TÜRKİYEDE BİLGİ VE İLETİŞİM TEKNOLOJİLERİNDE BİLGİ GÜVENLİĞİ

Dilek ÇELEBİOĞLU

UZMANLIK TEZİ

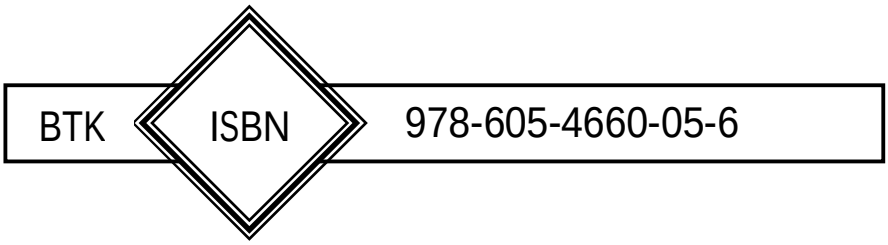
TELEKOMÜNİKASYON KURUMU

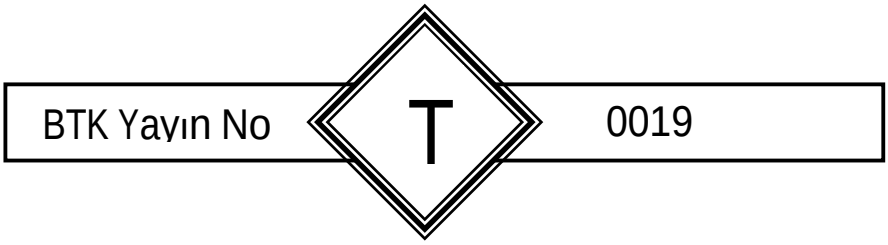
Şubat 2005

Ankara

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.





Dilek ÇELEBİOĞLU tarafından hazırlanan "TÜRKİYE'DE BİLGİ VE İLETİŞİM TEKNOLOJİLERİNDE BİLGİ GÜVENLİĞİ" adlı bu tezin Uzmanlık tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Mustafa ALKAN
Tez Yöneticisi

Bu çalışma jürimiz tarafından Uzmanlık tezi olarak kabul edilmiştir.

Başkan	:	Ahmet Hamdi ATALAY	
Üye	:	Prof. Dr. Derviş Z. DENİZ	
Üye	:	Doç. Dr. Atilla ÖZGİT	
Üye	:	Doç. Dr. Mustafa ALKAN	
Üye	:	Ö. Faruk KOÇAK	
Üye	:	Hüseyin ÇETİN	
Üye	:	Müminhan BİLGİN	

Bu tez, Telekomünikasyon Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

TÜRKİYE'DE BİLGİ VE İLETİŞİM TEKNOLOJİLERİNDE BİLGİ GÜVENLİĞİ

(Uzmanlık Tezi)

Dilek ÇELEBİOĞLU
TELEKOMÜNİKASYON KURUMU
Şubat 2005

ÖZET

Bu çalışmada, bilgi güvenliğinin genel tanımı yapılarak, bilgi güvenliğinin temel unsuru olan kişisel verilerin korunması ve mahremiyetin sağlanması ile güvenlik kültürüne ilişkin hususlar incelenmiştir. Ülkemizin üyesi olduğu ve Kurumumuzun çalışmalarını yakından takip ettiği uluslararası kuruluşlardan Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Avrupa Birliği (AB) ve Uluslararası Telekomünikasyon Birliği (ITU) tarafından geliştirilen ilkeler, düzenlemeler ile bunları esas alan ülke uygulamalarından en iyi örnekler seçilmiştir. Bu kapsamda, Türkiye'deki mevcut durum değerlendirilmeye çalışılmış ve bu konuda önümüzdeki dönemlere ilişkin öneriler ortaya konulmuştur.

Anahtar Kelimeler : Bilgi güvenliği, kişisel verilerin korunması, güvenlik kültürü
Sayfa Adedi : 137
Tez Yöneticisi : Doç. Dr. Mustafa ALKAN

DATA PROTECTION IN THE INFORMATION AND COMMUNICATION TECHNOLOGIES IN TURKEY

(Expert Thesis)

Dilek ÇELEBİOĞLU
TELECOMMUNICATIONS AUTHORITY
February 2005

ABSTRACT

In this thesis, the related issues on the security culture and providing protection of privacy and protection of the personal data as being the essential element of the information security by making general definition of the information security have been considered. The principles and regulations developed by the Organization for Economic Cooperation and Development (OECD), the European Union (EU) and the International Telecommunication Union (ITU) which our country is a member and our Authority follows closely their studies, and the best examples of the country implementations which are based on these have been selected. In this context, the current status in Turkey has been tried to be evaluated and the proposals for the next future on this issue have been arised.

Key Words : Information security, protection of personal data, security culture
Number of Page : 137
Thesis Advisor : Assoc. Prof. Dr. Mustafa ALKAN

TEŞEKKÜR

Tez çalışmam boyunca değerli görüş ve katkılarından dolayı tez danışmanım Sayın Doç. Dr. Mustafa ALKAN'a, Daire Başkanım Sayın Ö. Faruk KOÇAK'a ve Sayın Köksal ÖZENÇ'e, gösterdikleri anlayıştan dolayı Uluslararası İlişkiler ve AB ile Koordinasyon Dairesi çalışanlarına, her zaman desteğini hissettiğim sevgili eşim Mehmet Hanifi ÇELEBİOĞLU'na, sonsuz anlayış ve sabır gösteren kızlarım Merve ve Gökçe'ye ve manevi desteklerini esirgemeyen tüm aileme içten teşekkürü borç bilirim.

ÇİZELGELER LİSTESİ

ÇİZELGELER LİSTESİ

ŞEKİLLER LİSTESİ

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılan simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltma	**Açıklama**
AB	Avrupa Birliği
AB	Adalet Bakanlığı
ABD	Amerika Birleşik Devletleri
ABGS	Avrupa Birliği Genel Sekreterliği
ACA	Avustralya Haberleşme Kurumu Australian Communications Authority
ACCC	Avustralya Rekabet ve Tüketici Komisyonu Australian Competition and Consumer Commission
AGIMO	Avustralya Bilgi Yönetimi Ofisi Australian Goverment Information Management Office
ART	Fransa Telekomünikasyon Otoritesi The French Telecommunications Regulation Authority
AusCERT	Avustralya Bilgisayar Acil Durum Müdahale Ekibi Australian Computer Emergency Response Team
BDSG	Federal Veri Koruma Yasası Federal Data Protection Act- Bundesdatenschutzgesetz
BSI	Enformasyon Teknolojileri Güvenlik Kurumu Bundesant für Sicherheit in der Information Stechnik
CERT	Bilgisayar Acil Durum Müdahale Ekibi Computer Emergency Response Team
CIP	Kritik Altyapı Koruma Critical Infrastructure Protection
CNIL	Medeni Haklar Enformasyon Teknolojisi Ulusal Komisyonu National Commisison on Information Technology and Civil Liberties
DMA	Doğrudan Pazarlama Birliği Direct Marketing Association
DPA	Veri Koruma Yasası Data Protection Act
DPT	Devlet Planlama Teşkilatı
DSD	Savunma Sinyalleri Müdürlüğü Defence Signals Directorate
DTI	Sanayi ve Ticaret Bakanlığı Department of Trade and Industry

EAÜ	Elektronik Araştırma Ünitesi
EDPS	Avrupa Veri Koruma Kurumu European Data Protection Supervisor
E-MPS	E-Mail Tercih Servisi E-Mail Preference Service
ENISA	Avrupa Şebeke ve Bilgi Güvenliği Kurumu Europa Network and Information Security Agency
EU	Avrupa Birliği European Union
FCC	Federal Haberleşme Komisyonu Federal Communication Commission
FPS	Faks Tercih Servisi Fax Preference Service
FTC	Federal Ticaret Komisyonu Federal Trade Commission
GCH	Kamu Haberleşmesi Merkezi Government Communications Headquarters
GSM	Global System for Mobile Communications Küresel Mobil Haberleşme Sistemi
GPS	Küresel Konum Bulma Sistemi Global Positioning System
IBM	Uluslararası İş Makinaları International Business Machines
ICO	Bilgi Görevlisi Information Commissioner
IDC	Uluslararası Veri Şirketi International Data Corporation
IP	İnternet Protokolü Internet Protocol
ISDN	Tümleşik Hizmetler Sayısal Şebekesi Integrated Services Digital Network
ISO/IEC	Uluslararası Standart Organizasyonu/Uluslararası Elektroteknik Komitesi International Organization for Standardization/ International Electrotechnical Committee
ITU	Uluslararası Telekomünikasyon Birliği International Telecommunication Union
ITU-D	Uluslararası Telekomünikasyon Birliği-Telekomünikasyon Kalkınma Sektörü International Telecommunication Union-Telecommunication Development Sector
ITU-R	Uluslararası Telekomünikasyon Birliği-Radyokomünikasyon Sektörü

	International Telecommunication Union-Radiocommunication Sector
ITU-T	Uluslararası Telekomünikasyon Birliği-Telekomünikasyon Standardizasyon Sektörü International Telecommunication Union-Telecommunication Standardization Sector
İSS	İnternet Servis Sağlayıcı
MMS	Çokluortam Mesaj Sistemi Multimedia Messaging System
MoU	Mutabakat Zaptı Memorandum of Understanding
NSA	Ulusal Güvenlik Kurumu National Security Agency
OECD	Ekonomik İşbirliği ve Kalkınma Teşkilatı Organisation for Economic Cooperation and Development
OFCOM	Haberleşme Ofisi Office of Communications
PC	Kişisel Bilgisayar Personal Computer
PET	Mahremiyet Artırıcı Teknolojiler Privacy Enhancing Technologies
PP	Tam Yetkili Temsilciler Konferansı Plenipotentiary Conference
Reg TP	Almanya Telekomünikasyon ve Posta Kurumu The Regulatory Authority for Telecommunications and Posts
SMS	Kısa Mesaj Servisi Short Message Service
TASO	Türk Anti Spam Organizasyonu
TBD	Türkiye Bilişim Derneği
TBV	Türkiye Bilişim Vakfı
TCP/IP	İletim Kontrol Protolü/ İnternet Protokolü Transmission Control Protocol/Internet Protocol
TDSG	Telekomünikasyon Hizmetlerinde Veri Koruma Kanunu Teledienstedatenschutzgesetz
TEMPEST	Geçici Emisyon ve İstenmeyen Transmisyon Temporary Emission and Spurious Transmission
TISN	Kritik Altyapı Koruması için Güvenli Bilgi Paylaşım Şebekesi Trusted Information Sharing Network for Critical Infrastructure Protection
TK	Telekomünikasyon Kurumu
TKG	Telekomünikasyon Kanunu

	Telecommunication Act
TPS	Telefon Tercih Servisi
	Telefone Preference Service
TSE	Türk Standartları Enstitüsü
TÜBİSAD	Türkiye Bilişim Sanayicileri ve İşadamları Derneği
TÜBİTAK	Türkiye Bilimsel ve Teknik Araştırma Kurumu
TTGV	Türkiye Teknoloji Geliştirme Vakfı
TZV	Türkiye Zeka Vakfı
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UPS	Kesintisiz Güç Kaynağı
	Uninterruptible Power Supply
UWG	Haksız Rekabet Kanunu
	Gesetzgegen unlauteren Wettbewerb

1. GİRİŞ

Günümüzde, gelişmiş ülkeler başta olmak üzere, bilgi toplumu olma yolunda hızlı bir değişim süreci yaşanmaktadır. Bu süreçte etkin rol oynayan bilgi ve iletişim teknolojileri, iletişim, elektronik bankacılık, elektronik ticaret, eğitim, kamu hizmetleri ve savunma sistemleri gibi pek çok alanda yer alarak günlük yaşamı bütünüyle değiştirmeye başlamıştır.

Zaman ve mekan farklılıklarının etkisini ortadan kaldıran, çalışma, ticaret, eğitim ve eğlence biçimlerine yeni boyutlar kazandıran bilgi ve iletişim teknolojileri, tek başına bir sektör olmaktan çıkmış ve diğer tüm sektörleri etkileyen, geliştiren temel bir sektör halini almıştır. Bu itibarla sektör, hizmet bileşeni ile birlikte, üretim ve satış değerleri itibarı ile dünyanın en büyük sektörü konumuna yükselmiştir. Yirmibirinci yüzyılda, gelişmekte olan ülkelerin gelişmiş ülkeler arasında yer alması için bilgi ve iletişim teknolojilerini özümseyip, üst düzeyde üretir hale gelmesi vazgeçilmez bir koşul halini almıştır.

Ancak, sektörün bu kadar hızlı yükselmesi, iş ve günlük yaşam sürecinin her alanında önemli bir yere sahip olması, bu sektör üzerinden yapılan saldırı ve tehdit risklerini de artırmıştır. Risk ve tehditlerin artması ise bilgi ve iletişim teknolojileri ile yapılan haberleşme ve bilgi alışverişlerinde güvenlik ve güvenliğin temel unsuru olan kişisel mahremiyet sorunlarını ortaya çıkarmıştır.

Bilgi toplumu hedefine ulaşılmasında, elektronik ticaret ve elektronik devlet uygulamalarının yaygınlaşmasında büyük önem taşıyan bilgi ve iletişim teknolojilerinde, güvenli bir ortamın sağlanması, açık ağlarda dolaşan bilginin güvenliğinin, kişisel verilerin gizliliğinin ve mahremiyetinin sağlanması ile

mümkün olmaktadır. Bu nedenle, taraflararası iletilerde bilginin gizliliği, bütünlüğü ve her istenilen anda ulaşılabilirliğinin sağlanmasının yanı sıra elektronik ortamda işlenen kişisel verilerin korunması için teknik ve yasal önlemlerin alınması oldukça büyük önem arzetmektedir.

Ancak, 11 Eylül 2001'de Dünya Ticaret Merkezi ve Pentagon'a yapılan saldırılarda İnternet'in iletişim aracı olarak kullanılması ve bu merkezlerin bilgisayar sistemine sızılması ihtimalinin göz önünde bulundurulması, bilgi ve iletişim teknolojileri ile bilgi güvenliğinin önemini ortaya koymuş ve bilgi güvenliği alanında alınan teknik ve yasal önlemlerin tek başına yeterli olmayacağını, bunun bir kültür olarak yerleşmesi gerektiğini, aksi takdirde alınacak her türlü önlemin güvenliği sağlamada yetersiz kalacağını göstermiştir.

Bu nedenle, her ülkenin kendi toplum değerleri ile bağdaşık güvenlik kültürü yaratması ve özümsemesi bu alanda olabilecek risklerin önüne geçilmesinde büyük yarar sağlayacaktır.

Bu tez ile, ülkemizin üyesi olduğu ve Kurumumuzun çalışmalarını yakından takip ettiği ITU, OECD gibi uluslararası kuruluşlar ile AB'nin bilgi güvenliği, özellikle de bilgi güvenliğinin temel unsuru olarak kabul edilen kişisel verilerin korunması ile mahremiyetinin sağlanması ve bilgi güvenliği kültürü oluşturulması hususunda yapılan çalışmalarından yola çıkılarak, Avrupa Birliği mevzuatını uyumlaştırma sürecinde, Türkiye açısından eksik olduğu düşünülen noktalara ışık tutmak ve toplum değerlerimizle bağdaşık bir "Güvenlik Kültürü" oluşturma konusunda atılacak adımlara değinmek amaçlanmıştır.

Bu çalışmada, Türkiye'de ve dünyada, bilgi güvenliğini sağlama hususunda somut adımlar atılamamış olması nedeniyle bilgi güvenliğini sağlamada etkin

bir unsur olan güvenlik kültürü ile günümüzde en çok endişe yaratan kişisel verilerin korunması ve mahremiyet konuları temel alınmış, bu konuda uluslararası kuruluşların ve özellikle AB'nin çalışmaları göz önünde bulundurulmak suretiyle Türkiye'de yapılan ve yapılması gereken düzenlemelere ilişkin öneriler ortaya konulmuştur.

Türkiye'de henüz bilgi güvenliğinin kavramsal olarak bile kullanımının yaygınlaşmamış olması, bu konudaki yasal hazırlıklar ve düzenlemelerin yetersiz kalması ve ilgili sorunların çözüm yollarının müzakere edileceği ortak bir anlayışı tesis edecek, üzerinde mutabakata varılmış yöntemlerin olmaması çalışmanın en büyük zorluğunu oluşturmuştur.

Tez hazırlama metodolojisi bakımından önem taşıyan kaynak incelemesinde, bilgi güvenliği ve mahremiyetin korunması hususunda Türkiye'de yazılı kaynakların az olması nedeniyle büyük ölçüde internet vasıtasıyla ulaşılan belgeler ve raporlardan faydalanılmıştır. Ayrıca, tez çalışmasının, uluslararası kuruluşlar ile AB'nin çalışmalarına ilişkin güvenilir bilgiler içermesi temel amaç ve yöntem olarak benimsenmesi nedeniyle AB ile ITU ve OECD gibi uluslararası kuruluşların yayınları ve verileri esas alınmıştır.

Elektronik imza ve kurumsal güvenlik, bilgi güvenliği ve mahremiyetin korunmasına yönelik hususları içermesine rağmen, bu konularda Kurum bünyesinde tez hazırlanması nedeniyle bu konular kapsam dışı bırakılmıştır.

Girişi takiben tezin ikinci bölümünde, bilgi güvenliği kavramı ele alınarak bilgi ve iletişim teknolojileri vasıtasıyla depolanan ve aktarılan bilginin gizliliği ve bilgi güvenliğinin temel unsuru olan kişisel verilerin ve mahremiyetin korunması konusu incelenmiştir.

Üçüncü bölümde, AB ve uluslararası kuruluşların çalışmalarına yer verilmiştir. Ancak, yukarıda da belirtildiği üzere bilgi güvenliği konusunda ortak mutabakata varılmış çalışmaların bulunmaması nedeniyle, bu konuda uluslararası kuruluşların, kişisel verilerin korunması ve ülkelerin toplum değerleri ile bağdaşık güvenlik kültürü yaratmaya yönelik çalışmaları esas alınmıştır. Diğer taraftan, elektronik ortamda tutulan ve aktarılan kişisel verilerin ve mahremiyetin korunmasına yönelik olarak Türkiye'de yapılan düzenlemelerde referans alınan uluslararası kuruluşların karar ve direktiflerine yer verilmiştir.

Dördüncü bölümde, üçüncü bölümde ele alınan uluslararası kuruluşlar ile AB üyesi olan ülkelerden bilgi güvenliği alanında güvenlik kültürü ve kişisel verilerin korunması ile mahremiyetin sağlanması hususunda önemli çalışmalar yapmış olanlara yer verilmiştir.

Beşinci bölümde, Türkiye'de bilgi güvenliği, güvenlik kültürü ve mahremiyetin sağlanması hususunda yapılan çalışmalar ve düzenlemeler incelenerek bunlara ilişkin değerlendirmeler yapılmıştır.

Tezin son kısmı olan sonuç ve öneriler bölümünde ise, daha önceki bölümlerde ele alınan konular gözönünde bulundurularak, bu konuda Türkiye'de ve Telekomünikasyon Kurumu'nda yapılması gerekli olan çalışmalar konusunda önerilerde bulunulmuştur.

2. BİLGİ GÜVENLİĞİ

Bu bölümde bilgi güvenliği kavramının tanımı yapılarak, elektronik ortamda tutulan ve aktarılan bilginin güvenliğini sağlamaya yönelik yöntemlerden bahsedilerek, günümüzde en çok endişe yaratan ve bilgi güvenliğinin temel unsuru olarak kabul edilen bilgi ve iletişim teknolojileri üzerindeki kişisel verilerin korunması konusu ele alınmaktadır.

2.1. Bilgi Güvenliği Kavramı

Çağımızda bilginin giderek önem ve değer kazanmaya başlaması, bilgiye sahip olan ülkelerin gelişmiş ülke düzeyine ulaşması, bu varlığın korunması gerekliliğini yani bilgi güvenliği kavramını ortaya çıkarmıştır. Türkiye'de oldukça yeni olan bu kavram, bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme olarak [1] tanımlanmaktadır. Bu konuda diğer bir tanımlama ise bilginin, ticari sürekliliğini sağlamak, ticari kayıpları en aza indirmek ve ticari fırsatların ve yatırımların dönüşünü en üst seviyeye çıkarmak için geniş tehlike ve tehdit alanlarından korunması [2] olarak ifade edilmiştir.

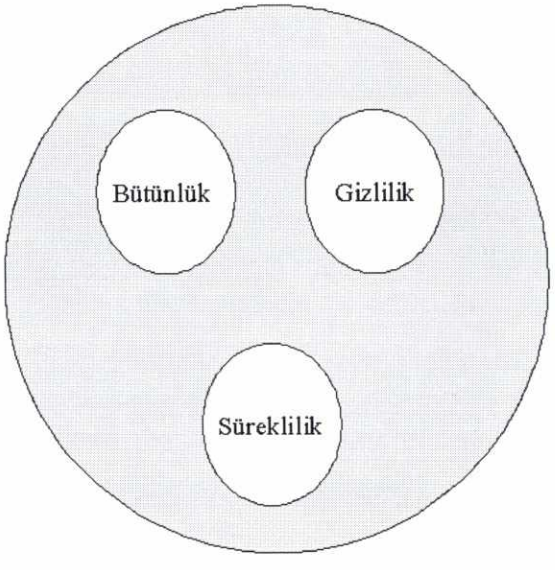
Etkin bir bilgi güvenliği oluşturabilmek için öncelikle bilginin analiz edilmesi ve sınıflandırılması gerekmektedir. Olabilecek risk faktörleri belirlenmeli ve risk faktörlerine göre uygun güvenlik önlemleri alınmalıdır. Etkin bir şekilde oluşturulan güvenlik, bilginin sürekliliğini sağlamakla birlikte kayıpları en aza indirmede de önemli rol oynamaktadır. Bununla birlikte, bilginin azami olarak güvenliğinin sağlanması, bilginin tutulduğu ortamın güvenliğinin sağlanması ve güvenli bilgi iletiminin gerçekleştirilebilmesi ile mümkün olmaktadır. Güvenli bilgi, bilginin her zaman ulaşılabilir durumda olması,

bilginin bütünlüğünün ve gizliliğinin sağlanması anlamına gelmektedir. Bu kapsamda üç temel unsura gerek vardır. Bunlar:

Bütünlük (integrity) Bilginin bütün oluşu, bilginin her şeyden önce doğru ve kesin oluşu, şüphe uyandırmayan bir durumda oluşudur. Ayrıca bilginin bütünlüğü gönderilen, alınan ya da işlenen her türlü verinin izin verilen kişilerin izin verilen yollarla erişimi ile sağlanabilmektedir. Bilginin anlamlı ve tutarlı oluşu, kendi içinde çelişkili olmaması da bilgi bütünlüğündeki amaç olarak sıralanmaktadır [3].

Gizlilik (confidentiality): Bilginin gizliliği ise verinin alıcısı dışında hiç kimse tarafından okunamaması, yani bilgiye sadece izin verilen kişilerin izin verilen yollarla erişimidir.

Süreklilik (availability): Süreklilik en az bilginin gizlilik ve bütünlük amaçları kadar önemli olup, doğal felaketler, güç kaynağı kesintileri, kazalar ya da saldırı gibi olumsuz ve istenmeyen her türlü şart altında bilgi ve verilere erişilebilmesidir.



Şekil 2.1. Bilgi Güvenliği Temel Unsurları

Bu üç unsuru bir araya toplayan bilgi güvenliği için

- Donanım güvenliği,
- Yazılım güvenliği,
- Kripto güvenliği,
- Emisyon güvenliği,
- Ağ güvenliği,
- Fiziki güvenlik,
- Personel güvenliği,
- Doküman güvenliği

gibi unsurların bir arada gözönünde tutulması gereklidir. Bu unsurlardan herhangi birinin eksik kalması bilgi güvenliğinin sağlanmasında bir açık oluşması anlamını taşıyacaktır. Örneğin; pahalı yatırımlarla, yazılım ve donanım güvenliğinin sağlanmasına karşın personel gizlilik konusunda yeterli eğitim ve bilinçle donatılamazsa bilgi güvenliğinin sağlanması hayalden öteye gidemez [4]. Bu yaklaşımla yukarıda verilen her bir başlık için güvenliğin tesis edilmesi gerekmektedir.

2.1.1. Donanım güvenliği

Yazılımın altyapısını oluşturan fiziksel cihazlar donanım olarak adlandırılmaktadır. Donanım çoğunlukla hassas elektronik devrelerden oluştuğundan, taşınırken veya fiziksel bir müdahalede olağandan biraz daha fazla dikkat edilmesi gereken unsurlardır. Donanımın maruz kalacağı saldırı türleri, zarar verme ve izinsiz erişimdir. Zarar verme kasıtlı veya kasıtsız olarak donanım parçalarının çalınması, kırılması, bozulması ve parçalanması veya üçüncü şahısların eline geçmesi şeklinde gerçekleşebilmektedir. Diğer taraftan ihmal ya da umursamazlık sonucu ortaya çıkan kazalar sonucunda donanım güvenliği tehlikeye düşebilmektedir [5].

Bunun yanında küçük böceklerin elektronik devrelere girerek kısa devreye yol açması ya da farelerin kabloları kemirmesi de donanımın güvenliğini tehdit eden unsurlardır. Ayrıca, temizliğin ihmal edilerek donanım parçalarının üzerinde zamanla toz birikmesi devrelerde ve güç kaynağında, özellikle soğutucu sistemlerde bulunan parçaların çalışmasını engelleyerek donanım güvenliğinin tehlikeye düşmesine neden olabilmektedir [5].

2.1.2. Yazılım güvenliği

Yazılım güvenliğini oluşturmak için öncelikle yazılımın maruz kalabileceği saldırıları ortadan kaldırmak gereklidir. Yazılımın maruz kalabileceği saldırılar arasında, silinme baş sırayı almaktadır.

Bunun yanı sıra, yazılım üzerinde aynı zamanda değişiklik de yapılabilmektedir. Derlenmiş bir program üzerinde değişiklik yapmak metin bir dosya üzerinde değişiklik yapmaktan çok daha zor ve özel bir bilgi ve özel programlar kullanmayı gerektirmektedir. Bununla birlikte, herhangi bir programın üzerinde değişiklik yapacak programlar yazılabilmektedir. Belki de bu konuda aşina olunan saldırı türü, yazılıma yönelik değişiklik yapma saldırısı, olan virüsler[1], kurtlar[2] ve truva atları[3]dır [5].

Ayrıca, yazılım güvenliğinin sağlanması için bilgisayarda kullanılan tüm yazılımların (işletim sistemi-operating system, paket programlar-database, word, excel, outlook vs gibi) lisanslı olması ve bu yazılımlara ait gelişmelerin

---

[1] Modern bilgisayar virüsleri 80'lerin başlarında IBM PC'lerin başlangıcıyla ortaya çıkmıştır [6].

[2] Kurtlar (worm) virüs olarak adlandırılmakla birlikte teknik olarak farklılıkları bulunmaktadır. Kurtlar bilgisayar ağı üstünde yayılmakta ve aktif hale gelmesi için kullanıcı tarafından bir müdahaleye ihtiyaç duymaktadır.

[3] Truva, eski Yunan mitolojisindeki ünlü tahta attan ismini alan bilgisayarın kontrolünü ele geçirmek için kullanılan zararlı bir yazılımdır [7].

yakından takip edilerek, özellikle güvenlik açıklarını kapatmaya yönelik yamaların yüklenmesi ve gerekli güncellemelerin yapılması şarttır.

2.1.3. Kripto güvenliği

Kripto, bilginin bütünlüğünü, gizliliğini ve işlemi yapan tarafın bunu reddedememesi, hem de tarafların onaylanması için şifreleme ve şifre çözme yöntemlerinin kullanılması işlemidir. Şifrelemede özgün bilgi, şifre anahtarı ile içerik açısından anlamsız alfa-sayısal bir veriye dönüştürülmektedir. Bu şifrenin çözümü ise yine bir şifre anahtarı ile özgün verinin yeniden elde edilmesidir. Kripto literatüründe değişik şifreleme yöntemleri ve şifre altyapıları bulunmaktadır.

Günümüzde kripto donanım üzerinden yazılıma kaymış durumdadır. Pek çok devlet kripto güvenliğinin sağlanması amacıyla kriptografik teçhizatın ihracatına kısıtlama getirmiş ve devlet denetimine almışlardır[1]. Bu nedenle kripto ihtiyacının milli imkanlarla yurtiçi kaynaklardan temin edilmesi yoluna gidilmesi, onaysız kripto yazılım ve donanımlarının kullanılmaması kripto güvenliğinin sağlanmasında atılacak en önemli adımı oluşturacaktır.

2.1.4. Emisyon güvenliği

Ulusal Bilgi Güvenliği Kanunu Tasarısı'nda, tüm elektronik teçhizattan ve bunların kuruluşundan iletkenlik ve ışıma yoluyla istem dışı yayılan bilginin önlenmesine ilişkin olarak alınan tedbirler emisyon güvenliği veya tempest (Temporary Emission and Spurious Transmission) güvenliği olarak adlandırılmaktadır.

---

[1] Türkiye'nin de Aralık 1998 yılında 33 ülke ile imzalamış olduğu Wassenr Anlaşması kriptoloji ürünlerinin ihracaatına sınırlama getirmektedir.

Bu kapsamda elektromanyetik güvenlik yöntemleri şu şekilde sağlanabilmektedir:

- Kullanılan aletlerin sözkonusu açık verici dalgaları yaymasını zırhlama ve filtreleme gibi yöntemlerle engellemek,
- Yayılan dalgalara gürültü ekleyerek anlaşılmaz kılmak veya aletlerin çalışma temelini değiştirerek yayılan işaretleri işlenen bilgiden arındırmak.

Birinci yöntemle ya doğrudan kullanılan elektronik malzemeler zırhlanmakta ve giriş/çıkışları filtrelenmekte ya da zırhlı olması gerekmeyen aletler zırhlı odalarda kullanılmaktadır. Askeri ve diplomatik uygulamalarda genellikle ikinci yöntem kullanılmaktadır. Zırhlanacak odalar tamamen yalıtkan bir maddeyle kaplanarak elektromanyetik yayılımları durdurucu Faraday kafesi oluşturulmaktadır. Odaların havalandırma girişlerine dalga kırıcı yansıtıcılar konulmaktadır. Elektrik şebekesine olan bağlantılar açıkverici işaretlerin bulunabileceği frekansları kesen filtreler aracılığıyla yapılmaktadır. Bu tip odalar genellikle ses yalıtımına da tabi tutulmaktadır [8].

Gizli servislerin ortaya çıkmasından hoşlanmadıkları tempest güvenliği ile Türkiye'de ilgilenen başlıca kuruluşlar Tübitak ve Aselsan'dır.

2.1.5. Ağ güvenliği

Ağ güvenliği, şebeke üzerinde istenmeyen erişimlerin engellenmesi ve sisteme giriş ve çıkışların sürekli kontrol edildiği "firewall"[1] tipi sistemlerin oluşturulmasıdır. Ağ güvenliğinde ayrıca, sisteme yapılan saldırıların tespiti,

[1] Firewall (Internet Güvenlik Sistemi), internet üzerinden bağlanan kişilerin, bir sisteme girişini kısıtlayan/yasaklayan ve genellikle bir internet gateway servisi (ana internet bağlantısını sağlayan servis) olarak çalışan bir bilgisayar ve üzerindeki yazılıma verilen genel isimdir [9].

denetleme ve istenmeyen erişimlerin kontrolü için geliştirilmiş sistemler kullanılmaktadır.

2.1.6. Personel güvenliği

Bilgi güvenliğini tehdit eden unsurların başında kurum ve kuruluş çalışanları gelmektedir. GartnerPro tarafından yapılan araştırmalarda, bilişim teknolojilerinde güvenlik açıklarının % 81'i mevcut çalışanlar tarafından verilmektedir [1]. Yani konu ile ilgili olarak eğitimsiz kişilerin bu alanda çalışması ve bu kişilere gerekli eğitimin verilmemesi bilgi güvenliği riskini doğurmaktadır. Ayrıca, canı sıkılan veya şirketten ayrılan eski personelin öç alma duygusu ile sistemde bulunan bilgilere saldırma ihtimali de gözardı edilmemelidir.

Bu nedenle, personel güvenliği konusunda, personelin bilinçlendirilmesi, gizli bilgilere erişimin kontrol altında tutulması ve ancak yetkili kişilerin ulaşımına imkan verilmesi gereklidir. Ayrıca güvenlik sorununun ilgililer arasında paylaştırılarak, sorumluluğun dağıtılması, kurum içinde uygulanan güvenlik politikalarının yazılı hale getirilerek çalışanlara dağıtılması personel güvenliğini sağlamada etkin bir rol oynayacaktır.

2.1.7. Fiziki güvenlik

Fiziki güvenlik, iş alanına ve bilgilerine yetkisiz erişim, hasar ve müdahalenin engellenmesi amacıyla alınan önlemler olarak tanımlanmaktadır [2].

Bilgisayara fiziksel olarak erişebilen saldırgan, cihazın kontrolünü rahatlıkla ele geçirebileceği ve kötü niyetler için kullanabileceği (e-posta göndermek, virüs yüklemek veya bilgilere ulaşarak değişiklikler yapmak gibi) için çeşitli önlemler geliştirilerek fiziksel güvenliğin sağlanması gereklidir.

Bu amaçla kullanılmayan durumlarda bilgisayarı kilitli tutmak, parolalı ekran koruyucular kullanmak, kullanılmayan durumlarda mutlaka bilgisayarı kapatmak, açılış şifresi koymak gereklidir. Ayrıca bilgisayardaki bilgilerin diğer kişilerin kullanımına açık olup olmadığından emin olunması gereklidir, eğer açıksa bunu ancak bilgilere erişmesi uygun olan kişilerin erişimine açmak en doğru yöntemdir. Bunun yanı sıra bilgilerin elektronik olarak tutulduğu ortamlara giriş çıkışların da kontrol altına alınması gereklidir.

Ayrıca, verinin saklandığı ortamların deprem, yanardağ gibi doğal felaketler, yangın, su basması, terör olayları gibi olayların herhangi birinin gerçekleşmesi durumunda iş sürekliliğinin sağlanması için önceden yapılması gereken çalışmalar ve alınması gereken önlemler de fiziksel güvenliği sağlama kapsamında değerlendirilmektedir.

Bu kapsamda, bilgilerin kesintiye veya herhangi bir bozulmaya uğramadan akışının sağlanması için güvenli bir bilişim alt yapısı oluşturulmalıdır. Meydana gelebilecek bir felaket sonucunda kullanılan binanın hasar görmesi durumunda sorun yaşanmaması için ikinci bir çalışma ortamının hazır tutulması ve bir felaket planlamasının yapılarak sorumluların belirlenmesi gereklidir.

Diğer yandan, bilgisayardaki verilerin servis kesintisine yol açabilecek tüm durumlar için sistemdeki kritik yazılım ve sunucuların yedeklenmesi, şehir şebekesinden kaynaklanan elektrik kesilmeleri ve düzensiz bir elektrik akımı için jeneratör ve/veya UPS (Uninterruptible Power Supply-Kesintisiz Güç Kaynağı) gibi kaynakların oluşturulması gereklidir. Ayrıca, ihtiyat gereği hemen her türlü cihazın bir yedeğinin bulundurulması konusunda gerekli düzenlemelerin de yapılması gereklidir.

2.1.8. Doküman güvenliği

Doküman güvenliği, oluşturulan doküman arşiv sistemi ile elektronik ortamda arşivlenen dokümanların güvenliği konusu olup, özellikle e-kurum ve e-devlet uygulamalarında ön plana çıkmaktadır. Elektronik ortamda tutulan dokümanları korumaya yönelik alınacak her türlü önlem de doküman güvenliği olarak adlandırılabilmektedir.

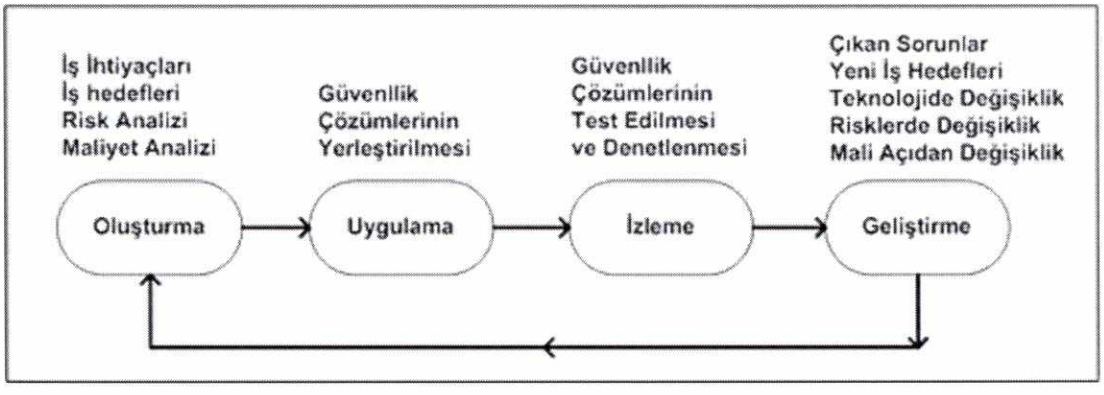
Bu kapsamda, dokümanların güvenlik seviyeleri ve bunlara ulaşabilecek kullanıcılar ve bunların yetkileri belirlenmektedir. Ayrıca çok gizli olarak saklanması gerekli dokümanlar tanımlanarak bunlara ulaşımın çeşitli donanımlarla (akıllı kart ya da token) erişimi sağlanmaktadır. Bu dokümanlara erişim yetkisi belirlenmiş kişiler akıllı kartlarını ve PIN numaralarını girerek dokümana erişebilmektedirler. Sistemde belirlenen güvenlik seviyesine göre (örneğin çok gizli) dokümanlar havale edilirken de yine akıllı kart ile PIN kontrolü yapılarak havale işlemi gerçekleştirilmektedir. Bu yöntemle, kullanıcı bilgisayarında programı açık bırakıp bilgisayarının başından ayrılması durumunda bile başka bir kullanıcının onun adına işlem yapması önlenmiş olmaktadır.

2.2. Bilgi Güvenliği Standardı

ISO[1] tarafından 2000 yılında hazırlanan Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri ISO/IEC 17799 (Uluslararası Standart Organizasyonu/Uluslararası Elektroteknik Komitesi - International Organization for Standardization/International Electrotechnical Committee) standardı TSE (Türk Standartları Enstitüsü) tarafından 2002 yılında çevirisi yapılarak Türk standardı haline getirilmiştir. Dünyaca kabul gören bu standart, bilginin bir varlık olarak hasarlardan korunması gerektiğini vurgulayarak etkin

[1] ISO, yaklaşık 130 ülkenin standardizasyon kuruluşunun üyesi olduğu bir kuruluştur. ISO'nun çalışmaları uluslararası anlaşmalar niteliğinde olan Uluslararası Standartlar olarak yayınlanmaktadır.

bir güvenlik için bilginin sınıflandırılmasını öngörmektedir. Ayrıca standart, içerden ve dışardan gelebilecek saldırılara karşı var olan alt yapıyla uyumlu çözümler konusunda açıklamalar getirmekte, fiziki güvenlik, personel güvenliği, sistem ve cihaz güvenliği gibi temel konulara ilişkin bilgiler içermekte, sağlıklı bir güvenlik politikası oluşturmak için gerekli yöntemleri sunmaktadır. Bu kapsamda oluşturulan güvenlik politikası Şekil 2.2'de sunulmaktadır:



Kaynak: Türkiye Bilişim Şurası [10].

Şekil 2.2.Güvenlik Politikası

Diğer taraftan günümüzde iletişim teknolojileri vasıtasıyla aktarılan bilginin güvenliğinin de oldukça önemli olması nedeniyle bilginin gizliliği, bütünlüğü, erişilebilirliği ve bunu sağlamak için kullanılan kriptografi ve sayısal imzaların da önemli olduğu hususuna dikkat çekilmiştir.

Standart, bireysel ve kurumsal güvenlik politikaların oluşturulmasında son derece önemli bir yere sahip olmakla birlikte ülkemizde bu konuda bilinç oluşturulması hususunda da oldukça büyük önem arzetmektedir. Zira artık kurum ve kuruluşlar izledikleri yöntemlerin doğruluğunu ve güvenilirliğini bu konuda hazırlanan standartlarla pekiştirmektedirler.

2.3. İnternet ve Bilgi Güvenliği

İnternet, İngilizce'de uluslararası ağ anlamına gelen international network sözcüklerinin birleştirilmesinden oluşan tüm dünyaya yayılmış, bilgi paylaşımı için birbirleri ile bağlantılı bilgisayarlardan oluşan bir ağdır. 1969 yılında Amerikan Savunma Bakanlığı'nın askeri projeleri desteklemek için Arpanet adında ağ oluşturmasıyla başlayan İnternet TCP/IP (İletim Kontrol Protokolü/ İnternet Protokolü - Transmission Control Protocol/Internet Protocol) İletim Protokol Setinin geliştirilmesi ile kullanım alanını daha da artırarak tüm dünyaya yayılmıştır [11].

İnternetin bu kadar yaygın olarak kullanımı ve bankacılıktan ticarete kadar pek çok bilginin internet üzerinden aktarımının yapılması beraberinde pek çok güvenlik riskini de ortaya çıkarmıştır. İnternet üzerinden aktarılan bir bilgi, kaynağından çıktıktan sonra çeşitli noktalardan geçmekte ve bu noktalardan birinde bozulma, kaybolma veya yerine ulaşamama gibi riske maruz kalabilmektedir. Bu nedenle ağlar üzerinde aktarılan bilginin bütünlüğü, gizliliği ve sürekliliğinin yanı sıra gönderenin kimliği ve alıcının inkar edememesi gibi konular oldukça önem kazanmaktadır.

Bu amaçla İnternet üzerinden aktarılan verinin güvenliğini sağlamak için kriptografi ve elektronik imza yöntemleri kullanılmaktadır. Kriptografi literatüründe değişik şifreleme yöntemleri ve şifre altyapıları bulunmaktadır. Ancak günümüzde internet üzerinden yapılan işlemlerde güvenliği sağlamak için üzerinde en çok durulan kriptografi sistemi Açık Anahtar Kriptografi'sidir. Elektronik imza da Açık Anahtar Kriptografi sistemine dayalı bir yöntemdir. Açık anahtar tabanlı sistemler yapıları nedeniyle yavaştırlar ancak kırılmaları oldukça güçtür. Bankacılık, elektronik alışveriş gibi paraya dayalı ödemelerde genellikle açık anahtar tabanlı sistemler kullanılmaktadır.

2.4. Kişisel Verilerin Korunması

Bireyi tanımlayan isim, adres, banka hesabı, telefon numarası gibi her türlü bilgi kişisel veri olarak adlandırılmaktadır. Bankacılık, sigortacılık, sosyal güvenlik, sağlık, pazarlama, elektronik haberleşme ve elektronik ticaret gibi bir çok alanda birbirinden ayrı ve bağımsız olarak kişisel veriler işlenmekte ve depolanmaktadır [13].

Bilgisayar teknolojilerindeki gelişmeler birbirinden ayrı ve bağımsız olarak tutulan bu kişisel verilerin elektronik ortamda kolayca işlenerek veri tabanları oluşturulmasına imkan sağlamaktadır. Bu durum, bilgi güvenliğinin temel unsuru olan kişisel verilere kolayca ulaşılabilmesini sağlarken diğer taraftan art niyetli kişilerin eline geçerek kötü amaçlar için kullanılabilmesini de kolaylaştırmaktadır.

Bu tür verilerin art niyetli kişilerin eline geçmesi ile oy ve nüfus sahteciliklerinin yanı sıra vergi borcunu silme, ölü birisini yaşıyor gibi veya herhangi bir sınavı kazanmış gibi gösterme, emekli maaşı bağlama gibi bir çok sahtecilik yapılabilmektedir. Bunlara ilaveten, başkasının zararına olarak kayıtlar değişitirilebilmekte ve de en önemlisi bireylerin evrensel ve anayasal hakkı olan özel hayatın gizliliği ihlal edilebilmektedir [14].

Bu nedenle, kişisel verilerin üçüncü kişilere açıklanması durumunda ilgili kişinin bilgilendirilmesi ve rızasının alınması gereklidir. Diğer taraftan, verilerin yasal sınırlar içinde kalmak şartıyla, sadece veri toplamadaki amaç çerçevesinde kalınarak elde edilmesi ve kişilere kendilerine ilişkin bu verileri öğrenme ve eğer varsa verilerdeki eksik veya yanlışları düzeltme imkanının da tanınması gereklidir. Ayrıca dini, siyasi inanç ve tıbbi özellikler gibi özel niteliği olan hassas veriler diğer verilere nazaran daha özel yöntemlerle

korunmalıdır. Bu kapsamda, bünyesinde hassas veri barındıran meslek dalları konuyla ilgili etik ilke ve kuralları yazılı hale getirmelidirler [13].

Diğer taraftan, yukarıda bahse konu olan verilerin elektronik ortamda tutulması konusu, gittikçe endişe yaratan bir konu olmanın yanısıra günümüzde internette "cookie"[1] veya "spyware"[2] gibi programların bulunması da kişisel verilerin ihlaline neden olmaktadır. Bu programlar sayesinde kişilerin bilgisi ve rızası olmaksızın, e-posta gönderen ya da bir İnternet sitesini ziyaret eden bireyler hakkında kişisel verilerin toplanması ve bu veriler sayesinde kişinin zevklerinin ya da alışkanlıklarının öğrenilmesi mümkün olmaktadır.

Bu programlar sayesinde İnternette faaliyet gösteren "Flycast" ve "Doubleclick"[3] gibi şirketler, elde ettikleri verileri pazarlama amacıyla kullanarak reklam şirketlerine satmaktadırlar[4]. Bu ise kişilik hakkının ihlal edilmesine neden olmaktadır.

Bu nedenle, bazı ülkelerde İnternet vasıtasıyla kişisel verilerin toplanması, işlenmesi ve dağıtılmasını düzenlemek amacıyla hukuki ya da self-regülasyon düzenlemeleri yapılmıştır. Bu tür düzenlemelerin ülkemizde de yapılması,

---

[1] Cookieler, hizmet sağlayıcısı tarafından otomatik olarak tanımlanabilen bir işaret ya da belirteç gibi davranan özel bir yazılım olup İnternet kullanıcısının terminalinde depolanarak, çok çeşitli amaçlar için kullanılmaktadır. Bazı İSS (İnternet Servis Sağlayıcı)'ler cookieleri kullanıcıların internet sitelerini ziyaretleri ile ilgili bilgileri tutarak istatiksel verilerileri elde etmek amaçlı kullanırken, bazı İSS'ler abonelerinin internet sitesinde ziyaret ettikleri sayfalar sayesinde eğilimlerini öğrenebilmektedirler.

[2] Spyware, İnternet kullanıcıları tarafından kişi ve bilgisayarı hakkında bilgi toplayıp başkasına gönderen yazılımlara verilen isimdir. Genelde zararsız olmasına rağmen gizlice çalışması bilgisayar kullanıcılarını rahatsız etmektedir.

[3] Kişisel verilerin satın alınması, veri bankalarının işletilmesi ve idare edilmesi, adres aracılığı, e-posta reklamcılık kampanyalarının geliştirilmesi gibi farklı alanlarda hizmet göstermektedirler. Dünyanın en büyük İnternet servis sağlayıcılarından biri olan "DoubleClick" sadece 1 yılda 10 milyon İnternet kullanıcısını içeren bir dosyayı oluşturmuştur [15].

[4] Ocak 2001 tarihi itibariyle İnternette bir e-posta adresi 20 Cent'e satılmaktaydı [15].

ayrıca kullanıcıların İnternette kişisel verilerini nasıl korumaları gerektiği hususunda bilgilendirilmesi ve bilinçlendirilmesi gereklidir.

Bilgi teknolojilerinin yanı sıra iletişim teknolojilerinin analog sistemlerden sayısal sistemlere dönüşmesi, interaktif hizmetlerin artması iletişim güvenliğini ve özellikle de bu sistemler vasıtasıyla işlenen kişisel verilerin güvenliği sorununu ortaya çıkarmıştır. Bunun için iletişim hizmeti sunan işletmeciler, iletişim ağı üzerinde teknik önlemleri alarak sundukları hizmetin ve bu sistemler üzerindeki kişisel verilerin güvenliğini sağlamak zorundadırlar.

2.5. E-Posta Güvenliği

Elektronik haberleşmenin getirdiği en önemli faydalardan biri elektronik posta servisidir. Elektronik iletişim ağı üzerinden gönderilen ve İnternette ya da kullanıcının bilgisayarında kaydedilebilen her türlü yazı, ses, resim ya da dil iletileri "elektronik posta" ya da "e-posta" olarak adlandırılmaktadır. E-postanın diğer haberleşme araçlarına göre oldukça ucuz olması ve bir mesajın aynı anda binlerce kişiye çok kısa bir sürede gönderilebilmesi gibi üstünlükleri, bu servisi iş ve ticaret dünyasının vazgeçilmez aracı haline getirmiştir[1].

Ancak e-posta, iletişime düşük maliyet ve yüksek hız kazandırmakla birlikte sistemin yapısı itibariyle mesajların kolayca izlenmesini, kopyalanmasını, silinmesini veya değiştirilmesini mümkün kılmaktadır. Özel koruma önlemleri alınmadığında mesajların güvenliğini sağlamak mümkün olmadığı gibi, gerçekleşen tehditleri tespit etmek de çoğu zaman mümkün olmamaktadır [16].

---

[1] IDC (Uluslararası Veri Şirketi-International Data Corporation) tarafından dünyada 700 milyon adet e-posta adresinin olduğu 2005 de ise bu rakamın 1,2 milyar olacağı hesap edilmektedir [17].

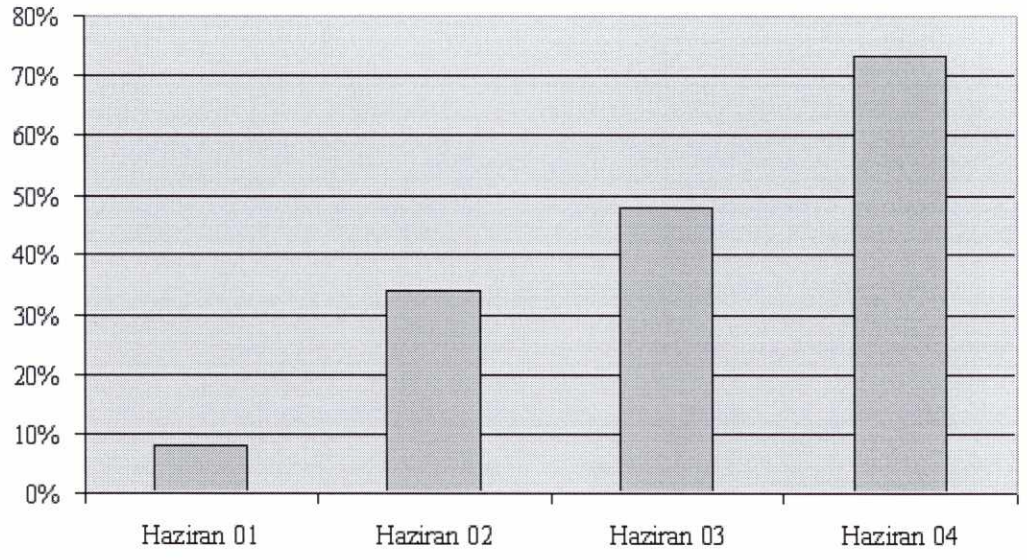
Günümüzde e-posta güvenliği, elektronik ortamda aktarılan mesajın kaynağından çıktıktan sonra gideceği yere ulaşana kadar gizliliğinin ve bütünlüğünün ve gönderici ile alıcının kimliğinin doğrulanmasının yanısıra, kişisel veri olarak da kabul edilen e-postanın mahremiyetinin sağlanmasına yönelik tedbirlerin alınması ile sağlanmaktadır. Bu kapsamda e-posta yoluyla gönderilen bilginin gizliliği, bütünlüğü, alıcı ile gönderenin kimliğinin doğrulanması elektronik imza ve kriptolama yöntemleri ile sağlanmaktadır.

Günümüzde e-posta adreslerine spam olarak adlandırılan istek dışı mesajların gönderilmesi gittikçe artan bir sorun haline gelmekte ve e-postanın mahremiyetine gölge düşürmektedir.

2.5.1. İstek dışı haberleşme

Çok çeşitli tanımlaması olmakla birlikte İnternet üzerinden aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi spam [18] ya da istek dışı haberleşme olarak adlandırılmaktadır.

Burada amaç, çeşitli şekillerle ele geçirilen e-posta adreslerine gereksiz mesaj göndererek e-postanın işlemez hale getirilmesidir. Bu tür mesajlar alıcıyı rahatsız etmekte ve e-posta sistemleri üzerinde aşırı yük oluşturmaktadırlar. Öyle ki istek dışı haberleşmeye karşı korunmayan e-posta sistemleri, bu mesajlar yüzünden gereksiz dolmakta, kullanıcı gereksiz zaman kaybetmekte ve asıl alması gereken mesajları alamamaktadır.

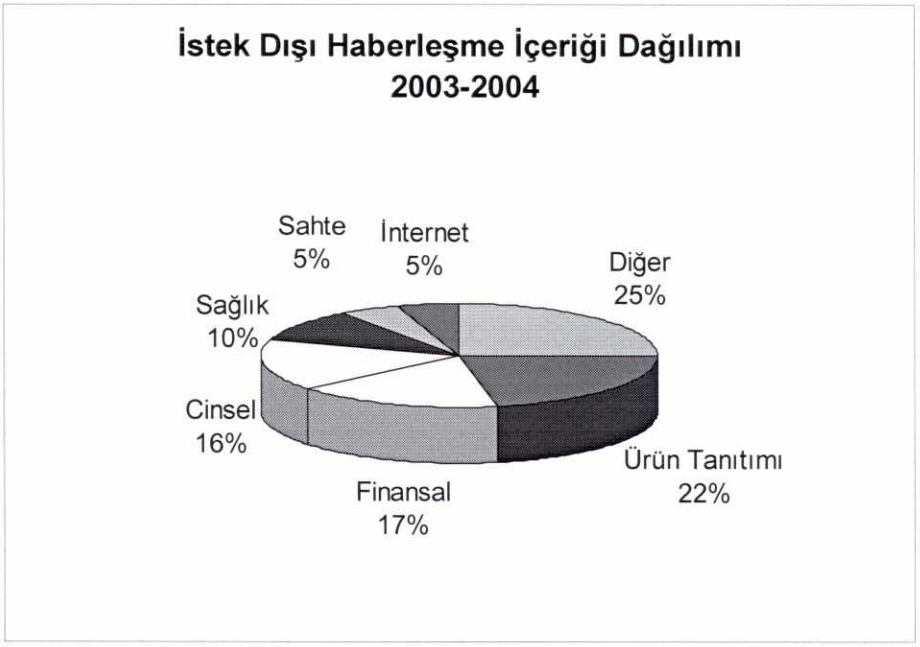


Kaynak ITU [19]

Şekil 2.3.2001-2004 Yılları Arasında İstek Dışı Haberleşme Oranları

Çoğunlukla bireysel ve kurumsal kullanıcıların e-posta adreslerinden oluşturulmuş veri tabanlarının bir ücret karşılığı[1] reklam şirketlerine satılması istek dışı haberleşmeyi yaygın hale getirmektedir. Bu mesajlar genelde ticari reklam niteliğinde olup, tüketicileri aldatmaya yönelik içerik taşıyabileceği gibi, yasadışı ve pornografik içerik veya siyasi bir amaca yönelik propaganda mahiyetinde de olabilmektedir. Şekil 2.4'te istek dışı haberleme içeriklerinin dağılımını göstermektedir. Artan bir tehdit olmayı sürdüren istek dışı haberleşmenin asıl kaynağını ABD (Amerika Birleşik Devletleri) oluşturmakta bunu Çin, Güney Kore, Brezilya ve Kanada izlemektedir.

[1] İnternette e-posta adresi satış hizmeti veren şirketlerden aylık ortalama 20 ABD doları üyelik ücreti karşılığında haftada 300.000 e-posta adresi satın alınabilmektedir [20].

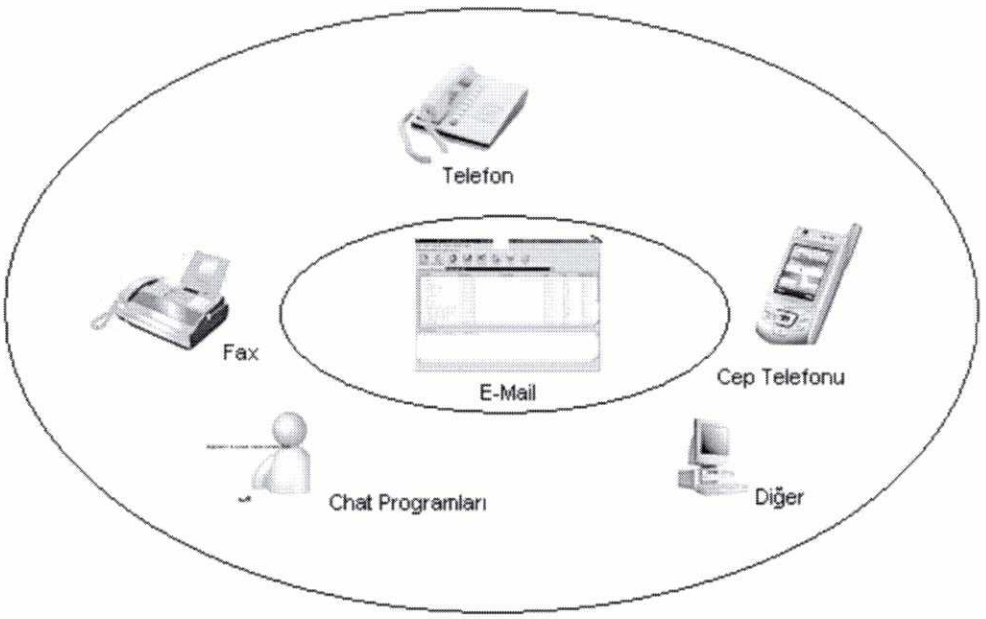


Kaynak: ITU [19]

Şekil 2.4.İstek Dışı Haberleşme İçeriği Dağılımı

İstek dışı haberleşmede mali yük büyük ölçüde mesaj alıcıları veya servis sağlayıcı işletmeler-İSS tarafından karşılanmak zorunda kalmaktadır. İSS'ler her gün binlerce gelen istek dışı mesajları depolamak veya filtrelemek için gereksiz yere yatırım yapıp sistemlerinin kapasitelerini artırmak zorunda kalmaktadırlar. Bu nedenle, göze gözükmemekle beraber istek dışı haberleşmenin çok büyük mali külfeti bulunmaktadır. AB'nin yaptığı araştırmaya göre istek dışı postanın tüm dünyada yılda 10 milyar Euro'ya yakın bir maddi kayba neden olduğu tespit edilmiştir. Ayrıca, bu tür mesajlar ile virüs bulaşması ve bilgisayarın kontrolünü ele geçirmesi de ayrı bir kayıp olarak nitelendirilmektedir. Diğer bir tehlike, "spamming" yaparak internette faaliyet gösteren her bir reklam şirketinin, teknik ilerlemeye bağlı olarak donanımlarını geliştirerek, yakın gelecekte İnternete günde yüz milyon adet reklam iletisi göndermesi tehlikesidir. Bu günümüzdeki rakamlarla ortalama 569 milyon posta kutusunun kilitlenmesi anlamına gelmektedir [21].

Bunların yanısıra, istek dışı haberleşme, günümüzde sadece bilgisayarda bir tehdit olmaktan çıkmıştır. Yani cep telefonu, PDA (Personel Digital Assistant) denilen hem cep telefonu hem de bilgisayar özelliğine sahip avuçiçi bilgisayarların yanı sıra faks, telefon gibi cihazlar da artık istek dışı haberleşme tehdidi altında bulunmaktadır.



Kaynak:ITU [19]

Şekil 2.5. İstek Dışı Mesajların Gönderildiği Kaynaklar

Bu kadar mali zararı olan ve kişisel mahremiyeti ihlal edici eylemin önlenmesi için IP[1] adresleri bilinen istek dışı haberleşmecilerin bir listeye dahil edilerek filtrelenmesi mümkündür. Ancak, bu listenin oluşturulması için tüm sektör aktörlerinin işbirliği ve katılımının sağlanması gerekmektedir. Ayrıca istek dışı haberleşmeyi önlemek için "Spam Tarayıcı ve Bulucu" bazı özel programlar ve yazılımlar geliştirilmiştir. Bu "Anti Spam Tool" denilen yazılımlar sayesinde istek dışı olarak nitelendirilen mesajlar

[1] İnternet dünyasındaki her makinanın bir numarası bulunmaktadır.

engellenebilmektedir [22]. Bunun yanısıra "firewall" denilen programların kullanılması da büyük yarar sağlamaktadır. Ancak istek dışı haberleşmeyi önlemek için mevcut tüm teknik çözümlerin beraber kullanılması gereklidir. Zira herbiri birbirini tamamlar niteliktedir.

Ayrıca, hizmet alınan servis sağlayıcıya veya mobil işletmecilere başvurularak da önlem alması istenebilir. Zira İSS'ler, istek dışı posta gönderen kaynakları tespit ederek, mesaj alımını durdurulabilmekte veya sistemin zarar görmesini önleyebilmektedir. Ancak, bu konuda sadece teknik önlemlerin alınması yeterli olmamakta, yasal önlemlerin alınması da gereklilik arz etmektedir. Zira, bireylerin özgür iradesine müdahele edici, bireysel ve ulusal kaynak israfına yol açıcı olması nedeni ile, istek dışı haberleşme bir kamu suçu olarak görülmektedir. Diğer taraftan beraberinde getirdiği risk ve tehditler bilgi toplumunun oluşturulmasına ve yaygınlaştırılmasına en büyük engeli teşkil etmektedir.

İstek dışı haberleşme sadece tek bir ülkeye ya da bölgeye ait olmadığından uluslararası işbirliği ve dayanışma ve kişilerin konu hakkında bilgilendirilmesi ve bilinçlendirilmesi bu konunun asgari seviyeye indirilmesinde büyük yarar sağlayacaktır.

3. ULUSLARARASI ve BÖLGESEL KURULUŞLAR İLE AVRUPA BİRLİĞİNİN BİLGİ GÜVENLİĞİ POLİTİKALARI

Bilgi ve iletişim teknolojilerinin küresel bir ağ haline gelerek uluslararası bir yapıya bürünmesi nedeniyle uluslararası ve bölgesel kuruluşlar ile Avrupa Birliği bilgi ve iletişim ağları üzerindeki bilginin güvenliğini sağlamak amacıyla ülkelerin kendi toplum değerleri ile bağdaşık güvenlik kültürü yaratmaları ve bilgi ve iletişim teknolojileri ile işlenen kişisel verilerin korunması ile ilgili olarak üye ülkelerde zamanla ortaya çıkan farklı uygulamaları ortadan kaldırmak ve uygulamalar arasında yeknesaklığı sağlamak için çeşitli çalışmalar yürütmüşlerdir. Bu çalışmalar genel olarak birbirine benzemekle birlikte birbirini tamamlar nitelik taşımaktadır.

Bu bölümde, ülkemizdeki düzenlemeler ve uygulamalarda referans alınan karar, direktif ve çalışmalara yer verilmiştir.

3.1. Avrupa Konseyi

Kişisel hak ve özgürlüklerin en önemlilerinden biri olan özel yaşamın gizliliği ve kişisel verilerin mahremiyeti, uluslararası belgelerle güvence altına alınmaya çalışılmıştır.

Avrupa İnsan Hakları Sözleşmesinin Özel Yaşamın ve Aile Hayatının Korunması başlığı altında; "*Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığının veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir*" denilmektedir.

Kişisel verilerin korunması konusu, ilk olarak Avrupa Konseyi tarafından ele alınmıştır. Konsey 1970'li yıllarda, elektronik ortamda işlenen kişisel veriler hususunda, bireylerin özel hayatının korunması için gereken ilkeleri belirlemek üzere çalışma başlatmıştır.

Bu çalışmalar sonucunda Avrupa Konseyi, Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkındaki Sözleşme'yi 1980 yılında kabul etmiştir. Sözleşme, esas itibariyle Bölüm 3.2'de ele alınan OECD (Ekonomik İşbirliği ve Kalıkınma Teşkilatı-Organisation for Economic Cooperation and Development) Rehber İlkeleri'ne benzemekle birlikte etnik köken, dini fikir ya da politik görüş, sağlık durumu, cinsel hayat ya da cinsel tercih gibi tanımlanan hassas veriler için özel bir sınıflandırma yapmıştır.

Sözkonusu sözleşme, sadece Avrupa Konseyi ülkelerinde değil tüm dünyada kabul görmüş bağlayıcı nitelikte bir belgedir [13].

Bu Sözleşme'de, gerek kamu ve gerekse de özel sektörde kişisel verilerin otomatik işlenmesi ile ilgili olarak uygulanacak usul ve esaslar belirlenmiştir.

Sözleşme ile ilgili olarak bugüne kadar çeşitli tavsiye kararları alınmış, 1999 yılında bilgi teknolojilerindeki gelişmeler doğrultusunda bazı değişiklikler yapılarak, İnternette kişisel verilerin korunması amaçlanmış, kişisel veri uygulaması konularında İnternet kullanıcıları ve servis sağlayıcıları için prensipler ortaya konularak, İnternette kişisel veri güvenliğine yönelik önlemler açıklanmıştır [13].

Türkiye'nin de üyesi bulunduğu Avrupa Konseyi tarafından 18 Eylül 1980 tarihinde kabul edilen Sözleşme 28 Ocak 1981 tarihinde Avrupa Konseyi üyesi ülkeler tarafından imzalanmıştır.

Çizelge.3.1.108 Sayılı Sözleşmenin Ülkelerdeki Durumu

	108 Sayılı Sözleşmenin Onayı
Avustralya	
Avusturya	X
Belçika	X
Kanada	
Çek Cumhuriyeti	X
Danimarka	X
Finlandiya	X
Fransa	X
Almanya	X
Yunanistan	X
Macaristan	X
İzlanda	X
İrlanda	X
İtalya	X
Japonya	
Kore	
Lüksemburg	X
Meksika	
Hollanda	X
Yeni Zelenda	
Norveç	X
Polonya	X
Portekiz	X
İspanya	X
İsveç	X
İsviçre	X
Türkiye [1]	
İngiltere	X
ABD	

Kaynak [23]

[1] 108 sayılı sözleşmeyi Türkiye 28.01.1981 tarihinde imzalamıştır. Ancak onay yasası çıkarılmadığı için Türkiye'de sözleşme henüz yürürlüğe girmemiştir.

3.2. Ekonomik İşbirliği ve Kalkınma Teşkilatı

OECD, bilgi ve iletişim teknolojileriyle yapılan haberleşme ve bilgi alışverişinde güvenliği ve mahremiyeti sağlamak amacıyla çalışmalarına 1970'li yıllarda başlamıştır. OECD bu kapsamda, bazı tavsiye kararları ve bildiriler yayınlamıştır. Bunlardan en önemlileri:

a) 23 Eylül 1980 tarihli Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına ilişkin Rehber İlkeler,
b) 26 Kasım 1992 tarihli Bilgi Sistemlerinin Güvenliğine ilişkin Rehber İlkeler.

OECD'nin bildiri ve tavsiye kararları, bilgi güvenliği hususunda kesin bir çözüm yolu üretme amacını taşımamaktadır. Hukuki yönden bağlayıcı nitelikte olmayan bildiri ve kararlar, üye ülkelerde her kesimden kullanıcının dikkatini çekmek, gelişen teknolojiye paralel bilgilendirme ve bilinçlendirme sağlamak ve her ülkenin demokratik toplum değerleriyle bağdaşık güvenlik kültürü oluşturma amacını taşımaktadır.

3.2.1. Kişisel verilerin korunmasına ilişkin politika

Kişisel verilerin toplanması ve işlenmesi konusunda üye ülkeler arasında yeknesaklığı sağlamak amacıyla 23 Eylül 1980 tarihinde OECD Konseyi tarafından Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına ilişkin Rehber İlkeler kabul edilmiştir.

Rehber İlkeler'de kişisel veri, kişiyi tanımlayan ve kişiye ait olan her türlü bilgi şeklinde tanımlanmaktadır. Ayrıca, Rehber İlkeler'de, kişisel verilerin korunması ve işlenmesinden sorumlu yetkili otoritenin kurulmasının gerekliliği vurgulanmıştır. Veri kontrolörü olarak adlandırılan bu otorite,

kişisel verilerin toplanması, işlenmesi, dağıtılması, depolanması, bu verilerin içeriğinin ne olması gerektiğine ve nerede nasıl kullanılacağına karar verebilme yetkisine sahip tarafı oluşturmaktadır.

Rehber İlkeler, kamu veya özel sektör tarafından işlenen, toplanan, dağıtılan veya depolanan elle veya elektronik yöntemlerle işlenen tüm kişisel verilere uygulanmaktadır. Ayrıca ilkeler genel anlamda sınır ötesi veri aktarımında gereksiz engellemelerden sakınılmasını da öngörmektedir. Ancak, veri aktarımında eğer aktarılan veri, verilerin aktarılacağı ülkenin yasal düzenlemelerinde gerekli güvence altına alınmamış ise bu konuya kısıtlama getirilebilmektedir [24].

Diğer yandan rehber, üye ülkelerin ulusal mevzuatlarını oluştururken kişisel verilerin korunması ve mahremiyetin sağlanması için hukuki, idari ve kurumsal düzenlemeleri gerçekleştirmelerine dikkat çekmiştir. Bu çerçevede üye ülkelerin;

- Uygun mevzuat yürürlüğe koymaları, herhangi bir ihlal durumunda gerekli ceza ve müeyyide uygulamaları,
- Uygulama esasları ve self-regülasyon uygulamalarını teşvik etmeleri ve desteklemeleri,
- Bireylerin hak ve özgürlüklerinin teminat altına alınmasını sağlamaları ve bunun için gerekli tedbirleri almaları,
- Hakkında veri toplanan kişiler arasında ayrım yapılmamasını sağlamaları [25]

gerektiği vurgulanmaktadır.

Diğer yandan sınır ötesi veri transferinde bir sorunla karşılaşılmaması için uluslararası işbirliğine önem verilmesi, kişisel verilerin korunması ve sınır ötesi serbest dolaşımı konusunda uygulanan prosedür ve işlemlerin diğer üye ülkelerdeki uygulamalarla paralel olması gerekliliği de vurgulanmıştır.

Rehber İlkeler, kişisel verilerin korunması ve sınır ötesi transferinde 8 temel ilke benimsemiştir. Bunlar:

1) **Veri toplamada sınırlama:** Kişisel veriler yasal hükümler çerçevesinde belirli amaçlar için toplanmalı ve hakkında veri toplanan kişinin onayı alınmalı,

2) **Verilerin niteliği:** Kişisel veriler, kullanım amacına uygun toplanmalı,

3) **Veri toplamanın amacı ve şartı:** Kişisel verilerin toplanma tarihi ve toplanma amacının belirlendiği tarih aynı olmalı,

4) **Kullanıma ilişkin sınırlama:** Kişinin rızası olmadan ya da ulusal mevzuata uygunluğu sağlanmadan, kişisel veriler, toplanma amacının dışında ve bu amaca aykırı olarak ifşa edilmemeli, başkalarının kullanımına açık olmamalı, başka bir amaçla kullanılmamalı,

5) **Emniyet tedbirleri:** Kişisel veriler, yetkisiz açıklanma ya da ifşa edilme, yetkisiz erişim, kaybolma, değiştirilme gibi çeşitli risklere karşı uygun ve yeterli emniyet tedbirleriyle korunmalı,

6) **Açıklık:** Kişisel verilere ilişkin olarak uygulanan politikalar, yapılan uygulamalar ve gelişmeler konusunda genel bir açıklık politikası bulunmalı,

7) **Bireysel katılım:** Kişi kendisi ile ilgili işlenen bilgiler konusunda, bilgi sahibi ve değiştirme hakkına sahip olmalı,

8) **Hesap verebilirlik:** Verilerin işlenmesinden sorumlu olan veri kontrolörü, verilerin işlenmesi ve korunması için gerekli tedbirlerin alınmasından sorumlu olmalıdır [26].

Ancak, zamanla gelişen teknolojiye paralel olarak ilkelerin güncellenme gerekliliğinin ortaya çıkması üzerine OECD Konseyi 11 Nisan 1985 tarihinde OECD üye ülkelerince kabul edilen Sınır Ötesi Veri Akışı Bildirisi ve 7-9 Aralık 1998 tarihinde Küresel Ağlarda Mahremiyetin Korunmasına İlişkin Bakanlar Konseyi Bildirisi'ni yayınlamıştır.

Bu bildiriler, içerik olarak Rehber İlkeler ile aynı olmakla beraber ayrıca, İnternetin kullanımının yaygınlaşması ile İnternette kişilerin mahremiyetini tehdit eden cookie veya spyware gibi casus programların artmasına yönelik, üye ülkelerde PET[1] (Mahremiyeti Artırıcı Teknolojiler-Privacy Enhancing Technologies)'in kullanımının teşvik edilmesi gerektiğini ve bu teknolojinin mahremiyetin korunmasında önemli rol oynayabileceğini teyit etmiştir.

PET'ler OECD Mahremiyet Rehber İlkeleri'nde yer alan temel ilkeler çerçevesinde sanayinin önderlik ettiği self-regülasyon ve hukuki düzenlemeler ile bunların karışımı olan yöntemler çerçevesinde mahremiyetin korunmasına yönelik ilke ve hedeflerin gerçekleştirilmesine yardımcı olmaktadır. PET'ler

[1] PET teknolojileri, İnternette boy gösteren ve kişisel mahremiyeti tehdit eden programlara karşı geliştirilmiş, koruyucu programlardır. Örneğin, cookieleri önlemek için cookie engelleyici yazılımlar gibi.

bir anlamda kişilerin kendi kişisel bilgilerini kontrol etmelerine imkan sağlamaktadır.

3.2.2. Güvenlik kültürüne ilişkin politika

Bilgi sistem ve ağlarına yönelik tehdit ve risklerin artması ve bunlarla mücadele etmek amacıyla uluslararası işbirliğini geliştirmek için 1992 yılında OECD Konseyi tarafından "Şebeke ve Bilgi Sistemlerinin Güvenliğine ilişkin Rehber İlkeler: Güvenlik Kültürüne Doğru" adlı rehber ilkeler hazırlanmıştır.

Gelişen teknolojiye uyumun sağlanması amacıyla 1997 yılında gözden geçirilen söz konusu Rehber İlkeler, OECD Konseyi tarafından onaylanarak üye ülkelere tavsiye olarak sunulmuştur. Ancak 11 Eylül saldırılarının meydana gelmesi, konunun uluslararası boyutuna dikkat çekmiş ve Rehber İlkeler 2002 yılında oluşturulan OECD Uygulama Planı (Implementation Plan) kapsamında günün teknolojik gelişmelerine paralel olarak yeniden güncellenmiştir.

"Güvenlik Kültürüne Doğru" adlı Rehber İlkeler, üye ülkelerin

- Toplum değeri ile bağdaşık güvenlik kültürü benimsemelerini ve teşvik etmelerini, mevcut politika, uygulama, önlem ya da prosedürlerini değiştirmelerini ya da yenilerini oluşturmalarını,
- Rehber İlkeleri uygulamak için ulusal ve uluslararası düzeyde işbirliği yapmalarını, koordinasyon sağlamalarını ve tüm kullanıcıların sorumluluklarını belirlemelerini [27]

tavsiye etmektedir.

Ayrıca, sözkonusu ilkeler kamu kurumları, iş çevreleri, sivil toplum kuruluşları ve bireysel kullanıcılar da dahil olmak üzere tüm kamu ve özel sektöre dağıtılmasının, uygulamaya konulmasının ve bilgi sistem ve ağlarının güvenliği ile ilgili konularda uluslararası işbirliğinin kuvvetlendirilmesi için her beş yılda bir gözden geçirilmesinin faydalı olacağını vurgulamıştır.

Ülkelerin haberleşme özgürlüğü ve mahremiyet gibi demokratik toplum değerleri ile bağdaşık "Güvenlik Kültürü" nü oluşturmayı hedef alan Rehber İlkeler Ek'te kapsamlı şekilde sunulmaktadır.

3.2.3. İstek dışı haberleşmeye ilişkin politika

OECD'nin istek dışı haberleşme ile ilgili çalışmaları 2000'li yıllarda başlamıştır. Bu kapsamda OECD, üye ülkelere başta hükümetler, ilgili kamu kurumları ve düzenleyici kurumlar olmak üzere, İSS'ler, iş ve ticaret dünyası, sivil toplum kuruluşları gibi bir çok aktörün dayanışma ve işbirliğinde bulunmalarını ve konuyla ilgili düzenleme yapmalarını tavsiye etmektedir.

İstek dışı haberleşmenin azaltılması için hukuki ve teknik alanda yapılacak çalışmaların ve düzenlemelerin yanı sıra eğitim, bilinçlendirme ve daha da önemlisi self-regülasyon ile desteklenmesinin bu konuda büyük yarar sağlayacağını da vurgulamaktadır [23].

Ayrıca, İSS'lere istek dışı mesajları bloke etme yetkisi ve yükümlülüğünün verilmesi, yapılacak hukuki düzenlemelerde mesaj gönderen kişilerin sahte isim kullanmaları, mesajın içeriği ile ilgili olmayan ve kişiyi yanıltıcı ve aldatıcı konu başlığı ve başka kişiye ait e-posta adresi kullanılması hususunda cezai müeyyide uygulanmasını ve uluslararası işbirliğini önermektedir.

Üye ülkelere bakıldığında Türkiye ve Yeni Zelenda dışında diğer ülkelerin konuya ilişkin düzenleme yaptıkları ve tedbir aldıkları görülmekte, bunun yanısıra, bazı ülkelerin ikili işbirliğine girerek istek dışı haberleşmeye karşı mücadele etmekte olduğu görülmektedir .

3.3. Avrupa Birliği

AB (Avrupa Birliği)'nin, bilgi güvenliği ve mahremiyetin korunması konusundaki çalışmaları 1987 yılında başlamıştır.

Bu çerçevede AB, bilgi ve iletişim teknolojileri üzerinde bilgi güvenliğinin sağlanması ve mahremiyetin korunması konusunda gelişen teknolojik ve sosyal ihtiyaçları da dikkate alarak telekomünikasyon sektöründe serbestleşmenin Topluluk içinde 2000 yılına kadar tamamlanmasının hedeflendiği 1998 mevzuatı çerçevesinde, aşağıda belirtilen mevzuatı düzenleyerek yürürlüğe koymuştur:

a) Kişisel verilerin işlenmesi ve bu bilgilerin serbestçe dolaşımı hususunda bireylerin korunmasına ilişkin 95/46/EC sayılı AB Direktifi [28],
b) Telekomünikasyon sektöründeki kişisel verilerin işlenmesi ve mahremiyetin korunmasına ilişkin 97/66/EC sayılı AB Direktifi [35].

Diğer taraftan AB, özellikle 1995'li yıllardan itibaren İnternet ve multimedya teknolojilerinin toplum tarafından çok büyük bir hızla kullanılır hale gelmesiyle birlikte özellikle, İnternet teknolojilerinin beraberinde getirdiği bazı kolaylıklar ve imkanlara ilaveten küçük çoçukların İnternet ortamındaki

muzır yayınlardan korunması amacıyla "Küresel ağlar üzerinde zararlı ve yasadışı içerikle mücadeleyle İnternetin daha güvenli kullanımı" hususunda 99/276/EC sayılı bir Karar yayınlamıştır.

Ayrıca, 1998 tarihli mevzuat çerçevesinde telekomünikasyon sektöründe hedeflenen serbestleşmeyi tamamlayan AB, bu kez teknolojideki ve buna bağlı olarak da telekomünikasyon sektöründe

- ses ve veri
- telekomünikasyon ve radyo-TV yayını
- sabit ve mobil

hizmetler olmak üzere üç farklı alanda gerçekleştirilen ve toplum hayatını ve dolayısı ile de telekomünikasyon alanındaki düzenlemeleri derinden etkileyen yakınsama konusunu dikkate alarak 2002 tarihinde yeni bir düzenleyici çerçeve mevzuatını hazırlayarak yürürlüğe koymuştur.

Yukarıda belirtilen hususlar çerçevesinde telekomünikasyon, radyo-TV yayın, sabit ve mobil hizmetler, ses ve veri hizmetleri, İnternet ve multimedya hizmetlerindeki bu yakınsama nedeniyle artık AB, 1998 tarihli çerçeve mevzuatında yer alan ve teknolojiye bağlı olan diğer bir deyişle belirli bir teknolojiyi çağrıştıran "telekomünikasyon", radyo-TV yayıncılığı", "uydu hizmetleri", "sabit ses hizmetleri", "mobil hizmetler", "veri hizmetleri" gibi tanım ve ifadeler yerine tüm bunları tek bir başlık altında kapsayacak şekilde ve teknoloji nötür bir ifade olan dolayısı ile de teknolojilerin her alanında yakınsamayı ifade eden "elektronik haberleşme şebekeleri ve hizmetleri" şeklinde farklı bir tanımı gündeme getirmiştir.

Bu kapsamda, 2002 yılında kabul edilen ve 2003 yılında AB üyesi ülkelerde yürürlüğe giren yeni çerçeve düzenleyici paket kapsamında 1998 tarihli

mevzuatta yer alan telekomünikasyon sektöründeki kişisel verilerin işlenmesi ve mahremiyetin korunması konusundaki 97/66/EC sayılı AB Direktifi'nin [35] yerine geçen elektronik haberleşme sektöründe mahremiyetin korunması ve kişisel verilerin işlenmesi hususundaki 2002/58/EC [33] sayılı Direktifi yürürlüğe koymuştur.

Bunların yanı sıra, AB yukarıda sayılan direktifleri tamamlayıcı nitelikte olmak üzere aşağıda belirtilen bazı kararlar almıştır.

a) Bilgi güvenliğinin sağlanmasına ilişkin 31 Mart 1992 tarih ve 92/242/EC sayılı Konsey Kararı,
b) Şebeke ve bilgi güvenliği kültürüne doğru Avrupa'nın yaklaşımına ilişkin 18 Şubat 2003 tarih ve 2003/48/EC sayılı Konsey Kararı,
c) Şebeke ve bilgi güvenliğinin iyileştirilmesi ve uygulamanın yayılması ile ilgili e-Avrupa Eylem Planı'nın izlenmesine ilişkin 17 Kasım 2003 tarih ve 2256/2003/EC sayılı Konsey Kararı,

Ayrıca, yukarıda belirtildiği üzere kişisel verilerin ve mahremiyetin korunmasına yönelik olarak bir çok farklı alanda düzenleme yapma ihtiyacı hisseden AB, sözkonusu düzenlemelerden özellikle genel anlamda ve sektör spesifik alanda olmak üzere iki ayrı yapı halinde kurumsallaşmaya doğru da bir adım atmıştır. Bu çerçevede kişisel verilerin ve mahremiyetin korunmasına yönelik olarak 95/46/EC sayılı Direktifte belirtilen hususlara kurumsal bir yapı kazandırmak amacıyla "Topluluk kurumları tarafından kişisel verilerin işlenmesi, kişilerin korunması ve bilgilerin serbest dolaşımı"na ilişkin olarak onayladığı 2001/45/EC sayılı Tüzük ile AB içinde ilk kez "Veri Koruma Görevlisi" ve "Avrupa Veri Koruma Denetmeni" gibi bazı görev ve fonksiyonlara işlerlik kazandırılmıştır.

Benzer şekilde sektör spesifik bir alanda, sadece telekomünikasyon sektörüne özgü olmak üzere ve bu kapsamda düzenleme amacıyla yürürlüğe konulan 2002 tarihli yeni düzenleyici çerçeve mevzuatı kapsamında kabul edilen elektronik haberleşme şebeke ve hizmetleri konusundaki 2002/58/EC sayılı Direktif ve 99/276/EC sayılı Karar'a ilişkin hükümleri de kapsayacak şekilde AB tarafından "Avrupa Şebeke ve Bilgi Güvenliği Kurumu"nun (ENISA) kurulması amacıyla 2004/460/EC sayılı Tüzük [40] yayınlanmıştır.

Yukarıda belirtilen hususlara ilaveten AB, özellikle tüm dünyada 1990'lı yıllardan itibaren gelişen ve yaygınlaşan elektronik ticaret ve elektronik imza uygulamalarına özgü çıkartmış olduğu 2000/31/EC ve 99/93/EC sayılı Direktifler'de de kişisel verilerin ve mahremiyetin korunmasını sağlamak üzere kriptografi ve elektronik imza teknolojileri çerçevesinde uygulanan standartlara ilişkin olarak bazı hükümler getirmiştir, ancak tez kapsamı dışında bulunması nedeniyle bu iki Direktif incelenmemiştir.

3.3.1. Kişisel verilerin korunmasına ilişkin politika

Avrupa Birliği, bünyesindeki kurumlar ile üye devletler arasında hukuki, ticari ya da idari işlemler nedeni ile kişisel verilerin serbest dolaşımının her geçen gün artması ve buna bağlı olarak kişisel verilerin, bireylerin hak ve özgürlüklerine dokunmadan mahremiyetlerinin korunmasındaki zorunluluk nedeniyle hukuki bir düzenlemeye gerek duymuştur.

Bu gereklilik üzerine AB üyesi ülkeler arasında farklı veri koruma uygulamalarını kaldırmak ve uygulamada bütünlüğü sağlamak amacıyla, kişisel verilerin korunması ve mahremiyetin sağlanması ile ilgili olarak 95/46/EC Sayılı Direktif [28] yayınlanmıştır.

Bunun yanı sıra, 1980'li yıllarda geliştirilen yeni sayısal teknolojiler sayesinde telekomünikasyon şebekelerinde interaktif hizmetlerin artması ve ISDN (Tümleşik Hizmetler Sayısal Şebekesi-Integrated Services Digital Netwok) olarak da adlandırılan sayısal santrallerin kullanıma girmesi bu alanda kişisel verilerin ve mahremiyetinin sağlanması hususunu gündeme getirmiştir.

Bu nedenle, AB üyesi ülkelerdeki telekomünikasyon alanında kişisel verilerin işlenmesi ve saklanması ile ilgili topluluk içinde bir uyum sağlamak üzere 97/66/EC sayılı Direktif [35] çıkarılmıştır. 15 Aralık 1997 tarihli Telekomünikasyon Sektöründeki Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması ile ilgili Direktif kişisel veriler konusunda Topluluk hukuku alanında bir çerçeve oluşturmaktaydı. Sektör spesifik bir alanda düzenleme yapan bu direktif ile telekomünikasyon sektöründe mahremiyetin korunması ve kişisel verilerin işlenmesi hususu teminat altına alınmıştı.

Diğer taraftan, direktif doğrudan telekomünikasyon sektöründeki kişisel verilerin işlenmesi ve mahremiyetin korunması hususunu içermesi nedeniyle 95/46/EC sayılı Direktifi tamamlar nitelikteydi.

Ancak ISDN Direktifi olarak da adlandırılan sözkonusu direktif, telekomünikasyon sektöründe meydana gelen gelişmeler üzerine güncellenme gerekliliğini ortaya koymuştur. Bunun üzerine 97/66/EC [35] sayılı Direktif 30 Ekim 2003 tarihi itibariyle yürürlükten kaldırılarak bunun yerine direktifin içeriğini daha da genişleten 2002/58/EC sayılı Direktif [33] yürürlüğe konmuştur.

Çizelge 3.2. Kişisel Verilerin Korunmasına İlişkin AB Mevzuatı

Yürürlük Tarihi	Direktif Adı
24 Ekim 1995	Kişisel Verilerin İşlenmesi ve Bilgilerin Serbestçe Dolaşımı Hususunda Bireylerin Korunmasına İlişkin 95/46/EC Sayılı Direktif
15 Aralık 1997	Telekomünikasyon Sektöründeki Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunmasına İlişkin 97/66/EC Sayılı AB Direktifi
1 Ağustos 2002	Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması
18 Aralık 2001	Topluluk Kurumları Tarafından Kişisel Verilerin İşlenmesi Kişilerin Korunması ve Bilgilerin Serbest Dolaşımına ilişkin 2001/45/EC Sayılı Tüzük

3.3.1.1. Kişisel Verilerin İşlenmesi ve Bilgilerin Serbestçe Dolaşımı Hususunda Bireylerin Korunmasına İlişkin 95/46/EC Sayılı Direktif

Direktif, Avrupa Birliği'nde bireylerin AB vatandaşı olsun olmasın kişisel verilerinin Avrupa Birliği sınırları dahilinde serbest dolaşımını sağlayacak açık ve güvenli bir düzenleme yapılmasını amaçlamaktadır. Nitekim bu amaç altında bilgi toplumunun ve hizmet sektörünün gelişimini kolaylaştırılacak ve aynı zamanda kişisel verilerin işlenmesinde gerçek kişilerin korunması için yüksek bir koruma düzeyi sağlanmış olacaktır [15].

Bilgi toplumu çalışmaları çerçevesinde, kullanılan teknoloji sayesinde kişilere ilişkin her türlü ses ve görüntünün iletilmesi, muhafaza edilmesi, alınması, depolanması ve işlenmesi, kişilerin mahremiyetinin korunması açısından önemli olduğundan, sözkonusu direktifin hükümleri bu tip verilerin işlenmesi ile ilgili hususlara da uygulanabilmektedir. Ayrıca, bu tip verilerin işlenmesi

otomatik olarak yapılıyor ise, bu direktifin kapsamı içinde değerlendirilmesi gerekmektedir.

Direktifte, Avrupa İnsan Hakları Sözleşmesi'nin ilgili hükümleri çerçevesinde, kişilerin temel hak ve özgürlüklerinin yasal bir gerekçe olmadığı sürece herhangi bir şekilde kısıtlanamayacağı belirtilmekte ve bu çerçevede kişisel verilerin iletilmesi, işlenmesi ve kaydedilmesinde uygulanacak olan usul ve esaslar ele alınmaktadır. Bununla beraber, cezai ya da adli soruşturma gibi yasal gerekçesi olan durumlarda sözkonusu direktifin hükümleri uygulanmamaktadır.

Direktifte kişisel verilerin işlenmesi ve üye ülkelerde serbestçe dolaşımına ilişkin kısaca şu hususlara yer verilmektedir:

- Kişisel verilerin sadece Topluluk içindeki kurumlar ve üye devletler arasında herhangi bir engelle karşılaşmadan serbest dolaşımının sağlanmasının garanti edilmesi, hakkında bilgi toplanan kişilerin mahremiyetinin sağlanması ve bu bilgilerin tüm üye ülkelerde aynı derecede korunması,
- Yasal hükümler çerçevesinde gerektiğinde ilgili idare tarafından kamu sağlığı ve güvenliğinin sözkonusu olduğu durumlarda bu direktif haricinde karar alınabilmesi,
- Kişisel verilerin yasal hükümler çerçevesinde belli bir amaçla toplanabilmesi ve hakkında bilgi toplanan kişinin bu hususta bilgilendirilmesi,
- Toplanan verilerin toplanma amacı dışında kullanılmaması,
- Kişilere ait hassas verilerin sadece amacı kapsamında muhafaza edilmesi ve işlenmesi, kişinin rızası olmadığı sürece bu verilerin yasaklanması gerektiği, ancak sağlık sorunları gibi herhangi bir

sebepten ilgili kişinin rızasının alınması olanak dahilinde değilse, ilgilinin kişisel verilerinin kamu gereği işlenmesi,

- Tarihi inceleme, istatistiksel araştırma ya da diğer bilimsel çalışmalar nedeniyle kişisel verilerin yasal düzenlemeler çerçevesinde toplanarak işlenmesi,
- Kişilere ilişkin verilerin toplanarak işlendiğinde ya da üçüncü şahıslara bu bilgilerin ifşa edilmesi durumunda, sözkonusu kişinin haberdar edilmesi [28] gerektiği ifade edilmektedir.

Direktif sadece bilgisayarda işlenen verileri değil kağıt üzerinde toplanan verileri de koruma altına almaktadır. Ancak kişinin kendisi için tuttuğu özel kayıtlar direktif kapsamına girmemektedir [15].

Direktif kişisel verilerin Topluluk kurumları içinde ve üçüncü ülkelere transferinde de bir takım düzenlemeler ortaya koymaktadır. Bu kapsamda, AB üyesi olmayan ülkelere veri transfer edilebilmesi ancak o ülkenin AB veri koruma ölçütlerine uygun olması halinde yerine getirilebilmektedir. Bu durumda üçüncü taraf ülkenin veri koruma mevzuatı, ülkedeki temel hak ve hürriyetlerin korunması ve kişinin mahremiyet alanının korunma düzeyi dikkate alınmaktadır. Bu şartlar arasında, transfer edilen verilerin niteliği (özellikle hassas olup olmamaları) ve ilgililerin kimliğinin belirlenebilirliği önem kazanmaktadır. Ayrıca transferde amaca bağlılık, verilerin hangi boyutta farklı işlem çeşitlerine tabi olduğu, ilgililerin bilgi edinme hakkının olup olmadığı ve uygulaması değerlendirilmektedir. Ancak 108 nolu Avrupa Konseyi Sözleşmesi'ni imzalayan ülkeler etkin veri koruması mekanizması geliştirmiş olmaları şartıyla koruma düzeyi itibariyle uygun kabul edilmektedir.

Buna ilaveten, veri güvenliğini uygun koruma altına almamış ülkelerle karşılıklı taahhüt anlaşması imzalanarak da yeterli garantinin sağlanması durumunda veri transferi gerçekleştirilebilmektedir.

Bu bağlamda 1988 yılında Fiat bünyesinde faaliyet gösteren Fransız şirketinin yönetim kadrosunun kişisel verilerini Torino'da bulunan merkeze transfer etmek için Fransa, veri koruması kontrol biriminden CNIL (Medeni Haklar Enformasyon Teknolojisi Ulusal Komisyonu-National Commisison on Information Technology and Civil Liberties) izin istemiştir. Amaç, verileri o dönemde merkezde oluşturulan insan kaynakları veri bankasına dahil etmekti. Ancak CNIL, İtalya'da o dönemde henüz yeterli bir koruma düzeyi yaratılmadığı için veri transferine izin vermemiştir. Bu sebeple Fiat ile Fransız şirket arasında Fransız veri koruması ilkelerini içeren bir sözleşme imzalanmıştır. Yapılan sözleşme üzerine CNIL veri transferine izin vermiş ve verileri transfer edilen kişiler bilgi edinme ve düzeltme haklarından yararlanmışlardır [15].

Diğer bir örnek ise, AB standartlarına uygun veri koruma düzeyine sahip olmayan ABD ile AB arasındadır. ABD adına Ticaret Bakanlığı ve AB adına da Avrupa Komisyonu arasında Temmuz 2000'de yapılan anlaşma sonucu "Safe Harbor" (Güvenli Liman)[1] olarak tabir edilen bir çerçeve yapı geliştirilerek uygulamaya koyulmuştur [29]. Böylece AB firmaları, ticari ilişkide bulundukları ABD firmalarına transfer ettikleri kişisel verilerinin AB mevzuatına uygun olarak korunmasını garanti altına almış bulunmaktadırlar.

---

[1] "Safe Harbor" uygulamasına iştirak eden firmaların listesi http://export.gov/safeharbor internet adresinde yayınlanmakta ve liste peryodik olarak güncellenmektedir. Listeye kayıt olan firmalar "Safe Harbor" ilkesi çerçevesinde davranmaktadırlar. Sözkonusu listeye iştirak, ABD firmaları açısından tamamen keyfi olup, her firma "Safe Harbor" uygulamaları çerçevesinde belirlenen ilkelere uygun olarak kendi mahremiyet ilkelerini hazırlamak ve bunu kendi internet sitelerinde yayınlamak ve buna uymakla yükümlü bulunmaktadır.

Böylece AB üyesi ülkelerin, ABD firmaları ile çok daha rahat ticari ilişkide bulunması sağlanmıştır. Bu çerçevede kişisel verilerin transferinde AB üyesi ülke tarafından talep edilen ön izin kaldırılarak eşit koruma garantisi sağlanmış olmaktadır.

Yukarıda belirtilen hususlar ışığında, sözkonusu Direktif gereğince her üye devletin ulusal sınırlar dahilinde kişisel verilerin işlenmesi ve buna ilişkin usul ve esasların uygulamasından sorumlu olmak üzere bağımsız kamu kurumu niteliğinde bir "Denetim İdaresi" (Supervisiory Authority) kurmaları gerekmektedir.

Bu denetim idaresinde görev yapacak olan, gerçek ya da tüzel kişi olabilen kontrolör (controller), kişisel verilerin işlenmesinde kullanılacak araç ve yöntemi belirlemekle ve bu bilgilerin hangi amaçla işleneceğini tespit etmekle görevlidir. Ayrıca, kişisel verilerin kazara ya da yasadışı yolla imhası, alıkonulması ya da işlenmesini önlemek için gereken her türlü tedbiri almakla yükümlü bulunmaktadır.

AB'ye üye devletlerin tümü verilerin korunması ile ilgili olarak sözkonusu direktifi ulusal mevzuata geçirerek, ilgili yasaları yürürlüğe koymuşlar ve bu yasaların uygulanmasından sorumlu bağımsız düzenleyici kurumu hayata geçirmişlerdir [30].

Çizelge 3.3. 95/46/EC sayılı Direktifin AB Üyesi Ülkelerdeki Durumu

Ülke	Yasal Düzenleme	Veri Koruma Kurumu
Almanya	1977 yılında yürürlüğe giren Federal Veri Koruma Yasası, Direktifi uyumlaştırmak amacıyla 2001 yılında güncellenmiştir.	Federal Veri Koruma Görevlisi (Federal Data Protection Commissioner)
Avusturya	Veri Koruma Yasası ile Direktif 1 Ocak 2000 tarihinde iç mevzuata aktarılmıştır.	Veri Koruma Komisyonu (Data Protection Commission)

Belçika	8 Aralık 1992 yılında yürülüğe giren Kişisel Verilerin Korunması Yasası, Direktifi uyumlaştırmak amacıyla 11 Aralık 1998 tarihinde güncellenmiştir.	Mahremiyeti Koruma Komisyonu (Commission for the Protection of Privacy)
Danimarka	Kişisel Verilerin İşlenmesi Hakkındaki Yasa ile Direktif 31 Mayıs 2000 tarihinde iç mevzuata aktarılmıştır.	Veri Koruma Ajansı (Data Protection Agency)
Finlandiya	Kişisel Veri Koruma Yasası ile Direktif 1 Haziran 1999 tarihinde iç hukuka aktarılmıştır.	Veri Koruma Kurulu (Data Protection Board)
Fransa	6 Ocak 1978 tarihinde yürülüğe giren Enformasyon Teknolojisi, Dosya ve Özgürlükler Yasası, Direktifi uyumlaştırmak amacıyla 15 Temmuz 2004 tarihinde güncellenmiştir.	Medeni Haklar ve Enformasyon Teknolojisi Ulusal Komisyonu (National Commission on Information Technology and Civil Liberties-CNIL)
Hollanda	Kişisel Verilerin Korunması Yasası ile Direktif 6 Temmuz 2000 tarihinde iç mevzuata aktarılmıştır.	Veri Koruma Kurumu (Data Protection Authority)
İngiltere	Veri Koruma Yasası ile 1998 yılında Direktif iç mevzuata aktarılmıştır.	Bilgi Görevlisi (Information Commissioner's Office)
İrlanda	1998 yılında yürülüğe giren Veri Koruma Yasası 10 Nisan 2003 tarihinde Direktif ile uyumlaştırılmak amacıyla güncellenmiştir.	Veri Koruma Görevlisi (Data Protection Commissioner)
İspanya	Gerçek Kişilere dair Verilerin Korunması Yasası ile 1999 yılında Direktif iç mevzuata aktarılmıştır.	Veri Koruma Ajansı (Data Protection Agency)
İsveç	Kişisel Verilerin Kaydedilmesine ilişkin Yasa ile Direktif 1998 yılında iç mevzuata aktarılmıştır.	Veri Teftiş Kurulu (Data Inspection Board)
İtalya	1996 yılında yürülüğe giren Veri Koruma Yasası Direktif ile uyumlaştırılmak amacıyla 30 Haziran 2003 tarihinde güncellenmiştir.	Kişisel Verileri Koruma Kurumu (Authority for the Protection of Personel Data)
Lüksemburg	30 Mart 1979 tarihinde yürürlüğe giren Veri Koruma Yasası 2 Ağustos 2002 tarihinde Direktif ile uyumlaştırılmıştır.	Veri Koruma Ulusal Komisyonu (National Data Protection Commission)
Norveç	Kişisel Veriler Yasası ile Direktif 2000 yılında iç mevzuata aktarılmıştır.	Veri Teftiş Kurulu (Data Inspection Board)
Portekiz	Kişisel Verilerin Korunması Yasası ile Direktif 26 Ekim 1998 tarihinde iç mevzuata aktarılmıştır.	Ulusal Veri Koruma Komisyonu (National Data Protection Commission)
Yunanistan	Kişisel Verilerin İşlenmesi ile ilgili Bireylerin Korunması Hakkındaki Yasa ile Direktif 1997 yılında iç mevzuata aktarılmıştır.	Veri Koruma Kurumu (Hellenic Data Protection Authority)

Kaynak [31]

3.3.1.2. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunmasına ilişkin 2002/58/EC Sayılı Direktif

1 Ağustos 2002 tarihinde yürürlüğe giren 2002/58/EC sayılı Direktif, özünde 97/66/EC sayılı Direktif ile aynı olmakla beraber internet ve multimedya teknolojilerinin yaygın olarak kullanıma girmesi ile beraber eski direktifte bulunmayan istenmeyen e-posta, SMS (Kısa Mesaj Servisi-Short Message Service), MMS (Çoklu Ortam Mesaj Sistemi-Multimedia Messaging System) ve "cookie"ler gibi yeni kavram ve tanımları ele almıştır. Dolayısı ile ISDN teknolojisi kapsamında kişisel verilerin işlenmesi ve korunması yönünde çıkartılmış bulunan 97/66/EC sayılı AB Direktifinden farklı olarak 2002/58/EC sayılı Direktifin temel ve en önemli özelliği, teknolojideki yakınsamayı dikkate alarak teknoloji nötür olarak kişisel verilerin ve mahremiyetin korunmasını sağlamasıdır.

Sözkonusu direktifte şu hususlara yer verilmiştir:

Haberleşmenin gizliliği, direktifte haberleşmenin gizliliği esas alınarak telefon, e-posta SMS ve MMS mesajları dahil her türlü haberleşmenin başka kişilerce dinlenmemesi öngörülmektedir. Diğer taraftan günümüzdeki haberleşme trafiğinde bilgisayarların da önemli bir yeri olduğundan internet uygulamalarında çok sık kullanılan "spyware" ve "cookie"lere dikkat çekilmiştir.

Bu tür yazılımlar, kişinin bilgisayarındaki verilere ulaşılabilmesinin yanısıra, kişinin hangi siteyi ne zaman ve hangi sıklıkla ziyaret ettiği gibi bilgilere de ulaşılabilmesine imkan sağlayarak kişisel verilerin elde edilmesini mümkün kılmaktadır. Bu nedenle direktif bu tür programların kullanılması durumunda kullanıcının haberdar edilmesini ve eğer kişinin rızası yoksa kişinin bunu reddetmesine imkan sağlanmasını öngörmüştür. Ancak e-ticaret

uygulamalarında bu tür uygulamalar oldukça büyük avantaj sağlamakta olduğundan bu tür programlarla elde edilen kişisel verilerin anonimleştirilerek istatistiki amaç için kullanılması serbest bırakılmıştır.

Bu kapsamda, her internet sitesinin kullanıcının hak ve yükümlülüklerinin ne olduğu ve sitenin mahremiyet konusunda kullanıcıyı bilgilendirmesi gereklidir.[1]

Trafik verilerinin işlenmesi ve depolanması, direktif trafik verilerinin[2] iletişimin sonunda silinmesini ya da kime ait olduğunun belirsizleştirilmesini öngörmektedir. Zira, kişilerin telefon görüşmesi, e-posta, SMS mesajları telekomünikasyon şebekelerinde, ayrıntıları ile saklanabilmektedir. Tüm bu ayrıntılar sayesinde kişilerin portresi çıkartılabilmektedir. Bu nedenle, direktif trafik verilerinin gizliliğinin garanti edilmesini öngörmektedir. Ancak direktif, elektronik şebeke ve hizmet sağlayıcılarının, trafik verilerini sadece faturalandırma ve ücretlendirme amacıyla kullanabilmesini ve bu işlem yapıldıktan sonra verilerin silinmesi gerektiğini hükme bağlamıştır. Faturalandırma amacıyla trafik verilerinin depolanma süresi, genel olarak bir faturaya hukuken itiraz edilebilecek süreyle bağlantılı olup AB üyesi ülkeler arasında bu konuda çok büyük farklılıklar bulunmaktadır[3]. [32]

Telefon rehberlerinin oluşturulması, ilgili idare tarafından gerek görüldüğünde telekomünikasyon hizmetlerinde kullanılan ve halka dağıtılan telefon rehberi ya da 118 bilinmeyen numaralar hizmetinde olduğu gibi, gerçek kişilere ait kişisel verilerin yayınlanmasını ve arzu edilmeyen bir

---

[1] IAB (İnteraktif İlan Bürosu-Interactive Advertising Bureau) çevrim içi yapılan işlem ve prosedürlere ilişkin uygulanacak usul ve esasları geliştiren bir kuruluştur. Kuruluş, kendi kurduğu site ile kullanıcılara cookielerin ne olduğu, nasıl çalıştığı hususunda bilgi vermektedir.

[2] Trafik verisi, bir elektronik haberleşme şebekesindeki bir haberleşmenin iletilmesi için ya da bu haberleşmenin faturalandırılması için işlenen her türlü bilgidir.

[3]Finlandiya'da 3 ay, İngiltere'de 6-12 ay, Hollanda'da ise 3 ay arasında değişmektedir.

şekilde kullanılmasını önlemek amacıyla kişisel verilerin yer aldığı rehberlerin yayınlanmasına ve dağıtılmasına bazı kısıtlamalar getirilebilmektedir. (Kişisel verilerin açıklanması gerekli olduğu ölçüde yani isim sorulduğunda sadece telefon bilgisinin açıklanması gibi.)

Ayrıca kullanıcılarda

- Telefon rehberinde yer almama,
- Cinsiyetlerine ilişkin herhangi bir verinin yer almaması,
- Adresinin kısmen yada tamamen telefon rehberinde yer almaması,
- Kişisel verilerinin doğrudan pazarlama amacıyla kullanılmaması

gibi istekte bulunma haklarına sahip bulunmaktadır.

Bu konuda, sözkonusu direktifin 97/66/EC sayılı Direktiften [35] farkı bu hizmetlerin ücret alınmadan gerçekleştirilmesidir.

Konum bilgisi, abonenin terminal cihazının bulunduğu coğrafi konumu [33] tanımlamaktadır. Günümüzde GPS (Global Positioning System)'ler[1] ve mobil telefonlar sayesinde kişinin konum bilgisi bir kaç metre hassasiyete kadar belirlenebilmektedir. Bu nedenle kişinin konum bilgisi kişisel veri olarak nitelendirilmekte olduğundan, sözkonusu direktife 97/66/EC sayılı Direktiften [35] farklı olarak konum bilgisi hükmü getirilmiştir. Konum bilgisi, ulusal mevzuat çerçevesinde abonenin konumuna bağlı verilerinin o abonenin bilgisi ve rızası dahilinde işlenmesi, bu verilerin üçüncü bir tarafa iletilip iletilmemesi ve bu verilerin türü ve işlenme süresi konusunda abonenin bilgilendirilmesini öngörmüştür. Ancak, acil durumlarda ulusal güvenlik ya da adli soruşturmada

[1]Uydular vasıtasıyla cisimlerin yerini kesin olarak tesbit etmeye yarayan sistem GPS olarak adlandırılmaktadır.

bu konum bilgileri abonenin rızası dışında yasalar çerçevesinde kullanılabilmektedir.

İstenmeyen mesajlar, bu kapsamda direktif, 97/66/EC sayılı Direktife [35] e-posta, SMS ve MMS kriterlerini getirmiş bulunmaktadır. Direktif, faks, e-posta, SMS ya da MMS gibi her türlü mesajın kişinin önceden rızası ve bilgisi olmadan gönderilemeyeceği ve ticari amaçla kullanılamayacağını hükme bağlamış ve üye ülkelerin bu konuda kurallar koyması gerekliğini vurgulamıştır. Ancak ülkeleri kapsam içi (opt-in)[1] veya kapsam dışı (opt-out)[2] seçeneği konusunda serbest bırakmıştır [34].

Diğer taraftan, müşterilerinin e-posta adreslerini alan gerçek ya da tüzel kişiler, müşterilerine kendi ürünleri ile ilgili olarak doğrudan reklam amaçlı iletiler gönderebilecektir. Ancak, müşterilerine reklam amaçlı e-posta gönderecek olan firmaların mesaja konu ile ilgili açıklayıcı başlık koyması ve bir daha bu tür mesajın alınmamasını kolaylaştıracak yöntemleri kolay ve ücretsiz bir yolla sunması gereklidir. Aksi durum istenmeyen mesaj olarak değerlendirilecek ve istek dışı haberleşme yasağına tabi olacaktır.

AB ülkelerinde e-posta ve SMS dahil olmak üzere ticari haberleşmede istek dışı haberleşme için kapsam içi yöntemi genel olarak kabul görmüş, bu konuda üye ülkelerin gerekli tedbirleri alması istenmiştir.

Arayan ve aranan hattın kimliğinin gösterilmesi, hizmeti 97/66/EC sayılı Direktifte [35] de ele alınmıştır. Ancak sözkonusu direktifte teknoloji nötr olarak ifade edilmektedir. Direktif arayan hattın aranan hattın ekranında görülebilmekte ise, arayana her bir arama için ücrete tabi olmaksızın

[1] Kişinin rızası ve onayının olmaması durumunda hiçbir şekilde mesaj gönderilememesi.
[2] Gelen mesajın içinde bir daha mesajın alınmamak istemesini kolaylaştıran bir yöntemin olması veya mesaj almak istemediklerini belirten kişiler dışındakilere mesajın gönderilmesi.

numarasının görünmesini engelleme olanağı verilmesini, aynı şekilde, aranan kullanıcıya da arayan hattın ekranında görülmesini engelleme olanağı ücretsiz olarak sunulmasını hükme bağlamıştır.

Acil durum çağrıları, 97/66/EC sayılı Direktiften [35] farklı olarak sözkonusu direktife konulan bu hizmette, telekom operatörleri arayan hattın ekranda görünmesi hizmetini trafik kazası, deprem, sel yangın gibi acil durumlarda can ve mal güvenliğini sağlamak için, ilgili sağlık ve ilk yardım kurtarma kuruluşlarına vermekle yükümlüdürler.

Otomatik arama yönlendirme, direktif, tüm abonelerin ücretsiz ve basit bir işlemle üçüncü bir tarafın abonenin kendi terminaline otomatik olarak yönlendirmede bulunmasını engelleme olanağına sahip olmasını hükme bağlamıştır.

Çizelge 3.3. 2002/58/EC Sayılı Direktifin AB Üyesi Ülkelerdeki Durumu

Ülke	Hukuki Durum
Almanya	1997 tarihli Telekomünikasyon Hizmetlerinde Veri Koruma Yasası ile (Teledienstedatenschutzgesetz, TDSG) özel olarak internete ilişkin hükümler getirmekte, ayrıca 1997 tarihli Telekomünikasyon Yasası da (Telekommunikationsgesetz, TKG) verilerin korunmasına ilişkin bazı hükümleri içermektedir. Bunun yanı sıra Haksız Rekabet Yasası ile 2002/58/EC sayılı Direktif 3 Temmuz 2004 tarihinde iç mevzuata aktarılmıştır.
Avusturya	Telekomünikasyon Yasası (Telekommunikationsgesetz) ile 2003 yılında Direktif iç mevzuata aktarılmıştır.
Belçika	E-Ticaret Yasası (E-Commerce Law) ile 11 Mart 2003 tarihinde Direktif iç mevzuata aktarılmıştır.
Danimarka	Marketing Practices Act Yasası ile Direktif 10 Haziran 2003 tarihinde iç mevzuata aktarılmıştır.
Finlandiya	Telekomünikasyon Alanında Veri Güvenliği ve Mahremiyetin Korunmasına ilişkin Yasa (Protection of Privacy and Data Security in Telecommunications Act) 2000 yılında 97/66/EC sayılı Direktifi iç mevzuata aktarmıştır. Ancak 2002/58/EC sayılı direktifi iç mevzuata

	aktarmak amacıyla hazırlanan Elektronik Haberleşme Alanında Mahremiyetin Korunması Yasası (Act on Privacy in Electronic Communications) taslak halinde bulunmaktadır.
Fransa	2002/58/EC sayılı iç mevzuata aktarmak amacıyla hazırlanan Elektronik Ekonomi Yasası (Trust in Electronic Economy Act) taslak halinde bulunmaktadır.
Hollanda	Wet implementatie Europes regelgevingskader Yasası ile Direktif 20 Nisan 2004 tarihinde iç mevzuata aktarılmıştır.
İngiltere	1998 tarihli Veri Koruma Yasası, Direktifi iç mevzuata aktarmıştır. (Data Protection Act –DPA)
İrlanda	Direktif Elektronik Haberleşme Şebekeleri ve Servisleri (Electronic Communications Networks and Services), Veri Koruma ve Mahremiyet (Data Protection and Privacy) özel düzenlemeleri ile iç mevzuata aktarılmıştır.
İspanya	Direktif 32/2003 sayılı yasa ile iç mevzuata aktarılmıştır.
İsveç	Direktif özel düzenlemeler ile 1 Nisan 2004 tarihinde iç mevzuata aktarılmıştır.
İtalya	Direktifi iç mevzuata aktarmak amacıyla hazırlanan yasa 1 Ocak 2004'te yürürlüğe girmiştir.
Lüksemburg	Direktifi iç mevzuata aktarmak amacıyla hazırlanan 5181 nolu yasa taslak halinde bulunmaktadır.
Norveç	2000 tarihli Kişisel Bilgiler Yasası (Personopplysningsloven), Direktifi iç hukuka aktarmıştır.
Portekiz	Direktif Elektronik Haberleşme Yasası (Electronic Communications Law) ile 18 Ağustos 2004 tarihinde iç mevzuata aktarılmıştır.
Yunanistan	1999 tarihli 2774 sayılı yasa iletişimde kişisel verilerin korunmasını düzenlemekte olup, 2002/58/EC sayılı Direktifi iç mevzuata aktarmak amacıyla hazırlanan yasa taslak halinde bulunmaktadır.

Kaynak [31]

3.3.1.3. Topluluk Kurumları Tarafından Kişisel Verilerin İşlenmesi Kişilerin Korunması ve Bilgilerin Serbest Dolaşımına ilişkin 2001/45/EC Sayılı Tüzük

18 Aralık 2001 tarihinde kabul edilen 2001/45/EC sayılı Tüzük, 95/46/EC ile 97/66/EC sayılı AB Direktiflerini tamamlayıcı nitelikte olup, Topluluk kurumları tarafından kişisel verilerin işlenmesi ve bu bilgilerin serbest dolaşımına ilişkin usul ve esasları belirlemektedir. Esasen bu Tüzük ile AB bünyesinde ilk kez kişisel verilerin ve mahremiyetin korunması hususuna kurumsal bir nitelik ve yapı kazandırılmıştır.

Sözkonusu Tüzük'te 95/46/EC sayılı Direktifte ve 97/66/EC sayılı Direktifte yer alan hususlara da değinilmiştir. Ayrıca hakkında bilgi toplanan kişiye temin edilecek bilgiler hususunda da bazı açıklamalar getirilmiştir. Bunlar:

- Kontrolörün kimliği,
- Verilerin toplanma, işlenme amacı,
- Bu bilgileri talep edenlerin kimliği,
- Hakkında toplanan bu bilgilere erişim hakkı ve gerekiyorsa düzeltme imkanı,
- Verilerin toplanma ya da işlenmesinin amacı, hukuki dayanağı,
- Verilerin saklanmasına ilişkin süre,
- Avrupa Veri Koruma Kurumu-EDPS (European Data Protection Supervisor)'ye herhangi bir zamanda başvurabilme hakkıdır. [36]

Ayrıca, Tüzük kişisel verilerin toplanmasından ve işlenmesinden sorumlu bağımsız bir kurumun kurulmasını öngörmektedir. Bağımsız teftiş kurumu niteliğinde olan EDPS, topluluk kurumları tarafından yürütülen tüm faaliyetleri bu Tüzüğün maddelerine ve hükümlerine uygunluk açısından denetlemekle yükümlüdür.

Avrupa Veri Koruma Kurumu

Kurum, her üye devletin veri koruma kurumlarından gelen bir temsilcinin yanı sıra AB içinde yer alan kurumlardan gelecek bir temsilciyle AB Komisyonundan gelen bir temsilciden oluşmaktadır.

Kurum Başkanı, Avrupa Veri Koruma Amiri olarak 5 yıllık süre için atanmakta olup, yardımcısıda aynı süreyle görev yapmaktadır. Tekrar seçilme imkanı bulunan kurum başkanı, yardımcı eleman çalıştırabilmektedir. Ayrıca

kurum başkanı ve çalışanlarının bağımsız olmalarına ilaveten konularında bilgili, tecrübeli, uzman olmalarının yanısıra sır saklamaları da zorunludur.

EDPS, veri güvenliği ve mahremiyet konusunda şikayetleri almakta ve gerekli incelemeleri yapmakta, kişisel verilerin korunması ve mahremiyetin gizliliği konusunda gerektiğinde topluluk kurumlarını bilgilendirmektedir. Ayrıca bilgi ve iletişim teknolojilerindeki gelişmeleri takip ederek toplumu bilgilendirme görevini de yürütmektedir.

3.3.2. Güvenlik kültürüne ilişkin politikası

Bilgi toplumu hizmetlerinin gelişmesiyle bilgi güvenliği, iş dünyasının vatandaşın ve kamu sektörünün yaptığı her işlemde vazgeçilmez bir unsur olmuştur. Bu nedenle, AB bünyesinde ortak tutum, fikir ve anlayış birliğinin kurulması ve iç pazarın sağlıklı çalışması amacıyla, AB içinde güvenlik kültürü oluşturulması hedeflenmiştir. Bu kapsamda, 92/242/EC sayılı Konsey Kararı ile 2002 yılı e-Avrupa Eylem Planı ve 2256/2003/EC ve 2003/48/EC Sayılı Konsey Kararları ile 2005 yılı e-Avrupa Eylem Planları oluşturulmuştur. Bu eylem planlarında;

- Elektronik ortamda depolanan, işlenen ve iletilen bilginin kazara veya kasıtlı tehditlere karşı uygun şekilde korunması,
- Konu ile ilgili uluslararası standartların kabul edilmesi,
- Konu ile ilgili üye devletlerde gerekli düzenlemelerin yapılmasının gerekliliği,
- Bilgi sistemlerinin güvenliği için kullanıcı ve servis sağlayıcılara düşen görevlerin tanımlanması,

- Her kesimden kullanıcının bilgilendirilmesi ve bilinçlendirilmesi için bilgi ve veri güvenliği ile mahremiyetin korunması eğitimlerine önem verilmesi,
- Özel sektör, Ar-Ge kuruluşları ve hükümetlerin işbirliği içinde olması,
- Bilgi güvenliği ile mahremiyet ihlallerini asgari seviyede tutmak için hukuki, teknik ve idari tedbirlerin alınması,
- Uluslararası işbirliğine önem verilmesi [37, 38]

gerektiği vurgulanmıştır.

3.3.2.1. Avrupa Şebeke ve Bilgi Güvenliği Kurumu

AB üyesi devletlerde yeterli seviyede yüksek dereceli güvenlik seviyesini elde etmek ve bu bağlamda bilgi güvenliği konusunda Avrupa koordinasyonunu kurmak ve geliştirmek amacıyla, 13.3.2004 tarih ve 460/2004/EC sayılı Tüzük ile merkezi başlangıçta Brüksel'de daha sonra Yunanistan'da [39] olmak üzere Avrupa Şebeke ve Bilgi Güvenliği Kurumu–ENISA (Europa Network and Information Security Agency)'nın kurulması hedeflenmiştir.

ENISA, iç pazarın sağlıklı ve güvenli bir ortamda çalışmasını sağlamak ve şebeke ve bilgi güvenliği konusunda temel güvenlik ihtiyaçlarını karşılamak üzere Komisyona ve üye devletlere gerekli her türlü katkıyı ve desteği sağlamakla görevlendirilmiştir. Kurum, gerektiğinde gelişen teknoloyi de göz önüne alarak Topluluğun şebeke ve bilgi güvenliği konusundaki mevzuatının güncelleştirilmesine katkı sağlamakta ve ilgili taslak mevzuatın hazırlanmasına yardımcı olmaktadır [40]. Ayrıca, Kurum aşağıda sayılan görevleri yerine getirmekle sorumlu bulunmaktadır:

- AB Komisyonuna ve ilgili diğer kurumlara (emniyet, güvenlik teşkilatı vs.) gerekli desteği sağlamak ve görüş vermek,
- Bilgi güvenliği ile ilgili tüm taraflar ve aktörler arasında işbirliğinin kurulması ve geliştirilmesine katkıda bulunmak,
- Şebeke ve bilgi güvenliği hususunda olabilecek riskler ve tehditler karşısında tüm kullanıcıları önceden bilgilendirmek,
- Topluluk mevzuatında verilerin korunması hususundaki direktifler ve tüzük doğrultusunda gerekenlerin yerine getirilmesini sağlamak,
- Risk değerlendirme faaliyetlerini değerlendirerek şebeke ve bilgi güvenliği konusundaki standartların değerlendirilmesine katkı sağlamak,
- AB dışındaki diğer ülkelerle şebeke ve bilgi güvenliği konusunda işbirliği kurmak ve geliştirmek.

3.4. Uluslararası Telekomünikasyon Birliği

3.4.1. Güvenlik kültürü ve kişisel verilerin korunmasına ilişkin politikası

ITU (Uluslararası Telekomünikasyon Birliği)'nun, bilgi güvenliğine yönelik çalışmaları Dünya Bilgi Toplumu Eylem Planı altında yürütülmektedir. ITU'nun bu konudaki çalışmaları yeni olmamakla birlikte, 10-12 Aralık 2003 tarihleri arasında Cenevre'de yapılan Dünya Bilgi Toplumu Zirvesi'nden sonra daha da yoğunluk kazanmıştır. Sağlıklı bir bilgi toplumu oluşturulması için kişisel verilerin korunması ile mahremiyetin sağlamasını bilgi güvenliğinin vazgeçilmez bir koşulu olarak gören ITU'nun, konu ile ilgili çalışmaları prensipler ve tavsiye kararları düzeyinde olup, bağlayıcı nitelik taşımamaktadır.

Bilgi güvenliği çalışmalarına son derece önem veren ITU, yapılan pek çok toplantıda bilgi güvenliği ve mahremiyetin sağlanması konularına değinmektedir. Bunlardan başlıcaları olan 23 Eylül-18 Ekim 2002 yılında Fas'ta Tam Yetkili Temsilciler Konferansı (Plenipotentiary Conference-PP), 10-12 Aralık 2003 tarihinde Cenevre'de Dünya Bilgi Toplumu Zirvesi (World Summit on the Information Society-WSIS) ve Ekim 2004'te Brezilya'da gerçekleştirilen Dünya Telekomünikasyon Standardizasyon Genel Kurulu (World Telecommunication Standardisation Assembly-WTSA)'dur. Bu toplantılarda bilgi güvenliği konuları değerlendirilerek çeşitli kararlar alınmıştır. Kişisel veri ve mahremiyet konularını bilgi güvenliğinin vazgeçilmez koşulu olarak değerlendiren ITU, güvenliği sağlama hususunda teknik, yasal ve kültürel çözümlerin herbirini sürecin bir parçası olarak görmektedir [42].

Radyokomünikasyon Sektörü (ITU-R), Telekomünikasyon Standardizasyon Sektörü (ITU-T) ve Telekomünikasyon Kalkınma Sektörü (ITU-D) olmak üzere 3 sektörden oluşan ITU'nun bilgi güvenliğini sağlamaya yönelik teknik çalışmaları ITU-T altında bulunan Çalışma Grubu 17 (SG-17) tarafından yürütülmektedir. ITU-D sektöründe ise daha ziyade kültür kavramını yaymak, yaygınlaştırmak ve işbirliği mekanizmalarını genişletmek amaçlı çalışmalar yürütülmektedir.

Küresel anlamda bilgi güvenliği kültürü oluşturmaya çalışan ITU, bu kapsamda;

- Bilgi ve şebeke bütünlüğünün korunması ve kullanıcı güveninin tesis edilmesi amacıyla tüm hükümetler ve taraflar arasındaki işbirliğinin kurulması ve buna işlerlik kazandırılmasını,

- Bilgi güvenliği ile mahremiyet alanlarında rehber ilkelerin hazırlanması, uygun mevzuatın yürürlüğe konması ve uygulanmasının sağlanmasını,
- Toplumun bilgi güvenliği ile mahremiyet konularında eğitilmesi ve bilinçlendirilmesini,
- İlgili tüm hükümetler ve taraflar arasındaki işbirliğinin sadece bireylerin eğitilmesinde değil, aynı zamanda mahremiyetin korunmasına yönelik olarak gerekli teknik ve idari tedbirlerin alınması hususunda da yürütülmesini,
- İlgili tüm taraflarca şebeke ve bilgi güvenliği alanındaki mevcut en iyi uygulama örneklerinin ve bu çerçevede elde edinilen tecrübelerin paylaşılmasını,
- Güvenliğe ilişkin olarak meydana gelen olaylarda bilginin ve teknolojik imkanların paylaşılması, bu alanda sıkı bir işbirliği politikasının oluşturulmasını,
- Çevrimiçi işlemleri kolaylaştırmak üzere güvenli ve güvenilir uygulamaların geliştirilmesinin desteklenmesi ve teşvik edilmesini,
- Bilgi ve iletişim teknolojilerinde güvenlik ve güvenilirlik kavramlarına işlerlik kazandırılabilmesi amacıyla diğer uluslararası kuruluşların çalışmalarına aktif bir şekilde iştirak edilmesi ve bu yönde tüm ülke ve tarafların teşvik edilmesini,
- Bilgi güvenliği ihallerinin asgari seviyeye indirilmesi için işbirliği mekanizmaları ve yasal mevzuat geliştirilmesini [44]

tavsiye etmektedir.

3.4.2. İstek dışı haberleşmeye ilişkin politikası

ITU'nun mahremiyetin korunması kapsamındaki çalışmaları istek dışı haberleşme konusuna yoğunlaştırmaktadır. İstek dışı haberleşmeyi önlemek için teknik, yasal önlemlerin yanı sıra uluslararası işbirliğinin önemini E. Liikanen'in *"İstek dışı haberleşme küresel bir problemdir ve küresel işbirliği gerektirir"* sözleri ile vurgulayarak, bu konuda mutlak bir uluslararası işbirliği yapılması gerektiğini vurgulamakta [45] ve çalışmalarına bu konuda ağırlık vermektedir. Bu kapsamda ITU üye ülkelere;

- Uygun yasal mevzuat hazırlamalarını ve etkin şekilde uygulamalarını,
- Self-regülasyon uygulamalarına ağırlık vermelerini,
- Kullanıcıların bilgilendirilmesi ve bilinçlendirilmesi için eğitim seminerleri düzenlemelerini,
- Teknolojik gelişmeleri takip etmelerini,
- Sözleşme ve pazarlama uygulamaları gibi özel durumlarda sınır ötesi işbirliği kurma ve geliştirmelerini,
- Filtreleme ve benzeri diğer güvenlik önlemleri kullanmalarını,
- İlgili kurumlar arasında sıkı işbirliği kurmalarını,
- Ülkeler arasında işbirliği mekanizmaları geliştirmelerini [44, 45]

tavsiye etmektedir.

Ayrıca ITU, OECD ve AB gibi diğer uluslararası ve bölgesel kuruluşlar ile işbirliği içinde bulunmakta ve bu kuruluşların çalışmalarına destek vermektedir.

Bu kapsamda ITU,

- Küresel bir mutabakatın kabul edilmesine vesile olacak olan uluslararası işbirliği için uygun bir yapının oluşturulması ve desteklenmesi,
- Diğer uluslararası kuruluşlarla işbirliğinin kurulması ve tüm dünyada istek dışı haberleşme ile ilgilenen kurumlarla işbirliğinin gerçekleştirilmesi,
- Mevcut ve uygulanmakta olan yasal düzenlemelerin bir araya toplanması [46]

çalışmalarını sürdürmektedir.

4. BİLGİ GÜVENLİĞİ KONUSUNDA ÜLKE İNCELEMELERİ

Bilgi güvenliği ve mahremiyetin sağlanması ile ilgili olarak AB, OECD, ve ITU gibi uluslararası kuruluşlara üye ülkelere bakıldığında hepsinin bilgi güvenliği ile mahremiyetin sağlanması hususunda düzenleme yaptıkları, bu görevlerin yürütülmesinden sorumlu kuruluşlara sahip oldukları görülmektedir. Ülke örnekleri seçilirken de bu kuruluşlara üye farklı coğrafyadan konuyla ilgili en iyi düzenleme yapmış olan ülkeler seçilmiştir.

4.1. Avustralya

4.1.1. Güvenlik kültürü sağlanmasına yönelik çalışmalar

OECD tarafından hazırlanan Güvenlik Kültürü Rehber İlkeleri, Avustralya'da büyük ilgi görmüş olup, ülkede güvenlik kültürü oluşturmak amacıyla kamu ve özel sektör sıkı bir işbirliği içine girmiş bulunmaktadır.

Bu kapsamda, Avustralya hükümeti şebeke ve bilgi güvenliğini sağlamak amacıyla kamu ve özel sektör temsilcilerinden oluşan Kritik Altyapı Koruma (Critical Infrastructure Protection-CIP) çalışma grubunu kurarak Nisan 2003'de Kritik Altyapı Koruması için Güvenli Bilgiyi Paylaşan Şebeke (Trusted Information Sharing Network for Critical Infrastructure Protection-TISN) eylem planını başlatmıştır. Bu eylem planının yürütülmesinden sorumlu olan Haberleşme, Bilgi Teknolojileri ve Sanayi Bakanlığı öncelikle konuyla ilgili politika oluşturmakta ve oluşturulan politikalar doğrultusunda güvenlik kültürü yaratmaya çalışmaktadır [47].

Bu amaçla, toplumun bilgilendirilmesine yönelik seminerler, konferanslar düzenlenmekte, internet siteleri kurulmakta ve basılı-görsel yayınlar

hazırlanmaktadır. Avustralya'da ulusal bilgi güvenliğini sağlamak ve istihbarat görevini yürütmek amacıyla kurulmuş olan DSD (Savunma Sinyalleri Müdürlüğü-Defence Signals Directorate)'de bu çalışmalara büyük destek vermektedir.

Avustralya hükümeti güvenlik kavramını daha geniş kitlelere yaymak amacıyla Mayıs 2003'te AusCERT (Avustralya Bilgisayar Acil Durum Müdahale Ekibi-Australian Computer Emergency Response Team)'i kurmuştur. Söz konusu kurum aşağıdaki görevleri yapmakla yetkili kılınmıştır:

- Bilgi ve iletişim teknolojilerinde bilgi güvenliği konusunda bilgilendirme yapmak,
- Güvenlik problemlerine ilişkin tesbit ve çözüm önerilerinde bulunmak,
- Güvenlik açıklarını tesbit ederek bunların nasıl kapatılabileceği hususunda önerilerde bulunmak,
- Güvenliğe ilişkin her türlü konuda ilgili kurum veya kuruluşlarla işbirliği yapmak,
- Gerektiğinde teknik danışmanlık yapmak ve bu çalışmaları koordine etmek,
- Güvenlik kültürü yaratmak amacıyla doküman, yayınlar ve çeşitli eğitim faaliyetleri düzenlemek [48].

Bilgi ve şebeke güvenliği konusunda uluslararası işbirliğinin de önemli olduğunun bilincinde olan Avustralya ABD, Kanada, Yeni Zelanda ve İngiltere başta olmak üzere diğer ülkelerle yakın işbirliği içinde bulunmaktadır [47].

4.1.2. Kişisel verilerin korunmasına yönelik çalışmalar

Avustralya'da 1988 tarihinde yürürlüğe giren "Mahremiyet Kanunu" (Privacy Act), kamu ve özel sektörde kişisel verilerin korunmasına yönelik gerekli hususları içeren temel bir yasa niteliğini taşımaktadır. Bu kanunda, OECD tarafından hazırlanan Mahremiyet Rehber İlkeleri'nde yer alan ilkeler esas alınmıştır. Ayrıca sözkonusu kanunla, kişisel verilerin korunmasından sorumlu Federal Mahremiyet Görevli Bürosu (Office of the Federal Privacy Commissioner) kurulmuştur.

Avustralya'da hassas veri olarak da nitelendirilen verileri korumak amacıyla çeşitli meslek gruplarının ilke ve kurallarını içeren düzenlemeler bulunmaktadır. Bunlar:

1) Kişilerin işledikleri suçlardan dolayı hüküm giydikleri bazı suçların mahkumiyetin bitiminden itibaren yetkisiz olarak ifşa edilmesini önleyen 1914 tarihli "Suç Kanunu",
2) Telekomünikasyon işletmecileri tarafından haberleşmenin gizliliğini sağlayan ve kişisel verilerin ifşa edilmesini önleyen 1997 tarihli "Telekomünikasyon Kanunu",
3) Sosyal yardım ve vergiye ilişkin kişisel verilerin korunmasına yönelik olarak bazı hükümler içeren 1990 tarihli "Yardım ve Vergi Kanunu" şeklinde sıralanmaktadır [47].

4.1.3. İstek dışı haberleşmeye yönelik çalışmalar

Avustralya'da istenmeyen e-posta uygulamalarında kapsam içi yöntem tercih edilmiş olup, sözkonusu yöntemi düzenleyen "Spam Kanunu" 2 Aralık 2003 tarihinde onaylanmıştır. Kanunda elektronik mesaj kavramı, mobil telefonlarla

gönderilen görüntü ya da metin mesajları ve e-postalar şeklinde ele alınmıştır. Sözkonusu kanun gereğince mesaj gönderenin doğru ve gerçek bir adresinin gönderilen mesaja ekli olması ve tekrar gönderilmemesine imkan sağlayan bir yöntemin bulunması zorunlu kılınmıştır [17].

Kanunda istek dışı haberleşmeye ilişkin hükümleri ihlal eden gerçek kişilere 44.000 Avustralya doları, kuruluşlara ise 220.000 Avustralya doları ceza öngörülmüştür [46].

Kanunun uygulamasından sorumlu olan ACA (Avustralya Telekomünikasyon Otoritesi-Australian Communications Authority), kanun gereğince ihlale ilişkin soruşturma ve incelemeleri yapmakla yetkili ve görevli kılınmıştır. Bu kapsamda ACA, oluşturduğu şikayet merkezi ve internet sayfası ile istek dışı haberleşme alan kişilerin sorunlarına çözüm bulmaya çalışmaktadır.

Bunun yanı sıra ACA, istek dışı haberleşmeyi önleme konusunda ACCC (Avustralya Rekabet ve Tüketici Komisyonu-Australian Competition and Consumer Commission), AGIMO (Avustralya Devlet Bilgi Yönetim Ofisi - Australian Goverment Information Management Office), Ulusal Bilgi Ekonomisi Ofisi (National Office for the Information Economy), DMA (Avrupa Doğrudan Pazarlama Birliği-Australian Direct Marketing Association) ile yakın işbirliği içinde bulunmaktadır.

İstek dışı haberleşmeyi önleme konusunda uluslararası işbirliğinin önemli olması nedeniyle ACA diğer ülkelerle ikili işbirliğine girerek istek dışı haberleşmeye karşı mücadele etmektedir. Bu konuda ACA ABD, İngiltere ve Kore ile Mutabakat Zaptı (MoU) [17] imzalamıştır.

4.2. Amerika Birleşik Devletleri

4.2.1. Güvenlik kültürü sağlanmasına yönelik çalışmalar

ABD, bilgi güvenliğine yönelik düzenlemeler bakımından sistemini en çok oturtmuş ülkedir. Ülkenin ulusal bilgi güvenliğini sağlamak amacıyla 1952 yılında kurulmuş olan NSA (Ulusal Güvenlik Teşkilatı-National Security Agency), ABD çıkarları doğrultusunda uluslararası elektronik istihbarat ve devletin bilgi güvenliğini sağlamaktan sorumludur [49]. NSA, uzman teknik fonksiyonları sağlamaktan sorumlu kılınan Savunma Bakanı'nın yetki, kontrol ve yönlendirmesinde olup, Savunma Bakanlığı bünyesinde bağımsız bir teşkilat olarak çalışmalarını yürütmektedir.

Bunun yanısıra ABD, internet yoluyla işlenen suçlarla mücadelede önemli mesafeler kaydetmiş, internet üzerindeki hak ve yükümlülükleri kanunlarla düzenlemiş bulunmaktadır. Ancak, 11 Eylül terör saldırılarında iletişim aracı olarak internetteki porno içerikli sitelerin kullanılması üzerine, internet haberleşmesinde sansür ve izleme yöntemine gidilmiş ve bilgi ve iletişim ağlarının korunmasına daha fazla önem verilmeye başlanmıştır.

Bununla birlikte saldırı olayları, alınan veya alınacak her türlü önlemin yeterli olmayacağını bunun bir kültür kavramına dönüşmesinin gerekliliğini ortaya çıkarmasıyla bu konuda da çalışmalar yoğunlaşmıştır.

ABD'de güvenlik kültürü oluşturma çalışmaları başlıca FTC (Federal Ticaret Komisyonu-Federal Trade Commission) tarafından yürütülmektedir. FTC bu konuda

- Olası saldırı ve tehditler karşısında bilgilendirme,
- Saldırılara karşı korunma yöntemleri,
- İnternet üzerinde kişisel verilerin korunma yöntemleri,

- İstek dışı haberleşme v.s.

gibi konularda kişileri bilgilendirme ve bilinçlendirme amacıyla pek çok çalışma yürütmektedir.

Ülkede bilişim teknolojileri alanında kurulmuş bulunan sivil toplum örgütleri, kamu ve özel sektör kuruluşları ve üniversiteler yakın işbirliği içinde bulunarak konuyla ilgili olarak çok sayıda atölye çalışması, konferans ve seminerler düzenleyerek, basılı ve görsel yayınlar dağıtmaktadırlar. Ayrıca FTC 24 saat süreyle kişilerin şikayetlerini anlatabilecekleri ve çözüm yolu bulabilecekleri şikayet ve bilgilendirme merkezleri ve telefon hatları tahsis etmiştir [21].

Bunun yanı sıra güvenlik risk ve tehditlerinin genellikle İnternet üzerinden olması nedeniyle İnternet güvenliği konusunda da kişileri bilgilendirme amaçlı ABD'de çok sayıda organizasyon, kuruluş ve sivil toplum örgütleri bulunmaktadır. Ancak bunların en önemlisini 1988 yılında kurulan CERT (Bilgisayar Acil Durum Müdahale Ekibi-Computer Emergency Response Team) oluşturmaktadır. CERT, dünya genelinde yaygın merkezleri ile sürekli İnternet, sistem ve platformlarda güvenlik açıklarını ortaya çıkarmak, raporlar halinde dünyaya açıklamak, çözüm yolları önermek gibi bir misyonu yerine getirmektedir.

Ayrıca ABD'de kamu sektöründe çalışan kesimin bilgi teknolojilerinde güvenlik konusunda eğitilmelerini sağlamak amacıyla ülke çapında çeşitli eğitim programlarının düzenlendiği görülmektedir .

Bilgi güvenliği hususunda uluslararası işbirliğinin gerekli olduğuna inanan ABD, Avustralya ve AB üyesi ülkelerle ikili anlaşmalar yaparak ve temas

noktaları belirleyerek muhtemel risk ve tehditler konusunda önceden uyarma, bilgilendirme, işbirliği ve bilgi alış verişinin yapılmasına çalışmaktadır.

Bilgi güvenliği konusunda, ABD telekomünikasyon otoritesi FCC, bilgi ve iletişim teknolojilerindeki veri aktarımının telekomünikasyon altyapısı sayesinde gerçekleştirilmesi nedeniyle, altyapı güçlendirme çalışmalarına ilişkin düzenlemeleri yapmaktadır [51].

4.2.2. Kişisel verilerin korunmasına yönelik çalışmalar

ABD'de genel olarak kişisel verilerin korunmasına ilişkin bir mevzuat bulunmamakta, kişilerin mahremiyet hakları self-regülasyon ve sektör spesifik düzenlemelerle korunmaya çalışılmaktadır. Bunlardan bazıları:

- Mali Mahremiyet Kanunu (1978),
- Adil Kredi Raporlama Kanunu (1970),
- Telekomünikasyon Kanunu (1996),
- Görüntü Mahremiyeti Koruma Kanunu (1998),
- Aile Eğitim Hakları ve Mahremiyet Kanunu (1974) [47].

Bunun yanı sıra ABD'nin federal bir yapıya sahip olması nedeniyle bir çok eyalet anayasasında ve kanunlarında mahremiyetin korunmasına yönelik düzenlemeler bulunmaktadır.

ABD'de FCC telekomünikasyon alanında, FTC ise ticari alanda mahremiyeti sağlamakla sorumlu olup, bu yönde düzenlemeler yapmaktadırlar. Ülkedeki konuyla ilgili genel eğilimin self-regülasyon olması nedeniyle ilgili kuruluşlar uyulması gereken genel hat ve politikaları belirlemekte, bu çerçevede kurum ve kuruluşlar ise kendi mahremiyet politikalarını belirleyip uygulamaktadırlar.

Telekomünikasyon alanındaki mahremiyetin korunmasından sorumlu bulunan FCC, bu alanda kişisel verilerin ve tüm işletmecilerin kişilerin konum bilgisi, acil çağrı, arayan numaranın kimliği gibi mahremiyetin korunması ile ilgili uyulması gereken kuralları belirlemekte ve uygulanıp uygulanmadığını kontrol etmektedir.

FTC ise ticari ilişkilerde haksız ve hileli işlemlerin yapılmasının önlenmesini sağlarken diğer ilgili kurumlar sağlık, ulaştırma ve mali hizmetler gibi çeşitli sektörlerde mahremiyete ilişkin kurallara riayet edilmesini sağlamaktadırlar.

4.2.3. İstek dışı haberleşmeye yönelik çalışmalar

ABD'de istek dışı haberleşmenin önlenmesi konusunda federal yasa olan "Can Spam Act"tan önce çeşitli eyaletlerde e-posta yoluyla reklam yapılması kanunlarla yasaklanmıştır. Bu kanunlardan 1999 yılında Kaliforniya'da yürürlüğe giren kanun, istek dışı haberleşmeyi önleme konusunda örnek teşkil etmekteydi .

Sözkonusu kanunda, İSS'lerin aboneleri ile yaptıkları sözleşmelere e-posta yoluyla istenmeyen reklamlar gönderemeyecekleri, aksi takdirde zararı gidermek zorunda kalacakları konusunda hüküm koymaları gerekmekte olup, bu hükmü ihlal edenlerin e-posta başına 50 veya 25 bin dolar ceza öngörülmüştür [50]. Kanunda, çocuklar için sakıncalı e-postaların gönderilmesi, gönderici adresinin yanlış yazılması ve aldatıcı konu başlıklarının kullanılması da yasaklanmıştır.

Ancak ABD'de istek dışı haberleşmenin oldukça rahatsız edici boyuta ulaşması ile federal bir yasa düzenleme gereği hissedilmiş ve 16 Aralık 2003'de istek dışı haberleşmeyi önleme konusunda kapsam dışı (opt-out)

yöntemini benimseyen "İstenmeyen Pornografik ve Pazarlamanın Denetlenmesi Kanunu-The Controlling the Assault of Non-Solicited Pornography and Marketing Act" kabul edilmiştir. "Can Spam Act" olarak ta bilinen kanun 1 Ocak 2004 tarihinde yürürlüğe girmiştir. Kanun gereğince

- Aldatıcı ve yanlış başlık içeren mesajların gönderilmesi,
- Gönderici adresinin yanlış yazılması,
- Pornografik içerikli mesajların gönderilmesi,
- Sahte e-posta adreslerinin üretilmesi ve geçersiz e-posta adreslerinin kullanılması yasaklanmış olup,
- Göndericinin mesajı bir daha almak istememesi durumunda, mesajın tekrar gönderilmemesine imkan tanıyan bir yöntemin alıcıya sunulmuş olması zorunlu kılınmıştır [52].

Ayrıca mesaj ticari reklam içerikli ise mesajın ticari içerikli olduğunu açıkça belirten ifade de içermelidir. Aksi kanunla suç olarak kabul edilmekte ve e-posta başına 250 – 2 milyon ABD doları kadar para cezası ya da hapis cezası verilebileceğine ilişkin hükümler bulunmaktadır [45].

Bunun yanı sıra kanun gereğince e-posta adreslerinin çeşitli vasıtalarla toplanması da suç olarak kabul edilmektedir. İnternet hizmeti sağlayan İSS'lerin müşterileri ile yaptıkları sözleşmelerde e-posta ile istek dışı haberleşme gönderemeyecekleri, aksi takdirde zararı gidermek zorunda kalacakları konusunda hüküm yer almaktadır.

ABD'de istek dışı haberleşme ile ilgili düzenlemelerden FCC, uygulamalardan ise FTC sorumlu bulunmaktadır. Bu kapsamda, FTC istek dışı haberleşmeden rahatsız olan kişilerin kendilerine gelen istek dışı haberleşmeyi iletebilecekleri şikayet merkezleri kurmuştur [53]. Ayrıca İSS'ler istek dışı haberleşmeyi

önlemek amacıyla filtreleme yöntemleri geliştirmişler ve aboneleri ile yaptıkları sözleşmelere abonenin istek dışı haberleşme yapmamalarını, aksi takdirde cezalandırılacakları hükmünü koymuşlardır.

Kanun kapsamında, Mayıs 2004'te cinsel içerikli bir malzemenin tanıtımı amacıyla 825 milyon adet istenmeyen e-postayı gönderen Earthlink firması aleyhine bir şahıs tarafından açılan dava sonucu ilgili firma sahipleri 7 yıl hapis ve 16.4 milyon ABD doları para cezasına çarptırılmıştır [19].

Yine aynı şekilde, Ekim 2003'te Californiya'da e-postaların toplanması amacıyla bazı araç ve yazılımların kullanıldığı iddiasıyla PW adlı bir pazarlama firması aleyhine açılan dava sonucunda firmaya 2 milyon ABD doları para cezası verilmiş ve ayrıca firma sahipleri 10 yıl süreyle internete ilişkin faaliyetlerde bulunmaktan men edilmiştir [19].

ABD'de DMA (Direct Marketing Association-Doğrudan Pazarlama Birliği) örnek bir self-regülasyon uygulaması yaparak e-MPS (e-Mail Preference Service) sistemi kurmuştur. İstek dışı haberleşme almak istemeyen kişiler e-MPS'ye başvurarak istek dışı posta almak istemediklerini beyan etmektedirler. Ticari nitelikli mesaj göndermek isteyenler bu liste dışındaki kişilere mesaj gönderebilmektedirler. Ancak, bu uygulamada mesaj gönderenin açık adresi, aldatıcı olmayan konu başlığı ve mesajın tekrar alınmak istemediğini kolaylaştırıcı yöntemlerin bulunması gerekmektedir [46].

Diğer taraftan, istek dışı haberleşmenin ulusal sınırları aşması nedeniyle bu konuda uluslararası ilişkilere önem veren ABD, İngiltere ve Avustralya ile Mutabakat Zaptı imzalamıştır.

4.3. Almanya

4.3.1. Güvenlik kültürü sağlanmasına yönelik çalışmalar

Almanya'da bilgi güvenliğinin sağlanmasına yönelik olarak BSI (Bundesamt für Sicherheit in der Informationstechnik-Enformasyon Teknolojileri Güvenlik Kurumu) bulunmaktadır.

BSI, istihbarat işlevi olmayan bilgi ve bilgisayar sistemleri güvenliği konularında araştırma yürüten bir kurumdur. Araştırma sonuçları, kamuda söz konusu güvenlik uygulamalarının yapılmasına yarar sağlamaya çalışmaktadır. Kurum adli olaylarda da emniyete talep olduğu takdirde danışmanlık hizmeti de verebilmektedir [49].

BSI, Almanya'da kişilerin bilgi güvenliği konusunda bilinçlendirilmesi amacıyla, çeşitli çalışmalar yürütmektedir. Bu çalışmaların başında konferanslar, seminerler gelmektedir. Bunun yanı sıra eğitici çeşitli broşürler ya da yayınlar, CD'ler hazırlanıp halka dağıtılmaktadır [47].

4.3.2. Kişisel verilerin korunmasına yönelik çalışmalar

Almanya'da kişisel verilerin korunması konusunda çalışmalar 70'li yıllarda başlamıştır. Bu kapsamda, 1990 tarihinde yürülüğe konan Federal Veri Koruma Kanunu (Federal Data Protection Act-Bundesdatenschutzgesetz-BDSG) ile gerçek kişilere ait verilerin korunması amaçlanmıştır. Sözkonusu kanun, kamu ve özel sektördeki kişisel verilerin korunmasına ilişkin hükümleri içermekte olup, bilgisayar veya elle işlenen kişisel verilerin kaydedilmesi ve korunmasına ilişkin hususları düzenlemektedir. Sözkonusu

kanun, 2001 yılında 95/46/EC sayılı Direktifi ulusal mevzuata aktarmak amacıyla yeniden güncellenmiştir [47].

Ayrıca, sözkonusu kanun kapsamında, kişisel veriler ile ilgili işlemlerin uygulamasından sorumlu olmak üzere bağımsız bir yapı da öngörülmüştür. Bu doğrultuda kurulan Federal Veri Koruma Görevlisi (Federal Data Protection Commisisoner), kamuda kişisel veri ve dosyaların işlenmesi işlemini yürütmektedir. Özel sektördeki bağımsız veri koruma görevlisi ise, Almanya'daki her bir eyaletin kendi özel kanunları çerçevesinde oluşturulmaktadır [55].

Bu kapsamda, kişisel verilerinin ihlal edildiğini düşünen kişiler Federal Veri Koruma Görevlisi'ne şikayet dilekçesi verme hakkına sahip bulunmakta ve Federal Veri Koruma Görevlisi ilgili mevzuata uygun olarak şikayetleri bir sonuca bağlamaktadır. Özel sektör kuruluşlarına karşı yapılan şikayetler ise, özel sektördeki ilgili bağımsız veri koruma görevlileri tarafından sonuçlandırılmaktadır [47].

4.3.2.1. Telekomünikasyon alanında kişisel verilerin korunmasına yönelik çalışmalar

Almanya'da 97/66/EC sayılı Direktif, Telekomünikasyon Hizmetlerinde Veri Koruma Kanunu (Teledienstedatenschutzgesetz-TDDSG), 1997 tarihli Telekomünikasyon Kanunu (Telekommunikationsgesetz, TKG) ve Telekomünikasyon Taşıyıcıları Veri Koruma Yönetmeliği (Telekommunikationsdienstunternehmen-Datenschutzverordnung, TDSG) ile uyumlaştırılmıştır [34].

TDDSG, telekomünikasyon alanında kişisel verilerin depolanması, işlenmesi veya kullanılması ile ilgili hükümleri düzenlemektedir.

TKG ise TDDSG'ye nazaran daha genel kurallar içermektedir. Kanunun temel amacı, rekabetin teşvik edilmesi ve arttırılması, ülke içinde tüm hizmetlerin yeterli ve uygun şekilde sunulmasının sağlanması, frekans düzenlemesinin yapılması ve kişisel verilerin korunmasının sağlanmasıdır.

Sözkonusu kanun gereğince, haberleşme gizliliğinin sağlanması zorunlu olup, telekomünikasyon işletmecileri kullandıkları tüm sistem, cihaz ve şebekenin olduğu kadar sundukları hizmetin de güvenliğini sağlamakla ve gerekli tedbirleri almakla yükümlü bulunmaktadırlar. Bu çerçevede RegTP, telekomünikasyon işletmecilerinin şebeke ve hizmet güvenliği açısından uygulamalarını denetlemektedir [58].

Kanun, abonenin rızasının bulunması şartıyla kişisel verilerin pazar araştırması, reklam ya da müşteriye danışma amacıyla işlenip kullanılabilmesine imkan tanımaktadır.

TDSG Yönetmeliği ise Yabancıların Merkezi Kayıt Kanunu ve Federal Telekomünikasyon Kanunu çerçevesinde bu kanunların ilgili olduğu spesifik alanlarda kişisel verilerin ve mahremiyetin korunması konusundaki hükümleri düzenlemektedir.

Düzenleyici Kurum olan RegTP, TKG Kanunu ve TDSG Yönetmeliği ile, kişisel verilerin işlenmesi ve mahremiyetin korunmasına yönelik olarak bulunan hükümlerin yerine getirilip getirilmediğini denetlemek ve kontrol etmekle yükümlüdür. Ayrıca, RegTP, sözkonusu mevzuatın uygulanmasına ve

denetlenmesine yönelik olarak gerektiğinde şartlara uygun olarak hukuki, teknik ve idari tedbirleri almakla da yetkilendirilmiştir.

Federal Veri Koruma Görevlisi ve RegTP arasında yakın bir işbirliği mevcut olup telekomünikasyon sektöründe kişisel verilerin işlenmesi ve mahremiyetin korunması konusunda mevcut durumu ve muhtemel gelişmeleri değerlendirmektedir.

4.3.3. İstek dışı haberleşmeye yönelik çalışmalar

Almanya'da e-posta yolu ile reklamı açıkça yasaklayan bir kanun bulunmamaktadır. Fakat Alman hukukunda mevcut kanunlarla istek dışı haberleşme sorununa çözüm arandığı görülmekte olup, sözkonusu durum UWG (Gesetz gegen unlauteren Wettbewerb-Haksız Rekabet Kanunu) ile çözüme kavuşturulmaya çalışılmaktadır [50].

Kanunun temel amacı, AB'nin 2002/58/EC sayılı Direktifini [33] uyumlaştırmak olup, bu çerçevede gerçek ya da tüzel kişilere rızaları olmadan ticari amaçlı olarak e-posta, faks ya da otomatik arama cihazı vasıtasıyla istenmeyen reklam ya da ilan vs. göndermeleri yasaklanarak kapsam içi yöntem benimsenmiştir.

Bu kapsamda hazırlanan Telekomünikasyon Müşterilerini Koruma Yönetmeliği-TKV gereğince, RegTP tüm kullanıcılardan istenmeyen arama, faks ve e-postalar konusunda gelen şikayetleri değerlendirmek üzere bir hakemlik müessesesi kurmuştur. Bu konuda RegTP tarafından yayınlanan 30 Haziran 2001 tarihli yıllık faaliyet raporunda, 284 farklı şikayetin hakemlik prosedürü kullanılarak çözüme kavuşturulduğu ifade edilmiştir [59].

4.4. İngiltere

4.4.1. Güvenlik kültürü sağlanmasına yönelik çalışmalar

İngiltere'de bilgi güvenliğini sağlamak amacıyla GCH (Kamu Haberleşmesi Merkezi-Government Communications Headquarters) kurulmuştur. GCH, bilgi ve bilgisayar sistemleri güvenliği konularında araştırma yürüten bir kurum olmanın yanısıra istihbarat işlevi yürüten bir kuruluştur [49].

GCH, ülkedeki diğer aktörlerle birlikte, İngiltere bilgi güvenliğini bir kültür haline getirmek için diğer ülkelerde olduğu gibi konu ile ilgili eğitici seminer ve konferansların yanı sıra, basılı ve görsel yayınlar oluşturmaktadır.

4.4.2. Kişisel verilerin korunmasına yönelik çalışmalar

1984 tarihli DPA (Veri Koruma Kanunu -Data Protection Act), hem kamu ve hem de özel sektörde otomatik olarak işlenen kişisel verilere yönelik olarak hazırlanmıştır. Söz konusu kanunla, kişiler kendileri hakkında veri toplandığında bunu öğrenme, düzeltme yapma, bilgilerin toplanma yöntemine itiraz etme ve kendilerine ait bilgilerin kötüye kullanılması durumunda uğradıkları zararın tazmini için dava açma hakkına sahiptir [32].

Kanun ile 95/46/EC sayılı Direktif [28] ulusal mevzuata aktarılmak amacıyla 1998 yılında güncellenmiş, ayrıca verilerin işlenmesi ve korunmasından sorumlu olarak kurulan Veri Koruma Görevlisi (Data Protection Commissioner), Bilgi Görevlisi (Information Commissioner-ICO) olarak değiştirilmiştir. ICO, hem genel anlamda ve hem de telekomünikasyon alanında kişisel verilerin güvenliğinin sağlanması ve korunması hususundaki ilgili mevzuatın uygulanmasından sorumlu bulunmaktadır [61].

Ayrıca, çeşitli meslek kuruluşları ve ticari firmalar da kişisel verilerin işlenmesi ve korunmasına yönelik olarak uymak zorunda oldukları kuralları içeren çeşitli düzenlemeler ortaya koymuşlardır. Bunlardan bazıları:

- 1986 tarihli Mali Hizmetler Kanunu,
- 1990 tarihli İnsan Kısırlaştırması ve Embriyoloji Kanunu,
- 1993 tarihli Sosyal Yardımlar Kanunu,
- 1993 tarihli Adli Suçlar ve Kamu Düzeni Kanunu [47]

gibi bazı kanunlarda da kişisel verilerin işlenmesi ve korunmasına yönelik hükümler bulunmaktadır.

4.4.2.1. Telekomünikasyon alanında kişisel verilerin korunmasına yönelik çalışmalar

İngiltere'de telekomünikasyon alanında kişisel verilerin korunması hususundaki düzenlemeler yani 97/66/EC sayılı Direktif [35], 1998 yılında "Veri Koruma ve Mahremiyet" ve "Doğrudan Pazarlama" konusundaki düzenlemelerle bir kaç aşamada uyumlaştırılmıştır [61]

Yürürlükte bulunan mevzuat gereğince, telekomünikasyon hizmet ve şebeke sağlayıcısı, sunulan hizmetin ve şebekenin güvenliğini sağlanmakla sorumlu olup, teknolojik gelişmeleri de dikkate alarak şebeke ve hizmetin güvenliğine karşı her türlü tedbiri almakla yükümlüdür [62].

Bu konuda düzenleyici otorite olan OFCOM, özellikle telekomünikasyon sektöründe kişisel verilerin işlenmesi ve mahremiyetin korunması konusunda çalışmalar yürütmektedir [59].

4.4.3. İstek dışı haberleşmeye yönelik çalışmalar

İngiltere'de istek dışı haberleşmeler konusunda, genel olarak kapsam içi yöntem kabul görmüştür. Bu kapsamda, Sanayi ve Ticaret Bakanlığı bünyesinde kurulmuş olan DTI (Sanayi ve Ticaret Bakanlığı-Department of Trade and Industry) "Anti-Spam Kanunu" hazırlamıştır. Eylül 2003'de onaylanan ve 11 Aralık 2003'de yürürlüğe giren sözkonusu kanun gereğince, mesaj ya da arama göndermeden önce firmaların e-posta alıcılarından açık bir onay almaları zorunlu olup, istenmeyen mesaj gönderilmesi durumunda kişiler firmaları şikayet edebilme hakkına sahip bulunmaktadır [63].

Benzer şekilde, internet sitelerinin, bu siteleri ziyaret eden kişilere eğer sitede cookie denilen özel yazılımlar var ise kullanıcıları bilgilendirmesi ve kullanıcılara cookileri reddetme hakkının ve imkanının sunulmasını da hükme bağlamıştır.

Bu kapsamda OFCOM, bünyesinde Doğrudan Pazarlama Birliği (Direct Marketing Association-DMA) ile telefon tercih servisi (Telefone Preference Service-TPS) ve faks tercih servisi (Fax Preference Service-FPS) kurmuştur. Kurulan bu servislerde, kayıtlı abonelerden gelen şikayetlerin kaydedilmesi ve değerlendirilmesi işlemi yapılmaktadır. Ayrıca, bu servisler abonelerden gelen şikayetlere ilişkin olarak şikayet sahibinden delil, bulgu ve belge talep etmektedir. Edinilen bilgiler yıllık olarak kişisel verilerin korunmasından sorumlu bulunan Bilgi Görevlisi'ne raporlar şeklinde sunulmaktadır.

İstek dışı haberleşme konusunda uluslararası işbirliğinin önemli olması nedeniyle DTI ve ICO, ABD'de de FTC ve Avustralya'da ACA ve ACCC ile istek dışı haberleşmeyi önleme konusunda mutabakat zaptı imzalamışlardır [65].

4.5. Fransa

4.5.1. Kişisel verilerin korunmasına yönelik çalışmalar

Kişisel verilerin korunması amacıyla 1978 tarihinde hazırlanan "Verilerin İşlenmesi, Veri Dosyaları ve Kişisel Özgürlükler Kanunu"nda, kamu ve özel sektördeki gerçek kişilere ilişkin bilgilerin ve mahremiyetin korunmasına ilişkin usul ve esaslar yer almaktadır. Ayrıca, kanun gereğince bağımsız Veri Koruma Kurumu tarafından idare edilen bir kayıt ve onay sistemi tesis edilmiştir. Veri Koruma Kurumu'nun temel görevleri arasında ilgili mevzuat çerçevesinde,

- Bireylerin ve toplumun kişisel verilerin ve mahremiyetin korunması konusundaki hak ve yükümlülüklere ilişkin olarak bilgilendirilmesi ve bilinçlendirilmesi,
- Gerektiğinde sosyal, toplumsal ya da teknolojik gelişme ve değişimlere göre mevzuatta değişiklik önerisinde bulunması

sayılabilmektedir [67].

Bu çerçevede, 95/46/EC sayılı direktif ulusal mevzuata kısmen de olsa aktarılmış ve Medeni Haklar ve Enformasyon Teknolojisi Ulusal Komisyonu (National Commisison on Information Technology and Civil Liberties-CNIL) ülkedeki kişisel verilerin işlenmesi ve korunmasından sorumlu olarak kurulmuştur. Direktifi, ulusal mevzuata aktarmak amacıyla 15 Temmuz 2004 tarihinde yeni bir yasa yürürlüğe konulmuştur [64].

Fransa'da ayrıca "İş Kanunu" ve "Video Teftiş Kanunu"nu çerçevesinde bu kanunların ilgili olduğu spesifik alanlarda kişisel verilerin ve mahremiyetin

korunması konusundaki hak ve yükümlülükler düzenlenmiştir [47].

4.5.1.1. Telekomünikasyon alanında kişisel verilerin korunmasına yönelik çalışmalar

Telekomünikasyon alanında kişisel verilerin korunmasına yönelik olarak 97/66/EC sayılı Direktif [35], "Telekomünikasyon Kanunu" ile uyumlaştırılmıştır. Mevzuat uyumu çerçevesinde Temmuz 2001'de kabul edilen düzenleme ile uyumlaştırma büyük ölçüde tamamlanmıştır [58].

Telekomünikasyon alanında düzenleyici otorite olan ART, telekomünikasyon alanında kişisel verilerin korunmasına yönelik düzenlemeleri sağlamakla sorumlu bulunmaktadır. ART, direktifi uyumlaştırmak amacıyla 2002 yılında telekomünikasyon alanında kişisel verilerin korunması ve mahremiyetin sağlanması amacıyla yönetmelik ve tebliğ yayınlamıştır.

4.5.2. İstek dışı haberleşmeye yönelik çalışmalar

Fransa'da istek dışı haberleşme hükümetin öncelikli konuları arasında yer almakta olup, konu ile ilgili çalışmaları CNIL yürütmektedir. CNIL, istek dışı haberleşmeyi önlemek amacıyla Ocak 2003'te "Sayısal Ekonomiye Güven" isimli kanunu çıkarmıştır. Sözkonusu kanun gereğince kişileri hedef alan e-posta için kapsam içi yaklaşım kabul edilmiştir [66].

Kanun, ticari amaçlı olarak e-posta gönderen tarafın, bu mesajların bir daha gönderilmemesine imkan tanıyan yöntemleri ücretsiz ve kolay bir yöntemle alıcıya sağlamasını hükme bağlamıştır. Ayrıca, mesaj gönderen tarafın açık ve doğru kimliğinin mesaja ekli olması ve mesajın başlığında yanlış bilginin olmaması zorunlu bulunmaktadır.

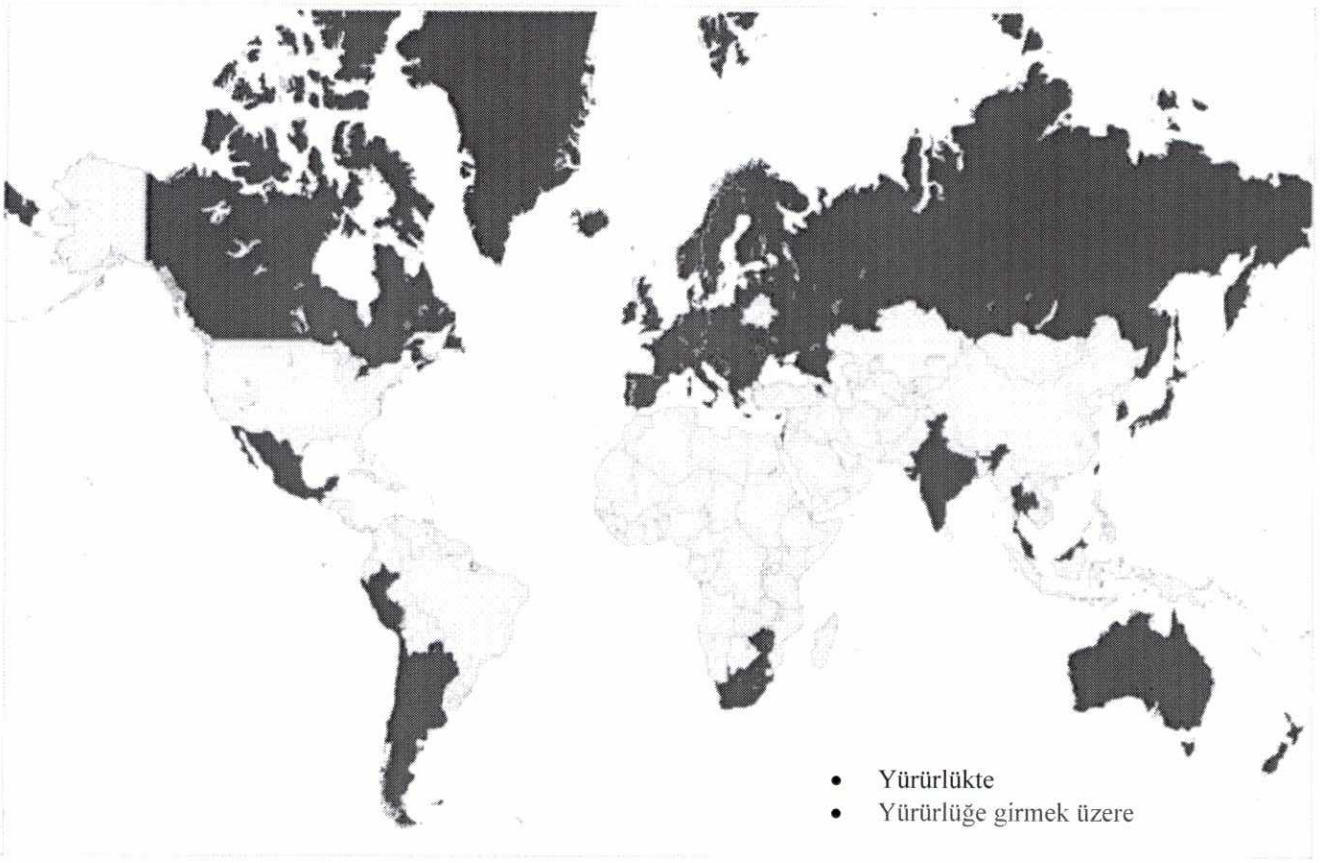
Kanun kapsamında, 5 Mayıs 2004 tarihinde bir milyon adet istenmeyen e-postanın gönderilmesi iddiasıyla Microsoft şirketi ile AOL France firmaları aleyhine açılan davada sözkonusu firmalar 22.000 Euro cezaya çarptırılmıştır [19].

Benzer şekilde 7 Kasım 2003 tarihinde Co. Smith & Nephew firması ile eski çalışanı arasında açılan dava sonucu, eski çalışan personelin firmanın bilgi sistemini e-posta bombardımanına tutarak çalışamaz duruma getirmesi, 34.413 Euro para cezası ile sona ermiştir [19].

CNIL, kişilerin istek dışı haberleşmeye karşı bilinçlendirilmesini sağlamak ve küçükleri İnternette zararlı içeriklerden korumak amacıyla İnternet sayfası hazırlamıştır. Ayrıca istek dışı haberleşme konusunda kişilerin şikayetlerini almak üzere bir şikayet birimi kurmuştur.

Bu konuda uluslararası işbirliğinin önemli olması nedeniyle ABD ile işbirliği yoluna gidilmiştir.

KİŞİSEL VERİLERİ KORUMA KANUNUNUN DÜNYADAKİ DURUMU (2003)



Kaynak:[71]

Çizelge 4.1 Bilgi Güvenliğinin Sağlanmasına İlişkin Uluslararası Anlaşmalar

Ülke	Avrupa Konseyi Siber Suç Sözleşmesi	Kişisel Verilerin İşlenmesi ve Bu Bilgilerin Serbestçe Dolaşımı Hususunda Bireylerin Korunması Hakkında AB Direktifi	Avrupa Konseyinin Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkındaki Sözleşmesi	Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına ilişkin OECD Rehber İlkesi	İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Konseyi Sözleşmesi	Mahremiyet Yasası
Avustralya				X		X
Avusturya	X	X	X	X	X	X
Belçika	X	X	X	X	X	X
Kanada				X	X	X
Çek Cumhuriyeti	X	X	X	X	X	X
Danimarka	X	X	X	X	X	X
Finlandiya	X	X	X	X	X	X
Fransa	X	X	X	X	X	X
Almanya	X	X	X	X	X	X
Yunanistan	X	X	X	X	X	X
Macaristan	X	X	X	X	X	X
İzlanda	X	X	X	X	X	X
İrlanda	X	X	X	X	X	X
İtalya	X	X	X	X	X	X
Japonya				X	X	X
Lüksemburg	X	X	X	X	X	X
Hollanda	X	X	X	X	X	X

Norveç	X	X	X	X	X	X
Polonya	X	X	X	X	X	X
Portekiz	X	X	X	X	X	X
İspanya	X	X	X	X	X	X
İsveç	X	X	X	X	X	X
İsviçre	X		X	X	X	X
İngiltere	X	X	X	X	X	X
ABD				X	X	X
Türkiye				X	X	

Kaynak:[57,58,59,60,68]

Çizelge 4.2. İstek Dışı Haberleşmenin Diğer Ülkelerdeki Durumu

	MEVZUAT	MEVZUATIN İSMİ VE YÜRÜRLÜK TARİHİ	KAPSAM İÇİ/KAPSAM DIŞI	KAPSAM İÇİ/KAPSAM DIŞI YÖNTEMİNDE İSTİSNA	AÇIKLAMA
Avustralya	Spam kanunu	2.12.2003	Kapsam içi	Kamu kurumları, siyasi partiler, dini kuruluşlar, yardım kuruluşları, eğitim kurumları	
Avusturya	Telekomünikasyon düzenlemeleri kanunu	2003	Kapsam içi		
Belçika	Elektronik ticaret kanunu	11.3.2003	Kapsam içi	Tüzel kişi, önceden var olan ilişki	
Kanada	Mevcut kanun olan elektronik doküman kanunu	Ocak 2001	Kapsam içi		

Çek Cumhuriyeti	Mevcut kanun olan reklamların düzenlenmesi kanunu	1995	Kapsam içi		
Danimarka	Pazarlama faaliyetleri kanunu		Kapsam içi	Önceden var olan ilişki	
Finlandiya	Telekomünikasyonda veri güvenliği ve mahremiyetin korunması kanunu	1999	Kapsam içi	Tüzel kişi	Yeni bir taslak hazırlanmakta
Fransa	Sayısal ekonomiye güven	Pour la confiance dans i'economie numerique	Kapsam içi	Önceden var olan ilişki, tüzel kişi	
Almanya	Mevcut kanun olan haksız rekabet kanunu	Haksız rekabet kanununa ilişkin değişiklik tasarısı	Kapsam içi	Önceden var olan ilişkide kapsam dışı	
Macaristan	Uzaktan satış konusundaki tebliğ	1999	Kapsam dışı		
İrlanda	Elektronik haberleşme şebekeleri ve hizmetleri	2003	Kapsam içi	Önceden var olan ilişki	
Japonya	Özel e-postaların iletilmesi konusundaki kanun, özel ticari işlemler konusundaki kanun	Temmuz 2002	Kapsam dışı		
Kore	Bilgi şebekesi ve korunması kanunu	Temmuz 2001	Kapsam dışı		
İspanya	Bilgi toplumu hizmetleri kanunu, telekomünikasyon kanunu	Haziran 2002 Kasım 2003	Kapsam içi	Önceden var olan ilişki	
İsviçre	Opt-in konusunda mevzuat hazırlanmakta	Telekomünikasyon Kanunu Haksız Rekabete ilişkin Kanun	Kapsam içi	Önceden var olan ilişki	

İngiltere	Mahremiyet ve elektronik haberleşme düzenlemeleri	11.12.2003	Kapsam içi	Mevcut müşteri ilişkileri için kapsam dışı istisnası uygulanmaktadır. Tüzel kişiler, yeni e-posta kapsam içi kuralları gereğince kapsanmamaktadır.	2002/58/EC sayılı AB Direktifi uygulanmaktadır.
ABD	Can-Spam Kanunu	1.1.2004	Kapsam dışı		Mevzuat, temel amacı ticari bir ürün ya da hizmetin promosyonu veya ticari reklamı olan her türlü ticari e-posta mesajını kapsamaktadır.

Kaynak:[57,58,59,60,68]

5. TÜRKİYE'DEKİ MEVCUT DURUM

Ülkemizde bilgi ve iletişim teknolojilerini kullananların sayısının hızla artmakta olduğu Devlet İstatistik Enstitüsü'nün Ekim 2004'te açıkladığı bir raporda dile getirilmektedir [72].

Ülkemizdeki İnternet kullanıcı sayısında 2000-2004 döneminde sürekli artan bir ivme yakalanmıştır. 2000 yılında 2,5 milyon olan kullanıcı sayısının, 2004 yılı sonunda 10 milyonu aştığı değerlendirilmektedir. Çizelge 5.1'de, 2000 ve 2004 yılları arasındaki İnternet kullanıcı sayısına ilişkin bilgilere yer verilmektedir.

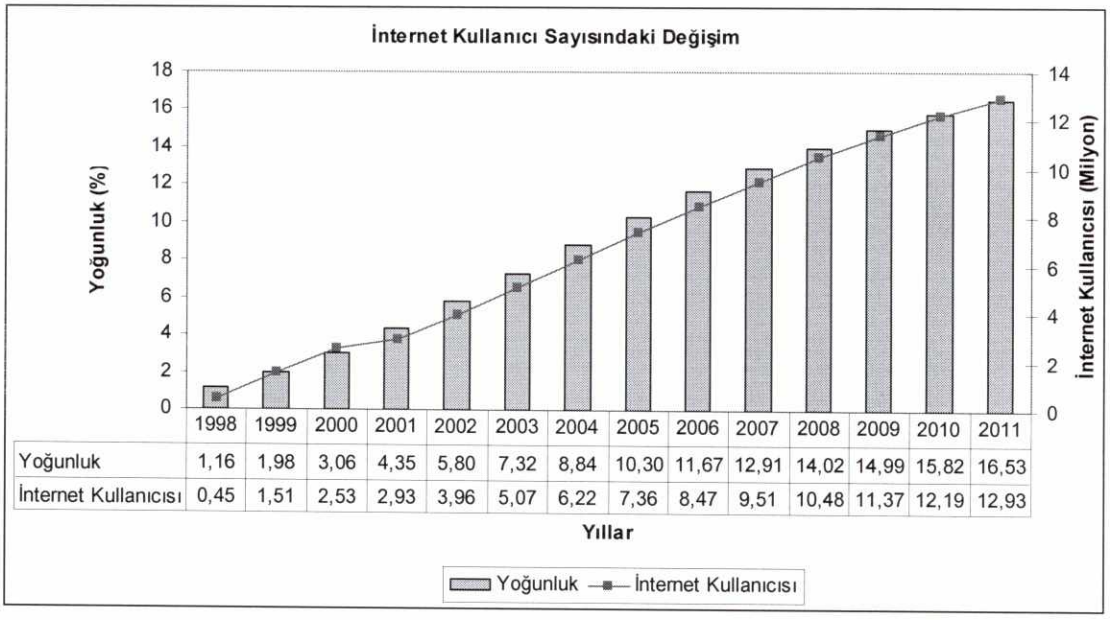
Çizelge 5.1 Yıllar İtibariyle İnternet Kullanıcı Sayıları

Yıllar	Kullanıcı Sayısı	Artış Oranı (%)
2000	2.500.000	25,00
2001	3.200.000	28,00
2002	4.300.000	34,38
2003	6.000.000	39,54
2004	10.220.000	70,33

Kaynak:[73]

Ülkemizdeki İnternet kullanıcı sayısındaki bu hızlı artışa karşın, kullanıcı sayısı gelişmiş ülkelere nazaran düşük seviyelerde seyretmektedir. Çizelge 5.1'den görüleceği üzere, İnternet kullanımındaki artış oranı 2000 yılı için %25,00, 2001 yılı için %28,00, 2002 yılı için %34,38, 2003 yılı için %39,54 ve 2004 yılı için %70,33'tür. Sözkonusu artış oranlarının yükselen bir eğilim içerisinde olması, orta vadede İnternet kullanımının daha fazla yaygınlaşacağının bir göstergesi olarak değerlendirilmekte [73] olup, bu

durumun önümüzdeki yıllarda erişeceği rakamlar Şekil 5.1'de olduğu gibi tahmin edilmektedir.

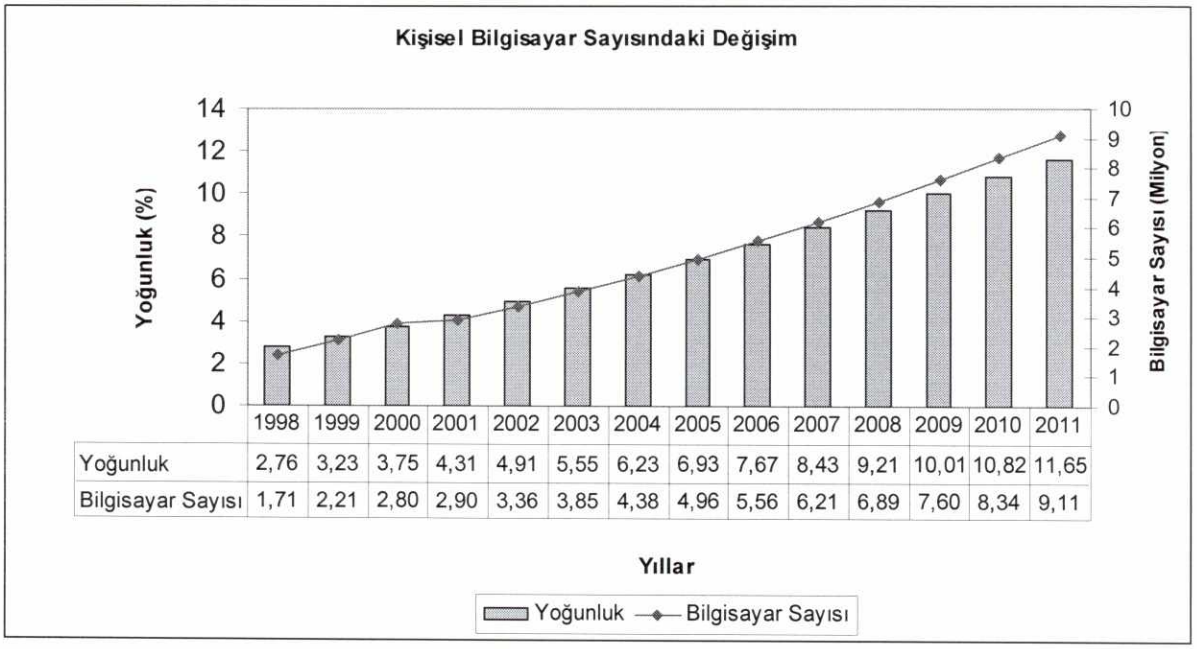


	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Yoğunluk	1,16	1,98	3,06	4,35	5,80	7,32	8,84	10,30	11,67	12,91	14,02	14,99	15,82	16,53
İnternet Kullanıcısı	0,45	1,51	2,53	2,93	3,96	5,07	6,22	7,36	8,47	9,51	10,48	11,37	12,19	12,93

Kaynak: [74]

Şekil 5.1. İnternet Kullanıcı Sayısındaki Değişim

Bununla birlikte, kişisel bilgisayar oranının diğer ülkeler ile kıyaslaması yapıldığında oldukça düşük olmasına rağmen, önümüzdeki yıllarda artış tahminleri Şekil 5.2'de gösterilmektedir.



	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Yoğunluk	2,76	3,23	3,75	4,31	4,91	5,55	6,23	6,93	7,67	8,43	9,21	10,01	10,82	11,65
Bilgisayar Sayısı	1,71	2,21	2,80	2,90	3,36	3,85	4,38	4,96	5,56	6,21	6,89	7,60	8,34	9,11

Kaynak: [74]

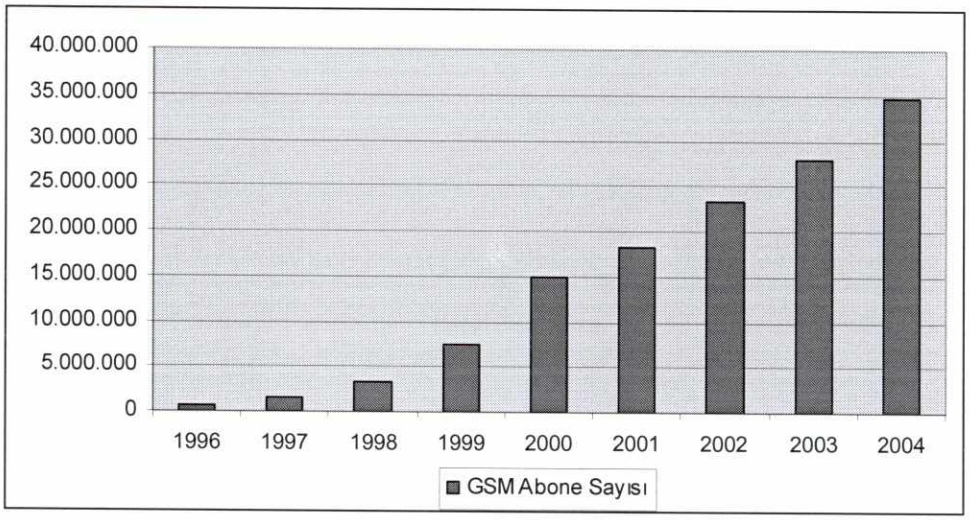
Şekil 5.2.Kişisel Bilgisayar Sayısındaki Değişim

Diğer taraftan ülkemizde iletişim alanında, özellikle de mobil iletişim alanında hızlı bir gelişim süreci yaşanmaktadır. Çizelge 5.2 ve Şekil 5.3'de ülkemizdeki GSM abone sayısındaki artış gösterilmektedir. Nüfus sayısı dikkate alındığında, AB-25 ülkelerinde 2004 yılı için GSM penetrasyon oranı yaklaşık %83 iken Türkiye'de bu oran %49 seviyesindedir. Çizelge 5.2'den de görüleceği üzere GSM abone sayısı Türkiye'de hızlı bir artış göstermiş ve 1996 yılında 692.779 olan abone sayısı 9 yıl gibi bir sürede yaklaşık 50 kat artarak 34.806.084'e ulaşmıştır.

Çizelge 5.2.GSM Abone Sayısı

Yıl	Abone Sayısı	Bir Önceki Yıla Göre Artış Oranı (%)
1996	692.779	58,53
1997	1.481.323	113,82
1998	3.360.000	126,82
1999	7.560.000	125,00
2000	14.970.000	98,02
2001	18.228.598	21,77
2002	23.323.113	27,95
2003	27.887.535	19,57
2004[1]	34.806.084	24,81

Kaynak:[73]



Kaynak:[73]

Şekil 5.3. GSM Abone Sayısı

GSM, İnternet ve bilgisayar kullanımındaki bu artışlara paralel olarak Türkiye'de elektronik ortamda yapılan işlemlerin sayısı hızla artmakta, kurum içi ve kurumlar arası iş süreçleri elektronik ortama taşınmakta, e-devlet ve e-iş süreçleri hızla günlük hayatın bir parçası olmaya başlamaktadır. Bu da ülkemizde bilgi güvenliğinin giderek önem kazanmasına neden olmaktadır [75].

[1] 2004 yılı Kasım ayı itibariyle mevcut GSM abone sayısını göstermektedir.

Ancak, ülkemizde bilgi güvenliği konusunda yapılan araştırmaların sonuçları değerlendirildiğinde, genel olarak karşılaşılan problemlerin en başında kişi ve kurumların, bilginin değerini fazlaca önemsemedikleri, kaynak sıkıntısı yaşadıkları, bilgi ve iletişim teknolojileri güvenliğine önem vermedikleri veya veremedikleri, hangi tedbirlerin alınması gerektiğini bilmedikleri, eğitimli personel sıkıntısı içerisinde oldukları, gerekli olan yazılım ve güvenlik sistemlerine ekstra para ödemek istemedikleri veya ödeyemedikleri, güvenliği dikkate alanların çoğunda ise bilgi ve eğitim eksikliği olduğu anlaşılmıştır [72]. Konuya çözüm bulmak amacıyla bir takım teknolojik önlemler alınmakta, ancak bunlar bilgi güvenliği gibi yaşayan bir süreç içerisinde yetersiz kalmaktadır.

Tam anlamıyla bilgi güvenliğinden söz etmek mümkün olmamakla birlikte, güvenliğin azami ölçüde sağlanabilmesi için teknik önlemlerin yasal düzenlemelerle desteklenmesi gerekmektedir.

Ülkemizde, bilgi güvenliğine ilişkin yasal bir düzenleme bulunmamakta, bilginin ve haberleşmenin güvenliği ve mahremiyetin sağlanması hususları mevcut düzenlemelerle korunmaya çalışılmaktadır.

5.1. Bilgi Güvenliği, Haberleşmenin Gizliliği

5.1.1. Mevcut yasal düzenlemeler

Anayasanın "Haberleşme Hürriyeti" başlığı altında yer alan, 22. madde; "*Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hakim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz.*"

Türk Ceza Kanunu'nun "Haberleşmenin Gizliliğini İhlal" başlığı altında yer alan 132 ve 133. madde; "*Kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlâli haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur. Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ceza yarı oranında artırılır.*"

"*Kişiler arasındaki alenî olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır. Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aya kadar hapis veya adlî para cezası ile cezalandırılır. Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması hâlinde de, aynı cezaya hükmolunur.* "

2813 Sayılı Telsiz Kanunu'nun Genel Esaslar başlığı altında yer alan 4. maddenin (f) ve (g) fıkrasında, "*Olağanüstü haller ile ülkenin güvenliğini ilgilendiren durumlarda, sıkıyönetim, seferberlik ve savaş halinde tüm telsiz cihazları ve sistemleri alınacak tertip ve tedbirlerle, kamu yararına ve Milli Savunma amaçları doğrultusunda kullanılır. Müsaade edilen veya edilmeyen*

frekanslarda yapılacak usulsüz yayınların ve enterferansların izlenmesi ve önlenmesi amacıyla gerekli kontrol tertip ve tedbirleri alınır."

406 Sayılı Kanun (EK:3/5/1995 -4107/2 md.) *"Sermaye şirketleri haberleşmenin gizliliğine, milli güvenlik ve kamu düzenine aykırı davranışta bulunamazlar. Ulaştırma Bakanlığı, sermaye şirketlerinin görev alanlarıyla ilgili faaliyetlerini bütün aşamalarda denetler veya denetletebilir."*

4502 Sayılı Kanunun Madde 2 (a) ve Madde 2 (b)'sine göre TTAŞ (Türk Telekom A.Ş.), Ulaştırma Bakanlığı ile "Telekomünikasyon Hizmetlerinin Yürütülmesine İlişkin Görev Sözleşmesi" imzalamış ve bu sözleşmeyi, 4673 sayılı Kanuna göre Telekomünikasyon Kurumu ile yenilemiştir [76]. Görev Sözleşmesinin 31. Maddesi *"Türk Telekom, haberleşmenin gizliliği prensibine, milli güvenliğe ve kamu düzenine aykırı davranışta bulunamaz.*
Türk Telekom ve çalışanları, yasaların öngördüğü istisnalar dışında haberleşmeyi engelleyemez, gizliliğine dokunamaz, üçüncü şahıslara bildiremez ve açıklayamazlar. Türk Telekom ve çalışanları, Yasalarla belirlenen hallerde istenilen bilgilerin yasayla yetkili kılınan kişi ve kuruluşlara, yine yasalarla belirlenen işlemlere uyulmak sureti ile verilmesini ve söz konusu kişi ve kuruluşlar tarafından elde edilmesini engelleyemez."

Aynı şekilde, Ulaştırma Bakanlığı ile GSM işletmecileri arasında imzalanan İmtiyaz Sözleşmeleri 4673 sayılı kanun hükümlerine göre Telekomünikasyon Kurumu ile yenilenmiştir [76]. Yinelenen bu sözleşmelerin 46. maddesi, *"İşletmeci; haberleşmenin gizliliğine, milli güvenlik ve kamu düzenine aykırı davranışta bulunamaz. İşletmeci ve çalışanlar yasaların öngördüğü istisnalar dışında haberleşmeyi engelleyemez, gizliliğine dokunamaz, başkalarına bildiremez ve açıklayamazlar. İşletmeci ve çalışanları, yasalarla belirlenen*

hallerde istenilen bilgilerin Kanunla yetkili kılınan kişi ve kuruluşlara verilmesini ve elde edilmesini engelleyemezler."

demektedir. Böylelikle, ülkemizde haberleşmenin gizliliği ve bilgi güvenliği koruma altına alınmaktadır.

Bunun yanı sıra bilgi güvenliğine yönelik ihlaller ve bu konuda alınacak cezai önlemler Türk Ceza Kanunu'nda yerini almıştır.

Türkiye'de bilgi güvenliğine yönelik ihlaller, bilişim suçu olarak 1991 yılında, 3756 sayılı Kanunla Türk Ceza Hukuku'na girmiş olup, yeniden düzenlenen Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" başlığı altında 243-246 ncı maddeleri ile ele alınmış, banka ve kredi kartları ile ilgili hükümlere de yer verilmiştir. Kanuna göre

- Sisteme yasal olmayan yollardan veri sokulması, verilerin yok edilmesi, değiştirilmesi,
- Haksız kazanç elde etmek için bilişim sistemine girilmesi,
- Sistemin işleyişinin engellenmesi,
- Sisteme yasal olmayan yollardan veri yerleştirilmesi, var olan verilerin tahrif edilmesi sureti ile sahte belge oluşturulması,

suç olarak kabul edilmiştir. Kanun, bu ihlallere yönelik değişik hallere göre 1 ile 7 yıl arasında değişen hapis cezası öngörülmüştür [77].

5.1.2. Bilgi güvenliği alanında görev ve yetkilerin dağılımı

Türkiye'de bilgi ve iletişim teknolojilerinde bilgi güvenliğini sağlamak amacıyla Tübitak bünyesinde 1968 yılında Elektronik Araştırma Ünitesi-EAÜ kurulmuş, daha sonra da bu ünite 1995 yılında merkezi Gebze'de olmak üzere

UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü)'ne dönüştürülmüştür.

UEKAE, bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmekte ve uygulamaktadır [78].

Bunun yanı sıra ülkemizde pek çok özel şirket, kamu ve özel kuruluşlar bilgi güvenliğini sağlamak amacıyla yazılım, donanım ve danışmanlık hizmeti vermektedir. Ancak, bu kurumların bilgi güvenliği özellikle de ulusal bilgi güvenliği konusunda yetersiz kaldıkları görülerek Haberleşme Üst Kurulu'nda alınan bir kararla; 1997 yılında Genel Kurmay Başkanlığı koordinatörlüğünde ulusal güvenliği ilgilendiren bilgilerin korunması, devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, kısa ve uzun dönemli planların hazırlanması, kriter ve standartlarının saptanması, ihracat ve ithalat izinlerinin ve sertifikalarının verilmesi, bilgi sistemlerinin teknolojiye uyumunun sağlanması, uygulamanın takip ve denetimi kamu ve özel kurum ve kuruluşların arasında koordinasyonun sağlanması amacıyla Ulusal Bilgi Güvenliği Teşkilatı kurma çalışmaları başlamıştır.

Bununla birlikte, Telekomünikasyon Kurumu bilgi güvenliğine ilişkin olarak, telekomünikasyon sektöründe iletişimin güvenliğini ve gizliliğini, işletmecilerin faturalandırma amacıyla abonelere ait tutmuş oldukları her türlü kişisel bilgi ile arama trafiğine yönelik verilerin ve saklanma sürelerine ait bilgilerin güvence altına alınmasına ilişkin düzenlemeleri yapmakla sorumlu bulunmaktadır. Nitekim Kurum, yukarıda yer verilen düzenlemeler ve Telekomünikasyon Hizmet ve Alt Yapılarına İlişkin Yetkilendirme Yönetmeliği ile telekomünikasyon alanında hizmet vermek amacıyla

yetkilendirilmiş işletmecilere getirdiği yükümlülükler ve Telekomünikasyon Sektöründe Kişisel Verilerin Korunması Yönetmeliği kapsamında bahsedilen hususlarla haberleşmenin gizliliği ve güvenliğini sağlamayı hedeflemiştir.

5.1.3. Güvenlik kültürü sağlanmasına yönelik çalışmalar

Türkiye'de bilgi güvenliği kültürü oluşturulmak amacıyla, Başbakanlık tarafından 17 Şubat 2003 tarihinde yayınlanan ve EK-I'de sunulan 2003/10 sayılı Genelge ile başta kamu kurum ve kuruluşları olmak üzere, bilgi ve iletişim teknolojilerinde güvenliğin sağlanması hususunda yürütülen çalışmalarda, 3. Bölüm'de yer verilen OECD'nin Güvenlik Kültürü Rehber İlkeleri'nin göz önünde bulundurulması gerektiği vurgulanmıştır. Ayrıca vatandaşlara daha kaliteli ve hızlı kamu hizmeti sunabilmek, katılımcı, şeffaf etkin ve basit iş süreçlerine sahip olmayı ilke edinmiş devlet yapısı oluşturmak amacıyla 27 Şubat 2003 tarih ve 2003/12 sayılı Genelge ile E-Dönüşüm Türkiye Projesi uygulamaya konmuştur. Bu kapsamda kurum ve kuruluşlar arasında elektronik ortamda bilgi aktarımı ve hizmet sunumunun yaygınlaşması ile bilgi güvenliğinin önemi ve ülkemizde güvenlik kültürü yaratılması gerekliliği ortaya çıkmıştır.

Bunun yanı sıra Türkiye'de bilgi ve iletişim teknolojileri alanında sivil toplum kuruluşu olarak faaliyet gösteren Türkiye Bilişim Derneği (TBD)[1], Türkiye Bilişim Sanayicileri ve İş Adamları Derneği (TÜBİSAD)[2], Türkiye Bilişim Vakfı (TBV)[3], Türkiye Teknoloji Geliştirme Vakfı (TTGV)[4] ve Türkiye Zeka

---

[1] TBD, kamu yararına çalışan dernek vasfına sahip olup, bireysel üyeliğe açık bir dernektir.

[2] TÜBİSAD, bilgisayar donanım ve yazılım, medya-publishing, tüketici elektroniği, dağıtım, telekom konusunda iştigal eden yaklaşık 90 şirketin üye olduğu bir dernektir.

[3] TBV, Türkiye'de internet altyapısının gelişimine ve bilişim sektörünün ekonomi içindeki payının arttırılmasına katkıda bulunmak üzere faaliyet gösteren bir vakıftır.

[4] TTGV, ülkemizin teknolojik altyapısının geliştirilip güçlendirilmesi ve Türk sanayinin uluslararası pazarlardaki rekabet gücünün artmasına katkıda bulunan bir vakıftır.

Vakfı (TZV)[1] bulunmaktadır. Sözkonusu kuruluşlar Türkiye'de güvenlik kültürü oluşturulmasına katkıda bulunmaktadırlar.

5.2. Kişisel verilerin korunması ve mahremiyetin sağlanması

Ülkemizde kişisel verilerin korunması, AB hedeflerine rağmen yeterince ilgi görmemiştir. Söz konusu durum, AB tarafından hazırlanan İlerleme Raporları'nda da dile getirilmiştir. Bu kapsamda, AB tarafından 6 Ekim 2004 tarihinde yayınlanan son ilerleme raporunda veri güvenliği konusuna dikkat çekilmiş ve şu hususlara işaret edilmiştir:

- Kişisel verilerin korunmasına ilişkin olarak hazırlanan taslak mevzuata yönelik çalışmaların halen devam ettiği,
- Kişisel verilerin korunması ve bilgi toplumu hizmetlerine yönelik mevzuat uyumunun tamamlanması ve bu çerçevede uygulamanın gerçekleştirilmesi,
- Ocak 2004 tarihinde her ne kadar E-imza Kanunu çıksa da, halen kişisel verilerin korunmasına yönelik olarak somut adımların atılmamış olduğu,
- Hazırlanan kişisel verilerin korunmasına ilişkin taslak yasanın, AB mevzuatı ile uyumlu olması gerektiği,
- Türkiye tarafından 1981 yılında imzalanmış ancak halen Meclis tarafından onaylanmayan 1981 tarihli Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkında Sözleşme'nin Türkiye tarafından bir an önce onaylanması gerektiği,
- Bağımsız veri koruma kurumunun bir an önce kurularak faaliyete geçirilmesi gerektiği [79, 80].

---

[1] TZV, bilgiye, zekaya, insana ve entelektüel değerlere gereken değerlerin verilmesini sağlayan bir dernektir.

Kişisel verilerin korunması diğer ülkelerle kıyaslandığında oldukça geri kalmış olmasına rağmen ülkemizde mevcut kanunlarla korunmaya çalışılmaktadır.

5.2.1.Mevcut yasal durum

Türkiye'de özel hayatın gizliliği Anayasa ile korunmuş haklardandır. Anayasanın "*Özel Hayatın Gizliliği ve Korunması*" başlığının 20 ve 21 nci maddeleri bu konuya ayrılmıştır.

20. Madde "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Adli soruşturma ve kovuşturmanın gerektirdiği istisnalar saklıdır.*
Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hakim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça, kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz."

21. Madde, "*Kimsenin konutuna dokunulamaz. Kanunun açıkça gösterdiği hallerde, usulüne göre verilmiş hakim kararı olmadıkça; gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınan merciin emri bulunmadıkça, kimsenin konutuna girilemez, arama yapılamaz ve buradaki eşyaya el konulamaz.*"

Ayrıca, Türk Medeni Kanunu'nun 24. maddesi ile özel hayatın gizliliği koruma altına alınmıştır.

24. Madde, "*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen*

kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."

Ayrıca Türkiye, herkesin özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesini hükme bağlayan Avrupa İnsan Hakları Sözleşmesi'ni onaylayarak kişilerin özel değerlerinin korunmasını garanti altına almıştır.

Bu itibarla, Türkiye Avrupa Konseyi tarafından hazırlanan Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması hakkında 1981 tarihli Avrupa Konseyi Sözleşmesi'ni 28.01.1981 tarihinde imzalamış, ancak yürürlüğe koyamamıştır. Ayrıca, Türkiye, Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin OECD Rehber İlkeleri'ni de imzalamıştır. Özel hayatın gizliliği Türk Ceza Kanunu'nda da yerini almış, *"Hayatın Gizli Alanına ve Özel Hayata Karşı Suçlar"* başlığını taşıyan Dokuzuncu Bölüm altında yer alan 134-136. maddelerinde kişisel verilerin korunması ile ilgili hükümlere yer verilmiştir.

Kanuna göre

- Kişinin rızası olmaksızın veya kanunun öngördüğü şekil ve usullere uyulmaksızın kişisel verilerin bilişim sistemine yerleştirilmesi veya işlenmesi,
- Bilişim sistemine yerleştirilen verilerin gerekli güvenlik tedbirleri alınmaksızın başkalarının eline geçmesine neden olunması,
- Hassas verilerin kişinin rızası alınmaksızın sisteme yerleştirilmesi ve bu verilerin yetkisiz kişilere açıklanması,

suç olarak sayılmış ve çeşitli durumlara göre 6 aydan 4 yıla kadar hapis cezası öngörülmüştür [81].

Ancak, genel nitelikteki bu kurallar, bilgi ve iletişim teknolojilerinde meydana gelen değişiklikler karşısında yetersiz kalmıştır. Bu nedenle, Türkiye'nin gelişen teknolojiyi de göz önünde bulundurarak AB'nin olmazsa olmaz şartlarından olan kişisel verilerin güvenliğini garanti altına alması gereklidir [15].

Bu kapsamda, 95/46/EC sayılı Direktife uygun olarak Adalet Bakanlığı tarafından hazırlanan "Kişisel Verilerin Korunması Kanunu Tasarısı"nın yasallaşarak yürürlüğe girmesiyle Türkiye'deki bu konudaki eksiklik büyük ölçüde giderilerek Avrupa Birliği normlarına uygun bir kişisel veri güvenliği sağlanmış olacaktır [82].

5.2.2. Kişisel Verilerin Korunması Kanun Tasarısı

Kişisel nitelikteki verilerin otomatik işleme tabi tutulması ve bu yöntemle kişilik haklarının korunmasına ilişkin kanun tasarısını hazırlamak üzere ilk komisyon Adalet Bakanlığı bünyesinde 13 Eylül 1995 tarihinde kurulmuştur. Ancak, komisyonun çalışmalarını tamamlayamaması üzerine 18 Eylül 2000 tarihinde yeniden oluşturulmuştur. Yeniden oluşturulan komisyon, 2003 tarihi itibariyle "Kişisel Verilerin Korunması Kanun Tasarısı"nı hazırlamıştır.

Genel olarak AB'nin 95/46/EC sayılı Direktifi'nin izlerini taşımakta olan Kanun Tasarısı [15], kişisel verilerin işleme tabi tutulmasında kişiliğin, temel hak ve özgürlüklerin korunmasını ve kişisel verileri işleme tabi tutan kişi ve kurumların uyacakları esas ve usülleri düzenlemektedir. (madde 1) Tasarı hükümleri, kişisel verileri işleme tabi tutulan kişiler ile bu verileri işleme tabi tutan kamu kurum veya kuruluşları ile gerçek ve özel hukuk tüzel kişileri hakkında uygulanmaktadır [83]. (madde 2)

Tasarı, gerçek ve tüzel kişileri kapsamanın yanı sıra ayrıca, elektonik ortamda tutulan ve işlenen verilere uygulandığı gibi elle işlenen ve geleneksel dosyalama yöntemiyle tutulan verilere de uygulanmaktadır.

Tasarıda yer verilen ilkeler şu şekildedir:

- Kişisel veriler hukuka ve dürüstlük kurallarına uygun olarak elde edilmeli,
- Kişisel veriler, hukuka ve dürüstlük kurallarına uygun olarak işlenmeli,
- Kişisel veriler, güncel olmalı, bu nedenle gerektiğinde silinmeli veya düzeltilmeli,
- Kişisel veriler, toplandıkları amaç çerçevesinde kullanılmalı ve gerekli olan süre kadar saklanmalı,
- Dini, siyasi inanç, genetik ve tıbbi özellikler gibi hassas verilerin özel yöntemlerle korunması

gerekmektedir.

Ancak, bu ilkeler hukuki yükümlülüğün yerine getirilmesi, ilgili kişinin hayati çıkarlarının korunması, kamu yararı veya kamu düzeni gereği olması durumlarında bazı sınırlamalara tabi bulunmaktadır.

Taslak ayrıca, verileri işlenen kişinin bu verilere belirli ve makul aralıklarla kendine ait bilginin nelerden ibaret olduğunu, verilerin tutulma amacını, bilgileri hangi kurumun işleme tabi tutacağını ve işleme tabi tutacak kurumların kimliklerini öğrenme hakkı olduğunu vurgulamaktadır. Kişinin kendisine ait bilgiler üzerinde düzeltme ve değiştirme hakkı da bulunmaktadır. Ancak, özel kanunda açıkça öngörülmüş olması, üstün nitelikte bir kamu yararı, özellikle devletin iç ve dış güvenliğinin korunması

açısından gerekli olması, bilgi verilmesinin idarî veya cezaî bir soruşturmanın amacının gerçekleşmesini güçleştirmesi, durumlarında sınırlayabilmektedir [15].

Yabancı ülkelere verilerin yollanması durumunda ise veri sorumlusu kişilik haklarının korunması için, kişisel verinin aktarılacağı ülkede verinin kendisi ile eş değer koruma altına alınıp alınmayacağı hususunda Kurumun onayını almak zorundadır. Ancak, kanuni bir durumun olması veya ilgili kişinin rızası olması halinde bu onay aranmamaktadır.

Tasarıda, hassas verilerin aşağıda belirtilen istisnai durumlar

- Kanunla açıkça verilen bir görevin yerine getirilmesi,
- Hakkında hassas verisi işlenecek kişinin kişilik hakkının ihlal etmemek kaydıyla Bakanlar Kurulu kararıyla işleme izni verilmesi,
- İlgilinin rıza göstermesi,
- İlginin hassas verilerini herkese açıklaması ve herkes tarafından bilinmesi

halinde işlenebileceği vurgulanmıştır.

Tasarının 40. maddesi, Kanunla korunan kişisel verileri, kendisine veya başkasına yarar sağlamak veya başkasına zarar vermek amacıyla hukuka aykırı olarak toplayan, elde eden, kaydeden, düzenleyen, depolayan, uyarlayan, değiştiren, değerlendiren, kullanan, açıklayan, aktaran, ayıran, birleştiren, donduran, silen veya yok edenler, fiil başka bir suç oluştursa bile, altı aydan bir yıla kadar hapis veya bir milyar liradan iki milyar liraya kadar ağır para cezasıyla cezalandırmaktadır. Kişilik hakları kapsamında yer alan

değerlere ilişkin veriler ile özel niteliği olan verileri aynı maksatla hukuka aykırı olarak işleyenlerin cezası, üçte birden yarıya kadar artmaktadır. [15]

Bu durum ile genel olarak idari nitelikteki cezaî önlemlere yer verilmiş, cezaî yaptırımlar Türk Ceza Kanunu'nun 134-136. maddelerinde yer almıştır.

Tasarıda belirlenen görevleri yapmak üzere tüzel kişiliğe, idari ve mali özerkliğe sahip ve doğrudan Başbakanlığa bağlı, merkezi Ankara'da olmak üzere "Kişisel Verileri Koruma Kurumu"nun kurulması da öngörülmektedir.

5.2.3. Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

AB'ye uyum çalışmaları kapsamında, "AB Müktesabatının Üstlenilmesine İlişkin Türkiye Ulusal Programı"nda "Telekomünikasyon ve Bilgi Teknolojileri" başlığı altında bilgi ve iletişim teknolojileri konusuna yer verilmiştir. Ulusal Program'da belirlenen Mevzuat Takvimi uyarınca Telekomünikasyon Kurumu, genel nitelikli olarak hazırlanan "Kişisel Verilerin Korunması Kanun Tasarısı"nı telekomünikasyon sektöründe uygulamakla yükümlü kılınmıştır [88].

Bu kapsamda Kurum, telekomünikasyon alanında kişisel verilerin işlenmesi ve mahremiyetin korunması ile ilgili 15 Aralık 1997 tarih ve 97/66/EC sayılı Direktifi ve elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğinin korunması hakkında 12 Temmuz 2002 tarih ve 2002/58/EC sayılı Direktifi iki ayrı yönetmelik ile 31.12.2003 tarihinde yürürlüğe koymayı hedeflemiştir [15]. Ancak Kurum, 97/66/EC ve 2002/58/EC sayılı Direktifleri "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin

Korunması" hakkındaki yönetmelik ile birleştirmiş ve sözkonusu yönetmeliği 6 Şubat 2004 tarih ve 25365 sayılı Resmi Gazete'de yayınlayarak yürürlüğe koymuştur.

Telekomünikasyon şebekelerinde hizmetlerin yürütülmesi için işlenen kişisel bilgiler yönünden gizliliğin korunmasını hedef alan yönetmelik, ilgili AB Direktifi ile büyük ölçüde uyumlu bulunmaktadır [15].

Yönetmelik kapsam itibariyle, telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri kapsamaktadır. Yönetmeliğin ayrıntılı faturalar (madde 12), arayan hattın kimliğinin açıklanmasının engellenmesi (madde 13), arayan hattın bağlanmasının engellenmesi (madde 14) ve kötü niyetli ve rahatsızlık verici aramaların takibi amacıyla (madde 18), arayan abonenin kimliğini içeren bilgilerin saklanmasına ilişkin düzenlemeler yalnızca sayısal ve uygun işaretleşme sistemine sahip santraller ile sınırlı tutulmuştur. Ancak, sözkonusu durumun teknik olarak mümkün olmaması veya işletmeciye aşırı yük getirmesi durumunda, yönetmelik durumun işletmeci tarafından gerekçeli olarak Kuruma bildirilmesini zorunlu kılmıştır.

İletişim güvenliği, yönetmelik direktif ile uyumlu olarak işletmeciye, şebeke güvenliğinin ihlaline karşı tüm gerekli teknik ve yapısal önlemleri almasını ve bunu Kurum'un onayına sunması yükümlülüğünü getirmiştir. Ayrıca işletmeci, olağan bir risk durumunda da abonelerini uyarmak zorundadır.

İletişimin gizliliği, direktif iletişimin gizliliğinin sağlanmasını zorunlu kılmıştır. Bu kapsamda, yönetmelik yasaların öngördüğü durumlar haricinde, haberleşmeye taraf olanların izni olmaksızın, telekomünikasyonun üçüncü kişilerce dinlenmesi, kaydedilmesi, saklanması ve gözetimini yasaklamıştır.

Trafik verilerinin işlenmesi, direktif iletişim bağlantısının abone veya kullanıcının aksi isteği olmadığı sürece iletişimin sona ermesi ile beraber trafik verisinin silinmesini veya anonimleştirilmesini öngörmüştür. Bu kapsamda yönetmelik, trafik verilerinin işlenmesi ile ilgili olarak işletmecinin yetkisi altındaki kişiler telekomünikasyon hizmetlerini faturalama ve bu hizmetlerin trafiğinin düzenlenmesinden sorumlu idare yanında, müşteri hizmetleri, yolsuzluk tespitleri, elektronik telekomünikasyon hizmetleri pazarlama veya katma değerli hizmet ile görevli kişileri yetkili kılmıştır. İşlenebilecek veriler ise, iletişim hizmetinin sağlanmasında gerekli kapsam ve süre ile sınırlı tutulmaktadır. Ayrıca verilerin işlenmesinde kişinin rıza göstermesi şartı aranmaktadır.

Ayrıca, abone ve kullanıcılarla ilgili yer verileri sadece abone ve kullanıcıların isimsizleştirildiği veya katma değerli bir hizmetin sağlanması için gereken kapsam ve sürede abonelerin aksi başvuruları olmadığı hallerde işlenebilecek ve işletmeciler yer verilerinin işlenmesini geçici olarak reddetme olanağını basit bir yöntemle ve ücretsiz olarak kullanıcı veya abonelerine sağlayacaktır.

Arayan ve aranan hattın gösterilmesi, yönetmelik direktif ile uyumlu olarak, işletmeciye aramayı yapan abonesine basit bir yöntemle ve ücretsiz olarak her arama için arayan hattın kimliğinin açıklanmasını engelleme olanağı tanımasını ve arayan hattın kimliğini gizlemesi durumunda kullanıcıya aramayı reddetme imkanının ücretsiz olarak sağlanması zorunluluğunu hükme bağlamıştır. Ancak bu hüküm sadece sayısal ve uygun işaretleşme sistemine sahip santrallerden hizmet alan aboneler için geçerli olmaktadır.

Rehber bilgileri, yönetmelik abonelerin, yazılı ve elektronik rehberlere kaydedilmeden önce ücretsiz olarak rehberi oluşturan yetkili birimlerce bilgilendirilmesini ve abonelerin istedikleri zaman bu bilgileri ücretsiz olarak rehberi oluşturan yetkili birimlerden kaldırma veya değiştirme talebinde

bulunabilmesini hükme bağlamıştır. Bu konuda yönetmeliğin direktiften farkı tüzel kişilere yer vermiş olmasıdır. Ayrıca, yönetmelikte kişisel verilerin reklam amacıyla kullanılamayacağı, adresinin ve cinsiyetine ilişkin bilginin rehberde yer alıp almaması hususu netlik kazanmamıştır.

İstek dışı haberleşme, yönetmelik faks, elektronik posta, kısa mesaj gibi otomatik arama sistemlerinin kişinin önceden rızası olmadan siyasi propaganda ve doğrudan pazarlama amacıyla kullanılamayacağını (kapsam içi) belirtmiştir. Kullanılması halinde de kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkının ücretsiz ve kolay bir yolla sağlanması (kapsam dışı) gerektiğini vurgulamıştır. Ayrıca göndericinin kimliğini saklayan veya alıcının bu iletişimin sonlandırılması konusunda talepte bulunacağı bir adresi içermeyen elektronik postaların gönderilmesi abonenin talebi halinde engelleneceğini belirtmektedir.

5.3. Türkiye'de İstek Dışı Haberleşme

E-posta konusu, özel hayatın gizliliği ve iletişim özgürlüğü açısından son derece hassas bir konu olması nedeniyle kişisel veri kapsamında değerlendirilmekte ve bu verinin kişinin rızası olmadan kullanılması kişinin mahremiyetini ihlal etmek olarak algılanmaktadır [90].

Ancak, Türkiye'de istek dışı haberleşme hak ettiği öneme sahip olamamıştır. Konu bir takım teknik önlemler alınarak çözümlenmeye çalışılmaktadır. Sadece teknik önlemler ile çözüme kavuşturulamayacak olan istek dışı haberleşmeyi önleme konusunda Türk Mevzuatı içinde bir düzenleme bulunmamakta, mevcut düzenlemeler ile soruna çözüm bulunmaya çalışılmaktadır.

Tüketicinin Korunması Kanunu'nda haksız rekabete ilişkin hükümlerin yer aldığı 16'ncı maddede "*Ticari reklam ve ilanların kanunlara, Reklam Kurulunca belirlenen ilkelere, genel ahlaka, kamu düzenine, kişilik haklarına uygun, dürüst ve doğru olmaları esastır. Tüketiciyi aldatıcı, yanıltıcı veya onun tecrübe ve bilgi noksanlıklarını istismar edici, tüketicinin can ve mal güvenliğini tehlikeye düşürücü, şiddet hareketlerini ve suç işlemeyi özendirici, kamu sağlığını bozucu, hastaları, yaşlıları, çocukları ve özürlüleri istismar edici reklam ve ilanlar ve örtülü reklam yapılamaz*" denmektedir.

Türk Medeni Kanunu'nun 24'üncü maddesinde "*Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hakimden, saldırıda bulunanlara karşı korunmasını isteyebilir*" denmektedir.

Ayrıca istek dışı haberleşme, Telekomünikasyon Kurumu tarafından hazırlanan "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"in [92] 20'nci maddesinde "*İşletmeciler kişi müdahalesi olmadan çalışan fakslar, elektronik posta, kısa mesaj gibi otomatik arama sistemlerini, abonenin önceden izni olmadan siyasi propaganda amacıyla kullanamazlar. Sözkonusu otomatik arama sistemlerinin doğrudan pazarlama amacıyla kullanılması halinde kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı ücretsiz ve kolay bir yolla sağlanır. Doğrudan pazarlama amacıyla gönderilen ve kimin adına haberleşme yapıldığı hususunda göndericinin kimliğini saklayan veya alıcının bu iletişimin sonlandırılması konusunda talepte bulunacağı bir adres bulunmayan elektronik mektupların gönderilmesi abonenin bu yöndeki talebi halinde engellenir.*" denilerek düzenlenmeye çalışılmıştır. Bu konudaki değerlendirme yönetmeliğin ilgili maddesinde ele alınmıştır.

Bunların yanı sıra Türkiye'de istek dışı haberleşme ile mücadele amacıyla 1999 yılında sanal çalışma grubu olarak "Türk Anti-Spam Organizasyonu - TASO" kurulmuştur. Çeşitli kamu kurum ve kuruluşları ile üniversiteler tarafından da desteklenen sözkonusu grup çalışmalarını www.spam.org.tr web adresi ile sürdürmektedir. Bu web adresi ile kişileri istek dışı haberleşme konusunda bilgilendiren ve bilinçlendiren grup sitede Türkiye'de istek dışı haberleşmeye karşı alınabilecek teknik çözümler oluşturmaya çalışmaktadır.

İnternet Üst Kurulu, istek dışı haberleşme ile mücadele konusunda kişileri bilgilendirmek ve bilinçlendirmek amacıyla 2000 yılında "Spam Bildiri"si yayınlamıştır. Sözkonusu bildiride, istek dışı haberleşmenin sakıncaları anlatılarak bu konuda kısa, orta ve uzun dönemde yapılması gereken hususlara değinilmiştir. Kısa dönemde, elektronik adres veri tabanı ticaretinin engellenmesi kapsamında yasal sürecin başlatılması, istek dışı haberleşme eylemlerinin engellenmesi kapsamında İnternet servis sağlayıcılarının ve kurumsal kullanıcıların teknik işbirliği yapmaları gerekmektedir. Orta ve uzun dönemde ise, e-posta kullanarak reklam, bilgilendirme yapmak isteyen kuruluşlara yönelik düzenlemelerin yapılması, kullanıcı kitlesinin bilinçlendirilmesi ve örgütlenme çalışmalarının yapılması gerekmektedir [93].

6. SONUÇ VE ÖNERİLER

6.1. Sonuç

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler yeni bir çağ yaratmıştır. Bilgi çağı olarak adlandırılan bu çağda, bilgisayar ve İnternet kullanım oranı artmış, elektronik ortamda yapılan işlemler yoğunluk kazanmış, e-devlet ve e-ticaret uygulamaları yaygınlaşmıştır.

Bilgi ve iletişim teknolojilerindeki bu hızlı gelişme ve yaygınlaşma bilginin elektronik ortamda tutulması, işlenmesi ve dünyanın diğer bir ucuna hızlı bir şekilde aktarılmasını kolaylaştırmış, mobil telefon kullanıcılarının yerinin belirlenebilmesi, arayan ve aranan numaranın görülebilmesi gibi olanakları da sunmuştur. Ancak, imkan ve olanaklar bu teknoloji üzerindeki bilginin üçüncü kişilerin eline geçerek mahremiyetin bozulmasına sebep olmuştur. Bu da bilginin güvenliğini sağlamayı, bireylerin, işletmelerin ve ülkelerin en önemli sorunu haline getirmiştir. Bu nedenle, bireyler, işletmeler ve ülkeler bilgiyi korumadaki alışıla gelen yöntemleri terk ederek yeni teknik önlemler ve yasal düzenlemelerin yanı sıra diğer kurum, kuruluş ve ülkelerle işbirliği kurma şekline yönelmişlerdir.

Günümüzde, bilgi güvenliğinin bu kadar önemli olmasının temelinde, kişilerin, kurum ve kuruluşların iş devamlılığını sağlamak, meydana gelebilecek zararı en aza indirebilmek, kazancın ve iş fırsatlarının artırılması amacıyla bilgiyi değerli bir varlık olarak görmeleri ve korumak istemeleri yatmaktadır.

Bu itibarla, uluslararası kuruluşlar bilgi güvenliği konusuna oldukça önem vermekte ve yoğun çalışma yapmaktadırlar. Ancak, bilgi güvenliğinin oldukça

geniş, kapsamlı ve yaşayan bir süreç olması nedeniyle bilgi güvenliğini sağlama konusunda somut çıktılar elde edilememiştir. Bununla birlikte, ülkelerin kendi demokratik ve toplum değerleri ile bağdaşık güvenlik kültürü oluşturmalarının en iyi önlem olacağı sonucuna ulaşılmıştır.

Bu nedenle, ülkemizin bir güvenlik kültürü yaratmasının bilgi güvenliğini sağlamakta atılacak en büyük adım olacağı değerlendirilmektedir. Bilgi güvenliğini azami ölçüde sağlamak için etkin ve verimli bir "Güvenlik Kültürü"nün oluşturulması oldukça önemlidir. "Güvenlik Kültürü"nün oluşturulmasında hükümet, kamu kurum ve kuruluşları ile özel sektör, sivil toplum kuruluşları ve bireysel kullanıcılara önemli görevler düşmektedir. Zira küresel bir ağ haline gelen bilgi ve iletişim teknolojileri her bireyi, kurumu ve hükümeti birbirine karşı sorumlu kılmaktadır.

Diğer taraftan, bu çalışmanın üçüncü bölümünde ağırlıklı olarak yer verilen ve bilgi güvenliğinin temel unsuru olan kişisel verilerin korunması ve mahremiyetin sağlanması konusunda uluslararası kuruluşların, özellikle AB'nin titizlikle durmakta olduğu, üye ülkelere veri koruması konusunda düzenleme yapmaları ve veri koruması ile ilgili kurumları kurmaları gerektiği konusunda zorunluluk getirdikleri tespit edilmiştir.

Ülke örneklerinden de anlaşılacağı üzere AB, OECD gibi uluslararası kuruluşlara üye ülkelerin hepsinin veri koruması ile ilgili olarak düzenleme yaptıkları ve veri korumasından sorumlu kurumlara sahip oldukları görülmektedir.

Ancak, Türkiye'deki mevcut durum değerlendirildiğinde Ulusal Program hedeflerine rağmen veri koruması konusunda oldukça geri kalındığı

görülmektedir. Ülkemizin AB mevzuatını uyumlaştırma sürecinde, veri korumasına önem vermesi gerekmektedir.

Bu kapsamda, AB tarafından özel hayatın gizliliğine ilişkin temel hakların korunması amacıyla genel nitelikli olarak düzenlenen 95/46/EC sayılı Direktifi uyumlaştırmak için Adalet Bakanlığı tarafından hazırlanan "Kişisel Verileri Koruma Kanunu"nun ivedilikle çıkarılmasının gerekli olduğu sonucuna ulaşılmaktadır. Bu kanunla birlikte "Kişisel Verileri Koruma Kurumu"nun da kurularak AB'nin olmazsa olmaz şartının yerine getirilmesinin ve AB normlarında veri koruma düzeyinin sağlanmasının faydalı olacağı değerlendirilmektedir.

AB'nin 2002/58/EC sayılı Direktifi ile elektronik haberleşme sektöründe, kişisel verilerin ve mahremiyetin azami seviyede korunması ve telekomünikasyon şebekelerinin güvenliğinin ve bütünlüğünün sağlanması ve bunun sürdürülebilirliğinin temin edilmesi hususunda gerekli düzenlemeler hususu ele alınmıştır. Telekomünikasyon Kurumu, Ulusal Program'da da belirtildiği üzere "Kişisel Verileri Koruma Kanunu"nun sektör bazında uygulaması olan sözkonusu Direktifin uyumlaştırılmasından sorumlu bulunmaktadır.

Bu kapsamda, Telekomünikasyon Kurumu bilgi güvenliğine ilişkin olarak telekomünikasyon sektöründe iletişimin güvenliğini ve gizliliğini, işletmecilerin faturalandırma amacıyla abonelere ait tutmuş oldukları her türlü kişisel bilgi ile arama trafiğine yönelik verilerin ve saklanma sürelerine ait bilgilerin güvence altına alınmasına ilişkin düzenlemeleri yapmakla sorumlu bulunmaktadır.

Kurum, 95/46/EC sayılı Direktifi uyumlaştırmak amacıyla hazırlanmış olan Kişisel Verilerin Korunması Kanun Tasarısı'nda öngörülen güvencelerin, telekomünikasyon sektöründe tam ve etkin bir biçimde uygulamaya konulması amacıyla AB tarafından yayımlanan 97/66/EC ve 2002/58/EC sayılı Direktifleri uyumlaştırmak amacıyla Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" yayınlayarak telekomünikasyon alanında faaliyet gösteren işletmecilerin uymaları gereken usul ve esasları belirlemiştir.

AB'nin ilgili direktifleri ile büyük ölçüde uyumlu olan yönetmelik ülkemizde bilgi güvenliği konusunda atılan ilk adım olması nedeniyle Telekomünikasyon Kurumu açısından oldukça önemli bir yer tutmaktadır. Ancak, yönetmelikte "kişisel veri" tanımının "kişisel bilgi" olarak kullanılmış olması, "Kişisel Verileri Koruma Kanun Tasarısı" ile uyumlu olmaması dikkat çekmektedir. Tanımın sözkonusu kanun tasarısı ile uyumlu hale getirilmesinin uygun olacağı değerlendirilmektedir. Ayrıca işletmecilerle yapılan görev sözleşmelerinin de yönetmelik kapsamında yeniden gözden geçirilerek eksik olan hususların ele alınmasının faydalı olacağı sonucuna varılmaktadır.

Bununla birlikte, Kurum tarafından genel izin ile telekomünikasyon hizmetleri verme konusunda yetkilendirilen İSS'lere bilgi güvenliğini sağlamada bir takım yükümlülüklerin verilmesinin faydalı olacağı sonucuna varılmıştır. Her ne kadar İSS'lerin saniyede bir veri aktarımı yaptığı ve aktardıkları her bilginin içeriğini izlemelerinin ve denetlemelerinin hem mümkün olamayacağı, hem de etik açıdan yanlış olacağı düşünülse de kendi aboneleri ile yaptıkları sözleşmelerde bilgi güvenliğini sağlamaya yönelik bir takım hükümlerin konulmasının faydalı olacağı düşünülmektedir.

Diğer taraftan, bilgi güvenliğini ve mahremiyeti en çok tehdit eden unsur olan istek dışı haberleşmenin her geçen gün artan bir sorun oluşturduğu, OECD, ITU ve AB gibi uluslararası kuruluşların artan sorunu önlemek amacıyla pek çok çalışma yaptığı ve bu konuda bildiri ve tavsiye kararları yayınladığı tespit edilmiştir. Bu konuda AB'nin hazırlamış olduğu Mahremiyet Direktifi olarak da adlandırılan 2002/58/EC sayılı Direktif bağlayıcı nitelik taşımakta iken ITU ve OECD'nin bildiri ve tavsiye kararları yol gösterici nitelik taşımaktadır.

Dünya örnekleri incelendiğinde istek dışı haberleşmenin özellikle ABD'de rahatsız edici durumlara ulaştığı görülmektedir. Ülkemizde istek dışı haberleşme konusu diğer ülkelere kıyasla rahatsız edici boyuta ulaşmamış olduğu tespit edilmekle birlikte, e-posta ve İnternet kullanımının önümüzdeki günlerde artması ve bireylerin İnternette kişisel verilerini nasıl koruyacaklarını bilmemeleri ile istek dışı haberleşmenin önümüzdeki günlerde artan bir sorun olacağı düşünülmektedir.

İstek dışı haberleşmeyi önleme konusunda belirli bir kurum olmamakla birlikte dünya örneklerine bakıldığında ABD ve İngiltere örneğinde olduğu gibi tüketicileri koruma kurumunun, Fransa'da olduğu gibi kişisel verileri koruma kurumunun, Avustralya ve Almanya örneğinde olduğu gibi düzenleyici kurumların sorumlu olduğu görülmektedir.

Ülkemizde 2002/58/EC sayılı Direktifin uyumlaştırılmasından Telekomünikasyon Kurumu'nun sorumlu olması nedeniyle istek dışı haberleşmeyi önleme konusunda da düzenlemeleri yapmakla sorumlu olan kuruluşun Telekomünikasyon Kurumu olduğu sonucuna ulaşılmıştır.

Direktifi uyumlaştırmak amacıyla hazırlanan yönetmeliğin 20 nci maddesinde istek dışı haberleşme hususu düzenlenmeye çalışılmıştır. Ancak, sözkonusu

yönetmeliğin günümüzde artan bir tehdit unsuru oluşturan istek dışı haberleşmeyi önlemede yetersiz olduğu düşünülmektedir. Bunun yanısıra, AB'de kapsam içi yönteminin genel olarak kabul görmesi ve yönetmelikte de kullanıcı yararına olan bu yöntemin benimsenmesinin uygun olduğu düşünülmektedir.

Bunun yanı sıra, istek dışı haberleşmenin önlenmesi amacıyla cezai müeyyidelerin uygulanması yönetmelikle mümkün olmadığından, bu hususun kanunlarca suç olarak tanımlanması zorunluluğu ortaya çıkmaktadır. Bu nedenle istek dışı haberleşmenin Elektronik Haberleşme Kanunu ile düzenlenebileceği ve Kanuna bu hususta hükümlerin konmasının faydalı olacağı mütalaa edilmektedir.

6.2. Öneriler

Bilindiği gibi, günümüzün en değerli ve korunması gereken varlığı haline gelen bilgiyi korumada önemli ilerlemeler kaydetmiş ülkeler gelişmişlik düzeyinde önemli iyileşmeler kaydetmişlerdir.

Türkiye'nin de gelişmiş ülkeler seviyesine ulaşması, ekonomik değişim ve toplumsal dönüşümünü tamamlayabilmesi ve rekabetçi dünyada yerini alabilmesi için, bilgi ve iletişim teknolojileri üzerinde saklanan ve aktarılan bilginin güvenliğini ve kişisel mahremiyetini sağlaması gereklidir.

Güvenlik açısından göz önüne alınması gereken husus, güvenlik alanlarının çok iyi tespit edilerek bilginin özelliğine en uygun önlemlerin alınmasıdır. Ancak ünlü hacker Kevin Mitnick'in "Kırılamayacak site, sızılamayacak ağ yoktur" sözünden de anlaşılacağı üzere tam olarak bilgi güvenliğinden söz etmek mümkün olamamaktadır. Ancak, bu konuda atılacak en önemli adımın

etkin ve verimli bir güvenlik kültürünün oluşturulması, bilgi güvenliğinin temel unsuru olan kişisel verilerin korunması ile ilgili düzenlemelerin yapılması ve küresel bir ağ haline gelen bilgi ve iletişim teknolojilerinde uluslararası işbirliğine önem verilmesinin şart olduğu değerlendirilmektedir.

Tez çalışmasından çıkarılan sonuçların değerlendirilmesi ışığında, ülkemizde bilgi güvenliği konusunda yapılması gerekenler ve Telekomünikasyon Kurumu'nun bu konuda üstlenebileceği sorumluluklar hususunda aşağıdaki tespitler yapılmıştır:

- Bilgi güvenliğini sağlama hususunda oluşturulması gereken "Güvenlik Kültürü"nde

Hükümetin;

Tüm kesimden kullanıcının katılımını sağlayacak bir "Eylem Planı"nı başlatması, bilgi sistemlerinin güvenliği için ulusal politika geliştirmesi ve diğer ülkeler ile işbirliği yapması, eğitimler, broşürler, internet siteleri hazırlaması ve danışma birimleri kurması, konu ile ilgili uluslararası standartları Türk Standardı haline getirmesi ve kullanımını sağlaması, tüm kurumların, özel kuruluşların ve sivil toplum kuruluşlarının işbirliği içinde bulunmasını sağlaması, bilgi güvenliğini sağlayacak yasal düzenlemelerin bir an önce yürürlüğe girmesini sağlaması, bilgi teknolojilerinin gelişimi için araştırma-geliştirmenin devletçe desteklenmesi, bilgi güvenliği ve kişisel mahremiyete yönelik ihlalleri asgari düzeye indirecek cezai önlemlerin alınmasını sağlaması, bilişim suçları ile ilgili birimler kurması, diğer ülkelerde olduğu gibi bilgi güvenliği konusunda kişileri yönlendirebilecek ve olaylara müdahale edebilecek CERT gibi kurumlar

kurması, gereklidir. Ayrıca bu konuda uluslararası işbirliğinin önemli olması nedeniyle diğer ülkelerle işbirliği kurma yoluna gitmesi gereklidir.

Kurum ve kuruluşların;

Kurumun yapısına uygun "Kurumsal Güvenlik Politikası" geliştirmesi, bilgi güvenliği konusunda oluşturulan standartların kullanımına özen göstermesi gereklidir.

Bireysel kullanıcıların;

Bilgi sistem ve ağlarındaki diğer kullanıcılara karşı sorumlu olduklarının bilincinde olması, güncel antivirüs yazılımı ve lisanslı yazılımlar kullanması, İnternette kişisel verilerini nasıl koruyacaklarını bilmesi, bilgasayar ve e-postaları için parola kullanması ve bunları sık sık güncellemesi, güvenmedikleri sitelere girmemesi ve tanımadıkları kişilerden gelen e-postaları açmaması gereklidir.

- Güvenlik kültürü oluşturulmasında her kurum, kuruluş ve bireye sorumluluk düşmesi nedeniyle Telekomünikasyon Kurumu'nun da "Kurumsal Bilgi Güvenliği Politikası" oluşturması, Kurum çalışanlarının elektronik ortamda tutulan ve aktarılan bilginin güvenliğini sağlama hususunda uyması gereken kural ve politikaları belirlemesi gereklidir.

- İSS'lere bilgi güvenliği ihlallerini önleme yetkisi ve yükümlülüğü verilmelidir. İSS'lerin aboneleri ile yaptıkları sözleşmede kendi abonelerinin bilgi güvenliği ihlali yapamayacakları hüküm altına alınmalı ve kendi abonesinin ihlalinden İSS sorumlu tutulabilmelidir.

Ayrıca abonelerinin hazırlamış oldukları İnternet sitelerinde özellikle ticari sitelerde gizlilik politikalarının ne olduğu kişisel bilgilerin niçin istendiği, bilgilerin hangi amaçla kullanılacağı ve bilgilerin güvenliğinin nasıl sağlanacağına ilişkin bilgilerin sunulması sağlanmalıdır. Bununla birlikte siteler "cookie" gönderilip gönderilmediği konusunda kullanıcıyı bilgilendirmeli ve kullanıcıya bunu reddetme imkanı tanınmalıdır.

- Kurumun "Kişisel Verilerin Korunması Kanunu"nun yasallaşmasının ardından kurulacak olan "Kişisel Verileri Koruma Kurumu" ile yakın ilişkide ve istişarelerde bulunarak telekomünikasyon alanında kişisel verilerin korunması hususunda ortak politikalar gerçekleştirmesi gereklidir. Bu gerçekleştirilen politikalar ışığında işletmecilere, abone ve kullanıcılara dair kişisel verilerin korunması konusunda yükümlülükler getirilmelidir.

- Kurum önderliğinde tüm sektör aktörlerinin katılımı ile oluşturulacak ve "Telekomünikasyon Alanında Kişisel Verilerin ve Mahremiyetinin Korunması Komisyonu" olarak adlandırılabilecek bir komisyon sayesinde abone ve kullanıcılar dahil olmak üzere tüm sektör aktörlerinin yapacağı toplantılarda karşılıklı bilgi alış verişi ve istişarelerde bulunarak kişisel verilerin ve mahremiyetin korunmasına yönelik olarak ilgili mevzuatın varsa eksikliklerinin tespiti, usul ve esasların belirlenmesi, mevzuatın nasıl daha iyi ve sağlıklı olarak işletilebileceğinin değerlendirilmesi gereklidir.

- Kurumun diğer ülkelerdeki düzenleyici kurumlarla ikili işbirliği geliştirerek, onların telekomünikasyon alanında kişisel verilerin ve mahremiyetin korunması konusunda yaptıkları tecrübelerden

faydalanması, edindiği izlenim ve tecrübeleri sektöre aktarması oldukça büyük önem arzetmektedir.

- Kurumun, AB mevzuatını uyumlaştırma sürecinde, istek dışı haberleşme konusuna önem vererek bu konuda bir an önce yasal düzenleme çalışmalarına başlaması, bu konuda sorumluluk ve yaptırımları belirlemesi gereklidir. Yapılacak yasal düzenleme ile, abonenin önceden rızası olmadan istek dışı haberleşme yapılmasının önlenmesi, gerçek ve tüzel kişilerin kendi müşterilerine çıkan yeni bir ürün veya hizmet hakkında bilgi vermek amacıyla mesaj gönderebilmesi, ancak mesajın içeriğinde mesajı gönderenin açık bir şekilde belirtilmesi ve alıcının mesajı tekrar almak istememesi durumunda ücretsiz ve kolay bir yolla reddebilme imkanının tanınması, mesajın içeriğinin ahlaka ve kamu düzenine aykırı olmaması, mesaj gönderen kişilerin sahte isim ve şaşırtıcı konu başlığı kullanmalarının önlenmesi, kişinin rızası olmamasına rağmen mesajın zorla gönderilmemesi, ahlaka ve kamu düzenine aykırı olması durumunda cezai müeyyidelerin konulması, pornografik içerikli mesajların gönderimesinin yasaklanması sağlanmalıdır. Bunun yanı sıra, diğer AB üyesi ülkelerde olduğu gibi kapsam içi yöntemin uygulanması gereklidir.

- Kurum bünyesinde veya İSS'ler bünyesinde oluşturulacak kapsam içi veya kapsam dışı yöntem ile elektronik posta yoluyla istek dışı ticari reklam yapacak kişilerin kayıtları tutularak bu tarz reklamları almak istemeyen gerçek kişilerin buraya başvurarak kapsam içi veya kapsam dışı kaydı yaptırmaları sağlanmalı ve kayıtlar sık sık güncellenmelidir. Bu listelerin Kurum İnternet sayfasında yayınlanması istek dışı haberleşmeyi önleme konusunda yardımcı olacaktır. Bunun yanı sıra

istek dışı haberleşme alan kişilerin bunu iletebilecekleri birimler kurulmalıdır.

- Bilgi toplumunun oluşturulması ve yaygınlaştırılmasında en büyük engel olarak görülen istek dışı haberleşmenin artması toplumun hemen hemen tüm kesiminin (İnternet kullanıcıları, kamu sektörü, İSS'ler, hizmet sağlayıcılar) ortak kararlılığı, yapılacak işbirliği ve dayanışmayla oluşturulacak mücadelede başarı sağlayabilecektir. Bu itibarla Kurum diğer ilgili kurum ve kuruluşların işbirliği ile istek dışı haberleşmeyi önleme konusunda görüş, öneri ve politikaların oluşturulacağı forumlar düzenlemelidir.

- Ayrıca, İSS'lere istek dışı mesajları bloke etme yetkisi ve yükümlülüğü verilmelidir. Diğer taraftan İSS'lerin aboneleri ile yaptıkları sözleşmede kendi abonelerinin istek dışı haberleşme gönderemeyecekleri hüküm altına alınmalı ve kendi abonesinin gönderdiği istek dışı mesajdan İSS sorumlu tutulabilmelidir.

- İstek dışı haberleşmenin önlenmesinde uluslararası işbirliğinin önemli olması nedeniyle Kurumun istek dışı haberleşme konusunda uluslararası işbirliğine önem vermesi, diğer ülkelerin konuyla ilgili kuruluşları ile istişarelerde bulunması ve istek dışı haberleşmeyi önleme konusunda ikili işbirliği anlaşmalarını hayata geçirmesi gereklidir.

KAYNAKLAR

[1] Sağıroğlu, Ş., Say, M., Bilgisayar Veri Güvenliği Üzerine Bir İnceleme: Klavye Dinleme Sistemleri, s.1, 2

[2] TSE, 2002, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri ISO/IEC 17799 Standardı, s.1, 14

[3] Levi, A., 2002, Elektronik Posta Güvenliği için PGP Kullanımı I, s.1

[4] Sevgi, L., 2003, Bilgi Güvencesi ve Ulusal Savunma, TMMOB EMO Elektronik Dergisi, 411. sayı

[5] ODTÜ, 2002, Karadere, T., Bilgi Güvenliği, www.security.metu.edu.tr Son erişim tarihi 03.04.2004

[6] Bilişim Güvenlik, 2003, İnternet Güvenliğiyle ilgili Korkunç Hikayeler, s.51, 3. sayı

[7] Bilişim Güvenlik, 2003, Güvenlik Yatırımları, s.55, 2. sayı

[8] http://gsu.linux.org.tr/kripto.tr/tempest.html Son erişim tarihi 15.05.2004

[9] http://web.bilkent.edu.tr/turkce/css/inet-tr-HTML/bolum1.html#20 Son erişim tarihi 15.05.2004

[10] Türkiye Bilişim Şurası, E-Devlet Dönüşüm Sürecinde Bilişim Güvenliği, 2004, www.bilisimsurasi.org.tr/e-turkiye/docs/e-devlet_donusum_surecinde_bilisim_guvenligi.doc Son erişim tarihi 17.05.2004

[11] Çağıltay, K., 1997, İnternet, METU, s.5

[12] Yıldırımoğlu, M., Internet Information Server

[13] TBD, 2002, Bilişim Şurası Hukuk Çalışma Grubu Raporu http://bilisimsurasi.org.tr/home.php?golink=rapor Son erişim tarihi 24.04.2004

[14] Mernisin Hukuki İncelemesi, Av. M. Gökhan Ahi, www.hukukcu.com/bilimsel/kitaplar/mernis.htm Son erişim tarihi 27.04.2004

[15] Başalp, N., 2004, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, s. 92, 16, 34,38

[16] www.ak-kurt.com/emailguvenlik.html#1 Son erişim tarihi 02.05.2004

[17] OECD, DSTI/CP/ICCP(2004)1, 11 Mart 2004, s. 8,12

[18] www.spam.org.tr/nedir.html Son erişim tarihi 02.05.2004

[19] ITU, 2004, Countering Spam, Switzerland, s.16, 25, 34, 95, 97

[20] EC, Paul Rutherford, IT Security s.84

[21] OECD, 2004 DSTI/ICCP/REG(2003)8/FINAL, s. 2

[22] OECD, 2003, DSTI/ICCP/REG(2002)5/FINAL, s.7

[23] OECD, 2003, Privacy Online, France, s.7, 11, 25, 27, 48, 114

[24] OECD, 2004, DSTI/ICCP(2003)10/FINAL, s. 4

[25] OECD, 2004, DSTI/CP/ICCP(2004)1, s.8

[26] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personel Data www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html Son erişim tarihi 06.05.2004

[27] OECD, 2002, OECD Guidelines for the Security of Information Systems and Networks:Towards a Culture of Security www.oecd.org/topic/0,2686,en_2649_34255_1_1_1_1_37409,00.html Son erişim tarihi 29.04.2004

[28] AB, 95/46/EC sayılı Direktif

[29] www.export.gov/safeharbor/sh_overview.html Son erişim tarihi 08.07.2004

[30] EU, 2003, First Report on the Implementation of the Data Protection Directive, Brussels, s.13

[31] www.privacyknowledgebase.com/document.jsp?docid=REFDPEUR Son erişim tarihi 21.04.2004

[32] EU, 7. Implementation Report, http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/previousyears/index_en.htm

[33] AB, 2002/58/EC Sayılı Direktif

[34] EU, 8. Implementation Report, http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/previousyears/index_en.htm

[35] AB, 97/66/EC Sayılı Direktif

[36] AB, 2001/45/EC Sayılı Tüzük

[37] AB, 92/242/EC Sayılı Konsey Kararı

[38] AB, 2256/2003/EC Sayılı Konsey Kararı

[39] http://europa.eu.int/information_society/eeurope/2002/news_library/documents/nisa_en.pdf Son erişim tarihi 23.07.2004

[40] AB, 2004/460/EC Sayılı Direktif

[41] ITU, 2004, Security in Telecommunications and Information Technology

[42] ITU, 2003, Document WSIS-03/GENEVA/DOC/4-E, s.12

[43] ITU, 2003, Document WSIS-03/GENEVA/DOC/5-E, s.8

[44] ITU, 2002, Creating Trust in Critical Network Infrastructures

[45] http://www.itu.int/osg/spu/spam/index.phtml Son erişim tarihi 27.05.2004

[46] ITU News, June 2004, Spam: A Threat to the Information Society, s.5

[47] OECD, 2004, Online Services and Data Protection and Privacy, s.152

[48] Implementing a Culture of Security in Australia, http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase Son erişim tarihi 19.06.2004

[49] http://www.stradigma.com/turkce/kasim2003/makale_08.html son erişim tarihi 16.08.2004

[50] Hukuki Açıdan Kitlelere E-Posta Gönderilmesi, Doç. Dr. Tekin Memiş www.hukukcu.com/bilimsel/kitaplar/spamming.htm Son erişim tarihi 15.06.2004

[51] Positioning technology Relevant Regulations of USA, Japan, Germany and Italy, www.vtt.fi/virtual/navi/cd/International_Regulations.pdf Son erişim tarihi 12.08.2004

[52] http://www.spamlaws.com/federal/108s877.html Son erişim tarihi 22.09.2004

[53] http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm Son erişim tarihi 27.09.2004

[54] Windows 2000 Magazine, 2000, IT Security

[55] EU, Existing case law on compliance with Data Protection Laws and Principles in the Member States of the Europen Union, 1998, Belgium

[56] EC, Data Protection in the European Union, 2000, Luxembourg

[57] DPT, 2001, 8. Beş Yıllık Kalkınma Planı, Bilişim Teknolojileri ve Politikaları Özel İhtisas Komisyonu Raporu

[58] 9. Implementation Report, http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/previousyears/index_en.htm

[59] 10. Implementation Report http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/index_en.htm Son erişim tarihi 10.09.2004

[60] http://www.izmirbarosu.org.tr/mevzuat/tasari_ubg.htm Son erişim tarihi 01.09.2004

[61] EU, Implementation of the Directive on Privacy and Electronic Communications Goverment's Response to Consultation 18 September 2003, htttp://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html#consult

[62] EU, Protection of Information Handled in Information Technology and Communication System, 2001

[63] EU, Council Framework Decision on attacks against information systems, 2002, Brussels

[64] DTI, Implementation of the Directive on Privacy and Electronic Communications, 2003

[65] EU, Data Protection, http://europa.eu.int/comm/internal_market/en/dataprot/links.htm

[66] EU, Communication from the Commission to the European Patliament, the Council, the European Economic and Social Committee and the Committee of the on Unsolicited Commercial Communications or 'Spam',2004

[67] http://www.the-dma.org/antispam/spamlaws.shtml

[68] OECD, Guidance on Policy and Practice

[69] http://europa.eu.int/information_society/eeurope/2002/news_library/documents

[70] PC Magazine, 2003, Stop the Spam s. 10

[71] www.privacy.org/pi/survey/dpmap.jpg Son erişim tarihi 12.09.2004

[72] Telekom Dünyası, Sağıroğlu Ş, Say, M., Alkan M., 2004, Bilgisayar Sistemlerinde Güvenlik, s.48

[73] TK, 2004, 2004 Yılı Faaliyet Raporu s.15, s.20

[74] TK, Saygı, N., 2002, Telekomünikasyon ve Bilgi Teknolojileri Pazarı Mevcut Durum ve 10 Yıllık Bir Perspektif Çalışması, Uzmanlık Tezi, Ankara, s.45,46

[75] Türk Telekom, Erdağ, V., Bilgi Güvenlinliği:Kavramlar ve Yaklaşımlar, S. 2004/1 s. 42

[76] TK, Decdeli N., 2004, Kablo TV Şebekesi Üzerinden Verilecek İnternet Servisinde Çoklu İnternet Servis Sağlayıcı Uygulamaları: Mevcut Düzenlemeler ve Türkiye Önerileri, Uzmanlık Tezi, Ankara, s.113

[77] Cevat Özel, Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı www.hukukcu.com/bilimsel/kitaplar/bilisimsuclari_TCKtasarisi.htm Son erişim tarihi 27.07.2004

[78] www.uekae.tubitak.gov.tr Son erişim tarihi 17.08.2004

[79] EU, Regular Report on Turkey's Progress Towards Accession, Brussel 2002, s.106

[80] EU, Regular Report on Turkey's Progress Towards Accession, Brussel 2003, s. 67

[81] www.hukukcu.com/bilimsel/kitaplar/bilisimsuclari_TCKtasarisi.htm Son erişim tarihi 30.07.2004

[82] Bilişim Teknolojisi Hukuku Gündemi, Başalp, N., 2003-2004 Veri Koruması http://bthukuku.bilgi.edu.tr/tr/02_calisma_alanlari/02_2_veri_korumasi/02_2_1_tanim/index.asp Son erişim tarihi 17.05.2004

[83] AB, Kişisel Verilerin Korunması Kanunu

http://bthukuku.bilgi.edu.tr/tr/02_calisma_alanlari/02_2_veri_korumasi/02_2_2_ulusal_mevzuat/kisisel_verilerin_korunmasi_kanunu.doc son erişim tarihi 07.08.2004

[84] 4. Hukuk Raporu, www.bilisimsurasi.org.tr/raporlar/yeni Son erişim tarihi 24.08.2004

[85] Kişisel Verilerin Korunması ve Gizliliği http://eticaret.garanti.com.tr/icerik/goster.asp?c=4&t=a&i=0311200117 39551023201084705 Son erişim tarihi 2.08.2004

[86] TBD, Av. Beceni, Y., 2004, Hukuk Çalışma Grubu, Siber Uzayda Mahremiyet, http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf

[87] TK, Özenç, K., 2001, Avrupa Birliği'nde Telekomünikasyon Politikaları, AB Müktesebatı ve Türkiye Tarafından Alınması Gereken Önlemler Uzmanlık Tezi

[88] ABGS, 2003, AB Müktesebatının Üstlenilmesine ilişkin Ulusal Program, s.559, 560, 561

[89] TK, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

[90] Doç. Dr. Tekin Memiş, Hukuki Açıdan Kitlelere E-posta Gönderilmesi www.hukukcu.com/bilimsel/kitaplar/spamming.htm

[91] www.kurul.ubak.gov.tr

[92] TK, 2004, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/Kisisel_Bil_Yon_06_02_04.pdf

[93] Sırabaşı, V., 2003, Radyo Televizyon Aracılığıyla Kişilik Haklarına Tecavüz, Adalet Yayınevi, Ankara, s. 45

[94] Telepati Telekom, Mayıs 2004

[95] Açık Ağlarda Bilgi Güvenliği ve Dünyadaki Eğilimler, http://e-kimlik.bilten.metu.edu.tr/net/yayinlar/aabg.jsp

[96] Gelişmişliğin Vazgeçilmez Unsuru: Ulusal Bilgi Politikası, Mustafa SAĞSAN http://strateji.cu.edu.tr/BILGI/01.asp Son erişim tarihi 29.08.2004

[97] TK, 2001, İnternet Düzenlemeleri, Veri Gizliliği, Güvenliği, Kurumumuzun Görev ve Fonksiyonları, SİD

[98] Kandur, H., 2003, Sınır Ötesi Bilgi Akışı ve Ulusal Bilgi Politikaları www.archimac.org/JAS/JAS2001/JAS03_01.spml Son erişim tarihi 03.05.2004

[99] E-Europe+ 2003, E-Avrupa Eylem Planı Avrupa'da Bilgi Toplumunun Oluşturulması için Ortak Girişim Haziran 2001

[100] www.hukukcu.com/bilimsel/kitaplar/bilisimsuclari_TCKtasarisi.htm Son erişim tarihi 27.07.2004

EK-I

T.C.
B A Ş B A K A N L I K
Personel ve Prensipler Genel Müdürlüğü

Sayı: B.02.0.PPG.0.12-320-2789 17 ŞUBAT 2003
Konu : Bilgi Sistem ve Ağları İçin Güvenlik Kültürü

GENELGE
2003/10

Bilgi sistem ve ağlarına yönelik tehditler ve riskler ile mücadele için uluslararası koordinasyon ve işbirliğini geliştirmek amacıyla Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 1992 yılında yayımlanan ve 1997 yılında güncelleştirilen "Rehber İlkeler"in, bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim karşısında yeniden gözden geçirilmesi ihtiyacı doğmuş, Amerika Birleşik Devletlerinde yaşanan 11 Eylül 2001 olayları ise, bu ihtiyacı daha da acil kılmıştır.

Üyesi bulunduğumuz OECD'nin Bilişim, Bilgisayar ve İletişim Politikaları Komitesi'ne (ICCP) bağlı Bilginin Güvenliği ve Kişisel Gizliliği Çalışma Grubunca, bilgi ve iletişim teknolojileriyle yapılan haberleşme ve bilgi alışverişlerinde güvenliği ve kişisel mahremiyeti sağlamak amacıyla yürütülen çalışmalar tamamlanmış ve hazırlanan yeni rehber ilkeler OECD Konseyi tarafından onaylanmıştır.

Dünya çapında bilgi ve iletişim ağlarını kullanan hükümetler, iş çevreleri ve bireyler arasında, haberleşme özgürlüğü ve mahremiyet gibi demokratik toplum değerleri ile bağdaşık "Güvenlik Kültürü"nü oluşturmayı amaçlayan ve OECD üyesi ülkelerin ortak tutumunu yansıtmakta bulunan söz konusu Rehber İlkeler, iş dünyası ve sivil toplum örgütlerinin de desteğini

taşımaktadır.

Rehber İlkelerin üye ülkeler için resmi bir bağlayıcılığı bulunmamakla birlikte, ulusal sınırları aşan ve birbirlerine karşı bağımlılığı artan bilgi sistem ve ağlarına yönelik tehditler karşısında, her düzeydeki kullanıcılar tarafından benimsenip uygulanması yararlı olacaktır.

Bu itibarla, öncelikle ve başta kamu kurum ve kuruluşları olmak üzere, bilgi sistem ve ağlarının korunması için yürütülen çalışmalarda, Türkçe çevirisi ekte yer alan Rehber İlkelerin göz önünde bulundurulmasını rica ederim.

Abdullah GÜL
Başbakan

BİLGİ SİSTEMLERİNİN GÜVENLİĞİNE İLİŞKİN OECD REHBER İLKELERİ
GÜVENLİK KÜLTÜRÜNE DOĞRU

14 Aralık 1960 tarihli Ekonomik İşbirliği ve Kalkınma Teşkilatı Anlaşmasının, özellikle 1b), 1 c), 3 a) ve 5 b) maddeleri uyarınca;

23 Eylül 1980 tarihli Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkelerine yönelik Konsey Önerisi uyarınca;

11 Nisan 1985 tarihinde OECD Üye ülke hükümetlerince kabul edilen Sınır Ötesi Veri Akışı Bildirisi uyarınca [Ek C(85)139];

27 Mart 1997 tarihli Kriptografi Politikası Rehber İlkelerine İlişkin Konsey Önerisi uyarınca [C(97)62/FINAL];

7-9 Aralık 1998 tarihli Küresel Ağlarda Mahremiyetin Korunmasına İlişkin Bakanlar Konseyi Bildirisi uyarınca [Ek C(98)177/FINAL];

7-9 Aralık 1998 tarihli Elektronik Ticaretin Doğrulanmasına İlişkin Bakanlar Konseyi Bildirisi uyarınca[Ek C(98)177/FINAL];

Bilgi sistem ve ağlarının, hükümetler, iş çevreleri, kuruluşlar ve bireysel kullanıcılar tarafından kullanımının ve değerinin giderek arttığını;

Bilgi sistem ve ağlarının ve ulusal ekonomilerin, uluslararası ticaretin ve sosyal, kültürel ve siyasi yaşamın dengeli ve verimli işleyişi açısından giderek daha fazla önem kazanması nedeniyle söz konusu bilgi sistem ve ağların güvenilirliğinin korunması ve kuvvetlendirilmesi ihtiyacını;

Bilgi sistem ve ağlarının dünya çapında kullanımının beraberinde yeni ve artan oranda riskler getirdiğini;

Yetkisiz erişim ve kullanım, kötü kullanım, değiştirilme, kötü amaçlı kod iletimleri, hizmetteki aksaklık ya da tahribatlar karşısında bilgi sistem ve ağları aracılığıyla iletilen ve kaydedilen veri ve bilgilerin tehdit altında olduğu ve uygun korunma yöntemlerine ihtiyaç duyulduğunu;

Bilgi sistem ve ağlarına yönelik riskler ve bu risklerle ilgili politikalar, uygulamalar, önlemler ve prosedürler hakkında bilincin artması gerektiği ve bir güvenlik kültürünü geliştirmek için uygun tutum ve davranışların teşvik edilmesi gereksinimini;

Bilgi sistem ve ağlarına yönelik tehditlerden doğan zorluklara karşı hazırlıklı olmak için mevcut politika, uygulama, önlem ve prosedürlerin gözden geçirilmeleri gereksinimini;

Güvenlik eksiklikleri sebebiyle ulusal ekonomilerin, uluslararası ticaretin, sosyal, kültürel ve siyasi yaşamdaki katılımın karşı karşıya olduğu potansiyel hasarların yarattığı zorluklarla mücadele etmek için uluslararası eşgüdüm ve işbirliğini kuvvetlendiren bir güvenlik kültürü aracılığıyla bilgi sistem ve ağlarının güvenliğini teşvik etmenin ortak çıkarların gereği olacağını;

Bu Öneri Ekinde yer alan *Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkelerin* ulusların egemenlik haklarını etkilemediği ve isteğe bağlı olduğunu;

Rehber İlkelerin amacının güvenlik hususunda tek ve kesin bir çözüm ileri sürmek ya da belli bir durumda hangi politika, uygulama, önlem ve prosedürlerin uygun olduğu hususunda net bir açıklama getirmek olmadığı, daha ziyade kullanıcıların bir güvenlik kültürünü nasıl oluşturacağı ve aynı zamanda ondan nasıl yararlanacağı konusunda daha iyi bir anlayış yerleştirmek üzere çerçeve ilkeler sunmak olduğunu göz önüne alarak;

Konsey,

Bilgi sistem ve ağlarını geliştiren, sahip olan, yöneten, hizmete sunan ve kullanan hükümetler, iş çevreleri, diğer örgütler ve bireysel kullanıcılar için *Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeler: Güvenlik Kültürüne Doğru* adlı ilkeleri önermektedir.

Üye ülkelerin;

Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeler: Güvenlik Kültürüne Doğru adlı ilkeler uyarınca bir güvenlik kültürünü benimseyerek ve teşvik ederek mevcut politika, uygulama, önlem ya da prosedürlerini değiştirmelerini ya da yenilerini oluşturmalarını;

Rehber İlkeleri uygulamak için ulusal ve uluslararası düzeyde işbirliği yapmalarını, koordinasyon sağlamalarını;

Güvenlik kültürünü teşvik etmek ve tüm kullanıcıları sorumluluk alarak Rehber İlkelerini kendilerine düşen rollere uygun bir şekilde uygulamak amacıyla gerekli adımları atmaya teşvik etmek için Rehber İlkelerini hükümetler, iş çevreleri, diğer örgütler ve bireysel kullanıcılar da dahil olmak üzere tüm kamu ve özel sektöre dağıtmalarını;

Üye olmayan ülkelere zamanında ve uygun bir şekilde Rehber İlkeleri tanıtmalarını;

Bilgi sistem ve ağlarının güvenliği ile ilgili konularda uluslararası işbirliğini kuvvetlendirmek için her beş yılda bir Rehber İlkeleri gözden geçirmelerini tavsiye etmektedir.

OECD Bilişim, Bilgisayar ve İletişim Politikası Komitesini Rehber İlkelerin uygulanmasını teşvik etmekle görevlendirmektedir.

Bu Öneri, Bilgi Sistemlerinin Güvenliği için Rehber İlkeler başlıklı 26 Kasım 1992 tarihli Önerinin [C(92)188/FINAL] yerine geçmektedir.

BİLGİ SİSTEMLERİNİN GÜVENLİĞİNE İLİŞKİN OECD REHBER İLKELERİ- GÜVENLİK KÜLTÜRÜNE DOĞRU

ÖNSÖZ

1) *Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkelerin* ilk kez 1992'de OECD tarafından yayınlanmasından günümüze kadar, bilgi sistemleri ve ağlarının kullanılması ve tüm bilgi teknolojileri büyük ölçüde değişime uğramıştır. Devam edegelen bu değişiklikler önemli avantajlar sunmakla birlikte, aynı zamanda bilgi sistemlerini ve ağlarını kullanan, geliştiren, sahip olan, yöneten, sağlayan, sunan ve kullanan hükümetler, iş çevreleri, diğer örgütler ve bireylerin ("kullanıcılar") güvenlik hususuna daha fazla dikkat etmelerini gerektirmektedir.
2) Daha güçlü kişisel bilgisayarlar, ilerleyen teknolojiler ve İnternetin geniş kapsamlı kullanımı, kapalı ağlardaki basit ve tek başına işletilen sistemlerin yerini almıştır. Günümüzde, kullanıcılar giderek artan oranda birbirine bağlanmakta ve bu bağlantılar ulusal sınırları aşmaktadır. Ayrıca İnternet enerji, ulaştırma ve finans gibi önemli altyapıları da desteklemekte olup, şirketlerin işleyişinde, hükümetlerin vatandaşlara ve teşebbüslere sundukları hizmetlerde ve bireylerin iletişim ve bilgi alışverişinde önemli bir rol oynamaktadır. İletişim ve bilgi altyapısını oluşturan teknolojilerin yapısı ve çeşidi de oldukça değişmiştir. Altyapı erişim araçlarının sayısı ve yapısı sabit, kablosuz ve mobil araçları kapsayacak şekilde çoğalmıştır. Erişim, artık artan bir oranda sürekli çevrimiçi olan bağlantılar aracılığıyla yapılmaktadır. Sonuç olarak bilgi alışverişinin doğası, hacmi ve hassasiyeti büyük ölçüde artmıştır.

3) Bilgi sistemleri ve ağlarının birbirleri ile bağlantısındaki artışın sonucu olarak, bilgi sistemleri ve ağlarının güvenliği artık artan sayıda ve çeşitlilikte tehditlere maruzdur. Bu durum güvenlik açısından yeni konuları gündeme getirmektedir. Bu nedenlerle, bu Rehber İlkeler, yeni bilgi toplumunda yer alan tüm kullanıcılara yöneliktir ve güvenlik konularını daha bilinçli olarak ele alınmasının ve bir "güvenlik kültürü"nü geliştirmenin gereğini vurgulamaktadır.

I. GÜVENLİK KÜLTÜRÜNE DOĞRU

4) Bu Rehber İlkeler, sürekli değişen güvenlik ortamına güvenlik kültürünün geliştirilmesini teşvik etmek suretiyle cevap vermektedir. Bilgi sistem ve ağlarının geliştirilmesinde güvenlik hususuna dikkat edilmesini ve bilgi sistem ve ağlarını kullanırken yeni düşünme ve davranış yöntemlerinin benimsenmesini önermektedir. Rehber İlkeler, sistem ve ağların güvenliğinin tasarımını ve kullanımını genelde daha sonra ele alan eski yöntemi geride bırakmaktadır. Kullanıcının, bilgi sistemleri, ağlar ve ilgili hizmetlere daha bağımlı hale gelmesinden dolayı bu sistemlerin güvenli olması gerekmektedir. Sadece tüm kullanıcıların çıkarları ile sistem, ağ ve ilgili hizmetlerin doğasını göz önünde bulunduran bir yaklaşım etkili bir güvenlik sağlayabilir.

5) Güvenliği sağlamak açısından her kullanıcı önemli bir unsurdur. Kullanıcılar, rolleri gereği karşı karşıya oldukları güvenlik riskleri ve önleyici tedbirlerden haberdar olmalı, sorumluluk almalı ve bilgi sistem ve ağlarının güvenliğini artırmak için gerekli adımları atmalıdır.

6) Güvenlik kültürünün geliştirilmesi hem liderlik hem de geniş kapsamlı bir katılım gerektirmekte, bu da, tüm kullanıcılar arasında güvenliğin sağlanması konusundaki anlayış kadar, güvenlik planlaması ve yönetimine de öncelik tanınması sonucunu doğurmaktadır. İdarenin tüm seviyeleri, iş çevreleri ve tüm kullanıcılar, güvenlik konularında

sorumluluk almalıdır. Bu Rehber İlkeler, toplum aracılığıyla bir güvenlik kültürü oluşturmak için gerekli temeli sağlamaktadır. Böylelikle kullanıcılar, güvenlik unsurunu bilgi sistemleri ve ağlarının kullanımı ve tasarımına dahil edebilirler. Rehber İlkeler, tüm kullanıcıların, bilgi sistem ve ağlarıyla ilgili işlemlerde güvenlik kültürünü bir düşünce, değerlendirme ve faaliyet yöntemi olarak benimsemesini ve teşvik etmesini önermektedir.

II. AMAÇLAR

7. Bu Rehber İlkeler;

- Bilgi sistem ve ağlarının koruma aracı olarak tüm kullanıcılar arasında güvenlik kültürünü teşvik etmeyi,

- Bilgi sistemleri ve ağlarının karşı karşıya olduğu riskler ve bu risklere karşı mevcut politikalar, uygulamalar, önlemler ve prosedürlerle ilgili bilinci arttırmak ve bu yöntemlerin uygulanmasının gerekliliğini vurgulamayı,

- Bilgi sistemleri ve ağları ile bunların sunum ve kullanım yöntemleri konusunda tüm kullanıcıların güvenini artırmayı,

- Bilgi sistemlerinin ve ağlarının güvenliğine yönelik uyumlu politika, uygulama, önlem ve prosedürlerin geliştirilmesi ve uygulanması ile ilgili etik değerlere kullanıcılar tarafından saygı gösterilmesi ve güvenlik konularının iyi anlaşılmasına yardımcı olacak genel bir referans çerçevesi oluşturulmasını,

- Güvenlik politikalarının, uygulamalarının, tedbir ve prosedürlerinin geliştirilmesi ve uygulanması açısından tüm kullanıcılar arasında işbirliği ve bilgi paylaşımını teşvik etmeyi,

- Standartların geliştirilmesi ve uygulanmasında rol alan tüm kullanıcıların güvenlik konusunu önemli bir hedef olarak belirlemelerini teşvik etmeyi amaçlamaktadır.

III.İLKELER

8. Aşağıda sayılan dokuz ilke birbirini tamamlayıcı nitelikte olup, bir bütün olarak okunmalıdır. İlkeler, politika ve uygulama seviyeleri de dahil olmak üzere tüm kullanıcıları ilgilendirmektedir. Bu Rehber İlkeler çerçevesinde kullanıcıların sorumlulukları rollerine göre değişiklik göstermektedir. Daha sağlam bir güvenlik anlayışının yerleşmesi ve uygulamaların benimsenmesi için eğitim, bilgi paylaşımı ve öğretim sayesinde tüm kullanıcılara yardımcı olunacaktır. Bilgi sistemleri ve ağlarının güvenliğini artırma çabaları, demokratik toplum değerleri ile, özellikle de kişisel mahremiyet ile ilgili temel konular ve bilginin açık ve serbest akışı gereksinimi ile uyumlu olmalıdır.

1) Bilinç

Kullanıcılar, bilgi sistemleri ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabilecekleri konularında bilinçli olmalıdır.

Bilgi sistemleri ve ağlarının güvenliği açısından, riskler ve mevcut korunma yöntemleri konularındaki bilinç ilk savunma adımını oluşturmaktadır. Bilgi sistem ve ağları hem iç hem de dış risklerden etkilenebilir. Kullanıcılar güvenlik konusundaki eksikliklerin kontrolleri altındaki sistem ve ağlara büyük ölçüde zarar verebileceğini bilmeli, birbirine bağlı ve bağımlı olan sistemler nedeniyle diğer kullanıcılara da zarar verebileceklerini unutmamalıdırlar. Kullanıcılar, sistemlerinin konfigürasyonu, güncelleştirilmesi ve ağ içindeki yeri ile güvenliği artırmak için uygulayabilecekleri iyi örnekler ve diğer kullanıcıların gereksinimleri konularında bilgi sahibi olmalıdır.

2) Sorumluluk

Tüm kullanıcılar bilgi sistem ve ağlarının güvenliğinden sorumludur.

Yerel ve küresel bilgi sistemlerine ve ağlarına bağlı olan kullanıcılar, sistem ve ağların güvenliği hususunda kendilerine düşen sorumlulukların farkında olmalıdır. Kendilerine düşen rollere uygun bir şekilde davranmalıdırlar. Kullanıcılar kendi politika, uygulama, önlem ve prosedürlerini düzenli olarak incelemeli ve uygun olup olmadıklarını değerlendirmelidir. Ürün ve hizmet sağlayan, geliştiren ve tasarlayan kullanıcılar, kullanıcıların ürün ve hizmetlerin güvenlik fonksiyonlarını daha iyi anlayabilmeleri ve bu konuda kendi sorumluluklarının bilincine varabilmeleri için sistem ve ağ güvenliği konusunu dikkate almalı ve güncelleme dahil gerekli bilgileri sunmalıdır.

3) Tepki

Kullanıcılar, güvenlik tehditlerini önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmelidir.

Kullanıcılar, bilgi sistem ve ağlarının birbirlerine bağlı olan yapısı ve potansiyel hasarların hızla ve geniş kapsamda yayılabileceğini göz önüne alarak, güvenlikle ilgili tehditler karşısında işbirliği içinde olmalı ve zamanında müdahale etmeli; tehdit ve zayıf noktalar konusundaki bilgileri mümkün olduğunca paylaşmalı, güvenlik tehditlerini önlemek, saptamak ve müdahale etmek amacıyla hızlı ve etkili bir işbirliği sağlamak için gerekli prosedürleri uygulamalıdırlar. İzin verildiği durumlarda sınır aşan bilgi paylaşımı ve işbirliği de buna dahil edilebilir.

4) **Etik**

Kullanıcılar birbirlerinin yasal çıkarlarına saygı göstermelidir.

Bilgi sistem ve ağlarının toplumumuzda ne kadar hızlı yaygınlaştığı düşünülürse, kullanıcıların eylemlerinin veya tepkisizliklerinin diğerlerine zarar verebileceğini bilmeleri gerekmektedir. Bu sebeple ahlaki davranışlar çok önemli olup; kullanıcılar en iyi uygulamaları geliştirmeye ve benimsemeye özen göstermeli, güvenlik ihtiyaçlarını göz önünde bulunduran davranışları teşvik ederek, diğer tarafların çıkarlarına saygı göstermelidir.

5) Demokrasi

Bilgi sistem ve ağlarının güvenliği, demokratik toplumun temel değerleri ile uyumlu olmalıdır.

Güvenlik uygulamaları, düşünce ve ifade özgürlüğü, bilginin serbest akışı, bilgi ve iletişimin güvenilirliği, kişisel bilginin korunması, açıklık ve şeffaflık gibi demokratik toplumlardaki değerler ile uyumlu bir şekilde yürütülmelidir.

6) Risk değerlendirmesi

Kullanıcılar risk değerlendirmeleri yapmalıdır.

Tehdit ve hassasiyetleri tanımlayan risk değerlendirmeleri, teknoloji, fiziksel ve insani etkenler, politikalar ve üçüncü taraf hizmetleri gibi önemli iç ve dış faktörleri kapsayacak şekilde geniş bir tabana teşmil edilmelidir. Risk değerlendirmeleri kabul edilebilir risk seviyesinin belirlenmesini sağlar ve korunması gereken bilginin yapısı ve önemi doğrultusunda, bilgi sistem ve ağlarının karşı karşıya olduğu potansiyel zarar risklerini yönetmek için gerekli kontrollerin seçilmesine yardımcı olur. Bilgi sistemlerinin giderek daha bağlı bir hale gelmeleri nedeniyle risk değerlendirmeleri, diğer kullanıcılardan

kaynaklanan ya da onları etkileyebilecek potansiyel hasarları da göz önüne almalıdır.

7) Güvenlik tasarımı ve uygulama

Kullanıcılar, güvenliği, bilgi sistem ve ağlarının önemli bir unsuru olarak ele almalıdır.

Güvenliği optimum kılmak için sistemler, ağlar ve politikalar uygun şekilde tasarlanmalı, uygulanmalı ve koordine edilmelidir. Bu çabaların önemli bir parçası da, tanımlanmış tehdit ve hassasiyetlerden kaynaklanabilecek potansiyel hasarları engellemek ya da en aza indirmek için uygun korunma yöntemleri ve çözümlerinin tasarlanması ve benimsenmesidir. Hem teknik hem de teknik olmayan korunma yöntemleri ve çözümleri gerekmekte olup, bunlar, organizasyonun sistem ve ağlarında bulunan bilginin değeri ile orantılı olmalıdır. Güvenlik, ürün, hizmet, sistem ve ağların temel bir unsuru olmalı ve sistem tasarımı ve mimarisinin bölünmez bir parçası haline gelmelidir. Uç kullanıcılar için güvenlik tasarımı ve uygulanışı genelde kendi sistemleri için ürün ve hizmetleri seçmek ve yapılandırmak anlamına gelmektedir.

8) Güvenlik Yönetimi

Kullanıcılar güvenlik yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.

Güvenlik yönetimi, risk değerlendirmesine dayalı ve kullanıcıların tüm faaliyet düzeylerini ve işlemlerinin her safhasını kapsayacak şekilde dinamik olmalıdır. Yeni tehditlere karşı ileri görüşlü çözümler içermeli, sistem onarımı, bakım, inceleme ve arızalara karşı önlem, saptama ve müdahale gibi konulara dikkat etmelidir. Bilgi sistem ve ağ güvenlik politikaları, uygulamaları, önlemleri ve prosedürleri tutarlı bir güvenlik sistemi oluşturmak için koordine

edilmeli ve bütünleştirilmelidir. Güvenlik yönetimi gereksinimleri, katılım seviyesine, kullanıcının rolüne, riske ve sistem gereksinimlerine bağlıdır.

9) Yeniden değerlendirme

Kullanıcılar bilgi sistem ve ağlarının güvenliklerini incelemeli ve yeniden değerlendirmeli; güvenlik ile ilgili politika, uygulama, önlem ve prosedürlerde gerekli değişiklikleri yapmalıdır.

Sürekli olarak yeni ve değişen tehdit ve hassasiyetler ortaya çıkmaktadır. Kullanıcılar, değişen bu riskler ile mücadele etmek için güvenliğin tüm unsurlarını devamlı olarak incelemeli, yeniden değerlendirmeli ve değiştirmelidir.

ÖZGEÇMİŞ

1970 yılında Kırşehir'de doğdu. İlk, orta ve lise eğitimini Kırşehir'de tamamladı. 1990 yılında H.Ü. Fen Fakültesi Matematik Bölümünden mezun oldu. 1991 yılında Telsiz Genel Müdürlüğü'nde göreve başladı. Halen Telekomünikasyon Kurumu Uluslararası İlişkiler ve AB ile Koordinasyon Dairesi Başkanlığında görev yapmaktadır. Evli ve iki çocuk annesidir.