Uluslararası Ülke Güvenliğinde Hukuki ve Teknik Yaklaşım

Köksal ÖZENÇ,Mustafa ALKAN, Tayfun ACARER

Abstract- **And the risks against the security of the information and data because of our today's developing technology increase too. The certain sources say that the market on the software programs for the internet security was about USD 4,4 bn as for the last of 1999 and also this figure amounts to USD 8,3 bn with an increase of % 23 on average per year. Furthermore while the overheads done for information security in the information and communication technologies which has great importance for EU were USD 465 million, this amount increased up to USD 2,74 bn in 2006. Because Euro 1,4 bn in the term of 2007/2013 has been assigned for the R&D projects in the field of information security technologies within the context of the 7th Framework Program which has a budget of Euro 5,3 bn. [1]**

In deed while the market share of security software was USD 8,2 bn in 2006, it has been estimated that this share will be USD 9,1 bn in 2007 and the share for antivirus software USD 4,9 bn with the increasing of 54% in 2007. Therefore it has been understood that the financial burden to be realized for the information security is how much important taking into account this issue.

Keywords—**Information security, Echelon, CETS, TEMPEST**

I. GİRİŞ

Bilindiği üzere günümüzün gerek gelişen ve gerekse de birbirine yakınsayan teknolojileri sayesinde ses, data ve görüntü olmak üzere her türlü bilgi ve verilerin hızlı bir şekilde iletilmesi, alınması ve işlenmesi büyük ölçüde hayatımızı kolaylaştırmakla beraber bilgi ve iletişim teknolojilerinde "bilgi güvenliği" gibi oldukça önemli bir hususu da gündeme getirmektedir. Zira, bilgi ve iletişim teknolojilerinin toplum bazında yaygınlaştırılması, sadece etkin ve verimli kullanımına değil aynı zamanda sözkonusu teknolojilerde kullanılan tüm cihaz, ekipman ve sistemlerde bilgi güvenliğinin de tam olarak sağlanmasına bağlıdır.

Bilgi toplumu hedefine ulaşılması ve elektronik imzaya dayalı elektronik devlet ve elektronik ticaret uygulamalarının yaygınlaşması, bilgi ve iletişim teknolojilerinde güvenli bir ortamın, açık ağlarda dolaşan bilginin güvenliğinin ve kişisel verilerin gizliliğinin sağlanması ile mümkün olmaktadır. Bu nedenle, taraflararası iletilerde bilginin gizliliği, bütünlüğü ve her istenilen anda erişilebilirliğinin sağlanması için teknik ve hukuki önlemlerin alınması büyük önem arzetmektedir.

Bilgi Teknolojileri ve İletişim Kurumu,
kozenc@tk.gov.tr, malkan@tk.gov.tr, tacarer@tk.gov.tr

Çok çeşitli sayıda bilgi ve iletişim teknolojilerinin günümüzde hızla artan bir oranda kullanılır hale gelmesi ekonomik ve sosyal hayatta karşılaşılan pek çok işlemleri kolaylaştırdığı ölçüde bilgi güvenliğine karşı çeşitli boyutlarda risk ve tehditleri de beraberinde getirebilmektedir. Zira yabancı ülkelerde olduğu gibi ülkemizde de bilgisayar ve mobil iletişim teknoloji cihaz ve sistemlerini kullanan kişiler çoğunlukla bilgi güvenliğine karşı oluşabilecek risk ve tehditlerin farkında değildir. Oluşan bu risk ve tehditler, kişilerin çoğunlukla maddi kayba uğramalarına ya da bilgilerinin değiştirilmesi, silinmesi ya da izinsiz olarak erişilmesi gibi istenmeyen bazı durumlara neden olabilmektedir.

II. BİLGİ GÜVENLİĞİNİN EKONOMİK BOYUTU

1995 yılında sadece 20.000 olan web sitesi sayısının 2008 yılında 101 milyonu geçtiği dikkate alındığında internet ve multimedya ortamında kullanılan ses, data ve görüntü olmak üzere her türlü bilgi ve verinin güvenlik boyutunun ne kadar önemli olduğu ve buna bağlı olarak da güvenliğin sağlanması sorununun çözülmesinin de bir o kadar karmaşık ve zor olduğu ortaya çıkmaktadır. Ayrıca bilgi ve iletişim teknolojilerinin özelliği nedeniyle veri güvenliği hususunda uluslararası işbirliği de çok önemlidir. Zira günümüzün gelişen teknolojisi sayesinde bilişim suçları artık sınırları aşan bir boyut kazanmıştır. Örneğin, 2000 yılında ortaya çıkan Love Letter virüsünün tüm dünyada yaklaşık 7 milyar ABD Doları zarar verdiği tahmin edilmektedir.

Benzer şekilde 2001 yılında Code Red Worm virüsü ortaya çıktığından itibaren ilk 14 saat içinde 359.000 adet sisteme zarar verirken, 2003 yılında ortaya çıkan Sequel Slammer virüsü ise bundan çok daha hızlı bir şekilde yayılma göstererek sadece ilk 10 dakika içinde 75.000 adet sisteme zarar verdiği tahmin edilmektedir. FBI tarafından yapılan araştırmaya göre halen günümüze kadar yaklaşık 70.000 adet virüsün tesbit edildiği ve dünyada mevcut olan internet web server'lerinin yaklaşık %85'inin en az bir kez siber saldırıya maruz kaldığı dikkate alındığında konunun ekonomik boyutunun olduğu kadar uluslararası ilişkiler boyutunun da ne kadar önemli olduğu ortaya çıkmaktadır.

III. BİLGİ GÜVENLİĞİNDE AB'NİN HUKUKİ YAKLAŞIMI

Yukarıda belirtilen hususlar çerçevesinde istenmeyen bu durumların engellenebilmesini teminen AB, hukuki alanda aşağıda belirtildiği üzere bazı düzenlemeler yapmıştır. [2]

Avrupa Birliği'ndeki bilgi güvenliği alanındaki çalışmalar esas itibariyle 1987 yılında başlamıştır. 1987 yılında yayınlanan Green Paper (Yeşil Rapor) ile AB, telekomünikasyon sektöründeki bilgi güvenliğinin önemine işaret etmiştir. Ayrıca 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 95/46/EC ve 97/66/EC sayılı AB Direktifleri düzenlenerek yürürlüğe konulmuştur.

Diğer taraftan AB, özellikle 1995'li yıllardan itibaren internet ve multimedya teknolojilerinin toplum tarafından çok büyük bir hızla kullanılır hale gelmesiyle birlikte özellikle internet teknolojilerinin beraberinde getirdiği bazı kolaylıklar ve imkanlara ilaveten küçük çocukların internet ortamındaki muzır yayınlardan korunması amacıyla "Küresel ağlar üzerinde zararlı ve yasadışı içerikle mücadeleyle internetin 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, internet 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 yerine geçen elektronik haberleşme sektöründe mahremiyetin korunması ve kişisel verilerin işlenmesi hususundaki 2002/58/EC sayılı Direktifi yürürlüğe koymuştur. AB mevzuat uyum çalışmaları çerçevesinde sözkonusu Direktifin uyumlaştırılması amacıyla Kurum tarafından 06.02.2004 tarihinde Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik çıkartılmıştır.

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

- Bilgi güvenliğinin sağlanmasına ilişkin 31 Mart 1992 tarih ve 92/242/EC sayılı Konsey Kararı,
- Şebeke ve bilgi güvenliği kültürüne doğru Avrupa'nın yaklaşımına ilişkin 18 Şubat 2003 tarih ve 2003/48/EC sayılı Konsey Kararı,
- 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-European Network and Information Security Agency) kurulması amacıyla 2004/460/EC sayılı Tüzük 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.

Son olarak da AB tarafından elektronik haberleşme şebekeleri kullanılarak gerçekleştirilen tüm haberleşmenin (telefon, faks, VoIP, e-posta vs.) kim tarafından ne zaman ve kimle yapıldığına dair ve haberleşmenin içeriği de dahil olmak üzere ileride meydana gelebilecek herhangi bir yasal soruşturma ya da incelemede kullanılabilmesini teminen gerekli olabilecek tüm bilgilerin 6 aydan az olmamak ve 2 yıldan fazla olmamak şartıyla depolanması yönünde telekomünikasyon sektöründeki mobil işletmecilere, sabit işletmecilere, MVNO ve ISP gibi diğer tüm sektör aktörlerine bir görev verilmiştir. Bu çerçevede 13.4.2006 tarihli AB Resmi Gazetesi'nde yayınlanan 2006/24/EC sayılı Direktif gereğince bu husus yasal bir zorunluluk haline getirilmiştir.

IV. AVRUPA BİRLİĞİ'NDE GÜVENLİK POLİTİKASI

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, gerektiği vurgulanmıştır.

V. ULUSLARARASI BİLGİ GÜVENLİĞİNE İLİŞKİN BAZI ÖRNEKLER

A. İngiltere

İngiltere, biyometrik güvenlik önlemlerini de içeren kimlik kartlarının vatandaşlara dağıtılması için bir proje başlatmıştır. Zira kimlik bilgilerinin çalınarak kopyalanması sonucu çok sayıda insan maddi ve manevi zarara uğramış bulunmaktadır. İngiltere'de kimlik bilgilerinin çalınmasına karşı mücadele vermek üzere sivil toplum kuruluşu sıfatıyla kurulmuş olan Cifas'a göre örneğin sadece 2004 yılında 119.000 kişinin kimlik bilgileri kullanılarak maddi çıkar sağlanmıştır. Cifas, İngiltere'de 240 üyesi ile beraber başta telekomünikasyon şirketleri olmak üzere bankacılık sektörü ve çeşitli ticari firmalardaki kişisel bilgilerin başka amaçlarla kullanılmasını önlemek ve kullanıldığı takdirde bunu yetkili makamlara ihbar etmek üzere kar amacı gütmeden çalışma yapan çok sayıdaki sivil toplum kuruluşundan birisidir. [3]

B. Kanada'da Çocuk Pornosunun Önlenmesine Yönelik Bir Sistem: CETS

Bilindiği üzere günümüzde internet kullanımının her geçen gün artması, beraberinde çocukların internet kullanılarak istismar edilmesi ve bu çerçevede çocuk pornosunun çok büyük bir boyuta ulaşmış olması toplumda büyük bir rahatsızlığa neden olmaktadır. Bu rahatsızlıktan hareketle Kanada polisi, 2003 yılında bir çocuk pornosunun kullanıldığı bir web sitesinin izlenmesi ve tespit edilebilmesini teminen Microsoft firmasından yardım talep edilmiştir. Sözkonusu talep üzerine Microsoft tarafından hazırlanan ve adına CETS (Chield Exploitation Tracking System) denilen özel bir yazılım sayesinde tüm internet siteleri önceden belirlenmiş olan kelime ve/veya kelime grupları ve belirli resimler taranarak çocuk pornosunun kullanıldığı sitelerin tespit edilmesi sağlanmıştır. Sözkonusu projenin maliyeti yaklaşık 2,5 milyon ABD Doları olup, internete erişim yapan çocukların yaklaşık % 20'sinin pornografik saldırıya maruz kaldığı tahmin edilmektedir. [4]

C. Carnivore

Carnivore, ABD'de FBI tarafından 2000'li yılların başında geliştirilen özel bir elektronik izleme sistemine verilen isimdir. Bu sistem FBI tarafından daha önceden kullanılan Omnivore adlı sistemin geliştirilmiş versiyonudur. Carnivore sistemi, adli mercilerin izni ile internet üzerinden gerçekleştirilebilecek suçları ve suçluları önleme ve izleme amacıyla ya internet servis sağlayıcısına bağlanır. Bu sayede takibe alınan kişinin e-posta mesajları, ICQ mesajlaşmaları ve hangi web sayfasında ne kadar süre gezindiği ve ne yaptığı gibi her türlü işlem dahil olmak üzere internet vasıtasıyla gerçekleştirmiş olduğu her türlü işlem takibe alınır. Carnivore sisteminin FBI tarafından kullanılması sayesinde 25600 suçlu yakalanmıştır.

11 Eylül 2001'de ABD'de yaşanan terörist saldırı sonucu iki adet gökdelenin çökmesi sonucu ABD Temsilciler Meclisi tarafından 24 Ekim 2001 tarihinde kabul edilen ABD Vatandaşlık Kanunu ile internetteki her türlü verilerin FBI tarafından izlenmesi ve kayıt altına alınması hüküm altına alınmıştır.

Ancak her şeye rağmen Carnivore sisteminin kullanılmasının, 2001 yılında FBI tarafından terk edildiği 2005 yılında ilan edilmiştir. Bunun yerine daha da geliştirilmiş olan ve kod adı "DragonWare Suite" olan ve üç ayrı amaca yönelik olarak hazırlanmış olan "Carnivore", "Packeteer" ve "CoolMiner"dan oluşan bir sistem hizmete alınmıştır. FBI bu ve buna benzer sistemleri daha ziyade suçluları, casusları, kaçakçıları ve teröristleri takip etmek amacıyla yoğun bir şekilde kullanmıştır. Sözkonusu sistemin toplam maliyetinin 6-15 milyon ABD Doları olduğu ifade edilmektedir. [5]

D. Echelon

Echelon sistemi küresel bir haberleşme müdahale (COMINT - Communications Interception) sistemi olup,

tüm dünyadaki askeri ve sivil her türlü haberleşme izlenmekte ve kaydedilmektedir. Sistemin yönetimi, tamamen ABD'nin Ulusal Güvenlik Kurumu (NSA - National Security Agency) olup, sistemin varlığı 1999 yılına kadar sürekli olarak inkar ediliyordu. Ancak 16 Mart 1999'da Avustralya'daki Ulusal Askeri Muhabere Merkezi (DSD - Defense Signals Directorate) Müdürü Martin Bradley'in bir muhabir olan Ross Coulthart'a yazdığı mektupta ortaya çıktı. Bunun üzerine Avustralya hükümeti, Mayıs 1999'da yapılan bir açıklama ile Echelon sisteminin bir parçası olduklarını kabul etti.

Sistem çok güçlü bir yazılım ve donanım altyapısına sahipti. Zira 1992 yılında NSA'den emekli olan ve buranın müdürlüğünü yapmış olan Amiral William Studeman'ın yaptığı açıklamaya göre Echelon sistemi, saatte 2 milyondan fazla telefon, teleks, e-posta ve faks mesajını izleyebiliyor ve kaydedebiliyordu ki bu rakam bir yılda 17,5 milyar mesaja karşılık gelmektedir. 1992 yılındaki teknolojik imkanlar sayesinde 2 milyon olan bu rakamın, günümüzde çok daha fazla bir değere ulaştığı düşünülebilir.

Echelon sayesinde yapılan tüm izleme ve kayıtlar doğrudan NSA ve CIA'ya yönlendirilmektedir. 11 Temmuz 2001 tarihinde Echelon sisteminin mevcut olup olmadığı konusunda AB Parlamentosu tarafından çok kapsamlı bir şekilde hazırlanan ve yayınlanan rapor, Echelon sisteminin mevcut olduğunu kanıtlamıştır. Ayrıca sözkonusu raporda Echelon sistemine benzer başka sistemlerin Rusya, Çin ve Fransa gibi bazı ülkelerde de kurulu olabileceği ifade edilmektedir.[6]

VI. TEMPEST (TRANSIENT ELETROMAGNETIC PULSE SURVEILLANCE STANDARD)

Bakır kablo ve monitör gibi ilave bazı donanımlardan oluşan tüm bilgisayar sistemleri, Hollanda'lı bilim adamına hitaben adını Van Eck'ten alan alıcılar tarafından alınabilen ve kaydedilebilen elektromanyetik yayınları yaymaktadır. Tempest teknolojisi, bu yayınların kullanılarak ve ortamdaki parazitlerden arındırılarak ve güçlendirilerek ilgili cihaz tarafından yaklaşık 500 m kadar uzaktan alınmasını engellemeye yönelik olarak oluşturulmuş bir teknolojidir.

Bilgisayarın klavyesinden, ekranından, modem kablosu gibi çeşitli yerlerden elektromayetik sinyaller klavyede basılan tuşlara, ekrandaki görüntüye ve modemle bilgisayar arasında geçen bilgileri içermektedir. Yeterli donanıma sahip herhangi biri bu yayınları bir veya iki kilometreye varabilen bir mesafeden kaydedebilir ve ekranınızda ne göründüğünü, klavyede ne girildiği veya modemden ne geçtiği bu yayınlar işlenerek tekrar oluşturabilir. [7]

Tempest'de ekranlama, filtreleme veya yayılan dalgalara gürültü ekleyerek sinyali anlaşılmaz kılmak gibi uygulanabilecek bazı elektromanyetik güvenlik yöntemleri mevcuttur. Bu tip yöntemlerde ya doğrudan kullanılan elektronik malzemeler ekranlanır ve giriş/çıkışları filtrelenir veya ekranlı olması gerekmeyen aletler ekranlı odalarda (Faraday kafesi) kullanılır. Ekranlanacak odalar tamamen iletken bir maddeyle kaplanarak elektromanyetik yayınları durdurucu Faraday kafesi oluşturulur. Odaların havalandırma girişlerine dalga kırıcı yansıtıcılar konur. Elektrik şebekesine olan bağlantılar açıkverici işaretlerin bulunabileceği frekansları kesen filtreler aracılığıyla yapılır. Bu tip odalar genellikle ses yalıtımına da tabi tutulur.

VII. İSTEK DIŞI HABERLEŞME

Ülkemizin AB mevzuatına uyumlaştırma sürecinde, istek dışı haberleşme konusuna önem verilerek bu konuda bir an önce yasal düzenleme çalışmalarına başlanması, bu konudaki sorumluluk ve yaptırımların belirlenmesi gerekmektedir. 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 gerekmektedir.

VII. SONUÇ VE DEĞERLENDİRMELER

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.

A. 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, ülke 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.

B. Kurum ve kuruluşlarının;

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

C. 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.

D. Düzenleyici otoritelerin

Güvenlik kültürü oluşturulmasında her kurum, kuruluş ve bireye sorumluluk düşmesi nedeniyle Telekomünikasyon Kurumu (TK) tarafından "Kurumsal Bilgi Güvenliği Politikası" oluşturulması, Kurum çalışanlarının elektronik ortamda tutulan ve aktarılan bilginin güvenliğini sağlama hususunda uyması gereken kural ve politikaların belirlenmesi gerekmektedir.

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, "çerez" (cookie) gönderilip gönderilmediği konusunda kullanıcıyı bilgilendirmeli ve kullanıcıya bunu reddetme imkanı tanınmalıdır.

TK önderliğinde tüm sektör aktörlerinin katılımı ile oluşturulacak ve **"Elektronik Haberleşme Sektöründe 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.

Bilgi toplumunun oluşturulması ve yaygınlaştırılmasında en büyük engel olarak görülen istek dışı haberleşmenin artması toplumun hemen hemen tüm kesiminin (internet 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 kamu kurum ve kuruluşlarında ülke güvenliğine yönelik olarak Bilgi Güvenliği Yönetim Sistemi'nin (ISO/IEC 27001, COBIT vs.) kurulması ve bu çerçevede imkanlar ölçüsünde tüm bireylerin ve kamu çalışanlarının bilgi güvenliği konusunda bilgilendirilmesi ve bilinçlendirilmesi çalışmalarının bir an önce başlatılması ve bu bağlamda eğitim çalışmalarının yapılması son derece önemlidir.

Sadece bilgi ve iletişim teknolojileri boyutunda değil, günümüz kullanıcılarında olduğu kadar üretici ve işletmeciler gibi daha bir çok sektör aktörlerinin hepsinde ortak duyulan bir endişe sözkonusudur. **"Güvenlik".** Zaten konu ile ilgili olarak çeşitli platformlarda halen çalışmaları yürütülmekte olan tüm standardizasyon faaliyetlerinin temel hedefi sistem ve cihazlar arasında uyumlu çalışabilmeyi sağlamak olduğu kadar, güvenlik unsuru da birinci derecede rol oynamaktadır. Ülke güvenliği kavramı içinde kişisel ve kurumsal bilgi güvenliği gibi temel hususlar yer almakla birlikte, bunların altında iletişim ağı güvenliği, işletim sistemi güvenliği, veri tabanı güvenliği, internet erişim güvenliği, terminal cihazı ve sistem güvenliği gibi oldukça önemli hususlar bulunmaktadır. Özetle, burada sayılanların hepsinin **"Toplam Sistem Güvenliği"** adı altında toplanması mümkündür.

Yukarıda belirtilen hususlar, geniş bandlı teknolojilerin toplum bazına yaygınlaştıkça ülke güvenliği ve veri güvenliği olgusunun beraberinde getireceği muhtemel risklerin ve siber saldırıların da doğru orantılı olarak artacağına işaret etmektedir. Dolayısı ile, konu sadece bilgisayar suçlarına yönelik olarak ülkelerde görevli bir Kuruma işlerlik kazandırılmasını değil aynı zamanda yargı organları, sanayi, tüketici kuruluşları, üniversiteler ve veri koruma kurumları arasında işbirliğinin artırılmasını ve geliştirilmesini gerektirmektedir. Bununla beraber, bilgi ve iletişim teknolojilerinde veri güvenliğinin belki de en önemli kısmını oluşturan telekomünikasyon işletmecileri

ile erişim sağlayıcılarının gelişen teknoloji çerçevesinde tesbit edilecek olan asgari seviyedeki güvenlik kriterlerine uymaları da büyük önem arzetmektedir. Bu bağlamda "siber-suç polisi" ve "siber-suç savcısı" gibi yeni tanım ve meslek dallarının ya da diğer bir deyişle bilgi ve iletişim teknolojileri alanında veri güvenliği konusunda hukuki ve teknik ihtisas gerektiren yeni branşların gündeme gelmesi bir teknolojik zorunluluk olarak ortaya çıkmaktadır.

Bu çerçevede; bilgi ve iletişim teknolojileri alanında bilgi güvenliği ve mahremiyetin korunmasına yönelik olarak AB'de halen çok çeşitli platformlarda mevcut çalışmalar, dikkate alınır ise, konu sadece Ülkemizin AB'ne uyumu açısından değil; aynı zamanda günümüz teknolojisinin gereklerine ve ihtiyaçlarına mümkün olan en kısa sürede uyum sağlayabilme ve hatta gerçekleştirilebilir ise; Ülkemizde başta bilgi ve iletişim teknolojilerinde veri güvenliği olmak üzere, diğer teknolojik alanlarda da **Devlet-Sektör-Üniversite işbirliğinin geliştirilebilmesi** için, sözkonusu çalışmaların mümkün olan en kısa sürede başlatılmasının, Ülkemiz menfaatleri açısından doğru bir yaklaşım olacağı değerlendirilmektedir. Zira burada önemli olan husus, bir çok gelişmiş ülkede yazılım ve donanım ürünleri dahil olmak üzere bilişim sektörünün **"Stratejik Sektör"** olarak ilan edildiği olgusunun gerektirdiği ölçüde Ülkemizde topyekün bir işbirliğinin ve eyleminin gerektiğidir.

Bu çerçevede ülkemizde başta Telekomünikasyon Kurumu olmak üzere, Ulaştırma Bakanlığı gibi ilgili tüm kamu kurum ve kuruluşlarının ve diğer sektör aktörlerinin de iştirakinin sağlandığı **"Bilgi Güvenliği Ulusal Koordinasyon Kurulu"**nun kurulması son derece önem arzetmektedir. Kurulun temel amacı, telekomünikasyon sektöründeki abone ve kullanıcılar dahil olmak üzere tüm sektör aktörlerinin ve ilgili kamu kurum ve kuruluşlarının iştirak edeceği toplantıların düzenlenmesi ve bu çerçevede ilgili tüm taraflar arasında bilgi, tecrübe ve doküman paylaşımının yapılmasıdır. Ayrıca **"Bilgi Güvenliği Ulusal Koordinasyon Kurulu"** tarafından yürütülecek çalışmaların kapsamı ise, ilgili taraflarla karşılıklı bilgi alış verişi ve istişarelerde bulunarak bilgi güvenliğinin teminine yönelik olarak ülkemizde ihtiyaç analizinin yapılması, hazırlanacak rapor ışığında alınabilecek hukuki ve teknik tedbirlerin tespit edilmesi ve bu kapsamda yapılabilecek önerilerin değerlendirilerek ülkemiz açısından bir raporun hazırlanması olarak belirlenmelidir.

KAYNAKLAR

[1] European Innovation, May 2007, pp8
[2] http:// ec.europa.eu/information_Society/index_en.htm
[3] www.eurocomms.co.uk, Identity Crisis, Lynd Morley, pp7
[4] http://ncecc.ca/cets_e.htm
[5] www.foxnews.com
[6] http://en.wikipedia.org/wiki/echelon
[7] System Security, Srdjan Capkun, pp6