütün hukuki işlemlerin gerçekleştirilmesinde ilk adımı oluşturmaktadır. Bu nedenle elektronik hizmet sunumunda kimlik doğrulama araçlarından sağlıklı olanlar tercih edilmelidir.

Elektronik imza; bilginin, orijinalliği bozulmadan, tarafların kimliğini de belirleyebilecek şekilde elektronik ortamda karşı tarafa aktarılmasını garanti eden bir teknolojidir.

Akıllı kartlar: Akıllı kartlar,elektronik imza altyapılarında ve gizliliğinin korunması gereken bilgilerin taşınmasında sıklıkla kullanılan donanımlardır.Bu kartlar, gizli bilgilerin taşınması amacıyla kullanılabileceği gibi, şifreli yayınlara erişim gibi elektronik şifreleme vb. bazı özel fonksiyonları yerine getirmede veya GSM telefonları veya kredi kartlarında kullanılabilir.

Akıllı kartlar,gizli bilgilerin korunması ve bu bilgilerle işlem yapılması konusunda güvenli yapılardır. Bu nedenle söz konusu kartlar, elektronik imzanın gizliliğinin korunması gereken bazı uygulamalarında (örneğin, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verilerin korunmasında) yaygın ola kullanılmaktadır. Bu kartlar, kimlik tespiti gerektiren hizmetlerin sunumunda da oldukça güvenli araçlar olarak kabul edilmektedir.(12)

[2] Privacy Enhancing Technologies (PET)

10. Kişisel Bilgilerin Gizliliği

Bilgi güvenliği, bir bilginin yetkisiz kişilerce ele geçirilmesini,yetkisiz kişilerce değiştirilmesini engelleme ve bilgiye yetkili kişilerin istenilen zamanda ve istenilen kalitede erişmesini sağlama anlamına gelmektedir(15).Kaza veya kasta dayalı güvenlik risklerine karşı bir ağın ya da bilgi sisteminin karşı koyabilme kapasitesi, kişisel verilerin korunması ile sıkı sıkıya ilişkilidir.Zira kişisel veriler, devletlerin geliştirdikleri bilgi güvenliği strateji ve politikaları içinde korunması gerekli görülen en önemli bilgilerdendir.

Ağ ve bilgi güvenliği konusu, pratikte siber suç, kişisel veri koruma yasaları ve telekomünikasyon alanında yapılan düzenlemelerle iç içe geçmiş durumda olduğundan, bu konuya ilişkin alınacak politika tedbirlerinin de mevcut telekomünikasyon, veri koruma ve siber suç politikalarından bağımsız düşünülmemesi gerekmektedir.

Dünyadaki mahremiyet ve veri koruma kanunlarında da ağ ve bilgi güvenliğine ilişkin hükümler bulunabilmektedir.Bu hükümler genellikle kişisel veri kontrolörü[3] veya işleyicisi olan kurum ve kuruluşların uymaları gereken yükümlülükleri belirtmektedir. Bu yükümlülüklere örnek olarak; ilgili kurum ve kuruluş içindeki birimlerin hangi verileri nasıl kullanacakları konusunun açıkça belirlenmesi, verilerin kullanılabilmesi için gereken talimatların açık ve net olması veri işleyenlerin veri koruma ve bilgi güvenliği kanunları hakkında bilgilendirilmeleri, bu kişilerin görev ve yetkilerinin düzenlenmesi ile veri işlemelerinin kaydının en fazla tutulacağı sürenin belirtilmesi sayılabilir.

AB Komisyonunun 2001 yılında Konsey'e yönelik bildirisinde bu durum,aşağıdaki şema ile izah edilmeye çalışılmış ve bu üç politika alanının nasıl bir ilişki içinde oldukları örneklendirilmiştir.

Şekil 1. 1. Bilgi Güvenliği Politika Alanları ve Etkileşim(16)

Bir veritabanında korunması gereken veriler değişik öncelik ve gruplara göre tasnif edilebilir.Bilgi güvenliğinin sağlanmasında teknik araçlar ve teknolojik güvenlik çözümlerinden genellikle virüsleri yok etme, ağ problemlerini giderme, yetkisiz kullanıcıların erişim yetkisini sınırlandırma yöntemleri kullanılmaktadır.Kişisel verilerin korunması hukuku ise, kişiye ait verilerin mümkün olduğunca teknik araçlarla korunması ile bu bilgilerin istenmeyen şekillerde kullanılmasının önüne geçecek hukuki ve sosyal tedbirlerin alınmasını ve nihayet bireyin kendisine ait verilerin kullanılması sürecinde söz sahibi olmasını hedeflemektedir.Kişisel verilerin kötüye kullanılması da genellikle bir bilgi güvenliği sorunudur.Eğer bir sistemde kişisel veri yoksa, sadece bilgi güvenliği önemli hale gelecektir.

Tüm dünya da kabul edilen yaygın bir yaklaşımla bilgi güvenliğinin sağlanabilmesi için aşağıdaki şartların yerine getirilmesi gerekmektedir.

- Önemli ve hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmesi önlenmelidir ve sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğu garanti altına alınmalıdır (Confidentiality -Gizlilik).
- Bilginin sahibi dışındaki kişilerce değiştirilmesinin ve silinmesinin önlenmesi gerekmektedir (Integrity – Bütünlük).
- Bilgi veya bilgi sistemleri sürekli kullanıma hazır ve kesintisiz çalışır durumda olmalıdır (Availability – Sürekli Kullanılabilirlik).
- Kullanıcı kimliğinin doğrulanması

[3] Veri kontrolörünün tanımı, bu çalışmanın 3'üncü bölümündeki "Veri Koruma Direktifindeki temel kavramlar" kısmında yapılmıştır.

(Authentication) gerekmektedir.

Araştırmalar göstermektedir ki; sadece teknolojik önlemlerle (virüsleri tespit eden yazılımlar, güvenlik duvarı sistemleri, kriptolama vb.) iş süreçlerinde yukarıda belirtilen maddeleri içeren bilgi güvenliğinin tam olarak sağlanması mümkün olamamaktadır. Bilgi güvenliği, süreçlerin ayrılmaz bir parçası olmalı ve bu bakımdan bir iş anlayışı, yönetim ve kişisel/kurumsal kültür açısından ele alınmalıdır.Elektronik ortamlarda yapılan işlem sayısının ve çeşitliliğinin günden güne artış göstermesi, kişisel verilerin korunması ve gizliliğinin sağlanması konusunda yeni önlemler alınması ve düzenlemeler yapılmasını zorunlu hale getirmiştir. Kişisel verilerin işlenmesini yaygınlaştırarak bu verilerin elektronik ortamlarda kullanılması zorunlu hale gelirken, diğer yandan da hakkında veri toplanan kişinin kişilik haklarının korunması gerekmektedir(17).

Güvenlik Politikasının Yazılması:

Güvenlik ihtiyaçları belirlendikten sonra, güvenlik politikasında yeralması gereken noktalar ortaya çıkmıştır. Güvenlik politikalarında genellikle aşağıdaki bölümler yeralır:

1. Giriş mektubu:

Genellikle Genel Müdür veya şirket yönetiminden yetkili bir kişinin imzasını taşıyan böyle bir mektup, Güvenlik Politikasına verilen yönetim desteğini göstermek için önemlidir.

2. Amaç:

Bu noktada güvenlik politikasının hangi amaçla hazırlandığı, kimler tarafından kullanılacağı ve kullanımının kimler tarafından izleneceği açık ve net şekilde belirtilmelidir.

3. Yetki ve Sorumluluklar:

Yukarıdaki Amaç bölümünde belirtilen kullanıcı ve yöneticilerin, Güvenlik politikası çerçevesindeki yetki ve sorumlulukları belirtilir. Bu, kullanıcı ve yöneticilerin yetki ve sorumluluklarını belirtmenin yanı sıra, yetkili kişilerin veya yetkili pozisyonların da açık tarifini yapmalıdır.

4. Bilgisayar ve Internet kullanımı:

Bu bölüm, kurumun bilgisayarlarının ve bilgi işlem sistemlerinin kullanımı hakkında genel kullanım kuralları içerir. Bu bölümde, örneğin Internet'e hangi kullanıcıların gireceği, Internet'ten hangi tür dosyaların indirilmesine izin verilebileceği, kullanıcıların hangi durumlarda ne gibi sorumlulukları olduğu belirtilir.

5. Erişim kontrolü:

Bu bölümde, kimlik belirleme, onaylama, şifrelerin belirlenme ve kullanılma kuralları, hesap yönetimi, şirket dışı personel tarafından (örneğin bayiler) şirket kaynaklarına ulaşım hakları gibi alanlar düzenlenir.

6. E-posta:

Bu bölümde, belirli durumlarda e-postaların izlenebilmesi, e-postaların şifrelenmesi, mesajların arşivlenmesi gibi e-posta kullanım kuralları belirlenir.

7. Laptop, PDA ve Benzeri mobil cihazların kullanımı:

Laptop ve PDA gibi mobil cihazlar, şirket bilgilerini şirket sınırları dışında taşıdıklarından, bilgi işlem sistemleri için önemli açıklar içerebilmektedir. Bu nedenle mobil cihazlarda hangi koruma ve güvenlik yöntemlerinin kullanılacağı bu bölümde belirlenmelidir.

8. Internet Güvenliği:

Bu alanda Internet kullanım saatleri, kuralları, Internet'ten HTTP veya FTP protokolleri ile ile hangi dosya tiplerinin Internet'ten indirilebileceği gibi noktalar belirtilir. Ayrıca kurum elemanlarının VPN gibi bir teknoloji ile Internet üzerinden kurum sistemlerine nasıl ulaşacağı, şifreleme yöntemleri irdelenir.

9. Ağ Güvenliği

Router, Firewall gibi ağ güvenliği ürünlerinin kullanımı, Internet üzerinden, VPN benzeri teknolojileri kullanarak şubeler arası bilgi paylaşımı, modem kullanımı gibi konular bu bölümde yeralır.

10. Fiziksel Güvenlik:

Binaya, server odalarına erişimin nasıl olacağı, kullanıcıların iş istasyonlarının zimmet kuralları, ağ altyapısı gibi konular bu bölümde yeralır.

sonuç

Günümüzün gelişen teknolojisi dikkate alındığında kişisel verilerin eskisine oranla daha büyük bir hızda ve oranda gizliliğinin, mahremiyetinin ve bütünlüğünün riske girdiği aşikardır.Dolayısı ile kişilerin bu hususa yeterince özen ve önem göstermeleri son derece önemlidir.Bu çerçevede kişilerin ve kurumların bilgi güvenliği konusunda bilinçlendirilmesi ve bilgilendirilmesi, olabilecek muhtemel sorunların en aza indirilmesine katkı sağlayacaktır. Toplumlarda bilgi teknolojileri kullanımının giderek artması, bilgisayar sistemlerine uzaktan erişimin olağan hale gelmesi ve Internet'in yaygınlaşması, bilgi güvenliği konusunun önemini artırmıştır.

Bu noktada öncelikle kişisel verilerin korunması kanunun bir an önce çıkarılması ve bağımsız bir Kişisel Verilerin Korunması Denetleme Kurumunun oluşturulması gerekmektedir. Ayrıca, veri koruması konusunun önemi dikkate alındığında, bilimsel alanda çalışmaların henüz yeterli çeşitlilikte ortaya çıkmadığı bir gerçektir. Oysa Türkiye'nin sağlıklı bir veri koruması politikası oluşturması AB hedefinin olmazsa olmaz şartlarındandır.

Günlük hayatta karşılaştığımız özel hukuka tabi bir çok iş ve işlem ile çevrimiçi hizmetlerin görüldüğü e-devlet uygulamalarıyla gündeme gelen kişisel veri ve mahremiyet kavramları, bazı *idari*, *yasal* ve *teknik* tedbirler ile korunmayı gerektirmektedir.Bu tedbirlerin, çevrimiçi hizmetlerin sunulmasından önce tasarlanması ve uygulanması, e-devlet hizmetlerinin sunumunda en ideal ve yerinde olanıdır.

Kaynaklar

[1] BAŞALP, N, Kişisel Verilerin Korunması ve Saklanması,Yetkin Yayınları, Ankara, 2004, s.21

[2] Dinç,E, Kişisel Verilerin Korunması Uluslar Arası Düzenlemeler ve Türkiye'nin Durumu,2006.

[3] TORTOP, N.,"Çağımızın Önemli Sorunu:Kişisel Bilgilerin Güvenliği Sorunu", Amme İdaresi Dergisi, cilt 33, Sayı3, Eylül 2000, s.1.

[4] AKILLIOĞLU, T.,"İdari Usul Ve Kişisel Verilerin Korunması", http://www.idare.gen.tr/akillioglu-idariusul.htm, 06-05-200

[5] ÖZTAN,B., Medeni Hukukun Temel İlkeleri, Turhan Kitabevi, Ankara 1999, s.181.

[6] OKANDAN, R.,Umumi Amme Hukuku, İ.Ü. Hukuk Fakültesi Yayınları, No:250, İstanbul, 1966, s.866.

[7] Bu konudaki müspet ve menfi görüşlere ilişkin olarak bkz. WALDEN/SAVAGE, s. 341-346;

[8] AKSOY , Hüseyin Can Kişisel Verilerin Korunmasında, Ankara 2008.

[9] OECD, "OECD Policy Guidance on Online Identity Theft". Haziran 2008

[10] Hildreth, S. A., "CyberwarfareCongressionalResearch Service Report forCongress", Congressional Research Service &The Library (2001), http://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html

[11] TURHAN, Oğuz, "Bilgisayar Ağları ile İlgili Suçlar", (DPT Uzmanlık Tezi), Ankara, 2006.

[12] **Yüksek Civelek**, dilek , Kişisel Verilerin Korunması ve Bir Kurumsal yapılanma önerisi ,Nisan 2011.

[13] **ŞİMŞEK**, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, 1. Baskı, Beta Yayınları, İstanbul, Şubat 2008.

[14] **BECENİ**, Yasin, "Siber Uzayda Mahremiyet", II. Türkiye Bilişim Şurası Hukuk Çalışma Grubu, Mart 2004, (çevrimiçi) http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf, 22 Ocak 2009.

[15] "Bilgiçağı" dergisi, Hayrettin Bahşi ile röportaj. "Kolaylık, Güvenlik Riskini de Getiriyor". Kasım 2008. s.12

[16] Kaynak: Commission of the European Communities, COM (2001) 298 final, s. 3, <http://www.justice.gov/criminal/cybercrime/intl/netsec_comm.pdf>.

[17] ERSOY, a.g.m., s.4 ERSOY,E., "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", http://ab.org.tr/ab06/bildiri/6.doc,10.04.2006