TBD Kamu-BİB

Kamu Bilişim Platformu IX

BİLİŞİM TEKNOLOJİLERİNİN KULLANILMASININ

HUKUKSAL BOYUTU

Mayıs 2007

2. ÇALIŞMA GRUBU

Çalışma Grubu Başkanı: Cengiz Tanrıkulu (Adalet Bakanlığı BİDB)

Çalışma Grubu Üyeleri

Eyüp AYAR	(Büyükşehir Belediyesi)
Adnan YILMAZ	(Yargıtay)
Leyla ERSUN	(ODTÜ BİDB)
Özgür ERALP	(Ankara Barosu)
Servet YETİM	(Yargıtay)
Cemal GEMCİ	(Cymsoft)
Emrullah AYCI	(Yargıtay)
Osman GÜNAYDIN	(DMO)
Çağatay CENGİZ	(Ankara Barosu)
Mehmet Ali UZUN	(Askeri Yargıtay)
Neziha ÇARKIT	(MEB)
Derya ORMAN	(Adalet Bakanlığı BİDB)
Mesut BUDAK	(Yargıtay)
Nuran GÖRGÜN	(Adalet Bakanlığı BİDB)
Ayşen Merih ACAR	(Ankara Barosu)
Murat TURAN	(Adalet Bakanlığı BİDB)
Özgür SAYAR	(EGM KOM Daire Başkanlığı)
Tekin MEMİŞ	(Kadir Has Üniversitesi)
Osman Nihat ŞEN	(Telekomünikasyon Kurulu)
Metin ÖZDERİN	(Ankara Barosu)
Ersin Tufan YALVAÇ	(Maliye Bakanlığı)
Çiğdem ÇAMURDAN	(Gümrük Müsteşarlığı)
Murat SOYSAL	(TÜBİTAK ULAKBİM)
M.Kemal AKGÜL	(Milli Prodüktivite Merkezi)

Kamu-BİB YK Temsilcisi

Ayla ALTUN	(ODTÜ BİDB)

TEŞEKKÜR

En başta grubumuzun üyesi olan ve çalışmalara başladığımız ilk günlerde aramızdan ayrılan değerli hukukçu hâkim İnci BİÇKİN'i rahmetle anıyor ve rapora olan katkılarından dolayı manevi huzurunda teşekkür ediyoruz.

Ayrıca Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu Grubu olarak Raporun oluşturulması sırasında yer ve lojistik destek sağlayarak katkılarını esirgemeyen Ankara Barosuna ve bizzat toplantımıza gelerek destekte bulunan Ankara Barosu Başkanı Avukat Ahsen COŞAR'a, Ankara Barosu Bilgi İşlem Merkezi Başkanı Av. Özgür ERALP ve yardımcısı Av. Hayri Çağatay CENGİZ'e, raporumuzdaki Bilişim Sistemleri Vasıtası ile Sahtecilik suçunun yazımında katkıda bulunan Av. Özge Evci ve Av. Beren ŞENTÜRK'e, "Sanal Kumar" kısmının yazımında katkıda bulunan Av. Aslı TATLIDİL'e, Raporun ek kısmında yer verilen, örnek bir e-Devlet yasası olarak, "ABD e-Devlet Yasası Özeti" kısmının yazarı DPT uzmanı Sayın Ramazan ALTINOK'a, grubun oluşturulması sırasındaki önerileri ve konuya vermiş oldukları önemden dolayı TBD Başkanlığına ve Adalet Bakanlığı Bilgi İşlem Dairesi Başkanı Sayın Ali KAYA'ya grubumuz adına teşekkür ederiz.

İÇİNDEKİLER

KISALTMALAR

BİDB	: Bilgi İşlem Dairesi Başkanlığı
BS	: Bilişim Sistemi
BT	: Bilişim Teknolojileri
BGB	: Alman Yüksek Mahkemesi
DMCA	: Dijital Millenium Copyright
DMO	: Devlet malzeme Ofisi
EGM	: Emniyet Genel Müdürlüğü
FSEK	: Fikri ve Sınaî Eserler Kanunu
HMK	: Hukuk Mahkemeleri Kanunun
HUMK	: Hukuk Usulü Muhakemeleri Kanunu
KOM	: Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı
KVK	: Kişisel Verilerin Korunması

1 GENEL GİRİŞ

BT alanındaki hızlı gelişmeler, teknolojinin sürekli olarak değişmesi ve gelişmesinin sonuçları sadece bilişim alanında değil, bilişimin yatay kestiği diğer bilim ve teknik alanlarında da büyük değişikliklere neden olmaktadır. Bu nedenle sadece BT alanındaki gelişmeleri takip etmek yetmemekte, bilişim alanındaki gelişmelerin yanı sıra diğer bilim ve teknik alanlarında meydana gelen bilişimin etkilerini ve bu etki sonucu ortaya çıkan değişimleri de takip etmek ve gerekli değişiklikleri yapmak gerekmektedir. Artık uzmanlar sadece tek bir alanla yetinmemekte, multi disipliner alanlarda uzman olmaya dikkat etmektedirler.

Türkiye Bilişim Derneği bilindiği üzere kamu yararı gözeten bir dernek olup bilişim alanındaki gelişmeleri takip etmekte ve ülkemizdeki bilişim alanındaki uygulamalara katkı sağlamakta, mevzuat çalışmaları konusunda değerlendirmelerde bulunmaktadır. Bu bağlamda TBD, bu yıl 9.sunu düzenlendiği Kamu BİB verimlilik toplantıları yapmakta ve yapılan bu toplantılarda BT alanındaki gelişmelere değinilmekte, sorunlu alanlar tespit edilerek bu alanlar hakkında tartışmalar yapılmakta ve ortaya çıkan sonuçlar ortak akıl ürünü olarak belgelere ve uygulamalara yansımaktadır.

Geçen yıl Antalya'da yapılan 8. Kamu BİB verimlilik toplantısında birçok BT konu ve sorunları tartışılmış, çözümler üretilmeye çalışılmıştı.

Bu toplantılar sırasında katılımcılar tarafından her ne kadar BT alanındaki gelişmelere 2006 Kamu BİB verimlilik toplantısında enine boyuna değinildiği belirtilmişse de konunun hukuksal boyutunun üzerinde biraz daha fazla durulması gerektiği görüşü ortak bir fikir olarak ileri sürülmüştü. Ayrıca toplantıda bu konuda artık bilişim teknolojilerinin hukuksal alt yapısı tam olarak sağlanmadan gelişmelerin sağlıklı bir şekilde devam edemeyeceğine vurgu yapılmış ve bu konuda çalışmalar yapılması, gruplar oluşturularak ortaya BT'nin hukuksal boyutu konusunda raporlar oluşturulması gerektiği görüşü vurgulanmıştır.

Bu talepleri yerinde gören TBD, BT'nin kullanılmasının hukuksal boyutu ile ilgili olarak daha önceki yıllarda Türkiye 2. Bilişim Şurası[1] kapsamında konuyu ele almış olduğunu belirterek bu temelden hareketle konunun tekrar ele alınmasının yararlı

[1] "Bilgi Toplumuna Doğru, Türkiye 2. Bilişim Şurası Sonuç Raporu" 2004 Ankara s. 277 vd.; 10–11 Mayıs 2004 tarihleri arasında ODTÜ Kültür ve Kongre merkezinde yapılan Türkiye 2. Bilişim Şurası TBD'ninde katkıları ile düzenlenmiş olup Bilgi Toplumuna Doğru, Türkiye 2. Bilişim Şurası Sonuç Raporu adı ile Ankara'da 2004 yılında basılmış olup, bu rapor kapsamında alt çalışma grubu olan hukuk grubu ve özellikle bilişim hukuku eğitimi, kişisel verilerin korunması, bilgi edinme hukuku, Telekominikasyon alanında kişisel verilerin korunması, Telekomünikasyon hukuku ve VoIP, Bilişim teknolojileri ve ceza hukuku, e-İmza kanunu ve son olarak da İnternet ve Tüketici hukuku konularını kapsayan 76 sayfalık bir rapor ortaya koymuştur.

olacağına karar verilmiş ve 9. Kamu BİB verimlilik toplantısında oluşturulacak gruplardan birisinin hukuksal boyut konusunda çalışmasına karar vermiştir. Daha sonra TBD bu yönde bir grup oluşturulması için harekete geçmiştir. Bu girişim sonucu oluşturulan Bilişim Teknolojileri Kullanımının Hukuksal Boyutu Çalışma Grubu, çalışmalarına 10 Kasım 2006 tarihinde ikinci grup olarak başlamıştır.

Grup genel olarak hukukçu ve bilişimcilerden oluşturulmuş ve çalışmanın başında yapılan beyin fırtınası metodu ile ele alınması gereken konu başlıkları belirlenmiştir.

Hukuk alanında TBD bünyesinde her ne kadar başka grup çalışmaları yapılmış ise de ilk kez verimlilik toplantısında bilişimin hukuksal boyutunu ele alan bir çalışma grubu oluşturulduğundan, bu ilk grup çalışmasında bilişim hukukuna genel bir bakış açısı ile yaklaşarak olabildiğince bütün konulara kuş bakışı da olsa değinilmeye çalışılmıştır.

Bu bağlamda ilk olarak özellikle 2006 yılından itibaren Türk Kamuoyunda çokça tartışılmaya başlanılan bilişim suçları ve bilişim güvenliği konuları başta olmak üzere, hukuku tamamlayan niteliğe sahip bilişimde etik konusuna da değinilmiştir. Bu bağlamda hukukun tamamlayıcısı olan etik konusuna da giriş kısmında ilk olarak değinilmiş ve etik konusunda neler yapılabileceği, etiğin önemi ve gerekliliği konularının da işlenmesinde fayda görülmüştür.

Yine tüm verilerin elektronik ortama taşınarak birçok hizmetinde bu ortamda verilmeye başlanması doğal olarak bu ortamın güvenliği sorununu da gündeme taşımıştır. Amerika ve Avrupa'daki birçok ülke 1980 yılların sonu 1990'lı yılların başlarında elektronik ortamın güvenliğini sağlamaya yönelik başta standartlar olmak üzere bir takım kurallar koyma çalışmalarına girişmiş ve bu çalışmalar daha sonra meyvelerini vererek, genel, ana ilkeleri belirleyen temel bilgi güvenliği yapısını ortaya koyan yasalar ortaya çıkmıştır. Henüz ülkemizde bu anlamda yasal bir düzenleme bulunmadığından örnek yasalar değerlendirilerek ve ülkemizde gündemde olan yasa tasarıları da dikkate alınarak değerlendirmelerde bulunulması yararlı görülmüştür. Bu yönde raporumuzda görüşlerimiz ortaya konulmaya çalışılmıştır.

Ülke olarak gündemimizi çok meşgul eden ve çok hassas bir konu olan kişisel verilerin korunması da elektronik ortamdaki kişisel verilerin artmasına koşut olarak önemini arttırmış ve bu konunun daha çok tartışılması ve gündemde tutulması zorunluluk haline gelmiştir. Bu zorunluluktan hareketle Grubumuz tarafından özellikle kişisel verilerin korunması hukukunun temellerini kısaca ortaya koymaya çalışılmış ve özellikle idarenin kişisel verileri ne şekilde toplayabileceği ve kişisel verileri koruma

hukukunda ne şekilde etkileneceği ve etkilenmesi gerektiği konusunu tartışmaya açılması faydalı görülmüştür.

Öte yandan ülkemizi yakından ilgilendiren Medeni Usul Hukuku alanındaki gelişmelerde hızlanmış olup bu değişim sırasında acil ihtiyaç olan bilişimin Medeni Usul Hukuku alanına yansımaları üzerinde durulmasına ihtiyaç doğmuştur. Çünkü Cumhuriyetin kuruluşundan bu yana Medeni Usul alanını düzenleyen HUMK konusunda önemli gelişmeler yaşanmakta ve yaklaşık 80 yıllık bir uygulamadan sonra bu yasa da köklü değişiklikler yapılarak yeni bir yasa hazırlığı başlamış bulunmaktadır. Gerçekten de hukukun temel yasalarından olan HUMK özellikle hukuk alanındaki uygulamaları birinci dereceden ilgilendirmektedir. E-İmza, e-Belge gibi elektronik ortamdaki veri iletişiminin önünü açacak uygulamaların sağlıklı gelişebilmesi için de yeni Hukuk Muhakemesi Kanun Tasarısının özellikle üzerinde durulması ve ele alınması gerekmektedir. Raporumuzda da bu konuya genel hatları ile değinilmeye çalışılmıştır.

Son olarak grubumuz tarafından BT açısından fikri ve sınaî haklar konusunun ele alınmasının yararlı olacağını düşünülmüş ve bu konudaki mevzuattaki ve uygulamadaki mevcut durumun ele alınmasının gerekli olduğu görülerek bu konuda çalışma yapılması gerektiğine karar verilmiştir.

Elbette BT'nin kullanılmasının hukuksal boyutu yukarıda saydığımız konu başlıklarından ibaret değildir. Ancak sürenin kısıtlı olması ve rapora katkı veren kişilerin bu işi gönüllülük esası çerçevesinde ancak belli konu başlıkları üzerinde durulabilmesi sonucunu doğurmuş ve rapor kapsamındaki belirlenen konu başlıkları ile yetinilmesinin yerinde olacağı düşünülmüştür. Aslında BT'nin kullanılmasının hukuksal boyutu BT'nin çok geniş olan uygulama alanlarını yatay olarak kesmesi nedeni ile bir rapora sığmayacak kadar da etraflıdır. Ancak bu ilk rapor çalışmasından sonra TBD'nin bundan sonraki grup çalışmalarında da hukuksal boyutunda yeterince yer alacağına inancımız tamdır. Çünkü Türkiye Bilişim Derneği BT sorunlarının sadece teknolojik önlemler ve çözümlerle halledilemeyeceğinin, bu çözüm ve önlemlerin yanı sıra, BT'nin hukuksal boyutunun ve farkındalık çalışmalarının da BT sorunlarının çözümünde önemli rol oynadığının bilincindedir ve bu bilinçle sürekli değişik platformlarda çalışmalarını başarı ile yürütmektedir.

Raporun başlangıç aşamasında grup olarak belirlenen konuların ne şekilde ele alınacağı konusu enine boyuna tartışılmıştır. Bu tartışmalar sonucunda grup tarafından, güncelliğini koruyan hukuksal mevzuat konusunda genel açıklamalarda bulunmasına, mevcut mevzuattaki düzenlemelerde sıkıntıların bulunması halinde bunlara vurgu yapılması ve çözümlerinin önerilmesi ve son olarak da yasal düzenleme

yapılmamış alanlarda ne şekilde bir düzenleme yapılması gerektiği konusunda görüş ortaya konulması kararlaştırılmıştır. Bunlar yapılırken özellikle başta Avrupa Birliği Müktesebatı olmak üzere bilişim konusunda bir hayli mesafe almış ülkelerin mevzuatları ve uygulamaları da göz önünde bulundurulmaya çalışmıştır.

2 BİLİŞİM ETİĞİ

2.1 Etik

Türk Dil Kurumu Ansiklopedik Kültür Sözlüğünde Etik; insanların töresel ya da ahlaksal ilişkilerini, davranış biçimlerini ve görüşlerini araştıran bir felsefe dalı olarak tanımlanmıştır. Felsefenin en eski dallarından biri olan etik bazen ahlakla aynı anlamda kullanılmaktadır.

Ahlak; insan ilişkilerinde “iyi” ya da “doğru” yahut “kötü” ya da “yanlış” olarak adlandırdığımız değer yargılarını ifade eder.

“Yaşamın her alanında gözetilmesi gereken iyi nitelikli, erdemli davranış biçimlerinde kendini gösteren etik kavramı, tüm toplumlarda her zaman tartışma konusu olmuştur. Ancak, etik değerler, insanlığın tarih boyunca edindiği deneyim ve birikimler sonucunda, çağdaşlığın ve iyi yönetimin ön koşulu arasında yer almıştır.

Çağdaş toplumlarda, toplumsal yaşama yön veren ilkeler arasında etik değerlerin kendine özgü bir yeri bulunmaktadır,

Etik değerleri oluşturan kuralların değer ve anlamlarından ödün verilmeksizin yaşamın tüm alanlarında geçerli kılınması, bireyden başlayarak, tüm toplum kurumlarında yaşatılması temiz ve sağlıklı toplumu oluşturabilmenin tek yoludur,

Etik değerler toplumsal yaşam süreci içinde ortaklaşa yaratılmış ve genel kabul görmüş ise, hangi çağda olursa olsun işlerlik kazanır.

2.2 Etik ve Hukuk

Hukuk ve ahlak arasında yakın ilişki olmakla beraber, aralarında farklılıklar da bulunmaktadır. İnsanlık tarihi boyunca birçok temel ahlaki değerler zaman içinde hukuki norm haline gelmiştir. Hukuk kuralları insan davranış ve eylemlerini düzenler ve bazı sınırlamalar getirir. Hukuk kurallarının yaptırımı söz konusudur. Ahlak kuralları da insan davranışlarına sınırlamalar getirir. Ancak dışsal bir yaptırımı yoktur. Hukuk kuralları yazılı olduğu halde ahlak kuralları genelde yazılı değildir. Hukuk kuralları dışa yönelik iken ahlak kuralları daha çok içe yöneliktir. Hukuk kuralları devlet tarafından oluşturulurken ahlak kuralları devlet dışında topluluklar tarafından da oluşturulabilir.

Davranış normları bir gereklilik ve bir yükümlülük anlatırlar insanın irade hürriyetine sahip olması nedeni ile normal hayatta kişilerin belirli bir hareket biçimini tayin ederken kendi iradesi doğrultusunda serbestçe karar verir. Bu bağlamda insanlar

irade özgürlüğü sonucu kişiliklerini geliştirme imkanı bulurlar ve kişilikleri geliştirme insanlığin içinde bulunan tabi bir görevdir. Bu genel olarak böyle olmakla beraber ahlak ve hukuk kuralları müştereken kişilere belli davranış normları vasıtası ile şu hareketi yapmalısın şeklinde normlar ortaya koyar. Bu davranış normları müşterek bir zeminde bulunmakta olup Hateminin dediği gibi tabi hukukun yasakları aynı zamanda ahlakında yasakları olduğu ileri sürülmüştür. Bu kabulden hareketle hukuki olan aynı zamanda ahlakidir de. Kimi görüşlere göre ahlaka aykırı bu davranış hiçbir zaman hukuki koruma altına alınamaz denmektedir. Aralın dediğine göre ahlak bireyin kendi vicdanının ürünüdür ve tamamiyle bir iç kanun koymadan söz edilebilir. Ahlak normlarının onları koyan bireyin vicdanından başka bir kanun koyucusu yoktur. Arala göre hukuk ile ahlak arasındaki fark bulunmaktadır. Hukuka uygun olan bir fiil aynı zamanda ahlakada uygun olmak zorunda değildir. Aral hukukta sorumlu olan makamın dışta ahlakta ise içte bulunduğundan söz ederek farkı ortaya koymaya çalışmış ayrıca hukukun idesi ve idealinin adalet olmasına karşılık, ahlakın ide ve amacının iyiyi yani hayrı gerçekleştirmek olduğunu belirtmiştir. Arala göre adalet toplumsal bir değerdir ve toplumu ilgilendirir ve toplumun huzur ve refahını amaçlar buna karşılık ahlak ise tek tek insanlığa yani onun yetkinliği ile ilgili değer elde etmeye çalışarak kişi ile ilgilenir. Sonuç olarak Aral adaletin de iyi olduğunu iyi bir şey olarak adaletinde aynı zamanda ahlaki bir kavram olduğunu ve adaletin gerektirdiği toplumsal yaşamın kişisel yaşamların bir yanı olduğunu belirterek temel olarak hukukun ahlaki normlara tabi olduğunu belirtmektedir.

Hukuk kurallarının var olması onlara her zaman uyulması anlamına gelmemektedir. İş görenler etik değerler açısından yeterince gelişmemişlerse, yasalar etik davranışlar göstermelerini sağlayamamaktadır. Toplum ve toplumdaki alt gruplar içindeki resmi ve gayrı resmi ilişkiler ağı günümüzde o kadar karmaşık bir hale gelmiştir ki, iş görenlerin adil, doğru, tarafsız, çıkarsız davranmalarını sağlayacak başka ilkelere gereksinim doğmuştur.

Farklı değer yargıları nedeniyle etik kavramının çerçevesinin belirlenmesi güçtür. Etiğe uygun hareket edilmesinin sağlanmasında en büyük görev kamuoyuna düşmektedir.

Kişiler hukuki sorumluluklarını yerine getirince, etik sorumluluklarını da yerine getirdiklerini düşünmektedirler. Hâlbuki etik sorumluluklar proaktif olmayı veya kanunların ötesinde sorumluluklar yüklenmeyi gerektirmektedir.

Saydam devlet kavramını tanımlayan, etik değerlerin kurallarını belirleyen ve kurallara aykırı davranışlara yaptırımlar geliştiren etik yasaları, bu gün öncelikli bir gereksinim durumuna gelmiştir.

Alacakaptan'a göre hukuk ile ahlak birbirinden kesin olarak ayrılmış iki ayrı alandır. Öndere göre hukuk ve ahlak birbirini kesen iki daireye benzer ve ahlak kurallarının bir çoğu hem ahlak kuralıdır hemde hukuk tarafından bünyesine alınmıştır. Hukuk ve ahlak kurallarının iki daire gibi bir birini kestiği ve iki kuralın birleştiği halin duışında da hukuk kurallarının ahlak kurallarının kesiştiği durumda asgari ahlak kurallarının varlığından söz edilebilir. İçel/Donay ise ceza hukuku ve ahlakın iç içe iki daire olduğunu ceza hukukunun ahlak dairesinde alt küme olduğunu belirtmektedir. Toroslu ise ceza hukukunun önemli bir kesiminin ahlak ile ilgisi olmayan veya çok az ilgisi olan politik zorunluluk veya pratik elverişliliğinden esinlenmektedir. [2]

2.3 Bilişim Etiği İlkelerinin Gerekliliği Ve Etik Eğitimi

Bilişim sektöründe teknolojik gelişme akıl almaz hızda seyretmektedir. Dolayısıyla bilişim suçu türleri teknolojinin suç aracı olarak kullanılmasına paralel olarak artış göstermektedir. Bilgisayar ve bilgisayar sistemleri bir suçla ilintili olarak üç farklı şekilde kolluk birimlerinin karşısına gelebilir. Buna göre;

- Bilgisayar bir saldırının hedefi olabilir,
- Bilgisayar suç işlemek için bir araç olarak kullanılabilir
- Bilgisayarlar, belleğinde yasadışı bilgi, resim ve belgelerin depolanması yoluyla suça karışarak kolluk güçlerinin ilgi alanına girebilir.

Bilişim suçlarını daha ayrıntılı biçimde sınıflandırmak gerekirse altı başlık altında toplayabiliriz.

Bu suç tiplerinin en yaygın olanlarını şöyle sıralayabiliriz;

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme
- Bilgisayar Sabotajı
- Bilgisayar Yoluyla Dolandırıcılık
- Bilgisayar Yoluyla Sahtecilik
- Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı
- Yasadışı Yayınlar ve Siber Terörizm

Sınır tanımayan özelliğe sahip olan bilişim suçları ile mücadelede başarılı olabilmek için; yasal, teknolojik bilişim sektörü bazında çözümler bulmak zorunludur.

Ne var ki, çok fazla yasal düzenleme yapmak veya kısıtlayıcı yasalar çıkarmak hem teknolojik gelişmeleri hem de ticari hayatı olumsuz etkileyebilir. Bazı alanlarda

[2] Özgenç, İzzet; Türk Ceza Hukuku Genel Hükümler Ankara, 2006, S.24 vd.

kuralların devlet yerine serbest rekabet ortamında belirlenmesi bilişim suçları ile mücadelede daha etkin olabilmektedir.

Sınır tanımayan özelliğe sahip olan bilişim suçları ile mücadelede başarılı olabilmek için yasal ve teknolojik bilişim sektörü bazında çözümler üretmek ve bilişim etiği geliştirilmesi gerekmektedir.

Bireylerin yasalara uyması her zaman etik davranışlar sergiledikleri anlamına gelmemektedir. Bir davranış yasalara uygun olmakla birlikte, toplumun değer yargılarına uymayabilir.

Bilgisayar sistemlerinin tüketicileri olarak da kabul edilebilecek olan bireyler, sorumlu davranışları ile bu suçlar ile mücadeleye yardımcı olabilirler. Herkes evine hırsızların giremeyeceği şekilde güvenlik önlemini alsa, nasıl hırsızlık olaylarında önemli düşüş olacağı bir gerçek ise, bilişim alanında da tüketiciler, kurallara uygun olarak gerekli güvenlik önlemlerine uymuş olsa bilişim alanında görülen suçlarda bir azalma olacaktır.

Bilişim suçları ile mücadelede uluslar arası işbirliği olmadan başarılı olmak mümkün değildir Kolluk güçleri tarafından alınan önlemlerin yanında uzun soluklu bir çözüm yolu; siber etik ya da bilişim etiği dediğimiz sanal âlemde davranış kuralları konusunda özellikle genç kuşağın eğitilmesidir. İnternet çağının gençlerinin içine düştüğü sanal âlem-gerçek âlem çatışmasını eğitimle ortadan kaldırmak gereklidir.

Gençler ilköğretimden başlayarak bilişim etiği konusunda eğitilmelidir. Bu çalışma, ABD'de olduğu gibi özel sektör ile işbirliği çerçevesinde yürütülebilir. Türkiye gibi sanal âleme sonradan dâhil olan ülkeler gelişmiş batı ülkelerine göre bu konuda daha şanslıdır. Sanal âlemi kullanan gençliği hala eğitme olanağımız vardır.

Bir de çocukların ve gençlerin eğitimi meselesine değinmekte fayda vardır. Günümüzde çocuklar çok küçük yaşlarda bilişim teknolojisiyle tanışmaktadırlar. Ailelerin çocuklara temel ahlak kurallarını yerleştirirken bu doğada nasıl davranılması gerektiğini de göstermeleri gerekmektedirler. A.B.D.'de Başsavcısı Janet RENO 'nun " Janet RENO'dan Ebeveynlere Siber vatandaşlık ve Siber etik Üzerine Mektup" başlıklı mektubunda bu husus çok güzel ifade edilmiştir."Birçok çocuk komşusunun evine gizlice girmenin veya arkadaşının günlüğünü okumasının yanlış olduğunu bilir; fakat pek çoğu komşusunun bilgisayarına ve başkalarının dosyalarına izinsiz girmesinin yanlış olduğunu bilmez. Bizlerin çocuklarımıza şu hususu anlatmaya ihtiyacımız var; bilgisayar sistemlerine veya dosyalarına yetkisiz giriş yapmak, hacker olmak onları zeki ve hiçbir şeyi başaramayacak bir insan yapmaz, onların suçlu olmalarına yol açar".

2.4 Genel Etik İlkeler, Bilişim Etiği İlkeleri

2.4.1 Genel Etik İlkeler

Bireyler bilişim devrimini anlayabilmek ve uygun davranış biçimlerini geliştirebilmek üzere bir takım etik prensiplere sahip olmalıdırlar. Bu da bireyin kendisinden başlayarak, içinde bulunduğu kurum ve meslek örgütleri ile giderek toplumun tüm kesimine yayılacak bir bilişim etiği anlayışının yerleşmesi ile mümkün olur.

Kişilerin bilişim teknolojilerinin kullanılması konusunda bir takım etik prensiplere sahip olmaları gerekmektedir.

Bireyler etik prensipleri kendi kendilerini ortaya koyabilecek yetkinliğe sahiptirler. Yalnız burada altını çizmemiz gereken nokta etik prensiplerle yeni çıkan durumların uyumlaştırılması sorununun ortaya konmasıdır. Bu da temel etik felsefesini hayata geçirmiş olan bir kişinin aşamayacağı bir zorluk göstermeyecektir.

Bu bağlamda hayatta uygulanabilecek olan genel etik ilkeleri şunlar olabilir;

1.Yasalara ve toplumun değer yargılarına uygun davranmak.

2.Başkalarının haklarına saygı göstermek.

3.Başkalarına zarar vermekten kaçınmak.

4.Dürüst ve güvenilir olmak.

5.Gizliliğe saygı göstermek.

6.Başkalarının özel yaşamlarına saygı göstermek.

7.Başkalarının manevi değerlerine saygı göstermek.

8.Çocukların gelişimlerini olumsuz yönde etkileyecek davranışlardan kaçınmak.

9.Yanıltıcı bilgilerden ve yönlendirmelerden kaçınmak.

10.Her tülü ayrımcılıktan kaçınmak.

2.4.2 Meslek Etik İlkeleri

Bilişim devriminin 20.yy ikinci yarısından itibaren başladığını kabul edersek bu kısa süre içersinde bu sektörün kendi içersinde meslek ilkelerini temellendirebilmesinin zorluğu kendiliğinden ortaya çıkar. Ancak genel etik ilkelerinden yola çıkarak bu ilkeleri mesleklere göre uyumlulaştırırsak meslek etik ilkelerini de şu şekilde sıralayabiliriz;

1.Dürüst ve güvenilir olmak ve iş yaptığı kişilerinde dürüst ve güvenilir olmasına özen göstermek.

2.Mesleki yükümlülüklere uymak, mesleki yetkinlik kazanmak ve mesleğin kurallarını öğrenip uygulamak.

3.Sahip olduğu bilgileri, başkasının zararına, kendi çıkarına kullanmamak ve gizliliğe özen göstermek.

4.Kendisinden beklenen işleri gerçekçi, yansız ve nitelikli yapmak.

5.Toplum çıkarlarının bireysel çıkarlarının önünde olmasına özen göstermek.

Ülkemizde Türkiye Bilişim Vakfı (TBV)'nın bu konuda belirlediği meslek ilkeleri bilişim mesleğini ifa edenler için yol gösterici nitelik taşımaktadır.[3]

Her kurum kendi bünyesinde çalışanlarının uyması gerekli bir takım etik prensipleri belirler. Özellikle bilişim teknolojilerinin özelliği dikkate alındığında kurumların yöneticileri bu teknolojilerin kullanılması ile ilgili etik prensipleri gizlilik, fikri mülkiyet haklarına saygı gösterilmesi, bireysel hak ve özgürlükler, müşterilerin korunması ve ürün kalitesi konularını içine alacak biçimde belirlemelidir.

2.5 Etik Kurul Önerisi

Getirilen her düzenleme ya da koyulan her kural, bu kurallara uyulup uyulmadığının denetlenmesi ile işlerlik kazanmaktadır. Genel ahlak kurallarını, o kuralları ortaya çıkaran toplum denetlerken, hukuk kurallarına uyulup uyulmadığını ise yine hukuk kurallarının belirlediği kurumlar denetlemektedir.

Bilgi ve iletişimdeki hızlı gelişmeler aynı zamanda insanların bilgiye ulaşmasını da kolaylaştırdığından, artık insanlar hem kendi ülkeleri dışındaki gelişmeleri hem de kendi ülkelerindeki kişilerin davranışlarını etkin olarak izleme, bu kişilerin salt hukuka uygun davranışlarını değil, aynı zamanda onların toplumda kabul gören genel ahlak kuralları ile mensubu oldukları toplumsal grupların ya da meslek gruplarının kendi içinde uyması gereken etik kurallarına uygun davranıp davranmadığını denetleme imkânına kavuşmuştur. Gelinen bu noktada, halka denetleme olanağı sunmak bir zorunluluk halini almıştır.

Etik davranış ilkelerini yerleştirmek ve belirlenen bu ilkelere uygun davranılıp davranılmadığını gözetmek işlevinin uygulamada "etik kurullar" tarafından gerçekleştirildiği görülmektedir. Örneğin; ABD'de The Office Of Government Ethics, İngiltere'de The Comity Of Standards In Public Life, Kanada'da The Office Of Ethics Council, Japonya'da National Public Service Ethics Board, Avustralya'da The Public Service And Merit Protection Commission, İrlanda'da The Public Office's Commission

[3] Bu ilkeler için bkz.; http://www.tbv.org.tr/default.asp?ID=25 (03.05.2008), Bu ilkeler 1998 Yılında kurulan Etik Çalışma Grubu tarafından geliştirilmiştir. Daha sonra TBV Yürütme ve Yönetim Kurullarının onayı ile kamuoyuna duyurulmuştur.

ve Portekiz'de The Inspection General For Public Administration. Türkiye'de ise; 5176 sayılı kanun ile kurulmuş olan, Kamu Görevlileri Etik Kurulu.

Gerek uluslararası gerekse ulusal örnekler göz önüne alınarak, bu çalışmada bir etik kurul modeli önerisi geliştirilmeye çalışılmıştır.

2.6 Etik Kurulu'nun Denetleme İşlevi

Bilişim alanında belirlenecek olan genel bir Etik Kurul, davranışın belirlenen ilklere uygun olup olmadığını kendiliğinden denetleyebileceği gibi, Kurul'a yapılan başvurular üzerine de denetleyebilmelidir. Etik ilkelere uygun davranışlarda bir standart geliştirilerek, aynı ilkenin farklı yorumlanmasının önüne geçilebilir. Bu bağlamda ülkemizde basın sektöründe önemli görevler yerine getiren Basın Konseyi örnek olarak ele alınabilir ve bu örnekten dersler çıkarılabilir.

2.7 Etik Kurul Kimlerden Kurulmalı

Grubumuzca yapılan değerlendirmeler sonucunda Etik Kurulun, belirlenen bir birimin (örneğin, Telekomünikasyon Kurumu veya yeniden daha geniş katılımlı ve Stok'ların daha çok içinde yer aldığı haliyle gündeme gelen İnternet Üst Kurulu) koordinasyonu ile aşağıda yer alan üyelerden kurulabilir:

- Telekomünikasyon Kurumu,1 temsilci
- Tubitak, 1 temsilci
- TOBB, Bilişim sektöründe faaliyet gösteren 2 şirket temsilcisi
- TMMOB, Bilgisayar mühendisi 1 temsilci
- Barolar Birliği, 1 temsilci
- Basın Konseyi, 1 temsilci
- YÖK, Üniversitelerden Çocuk Gelişim Uzmanı 1 temsilci
- YÖK, Üniversitelerden Sosyal Psikolog 1 temsilci
- STK, Bilişim alanında faaliyet gösteren STK'lardan 3 temsilci

2.8 Görev Süreleri ve Toplantılar

- Kurul üyelerinin görev süresi 4 yıl olmalıdır.
- Kurul üyeleri en çok 2 kez görev almalıdır.
- Kurul yılda en az 2 defa toplanmalıdır.
- Kurulun çalışma usul ve esasları, ilk toplantıda kurul üyelerince belirlenmelidir.

- İlk toplantıda, Kurul üyeleri arasından Raportör seçimi yapılmalıdır.

2.9 Başvuru Koşulları

- Yazılı dilekçe, e-posta ya da tutanağa geçirilen sözlü beyan ile başvuru yapılabilir.

- Dikkate alınmayacak başvurular:

- Daha önce incelenmiş ve karara bağlanmış olup, yeni bir kanıt ileri sürülmeden yinelenen başvurular.

- İncelenmekte olan konulara ait başvurular.

- Başvuranın kimliğinin tespit edilemediği başvurular.

- Yargı organlarınca incelenmekte olan durumlara ait başvurular.

- Kişi, kurum ya da kuruluşu karalama amacı güttüğü açıkça anlaşılan başvurular.

- Söz konusu durumun oluştuğu tarihi izleyen günden itibaren bir yıl içinde yapılmayan başvurular.

2.10 Başvuruların Kabulü, İncelenmesi ve Karara Bağlanması

- Yapılan başvurulara bir kayıt numarası verilerek, ilgiliye bu numara bildirilir.

- Başvurunun, başvuru koşullarına uygunluğu Raportör tarafından belirlenerek kurula sunulmak üzere ön rapor hazırlanır.

- Kurul tarafından işleme alınması uygun bulunan başvurular hakkında, taraflardan görüş ve belgeler talep edilir.

- Kurulca istene her türlü bilgi ve belge, ilgili kişi, kurum veya kuruluşlar tarafınca yasal istisnalar saklı kalmak koşu ile verilmek zorundadır.

- Gelen belgeler Raportör tarafından incelenerek son rapor hazırlanarak kurula sunulur.

- Kurul üye tam sayısının salt çoğunluğu ile karar verir.

- Taraflar, Kurul kararlarına karşı tebliğ tarihinden itibaren 15 gün içinde yeniden değerlendirme talebinde bulunabilir, bu talep üzerine verilen karar kesin karar olur.

- Kurul kararlarına karşı idari yargı yolu açıktır.

- İdare Mahkemesi tarafından kaldırılan kurul kararları geçersizdir.

- Kurul kararları, kurulun yayın organlarında ilan edilir ve hakkında karar verilen taraflara, varsa bağlı olduğu birimlere (oda, şirket, borsa, v.s.) bildirilir.[4] [5]

3 BİLİŞİM SUÇLARI

3.1 Kavram ve Tanım Sorunu

Genel olarak konuyu işleyen tüm eserlerde de ifade edildiği gibi bilişim Fransızca "informatique" kelimesinden Türkçeleştirilmiş ve bilişim olarak dilimize tercüme edilmiştir[6]. Yılmazoğlu'na göre bilişim yukarıdaki tanıma uygun olarak ; "Fransızca "information" (=bilgi) ve "automatique" (=otomatik) kelimelerinin birleşiminden türemekte ve bilginin otomasyona tâbi tutulması sonucunda işlenmesini yani verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması anlamlarını içermektedir." şeklinde tarif edilmiştir.[7] Yenidünya'ya göre ise bilişim; "teknik ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır"[8]. SSS bilişim kavramı yerine "bilgisayar sistemi"[9] terimini tercih ettiği ve bu kavramı; "bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı ifade edecektir" şeklinde tanımlamıştır.

Bilişimin anlamı üzerinde durduktan sonra bilişim suçu kavramı ve bu kavramın tanımı üzerinde de durmak gerekiyor. "Bilişim Suçları" kavramı aslında son zamanlarda

---

[4] http://www.hukukcu.com/bilimsel/kitaplar/yasinbeceni/bolum4.htm (20.03.07) Burada meslek örgütlerinin etik prensipleri saptama konusunda çaba içersinde olduğunu belirtmek gerekir. Örneğin A.B.D. Federal Hesaplama Makineleri Birliğinin belirlediği meslek ilkeleri konuya ışık tutması açısından önemlidir. Bu birliğin belirlediği ilkelere göre ;

- Toplumun ve insanlığın daha iyi şartlar altında yaşamasına katkıda bulunmak
- Zarar verici davranışlardan kaçınmak
- Telif ve patent haklarını da içeren mali haklara saygı duymak
- Dürüst ve güvenilir olmak
- Fikri mülkiyet haklarına gerektiği değeri vermek
- Sadece izin verildiği müddetçe bilgileri otomatik işleme tabi tutulmuş kaynaklara erişimin sağlanması
- Gizlilik ilkesine saygı gösterilmesi

[5] Bilişim Vakfı, Bilişimcilerin uymaları gereken toplumsal ve mesleki ahlak ilkelerini, uluslar arası çeşitli kurumların hazırladığı bilişim mesleği ile ilgili ahlak kurallarını da dikkate alarak hazırlamıştır.

[6] Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003, s.27

[7] MEDA kapsamında yürütülen "Yargının Modernizasyonu ve Cezaevi Reformu Projesi " çerçevesinde Adalet Akademisi tarafından düzenlenen 5-6-7 Şubat 2007 Tarihinde İstanbul Dedeman Otelinde gerçekleştirilen Adalet ve Bilişim Teknolojileri Sempozyumunda Doç. Dr. Yılmaz YAZICIOGLU tarafından yapılan "AB Uyum Komisyonu Çalışması Türk Mevzuatında Bilişim Suçları" başlıklı konuşma metninden alıntı yapılmıştır konuşmanın tamamı için tıklayınız;
http://www.taa.gov.tr/duyurularana/130606/bilisimsempozyum/sunum/makale.pdf (03.05.2008)

[8] Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003, s.27;

[9] "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. SSS tamamı için tıklayınız http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (03.05.2008)

sık kullanılır olmuş, daha önceki dönemlerde ise SSS' de olduğu gibi "bilişim suçu" yerine "bilgisayar suçu", Fransız Ceza Kanunun etkisi ile "bilgileri otomatik işletime tabi tutan sisteme karşı suçlar" gibi terimler kullanılmakta idi[10]. Gerçekten de bilişim kavramı bilgisayara göre bir üst kavram olup bilişim sistemlerinin en çok kullanılan unsuru bilgisayarlar olduğu için bu tip suçlara bilgisayar suçları dendiğini iddia edenlerde bulunmaktadır[11]. Ancak biz bilgisayarın ağların tanınmasında önce var olması ve bu suçların o aşamada işlenmeye başlanması nedeni ile bilgisayar suçları kavramının yerleştiğini ve daha sonra ağlar üzerinden suç işleme şeklinin çok sık rastlanır hale gelmesi ile bilişim suçları kavramı ihtiyacının kendini hissettirdiğini ve fakat kavramın yerleşmiş olması nedeni ile bilgisayar suçları kavramının bilişim suçları kavramı yerine de kullanılabildiğini düşünmekteyiz.

İlk kez bizim ceza hukukumuzda mevzuat olarak bilişim kavramına 1989 tarihli Öntasarıda rastlanmaktadır. Öntasarının 342. Maddesinde bilişim alanı; bilgileri toplayıp depo ettikten sonra, bunları otomatik işleme tabi tutma sistemlerinden oluşan alan" olarak tarif edilmiştir. Bu tanım aynen daha sonra Eski 765 Sayılı TCK'na 14.06.1991 tarihli değişiklikle eklenen 3756 sayılı Kanunun 21. Maddesinin gerekçesinde de bulunmaktadır[12].

5237 sayılı Yeni TCK'nun 243. Maddesinin gerekçesinde ise "Bilişim sistemi", " Verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir… Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır." Şeklinde tanımlanmış ve artık modası geçmeye başlayan bilgisayar suçları veya sistemi gibi kavramlara yer verilmemiştir[13]. Bu seçim bizce de yerinde bir seçimdir. Zira artık sadece bilgisayarlar ile sınırlı bir ortamdan nicedir LAN ların WAN' ların söz konusu olduğu bir ortamda yaşamaktayız. Evdeki bilgisayarları bir kenara bırakırsak özel ve resmi kurumlarda artık networklar haricinde kalan bilgisayar sayıca oldukça azalmıştır. Sadece veriler bilgisayarlarda işleme tabi tutulmamakta, ağlardan da geçmekte, elektronik ortamda bir trafik yaratmaktadırlar. Bilişim kavramı hem bilgisayarları, hem de bu ağları içine aldığı için bilişim suçları kavramı yerinde bir kavram olarak gözükmektedir.

Artık suçlular uzaktan erişim yöntemi ile ağlar üzerinde suç işlemenin görece kolaylığından faydalanarak suç işlemek için İnternet ortamını seçmeye başlamışlardır.

[10] Yenidünya- Değirmenci'nin çok yerinde belirttiğine gibi; Amerikada halen bilişim suçları yerine bilgisayar suçları (computer crime), bilgisyarla bağlantılı suçlar (computer related crime), bilgisayar yardımlı suç (computer assisted crime) ve bilgisyara karşı suç (crimes against computer) kavramları kullanılmaktadır. Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003, s.30

[11] Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003, s.31

[12] Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003, s.28

[13] http://www.ceza-bb.adalet.gov.tr/ (13.04.2007)

Bu genel gidişatta bilişim suçlarının İnternet ortamında işlenmesi nedeni ile bilişim suçlarının bu kısmına İnternet suçları denmeye de başlanılmıştır.

Adalet Bakanlığı tarafından Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısında ise konu ile yeni tanımların getirildiği görüyoruz. Tasarıda "Bilgi: Verilerin anlam kazanmış biçimini", "Bilgisayar: Belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçları", "Bilişim sistemi: Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi", "Bilişim ortamı: Bilişim sistemi ve bilişim ağından oluşan toplam ortamı", "Çevre birimler: Bilgisayara bağlanabilen, veri saklayıcılarını, veri giriş araçlarını, veri çıkış araçlarını ve veri giriş çıkış araçlarını" biçimlerinde tanımlanmışlardır. Gerekçenin 2. Maddesinde ayrıca Tasarıda yer alan terimlerin özel seçildiği ve özellikle Türkçe anlam ve karşılığına uygun terminoloji tercih edildiği ifade edilmiştir. Örneğin, "İnternet sitesi" yerine "içerik", "İnternet'" yerine bilişim ağlarını da kapsayacak şekilde "bilişim ortamı" terimleri kullanıldığına özellikle vurgu yapılmıştır[14]. Kanaatimizce bilişim sisteminin tanımlanmış olması olumlu bir gelişme olarak değerlendirilebilir ancak diğer terminolojinin bir süre daha tartışılmaya ihtiyacı bulunmaktadır.

Ayrıca bilişim suçları ile ilgili olarak üzerinde durulması gereken bir başka kavram ise siber suç (cyber crime) kavramıdır. Aslında bu terimle de bilişim suçları kastedilmiş olup, nüans olarak ise tek bir bilişim sistemi ile değil birden çok sistem üzerinde yapılan suçlar, özellikle de İnternet üzerinden yapılan suçlar kastedilmektedir[15]. Ancak yukarıda da değinildiği gibi bilişim suçları kavramı Türk hukuk literatüründe tüm bu kavramların üzerinde bir anlamda yerleşmiş gibi gözükmektedir.

3.2 Genel Olarak Bilişim Suçları

Birinci bölümde de belirttiğimiz gibi gelişen BT gelişmelere koşut olarak bilişim suçlarının işlenme sıklığı artmış ve bu suçlar giderek toplum hayatımızda daha çok işlenir ve gündemi işgal eder hale gelmiştir. Sadece etik kuralları ile bu suçların engellenmesinin mümkün olmadığı ve olamayacağı, asıl bu suçların engellenmesinin vicdani olan etik kurallarından çok, Devletin güç kullandığı, otoritesini konuşturduğu ve toplumun düzeni için vazgeçilmez olan cezaî veya idari yaptırımların uygulanması ile sağlanacağı açıktır. Elbette burada tüm suçların cezai yaptırımlarla önlenebileceğini iddia etmiyoruz. Sadece cezai ve idari yaptırımların bu suçların önlenmesinde önemli bir araç olduğunu söylemek istiyoruz.

[14] http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (13.04.2007)
[15] Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003, s.31

Kullanımı giderek artan ve tüm hizmet ve işlemlerin göç ettiği elektronik ortamların güvenliğinin sağlanmasında bu yaptırımların birinci derecede önemi ve yeri olmaktadır. Eğer bu yaptırımlara ilişkin mevzuat sürekli güncellenebilir, gelişen BT devamlı takip edilerek genel hatları ile mevzuata, zamanında ve yeterince tartışılarak ve tüm paydaşların görüş ve önerileri dikkate alınarak aktarılabilirse hukukun elektronik ortamların olabildiğince güvenli hale gelmesinde önemli bir katkısı olacaktır.

Çünkü sık sık konunun uzmanları tarafından dile getirildiği gibi; elektronik ortamların güvenli hale gelebilmesi, İnternet ortamının kişilerin mağdur olduğu yerler olmasından çok, güven içinde haberleşme yapabildikleri, istedikleri bilgilere ulaşabildikleri, kamu ve özel hizmetlere bürokratik engellere takılmadan ve zaman-mekân bağımsız erişebildikleri yerler olması için bilgi güvenliğinin sağlanması şarttır. Bunun için de üç önemli unsurun özellikle ele alınması ve bu konuda çalışmalar yapılması kaçınılmazdır. Üzerinde durulması gereken unsurlardan birincisi; **farkındalık**, ikincisi **teknolojik tedbirler**, üçüncüsü ve sonuncusu da konumuzla ilgili olarak **hukuksal alt yapı**nın oluşturulmasıdır. Bu süreç konunun bilgi güvenliğinin sağlanmasında bir saç ayağı gibi olduğunu kabul etmek ve birini diğerine üstünlüğünden ziyade üçünün aynı anda ele alınması gereken konular olduğunu ve birinin olmadığında diğerlerinin de pek işe yaramayacağını veya eksik kalacağını bilmek gerekir diye düşünmekteyiz.

Özellikle bilgi güvenliğinin sağlanması için şart olan sacayağının birisi olan hukuksal alt yapının parçası veya kısmı da kuşkusuz bilişim suçları ile mücadele ve bu suçların önlenmesidir. Bu nedenle TBD, geçen senenin sonu ve bu senenin başlarından itibaren ülkemizde gündemi daha çok işgal eder hale gelen bilişim suçlarının ele alınmasını gündeme taşımış ve bir çalışma grubu konusu olarak konunun ele alınmasını çok yerinde bir yaklaşımla karalaştırmış ve bu karar sonucu bu konuyu Grubumuz incelemeye çalışmıştır.

Bu bağlamda Raporun bu kısmında bilişim suçlarının genel olarak ortaya çıkış sürecinden ve gelişiminden bahsedilecek, sonrada bilişim suçlarının tanımı, ayırımları, ortaya çıkış şekilleri gibi konulara değinilecektir.

Bilişim Suçları olgusu BT kullanımının ve özellikle de İnternet'in yaygınlaşmasına paralel olarak tüm dünyada ve özellikle A.B.D ve Avrupa ülkelerinde gündeme gelmiş bu alandaki hukuki ve idari yapılanmaların düzenlenmesi için birçok çalışmalar başlatılmıştır. Özellikle bilişim teknolojilerindeki gelişmeler bilgisayar ağları sayesinde ulusal sınırları aşmış, bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmış ve ülkeler arası işbirlikleri ve düzenlemeler gündeme gelmiştir.

Özellikle son yıllarda bilişim suçları kavramı içersinde yer alan “Siber Terörizm”, “Phising” “kredi kartlarının kötüye kullanılması” gibi alt terminolojiler ile ifade edilen bilişim suçları ülkelerin suç gündemlerinde önemli yerler işgal etmeye başlamıştır. “Siber Terörizm” ve “Çocuk Pornografisi” gibi suçlar, özellikle ABD gibi İnternet’in yoğun olarak kullanıldığı ülkelerde önemli oranda artış göstermiş ve bu suçlarla mücadelede yeni yöntemler geliştirilmesi ve geliştirilen bu teknolojilerin bu suçlarla mücadele için kullanılması gerektiği anlaşılmıştır. Bu açıdan bakıldığında ABD’de meydana gelen 11 Eylül Saldırısı özellikle Siber Terörizm konusuna dünya kamuoyunun daha fazla ilgisini çekmiş ve elektronik ortamların kullanılması ile neler yapılabileceği konusunda esef verici de olsa tüm dünyaya bir fikir vermiştir. Global anlamda özellikle ABD başta olmak üzere tüm gelişmiş ve İnternet’i yoğun bir şekilde kullanan diğer ülkeler bu saldırıdan sonra siber terörizm başta olmak üzere bilişim suçları ile mücadele konusuna ajandalarında daha fazla yer verir hale gelmişlerdir.

Önümüzdeki yıllarda da bilişim suçlarında daha da artışlar beklenmekte ve yeni yeni birçok suç türünün ortaya çıkacağı iddia edilmektedir. Yine bu suçların daha organize işlenir olacağı da öngörüler arasında. Hatta artık trendin yaptıkları işin niteliğini bilmeyen 17–18 yaş grubundaki sırf heyecan olsun diye suç işlenen suçluların yerini konunun uzmanı ve bu işi para için yapan profesyonellerin alacağı söylenmektedir. Konunun uzmanları bu genel gidişatın yanı sıra bilişim suçlarında virüslerden, casus yazılımlara doğru gidildiğini ve casus yazılımlarda tehditlerin daha da büyümeye başladığını belirtmekteler. Bir uzman "Artık iş virüsten çok spyware'ye doğru gidiyor. Çünkü çok kolay yayılıyor. Yaşınız, ilgi alanlarınız, hangi sitelere girdiğiniz... Kısacası profiliniz hakkında bilgi toplanıyor ve sonuçta da size bir şeyler satılmaya çalışıyor. Artık ünlü olmak için bu tür işler yapmıyorlar, para kazanmak için yapıyorlar bunları... Tek amaçları kullanıcıların mali bilgilerini ya da şirketlerin kurumsal bilgilerini ele geçirmek" şeklinde konunun vahametini dile getiriliyor.[16]

Yine aynı uzmanlara göre bilişim suçluları en çok arkadaşlık ve çöpçatanlık gibi amaçlarla faaliyet gösteren siteleri kalkan olarak kullanarak saldıracaklar. İnternet’in hızının artması ve kolaylaşması doğrultusunda bunu fırsat bilen korsanlar da yarattıkları zararlı yazılımları toplumsal gruplaşma sitelerinde gizleme yoluna gidecekler.[17] İnternet’te bant genişliklerin artması ve giderek İnternet kullanımın yaygınlaşması bu trende paralel olarak birçok iş ve hizmetin elektronik ortama taşınması da bilişim suçlarının artmasında önemli pay sahibi olacak gibi gözükmektedir.

[16] '2007'de korsanlar arkadaşlık sitelerini hedef alacak'; http://teknoloji.milliyet.com.tr/detay.asp?id=2082 (21.01.07)
[17] '2007'de korsanlar arkadaşlık sitelerini hedef alacak'; http://teknoloji.milliyet.com.tr/detay.asp?id=2082 (21.01.07)

3.3 Bilişim Suçlarının Tarihçesi

Türkiye olarak 2007 yılı ile birlikte daha çok tartışmaya ve daha karşılaşmaya başladığımız bilişim suçları uluslararası alanda, ilk kanun tasarısı olarak Amerika Birleşik Devletleri Kongresine 1977 yılında gelmiş ve kabul edilmiştir. Amerika Birleşik Devletleri, bilgisayarın anavatanı olması nedeniyle bilişim suçlarıyla ilk defa karşılaşan ülke olmuştur. Bunun doğal sonucu olarak hem öğreti hem yasal düzenlemeler hem de uygulamada ABD merkez ülke konumundadır.[18] Diğer birçok ülke gibi ülkemizin de bilişim alanında hukuksal anlamdaki Amerika Birleşik Devletlerinin 1980 li yıllarda yaşadığı süreçleri çok daha sonra 1990 lı yılların sonlarında ve hatta 2000 li yıllarla birlikte yaşamaya başladığımız söylenebilir.

Bilişim suçları konusunda uluslar arası boyutta da bazı çalışmalar yürütülmekte olup bu anlamda en çok bilinen çalışma Avrupa Konseyi'nin Mayıs 2001'de taslağını oluşturduğu, 23 Kasım 2001 de ise imzaya açtığı "Siber Suçlar Sözleşmesi"dir. Sözleşme 26'sı AB Konseyi üyesi toplam 38 ülke tarafından imzalanmıştır[19]. Bu ülkeler arasında ABD, Japonya, Kanada ve Güney Afrika da bulunmaktadır.[20] Bu sözleşme ile özellikle bilişim suçlarına ilişkin tanımlar yapılmış ve hangi eylemlerin Sözleşmeyi imzalayan ülkeler tarafından iç hukuklarına suç olarak aktarma yapacakları belirlenmiş ve bunun da ötesinde Sözleşmeyi imzalayan ve imzalamayan ülkeler arasında nasıl bir işbirliği öngörüldüğü ortaya konulmaya çalışılmıştır. Sözleşmede düzenlenen suçlar özellikle üç kategoride ele alınabilir; bu suçlar yetkisiz erişim, fikri mülkiyet hakları ihlalleri gibi bilişim sistemlerinin araç olarak kullanıldığı suçlar, kötü zararlı kodlar yayma, üretme, DOS atakları, bilişim sistemi sabotajı gibi bilişim sistemlerini hedef alan suçlar ve son olarak da, bilişim sistemleri vasıtasıyla dolandırıcılık, hırsızlık, kimlik hırsızlığı, çocuk pornografisi, hukuka aykırı sanal kumar, İnternet vasıtasıyla işlenen hakaret suçları, klasik suçların bilişim sistemleri vasıtasıyla işlenmesine ilişkin suçlardır.[21]

Siber Suçlar Sözleşmesi uluslar arası alanda savunanlar tarafından bilişim suçları ile mücadelede önemli bir araç olarak görülmüş ve artık bilişim suçlularının, kendilerini dokunulmaz oldukları yönündeki duygu ve düşüncelerini terk etmek zorunda kalacaklarını ifade edilmiştir. Bunun ötesinde Siber Suçlar Sözleşmesinin etkili bir araç olamayacağı yönünde endişeler de bulunmakta olup, özellikle birçok ülkenin bu antlaşmayı imzalamamış olması ve imzalamanın da ülkelerin isteğine bırakılmış olması Sözleşme konusunda şüpheler doğurmakta ve Sözleşme bazı yönleri ile eleştirilmektedir.

---

[18] http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (20.03.07)
[19] http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (03.05.2008)
[20] Kurt, Levent; Tüm Yönleri ile Bilişim Suçları ve TCK'da Uygulaması; Ankara 2005, s.309
[21] http://en.wikipedia.org/wiki/Cybercrime (03.05.2008)

Özellikle şüpheler ve eleştirilerin yoğunlaştığı nokta, bu Sözleşmenin zaten bilişim suçları konusunda Ceza Hukuklarında yaptırım bulunan ve bu konuda görece çok fazla problem yaşamayan ülkelerin Sözleşmeye imza koymaları. Ancak özellikle bilişim suçu işleyenler tarafından portalleri üzerinden siber ataklar yapılan, suçun başladığı ülkeler olarak kullanılan Kuzey Kore, Yemen gibi ülkeler Sözleşmeye taraf olmamakta ve bu konuda mevzuat çıkarmamaktadırlar. Yine Filipinlerde ortaya çıkan "I love you" virüsünü yazan ve yayanlar milyonlarca dolar zarar vermiş olmasına rağmen bu ülkede bu konuları düzenleyen bir mevzuat olmaması nedeniyle cezasız kalmış ve bu fiili işleyenler hakkında cezai takip başlatılamamıştır. [22] Sonuç olarak bu tür ülkeleri bu Sözleşmeyi imzalamaya zorlayan bir hüküm SSS' de yer almamaktadır. Bu bir eksikliktir denmektedir.

Uluslar arası alanda bilişim suçları konusunda yardımlaşma ihtiyacının artması ve bu tür suçların birden çok ülkenin coğrafi sınırlarını kapsaması dikkate alındığında SSS'nin öngördüğü devletlerarası yardımlaşma ve işbirliğinin sağlanması bakımında bu sözleşmenin bir an önce tüm ülkeler tarafından imzalanması ve Sözleşmenin zayıf olan taraflarının düzeltilmesi gerekmektedir. Bu açıdan ülkemiz de biran önce SSS imzalayarak iç hukuka tam olarak adapte etmeli ve özellikle sözleşmenin ilerde bahsedilecek uluslar arası yardımlaşma hükümlerinden azami faydalanmalıdır.

3.4 Hukuk Sistemlerinde Bilişim Suçları

Bilişim suçlarının mevzuatta düzenlenmesine baktığımızda, ilk örnek bir yapı ile karşılaşmıyoruz. Her ülke kendi politikası ve hukuk anlayışına göre düzenlemeler yapmaktadır. Dünyada bilişim suçlarıyla ilgili düzenlemelerde iki ayrı metodun kullanıldığı ileri sürülebilir. ABD, İngiltere, İrlanda ve Portekiz gibi ülkelerin dâhil olduğu birinci sistemde mevcut kanunlardan ayrı olarak yeni ve özel düzenlemeler oluşturulmaktadır. Alman ve İtalyan Ceza Hukuk Sisteminde görülen ikinci sistemde, suç teşkil eden eylemler mevcut kanunun yapısı içinde düzenlenmekte, bilişim suçları için ayrı fasıllar ve kanunlar oluşturulmamaktadır. Bu sistemde örneğin kişisel verilerin ele geçirilmesi kişilere karşı işlenen suçların arasında düzenlenmektedir. Alman Ceza Kanunu suçların ihlal ettiği hukuki yarara göre ilgili bölümde düzenlenme sistemini benimsemiştir. Örneğin belirli bir program içindeki bilgilerin toplandığı ve işlendiği bilgisayar ağına girmek, bu bilgisayarla korunan sırra ulaşmak demek olduğundan bu suç kişiler aleyhinde işlenen suçlar arasında yer alır[23](ACK 202a md). Bilgisayara girilerek, programın bozulması, saklanması, tahrip edilmesi veya değiştirilmesi nası ızrar suçuna vücut verir (md. 303a)[24]. Yine, bilgi toplama sisteminde diğer kurum ve işletmeler için önemli olan bilgilerin tahrip edilmesi, zarar görmesi veya kullanılmaz hale

[22] http://fpc.state.gov/documents/organization/36076.pdf (03.05.2008)
[23] Hilgendorf, Jus, 1996, 509 (512), Schönke/Schröder-Lenckner, § 202a, Par.6
[24] Hören/Sieber-Sieber, Multimedia Recht, Kısım 19, Par. 424

getirilmesi bilgisayar sabotajı olarak mala karşı işlenen suçlar arasında yer almıştır (md. 303b). Bir kimse kendisine veya başkasına yarar sağlamak için bir bilgisayarı yanlış programlaması, yanlış bilgiler vererek bilgisayarın çalışma düzenini etkilemesi dolandırıcılık suçunun bilişim alanındaki halini oluşturacaktır. (md. 263 a). Bilgisayar işletim sistemine girilmek suretiyle hukukça hükmü haiz bir belge sahte olarak veya üzerinde tahrifat yapılarak temin edilir ve bu bilgi kullanıldığı takdirde eylem sahtekârlık olup, hüküm sahtekârlık suçları arasında yer almaktadır (md. 269, 270). [25]

Grubumuz da özellikle 5237 sayılı TCK'nun Alman Ceza kanunundan etkilendiği ve birçok ceza hukuku kurumunun bu ülkeden esinlenilerek alındığı nazara alınırsa bizim TCK daki düzenlemenin de bu ülkenin Ceza hukuku sistemine benzer bir yol tutulması genel ceza hukuku sisteminin bozulmaması açısından daha yerinde bir tutum olurdu düşüncesi genel olarak hâkimdir. Böylece korunan değerlere yönelik herhangi bir ihlal olduğunda, bu ihlal bilişim vasıtasıyla da olsa veya bilişim sistemlerine de yönelik de olsa benzer suçlar arasında bir harmonizasyon meydana gelecek ve uyum bozulmayacaktı. Ancak ne yazık ki hem mülga 765 sayılı, hem de yeni 5237 sayılı Türk Ceza Kanununda, Fransa'daki düzenlemelere paralel bir şekilde bilişim hukukuna ilişkin düzenlemeler ceza kanunu içinde ayrı bir bölümde düzenlenmiştir.

ABD'de ilk defa bilişim sistemleri ile ilgili suçlara odaklanan ve buna ilişkin bir suçu düzenleyen Yasa 1984 yılında "Counterfeit Access Device And Computer Fraud and Abuse Act"[26] (Erişim Araçlarını Taklit Etme, Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu) ile ortaya çıkmıştır. Daha sonra "Credit Card Fraud Act"[27] (Kredi Kartı Sahteciliği Kanunu) yürürlüğe girmiş, bu Kanunda daha sonra 1986 yılında hacking saldırılarını azaltmak amacıyla "Computer Fraud And Abuse Act" (Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Kanunu) ile değişiklik yapılmıştır. Yasa daha sonraları 1994, 1996 ve 2001 yılında çıkarılan ABD Yurtseverlik Yasası (USA Patriot Act) değişikliklere uğramıştır.[28]

Bunlarla birlikte ABD de bilişim suçlarıyla mücadele için daha başka yasal düzenlemeler de mevcuttur; 18. Başlık 1029 Paragraf Kodlu ABD Federal Yasada bilişim sistemlerine erişim cihazlarıyla ilgili sahtekârlık, bu fiille bağlantılı suçlar cezalandırılmıştır. Bu Yasa ya göre İnternet üzerinden parola ve kredi kart numarası ele geçirmek suretiyle yapılan haksız eylemler suçtur. Yasa bu yönde hem donanım kullanılmasını hem de yazılımsal çözümler kullanılmasını yasaklamıştır. Kanun ilk defa

[25] 21. A. Önder, 1994, s. 505
[26] http://law.enotes.com/major-acts-congress/counterfeit-access-device-computer-fraud-abuse-act (03.05.2008)
[27] http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001029----000-.html (03.05.2008)
[28] http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act (03.05.2008)

ihlalde bulunanlara 15 yıla kadar, ikinci ihlallerde ise 20 yıla varan hapis cezaları öngörmüştür.

18. Başlık 1030 Paragraf Kodlu ABD Federal Yasası[29] ise ABD tarafından özel korunmaya değer görülen bilişim sistemleri ile ilgili yetkisiz erişim ve bağlantılı suçlar düzenlenmiştir. ABD tarafından özel korunmaya değer görülen bilişim sistemlerinden kasıt ise Yasaya göre devlet kurumlarında bulunan bilişim sistemleri ile eyaletler arası ticaret faaliyetlerinde kullanılan bilişim sistemleridir. Bu Yasanın uygulanması için ilave bazı suç unsurları aranmıştır. Örneğin ihlalden doğan zarar en az 5000.-$ olmalıdır veya suç ile meydana gelen zarar kamu sağlığına ve ulusal güvenliğe zarar vermek şeklinde ortaya çıkmalıdır. Bu yasa ile aynı zamanda zararlı kod üreten ve yayan faillerde cezalandırılmaktadır. Kanun ilk defa ihlalde bulunanlara 15 yıla kadar, ikinci ihlallerde ise 20 yıla varan hapis cezaları öngörmüştür.

18. Başlık 1362 Paragraf Kodlu "İletişim Hatları, İstasyonları ve Sistemleri" başlıklı ABD Federal Yasasında[30] ise iletişim sistemlerine bilerek zarar verme ve tahrip suçunu düzenlemiştir. Bilgisayar sabotajı diye de isimlendirdiğimiz bu suça teşebbüsü de, yani kalkışmayı da cezalandırmıştır. Bu suçun öngörülen cezası 10 yıla kadar hapistir.

18. Başlık 2511 Paragraf Kodlu "Telli, Sözlü ve Elektronik İletişimin Ele Geçirilmesi ve İfşası" başlıklı ABD Federal Yasasında[31] kablolu veya sözlü ve elektrikli iletişim araçlarını bilerek dinleyen ve de bu cihazları bulunduran kişilerin cezalandırılmasını öngörmektedir.

18. Başlık 2701 Paragraf Kodlu "Hukuka Aykırı Saklanmış İletişime Erişim" başlıklı ABD Federal Yasasında[32] elektronik iletişimin sağlandığı ve buna ilişkin verilerin saklandığı bir tesise yetkisi olmadan ve kasten girenler ve verileri ele geçirenler cezalandırılmıştır.

18. Başlık 2702 Paragraf Kodlu "İçeriğin İfşası" başlıklı ABD Federal Yasasında[33] iletişimin hukuka aykırı olarak dinlenilmesi ve dinlemeden elde edinilen verilerin başkalarına hukuka aykırı verilmesini düzenlemekte ve bu suçları yaptırıma bağlamaktadır.

18. Başlık 2703 Paragraf Kodlu "Yasal Erişim Şartları" başlıklı Kanun da ise bilişim sistemlerine hangi şartlarda yasal mercilerin ulaşabileceği açıklanmış ve bu husus belirli durumlarda mahkeme kararına bağlanmıştır.

---

[29] http://www.cybercrime.gov/1030NEW.htm (03.05.2008)
[30] http://www.cybercrime.gov/1362NEW.htm (03.05.2008)
[31] http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002511----000-.html (03.05.2008)
[32] http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002701----000-.html (03.05.2008)
[33] http://www.cybercrime.gov/usc2702.htm (03.05.2008)

Ayrıca ABD'de bilişim suçları ile ilgili olarak belirtilen mevzuatın yanı sıra; 1986 tarihli "Elektronik Haberleşme Gizlilik Kanunu, 1992 tarihli Bilgi ve Teknoloji Kanunu, Ulusal Bilgi Altyapısı Kanunu, 1998 tarihli Çocukların On-line Yayınlardan Korunması Kanunu, 1997 tarihli İnternet'te Kumarın Önlenmesi Kanunu, 2001 tarihli Anti-Terörizm Kanunu, 1996 tarihli İletişim Ahlâk Kanunu" gibi çok ayrıntılı düzenlenmiş mevzuat da bulunmaktadır.[34]

ABD'de ayrıca 11 Eylül sonrasının psikolojisi ile 26 Ekim 2001 tarihinde kabul edilen ve hukuk devleti ilkeleri ile bağdaşmadığı zaman zaman dile getirilen ABD Vatanseverlik Yasasında da bilişim suçları ile mücadeleye yönelik kimi maddeler yer almakta ve daha önce çıkan yukarıda belirtilen mevzuata göndermeler bulunmaktadır. Bu Yasanın özellikle üzerinde durduğu ve vurgu yaptığı bir konuda "Adli Bilişim" konusudur. Bu Yasa bazı durumlarda iletişimin dinlenilmesi sınırlarını, ABD tarafından korunan bilgisayar kavramının ve yurt dışındaki bilişim sistemlerini de kapsam olarak genişletmiştir. Yasa 342 sayfadan oluşmakta olup tam 15 farklı Yasada değişiklik yapmıştır. Bu Yasa bir tepki yasası olması nedeniyle kamuoyunda yeterince tartışılmaması[35] ve diğer mevzuatta izlenen yolların izlenmemesi nedeni ile ayrıca incelenmeye değer bir Yasa olarak önümüzde durmaktadır. Yasanın bir diğer özelliği de adli bilişimle ilgili araştırma ve delil tespit etme laboratuarlarının da ele alınmış ve bölgesel olarak kurulmasının zorunlu hale getirilmiş olmasıdır.[36]

Fransa'da da Almanya'da olduğu gibi ilk önce bilişim suçları, Ceza Kanunundaki hırsızlık, inancı kötüye kullanma ve dolandırıcılık gibi ihlal edilen baskın değer hangi babda düzenlenmiş ise o babda düzenlenmiş iken daha sonra Fransız Ceza Kanununda 5 Ocak 1988 tarih ve 88–19 sayılı Kanunla ayrı bir bilişim suçlarına ilişkin

---

[34] http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (03.05.2008)

[35] 11 Eylül 2001 tarihinden sadece 45 gün sonra 26 Ekim 2001 tarihinde kabul edilmiştir. http://en.wikipedia.org/wiki/USA_PATRIOT_Act (03.05.2008) http://www.epic.org/privacy/terrorism/hr3162.html(03.05.2008)

[36] Madde metni şu şekilde; "**sec. 816. Development and support of cybersecurıty forensıc capabılıtıes.**
(a) IN GENERAL- The Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability--
(1) to provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyberterrorism);
(2) to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime (including cyberterrorism);
(3) to assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime;
(4) to facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces; and
(5) to carry out such other activities as the Attorney General considers appropriate.
(b) AUTHORIZATION OF APPROPRIATIONS-
(1) AUTHORIZATION- There is hereby authorized to be appropriated in each fiscal year $50,000,000 for purposes of carrying out this section.
(2) AVAILABILITY- Amounts appropriated pursuant to the authorization of appropriations in paragraph (1) shall remain available until expended."

yasal düzenleme yapılmıştır. Bu Yasal düzenleme aslında bizim önceki yani 765 Sayılı TCK da esin kaynağı olmuştur. Bu kanunda suça teşebbüs (madde 462/7) ve iştirak (462/8) gibi genel hükümlerin yanında, SSS kaynaklı, yetkisiz erişim, sistemde haksız yere kalma, bilgisayar sabotajı, verileri değiştirme, yok etme veya başka veri yükleme, sistemin işleyişini engelleme veya bozma, bilgisayar belgelerinde sahtekârlık yapma, böyle bir belgeyi bilerek kullanma şeklinde beş tür bilişim suçu oluşturulmuştur. 1 Mart 1993 tarihinde yürürlüğe giren Yeni Fransız Ceza Kanununda konu, "Mal aleyhine suç ve cürümler" başlıklı birinci kitabın "Mala karşı diğer tecavüzler" başlıklı II. babının "Bilgileri Otomatik İşleme Tabi Tutmuş Sistemlere Yönelik Saldırılar" başlıklı III. faslın içerisinde öncekinden farksız bir şekilde düzenlenmiştir.[37]

Konunun başında da anlatıldığı üzere Alman Ceza hukuku Kıta Avrupa'sı sistemini benimseyerek bilişim suçlarını ihlal edilen hukuki yararlara göre ilgili maddeler içinde düzenlemiştir. Alman Ceza Kanununun 11/3, 176, 176a, 184, 202a, 263a, 269, 271, 274/2, 303a, 303b, 303c maddeleri İnternet'-bilgisayar suçluluğu alanında özel olarak düzenlenmiş maddelerdir. Diğer hükümler ise mevcut kanuni tanımlarda kullanılan terimler itibariyle bu tür suçluluğa da uygulanabilir nitelikte hükümlerdir. Bu hükümlerden 263a[38] maddesi bilgisayar dolandırıcılığı, 269 maddesi ispat gücü olan verileri sahte evrak oluşumuna neden olacak biçimde değiştirme veya değiştirilmiş bilgileri kullanma[39], 270. maddesi verilerin işlenmesinde yanıltma, 271 maddesi dolaylı olarak sahte evrak oluşturma, 274/2 maddesi ispat gücüne sahip verileri başkası zararına silme, gizleme, kullanılamaz hale getirme veya değiştirme, 303a maddesi verilerin değiştirilmesi[40], 303b maddesi bilgisayar sabotajı suçlarını düzenlemektedir [41]. Ceza Kanununun dışında bu konuda düzenleme içeren kanunlar Alman Tele servisler Kanunu madde 6, Fikri Haklar Kanunu madde 106[42], 107[43], 108[44], 108a[45]. Haksız Rekabet Kanunu madde 4, 6c. 17[46]. Telekomünikasyon Müşterilerin Korunmasına İlişkin Tüzük madde 18.; İlaçlar Hakkında Kanun madde 43.; Tütün. Vergisi Hakkında Kanun'un 20. maddesi; Tütün Vergisi Hakkında Kanun'un Yürürlüğüne ilişkin Tüzük madde. 22b. Medeni Kanun madde. 312e, 318 ve 661a. Federal ve Federe nitelikteki çeşitli basın kanunlarının ilgili hükümleri {örneğin BayPrG. Madde 6, 11, Rundf-StV. Madde 3, 32. BayMG. prg. 6, 34, 42. Btx-StV, prg. 9, 15).; Verilerin Korunması

[37] Kurt, Levent; Tüm Yönleri ile Bilişim Suçları ve TCK'da Uygulaması; Ankara 2005, s.103
[38] Schönke/Schröder-Cramer, § 263a, Par. 12, Arloth, Jura 1996, s.354
[39] Tröndle/Fischer, § 269, Par. 7, § 270
[40] Tröndle/Fischer, § 303a, Par.2
[41] Schönke/Schröder-Stree,§ 303b, Par.3
[42] Löwenheim, § 20 Par.4
[43] Schmid/Wirth, § 107 Par. 1
[44] Schmid/Wirth, § 108 Par. 1, 2
[45] Wandtke-Hildebrant §108a Par.2
[46] Köhler/Bornkamm- Köhler, Wettbewerbsrecht, § 17, Par.39

Hakkında Kanun (BDSG)[47], Gençliği Tehlikeye Sokan Yayınlar Hakkında Kanun (GjS)'un[48] ve Gençliğin Toplum İçinde Korunmasına İlişkin Kanun (JÖSchGj'un ilgili hükümleri71)46[49]

3.5 Türk Hukuk Sisteminde Bilişim Suçları

Hukukumuzda bilişim suçları, mülga 765 sayılı Türk Ceza Kanununda 6.6.1991 tarihli ve 3756 sayılı Kanunla yapılan değişiklikle ilk defa düzenlenmiştir. Bu düzenlemeyle mülga 765 sayılı Türk Ceza Kanununa "Bilişim Alanında Suçlar" adıyla 525/a, 525/b, 525/c ve525/d maddelerinden oluşan bir bab eklenmiştir.

5.12.1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 2 inci maddesinde 7.6.1995 tarihli ve 4110 sayılı Kanunla yapılan değişiklikle "Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları" da "eser" sayılarak bilgisayar programlarına yönelik bu Kanun kapsamındaki fiiller de suç sayılmıştır.

23.2.1995 tarihli ve 4077 sayılı Tüketicinin Korunması Hakkında Kanunun 6.3.2003 tarihli ve 4822 sayılı Kanunla değişik 3 nücü maddesinde mal; "elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayri maddi malları" da içerecek şekilde tanımlanmış, 9/A maddesiyle de mesafeli sözleşmelerin "…görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak" gerçekleştirilebileceği, elektronik ortamda yapılan sözleşmelerin teyit işlemlerinin yeni elektronik ortamda yapılabileceği hüküm altına alınmıştır. 15.1.2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 16 ncı maddesiyle imza oluşturma verilerinin izinsiz kullanımı ve 17 inci maddesiyle elektronik sertifikalarda sahtekârlık suç hâline getirilmiş bulunmaktadır.

5237 sayılı Türk Ceza Kanununda bilişim suçları, "Bilişim Alanında Suçlar" başlıklı ayrı bir bölümde 243 ve devamı maddelerinde düzenlenmiş bulunmaktadır. Bu bölümde "bilişim sistemine girme" (m.243), "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (m.244), "banka veya kredi kartlarının kötüye kullanılması" (m.245), ve "tüzel kişiler hakkında güvenlik tedbiri uygulanması" (m.246) düzenlenmiştir. Ayrıca "nitelikli hırsızlık" kenar başlıklı 142/2-(e) maddesinde hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi ve nitelikli dolandırıcılık kenar başlıklı 158/1-(f) maddesinde düzenlenen dolandırıcılık suçunun "bilişim

[47] S. Simitis, BDSG (Kişisel Verilerin Korunması Hakkında Kanun) Kommentar, § 43, Par. 70; Gola/Schomerus, BDSG Kommentar, § 43, Par. 23
[48] Merx-Todler-Hahn, s. 247, Schreibauer, s. 612
[49] Ü. Yener, 2001, s 71

sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi ağırlatıcı neden olarak hüküm altına alınmıştır.

Bilişim Suçları ile ilgili Adalet Bakanlığı tarafından Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı yaklaşık bir buçuk yıllık bir komisyon çalışması sonrasında hazırlanmış ve 28.12.2006 tarihinde Başbakanlığa sevk edilmiştir. Bu Tasarı ile özellikle 5237 sayılı TCK da yer almayan bilişim suçlarını Mevzuatımıza dâhil etmek ve mevcut olan ve ancak yetersiz olduğu ileri sürülen çocuk pornografisi gibi suçların daha etraflı düzenlenmesi ve cezalarının artırılması amaçlanmıştır[50]. Bu tasarı hakkında Raporun ilerleyen bölümlerinde daha geniş bilgi ve yorum bulabilirsiniz.

Ek-1'de 765 Sayılı TCK, 5237 sayılı TCK ve Adalet Bakanlığı tarafından hazırlanan Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısında bulunan veya bulunmayan bilişim suçları karşılaştırmalı olarak verilmiş ve bir tablo halinde sunulmuştur. Ek–2 de ise 5237 sayılı TCK'nun 6. Maddesine atıfta bulunulan İnternet ortamını da kapsayan basın yayın yolu ile işlenebilecek olan suçların tablo halinde bir listesi verilmiştir.

3.6 Bilişim Suçlarının Sınıflandırılması

Yenidünya- Değirmencinin çok yerinde belirttiğine gibi; bilişim suçlarının ilk ortaya çıktığı ve önemli gelişmeler gösterdiği Amerika'da halen bilişim suçları yerine bilgisayar suçları (computer crime), bilgisayarla bağlantılı suçlar (computer related crime), bilgisayar yardımlı suç (computer assisted crime) ve bilgisayara karşı suç (crimes against computer) kavramları kullanılmakta ve bilişim suçları bu şekilde kategorize edilmektedir. Yukarıda ABD'de mevcut olan Mevzuattan bahsedilirken de belirtildiği gibi bilişim suçları ile ilgili suçlara ilişkin yasaların adlarının belirlenmesinde bu kategorilerin de etkisi hissedilmektedir[51].

SSS' de de düzenlenen suçlar özellikle üç kategoride ele alınmaktadır. Bu kategorilerden birincisi; yetkisiz erişim, fikri mülkiyet hakları ihlalleri gibi "bilişim sistemlerinin araç olarak kullanıldığı suçlar", ikincisi kötü zararlı kodlar yayma, üretme, DOS atakları, bilişim sistemi sabotajı gibi "bilişim sistemlerini hedef alan suçlar" ve son kategori de, bilişim sistemleri vasıtasıyla dolandırıcılık, hırsızlık, kimlik hırsızlığı, çocuk

[50] Tasarıda amaç şu şekilde ifade edilmiştir;" Tasarı ile, ülkemizde kullanımı yaygınlaşan bilişim ağlarının ortaya çıkartmış olduğu hukukî ve cezaî sorunların çözüme kavuşturularak bilişim ağı alanında hukuk sistemimizin Avrupa Birliği normları ile uyumunun sağlanması amaçlanmıştır."
http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (13.04.2007)

[51] Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003, s.30

pornografisi, hukuka aykırı sanal kumar, İnternet vasıtasıyla işlenen hakaret suçları, klasik suçların bilişim sistemleri vasıtasıyla işlenmesine ilişkin suçlardır.[52]

Rapor kapsamında bilişim suçlarından örnekler verirken Mevzuatımızdaki bilişim sistemleri olmaksızın işlenemeyecek olan bilişim suçlarını doğrudan bilişim suçları olarak ele almayı uygun gördük[53].

3.7 Bilişim Sistemlerine Yetkisiz Erişim

Sistemin bir kısmına, bütününe, bilgisayar ağı veya içerdiği verilere, programlara; yine programlar, casus yazılımlar veya virüsler vb. ile ulaşma anlamındadır. Günümüzde özel hayatın gizliliğinin korunması için kanunlarda gerekli müeyyideler konulması ile birlikte dinlemeler, erişimler izinsiz özel ve şirket bilgisayarlarına ve sistemlerine girmek suç olarak kabul edilmiştir.

Günümüzde telefon dinlemeleri veya kişilerin özel mülklerine girmek nasıl savcı izni olmadan mümkün olmamakta ise yine kişiler veya kurumlar arası haberleşmenin bilgisayar üzerinden dinlenmesi veya izinsiz verilerin alınması da kişi özel alanlarına ya da kişilerin şahsiyetlerine taciz olarak kabul edilmekte ve suç oluşturmaktadır. Ülkemizde bu konuda TCK'nin (Türk Ceza Kanunu) 243. maddenin 1. 2. ve 3. fıkrasında açıkça belirtilmiştir.

5237 Sayılı TCK'nun 243. Maddesinin birinci fıkrası hukuka aykırı olarak bir bilişim sisteminin tamamına veya bir kısmına girmeyi ve orada kalmaya devam etmeyi suç saymıştır ve bir yıla kadar hapis veya adli para cezası öngörmüştür. Maddenin ikinci fıkrası bu yetkisiz erişimin bedeli karşılığı yararlanılan bilişim sistemi olması halinde cezanın yarı oranında azaltılacağı, üçüncü fıkrası ise bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasının hükmolunacağı açıklanmıştır. 5237 sayılı TCK'nun 243. Maddesinin 3. Fıkrası aslına yetkisiz erişim sırasında taksirli de olsa bir veri kaybından bahsetmektedir. Bu fiil

[52] http://en.wikipedia.org/wiki/Cybercrime (03.05.2008)

[53] "Ancak, doktrinde ve uygulamada, bilişim suçları kavramı ile bu suçların neleri kapsayacağı hususu hep tartışma konusu olmuştur. Bilişim suçlarının, bilişim alanının doğurduğu yeni hukukî yararlara karşı gerçekleştirilen «dar anlamda bilişim suçları» ve klâsik suçların bilişim olanakları marifetiyle gerçekleştirilmesi olarak karşımıza çıkan «geniş anlamda bilişim suçları» olarak ikiye ayrıldığı bilinmektedir. Yine gerçek bilişim suçları olarak adlandırılan birinci suç grubu da, "bilişim sistemlerine izinsiz girilmesi" (m.243), "bilişim sistemlerindeki verilere müdahalelerde bulunulması" (m.244), "bilişim sistemleri marifetiyle haksız menfaat temini" (m.244/4) gibi bilişim sistemlerinin özelliğinden kaynaklanan ve yeni hukukî yarar alanlarında gerçekleştirilen doğrudan bilişim suçları ya da dar anlamda bilişim suçları şeklinde adlandırılan gerçek bilişim suçları ve bilişim teknolojilerinin getirdiği imkânlar dolayısıyla ortaya çıkan "haberleşmenin gizliliğini ihlâl" (m.132), "haberleşmenin engellenmesi" (m.124), "eğitim ve öğretimin engellenmesi" (m.112), "kamu kurumu veya kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinin engellenmesi" (m.113), gibi dolayısıyla bilişim suçları diye de ikiye ayrılmaktadır." MEDA kapsamında yürütülen "Yargının Modernizasyonu ve Cezaevi Reformu Projesi " çerçevesinde Adalet Akademisi tarafından düzenlenen 5-6-7 Şubat 2007 Tarihinde İstanbul Dedeman Otelinde gerçekleştirilen Adalet ve Bilişim Teknolojileri Sempozyumunda Doç. Dr. Yılmaz Yazıcıoglu tarafından yapılan "AB Uyum Komisyonu Çalışması Türk Mevzuatında Bilişim Suçları" başlıklı konuşmadan alıntı yapılmıştır konuşmanın tamamı için tıklayınız;
http://www.taa.gov.tr/duyurularana/130606/bilisimsempozyum/sunum/makale.pdf (03.05.2008)

nedeniyle sistemin içerdiği veriler yok olur veya değişirse, demek suretiyle mevzuatımızda ilk defa bilişim suçlarıyla ilgili olarak taksirle işlenebilecek bir suç tanımlanmış olmaktadır.

5237 S TCK 243. Maddesinin 1. Fıkrası öncelikle ve bağlacı yerine veya bağlacı kullanılması ile eleştirilmektedir. Çünkü ve bağlacı sadece girmeyi değil, bir bilişim sistemine girmeyi ve bir süre orada kalmayı zorunlu kılmaktadır. Uygulamada yaşanacak olan sıkıntı ise fail ne kadar hukuka aykırı olarak girdiği sistemde kalırsa suçu işlemiş olacaktır belli değildir. Bu zaman belirsizliği önümüzdeki günlerde büyük olasılıkla Yargıtay tarafından içtihatlarla bir şekilde açıklığa kavuşturulacaktır. Ancak Yasanın bu önemli ayrıntıyı içtihatlara bırakmış olması kanımızca yerinde olmamıştır. Kanunu hazırlayan akademisyenler tarafından bu maddeye zaman ölçütünün konulmasının sebebi bu maddenin ihlali ile mahkemelerin iş yoğunluğu altında kalmamalarının sağlanması şeklinde açıklanmıştır.

5237 S TCK 243. Maddesinin 1. Fıkrasında yaşanması muhtemel ikinci sıkıntı ise fail bir bilişim sistemine hukuka uygun olarak girmiş ve fakat girdikten sonra belirli bir aşamadan sonra bu yasal giriş hukuka aykırı hale gelmiş ise o zaman ne olacaktır? Çünkü fıkra hukuka aykırı olarak girmeyi ve orada bir süre kalmayı suçun unsuru olarak ön görmüştür. Hukuka uygun girişin hukuka aykırı hale gelmesini düzenlememiş ve bağlacı ile bu yolun önünü kesmiştir. Bu nedenle "ve" bağlacının "veya" olarak düzeltilmesi gerekmektedir.

Nitekim Kanunun kaynak aldığı SSS'nin "Yetkisiz Erişim" başlıklı 2. Maddesi; "Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır." diyerek bir bilişim sistemine hukuka aykırı girmeyi düzenlemekle birlikte orada bir süre kalmayı öngörmemiştir.

SSS ayrıca taraf ülkelerin söz konusu suçu, bilgisayar verilerinin elde edilmesi amacıyla veya sahtekârlığa yönelik başka bir amaçla güvenlik sisteminin ihlal edilmesi şeklinde veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabileceklerini hükme bağlamıştır. 5237 S TCK da bu ikinci cümle nazara alınmış ancak örneğin ACK' nun düzenlemesi bu cümleye paralel olarak 202a maddesinde ancak asgari bir güvenlik önlemi alınmış bir sisteme girilerek veriler ele geçirilirse o zaman yetkisiz erişim suçu oluşması yönündedir.

5237 Sayılı TCK herhangi bir veri veya bilgi alınmadan da olsa "sırf yetkisiz erişimi" cezalandırmıştır. Bu yönüyle hem Eski 765 S. Türk Ceza Kanunun ve hem de ACK' nun 202a maddesinin ilerisinde bir düzenleme getirmiştir.

5237 STCK nun eleştirilen bir yönü de 2. Fıkradaki yetkisiz erişimin bedeli karşılığı yararlanılan bilişim sistemi olması halinde cezanın yarı oranında azaltılacağı hükmüdür. Kanun koyucunun bu hükmü neden koyduğuna ilişkin madde gerekçesinde bir açıklama görememekteyiz. Ancak kanaatimize göre Kanun koyucu burada bedel karşılığı bilişim sistemi işleten kurum ve kuruluşların bilişim sistemlerini hem yazılımsal, hem de donanımsal olarak daha fazla güvenlik önlemleri alarak korumaları ve zaten bu işi yaparak para kazandıkları için buradan gelecek zararları daha çok tazminat yolu ile almaları yönünde bir eğilim taşımıştır. Ancak bu sebeple veya sosyal devlet anlayışı gibi başka bir sebeple olsun böylesine bir ayrım kanaatimizce hem yerinde hem de hakkaniyetli olmamıştır.

Günümüzde bilişim sistemleri kullanan veya özellikle ağ yöneten kişilerin bekli de yaptıkları fiilin hukuksal alandaki karşılığını bilmeden veya bilerek işleyebilecekleri veya karşılaşabilecekleri suç 243. Maddede düzenlenen yetkisiz erişim suçudur. Ancak Türk Ceza Hukuku uygulamasında kamuoyuna bu suçlar zaman zaman çeşitli şekillerde yansısa da henüz adli davalar arasında bu suç türü ciddi boyutlara ulaşmamıştır. Sırf yasaya aykırı bilişim sistemine girme suçu yaptırım altına alındığı gözönünde bulundurulduğunda bugün bir çok bilişimci bu suçun gizli potansiyel faili durumundadır. Çünkü birçok sistem yöneticisi veya ağ kullanıcısı bir arkadaşının hatırına veya merak saikiyle bir üst düzey amirinin maaşına bakmak, mesai arkadaşının kişisel verilerine bakmak veya merak ettiği bir kişinin bilgisayarında neler var, hangi siteleri ziyaret etmiş, msn de neler konuşmuş gibi sebeplerle girebilmekte ve bu her bir girişte sonuç alamasa da aslında en azından TCK 243. Maddede düzenlenen yetkisiz erişim suçunu işlemiş olmaktadır.

3.8 Bilişim Sistemleri Sabotajı

Doğrudan veya dar anlamda bilişim suçu olan Bilişim Sistemi sabotajı iki şekilde karşımıza çıkmaktadır. İlk şekli; bilgisayar teknolojisi kullanarak sistemine sızılan bilişim sistemindeki verilerin silinmesi, yok edilmesi ve değiştirilmesi biçimindedir ki buna “veri sabotajı” da denmektedir. İkinci şekli ise hedef alınan sisteme uzaktan erişerek değil de bilakis fiziksel zarar vererek ya da sistem başında bulunarak bilgisayardaki bilgileri silmek, yok etmek veya değiştirerek zarar verilmesi yani “bilişim sistemi sabotajı suçu”dur. Burada önemli olan mala verilen zarardan ziyade içindeki bilgilere verilen zarar önem arz eder. Yetkisiz erişimin aktif sahası olarak da nitelendirilen “Bilgisayar Sabotajı”, yalnız sisteme erişimle kalmamakla birlikte, eriştiği bilişim sisteminin içerdiği bilgileri silme veya değiştirme olarak ifade edilmektedir.

Bir bilişim sistemine yetkisiz erişim sağlayanlar; sadece eriştiği bilgileri incelemekle, kopyalamakla kalmamakta, bu bilgileri değiştirmekte ve silmekte ise veya bu bilgileri kanun dışı kullanmak isteyenlere vermekte ise, veri sabotajı suçunu işlemiş

olmaktadırlar. 5237 sayılı TCK'nun 244/1. ve 2. maddeleri bu tür suçları düzenlemektedir.

5237 S. TCK'nun 244. Maddesinin 1. Fıkrası; "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır." hükmünü içermekte ve "bilgisayar sabotajı" suçunu tarif etmektedir.

5237 S. TCK'nun 244. Maddesinin 2. Fıkrası ise ; "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır." demek suretiyle veri sabotajı suçuna iç hukukumuzda yer vermektedir.

Aslında bu düzenlemenin kaynağını oluşturan SSS Madde 4'de de paralel şekilde "Verilere Müdahale", madde 5'de ise "Sistemlere Müdahale" suçları düzenlenmiştir. Dördüncü maddenin birinci fıkrasında "Verilere Müdahale"; "Taraflardan her biri, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiillerinin, kasıtlı olarak yapıldıklarında kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır." şeklindedir ve 5237 Sayılı TCK'nun 244. Maddesi incelendiğinde aradaki benzerlik hemen dikkat çekecektir.

Ancak SSS Madde 4'ün 2. Fıkrasında "verilere müdahale" suçunun özel bir halini şu şekilde düzenlemiştir; "Taraflar, yukarıda Paragraf 1'de tanımlanan fiili, söz konusu fiilin ciddi zararla sonuçlanması şartına bağlama haklarını saklı tutabilirler" şeklindeki tavsiyeye ülkemiz Kanun Koyucusu itibar etmemiş ve bu yönde madde metnine ek yapılmamıştır. Kanaatimizce bu yönde yapılacak bir düzenleme, özellik arz eden fiillerle, sıradan eylemler arasında veya fiilin meydana getirdiği zarar gözetilerek ceza verilmesinin sağlanması ile hakkaniyeti sağlamak açısından yararlı bir düzenleme olabilirdi.

SSS Madde 5'de ise "Sistemlere Müdahale" suçları; "Taraflardan her biri, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.

Verilere müdahale veya veriler sabotaj suçunun en çok karşılaşılan ortaya çıkış şekilleri Virüsler, Wormlar ve Zombiler gibi kötü amaçlı olarak yazılmış kodlardır. Bu tür kötü amaçlı yazılmış kodlar, başkalarına zarar vermediği sürece Mevzuatımız tarafından suç sayılmamaktadır. Fakat bu tür kodlar; bilgisayar veya bilişim sistemleri veya bileşenlerine intikal eder ve oradaki verilere zarar verirse artık bunlar suç teşkil

ederler. Yoksa sırf kod yazımı mevcut Mevzuatımıza göre saikten öte bir anlam ifade etmemektedir.

Ancak SSS Madde 6 da bu yönde taraf ülkelere tavsiye bulunmaktadır. Madde 6 gerek yetkisiz erişimi düzenleyen Madde 2 ile Madde 5 arasında kalan verilere müdahale, sistemlere müdahale gibi suçların işlenmesine yönelik üretilmiş kodların ve donanımların tedarikinin, elde edilmesinin, elde bulundurulmasının cezalandırılmasını tavsiye etmektedir. Taraflar, alacakları önlemlerde, cezaî sorumluluk doğması için söz konusu unsurlardan belli bir sayıda elde bulundurulması şartını da getirebileceklerdir.

Ancak madde 6'nın 2. Fıkrası ise istisnaları saymakta ve örneğin, bir bilgisayar sisteminin yetkili kişilerce test edilmesi veya korunması amacıyla bu yazılım veya donanımların yapılmasını ve elde bulundurulmasını cezaî yükümlülük doğurur şekilde yorumlanmamasını önermektedir[54].

3.9 Bilişim Sistemleri Vasıtasıyla Dolandırıcılık

Günümüzde İnternet'in yaygınlaşması, bilgisayar ve iletişim teknolojilerinin gelişmesi eğitimden ticarete, devlet sektöründen özel sektöre, eğlenceden alışverişe kadar yaşamın her alanında bilgisayarların daha yaygın ve etkin bir şekilde kullanılmalarına neden olmuştur. Bugün kişiler, İnternet üzerinden, e-posta hizmetleri, e-bankacılık, e-alışveriş gibi konuları çok rahat bir şekilde halledebilmektedir.

Ancak yaşamı kolaylaştıran teknoloji, bir kısım kötü niyetli insanların elinde kötü amaçlar için kullanılmakta ve iyi niyetli kişilerin teknoloji kullanılmak suretiyle tuzağa düşürülmelerine ve istekleri dışında bazı bilgi ve şifrelerin kendilerinden temin edilerek maddi yönden sömürülmelerine sebebiyet vermektedir.

Dolandırıcılık genel bağlamda "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamaya" denmektedir. Bilişim vasıtasıyla "Dolandırıcılık" ise; "bilgisayar veya iletişim araçlarıyla kişileri şaşırtma, aldatma, kandırma" olarak tarif edilebilir.

Bilgisayar Yoluyla Dolandırıcılık suçu; Kredi kartlarının bir benzerinin yardımcı programlarla oluşturulması yetkisiz ve izinsiz erişilen bilgilerin kopyasını almak şeklinde Finans bilgilerinin tutulduğu programlarla yapılan değişiklik ile istenilen kişinin hesabına istenildiği kadar para aktarmak suretiyle kişiler arasında mali alışverişi olan kişilerin adına mail vs. şeklinde iletişim kurarak; kişileri kandırarak, işlenmektedir. Ülkemizde bu tür suçlar 5237 S. TCK'da 158. maddenin (1). Fıkrasının (f) bendinde ve 244.maddenin (3).fıkrasında ve 245.maddesinin (1). Fıkrasında hüküm altına alınmıştır.

[54] SSS; **Madde 6 – Cihazların Kötüye Kullanımı**

Bilgisayar Yoluyla Dolandırıcılık; kredi kartlarının bir benzerinin yardımcı programlarla (Card Generator vb.) oluşturulması ile yetkisiz ve izinsiz erişilen bilgilerin kopyasını almak şeklinde, finans bilgilerinin tutulduğu programlarla yapılan değişiklik ile istenilen kişinin hesabına istenildiği kadar para aktarmak suretiyle ve kişiler arasında mali alışverişi olan kişilerin adına mail vs. şeklinde iletişim kurarak; kişileri kandırarak işlenebilmektedir.

TCK. 158.maddenin (1). Fıkrasının (f) bendinde dolandırıcılık suçunun **bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi** nitelikli dolandırıcılık kabul edilerek, dolandırıcılık suçunun temel şekline göre cezanın artırılmasını gerektiren nitelikli bir unsuru olarak kabul edilmiştir. Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsiden, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir.

5237 S. TCK. nun 245. maddesinin 1 ve 3 üncü fıkralarında ise Mevzuatımızda ilk kez dolandırıcılık suçunun özel halini düzenleyen banka ve kredi kartlarının kötüye kullanılması şeklinde dolandırıcılık suçunun işlenmesi ile ilgili hükümler bulunmaktadır [55]. 765 S. TCK ise bu suç daha çok 525b maddesinde belirtilen bilişim sistemleri aracılığı ile yarar sağlamak suçu içersinde değerlendiriliyordu. Örneğin Yargıtay 11. Ceza Dairesi bir kararında ; "Hükümlünün haksız olarak ele geçirdiği müştekiye ait kart ile şifreyi kullanarak para çekme makinesindeki kredi hesabından para çekmesi suretiyle oluşan suç için; süreklilik gösteren Dairemiz içtihatları ve YCGK. nun 11.4.2000 gün ve 2000/6–62–72 sayılı kararında belirtildiği gibi TCK. nun 525/b–2.madde ve fıkrası yerine aynı Yasanın 491/3 maddesi ile (yani hırsızlık suçu olarak) ceza tayini yasaya aykırıdır." demek suretiyle konuya açıklık getirmeye çalışmıştır[56]. Bu içtihat aslında Yeni 5237 S. TCK yürürlüğe girmesine kadar istikrar kazanarak genel uygulama halini almıştı.

Kararda geçen Mülga 765 S. ETCK' nun 525b maddesinin ikinci fıkrasında; "Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimse" ibaresi geçmekte olup kredi kartını kötüye kullanan kişinin bilişim sisteminden yararlanarak kendine yarar sağlaması bu kapsamda değerlendirilmekte idi. Bu maddenin benzer bir karşılığı 5237 S. YTCK da

[55] 5237 S.TCK **Madde 245 -** (Değişik madde: 29/06/2005-5377 S.K./27.mad)

[56] Yargıtay 11.C.D. 6.2.2001 tarih ve 2000/5573-2001/991 sayılı Kararı. Kararın Özeti için Bkz. http://www.hukukcu.com/bilimsel/kitaplar/bilisim_İnternet_suclari.htm (14.04.2007)

bir fıkra yer almakla birlikte artık 5237 S. YTCK da 245. Madde tamamen kredi kartların kötüye kullanılması suçlarına ayrılmış olması kredi kartları bakımından bu fıkranın artık pek gündeme gelmeyeceği söylenebilir.

Anılan 244. Maddenin son fıkrası; **"Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur"** şeklindedir.

Elektronik ortamdaki bilgisayar dolandırıcılığı olarak kullanılan yöntemlerden en sık rastlananlar hacking, Phising, keylogger, screnn logger ve pharming gibi yöntem başlıkları altında incelenebilir.

Hacking yönteminde; elektronik ortamda kart ve müşteri bilgileri daha önce bilgisayara yerleştirilen virüs programlarla hackerlerin eline geçmektedir. Bankalar önlem olarak sanal klavye kullanma yolunu seçmişlerse de hackerler yeni geliştirdikleri ekran kopyalama usulü ile sanal klavyelerin şifrelerini de çözebilmektedirler.

Yakın bir geçmişte gerçekleşen bir olayda hacking yöntemi şu şekilde gerçekleştiği ileri sürülmüştür; failler genç bir kadının cep telefonu hattını da bloke ederek bir şirkette çalışan İF'ye e-mail yoluyla gönderdikleri virüslü program aracılığı ile atıp kendisine ait tüm bilgileri ele geçirirler. Daha sonra İF'ye ait cep telefonu hattını bloke eden dolandırıcılar, özel cep telefonu şirketine giderek bloke olan hat için yeni bir kart alırlar. Ardından, Fanin eşi ile ortak kullandığı 31 bin TL'lik parayı, değişik illerde bulunan iki ayrı banka şubelerinden kendi hesaplarına gönderen failler, para transferi için arayan banka görevlilerine de çıkardıkları yeni hattan onay verirler. Durumu fark eden F, savcılığa giderek hem banka hem de cep telefonu şirketi hakkında şikâyetçi olur[57]. Bu olayda da görüldüğü üzere failler muhtemelen TCK 158. Maddesinin 1. Fıkrasının "f" bendinde yer alan "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlama" suçunu bilişim sistemleri vasıtasıyla işleme suçunu işlemiş gözükmektedirler. Failler F'ye karşı hileli davranışlarla F'nin zararına, kendi yararlarına belirtilen eylemleri gerçekleştirmiş gözükmektedirler. Eğer bu eylemler bilişim sistemlerindeki otomatiğe edilmiş programlar yanıltılarak veya verilerin manipüle edilmesi ile gerçekleştirse idi o zaman TCK'nun 244. Maddesinin 4. Fıkrasındaki suçu oluşturması gündeme gelebilirdi.

Diğer bir yöntem Balık avlama yöntemi de denilen Phising (avlama) ve fake-mail (sahte elektronik posta) yöntemleridir. İngilizce "Balık tutma" manasındaki "Fishing" sözcüğünün "f" yerine "ph" konulmasıyla oluşturulmuş bir bilişim terimi olan Phising yöntemi sahte posta (fakemail) ile hedef kullanıcıya ulaşarak yapılmaktadır.

[57] http://www.bugun.com.tr/haberler/180407/p45737.html (20.04.2007)

Dolandırıcıların rasgele kullanıcı hesaplarına milyonlarca elektronik ileti gönderdikleri bir online saldırı türüdür. Elektronik iletiler, bilinen İnternet sitelerinden veya kullanıcın bankasından, kredi kartı şirketinden, e-mail ya da İnternet hizmeti sağlayıcısından gönderilmiş gibi gösterilerek, genellikle hesapları güncelleyebilmek için kredi kartı numarası veya şifre gibi kişisel bilgilere şirketin ihtiyaç duyduğunu bildirilen mesajlar gönderilerek gönderilen kişinin kredi, ATM kart numaraları (şifreleri, güvenlik kodları) , genel bağlamda şifreler veya parolalar, hesap numaraları, İnternet bankacılığında kullanılan kullanıcı adı ve şifreleri vs. ele geçirilebilmektedir. İnteraktif bankacılık hesaplarında güncelleme ve/veya güvenlik ayarlarını yapmalarını istemekte ve e-posta gönderisinde bankanın İnternet adresine benzeyen fakat farklılıkları bulunan bir link vererek buradan sisteme giriş yapabilecekleri belirtilmektedir. İlk bakışta herhangi bir bankadan gönderildiği düşünülen bu elektronik iletiyi alan kullanıcılar istenilen güncellemeleri yapmak üzere belirtilen adrese tıklarlar ve karşılarına ilgili banka sayfasına çok benzeyen bir sayfa geldiğinden herhangi bir şüpheye düşmeden istenilen bütün bilgileri verirler ve bu bilgiler anında dolandırıcılık faillerine aktarılmış olur. Bu yöntemde genelde, gerçek kuruluşların doğrudan meşru İnternet sitelerinden alınan ve gerçek gibi görünen logolar ve diğer tanımlayıcı bilgiler kullanılır.

Dolandırıcıların yaygın olarak kullandığı bir başka teknik de, ilk bakışta tanınmış bir şirket adı gibi görünen, ama kasti olarak harfler eklemek, çıkarmak veya sırasını değiştirmek yoluyla değiştirilen bir Tekdüzen Kaynak Konum Belirleyicisi (URL) kullanmaktır. Örneğin, "www.Microsoft.com" URL'si yerine aşağıdakiler görünebilir: www.micosoft.com, www.mircosoft.com, www.verify-microsoft.com. Bu teknik yaygın olarak kullanılma eğilimindedir ve dolayısıyla dikkatli olunmalıdır.

Bazen de yarışma olduğunu ya da e-kart geldiğini söyleyerek gerekli formların doldurulması sağlanmak suretiyle “Phising” yapılmış olur. Bu tür olaylar sonrası Savcılıklara yapılan müracaatlarda bilirkişi tayini söz konusu olmakta bu yüzden bu suçu işlemek amacıyla gönderilen e-postaların silinmemesi ya da bu konuda karşı tarafın bilgi sahibi olmaması gerekmektedir. Aksi takdirde delillerin yok olması mümkündür. Uluslararası bağlamda; bu tür suça hazırlıksız yakalan ülkeler yeni kanun tasarılarıyla “Phising” yoluyla dolandırıcılığı özel bir suç olarak kabul etmeye yönelik çalışmaları sürdürmektedirler. Örnek olarak; ABD’li hukukçular bu konuda “The Anti-Phising Act” olarak adlandırdıkları kanun tasarısı ile büyük finansal kayıplara yol açan sahte elektronik posta eylemleri ve bilişim suçlarının önlemek istemektedirler. Örneğin ABD bu konuda Anti Phising Kanun Tasarısı 2005 yılında hazırlanmıştır. Bu Tasarının uzun adı “Hileli Yollarla Kişisel Verilerin Ele Geçirilmesi de Dâhil Olmak Üzere İnternet Dolandırıcılığını Cezalandırmak Amaçlı Tasarı”dır. Tasarının amacı giderek yaygınlaşan dolandırıcılık amaçlı kimlik hırsızlama ve yanlış İnternet ve e-posta

sayfalarına yönlendirme anlamına gelen Pharming suçlarını genel bilişim suçlarından ayırarak daha ayrıntılı hükümlere tabi kılmak ve cezalarını arttırmaktır. Tasarıya göre bu suçlarda failler ABD'de 5 yıla kadar hapis cezaları alabileceklerdir[58]. Özellikle ülkemizde de artan Phising yöntemiyle işlenen dolandırıcılık suçlarının öneminin artması nedeni ile yeni hukuki düzenlemelerin yapılması gereksinimi açıkça ortaya çıkmaktadır.

Ülkemizde bilişim sistemleri vasıtasıyla suçlara yönelik kanunlarda dolandırıcılık suçlarında TCK'nin 157. Maddesi ve 158/1 inci maddesinin f bendi hükümlerinin uygulanılabilirliği söz konusudur.

Ancak, bu suçların bilişim ağları yani İnternet kullanılarak işlenmesi halinde 5237 S. TCK'nun 244. Maddesinin 4. Fıkrası gündeme gelebilecektir[59]. Zira 5237 S TCK'nun 157. maddesi sadece hileli davranışlarla bir gerçek kişiyi aldatmayı dolandırıcılık olarak tanımlamış, 158. Maddenin 1. Fıkrasının f bendi ise bu tanıma dayanarak bu suçun bilişim sistemleri vasıtasıyla işlenmesini düzenlemiştir. Dolaysı ile insan unsurunun olmadığı, otomatize edilmiş bir program vasıtasıyla dolandırıcılık suçu işlenirse yani yanıltma bilişim sistemi tarafından gerçekleştirilirse o zaman dolandırıcılık suçunun unsurları olayda gerçekleşmediğinden fail 244. Maddenin 4. Fıkrası gereği cezalandırılması gündeme gelebilecektir[60].

Nitekim Yazıcıoğlunun da çok yerinde değindiği gibi; "… Dolandırıcılık suçunun oluşabilmesi için suç mağduru kişinin iradesinin hile ve desise sonucu kandırılması, etkilenmesi gerekmektedir, hâlbuki eylem bir bilgisayara, bir bilişim sistemine karşı gerçekleştirildiğinde bilgisayarın iradesi diye bir şey söz konusu olamayacağından yani ortada etkilenen bir irade bulunmayacağından eylem dolandırıcılık suçunu değil ve fakat bilgisayar marifetiyle haksız menfaat sağlaması suçunu oluşturacaktır. Fiil, eğer, banka kartı veya kredi kartı kullanmak suretiyle bir bilişim sistemi kullanılmaksızın, örneğin slip makinelerinin kullanılması gibi, mağdurun iradesini etkileyecek surette hile ve desise söz konusu olursa, bu takdirde fiil bir bilişim sistemine karşı işlenmiş olamaz, zira daha henüz bir bilgisayara veri yüklemek veya mevcut verileri manipüle etmek söz konusu olmamıştır bu sebeple burada sadece mağdurun iradesi etkilendiğinden dolandırıcılık suçu söz konusu olacaktır."[61]

---

[58] http://en.wikipedia.org/wiki/Anti-Phishing_Act_of_2005 (14.04.2007)

[59] 5237 S. TCK 244/1-f; "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur"

[60] Bilişim Suçları; Adalet Bakanlığı Hakim ve Savcı Adayları Eğitim Merkezi, Panel 28 Şubat 2001, Ankara; s.12

[61] MEDA kapsamında yürütülen "Yargının Modernizasyonu ve Cezaevi Reformu Projesi " çerçevesinde Adalet Akademisi tarafından düzenlenen 5-6-7 Şubat 2007 Tarihinde İstanbul Dedeman Otelinde gerçekleştirilen Adalet ve Bilişim Teknolojileri Sempozyumunda Doç. Dr. Yılmaz YAZICIOGLU tarafından

Nitekim Alman Ceza Kanunu bu durumu dikkate almış ve dolandırıcılık suçunu hem insan iradesine karşı olan, hem de bilişim sistemine karşı olan hileli davranışlara göre ikiye ayırmış ve iki ayrı madde de iki ayrı suç tanımlanmıştır. Örneğin İnternet ortamında kendisini B gibi tanıtan A bir açık artırmaya katılsa ve bu hileli eylemi sonucunda açık artırma kendisine kalsa, eğer açık artırmayı İnternet ortamında da olsa bir insan iradesi sonlandırmışsa, dolaysı ile bir kişi olan fail hileli davranışlarla yanlış bir karara varmışsa o zaman bilişim sistemleri aracılığı ile dolandırıcılık yani 158/1-f bendindeki suç, yok eğer bilişim sistemi otomatik olarak yazılan bir yazılım ile açık artırmayı sona erdirmiş ise o takdirde TCK da 244/4 maddesindeki suç oluşacaktır. Birinci durumda ceza iki yıldan yedi yıla kadar hapis ve beş bin güne kadar adlî para cezası olacak iken, ikinci durumda iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına mahkûm olabilecektir.

Bilişim sistemleri vasıtasıyla dolandırıcılık eyleminin İnternet yoluyla işlenmesi çok karşılaşılan adli vakalardan biridir. Örneğin çok sık rastlanan bir dolandırıcılık örneğini farkındalık açısından veriyoruz; İstanbul'daki bir inşaat şirketinin İnternet bankacılığı şifresini kırarak 50 bin 700 TL'sini başka hesaplara havale eden ve 10 bin TL'sini çeken 4 kişi, paranın geri kalanını çekmek isterken bir ilimizde polis tarafından yakalanır. Başka bir ilde bir banka şubesinde hesabı bulunan mağdur M. haberi olmadan 50 bin 700 YTL' sinin başka hesaplara havale edildiğini fark eder. Banka yetkilileriyle yapılan görüşmeler sonunda, M.nin hesabından havale edilen paranın bir kısmını başka bir yerde bulunan A.'nın hesabına, kalan kısmını da başka bir ildeki M.' ye ait hesaba gönderildiğini belirlerler. Şikâyet üzerine ekipler, M.nin parasının aktarıldığı hesaplardaki 10 bin TL'nin, bir banka şubesinden M.D. tarafından sahte kimlikle çekildiğini saptanır. Harekete geçen polis, mağdurun parasının aktarıldığı A.'nın ve M.nin hesaplarından başka bir hesaba ikinci bir transfer yapıldığını, paranın bu hesaplardan bölümler halinde çekildiğini belirler. Takip sonucu, A.'nın hesabından başka bir hesaba aktarılan 10 bin 500 YTL' yi başka bir banka şubesinden çekmek isteyen M.D. suçüstü yakalanır. Zanlının ifadeleri doğrultusunda, suç ortakları A. S. ve N.'de mağdurun parasının, kalan kısmını çekmek için banka şubesine gidince yakalanır ve haklarında "bilişim yoluyla dolandırıcılık'' suçundan işlem yapılır.[62]

Buna benzer adli vakalara İnternet ortamında veya gazetelerde haber olarak rastlamak sıkılıkla mümkün hale gelmiştir. Hatta bu yolla mağdur olanlar kendilerine sanal ortamda İnternet sayfası açmışlar ve dernek kurmuşlardır[63].

---

yapılan "AB Uyum Komisyonu Çalışması Türk Mevzuatında Bilişim Suçları" başlıklı konuşmadan alıntı yapılmıştır konuşmanın tamamı için tıklayınız;
http://www.taa.gov.tr/duyurularana/130606/bilisimsempozyum/sunum/makale.pdf (03.05.2008)

[62] **İnternet'te havale dolandırıcılığı;** http://www.milliyet.com.tr/2007/01/22/son/sontur06.asp (22.01.07)

[63] http://www.sanalbankamagdurlari.com/ (14.04.2007)

3.10 Bilişim Sistemleri Vasıtasıyla Sahtecilik

Bilişim Sistemleri vasıtasıyla işlenen suçlardan biri de bir belge veya bilginin aslına benzetilerek yapılan düzmece olarak elektronik ortamlarda meydana getirilmesidir.

Mülga 765 S. Eski TCK'da 06.06.1991 tarih ve 3756 SK 23 maddesi ile giren 525/c maddesinde bilişim yolu ile sahtecilik şu şekilde tanımlanmakta idi; " Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir."Ancak 5237 Sayılı TCK nun 1 Haziran 2005 tarihinde yürürlüğe girmesi ile bu madde de mülga olmuş ve yeni yasada bu suça yer verilmemiştir.

Daha sonra Adalet Bakanlığının hazırlayarak Başbakanlığa sunmuş olduğu "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"nda 18 maddesinde; "Bilişim sistemini kullanarak sahtecilik" suçu Sahte belge düzenlemek amacıyla, bilişim sisteminde bulunan verileri silen, değiştiren, yok eden veya yeni veri giren kişi hakkında 16 ncı maddenin birinci fıkrasına göre verilecek ceza yarı oranda artırılır." şeklinde yer almıştır. Ayrıca maddenin 2. Fıkrasında; "Birinci fıkrada belirtilen fiillerin işlenmesi suretiyle oluşturulan verilere dayalı olarak sahte belge düzenlenmesi halinde, ayrıca 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun belgede sahtecilik suçuna ilişkin hükümlerine göre cezaya hükmolunur." hükmü getirilerek 5237 sayılı TCK'nun eksik bırakmış olduğu alan doldurulmaya çalışılmıştır.

Bilişim Sistemleri Vasıtasıyla Sahtecilik suçu, özetle hukuka aykırı bir şekilde kendisine ya da başkasına menfaat temini veya başkasına zarar verme kastıyla bilişim sistemlerindeki veri veya programları silmek, değiştirmek, müdahale etmek ve bu şekilde hukuken delil niteliğine sahip bir belge veya bilgi oluşturmaktır[64].

Avrupa Konseyi'nce de SSS' de bilgisayar yolu ile sahtecilik şu şekilde tarif edilmiştir: " Bilgisayarda yer alan veri ve programlara girmek, değiştirmek, silmek veya imha etmek veya hukukça sahtekârlık olarak kabul edilen hallere münhasır olarak kabul edilen hallere münhasır olarak verinin işlenmesine yönelik bir müdahalenin mevcudiyeti[65]."

Bilişim sistemlerinde tutulan veri, belge ve bilgilerde sahtecilik amacıyla yapılan değişikliklerle kişiler kandırılabilmekte ve bu tür belge ve bilgiler adli vakalarda sık sık

[64] Kurt, Levent, "Açıklamalı-İçtihatlı Tüm Yönleri ile Bilişim Suçları ve TCK'daki Uygulaması", Seçkin Yayınevi, Ankara 2005, s. 83
[65] Siber Suç Sözleşmesi, Budapeşte 2001

gündeme gelmektedir[66]. Bilgisayar Suçlarının tanımı içerisinde bu suçlara bakıldığında diğer sahtecilik suçlarından ayırt edebilmek için "Bilgisayar Yoluyla Sahteciliği" ayrı olarak ele almak gerekmektedir. Çünkü bilişim sistemlerinin kullanımı ile üretilmiş sahte para suçunda, olay yerinde delil niteliği teşkil edecek bilgilerin bulunması çok zor olabilir ve bu delillerin toplanması ve soruşturulması farklı tekniklerin kullanılmasını gerektirebilir[67].

Bu tür suçlarda bilişim sistemleri kullanılarak, ya mevcut bir evrak üzerinde tahrifat yapılır, ya da olmayan bir evrak varmış gibi gösterilir ya da mevcut bir evrak yok edilir (silinir)[68]. Bankacılık alanında ise, hesap sahiplerinin hesabının yapılan her işlem sonunda küsuratlarının ayrı bir hesaba otomatik olarak kesilmesi bu türe verilebilecek en meşhur örnektir[69].

Mülga 765 S. Eski TCK'da 06.06.1991 tarih ve 3756 SK 23 maddesi ile giren 525/c maddesinde yasa koyucu, gelişen teknolojinin hukuk ve ticaret alanındaki uygulamasını dikkate alarak evrakta sahtekârlık suçları açısından ceza yasasının bu alandaki boşluğunu gidermek istemiştir. Belge kavramının eski yasada bir tanımı verilmemişti belgenin tanımı uygulamaya bırakılmıştı. Bu nedenle bilişim sistemi üzerinde sahtekârlık yapılması ve bunların kullanılması eylemlerinin TCK'nin 339. ve devamı maddelerinde düzenlenen evrakta sahtekârlık suçları kapsamında değerlendirilmesi, suçların ve cezaların yasallığı ilkesi açısından mümkün değildir[70].

Bu suçlar ile korunan hukuksal değer evrakta sahtecilik suçuyla korunmak istenen hukuksal değerin aynısıdır; yani devlet tarafından fertlere yüklenilen hukuk alanında inandırıcılığı olan bu tür belgelere olan güven korunmak istenmektedir. Bu nedenle evrakta sahtekârlık suçları ile korunmak istenen hukuksal değer için yapılan açıklamalar bu suç tipleri açısından da geçerlidir; klasik evrakta sahtekârlık suçları ile inceleme konusu elektronik ortamlarda sahtekârlık suçları arasındaki fark, korunan hukuksal değerde değil, evrakın niteliğindedir[71].

Klasik evrakta sahtecilik suçlarında olduğu gibi, sanal alanda veriler halinde oluşturulanve hukuksal alanda delil niteliği bulunan belgelerin de sahte olarak üretilmesi, tahrif edilmesi ya da kullanılması eylemlerini içeren verilerde sahtekarlık yapılması ve üretilen sahte belgelerin kullanılması suçlarında da korunan hukuksal değer, kamunun bu belgelere duyduğu güven ve bu belgelerin doğruluğuna ilişkin inançtır.

---

[66] http://www.diyarbakir.pol.tr/bilisim/bilisim.htm (17.03.2007)

[68] İnanıcı,Haluk,"Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü", İstanbul Barosu Dergisi, Cilt:70, Sayı:7-8-9, s. 510-537

[69] Kurt, s. 3

[70] Dülger, Murat Volkan, "Bilişim Suçları", Seçkin Kitabevi, Ankara 2004,s. 198

[71] Dülger, s.196

Verilerde sahtekarlık yapılması ve üretilen sahte belgelerin kullanılması suçlarında fail açısından yasa herhangi bir özellik aramamıştır. Suçu herkes işleyebilir[72].

Bu suçlar mağdur açısından bir farklılık göstermez. Bu suçlarla korunan hukuksal değer kamunun güveni ve inancı olduğu için suçun mağduru da devlettir. Ancak aynı eylemler başka cinsten hukuksal değerleri de ihlal etmekte bu nedenle de, kamunun güveni aleyhinde bir suç sayılan sahtekârlık eyleminden zarar gören kişi de kamu davasına müdahale edebilmektedir. Ancak bu müdahale yetkisi kişiyi mağdur durumuna getirmemektedir[73].

Bu suçun mağduru daima devlettir. Verilerde sahtekârlık yapılması ve üretilen sahte belgelerin kullanılması suçları nedeniyle zarara uğrayan kimse mağdur olmayıp "suçtan zarar gören kisme" konumundadır[74].

Bilgisayar Yoluyla Sahtecilik Yine klasik olarak bilinen sahtecilik suçunun, yüksek teknoloji ürünü cihazlar kullanılarak yapılmasıdır. Bilgisayar Suçlarının tanımı içerisinde bu suçlara bakıldığında diğer sahtecilik suçlarından ayırt edebilmek için Bilgisayar Yoluyla Sahteciliği ayrı olarak ele almak gerekmektedir. Çünkü; bilgisayar kullanımı ile üretilmiş sahte para suçunda, olay yerinde delil niteliği teşkil edecek bilgilerin bulunması çok zordur ve bu delillerin toplanması ve soruşturulması teknik bir olay olarak karşımıza çıkacaktır[75].

Hukuk alanında delil olarak kullanılabilecek her türlü veri, verilerde sahtekarlık yapılması suçunun konusunu oluşturmaktadır. Buradaki veriler kavramıyla, bilişim sisteminde bulunan ve delil niteliği taşıyan bilgilerin kastedildiği belirtilmektedir. Delil değeri taşıyan bilgi kavramıyla ise; hukuksal işlemlerde bir olayın bir hakkın kanıtlanmasında kullanılma niteliğine sahip olan verilere işaret edilmektedir. Bunlara örnek olarak, cari hesap kayıtları, elektronik sözleşmeler, adlisicil kayıtları v.s verilebilir[76].

Ayrıca hukuk alanında delil olabilme ifadesiyle, adli mercilerde veya asli işlemlerde belgenin delil taşıyabilme özelliğine sahip olmasının kast edildiği, ancak suçun oluşması için bu belgenin adli merciler önünde kullanılmasının gerekmediği, bu tür işlemlerde kullanma olanağının bulunmasının yeterli olduğu ifade edilmektedir[77].

---

[72] Yazıcıoğlu,Yılmaz, "Bilgisayar Suçları:Krminolojik,Sosyolojik ve Hukuki Boyutları ile", Alfa Yayınevi, İstanbul 1997, s.280
[73] Dülger, s. 197
[74] Erman, Sahir, " Kamu Güvenine Karşı İşlenen Suçlar",Dünya Yayıncılık,İstanbul 1996, s. 11
[75] http://www.bilgisayarpolisi.com (19.03.2007)
[76] Dülger,s. 198
[77] Yazıcıoğlu,s. 198

Verilerde sahtecilik yapılması suçunun oluşabilmesi için hukuk alanında delil olarak kullanılacak bilginin sayısal veri halinde olmsı gerekir. Her ne şekilde olursa olsun söz konusu bu verilerin somut hale gelmesi, örneğin sözleşmenin yazıcıdan çıktısının alınarak somut hale getirilmesi ve bundan sonra maddi unsuru oluşturan eylemlerin bu belge üzerinde gerçekleştirilmesi halinde ise klasik evrakta sahtecilik suçu uygulanacaktır[78].

Üretilen sahte belgenin kullanılması suçunun konusunu ise, hukuk alanında delil olarak kullanılmak üzere yapılan sahtecilik eylemi neticesinde üretilen belgenin kendisi oluşturmaktadır. Verilerde sahtekarlık yapılması suçundan farklı oalrak bu suç açısından belge veri halinde olabileceği gibi çıktı haline getirilmiş örneğin elektronik imza ile onaylanmış yazılı bir sözleşme de olabilir[79].

Suçun unsurları klasik sahtecilik suçundan farklı olmayıp, bilişim sistemleri kullanılarak gerçekleştirilmektedir. Bilgisayar yolu ile sahtecilik suçundan kastettiğimiz, bilişim teknikleri kullanılarak gerçekleştirilen, başka türlü suçun maddi unsurunun gerçekleşmediği suçlardır. Adam öldürme suçunun bıçakla işlenmesi halinde, nasıl bu fiil bıçak suçu olmuyorsa, bilişim suçlarının araç olarak kullanıldığı, ama başka yöntemlerle de işlenebilecek bir suç bilişim sahteciliği değildir[80].

Verilerde sahtekârlık suçu seçimlik hareketli bir suç olarak düzenlendiği için fail tarafından ister yeni bir belge oluşturulsun, ister mevcut bir belge üzerinde değişiklik yapılsın, isterse de her iki eylem birlikte gerçekleştirilsin sonuç değişmeyerek tek bir suç işlenmiş olacak ve faile tek bir suçun cezası verilecektir. Ayrıca hem verilerde sahtekârlık suçu hem de verilerle oluşturulan sahte belgenin kullanılmasu suçu icrai hareketli suçlar olduğundan failin ihmali suretiyle işlenemeyeceklerdir, suçun oluşumu iin failin mutlaka bir eylemi gerekmektedir[81].

Veri yerleştirmek eylemi ile bilşim sisteminde ya da veri taşıma aracında gerçek olarak bulunan ancak sahteleştirilmek istenilen ya da bilişim sisteminde bulunmadığı halde sahte olarak oluşturulmak istenilen belgeler için; çeşitli verilerin sisteme kaydedilmesi, yüklenilmesi ya da eklenilmesi kast edilmektedir. Söz konusu veri yerleştirme eylemi, bilşim sisteminde ya da veri taşıma aracında bulunan herhangi bir verinin, sahte belge oluşturmak çin kullanılması yoluyla da gerçekleşebilecektir[82].

Ayrıca suçun oluşabilmesi için söz konusu verilerin blişim sistemine kaydedilmiş olması yani yerleştirme eyleminin tamamlanmış olması gerekir, henüz kaydetme işlemi gerçekleşmemiş ve sahte belge oluşturulmamış ise, örneğin, sahteleştirmeyi

[78] Yazıcıoğlu,s. 281,283

[80] KURT, s. 84
[81] AKBULUT,Berrin, “Türk Ceza Hukukunda Bilişim Suçları”, Konya 1999
[82] DÜLGER, s. 199

sağlayacak veriler, disket ya da cd-rom halinde bilişim sisteminin sürücülerine yerleştirilmiş ancak kopyalama eylemi gerçekleştirilmemiş ise suç gerçekleşmeyecektir[83].

Elektronik imza ve elektronik sertifika oluşturmak için veri yerleştirilmesi eylemleri ise bu eylemler kendi özel yasalarında suç tipi olarak düzenlendiği için verilerde sahtekarlık yapılması suçu kapsamında değerlendirilemeyeceklerdir, ancak elektronik imza ile onaylanmış bir belgenin içeriğinde veri ekleme yoluyla sahtecilik yapılması eyleminde ise EİK'nın 17. maddesi uyarınca her iki suçun cezası da faile verilerek cezaların içtimaı kuralı uygulanacaktır.

Verilerin tahrif edilmesi eylemiyle ise, bilişim sisteminde ya da veri taşıma aracında bulunan ve gerçek belgeyi oluşturan verilerin söz konusu belgenin sahteleştirilmesi amacıyla her ne şekilde olursa olsun değiştirilmesi belirtilmektedir. Tahrif etme eylemi çok çeşitli biçimlerde meydana geitrilebilir; sahteleştirilmek istenilen belgeyi oluşturan verilere yeni veriler eklenmesi, mevcut verilerin çıkarılması ya da yerlerinin değiştirilmesi buna örnek verilebilir.

Elektronik imzayla onaylamış elektronik sözleşmeler gibi belgelerde ise tahrifatın belgenin içeriğinde olması halinde hukuk alanıdna delil olmak üzere oluşturulan her türlü belgeyi onaylamak ya da irade beyanında bulunan kişiyi belirlemek için kullanılannve yine verilerden olşan elektronik imza ve/veya elektronik sertifika üzerinde gerçekleştirilen ve bunları sahte hale getiren eylemler 5070 sayılı Elektronik İmza Kanunu'nun 16 ve 17. maddelerinde suç olarak düzenlenmektedir. Hem belgenin içeriğinin hem de elektronik imza ve/veya elektronik sertifikanın tahrif edildiği durumlarda ise Elektronik İmza Kanununun 17. maddesi uyarınca her iki suçun cezası da faile verilecek ve cezaların içtima edilecektir.

Burada değinilmesi gereken bir diğer konu da verileri tahrif etmek eylemiyle, veri yerleşirme eyleminden farklı olarak sahte bir belgenin hiç yokken oluşturulamayacağıdır. Çünkü değiştirmek anlamına gelen tahrif etmenin olabilmesi için üzerinde veri değişikliği yapılabilecek bir belgenin önceden sistemin içinde zaten bulunan gerçek ya da sahte bir belgeyi oluşturan veriler üzerinde gerçekleştirilebilecektir.

765 Sayılı TCK'nın 525/c maddesinde düzenlenen verilerde sahtekârlık suçu ve oluşturulan sahte belgenin kullanılması suçlarının her ikisi de birer tehlike suçu idiler. Bu nedenle yasa her iki suçun gerçekleşmesi için de ayrıca bir zararın meydana gelmesini aramamakta maddi unsur oalrak gösterdiği eylemlerin yapılmasını suçun oluşumu için yeterli saymaktaydı. Ayrıca verilerde sahtekarlık suçu birden fazla ve farklı

[83] AKBULUT,s. 187

hareketle gerçekleştirilmekteyse de söz konusu harekletler sonucu gerçekleşen neticeler aynı olmakta, sonuçta sahte bir belge oluşturulmaktadır. Her iki suç tipi açısından yapılan hareketle gerçekleşen netice arasında bir zaman dilimi bulunmamaktaydı, hareketin yapılmasıyla sonuç da gerçekleşmekteydi. Bu nedenle verilerde sahtekârlık suçu ve oluşturulan sahte belgenin kullanılması suçlarının her ikisi de neticesi harekete bitişik suç niteliğinde idi[84].

5237 S. TCK da bilişim sistemleri aracılığı ile sahtecilik suçu düzenlenmemiştir. Özellikle UYAP gibi tüm adli evrakların elektronik ortama taşındığı bir Projeye sahip bir ülkede kanaatimizce böyle bir suçun ayrıca düzenlenmemiş olması eksikliktir. Her ne kadar bu tür eylemlere karşı TCK 244. Maddesi uygulanabilecek ise de herhangi bir veri değişikliği ile kamunun güvenerek bir değer atfettiği bu belgelere dayanarak kararlar verildiği de göz önünde bulundurularak, böylesi bir belgenin değiştirilmesi sonucu failin alacak olduğu ceza herhangi bir veri değişikliği yapan kişi ile aynı olamamalıdır düşüncesindeyiz.

Nitekim bu eksikliği gören Kanunkoyucu Adalet Bakanlığı tarafından hazırlanan Tasarıda bu suça yer vermiştir. Bilişim sistemini kullanarak sahtecilik suçu Tasarının 18. maddesinde düzenlenmiştir. Maddenin birinci fıkrası; “Sahte belge düzenlemek amacıyla, bilişim sisteminde bulunan verileri silen, değiştiren, yok eden veya yeni veri giren kişi hakkında 16 ncı maddenin birinci fıkrasına göre verilecek ceza yarı oranda artırılır. İkinci fıkra ise; “Birinci fıkrada belirtilen fiillerin işlenmesi suretiyle oluşturulan verilere dayalı olarak sahte belge düzenlenmesi halinde, ayrıca 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun belgede sahtecilik suçuna ilişkin hükümlerine göre cezaya hükmolunur.” diyerek sahte belge düzenlemeyi yaptırım altına almıştır.

3.11 İstenmeyen Elektronik İletiler

İnternet teknolojilerinin gelişmesi ile birlikte ortaya yeni sektörler çıkmakta, yeni iş kolları doğmakta veya mesleklerin icra şekli değişmektedir. Reklâm, bir ürün veya hizmetin tanıtımı için öteden beri kullanılan bir yoldur. Reklâmın niteliğinde bir değişiklik olmamakla birlikte İnternet teknolojisinin gelişmesi ile birlikte icrasında bir takım değişiklikler meydana gelmiştir. İnternet yoluyla reklâmın kullanıcılara ulaşması son derece kolaylaşmış, ayrıca elektronik posta adreslerine gönderilen reklâmlar ile aracısız reklâm imkânına kavuşulmuştur. E-posta ile yapılan reklâmlar, klasik usulde yapılan reklâmlara göre daha avantajlıdır. Bu tür reklâmlar öncelikle tüketiciye doğrudan ulaşmaktadır. Posta kutusunu açan kişi, içeriğini okumasa bile en azından firmanın adı ile karşılaşmaktadır. Ayrıca bu tür reklâmlar, diğer reklâm usullerine göre son derece masrafsızdır. E-posta yolu ile yapılan reklâmların bir başka avantajı ise

[84] Yazıcıoğlu, s.285

müşteri kitlesine hızlı ulaşmasıdır. Bir tuş yardımı ile aynı anda binlerce adrese reklâm gönderme imkanı mevcuttur. E-posta yolu ile reklâm yapmak telefon ile reklâmdan daha güvenlidir ve belirli bir zamanda yapılmasına da gerek yoktur. İş saatleri dışında da gönderilen e-postalar, ertesi iş günü reklâm yapılan kimsenin bilgisayarında okunabilecektir. Muhtemel müşteri kitlesinin seçimini yapmak daha kolaydır. Kitap alıcılarının e-posta adreslerinin toplanması ve sadece onlara yönelik kitap reklâmı yapılması gibi. Nihayet bu reklamlar daha ucuza mal edilebilmektedir[85]. Bütün bu avantajlı tarafları ile elektronik posta yoluyla reklâm günümüzde bir sektör haline gelmiştir[86].

Doğrudan müşteriye yapılan bu reklam türü, reklamı yapan ve reklamı yapılan açısından faydalı olmakla birlikte; elektronik postasına reklam gönderilen kimseler açısından faydalı görülmeyebilir. Posta kutusu dolan ve bu sebeple kendisine gönderilen diğer e-postaları alamayan İnternet kullanıcıları bu durumdan yakınmaktadır.

Birden fazla kimseye yapılan bu reklâmlar için adreslerin elde edilmesi çoğunlukla daha önceleri gerçekleşmektedir. Özellikle 'daha hızlı ve çok para para kazanmak istemez misniz' yahut 'yardım için bu e-maili siz de bütün tanıdıklarınıza yollayın' gibi mesajlarla muhtemel müşteri kitlesinin elektronik adresleri elde edilmektedir. Ayrıca bazı tartışma forumlarındaki adresler de spam amaçlı kullanılabilmektedir. Çoğu zaman da "whois" databankları veya haber grupları vasıtası ile de e-posta adresleri toplanmaktadır. Toplanan bu adreslerden oluşturulan ve satışa sunulan CD'lerde milyonlarca adres bulunabilmektedir[87].

E-posta adreslerinin de belirli bir kapasitesi bulunmaktadır. Dolayısıyla e-adreslere gönderilen özellikle reklâm türü postalar kişinin posta kapasitesini doldurmakta ve başka posta alabilmesine engel olmaktadır. Bu sebeple sık sık şikâyetler olmaktadır[88].

---

[85] Funk, A.: „Wettbewerbliche Grenzen von Werbung per E-Mail", CR, 1998/7, s. 413, 414; Rosenthal, D.: „Unverlangte Werbe E-Mail ohne Rechtsfolgen", Media Lex, 4/99, s.203.

[86] Örneğin 300.000 adres için haftalık 19, 95 Ş, 500.000 adres için haftalık 29.95 Ş, 1.000.000 adrese posta için haftalık 39.95 Ş alınmaktadır. Günlük ticari reklam amacı ile gönderilen e-posta sayısı 100 milyon olarak tahmin edilmektedir. Örnekler ve diğer e-posta reklam fiyatları için spammingin gelişimi için bkz. Kommission der Europäischen Gemeinschaften : „Unerbetene kommerzielle Kommunikation und Datenschutz, Zusammenfassung der Schlussfolgerung der Studie Januar 2001. http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamsumde.pdf, s. 6 vd.

[87] Örneğin böyle bir CD'de 80 milyonun üstünde e-posta adresi bulunmaktadır (bkz. Leupold, A.: „Die massenweise Versendung von Werbe-e-Mails: Innovatives Direktmarketing oder unzumutbare Belaestigung des Empfaengers" WRP, 1998/3, s. 271).

[88] Amerikanın büyük İnternet servislerinden Earthlink, ortalama günde 1000-3000 arasında spam şikayetinin geldiğini belirtmektedir. Göndericinin yanlış adres belirterek e-posta yollaması dolayısıyla en büyük mağdur sayılabilecek Samsung, günlük spam sayısının 6000-10.000 olduğunu, müşterilerinin bu duruma çok kızdığını ve markalarının imajının sarsıldığını açıklamaktadır (Bkz. Leupold, s. 271).

Son zamanlarda istenmeyen iletiler reklâmın ötesinde fikir ve düşüncelerin yayılması ve hatta propagandası vasıtası haline de gelmiştir. Bu nedenle istenmeyen mailler ilk zamanlar sadece reklam aracı olarak görülürken artık doğru veya yanlış fikirlerin yayılması ve hatta düşünce ve ifade özgürlüğünün bir aracı olduğu iddia edilir olmuştur. Örneğin yakın geçmişte bir Bakanlığın, çalışanın adı ve İnternet sayfası kullanılarak halkı paniğe sevkedecek şekilde ortada AIDSli iğnelerin dolaştığı ve sinema lokanta gibi yerlerde otururken veya kürdanlar kullanılırken dikkat edilmesi gerektiği, aksi takdirde istenmeyen sonuçlarla karşılaşılabileceği ileri sürülmüştür. Sonuç olarak kişiler boşu boşuna telaşa kapılmışlar ve Bakanlık gereksiz yere bu yönde gelen telefon, ileti ve görüşme trafiği ile uğraşmak zorunda kalmıştır[89].

Avrupa Birliğinde konu 4.6.1997 tarihli "Mesafe Ötesi Sürüm Sözleşmelerinde Tüketicinin Korunması Hakkında Direktif" [90] ile ele alınmaktadır[91]. Söz konusu Direktifin amacı, bir taraftan tüketicinin konumunu daha sağlamlaştırmak diğer taraftan mesafe ötesi mal ve hizmet sürümlerini geliştirmektir. Direktifin üye ülkelerin iç hukukuna aktarılmaksızın da uygulama alanına sahip olduğunu burada belirtmek gerekmektedir. Çünkü Avrupa Birliği Sözleşmesi m. 189/III' e göre direktiflerin uygulanması sadece kanun koyucuya değil, devlet gücünü kullanan bütün erklere yüklenmiş bir görevdir. Alman Mahkeme kararlarında da direktiflerin iç hukuka aktarılmasından önce de uygulama alanı bulduğu, mevcut kuralların direktifler doğrultusunda yorumlandığı görülmektedir[92].

Avrupa Birliğinin, 8 Haziran 2000 tarihli ve 2000/31/EG "Bilgi Toplumu Hizmetlerinin, Özellikle Elektronik Ticaretin Ortak Pazardaki Bazı Yönleri Hakkında Direktifi" ile 1997/66 ile 2002/58 sayılı "Elektronik İletişimde Kişisel Verilerin İzlenmesi ve Gizliliğinin Korunması Yönergesi" ile üye ülkeler için konu ile ilgili bir takım yükümlülükler öngörmektedir. Avrupa Birliğinin 2000/31 sayılı e-ticaret Direktifi ile bilgi toplumu alanında hizmet verenlerin tâbi olacakları hükümler, genel bilgilendirme yükümlülükleri, ticari iletişim için gerekli şartlar, istenmeyen elektronik iletiler, elektronik vasıtalarla yapılacak sözleşmelere uygulanacak kurallar ve sözleşme öncesi verilmesi gerekli bilgiler (özel bilgilendirme yükümlülüğü), ara hizmet sunucularının sorumlulukları ve mesleki davranış kurallarına ilişkin olarak üye ülkelere bir takım sorumluluklar yüklenmektedir.

---

[89] Sabah Gazetesi, 13 Nisan 2007; Adalet Bakanlığı logolu 'AIDS maili' korsan çıktı; http://img.sabah.com.tr/haber,CDF0DEBE5480464EBB8C0EA441030F80.html (14.04.2007)

[90] Bkz. 97/7/EG, ABl. Nr. L. 144.

[91] Avrupa Birliğinde spamingle ilgili geniş bilgi için bkz. Kommission der Europäischen Gemeinschaften : „Unerbetene kommerzielle Kommunikation und Datenschutz, Zusammenfassung der Schlussfolgerung der Studie Januar 2001, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamsumde.pdf, s. 6 vd.

[92] BGH, „Testpreis-Angebot", GRUR 1998, s. 2208.

Avrupa Birliğinin 2002/58 sayılı "Elektronik İletişimde Gizliğinin Korunması Yönergesinde" ise; Topluluk içinde elektronik iletişim ekipmanları ile elektronik iletişim vasıtasıyla işlenen kişisel verilerin, temel haklar ve özgürlüklerin korunması ilkesi de dikkate alınarak eşit seviyede korunmaları ve bu şekilde serbest dolaşımlarının sağlanması amaçlanmakta, bu çerçevede elektronik iletişime ilişkin bir kısım tanımlar yapılarak iletişimin gizliliğinin korunması, gerekli güvenlik tedbirleri, trafik bilgilerinin saklanması gibi konularda hükümler ihdas edilmektedir.[93]

Alman hukukunda bu direktif iç hukuka (Mesafe Ötesi Sürüm Kanunu /Fernabsatz Gesetz- FernAbG) uyarlanmış olmasına rağmen bu kanun da spam hakkında bir hüküm içermemektedir[94]. Yine Alman hukukunda e-posta yolu ile reklamı açıkça konu edinen bir kanun kuralı bulunmamaktadır. Fakat Alman hukukunda mevcut kanunlarla spam sorununa çözüm arandığı görülmektedir[95]. Alman mahkemelerinden ilk olarak Traunstein[96] mahkemesinde e-posta ile reklâmın hukuken uygun olup olmadığı incelenmiştir. Bu kararda istenmeyen reklâmların e-postaya gönderilmesi haksız rekabet olarak nitelenmiştir. Mahkeme bu tür reklâmın haksız rekabet teşkil ettiğine karar verirken Mesafe Ötesi Sözleşmeler hakkındaki Direktifin 10/II'inci maddesini bir engel olarak görmemiştir. Her ne kadar söz konusu direktif hükmü, telefon ve e-postanın ticari amaçlı reklâmlarda kullanılabilmesine izin vermiş ise de, yine aynı direktifin 14'üncü maddesi üye ülkelere daha dar ve katı hükümleri koyabilme yetkisi vermiştir. Alman Haksız Rekabet Yasası'nın 1'inci maddesi de böyle bir hükümdür. Bazı yazarlar da e-postayla yapılan reklâm sorununu haksız rekabet hükümlerine tabi tutmaktadır[97].

Amerika Birleşik Devletlerinin çeşitli eyaletlerinde e-posta yoluyla reklâm yapılması kanunlarla yasaklanmıştır. Eyaletlerde ilk kanun olan "Can the Spam" 1 Ocak 1999 günü Kaliforniya'da yürürlüğe girmiştir. Bu kanunla İnternet hizmetlerini sağlayan

---

[93] http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (20.03.07)

[94] Lettl, T.: „Rechtsfragen des Direktmarketings per Telefon und E-Mail", GRUR, 2000, s. 982, 983.

[95] Spam sorunu Alman hukukunda özellikle BGB Madde 823 açısından ele alınmaktadır. E-postanın mahiyetinden hareket edilen görüşlerin bu tartışmalarda özellikle dikkate alınması gerekmektedir. Doktrinde bir sunucu üzerinden yapılan E-postanın mahiyetinin karma sözleşme tipini oluşturduğu vurgulanmaktadır. Bu sözleşme içinde hizmet ve eser sözleşmesinin tipik unsurları bulunduğu gibi, kira sözleşmesine ait unsurlar da bulunmaktadır. Şayet kişi e-postasını kendi serveri üzerinden yapıyorsa bu takdirde burada bir mülkiyet hakkından bahsetmek gerekmektedir. Spam sorununun çok farklı açılardan incelendiği bu makale için bkz. Spindler, G./Schmittmann, J.M.: "Unerwünschte E-Mail-Werbung, Zivil- und wettbewerbsrechtliche Zulaessigkeit in Europa", MMR 2001, Beilage-8, s. 10 vd.

[96] LG Braunstein, 18.12.1997 (CR, 1998, s. 171).

[97] Bkz. Hoeren, T.: „Cybermannes und Wettbewerbsrecht-Einige Überlegungen zum Lauterkeitsrecht im İnternet", WRP, 1997/11, s. 994, 995; Hoeren, T.: „Werberecht im İnternet am Beispiel der ICC Guidelines on Interactive Marketing Communikation", İnternet-und Multimediarecht (Cyberlaw) (Hrg. Lehmann, M.) Stuttgart 1997, s. 115; Wendel, : Wer hat Recht im Internet?, Aachen 1997, s. 80; Peschel-Mehner, A.: „Wettbewerbliche Bewertung geschaeftlicher Aktivitaeten im Internet und in sonstigen Online Plattform", Cyberlaw (Hrg. Schwerdtfeger/Everyz/Kruezer/Peschel-Mehner/Poeck) Weisbaden 1999, s. 135, 136. Fakat burada hemen aksi fikirlerin olduğunu da belirtmek gerekmektedir. Bu yazarlara göre e-posta yoluyla yapılan reklamlar haksız rekabet oluşturmaz (bkz. Reichelsdorfer, J.: „eMails zu Werbezwecken-ein Wettbewerbsstoss?", GRUR, 1997, s. 191; Funk, s. 420).

servis sunuculara (Service-Provider) müşterileri ile yaptıkları sözleşmelere e-posta ile istenmeyen reklâmlar göndermeyecekleri, aksi takdirde zararı gidermek zorunda kalacakları konusunda uyarıcı bir hüküm koymaları gerekmektedir. Bu kanunla ayrıca spam yapanlara ceza da getirilmiştir. Buna göre her e-posta başına 50 veya günlük 25 bin dolara kadar ceza öngörülmüştür[98].

Ayrıca Kaliforniya Meclisi, spam yapan kimsenin çocuklar için sakıncalı sayılan mesajları göndermesini de yasaklamıştır. Bu kanuna göre ayrıca reklâm yapan kimse ücretsiz bir telefon numarasını veya kendisine ulaşılabilecek gerçek bir adresini de alıcıya sunmalıdır ki; alıcı bunlarla isminin listelerden çıkarılmasını sağlayabilsin. Bu kanunla e-posta ile reklam yapan kimsenin posta içine başka birinin domain ismini yazması, böylece alıcıyı yanıltması da yasaklanmıştır[99].

Benzer kurallar 1997 yılında Nevada ve Washington eyaletlerinde de yürürlüğe girmiştir. Washington'da yürürlüğe giren kanuna göre her e-posta yasaklanmamış, sadece konusu reklâm olarak görünmeyen e-postalar veya gönderici adresinin yanlış yazıldığı istenmeyen ticari reklamlar yasaklanmıştır. Bu kanunun uygulama alanı ise Washington'dan gönderilmiş veya oraya yollanmış reklamlarla sınırlanmıştır[100].

Virjinyada da benzeri bir kanun çıkarma çabaları görülmektedir. Bu kanunun temelinde de yanlış kimlik ve görünürde adresler altında e-posta gönderilmesi suç olarak nitelenmiş ve para cezalarına çarptırılması öngörülmüştür. Burada kasıtlı postalar dolayısıyla provider ve postayı gönderen kimse için her e-posta başına 10 dolar veya günlük 2500 dolar ceza istenmektedir[101].

Özellikle ABD de istenmeyen iletilere karşı kabul edilen "İstenmeyen Pornografik ve Ticari İhlallarin Kontrol Altına Alınması kanunu 2003" veya "'CANSPAM Act of 2003'' diye adlandırılan yasal düzenlemelerden bahsetmek gerekir. Sson zamanlarda terörle mücadele içine giren ABD 'nin ifade ve düşünce yayma özgürlüğüne önemli bir kısıtlama getirdiği söylenmeye başlanmıştır[102]. Ancak bu tür maillerin zaman zaman halkı paniğe sürükleyecek veya bazı şirketleri önemli oranda zarar etmesine neden olabilecek sonuçlar da doğurabileceği göz önünde bulundurularak özgürlük güvenlik dengesinin iyi ayarlanması gerekmektedir.

---

[98] Goerke, P.: „Amerika-Strafen für unverlangte E-Mail-Werbung", s. 249, WRP, 1999/2, s. 249.
[99] Naumann, T.: „Praesentationen im als Verstoss gegen §§ 1, 3 UWG, Unter besonderer Berücksichtigung der Online-Angebote von Rechtsanwaelten", Frankfurt am Main, 2001, s. 64.
[100] Goerke, s. 249.
[101] Fakat bu eyalette anti-spam yasasına ciddi tepki verildiğinin de vurgulanması gerekmektedir. Söz konusu yasanın düşünce açıklama özgürlüğü ile çeliştiğini, devletin genel menfaatleri koruması gerektiği, spam yapılmasında ise genel menfaatlere bir aykırılığın olmadığını, dolayısıyla da devletin yasa koymaması gerektiği ileri sürülmektedir. Ayrıca devletin her problemi kanun, polis, yasak ve hapishane çerçevesinde ele almasının yanlış olduğu, tekniğin halletmesi gereken şeylerde kanunlarla çözüme ulaşılamayacağı da belirtilmektedir. (Tartışmanın ayrıntıları için bkz. www.telepolis.de/deutsch/inhalt/glosse/2653/1.html).
[102] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf (14.04.2007)

Birçok ülkede olduğu gibi spamı doğrudan yasaklayan bir kural Türk hukukunda da henüz bulunmamaktadır. Gönderilen e-postaların içeriğine göre Türk Ceza Kanunu'nun uygulama alanı bulması da mümkündür. E-postanın içeriğinde tehdit, hakaret yasal olmayan propagandalar varsa bu takdirde bunlar ayrıca ceza davalarının konusunu oluşturacağı açıktır.

Adalet Bakanlığının hazırlayarak Başbakanlığa sunmuş olduğu "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"nda 2. maddesinin o) bendinde "İstenmeyen ileti"; "Gönderenine ulaşılamayan ve bu nedenle engellenemeyen veya kişinin istemediğini açıkça beyan etmesine rağmen gönderilmeye devam edilen ileti" şeklinde tanımlamış ve idari para cezalarını düzenleyen 28. Maddesinin e bendinde e) İstenmeyen ileti gönderene üç bin Türk Lirasından on beş bin Türk Lirasına kadar, idarî para cezası verileceği öngörülmüştür.

Kimileri tarafından ABD deki spam maillere verilen cezalar ile karşılaştırıldığında bu cezayı az ve yetersiz olarak görenler olmakla birlikte, spam maillerin aslında bir ifade özgürlüğü vasıtası olarak değerlendirilmesi gerektiği yönünde değerlendirilmeler de göz önüne alındığında konunun hassaslığını göz önünde bulundurmak gerekir. Öyle ya da böyle bu konuda az da olsa caydırıcılık bağlamında bir cezai yaptırım düzenlenmiş olması başlangıç olarak kanaatimizce yerinde olmakla birlikte özellikle halkı paniğe sürükleyen veya sürüklemesi muhtemel mailler konusunda daha ağır yaptırım öngören bir yasal düzenlemenin yapılması yerinde olur kanaatindeyiz.

E-posta sahiplerini spama karşı korumanın en etkin yolunun bir kanuni düzenleme olduğu açıktır. Yapılacak kanuni düzenlemede iki yol tercih edilebilir. Bunlardan birincisi kural olarak spam yapmanın yasal olduğu, ancak e-posta sahibinin reddi halinde bir daha yapılmaması; aksi halde cezalandırma yoluna gidilmesidir. Diğeri ise spam yapan kimsenin önceden e-posta sahibinden izin almasıdır. Ki bizde hazırlanan ve yukarıda bahsi geçen Adalet Bakanlığı tarafından Başbakanlığa sevk edilen Tasarı bu ikinci yolu tercih etmiştir. Ancak burada açıkça belirtmek gerekir ki her iki kanuni düzenleme biçimi de Avrupa Birliği Direktifine (Fernabsatzrichtlinie) uygundur.

Bir kimsenin e-adresine onun açık rızası olmadıkça içeriği reklâm mahiyetinde olan, kitlelere gönderilen ve şahsi olmayan postalar gönderilmemelidir. Kişilere gönderilecek spam mahiyetinde e-postalar için önceden rızası alınmalıdır ve kişi bu rızasından her zaman vazgeçebilmelidir.

İstenmeyen iletilerin Avusturya hukukunda olduğu gibi tanımlanması ve sonra müeyyidelerin getirilmesi gerekmektedir. Gerçekten istenmeyen iltilerin içeriğinden

bağımsız olarak tanımlamak ortaya çıkan problemlerin çözümlenmesinde kolaylık sağlayacaktır. Böylece ticari amaç dışında, e-adreslere gönderilen istenmeyen postalara karşı daha etkin bir koruma da sağlanabilir.

Spam sadece reklâm olarak kabul edilmemeli, istenmeyen ve kitlelere gönderilen e-posta olarak tanımlanmalı ve özellikle kimlik gizlenerek, yanlış adres verilerek ve görünürde e-posta adreslerinden posta göndermek cezalandırılmalıdır düşüncesindeyiz.

3.12 Kredi Kartları İle İlgi İşlenen Suçlar

Teknolojide sağlanan gelişmeler ve küreselleşmenin hız kazanması, banka kartları ve kredi kartlarının dünyadaki gelişimine paralel olarak ülkemizde de kullanımını yaygınlaştırmıştır. Bu kartları kullananların sayısı ve yapılan harcamalardaki artış, bankalar arasında rekabetin artmasına neden olmuştur. Banka kartları ve kredi kartları kullanılarak yapılan ödemelerin hızlı, kolay ve güvenilir bir şekilde gerçekleştirilmesi, tüketiciler ve işyerlerinin bu kartları kullanımını artırmıştır.[103]Ancak bu sayısal artışa paralel olarak bu kartlarla işlenen suç oran ve çeşitliliğinde de artış meydana gelmiştir.

İşte bu bölümde günlük hayatımızın vazgeçilmez bir parçası haline gelen ve bir zamanlar "sair alet" kavramı içerisinde [104] hırsızlık suçunun işlenmesinde kullanılan bir araç kabul edilen, daha sonra bilgileri otomatik işleme tabi tutmuş bir sistemi harekete geçirmede kullanıldığı için 765 Sayılı TCK.nun 525/b. maddesindeki suçu oluşturacağı kabul edilmesinden[105] sonra nihayet 5237 Sayılı TCK.nun 245.maddesinde banka ve kredi kartlarının kötüye kullanılmasını ilk defa bağımsız bir suç olarak düzenleyen madde ayrıntılı olarak ele alınmaya çalışılacaktır.

Banka kartı, kullanıcısına, bankanın müşterilerinin kullanımına sunduğu sisteme sadece kendince bilinen bir şifre yardımıyla girerek banka çalışanlarının yardımına muhtaç olmaksızın kendi banka hesabı üzerinde tasarrufta bulunma imkanı veren bir araçtır.[106]

5464 Sayılı "Banka Kartları ve Kredi Kartları Kanunu"nun 3.maddesinde ise ; "Banka Kartı; Mevduat hesabı veya özel cari hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanmayı sağlayan kartı" ifade eder, şeklinde tanımlanmıştır.

Öncelikle kişilerin bankada bir mevduat hesabı açtırmaları gerekmektedir. Bu aşamadan sonra banka kartı vasıtasıyla tüm bankacılık işlemlerini şubeye gitmeksizin kart sahibinin bu kart vasıtasıyla bankanın bilişim sistemine girerek yapması

[103] Aycı-Biçkin-Artuç, Banka Kartları ve Kredi kartları Kanunu, Kartal Yayınevi,(2006) sh. 7.
[104] Bkz. Yargıtay 6.C.D., 02.05.2000, E.2000/3194, K.2000/3239 sayılı içtihadı
[105] Bkz. Yargıtay Ceza Genel Kurulu E.2001/6–30, K.2001/57 sayılı içtihadı
[106] Erdağ, Ali İhsan , "Bilişim Alanında Suçlar", Ankara–2005

mümkündür. Para havalesi, fon transferi, döviz veya hisse senedi alım satımı, ödeme işlemleri, para çekilmesi, yatırılması kısaca tüm bankacılık işlemleri yapılabilir. Kart sahibinin kimseyle muhatap olmasına gerek yoktur. İnternet aracılığıyla bağlanabileceği bir bilişim sistemi ve bu sisteme girebileceği bir cihaz (ATM, Pos cihazı vs.) bulunması yeterlidir. Bu kartların bir başka fonksiyonları da, mevduat hesabı sahibinin hesabında para olmamasına karşılık belirli bir limit dâhilinde kredi çekilmesine imkan vermeleridir. Bu imkân ise mevduat hesabı sahibi ile banka arasında yapılan bir mevduat sözleşmesine dayanmaktadır.[107]

Kredi kartı ise; kullanıcısına banka ile arasında varılmış bir sözleşmeye dayanarak bankanın kendine sunduğu kredi olanaklarından yararlanma imkânı vermektedir.[108]

5464 Sayılı "Banka Kartları ve Kredi Kartları Kanunu"nun 3.maddesinde ise; Kredi Kartı; Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını, ifade eder şeklinde tanımlanmıştır.

Mal ve hizmet alımı ile her türlü ödeme yapma fonksiyonunun dışında nakit çekme imkânı da sağlamaktadır. Kredi kartı hizmetinin sunumunda üç taraf olup bunlar, kredi kartını çıkaran banka veya kurum, kart hamili ve üye iş yeridir.[109]Kredi kartı sisteminde kartı çıkaran kuruluş ile kart hamili arasındaki ilişkinin birer vekâlet akdi olduğu yaygın olarak savunulmaktadır.[110]

Kredi kartları hizmetinin sunumunda çeşitli sistemler bulunmaktadır. Kredi kartını çıkaran kuruluş müşterilerine sadece kendi mağazalarında geçerli olacak ve buradaki mal ve hizmet alımında kullanılabilecek bir kart ihdas edebilir. Burada kredi kartını çıkaran mağaza ile mal ve hizmetleri sağlayan aynı mağaza olduğundan, kredi kartı kullanıcısı ile kartı düzenleyen kuruluş olmak üzere hukuki ilişkide iki taraf bulunmaktadır. En yaygın olarak kullanılan sistemde ise, kredi kartını çıkaran kuruluş, kart hamili ve bu kredi kartı kullanımını kabul ederek mal ve hizmet sunumu yapan kuruluşlar bulunmaktadır. Bu sistemde kredi kartını çıkaran kuruluş ile bunu kabul eden farklı kuruluşlardır. [111]

Kredi kartları ile banka kartları arasındaki en önemli fark, banka kartı hamilinin kartın nakit karşılığı bulunması halinde bu kartı kullanarak alış veriş yapabilmesine

[107] Kurt, Levent .Tüm Yönleriyle Bilişim Suçları,Seçkin Yayınevi , (2005), s.180
[108] Erdağ, Ali İhsan, Kırıkkale Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Öğretim Üyesi, Bilişim Alanında Suçlar Makalesi,2005
[109] Yağcı, Ali. Kredi Kartı ile İşlenen Bilişim Suçları, Amme İdaresi Enstitüsü, 2003–2004 yılı öğretim dönemi Yönetim Bilişim Sistemleri Dersi Yayımlanmamış Dönem Ödevi, s.2
[110]Kurt, Levent .(2005),sh,180 (Kerem Ertan, "Banka Kredi Açma Sözleşmelerinin Hukuki Niteliği ve Özellikle Çerçeve Anlaşma Olma Özelliği", Legal Hukuk Dergisi, Sayı:7, 2003, s. 1674)
[111] Kurt, Levent; s.180

karşılık, kredi kartı hamilinin hesabında nakit bulunmaksızın alış veriş yapma imkânının bulunmasıdır.[112]

Kredi kartı sözleşmesi kurulduktan sonra kredi kartı kurumunun harcama belgeleri tutarlarını ödemek ve sistemin işleyişi için tüm bilgi ve gereçleri sağlamak, üye işyerinin yükümlülüğü ise kredi kartını kabul etmek ve kredi kartının geçerliliğini kontrol etmektir.[113]

765 Sayılı TCK'nda düzenlenmemiş bulunan ve banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya sözü geçen kart sahiplerinin zarara sokulmalarını ve bu yolla çıkar sağlanmasını önlemek amacıyla aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik gibi başkaca suçları da oluşturur nitelikteki bu türden fiillerin YTCK' nun cezalandırılır eylemler kataloguna **bağımsız bir suç olarak alınış sebebi, duraksamaları ve içtihat farklılıklarını gidermektir.[114]**

Günümüzde üzerinde kredi kartı bulundurması gereken, gerekmeyen, taşıdığı kredi kartının asgari tutarını ödeyecek gücü olan, olmayan kısacası ilgili ilgisiz birçok vatandaşımızın banka ve özellikle kredi kartı kullanması, ekonomik sıkıntı içerisinde bulunan bir kesim için bir tür cankurtaran sayılan bu tür kartların kullanımının artması suç işleme eğiliminde olanlar için yeni ve karlı bir kazanç kapısı olarak görülmektedir. Kullanımı ile beraber suça konu olma sayısı da artan bu kartlar ile işlenen suç türlerine her gün bir yenisi eklenmektedir.

Kredi kartlarının sahiplerinin bu kartı kullanımlarında yeterli dikkat ve özeni göstermemeleri bu kartların kötü niyetli kişilerin ellerine geçmesine ve mağduriyetlere yol açmaktadır. Özellikle yapılan alışveriş veya alınan hizmetten sonunda bedelini ödemek için kredi kartının ilgili kişilere ibrazından sonra bu kartın bir cihazdan geçirilerek şifre bandının okunup bir kopyasının alınması ve başka boş kartlara bu kartın bilgilerinin aktarılması suretiyle oluşturulan sahte kartların kullanılarak haksız menfaat elde edilmesi günümüzde en çok karşılaşılan yöntemdir.

Bir başka yöntem ise, bankamatik de denilen ATM (Automated Teller Machine) cihazlarında yapılan hileli hareketlerle gerçekleştirilebilmektedir.[115]

Karşılaşılan bu olaylarla ilgili Yargıtay 11.Ceza Dairesinin özellikle son içtihatları incelendiğinde uygulamada bu kartlar ile ne kadar farklı yöntemler kullanıldığı daha iyi anlaşılacaktır.

---

[112] Kurt, Leventsh, s.180
[113] Kurt, Levent; s.180 (Oğuzhan Buhur, Tüketici Kredisi Açısından Kredi Kartı Uygulaması, Seçkin Yayınları,
Ankara, 2004, s 59-64)
[114] 245.madde gerekçesi
[115] Karagülmez, Ali, Dr. Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, (2005) sh.198

Yargıtay 11.Ceza Dairesince; Sanıkların olay günü, başkasına ait manyetik kart bilgileri ile birlikte kart şifrelerini ele geçirip, bu şekilde ele geçirilen manyetik bilgileri beyaz kart denilen boş kartlara yazarak kartların ikizini üretmek suretiyle bu kartlarla alış veriş yapmak yada nakit para çekmek için, X Bank'a ait ATM makinesinin güvenlik kamerasını bantla kapatarak, yanlarında getirdikleri 60 cm uzunluğunda içinde çeşitli elektronik bağlantılar bulunan kamera düzeneğini ve kart kopyalama cihazını ATM makinesine monte ederek araçlarında beklemeye başladıkları sırada henüz kopyalama yapamadan yakalanmaları[116],sanıkların bilgileri kodlanarak sahte üretilmiş yurtdışı kredi kartını temin edip sahibi oldukları üye işyerindeki P.O.S. cihazından geçirdikleri ve alışveriş yapılmadığı halde yapılmış gibi gerçeğe aykırı bir biçimde üretilen slipleri katılan bankaya ibraz ederek haksız menfaat sağlamaları[117],eylemlerinin 5237 Sayılı TCK. nun 245.maddesindeki suçu oluşturduğuna karar verilmiştir.

TCK. nun 245.maddesinde dört çeşit suç türü öngörülmüştür:

1.) Başkasına ait bir banka veya kredi kartının, her ne suretle olursa olsun ele geçirilmesinden sonra, sahibinin rızası olmaksızın kullanılması veya kullandırttırılması yoluyla yarar sağlanması (m. 245, 1).

Açıklanan suretle sağlanan yararın zorunlu olarak failin kendi lehine olması şart değildir. Bir başkasına sağlanan yarar da suçun oluşumu bakımından yeterlidir.

Bu fıkradaki suçun oluşması için;

- Başkasına ait gerçek bir banka veya kredi kartını,
- Her ne suretle olursa olsun ele geçiren veya elinde bulunduran kişi
- Kart sahibinin rızası olmaksızın bu kartı kullanarak veya kullandırtarak,
- Kendisine veya başkasına yarar sağlayacak.

Bu sayılan hallerin mevcudiyeti durumunda 1.fıkradaki suçun tüm unsurları itibariyle oluştuğunu kabul edilecektir. Suça konu kartın artık ne şekilde ele geçirildiği önemli değildir.

Bu madde ile önceki 765 Sayılı TCK. nunda 525/b-2 veya 504/3.maddesi kapsamında cezalandırılan olaylar artık bu madde kapsamında değerlendirilecektir.

Örneğin; sanığın şikâyetçinin düşürdüğü cüzdandaki kredi kartını kullanarak A.T.M cihazından para çekmesi eylemi[118], bir bankada güvenlik görevlisi olan sanığın şikâyetçi adına düzenlenen kredi kartını ve şifresini haksız olarak ele geçirerek A.T.M

[116] Yargıtay 11.C.D. 26.04.2006 gün ve 06/1856 E, 06/3468 K
[117] Yargıtay 11.C.D. 19.04.2006 gün ve 05/1480 E, 06/3222 K
[118] Yargıtay 11.C.D. 22.11.2002, 8953/9326

den para çekme eylemi [119], sanığın ölen babasına ait bankamatik kartını kullanarak A.T.M. cihazından kesilmesi gereken emekli maaşını çekme eylemi [120] 765 Sayılı TCK. nun 525/b–2 maddesindeki suçu oluşturacağı belirtilmiş iken bu tür filler artık 5237 Sayılı TCK. nun 245/1.maddesinde değerlendirilecektir.

2.) Başkasına ait olan ve kendisine verilmesi gereken bir banka veya kredi kartının, elinde bulunduran kimse tarafından, kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanılması veya kullandırttırılması suretiyle kendisine veya başkasına yarar sağlanması (m. 245, 1).

Örneğin; Türkiye İş Bankası Manyas Şubesinde güvenlik görevlisi olarak görev yapan sanığın, şikâyetçi adına gelen bankamatik kartını teslim formunu onun yerine imzalamak suretiyle haksız olarak ele geçirip ATM makinesinden para çekmesi eylemi[121], banka tarafından düzenlenmiş kredi kartının kart hamiline ulaşmadan dağıtım şirketi elemanınca kullanılması eyleminin[122]765 Sayılı TCK. nun 525/b–2 maddesindeki suçu oluşturacağı belirtilmiş iken bu tür filler artık 5237 Sayılı TCK. nun 245/1.maddesinde değerlendirilecektir.

3.) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi satın alınması veya kabul edilmesi (m.**245,2**)

1. Başkasına ait gerçek bir banka hesabı ile ilişkilendirilerek,
2. Sahte banka veya kredi kartı
3. Üreten
4. Satan
5. Devreden
6. Satın alan
7. Kabul eden

Kişiler cezalandırılacaktır.

Bu fıkradaki suçun oluşması herhangi bir neticenin gerçekleşmesi şartına bağlanmamıştır. Yani suç başkasına ait gerçek bir hesabı ile ilişkilendirilmiş sahte banka veya kredi kartının üretildiği, satıldığı devredildiği, satın alındığı veya kabul edildiği anda oluşur. Ayrıca bir yarar sağlanma zorunluluğu yoktur.

4.) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartının kullanılması suretiyle yarar sağlanması (m. 245, 3).

[119] Yargıtay 11.C.D. 13.11.2002, 11255/8921
[120] Yargıtay 11.C.D. 06.10.2003, 6778/6714
[121] Yargıtay 11.C.D. 17.02.2004, 12910/827
[122] Yargıtay 6.C.D. 26.04.1999, 2418/2370

Bu durumda da yararın zorunlu olarak failin kendi lehine olması şart olmayıp bir başkasına sağlanması da suçun oluşumu bakımından yeterlidir.

- Sahte oluşturulan
- Veya gerçek olmasına rağmen üzerinde sahtecilik yapılan
- Bir banka veya kredi kartını
- Kullanmak suretiyle
- Kendisine veya başkasına
- Yarar sağlayan
- Kişi,
- Fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde

Bu fıkradaki suç kapsamına girmekte bu fıkra uyarınca cezalandırılmaktadır.

Bu fıkradaki suçun 1.fıkradaki suçtan farkı;1.fıkradaki suçun konusunu gerçek bir banka veya kredi kartı oluştururken,3.fıkrada sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartları bu suçun konusunu oluşturmaktadır.

Sahte kart oluşturmak, bu kartları üretmeye yarayan cihazlarla gerçekleştirilmektedir. Banka kartının üzerinde, kart sahibinin banka hesabıyla ilgili bilgileri içeren manyetik bir şerit vardır. Bu manyetik şeride söz konusu bilgiler, "**encoder**" adı verilen bir aygıtla yüklenmektedir. Böylece, sahte oluşturulan kartla, gerçek kart gibi haksız yararlanma yapılmaktadır.[123]

Örneğin; sanığın manyetik şeridi …bank A.Ş. ne ait kart bilgisinin kodlandığı sahte alışveriş ve kredi kartlarını kendi işyerinde bulunan dört bankaya ait P.O.S. cihazlarından birkaç gün içinde geçirdiği ve alış-veriş yapılmadığı halde yapılmış gibi gerçeğe aykırı biçimde üretilen sliplerin bedellerini bankadan tahsil etme eylemi[124],Katılan ...B. nın tüm elektronik cihazlarını karşılamak üzere faaliyet gösteren, bankanın yönetim ve denetimine sahip olduğu "B.... Bilgi İşlem ve Pazarlama A.Ş." de analist olarak görev yapan sanığın, kredi kartları sistemleri konusu ile ilgili serviste, 1997 yılının Şubat ayından 1999 yılının Ağustos ayına kadar müşterinin kredi kartı numara ve şifrelerini ele geçirerek, bu bilgileri evinde elde edilen "ENCODER" adlı cihaz aracılığıyla boş beyaz kartlardaki manyetik şerit üzerine kopyalayarak değişik zamanlarda farklı A.T.M. cihazlarından para çekmesi şeklinde oluşan eylemlerin[125] 765

[123] Karagülmez, Ali, Dr. Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, 2005sh.212
[124] Yargıtay 11.C.D. 25.03.2004, 2369/2304
[125] Yargıtay 11.C.D. 01.04.2004, 13869/27073

Sayılı TCK. nun 525/b–2 maddesi uyarınca cezalandırılması gerektiği belirtilmiştir. Bu eylemler hakkında artık 5237 Sayılı T.C.K. nun 245. maddesinin 2. fıkrasında belirtilen "başkalarına ait banka hesaplarıyla ilişkilendirilme" unsuru gerçekleşmişse sözü edilen fıkra, bu unsur gerçekleşmiyorsa ve fiil sadece sahte oluşturulan kredi kartı aracılığı ile menfaat temin etme ise aynı maddenin 3.fıkrasındaki suç oluşacaktır.

Banka ve Kredi Kartlarının kötüye kullanılması suçlarını düzenleyen 245.madde de dört çeşit suç düzenlenmiştir. Buradaki suç tiplerinden ikinci fıkradaki suçun oluşması bir neticeye bağlanmamış iken diğer üç suçun oluşması bir neticeye bağlanmıştır.

Buna göre 245.maddenin 1.fıkrasında düzenlenen "Başkasına ait bir banka veya kredi kartının, **her ne suretle olursa olsun ele geçirilmesi**nden sonra, sahibinin rızası olmaksızın kullanılması veya kullandırttırılması ile başkasına ait olan ve kendisine verilmesi gereken bir banka veya kredi kartının, **elinde bulunduran** kimse tarafından, kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanılması veya kullandırttırılması" ve 3.fıkrasında düzenlenen "**Sahte oluşturulan** veya **üzerinde sahtecilik yapılan** bir banka veya kredi kartının kullanılması" suçlarının gerçekleşmesini kanun koyucu faile veya başkasına lehine "bir yarar" sağlanması şartına bağlamış iken, aynı maddenin 2.fıkrasındaki "başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi satın alınması veya kabul edilmesi" suçunun oluşması için sadece sayılan hareketlerin yapılmasını suçun oluşumu için yeterli görmüş ayrıca bir netice öngörmemiştir.

Genel kural olarak kanundaki tanım, suçun failini, hareketi, suçun konusunu ve sübjektif unsurunu içerir. Bazı suçlarda herhangi bir kişi değil, ancak belli sıfatı ya da nitelikleri taşıyan kişiler fail olabilir. Rüşvet alma ve zimmet suçlarında, memur sıfatına sahip olma gibi. İşte, ancak belli bir sıfatı taşıyan kişiler tarafından işlenebilecek bu tür suçlara, özgü suçlar (mahsus suç) denir. Çoğu suçlarda ise suçun faili, kanundaki tanımda genellikle "her kim" ya da "bir kimse" olarak gösterilir. Bu tür suçları, herhangi bir kişinin işlemesi mümkündür. Buna, herkes tarafından işlenebilen suçlar da denir.[126] İşte "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu" da son sayılan suçlardandır. Failin bir sıfat veya nitelik taşımasının suçun oluşması açısından bir önemi yoktur. Sadece 245.maddenin son fıkrası uyarınca; Birinci fıkrada yer alan suçun;

> a)Haklarında ayrılık kararı verilmemiş eşlerden birinin,
> b)Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

[126] A. Taşkın, İ. Zengin, 2004, s. 36

c)Aynı konutta beraber yaşayan kardeşlerden birinin,
Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

Ayrıca yeni getirilen düzenleme ile TCK. nun 246.maddesi[127] uyarınca tüzel kişiler de bu suçun faili olabilirler.

Banka ve Kredi Kartlarının Kötüye Kullanılması suçlarının en önemli hususlarından biride bu maddedeki suçların mağdurlarının kim olduğunun tespit edilmesidir. Suçun mağduru açısından herhangi bir özellik aranmamıştır. Herkes bu suçun mağduru olabilir. Burada bu suçla korunan hukuki yararın ne olduğu sorusuna verilecek cevap suçun mağdurunun tespitini daha kolaylaştıracaktır.

245.maddedeki suçlarla, kişinin mal varlığının korunduğunda kuşku yoktur. Ancak, bir taraftan da bankacılık hizmetlerinin güvenle, hızlı bir şekilde yapılması ve dolayısıyla da, ekonomik yapının sağlıklı işlenmesi korunmak istenmektedir.[128]

Her suç açısından ayrı ayrı mağdur kavramını incelersek:

a**-** Başkasına ait bir banka veya kredi kartının, **her ne suretle olursa olsun ele geçirilmesi**nden sonra, sahibinin rızası olmaksızın kullanılması veya kullandırttırılması yoluyla yarar sağlanması suçunda suçun konusunu gerçek bir banka veya kredi kartı oluşturacağı için bu suçun mağduru kartın sahibi olan kişidir. Burada her ne kadar bir banka veya kredi kurumunun bilişim sistemi aracı olarak kullanılmakta ise de; bu sistemlerinin kullanılması banka veya ilgili kurumun bu suçun mağduru olduğu anlamına gelmemektedir.

b- Başkasına ait olan ve kendisine verilmesi gereken bir banka veya kredi kartının, **elinde bulunduran** kimse tarafından, kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanılması veya kullandırttırılması suretiyle kendisine veya başkasına yarar sağlanması suçunda da yine suçun konusunu gerçek bir banka veya kredi kartı oluşturacağı için bu suçun mağduru kartın kendisine verilmesi gereken kişidir. Ancak, kartın kendisine verilmesi gereken kişi bu kart ilk defa ilgili banka veya kredi kurumu tarafından kendisine teslim edilmesi gereken kişi ise ve kartın kendisine teslim edilmediğini ispat etmesi durumunda suçun mağduru bu kartın ait olduğu banka veya kredi kurumudur. Çünkü kart fiilen ve hukuken kart hamiline teslim edilmediği ve kart üzerindeki mülkiyet hakkı kurulmadığından söz konusu kart üreten banka veya kredi kurumuna ait kabul edilmelidir.

c- Başkalarına ait **banka hesaplarıyla ilişkilendirilerek** sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi satın alınması veya kabul edilmesi suçunda

[127] **MADDE 246.** - [1] Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.
[128] Karagülmez, Ali, Dr. Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, 2005sh.199

suçun oluşumu için herhangi bir zarar oluşması şartı aranmaktadır. Ancak yine de bu suçun mağduru hesabı ilişkilendirilerek sahte kart üretilen, satılan, devredilen veya kabul edilen **hesap sahibi**dir.

d- **Sahte oluşturulan** veya **üzerinde sahtecilik yapılan** bir banka veya kredi kartının kullanılması suretiyle yarar sağlanması suçunda ise; eğer gerçek bir banka hesap numarası kullanılarak sahte bir kart oluşturulmuş ise;bu kart sahibi suçun mağdurudur.Burada şöyle bir sorun bulunmaktadır.Özellikle son zamanlarda yurt dışında çeşitli ülkelerden elde edilen yabancı bankalara ait kart bilgileri ile sahte kartlar üretilip bu kartlar ile harcamalar yapılmaktadır.Söz konusu kartlarla satış yapan iş yeri sahipleri satış sliplerini pos cihazını kullandığı bankaya ibraz ederek bedelini tahsil etmekte ve dolayısıyla bir zararı olmamaktadır.Şimdi burada çözümlenmesi gereken konu işyeri sahibine slip bedelini ödeyen banka bu ödediği bedeli karta kopyalanan hesabın bulunduğu yabancı ülkedeki bankadan ödediği bedeli alıyor ise o zaman bu eylemden dolayı direkt olarak zarar gören yabancı ülkedeki bankada hesabı bulunan kişidir.Ancak bu hesap sahibi söz konusu kartın harcandığı tarihlerde Türkiye'de bulunmadığını veya slipteki imzaların kendisine ait olmadığını ispat ederse o takdirde zarara uğrayan hesabın bulunduğu yabancı bankadır.Ancak bu banka bu tür fiiller için sigorta işlemi yaptırmış ise dolayısıyla banka zararını sigorta şirketinden karşılayacağından bu fiilden dolayı mağdur olan zararı ödeyen sigorta şirketi olacaktır.

Eğer fail hayali hesap numaraları ile ürettiği sahte kartları kullanarak doğrudan bir banka veya kredi kurumunun mal varlığında bir zarara yol açmış ise;elbette mağdur ilgili banka veya kredi kurumudur.

Banka ve Kredi Kartlarının Kötüye Kullanılması suçlarını düzenleyen 245.maddesinin 1.fıkrasında düzenlenen her iki suçun konusunu "**gerçek bir banka veya kredi kartı**", 2.fıkrasındaki suçun konusu "**gerçek bir banka hesabıyla ilişkilendirilerek sahte üretilen banka veya kredi kartı**" ve 3.fıkrada düzenlenen suçun konusu " **ya tamamen sahte oluşturulan veya üzerinde sahtecilik yapılan gerçek bir banka veya kredi kartı** " dır.

245.maddenin 1.fıkrasında düzenlenen "Başkasına ait bir banka veya kredi kartının, **her ne suretle olursa olsun ele geçirilmesi**nden sonra, sahibinin rızası olmaksızın kullanılması veya kullandırttırılması ile başkasına ait olan ve kendisine verilmesi gereken bir banka veya kredi kartının, **elinde bulunduran** kimse tarafından, kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanılması veya kullandırttırılması" ve 3.fıkrasında düzenlenen "**Sahte oluşturulan** veya **üzerinde sahtecilik yapılan** bir banka veya kredi kartının kullanılması" suçlarının gerçekleşmesini için "**bir yarar**" sağlanması özel kastı aranmış iken, aynı maddenin

2.fıkrasındaki "başkalarına ait **banka hesaplarıyla ilişkilendirilerek** sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi" suçunun oluşması için failde ürettiğini, sattığını, devrettiğini, satın aldığını veya kabul ettiğini banka veya kredi kartının sahte olduğunu bilmesi kastı aranmaktadır. Burada özellikle sahte kredi kartının satılması, devredilmesi, satın alınması veya kabul edilmesi kastı ispat etmek hiç de zor olmayacaktır. Çünkü bir kişinin banka veya kredi kartını başkasına satması, devretmesi veya başkasına ait bir banka veya kredi kartını satın alması, kabul etmesi hayatın olağan akışına ters bir durumdur.

245. maddenin 1.fıkrasında düzenlenen "Başkasına ait bir banka veya kredi kartının, **her ne suretle olursa olsun ele geçirilmesi**nden sonra, sahibinin rızası olmaksızın kullanılması veya kullandırttırılması ile başkasına ait olan ve kendisine verilmesi gereken bir banka veya kredi kartının, **elinde bulunduran** kimse tarafından, kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanılması veya kullandırttırılması" ve 3.fıkrasında düzenlenen "**Sahte oluşturulan** veya **üzerinde sahtecilik yapılan** bir banka veya kredi kartının kullanılması" suçlarının gerçekleşmesini kanun koyucu faile veya başkasına lehine "**bir yarar**" sağlanması şartı arandığından bu yararın gerçekleşmesi ile suç tamamlanmış olacağından eğer bu yarar gerçekleşmemiş ise suçun teşebbüs aşamasında kaldığını söylemek mümkündür. Aynı maddenin 2.fıkrasındaki "başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi satın alınması veya kabul edilmesi" suçunun oluşması için sadece sayılan hareketlerin yapılmasını suçun oluşumu için yeterli görülmüş ayrıca bir netice öngörülmemiş olduğundan fail suçun tipik hareketlerine uygun bir şekilde sahte kart üretmek isterken yakalanmış ise kart üretimi henüz tamamlanmadı için suçun teşebbüs aşamasında kaldığından söz edilebilir.

Özellikle 245/1.fıkradaki suçta hem gerçek hem de fikri içtima kuralları uygulanabilir. Çünkü ilgili fıkrada banka veya kredi kartının"**her ne suretle olursa olsun ele geçirilmesi"**nden söz ettiği için dolandırıcılık, güveni kötüye kullanmak, kaybolmuş veya hata sonucu banka veya kredi kartı ele geçirilmiş ve üzerinde tasarrufta bulunulmuş ya da hırsızlık yoluyla ele geçirilmiş ise kartı kullanarak elde ettiği haksız menfaat nedeniyle mutlaka 245/1.fıkra uyarınca, ayrıca diğer suçlar yönünden ise şartları var ise mahkûmiyeti yönüne gidilmelidir.

Eğer kart yağma yoluyla elde edilmiş ise TCK. nun 148/1.maddesinde düzenlenen yağma suçunun cezası 245/1.maddesindeki cezadan daha ağır

olduğundan fail hakkında aynı kanunun 44.maddesi gereğince yağma suçundan cezalandırılma yoluna gidilecektir.[129]

TCK'nun 37. maddesinde, suçun kanuni tanımında yer alan fiili birlikte gerçekleştiren kişilerden her birisinin fail olarak sorumlu olduğu, ikinci fıkrasında ise, suçun işlenmesinde bir başkasını araç olarak kullanan kişinin de fail olarak sorumlu tutulacağı, kusur yeteneği olmayanları suçun işlenmesinde araç olarak kullanan kişinin cezasının da üçte birden yarısına kadar arttırılacağı düzenlenmiştir. Fiilin işlenişi üzerinde kurulan hâkimiyet ölçü olarak belirlenmiş, iştirak şekilleri ise, faillik, azmettirme ve yardım etme olarak sayılmıştır. Bilişim suçlarını birden fazla kişinin işlemesi durumunda bunlardan her birisi müşterek fail olarak sorumlu tutulacaklardır. Yine gerekçe bir suçun failine, onun haberi olmaksızın, tek taraflı iradeyle, suçun işlenmesine başlamadan önce veya suçun icrası sırasında yardım edilmesi hâlinde, müşterek fail olarak değil, yardım eden olarak sorumlu tutulmak gerektiği belirtilmiştir.[130]

Azmettirme başlıklı TCK. nun 38. maddesinde, başkasını suç işlemeye azmettiren kişinin, işlenen suçun cezası ile cezalandırılacağı, üstsoy ve altsoy ilişkisinden doğan nüfuz kullanılmak suretiyle suça azmettirme hâlinde, azmettirenin cezasının üçte birden yarısına kadar artırılacağı, çocukların suça azmettirilmesi hâlinde, bu fıkra hükmüne göre cezanın artırılabilmesi için üstsoy ve altsoy ilişkisinin varlığının aranmayacağı, azmettirenin belli olmaması hâlinde, kim olduğunun ortaya çıkmasını sağlayan fail veya diğer suç ortağı hakkında ağırlaştırılmış müebbet hapis cezası yerine yirmi yıldan yirmibeş yıla kadar, müebbet hapis cezası yerine onbeş yıldan yirmi yıla kadar hapis cezasına hükmolunabileceği, diğer hâllerde verilecek cezada, üçte bir oranında indirim yapılabileceği belirtilmiştir. Azmettirme konusunda ki bu genel hükümler bilişim suçları hakkında da uygulanacaktır.[131]

Yardım etme başlıklı TCK'nun 39. maddesinde, suç işlemeye teşvik etme, suç işleme kararını kuvvetlendirme, fiilin işlenmesinden sonra yardımda bulunacağını vaat etme, suçun nasıl işleneceği hususunda yol gösterme, fiilin işlenmesinde kullanılan araçları sağlama, suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunarak icrasını kolaylaştırma hallerinde bu fiilleri işleyen kişinin işlenen suçtan dolayı yardım eden sıfatıyla sorumlu olacağı, bu kişiye, işlenen suçun ağırlaştırılmış müebbet hapis cezasını gerektirmesi hâlinde, onbeş yıldan yirmi yıla; müebbet hapis cezasını gerektirmesi hâlinde, on yıldan onbeş yıla kadar hapis cezası verileceği, diğer hâllerde

[129] Aynı görüş için bkz. Karagülmez, Ali, Dr. Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, 2005 sh.208
[130] Kurt,2005 sh 267
[131] Kurt,2005 sh 268

cezanın yarısının indirileceği, bu durumda verilecek cezanın sekiz yılı geçemeyeceği, belirtilmiştir.

Başkasına ait bir banka veya kredi kartının, **her ne suretle olursa olsun ele geçirilmesi**nden sonra, sahibinin rızası olmaksızın kullanılması veya kullandırttırılması yoluyla **yarar sağlanması** veya başkasına ait olan ve kendisine verilmesi gereken bir banka veya kredi kartının, **elinde bulunduran** kimse tarafından, kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanılması veya kullandırttırılması suretiyle kendisine veya başkasına **yarar sağlayan** kişi hakkında; **3** yıldan **6** yıla kadar hapis ve **5.000** güne kadar adlî para cezası,

Başkalarına ait **banka hesaplarıyla ilişkilendirilerek** sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi satın alınması veya kabul eden kişi hakkında; **3** yıldan **7** yıla kadar hapis ve **10.000** güne kadar adlî para cezası,

Sahte oluşturulan veya üzerinde sahtecilik yapıla**n** bir banka veya kredi kartının kullanılması suretiyle yarar sağlayan kişi hakkında; fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, **4** yıldan **8** yıla kadar hapis ve **5.000** güne kadar adlî para cezasına Hükmolunacağı belirtilmiştir.

5560 Sayılı Kanunun 11.maddesi ile aşağıdaki fıkra 245.maddeye 5.fıkra olarak eklenmiştir.

"(5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır."[132]

Bu eklenen fıkra ile artık 245.maddenin 1.fıkrasındaki "Başkasına ait bir banka veya kredi kartının, **her ne suretle olursa olsun ele geçirilmesi**nden sonra, sahibinin rızası olmaksızın kullanılması veya kullandırttırılması yoluyla **yarar** sağlanması" suçu ile "Başkasına ait olan ve kendisine verilmesi gereken bir banka veya kredi kartının, **elinde bulunduran** kimse tarafından, **kartın kendisine verilmesi gereken kişinin rızası olmaksızın** kullanılması veya kullandırttırılması suretiyle kendisine veya başkasına **yarar** sağlanması" suçlarında sanığın TCK.nun 168.maddesinde öngörülen şartları yerine getirmesi halinde etkin pişmanlıktan yararlanma olanağı

[132] **Madde 168 -** (Değişik madde: 29.06.2005–5377 S.K./20.mad)
(1) Hırsızlık, mala zarar verme, güveni kötüye kullanma, dolandırıcılık, hileli iflâs, taksirli iflâs ve karşılıksız yararlanma suçları tamamlandıktan sonra ve fakat bu nedenle hakkında kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde, verilecek cezanın üçte ikisine kadarı indirilir.
(2) Etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi halinde, verilecek cezanın yarısına kadarı indirilir.
(3) Yağma suçundan dolayı etkin pişmanlık gösteren kişiye verilecek cezanın, birinci fıkraya giren hallerde yarısına, ikinci fıkraya giren hallerde üçte birine kadarı indirilir.
(4) Kısmen geri verme veya tazmin halinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır.

getirilmiştir.Ancak bu imkanın 1.fıkradaki suçların yanında 3.fıkradaki suç içinde getirilmesinin daha uygun olacağı kanaatindeyiz.

Ülkemizde son yıllarda banka ve kredi kartı kullanımının yaygınlaşması bu kartlarla işlenen suçların artışına sebep olmaktadır. “Her nimetin bir külfeti vardır” atasözünde belirtildiği üzere hayatımızı kolaylaştıran günün her saatinde üzerinizde para olmasa da cüzdanınızda bulunan küçük bir plastik kartla nakit para çekebilme veya alışveriş yapabilme imkânını size sağlayan bu teknolojik kolaylıklar, kötü niyetli insanların iştahlarını kabartmakta ve yeni suç çeşitlerini geliştirmek için kullandıkları bir alan olmaktadır. Hele bir de insanlarımızın bu konudaki umursamaz ve farkında olmama hallerini hesaba kattığımızda bu alanda yasa dışı gelir elde etmenin kolaylığı artık inanılmaz boyutlara ulaşmaktadır.

Uygulamada önümüze gelen dosya içeriğindeki olaylara baktığımızda büyük çoğunluğundaki esas sorun insanların banka ve kredi kartları konusundaki bilgisizliği, tecrübesizliği ve teknolojiye olan uzaklığı nedeniyle bu kartlarla başına gelebilecek olumsuzlukların farkında olmamasıdır. Bu farkındasızlığın cahillik, okuma yazma bilmemek veya kültürlü olmak veya olmamakla da alakası yoktur. Örneğin bir okulumuzda yaşanan bir olayda çocuklarımıza eğitim veren, bilgilendiren ve aydın kesim olarak kabul ettiğimiz bir kaç öğretmen maaş günü bankamatikten para çekilmesi için bir kâğıda bankamatik şifrelerini yazıp üzerine bankamatik kartlarını öğretmenler odasındaki masanın üzerine hizmetlinin alması için bıraktıkları, bu sırada odaya giren çaycının masa üzerinde şifrelerinin de yazılı bulunduğu banka kartlarını görünce dayanamayıp aldığı ve bu kartlardan günlük çekebileceği limitleri çekmesi şeklinde gelişen olaydaki problem nereden kaynaklanmaktadır. Teknolojinin eksikliğinden mi yoksa sevgili öğretmenlerimizin “farkındasızlığından mı”? Tabii ki bu tür suçlarda bütün kabahat daima kart sahiplerinde değildir. Devletin özellikle bankacılık sektöründe acilen bankalara bu tür kartların güvenliğini arttırmaları konusunda yükümlülükler yüklemesi gerekmektedir. Yine sahte kart üretiminde kullanılan “Encoder” cihazının ülkemizde alımı satımı dağıtımı hiçbir kurala ve mevzuata bağlı olmadığını görüyoruz. Bu tür cihazların satımının belli bir mevzuat çerçevesinde ancak belli kişi yada firmalara verilmesi ve satılan bu cihazların kime satıldığı, söz konusu cihazla ne kadar ve hangi numaralarda kart üretildiğinin yine yetkili organlar tarafından denetlenebilmeye müsait olması gerekmektedir.

1.1.2007 tarihinde tam olarak yürürlüğe giren kredi kartlarında zorunlu olarak uygulanacak olan “**Chip&Pin**” uygulaması bir nebze banka ve kredi kartlarının kötüye kullanılması suçlarının azalmasına yarayacağı kanaatindeyiz.Çünkü kredi kartının üzerindeki **chip**, kartın kopyalanmasına karşın koruma sağlarken, şifre (**PIN**) ise kartın

kaybolması ya da çalınması durumunda başkaları tarafından kullanılamaması nedeniyle ikinci bir koruma sağlayacaktır.

Sonuç olarak günlük hayatımızı kolaylaştıran ve cebimizde can dostumuz gibi birçok zaman imdadımıza yetişen kartlarımızın bilinçli ve dikkatli kullanmadığımız zaman bir anda hayatımızı karartacak bir nesneye dönüşebileceğini hiç unutmamalıyız.

Gerçekten de yetkililerin verdiği bilgilere göre "**Chip&Pin**" uygulaması bir nebze banka ve kredi kartlarının kötüye kullanılması suçlarının azalmasına yardımcı olabileceği görülmeye başlamıştır. Bu bağlamda son dört ay içersinde kredi kartları üzerinden yapılan dolandırıcılık ve sahtekarlık cirolarının Nisan- Aralık 2005 ile Nisan-Aralık 2006 arasında % 55, Ocak-Mart 2005 ile Ocak- Mart 2006 tarihleri arasında ise % 67 oranlarında düştüğü belirtilmiştir.

Bu oranların düşme eğiliminde iken şifrelerin alış verişlerde kullanımları da aksine artmakta ve % 70'lere ulaştığı söylenmektedir[133].

3.13 Çocuk Pornografisi

Bir çocuğun gerçek veya kurgulanmış herhangi bir cinsel aktivite içinde gösterilmesi veya vücudunun belli yerlerinin cinsel amaçla gösterilmesidir. Cinsel doyum diğer cinsel istismar türlerinden farklı olarak çocukla cinsel bir aktivitede bulunmak yerine, çocuklarla ilgili materyale bakmak veya izlemekle sağlanır. Görüntüler; Fotoğraflar, filmler, CD'ler veya videokasetler halinde olabilir, İstismarcının özel kullanımına ait olabileceği gibi, pornografi pazarında ticareti de yapılabilir, Etkiyi arttırıcı küçük bir hikâye ile porno magazinlerinde yer alabilir, Cinsel istismar türlerini sergiliyor / bunları özendiriyor olabilir.

Yeni teknolojiler pornonun doğasını değiştirmiştir. Dijital kameralar ve fotoğraf Makinelerinin ürünleri, çoğaltılırken eskimediği ve bozulmadığı içi üretim kolay ve ucuz hale gelmiştir. İnternet'in takip edilemezlik ve sınırları aşma özelliği de eklenince çocuk pornosu engellenmesi çok güç bir duruma dönüşmüştür. Bütün bunlara ek olarak, günümüzde dijital grafik programları iki görüntüyü birleştirme veya fotoğrafları bozarak ve değiştirerek yeni görüntüler elde etme becerisine sahiptir. Bu durumda, aslında pornografik olmayan fotoğraflar pornografik hale kolaylıkla getirilebilmektedir. Böylece "sanal çocuklar" yaratılmaktadır. Ancak, çocuk pornosu sadece çıplak çocuk fotoğraflarına indirgenemez. Gerçek ya da sanal bile olsa gerçek hayatta çocuk taciziyle direkt bağlantısı bulunmaktadır.

---

[133] "Çipli Kredi Kartları Sahtekarlıklığı Azalttı";
http://www.bugun.com.tr/haberler/180407/p45646.html (20.04.2007);
http://www.alomaliye.com/ekonomi/2007/cipli_kredi.htm (20.04.2007);
"Çipli kartlar sahtekarlığı yüzde 25 azalttı**"**
http://www.btdunyasi.net/index.php?module=news&news_id=3246&cat_id=1 (20.04.2007).

Evlerinden kaçmış çocuklar gibi sömürüye müsait çocukların ticari amaçla görsel materyal üretenler tarafından çocuk pornografisinde kullanılmalarına rastlanmaktadır. Çocuk pornosunda, kurban sömürüldüğünün farkına varmayabilir veya utanç ve korkuyla bu konuda sessiz kalmayı tercih edebilir. Ayrıca tehdit ve korkutma yoluyla da konuşmamayı tercih etme sıklıkla gözlenen bir olaydır. Özellikle son dönemde artık bebeklerin bile bu tarz cinsel sömürüde kullanıldıkları tespit edilmiştir.

Günümüzde yaygın kullanımı bulunan İnternet', çocuk pornosu malzemelerine ulaşılmasını ve bu tür malzemelerin dünyada serbest dolaşımını çok kolay hale getirmiştir. İnternet pornografinin yaygınlaşmasına hizmet etmiştir. Dünyada çocuk pornografisi milyonlarca dolarla ifade edilen bir sektördür. Onaltı yaşından küçük yaklaşık 600.000 çocuğun sektörde sömürüldüğü ve Amerika Birleşik Devletleri'nde toplam sektörün %7'sinin çocuk pornosuyla ilgili olduğu bildirilmiştir[134]. Bunun dışında hemen hemen tüm pornografi sitelerinin bir bölümü çocuk pornografisine ayrılmış durumdadır.

İnternet İzleme Vakfı'nın (IWF) hazırladığı rapora göre Çocuk Pornografisinin çıkış yeri Amerika Birleşik Devletleridir. ABD sitelerindeki pornografik fotoğraflar ve görüntüler, tüm dünyadakilerin % 51'ini oluşturmaktadır.

Çocuk Pornografisinde ABD'nin ardından
% 14.9'la Rusya,
- % 11.7'yla Japonya,
- % 8.8'le İspanya,
- % 3.6'yla Tayland,
- % 2.1'le de Güney Kore
- % 7.7 de Diğer Ülkeler, şeklinde sıralanmaktadır[135].

ABD hükümeti, çocuk pornografisiyle mücadele için nisan ayında hazırladığı yasa tasarısı İnternet servis sağlayıcılarına çocukların kullanıldığı pornografik görüntüleri yetkililere bildirme zorunluluğu getirmiştir.

Amerika'da çocuk pornografisinin, yıllık yaklaşık 2-3 milyar dolar hacme sahip büyük ve kirli pazarlardan biri olduğu belirtilmektedir. John Hopkins Üniversitesinin Koruma Projesine göre, bazı toplumlarda çocuk trafiği çok yüksek seviyelerde seyretmektedir. Elde edilen verilere göre,

- Indiana'da 14 yaşındaki 200.000 Nepallı kız çocuklarının seks kölesi olarak çalıştırıldığı,

[134] http://www.psikoloji.gen.tr/modules.php?name=News&file=article&sid=338 (14.04.2007)
[135] http://www.iwf.org.uk/media/news.196.htm (21.04.2007)

- Sri Lanka'da yaşları 6 ila 14 arasında değişen 10.000 çocuğun geneleve düştüğü,

- 600.000 Taylandlı çocuğun fahişelik için satıldığı ve

- 1991–97 arasında Kamboçyalı 15.000 kızın cinsel kölelik için satıldığı tespit edilmiştir.

Amerika Birleşik Devletleri'nde 1996 yılında Çocuk Pornografisinin Önlenmesi Yasası çıkarılmıştır. Federal Temel Yasa'nın 18. Bölümünün 2252. maddesi'nde gerekli değişiklikler yapılarak, çocukların görüntülendiği pornografik yayın ve materyallerin elde bulundurulması veya İnternet'te yayınlanması yasaklanmıştır [136].

İngiltere'de Cybercops olarak adlandırılan polisler, çocuk pornosuyla mücadelenin yanı sıra bu kanalla yapılan yasa dışı ticaret, bilgisayar programlarına girme ve kart yolsuzluğuyla da mücadele etmektedirler.

Fransa'da, küçüklere yönelik olmamak şartıyla pornografi suç teşkil etmemektedir. 1994 tarihli yeni Fransız Ceza Kanununa göre, (m.227–24) pornografik ve şiddet içerikli yayınların, İnternet'i de kapsayacak şekilde hangi araçla olursa olsun küçükler tarafından erişilebilir kılınması suçtur.

Almanya'da Alman Tele Servisler Kanunu'nda 14.12.2001 tarihinde yapılan bir değişiklikle, erişim sağlayanların kural olarak kısa süreyle yapılan depolama işleminden sorumlu tutulamayacağı açıklanmış; bilgilere müdahale etmesi, teknik şartlara uymaması ve kısa süreli olarak depoladığı bilgilerin ilk kaynak noktasında ağa girişinin kapatıldığını veya silindiğini öğrenmesi veya bilgilere ilişkin hukuka aykırılığın bir mahkeme veya idari bir makam tarafından bildirilmesine rağmen yayından kaldırmayarak muhafazaya devam etmesi durumların servis sağlayıcılar gibi sorumlu tutulacağı öngörülmüştür.

İtalya'da, Kişiye Karşı İşlenen Suçlar kısmında "Bireysel Kişiliğe Karşı Suçlar" başlıklı bölüme, çocuğun kişi hürriyetini korumak, onun fiziki ve psikolojik gelişmesine karşı kişiliğine zarar veren fiilleri cezalandırmak üzere, çocuk pornografisi ve çocuk ticareti, çocuğun fuhşa sevki gibi konularda 3.8.1998 tarih ve 269 sayılı kanunla İtalya Ceza Kanunu'na birtakım hükümler eklenmiştir[137].

---

[136] ANALAY,Cengiz., GÜLŞEN,Recep, Bilişim Suçları İçinde Çocuk Pornografisi ve Mücadele Yöntemleri, http://www.turkhukuksitesi.com/makale_154.htm (10.12.06)

[137] Polonya'da da, çocuk pornografisi yasaklanmıştır. 1997 tarihli Polonya Ceza Kanunu'na göre (m.200/2), çocukların cinsel yönden sömürülmesine engel olmak amacıyla, küçük çocukların katılımıyla gerçekleştirilen resim, film, videobantları gibi pornografiler cezalandırılmaya tabi tutulmaktadır.
Hollanda'da, 1993 tarihli 'Computer Crime Act' yasalaşmadan önce Hollanda polisi bilgisayar suçları ile mücadele için özel bir birim kurmuştur. Bilgisayar suçları birimleri Adalet Bakanlığına bağlı kriminal laboratuarları, 'Information Technology and Crime Department of the National Criminal Intelligence Division ve Detective's Training Collage ile birlikte çalışmaktadırlar.

Bilindiği üzere 18.05.2001 tarihli Bakanlar Kurulu kararıyla onaylanıp ülkemiz bakımından da yürürlüğe giren ve 17.06.1999 tarih ve 182 sayılı ILO sözleşmesinden, temel haklara ilişkin bir sözleşme olan "Kötü Şartlardaki Çocuk İşçiliğinin Yasaklanması ve Ortadan Kaldırılmasına İlişkin Acil Önlemler Sözleşmesi" uyarınca da çocukların cinsel istismarının etkin cezalandırmaya tabi tutulması gerekmektedir.

BM Genel Kurulu tarafından 23 Mayıs 2000 tarihinde imza, onay ve katılıma açılmış ve Türkiye tarafından da 9 Eylül 2000 tarihinde imzalanıp daha sonra onaylanarak yürürlüğe giren BM Çocuk Haklarına Dair Sözleşme' ye ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili Seçmeli Protokolde de, Sözleşmenin yukarıda anılan maddelerinin daha iyi uygulanmasını sağlamak üzere bir hüküm öngörülmüştür. Bu protokole göre, "Çocuk pornografisinin İnternet'te ve diğer gelişen teknolojiler üzerinde erişilebilirliği artmıştır. O nedenle, Seçmeli Protokolle ülkeler, çocuk pornografisini, üretim, dağıtım, yayma, ithal ya da ihracını, sunumunu, satışını veya zilyetliğini yasaklamayı ve cezalandırmayı garanti etmişlerdir .(Madde 3)

Birleşmiş Milletler Genel Asamblesi tarafından 20 Kasım 1989 tarihinde kabul edilerek 2 Eylül 1990 tarihinde de yürürlüğe konulan Çocuk Hakları sözleşmesine göre: On sekiz yaşına kadar her insan çocuk sayılır. Çocukların yaşamını korumak herkesin görevidir ve yaşamak her çocuğun temel hakkıdır. Yetiştirmekten sorumlu olanlar haklarını çocuklara zarar verecek şekilde kullanıyorsa her türlü önlemi almak devletin görevidir. Çocukları bedensel ve ruhsal yönden örseleyecek hiçbir yaklaşıma izin verilemez. Taraf Devletler, çocuğun, ekonomik sömürüye ve her türlü tehlikeli işte ya da eğitimine zarar verecek ya da sağlığı veya bedensel, zihinsel, ruhsal, ahlaksal ya da toplumsal gelişmesi için zararlı olabilecek nitelikte çalıştırılmasına karşı korunma hakkını kabul ederler. Ayrıca araf Devletler, çocuğu, her türlü cinsel sömürüye ve cinsel suiistimale karşı koruma güvencesi verirler.

İspanya'da Enformasyon Teknolojilerindeki Suçları Araştırma Birimi adı altında faaliyet gösteren emniyet görevlileri, teknoloji, iletişim, telekomünikasyon ve çocuk pornografisi alanlarında işlenen suçları ve ortaya çıkan şikâyetleri takip etmektedirler.
Japonya'da yapılan yasal düzenleme ile, siber suçlar alanında çocuk pornografisi de suç kapsamına alınmış, çocuklara yönelik her türlü pornografik materyalin satış, dağıtım, üretim, bulundurma ve ticaretini yapanlara üç yıl hapis ve 24.400 dolar para cezası öngörülmüştür.
Malezya'da teknolojik suçlara ilişkin çıkarılan Dijital Signature Act, Multimedia Convergence Act, Computer Crime Act, Telemedicine Development Act. gibi kanunlarda yer alan bilgisayar suçları arasında, çocuklara yönelik istismar ve müstehcenlik de yer almaktadır. Malezya'da siber suçlarla mücadele, Haberleşme, Multimedya ve Enerji Bakanlığı'nın sorumluluk alanına girmektedir.
Rusya'da İçişleri Bakanlığı, İnternet üzerinden suç ve suçluların takibi için delillerin korunması amacıyla İnternet hizmeti sağlayan servislerle işbirliği yapmakta; İnternet firmalarına verilerini 6 ay saklama ve yargı makamlarının talebi olduğu takdirde söz konusu verileri ilgili makamlara sağlama zorunluluğu getirmiştir.
İsrail'de Emniyet Müdürlüğü, bilgisayar üzerinde işlenen suçlarla 1996 yılında ilgilenmeye başlamış ve güvenlik teşkilatının içinde Bilgisayar Suçları Bölümü kurmuştur. Birimdeki bu görevliler, bilgisayar konusunda eğitimden geçirilmiş polislerden oluşmakta; gerektiğinde diğer polis birimlerince yürütülen soruşturmalara da yardımcı olmaktadırlar.

SSS madde 9'a göre her bir taraf devlet, hukuka aykırı olarak kasıtlı bir şekilde; Bilgisayar sistemi vasıtasıyla çocuk pornografisini üretmek, bilgisayar sistemi vasıtasıyla çocuk pornografisini temin edilebilir hâle getirmek veya göstermek Bilgisayar sistemi vasıtasıyla çocuk pornografisini aktarmak veya dağıtımını yapmak, kendisi veya başkası için bilgisayar sistemi vasıtasıyla çocuk pornografisi temin etmek, bir bilgisayar sisteminde veya bilgisayar veri depolama ortamında çocuk pornografisi çocuk pornografisine sahip olmak, fiillerinden sorumlu tutulması için gerekli kanuni düzenlemeyi yapmalı ve ihtiyaç duyulan önlemleri almalıdır.

SSS madde 9 fıkra 2'ye göre ise 1.paragrafta geçen "çocuk pornografisi" tanımı şu şekilde yapılmıştır; " Bir küçüğün cinsel olarak kullanılmasını, bir küçük gibi görünen kişinin cinsel olarak kullanılmasını, bir küçüğü temsil eden gerçekçi bir imajın cinsel olarak kullanılmasını görsel olarak içeren pornografik materyaldir."

SSS'ye göre 2.paragrafta geçen "küçük"den kasıt, 18 yaşın altındaki herkestir. Taraf devlet buna karşın, 16 yaşından az olmamak üzere daha düşük bir yaş sınırı belirleyebilir.

Türk kamuoyu çocuk pornografisi ile, İngiliz Gizli Servisi tarafından uluslararası yürütülen ve 18 ülkede çocuk pornografisi suçlarının faili 132 kişinin yakalandığı Landmark Operasyonu sonucunda Türkiye'den de faillerin yakalanması ile tanışmıştır[138].

Bu olayda ülkemizde ilk kez kullanılan bir teknikle, İnternet bağlantısını sağlayan firma belirlenerek, mahkeme kararıyla IP numarasının sahibi tespit edilmiş ve fail ele geçirilmiştir.

Aynı dönemde Bilişim Suçları ve Araştırma Büro Amirliği tarafından hazırlanan raporda, çocuk pornografisinin de içinde bulunduğu yasadışı yayınlara ilişkin suçlarda önceki yıllara nazaran bir artış görüldüğü, bunların içinde %40'lık pay ile çocuk pornografisi yayınının en çok işlenen suç olduğu iddia edilmiştir[139]. Ancak buradan belirtilmelidir ki adli istatistikler 5237 S. TCK yürürlüğü girdiği tarihe kadar özellikle bilişim suçları açısından sağlıklı tutulamamıştır. Çünkü Adli Siciller bu zamana kadar 525 a, b, c, d maddeleri sadece TCK 525 maddesi çatısı altında tutulmuş ve sağlıklı sonuçlar alınamamıştır.

765 sayılı TCK. nun çocuk-yetişkin ayrımı gözetilmeksizin, pornografik yayınlara ilişkin olarak para cezasını öngören TCK'nun 426. maddesinin çocuk pornografisi suçları bakımından hürriyeti bağlayıcı ceza öngörmüyor olması bakımından kanunun yürürlükte olduğu dönemde haklı olarak eleştirilmiştir.

---

[138] http://www.aksam.com.tr/arsiv/aksam/2004/10/31/gundem/gundemprn1.html (14.04.2007)
[139] http://www.turkhukuksitesi.com/makale_154.htm (14.04.2007)

26.09.2004 tarihinde kabul edilerek Haziran 2005 tarihinde yürürlüğe giren Türk Ceza Kanunu 6.bölümünde “Cinsel Dokunulmazlığa Karşı Suçlar” başlığı altında cinsel suçlar işlenilmiştir. Çocukların Cinsel istismarı ile ilgili olarak 5237 Sayılı TCK’da yer alan bazı maddeler ve içerikleri şunlardır;

Cinsel saldırı (Madde 102)

Çocukların cinsel istismarı (Madde 103)

Reşit olmayanla cinsel ilişki (Madde 104)

Cinsel taciz (Madde 105)

5237 sayılı TCK’nun yedinci bölümde ise “Genel Ahlaka Karşı Suçlar” başlığı altında yer alan müstehcenlik kavramı toplumun genel ahlakını tehdit edebilecek bir konu olarak değerlendirilmiştir. 7. bölümde yer alan bazı suçlar ve başlıkları şunlardır;

Hayasızca hareketler (Madde 225)

Müstehcenlik, (Madde 226)

Fuhuş (Madde 227)

En önemlisi Türk Ceza Kanunu Madde 226- Müstehcenlik başlıklı madde de direk başlığı çocuk pornografisi olmasa da dolaylı olarak çocuk pornografisi suçu da düzenlenmiştir. 226. Maddenin 3. maddesi Müstehcen görüntü, yazı veya sözler içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılacağına ve bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılıcağı düzenlenmiştir.

Adalet Bakanlığının hazırlayarak Başbakanlığa sunduğu Bilişim Suçları ile ilgili Tasarı’da çocuk pornografisi bağlantılı suçlar başlıklı tasarının 26. Maddesinin 1. Fıkrası; “ Bir çocuğa veya çocuk gibi görünen veya çocuk olduğu izlenimi veren bir kişiye ait gerçek ya da temsili görüntü, yazı veya sesleri içeren pornografik ürünleri bilişim ortamında dağıtmak amacıyla üreten kişiye sekiz yıldan on iki yıla kadar hapis ve beş bin güne kadar adlî para cezası verilir.” şeklinde düzenleme yapmış bulunmaktadır.

İkinci fıkra ise birinci fıkra kapsamına giren ürünleri, bilişim ağı üzerinden tanıtan, sunan, kiraya veren veya satışa arz eden kişiye iki yıldan beş yıla kadar hapis ve bin güne kadar adlî para cezası verilir demek suretiyle verilen cezaların artırım nedenini göstermektedir. Üçüncü fıkra ise birinci fıkra kapsamına giren ürünleri, bilişim ağı üzerinden kendisi veya başkaları için temin eden veya bulunduran kişilere altı

aydan bir yıla kadar hapis ve üç yüz güne kadar adlî para cezası verileceğini hükme bağlamıştır.

Ancak kanaatimiza göre 5237 sayılı Türk Ceza Kanunu'nun 226.maddesinde işlenilen çocuk pornografisi maddesine "benzeştirme" konusu da dahil edilmelidir.

Üniversiteler veya sivil toplum örgütleri tarafından düzenlenecek seminer ve konferanslar ile konunun önemi gündeme getirilmeli ve kamuoyunun bilgilenmesi aşamasında medya kurumlarından da faydalanılmalıdır. Özellikle kolluk ve adli makamların üst düzey yöneticilerini bilgilendirmek amacıyla çalışmalar yapılmalı seminerler düzenlenmelidir.

Bu alanda çalışan kolluk görevlileri ve adli makamların görevlilerinin teknik olarak ekipman eksiklikleri tamamlanmalıdır. Suçluların kullandığı teknik ekipmanların gerisinde kalmış teknik malzemeler ile sürdürülen çalışmaların yetersiz kalacağı aşikârdır.

Ceza Muhakemeleri Kanununun 135/6 maddesinde düzenlenen dinleme, kayda alma ve sinyal bilgilerinin düzenlenmesine ilişkin iletişimin dinlenebildiği suç türleri arasına TCK 226. madde hükmü de eklenmelidir.

Bunların ötesinde "Kayıp ve Sömürülen Çocuklar Uluslarası Merkez"in hazırlamış olduğu 2007 raporuna göre[140]; Türkiyede yapılması gereken bazı yasal düzenlemeler daha olduğu iddia edilmektedir. Raporla çocuk pornografisi ile tam bir mücadele içinde olabilmek için model bir mevzuatın ne olduğu konusunda bir çalışma yapılmış ve ülke mevzuatları incelenerek ortaya bazı ilkeler konulmaya çalışılmıştır.

Bu rapora göre yapılan çalışmalar sırasında ilk olarak ülke mevzuatlarında çocuk pornografisine özgü bir düzenleme olup olmadığı, ikinci olarak çocuk pornografisinin açıkça tanımı yapılmış olup olmadığı, üçüncüsü çocuk pornografisinin bilişim sistemleri aracılığı ile işlenmesi halinde özel bir cezai yaptırımın var olup olmadığı, dördüncüsü çocuk pornografisi içerikli verilerin bulundurulması cezalandırılıp cezalandırılmadığı, beşinci ve sonuncusu ise servis sağlayıcılar şüpheli pronografik içerikleri adli kolluğa veya benzeri resmi bir kuruma bildirme yükülülü olup olmadıkları konularında araştırma yapılmaya çalışılmıştır.

Çıkan sonuçlara göre sadece beş ülkenin mevzuatı araştırılan bu konulara olumlu yanıt vermekte, 23 ülke ilk dört kriteri mevzuatında barındırmakta, servis sağlayıcıların rapolaması konusunda kural bulundurmamakta, 95 ülkenin mevzuatında ise sırf çocuk pornografisine özgü bir düzenlemenin bulunmadığı bildidirilmiştir. Kalan ülkelerden ise 55 ülkenin mevzuatında çocuk pornografisini tanımlamadığını, 27

[140] Child Pornography Legistation: A Comperative Report; International Centre for Missing & Exploited Children (ICMEC) Daha fazla bilgi için bkz.; http://www.icmec.org/ (20.04.2006)

ülkenin ise yasalarında çocuk pornografisini açıkça tarif etmediği, 43 ülkede ise çocuk pornografik içeriklerin bulundurulmasının suç olmadığı iddia edilmiştir[141].

Raporda diğer ülkeler konusunda yapılan değerlendirmeler Türkiye hakkında da yapılmış ve ülkemizde çocuk pornografisinin kastedilerek Yeni 5237 S TCK'nunda düzenleme yapılmış olsa da Hükümet, kolluk güçleri ve sivil toplum tarafından çocuk pornografisinden tam olarak korunma sağlanması için daha çok şeyin yapılması gerektiğinin anlaşıldığını ifade etmiştir.

Rapora göre yukarıda belirtilen ilkeler ışığında ülkemizin çocuk pornografisi konusunda ABD ve Fransa'da mevcut olan mevzuat ile karşılaştırma durumu aşağıdaki tablodaki gibidir;

Ülke	Fransa	Türkiye	ABD
Çocuk pornografisine has mevzuat var mı?	Fransız Yeni Ceza Kanunu (FYCK) Madde 227–23	Yeni Türk Ceza Kanunu (YTCK) Madde226 " Müstehcenlik" ☑	18 Nolu ABD Federal Yasası 1466 (A), 2251, 2251A, 2252, 2252A, 2260, 2422, 2423
Çocuk tanımı yapılmış mı?	Fransız Medeni Kanunu Madde 488	YTCK 6 (1) b ☑	18 Nolu ABD Federal Yasası 2256 (1)
Çocuk pornografisinin tanımı yapılmış mı?	FYCK 227–23	YTCK 226 (3) Kısmi tanım olduğundan bahsediliyor ☑☒	18 Nolu ABD Federal Yasası 2256 (8)
Bilgisayarla işlenmesi kolaylaşan suç olarak düzenlenmiş mi?	FYCK 222–24 FYCK 225–7 (1) ile (10) arası FYCK 227–22 FYCK 227-23FYCK 227–26	Uygulanabilir karşılık olmadığı iddia edilmiş, ancak YTCK 226/5 ve 6/g maddeleri ile bu konu artırım maddesi halinde düzenlenmiş[142] ☑	18 Nolu ABD Federal Yasası 1030 (e)(1)

[141] http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=3085 (20.04.2007)

[142] 5237 S. YTCK 226/(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.
5237 S. YTCK 226/ (5) Üç ve dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.
5237 S. YTCK 6/g) Basın ve yayın yolu ile deyiminden; her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar,

Basit Bulundurma suç olarak var mı?	FYCK 227–23/ 3	YTCK 226/3 ☑	18 Nolu ABD Federal Yasası 1466(A) (b) 18 Nolu ABD Federal Yasası 2252 A (a) (5)
Servis sağlayıcılar tarafından raporlama var mı?	21 Haziran 2004 t. 2004–575 sayılı K. Madde 6 (1) - (7)	☒	42 Nolu ABD Fedaral Yasası 13032

Aynı Kurum'un 2006 yılında yayınlamış olduğu raporda da Avustralya, Belçika, Fransa, Güney Afrika ve ABD kurum tarafından çocuk pornografisi ile mücadelede olması gereken yasal düzenlemerlerden beş düzenlemenin de bu ülkelerde bulunduğunu belirtimiştir. Örneğin Almanya'da servis sağlayıcıların açıkça çocuk pornografisi içeren içerikleri raporlaması konusunda yasal zorunluluk olmaması nedeniyle her türlü önlemi alan ülkeler listesine alınmamıştır. Oysaki Alman Teleservisler Yasasına göre servis sağlayıcı hizmet sunduğu sunucularda çocuk pornografisi içeren yayın bulunduğu bilmesi halinde bunlara engelleme yapması ve yayından kaldırması yasal bir zorunluluk olarak bulunmaktadır. 2006 yılı raporunda ayrıca Türkiyedeki çocuk pornografisi ile ilgili yasal mevzuat hakkında yapılan değerlendirmelerde kanaatimizce bazı hatalı saptamalar bulunmaktadır[143].

ABD'nin 42 Numaralı Federal Yasasının 13032.maddesinin (b) fıkrasının (4) nolu bendinde elektronik iletişim konusunda faaliyet gösteren servis sağlayıcı veya uzaktan bilişim hizmeti sağalayan kişiler bilerek ve isteyerek çocuk pornografisi konusunda rapor çıkarma konusundaki görevini yerine getirmezse ilk defada 50.000$'a kadar, diğer seferlerde 100.000$'a kadar para cezası ile cezalandırılacaklarını düzenlemiştir[144].

ABD'de çocuk pornorafisi ile ilgili ilginç olan diğer hukuksal düzenlemeler ise çocuk pornografisi suçu işlemiş mahkumlar hakkında ayrıca adli sicil düzenleniyor olması ve bu kayıtların halka açık olması. Zira Amerikan yetkilileri çocuk pornografisi suçu işleyen kişiler şifası zor olan hastalıklı kişiler olarak değerledirilmekte ve verilen ceza sonrası normal hayata döner dönmez bu suçu yine işlemeleri nedeniyle[145] bu

[143] Child Pornography: Model Legistation&Global Review 2006; İnternational Centre for Missing and Exploited Children; 2. Baskı; s.15

[144] Child Pornography Legistation: A Comperative Report 2007; International Centre for Missing & Exploited Children (ICMEC); s.43 Daha fazla bilgi için bkz.; http://www.icmec.org/ (20.04.2006)

[145] Örnek olarak geçen sene Belçikada çocuk pornografisi suçundan hapis yatan bir mahkumun serbest kalmasından sonra 15 yaşında iki kız çocuğunu kaçırarak aynı suçu işlemesi göserilmekte. Sakin, Mehmet; "Çocuk İstismarından Kazanılan Para, Uyuşturucudan Elde edilenden Öne Geçti "Sektörsel Bilgi Teknolojileri, (26.04.2007 tarihli nüsha)

suçlularla mücadelede mecburen bu tür tedbirlere başvurmak zorunda kalmalarını göstermekteler. Ancak doğal olarak bu tedbirler özellikle kişisel verilerin korunması ve kişisel mahremiyet açısından yoğun şekilde eleştiriliyor olması kuvvetle muhtemel. Diğer önemli bir gelişme ise ABD'nin bu tür suçlarla mücadelede özel gelişmiş teknikler kullanarak suçları delillelendirme yöntemleri geliştirmesi. Uzmanların beyanına göre bu konuda özel uzmanlar da yetiştirilmekte.

3.14 Sanal Kumar

Dilimize Arapçadan gelen 'kumar' sözcüğü: "Ortaya para veya mal konularak oynanan bir talih oyunu." anlamına gelmektedir. Kumar oynatmak ise, belli bir pay karşılığında, uygun bir yer temin ederek, kumar oynanmasını sağlamak, olarak tanımlanmıştır. Hukuki açıdan kumar, 818 sayılı Borçlar Yasasında ve 5237 sayılı TCK'da farklı düzenlenmiştir. Borçlar Hukukunda kumar ve bahis kavramları ayrıntılı olarak açıklanmıştır. Medeni hukuka göre kumar: "Birden fazla kişinin eğlenmek, kazanç sağlamak yahut fikri ya da bedeni ustalıklarını geliştirmek amacı ile az veya çok ustalığa veya talihe bağlı birbirine zıt şartlar altında karşılıklı olarak aralarında kazanacak olana bir edim taahhüt ettikleri bir sözleşmedir"[146].

Borçlar hukukuna göre kumar ve bahis borcu doğuştan eksik borç olarak nitelendirilmiş; borçlu tarafından ifa edilirse, bu ifayı geçerli sayılmış ve bu ödemenin sebepsiz zenginleşme ve bağış teşkil etmeyeceği, taraflara arasında esas olarak borç ilişkisinin varlığını ve borçlu borcu bilerek ödemiş olduğu gerekçesi ile ifa edilen borcun geri istenmesini mümkün kılmamıştır. Kumar ve bahis borçlarından doğan alacaklar ile ilgili sözleşmeleri B.K. 19. ve 20. maddeleri kapsamına almış ve bu tür borçlarının ifası vaad edilemeyeceği gibi kefalet veya rehin yolu ile teminat altına alınamayacağı ve takas edilemeyeceği düzenlenmiştir. Kumar ve bahis borçları, borçlu tarafından yerine getirilmezse, alacaklı, dava ve icra takibi yoluna başvuramaz. Bu düzenlemenin istisnası ise; milli piyango, spor toto, loto, iddia ve at yarışlarıdır.

Ceza Hukuku açısından kumar : "Kazanç amacı ile icra edilen ve kar ve zararın talihe bağlı bulunduğu oyunlardır." Ceza Kanunu, kumar oynatmayı ve kumar oynamayı suç olarak nitelendirmektedir. Kumar oynama ve kumar oynatma suçu için görevli mahkeme sulh ceza mahkemesi olup, ön ödeme kapsamında olan suçlardan da değildir.

Sanal ortama da oynatılan kumar: Online kumar, e-kumar, İnternet'te kumar, online Casino veya sanal kumar gibi değişik ifadeler ile adlandırılmaktadır. Sanal kumarın hukuki olarak bir tanımı yapılmamıştır. Ancak bir tanım yapmak gerekirse:

[146] http://www.bilisimhukuku.net/index2.php?option=com_content&do_pdf=1&id=566 (14.04.2007)

Bilişim ortamlarında, şansa ve beceriye dayanan, oyun araç ve gereçleri ile veya bir kasaya karşı para veya benzeri maddi değerler karşılığı oynatılan oyunlardır. Tanımda, bilişim ortamları terimiyle anlatılmaya çalışılan: İnternet', İnteraktif televizyon ve artık günümüz teknolojileri ile cep telefonlarıdır.

İlk Türkçe kumar sitesini, 2000 yılında, Türklerin sanal kumara ilgisini fark eden Anthony Mataye adlı bir Amerikalı tarafından kurulmuştur. Kumar tutkunlarının yüzde 2.5'ini Türklerin oluşturduğunu ortaya çıkaran Mataye, Güney Amerika yakınlarındaki Antigua isimli bir adaya giderek kumar lisansı almıştır. Siteye isim olarak da Türkçede oyun kâğıtlarında en çok kullanılan kelimelerden biri olan "as" sözcüğünün içinde olduğu "ascasino.com"'u seçerek ilk Türkçe kumar sitesini kurmuştur[147].

Sanal kumar dünyanın en hızlı gelişen endüstri biri olup United States General Accounting Office GAO tarafından yapılan resmi araştırmaya göre 2003 yıllı verileri itibari ile yıllık 4 milyar dolarlık işlem hacmine ulaşmıştır. Bu hızlı gelişmeye paralel olarak dünyada sanal kumar ile ilgili düzenlemeler yapılmaya başlanmıştır. Ancak yasalaştırma süreçlerinin dünyanın hemen hemen her yerinde yavaş işliyor olması; adeta saniye saniye değişen bilgi teknolojileri karşısında hukukun egemenliği etkisiz kılmaya başlamıştır. Be nedenle yasa koyucular statik hukuk kuralları yerini esnek, değişken, yoruma açık ve teknolojik gelişimlere paralel olarak uygulanabilir türden yasalaştırma çalışmaları içerisine girmişlerdir. Aşağıda dünyanın farklı ülkelerine ait başlıca hukuk ekollerini temsil eden bazı bölgelerden sanal kumara dair düzenlemelerden örnekler verilmiştir[148].

İlk olarak Türkiye'de kumar oynamak ve kumar oynatmak için yer temin etmek Türk Ceza Kanununa göre suç teşkil etmektedir. Türkiye'de fiziki ortamlarda kumar oynamak ve oynatmak ceza-i yaptırımı nedeniyle gizli bir şekilde yapılmakta ve kumarhane sayısı sanal ortamdaki kumarhane sayısını nazaran daha az olmaktadır. Ancak, İnternet'e taşınan kumarhaneler sayesinde, kumar oynamak isteyen kişilere her hangi bir ceza-i yaptırım riski olmadan istedikleri her yerde ve istedikleri zaman kumar oynama olanağı sağlanmaktadır. Bilişim ortamında bulunan kumarhaneler sayesinde hem fiziki kumarhanelerde oynanabilen kumarların dışında dünyanın dört bir yanındaki futbol, basketbol, at yarışı, boks ve tenis maçları için iddiaya girme, pey sürme olanağı sağlamaktadır.

Yine bir Ticaret Odası'nın hazırladığı "SANAL TUZAK: İNTERNET' KUMARHANELERİ" raporuna göre; ülkemizde yeni kumar oynayan bağımlıların 75%'ni sanal ortamda kumar oynayanlar kişilerden oluşmaktadır ve bu 75%'lik oranın büyük bir çoğunluğunu kadınlar ve çocuklar oluşturmaktadır. Kadınlar, büyük bir oranla fiziki

[147] http://www.milliyet.com.tr/ozel/interaktif/000504/index.html (14.04.2007)
[148] http://www.bilisimhukuku.net/index2.php?option=com_content&do_pdf=1&id=566 (14.04.2007)

mahalde bulunan kumarhanelere gidememesi sebebi ile çocuklar ise merak ettikleri için ücretsiz olan kumar sitelerinde kumar oynamaya başlamaktadır[149].

Türkiye'de kumar oynatmak 5237 sayılı TCK'nun 228.maddesi uyarınca yasaklanmıştır. Kanun maddesi fiziki ve sanal ortam ayrımı yapmadan kumar oynatılmasını suç saymaktadır. Ancak; Ceza kanunun onuncu bölümünde bilişim suçları sayılmış olup İnternet üzerinden oynanan kumar sayılmamıştır. Bilişim suçlarını ayrı bir bölümde değerlendirilmesi ve bu bölümde bilişim ortamlarında oynanan kumarın sayılmaması sebebi ile sanal ortamda kumar oynamayı kanun koyucu ağırlaştırılmış sebep olarak kabul edilmemiştir.

Ülkemizde sanal kumarın öne geçebilmek için Milli Piyango İdaresi "Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik Taslağı" oluşturmuştur. Bu tasla hukuki dayanak olarak , Milli Piyango İdaresi Genel Müdürlüğü Kuruluş ve Görevleri hakkında 320 sayılı kanun hükmünde kararnamenin 3. maddesinin (e) fıkrası ile 15.,29., 31.,32. ve 35. maddesine istinaden düzenlenmiştir[150].

Milli Piyango İdaresi tarafından hazırlanan Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik Taslağı'nın amaç ve kapsamı taslağın 1. ve 2. maddelerinde açıkça belirtilmiştir. Yönetmeliğin 4. maddesinde; "Sanal ortam" kelimesinin tanımında teker teker sayma yerine "Bilişim ortamları" demesi yeterli olabilirdi. Ayrıca "Talih oyunları" kelimesinin açıklaması kumar kelimesinin kapsamını aşmıştır. Şöyle ki; Kumar; beceri ve şansa dayanan, oyun araç gereçleri ile bir kasaya karşı veya oyun makinelerine karşı para ve veya mukabili maddi değerler ile oynanan oyunlardır. Ancak tanımda veya sanal ortamlarda oynatılan oyunlar diyerek kumar tanımını aşmış ve idareye sanal ortamda para karşılığı oynanmayan İnternet sitelerini de denetleme yetkisi vermiştir. Tanım sanal ortamda oynatılan talih oyunlarını anlatmak için "bilişim ortamlarında, şansa ve beceriye dayanan, oyun araç ve gereçleri ile veya bir kasaya karşı para veya benzeri maddi değerler karşılığı oynatılan oyunlardır."şeklinde düzeltilmelidir.

3.15 Botnetler

BotNet kavramı ülkemizde bilinmeyen ancak birçok gelişmiş ülke güvenlik güçleri tarafından üzerinde çalışılan önemi ve riski bilinen bir dijital tehlikedir. BotNet'lerin oluşturduğu tehlikeyi anlamak için günümüzde bilgisayarlarda bulunan bilgilerin öneminin kavranması gereklidir. Günümüzde bilgisayar disklerinde sadece

[149] http://www.aksam.com.tr/arsiv/aksam/2004/11/21/ekonomi/ekonomi8.html (14.04.2007)
[150] http://www.ncp.com.tr/haber_detay.asp?ID=457&baslik_id=2 (14.04.2007)
"**Sanal kumara yasak geliyor"; "**Sanal ortamda oynanan şans oyunlarına yasak geliyor. Son 2 yıldır boyutları giderek artan sanal ortamda oynatılan yasadışı kumar ve bahis siteleriyle mücadele edilmesi için oluşturulan özel komisyonun çalışmalarının ardından Milli Piyango İdaresi Genel Müdürlüğü'nce hazırlanan "Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik Taslağı", Başbakanlığa gönderildi."

kişisel bilgiler değil, ekonomik ve hukuki değeri olan ve bilgi çağında değeri hiç bir parayla ölçülemeyecek kadar bilgi mevcuttur.

BotNet'in özet olarak neden olduğu şu şekilde ifade edebilir; suçlular ana bilgisayarlarıyla diğer bilgisayarlara virüsler göndermekte ve virüslü bilgisayarları esir almaktadırlar. Diğer taraftan bu yüz binlerce bilgisayarı aynı zamanda yönetebilmekte ve tek bir hedefe, **örneğin**; **200,000 bilgisayarın gücüyle tek bir hedef için saldırmaktadır. Maalesef bu kadar büyük bir gücün karşısında durabilecek kadar güvenli bilişim sistemi henüz icat olunmamıştır.** Diğer taraftan Botnet sunucularını yönetenler kendilerine köle ettiği bilgisayarların hepsindeki kayda değer tüm bilgileri (hesap bilgileri, şifreler, projeler, dosyalar, programlar, kişisel veriler) çalmaktadırlar. Örneğin; TÜBİTAK'ta yıllarca üzerinde çalışılmış ve para harcanmış bir proje bu tip bir saldırı sonucunda çalınabilir. **BotNet saldırılarının mağdurları; öncelikle özel ve kamu bilgisayarları, daha sonra özel ve kamu bilişim sistemlerdir.** Botnet saldırıları sadece bireysel güvenlik anlamında değil, **ulusal güvenlik anlamında da çok büyük bir risk oluşturmaktadır.**

Botnet yönetici bilgisayarlarının (saldırıların yönetildiği bilgisayar) 12 %si Türk Telekom'dan hizmet alan bilgisayarlar aracılığıyla gerçekleştirildiği bunun ise **dünya sıralamasında ikinci** olduğu anlaşılmaktadır.

Diğer taraftan yine dünya çapında Ocak- Mart 2006 aylarındaki istatistiklere göre bot olmuş (saldırgan yönetici bilgisayarın her istediğini yapacak hale özetle köle haline gelmiş) en büyük orandaki mağdur bilgisayar %13 ile Türk Telekom müşterisidir ve **Ülkemiz dünya birincisidir**. Türk Telekom (TTNET) müşterisi olan toplam **156686** tane bilgisayar korsanların yönetimine geçmiş ve bu haliyle dünyadaki en riskli bölge haline gelmiş olduğu ifade edilmektedir. Bu durum ülkemizin ne büyük bir risk altında bulunduğunu göstermektedir. Önde gelen bir bilgi güvenliği şirketinin yayınlamış olduğu raporda ise Türkiye en fazla saldırıda bulunan ülke bakımından dünya sıralamasında 17., bot enfekte olmuş bilgisayarlar bakımından EMEA (Avrupa, Ortadoğu, Afrika) Bölgesinde 8. Sırada yer aldığı iddia edilmektedir[151].

Bilgisayar terminolojisinde yer alan şifre kırma işlemi, uzun şifrelerde çok fazla varyasyon olduğundan çok uzun zamanlar alabilmektedir. Ancak 1 bilgisayarla 2 yılda ancak kırılabilecek bir şifre bot edilmiş bilgisayarlarla 5 dakika 20 saniyede çözülebilir. Bu tehlikeyi fark eden Microsoft ve diğer katılımcı ülkeler güçlerini birleştirerek ortak bir platform da bu tür saldırı networklarıyla mücadele etmektedirler. Diğer taraftan normal şartlarda Microsoft'tan adli istinabe ile bile zor temin edilebilecek çeşitli bilgiler basit bir prosedürle görev gücü yetkililerine güvenilerek verilmektedir.

[151] Sektörsel Bilgi Teknolojileri, "İnternet korsanları 'kişiye özel saldırıyor'"(26.04.2007 tarihli nüsha)

Ülkemiz ve teşkilatımızda **riskin tehlikenin büyüklüğü ve neler yapılabileceği konusunda farkındalığın oluşmasının sağlanması çok önemlidir.** Bir çok gelişmiş ülke bu alanda yatırım yaparken bizim BotNet riskini yeni fark etmemiz her ne kadar geç olsa da zararın neresinden dönülürse kardır.

BotNet tehlikesi sadece geleceğin değil günümüzün de büyük riskidir ve **Türkiye dünyadaki 1 numaralı mağdurdur.** Diğer taraftan Ülkemizin bu tür suçlarla mücadele etmek için daha fazla personel görevlendirmesi, eğitim imkânlarının oluşturulması gibi yatırımların büyük bir mağduriyetin ortaya çıkmasından önce yapılması akılcı olacaktır.

3.16 *Bilişim Suçları ile ilgili Hazırlanan Yasa Tasarıları*

3.16.1 Adalet Bakanlığının Hazırlamış Olduğu "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"[152]

Bilişim Suçları ile ilgili Adalet Bakanlığı tarafından Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı yaklaşık bir buçuk yıllık bir komisyon çalışması sonrasında hazırlanmış ve 28.12.2006 tarihinde Başbakanlığa sevkedilmiştir. Bu Tasarı ile özellikle 5237 sayılı TCK da yer almayan bilişim suçlarını Mevzuatımıza dahil etmek ve mevcut olan ve ancak yetersiz olduğu ileri sürülen çocuk pornografisi gibi suçların daha etraflı bir şekilde düzenlenmesi ve cezalarının artırılması amaçlanmıştır[153].

Tasarıda 1. Madde amaç, 2. Bilişim ortamı Madde genel tanımlar konusuna ayrılmış, ilk kez bilgi, bilgisayar, bilişim ağı, bilişim sistemi, çevre birimler, elektronik mühür, erişim, erişim sağlayıcı, içerik sağlayıcı, izleme, ortam sağlayıcı program, istenmeyen ileti yer sağlayıcı (hosting), gibi önemli kavramlar tanımlanmaya çalışılmıştır.

Tasarının ikinci bölümünde servis sağlayıcılarının sorumlulukları, yükümlülükleri ve denetimi düzenlenmiş ve esas ilkenin kişilerin bilgiye ve ifadeye erişimlerinin serbest olduğunun altı çizilmiştir.

Üçüncü bölümde daha çok **dar anlamda bilişim suçu** veya **doğrudan bilişim suçları** denilen suçları, yani bilgilerin gizliliği, bütünlüğü ve elde edilmesine ilişkin suçlar düzenlenmiş, ilk kez SSS'de bulunan hukuka aykırı olarak verilerin ele

---

[152] http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (14.04.2007)
(Kanunun Başbakanlığa Sevk Tarihi: 28.12.2006)

[153] Tasarıda amaç şu şekilde ifade edilmiştir;" Tasarı ile, ülkemizde kullanımı yaygınlaşan bilişim ağlarının ortaya çıkartmış olduğu hukukî ve cezaî sorunların çözüme kavuşturularak bilişim ağı alanında hukuk sistemimizin Avrupa Birliği normları ile uyumunun sağlanması amaçlanmıştır."
http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (13.04.2007)

geçirilmesini sağlayan kötü amaçlı yazılım ve donanım üretmek, bulundurmak, yaymak vs. gibi fiiller suç olarak tanımlanmıştır.

Dördüncü bölümde ise yine SSS deki yapıya uyularak **bilişim sistemiyle bağlantılı suçlara** yer verilmiş ve bu bağlamda bilişim sistemini kullanarak sahtecilik, bilişim ortamında yarar sağlamak, banka veya kredi kartlarının kötüye kullanılması, yanıltarak bilgi toplamak, taklit yoluyla yanıltmak gibi suçlara ve yaptırımlaraına yer verilmiştir. Tasarı ilk kez phishing denilen kimlik hırsızlama yolu ile dolandırıcılık diyebileceğimiz eylemi de suç olarak tanımlamıştır. Bunun yanı sıra sahte İnternet sayfası ve e-posta yollama eylemleri gibi taklit yolu ile kişileri kandırmayı da de suç kapsamına alarak bu konuda ki dünyada ki genel eğilime uymuştur.

Beşinci bölüm ise içerik bağlantılı suçlar ve bunların idari yaptırımlarına ayrılmıştır. Bu kapsamda; çocuk pornografisi bağlantılı suçlar, devletin güvenliğine ve kamu barışına karşı işlenen suçlar, kararın yerine getirilmemesi, cezaların arttırılması, tüzel kişiler hakkında güvenlik tedbiri uygulanması, idarî para cezaları ve özellikle de istenmeyen iletilere yönelik olarak**; "**İstenmeyen ileti gönderene üçbin Türk Lirasından onbeşbin Türk Lirasına kadar, idarî para cezası verilir" hükmü ile ilk kez idari para cezası yaptırımı öngörülmüştür.

Altıncı şu anda mevzuatımızda eksik olan erişimin engellenmesi konusu ele alınmış, bu bölümde Soruşturma ve Kovuşturma Usulleri açıklanmış ve hangi usulde yayınların içeriğinin erişiminin engelleneceği konusu üzerinde durulmuştur. Aynı zamanda bu konudaki talepler bakacak görevli mahkemeler ilgili usul açıklanmıştır.

Çeşitli ve son hükümleri düzenleyen yedinci ve son bölüm ise çıkarılacak yönetmeliklere temas etmiş ve aynı zamanda 32. Madde ile Türk Ceza Kanununun İkinci Kitabının Üçüncü Kısmının Onuncu Bölüm başlığı ile 243 ilâ 246 ncı maddeleri yürürlükten kaldırılmış olduğunu ifade ederek, Tasarının ilk halindeki gibi TCK daki hükümlere dokunmamazlık etmemiş ve haklı olarak çok eleştiri alan, bilişim suçlarının hem TCK'da, hem de bu Yasada yer almasının uygulamada kargaşa yaratacağı yolundaki eleştirileri dikkate aldığı söylenebilir.

16 Aralık 2006 günü Türkiye Bilişim Derneği Hukuk Çalışma Grubu'nun çağrısı ile Haymana'da bir araya gelen ve aralarında TBD Hukuk Çalışma Grubu üyesi Ankara Barosu ve İstanbul Barosu'na mensup avukatlarla, Askeri Yargıtay Üyeleri, Adalet Bakanlığı'nda görevli hakimler, Yargıtay Tetkik Hakimleri'nin bulunduğu hukukçular "Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı"nı iki gün süren bir çalışmada ele alınmış ve Tasarı ile ilgili aşağıdaki aşağıdaki tespitler yapılmıştır. Ancak daha sonra Adalet Bakanlığı tarafından Tasarı üzerinde bazı değişiklikler yapılmış ve Tasarıdaki bazı maddeler Tasarıdan çıkarılmıştır. Ayrıca

parelel yürüyen ve halen TBMM'de olan ve Adalet Komisyonunda kabul edilen Ulaştırma Bakanlığı tarafından hazırlanan "İnternet Ortamında İşlenen Suçlarla Mücadele Kanun Tasarısı" adı Komisyon çalışmaları sırasında , "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Kanunu Tasarısı" olarak değiştirilmesine karar verildiği ve sadece erişimin engellenmesi değil bunun yanı sıra Tasarının kapsamının genişletilirek Adalet Bakanlığının hazırlamış olduğu İnternet Servis Sağlayıcılarla ilgili bazı hükümlerin Ulaştırma Bakanlığı tasarısına alındığı anlaşılmaktadır. Bu bağlamda Ulaştırma Bakanlığının hazırlamış olduğu Yasa Tasarısının içerik sağlayıcı, yer sağlayıcı, ortam sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri de kapsayacak şekilde yasalaştırılacağı haber verilmektedir[154].

Türk Ceza Kanunu'nda gerek bilişim sistemleri aracı kılınarak işlenen suçlar gerekse de bilişim alanında suçlar düzenlenmiş olup, konunun yeniden ayrı bir kanunla ele alınması "genel kanun" "özel kanun" tartışmalarına gereksiz yere yol açacaktır. Ayrıca iki ayrı kanunda benzer fiiller için hüküm bulunması ve cezalar arasındaki oransızlık birçok karışıklığa sebebiyet verecektir. Bu nedenle tasarıdaki cezai hükümlerin 5237 Sayılı TCK'da, kabahatlerin Kabahatler Kanununda ve usul hükümlerinin de CMK'da düzenlenmesinin; ceza hükmü içermeyen düzenlemelere bu Kanun Tasarınında yer verilerek ayrı bir kanun olarak yürürlüğe konulmasının uygun olacağı değerlendirilmektedir.

Tasarının 1. maddesinde düzenlenen "Amaç ve kapsam" ile ilgili hükümlerinin, Tasarının diğer bazı maddeleri ile uyuşmadığı, Taslaktaki bir takım hükümleri amaçlamadığı ve kapsamadığı değerlendirildiğinden Tasarının 1. maddesinin yeniden gözden geçirilmesi yararlı olacaktır.

Bilişim ağı hizmetlerine yönelik bazı kavramların tasarıda tanımlanması doğru ve yerindedir, ancak, Tasarının 2. maddesindeki "Tanımlar" başlığı altındaki düzenlemelerin yanlış anlaşılmalara sebep vermemesi açısından özellikle "içerik sağlayıcı", "yer sağlayıcı", "erişim sağlayıcı", "hizmet sağlayıcı" ve "toplu kullanım sağlayıcı" ifadelerinin netleştirilmesinin yararlı olacağı değerlendirilmektedir.

Tasarının 2. maddesindeki "yaramaz ileti" ifadesinin uygun olmadığı, bu ifade yerine "istek dışı ileti" ifadesinin kullanılmasının ve "istek dışı ileti" tanımının net şekilde (Telekomünikasyon Kurumu'nun çıkarmış olduğu yönetmelikteki tanım gibi)

[154] Sabah Gazetesi; (27.03.2007); http://www.sabah.com.tr/tek100-20070327.html (03.05.2008)

yapılmasının yerinde olacağı değerlendirilmiştir. Daha sonra Tasarıda yapılan değişiklikle bu terim “istenmeyen ileti” olarak değiştirilmiştir[155].

Tasarının hazırlanmasında örnek alınan mevzuat arasında yer alan Alman Teleservisler Yasasının 2. maddesinde olduğu gibi uygulama sınırlarının net şekilde belirlenmesi gereklidir.

Tasarının içinde yer verilen toplu kullanım sağlayıcılarına ilişkin hükümlerin Taslaktan çıkarılıp İçişleri Bakanlığı koordinatörlüğünde hazırlandığı bilinen İnternet Kafelerle ilgili Taslağa dâhil edilmesinin; bu Taslakta ise İnternet Servis Sağlayıcılarına ilişkin hükümlere yer verilemesinin daha uygun olacağı düşünülmektedir.

Mağduriyetlere sebebiyet vermemek açısından, Tasarının 7. maddesinin 2. fıkrası kapsamında içerik sağlayıcısının, ancak ihtara rağmen başkalarına ait suç unsuru taşıyan içerikleri yayından kaldırmaması halinde sorumlu tutulmasının kanunun amacına daha uygun olacağı değerlendirilmektedir.

İnternet’te anonim kalma hakkı İnternet’in önemli özelliklerinden birisidir. Bu nedenle Tasarının 6. maddesindeki düzenlemenin İnternet’teki tüm kişilere uygulanmasının doğru ve yerinde olmadığı, sadece ticari mal e hizmet sunanlara böyle bir yükümlülük getirilmesinin yerinde olacağı, bu durumda söz konusu düzenlemenin Ticaret Kanunu, Borçlar Kanunu ve Tüketicinin Korunması Hakkında Kanun gibi ilgili kanunlarda yer almasının yerinde olacağı değerlendirilmiştir.

1 Ocak 2007 tarihinden itibaren gerçek kişiler açısından "Vergi Numaraları" yerine "TC Vatandaşlık Numarası" kullanılacağından, Taslakta bu konuda paralel düzenleme yapılması uygun olacaktır.

Tasarının 12. maddesinde yer verilen toplu kullanım sağlayıcılarına ilişkin hükümlerin Taslaktan çıkarılıp İçişleri Bakanlığı koordinatörlüğünde hazırlandığı bilinen Taslağa dahil edilmesinin ve toplu kullanım sağlayıcılarının mekanlarına girerek işlem yapanların kimliklerinin tespit edilmesi ve kayıtlarının tutulması yerine kameralı takip sisteminin getirilmesinin daha uygun olacağı düşünülmektedir. Ayrıca buralarda küçüklerin korunması için, küçüklerin kullanacağı bilgisayarlarda filtre sisteminin kullanılmasının zorunlu hale getirilmesi toplum sağlığı açısından yerinde olacaktır.

Tasarının 13. maddesinde, içerik sağlayıcıya ait bir içerik nedeniyle, uyuşmazlığın tarafı olmayan erişim sağlayıcı ve yer sağlayıcısı gibi üçüncü kişilere yükümlülük yüklenmesi ve kişilere içerik sağlayıcısına yönelik herhangi bir yargı kararı olmaksızın yaptırım uygulama yetkisi verilmesi doğru bulunmadığından bu düzenlemenin hakim kararı ve gecikmesinde sakınca bulunan hallerde, hakim kararı

[155] http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (15.04.2007)

daha sonra alınmak üzere Cumhuriyet savcısının kararı ile yapılmasının uygun olacağı düşünülmektedir. Diğer yandan Tasarının 15. maddesinde "içeriği düzeltme" yükümlülüğü sadece içerik sağlayıcıya yüklenmeli, yer sağlayıcı ve erişim sağlayıcıya bu konuda bir yükümlülük yüklenmemelidir.

TCK'da "Bilişim Alanında Suçlar" başlığı altında düzenlenen suçlar, sistematiği içerisinde "Topluma Karşı Suçlar" arasında yer almaktadır. Bu husus hukuka uygunluk nedenlerinin uygulanması (özellikle ilgili kişinin rızasının geçerli olup olmayacağı) bakımından sorunlara yol açabilecektir. Mukayeseli hukukta incelendiğinde maddelerde düzenlenen suçların yeri ve hukuki konularına ilişkin farklı yaklaşımlar mevcuttur. Özellikle 243 ve 244. maddelerde ve bunun paralelindeki taslaktaki 17, 19, 20, 21 ve 23. maddelerde iki farklı değere yönelik düzenlendiği görülmektedir. Örnek vermek gerekirse, yetkisiz erişimde verinin ele geçirilmesi bakımından Kıta Avrupası içerisinde İtalya ve Almanya bunları daha çok "özel hayatın gizliliği" kapsamında ele almaktadırlar. Buna karşın Fransa mal varlığına karşı suçlar arasında yer vermektedir. Her iki yaklaşımda da, korunan hukuki değerin hamili toplumdan (ya da kamudan) çok kişinin kendisidir. Bu tartışmalara yer verilmeden topluca topluma karşı suçlar arasında suçlar arasında düzenlenmesi korunan hukuki değer ve değerin hamili gibi konularda sorunlara yol açmaktadır. Bu suçların herhangi bir değeri korumak amacıyla şekillendirilmesi mümkün olmakla birlikte, TCK'nın 243 ve devamı maddelerindeki suçların kişiye ait değerleri koruduğu, hem suçların kaleme alınış şeklinden, hem de kanunun ilgili hükümlerinin gerekçesinden anlaşılmaktadır. Bu hususun dikkate alınarak, TCK'daki konuya ilişkin hükümlerin yeri bakımından tekrar gözden geçirilmesi gerekir. Raporumuzun ilk maddesindeki önerimiz dikkate alınarak düzenlemelerin TCK'da yapılması durumunda Ceza Kanunu'nda yapılacak düzenlemede korunan hukuki değer ve suçun unsurlarındaki sorunlarda dikkate alınarak bir düzenlemeye gidilmesi yerinde olacaktır.

Tasarının 18. maddesinde düzenlenen özel evrakta sahtecilik ve resmi evrakta sahtecilik TCK'nın 204 ve 207. maddelerinin nitelikli hali olarak TCK'nın ilgili maddelerinde düzenlenmelidir.

Tasarının 23. maddesindeki düzenleme TCK'nın 226. maddesindeki müstehcenlik suçu ile paralellik arzetmektedir. TCK'nın 226. maddesinin 3. fıkrasında çocuk pornografisi genel olarak düzenlenmiştir. TCK düzenlenmesindeki eksiklik, Siber Suçlar Sözleşmesi ve Çocukların Korunmasına ilişkin uluslararası sözleşmelerdeki tanımlarla tam olarak örtüşmemektedir. Özellikle "çocuk gibi görünen yetişkinler" ile "animasyonlar" TCK'nın mevcut düzenlemesine göre suç sayılmamaktadır. Bu nedenle TCK'nın 226. maddesinde yapılacak ekle çocuk pornografisi tanımlanarak sorun çözümlenebilir.

Tasarının İlk Halinin 35. maddesin "Adli Bilişim Uzmanı" 39. maddesinde ise "görevli mahkeme ve yargılama usulü" düzenlenmişti. Yapılan değerlendirmeler sonucunda; bilirkişilik kurumunun ve ilkelerinin belirlenesi gerektiğinin önem arz ettiği, söz konusu hususların mevcut hali ile Yönetmeliğe bırakılmasının sakıncalı olduğu ifade edilerek, Kanun'un mutlaka çerçeveyi çizip uygulama konusundaki düzenlemeleri Yönetmeliğe bırakmasının yerinde olacağı değerlendirilmiştir. Ayrıca "adli bilişim uzmanı" kavramı yerine Adli Tıp Kurumu çatısı altında adli bilişim ile ilgilenen bir ihtisas dairesi oluşturulmasının yerinde olduğu görüşü kabul edilmiştir. Bunun sağlanabilmesi açısından ise Adli Tıp Kurumu Kanununun değiştirilmesinin gerektiği belirtilmiştir. Adli Tıp Kurumu mevcut duruma göre tıbbi konuların da dışına çıkarak bilirkişilik görevini yapar duruma gelmiştir. (Fizik, biyoloji, grafoloji ve balistik gibi) Adli Tıp Kurumu ismi yerine "Adli Bilirkişilik Kurumu" şeklinde düzenleme yapılabilir. Diğer yandan ihtisas mahkemesi kurulması konusu tartışılmış ve bu kanunda yazılı suçlar dışında bir çok suçunda bilişim ağı aracılığıyla işlenebileceği göz önüne alınarak ihtisas mahkemelerinin kurulmasının yararlı olmadığı ifade edilmiştir. Sorunun çözümü açısından bahse konu Kanun Tasarınının yasalaşmasından önce bu konudaki usul hükümlerinin uygulayıcıya ayrıntılı bir şekilde aktarılması, özellikle adli, idari ve askeri yargı organları ile emniyet ve jandarma gibi kolluk kuvveti ve bu konuda çalışan teknik kurum ve kuruluşlar arasında çok başlılığın giderilerek, gerekirse tercihan Adalet Bakanlığı ile ilgilendirilmiş kamu tüzel kişiliğine haiz bir kurum kurularak, bu konuda prensipleri koyarak, tek merkezden uygulayıcıların eğitilmesi ve uygulama açısından bilgi bankasının oluşturulmasının, kanunun tatbikatında daha yararlı olacağı değerlendirilmiştir. Gerekirse bu konuda usulü düzenleyen yasa hükümlerinin yürürlüğe konulması ve teknik altyapının kurulması uygun olacaktır. Adli, idari ve askeri yargıda görevli olan hakim, Cumhuriyet savcısı ve diğer adli personelin öncelikle eğitimlerine uygulamalı olarak başlanmasının kanunun tatbikatı açısından amacına daha yararlı olacağı düşünülmektedir. Ancak daha sonra Tasarıda yapılan değişikle adli bilişim uzmanlığını düzenleyen madde Tasarıdan çıkartılmıştır. Ancak kanatimizce bilişim suçların her geçen gün arttığı, deliller arasında bilişim teknolojilerinin oranının arttığı bir ortamda adli bilişim uzmanı ihtiyacı da kendini giderek daha fazla göstermektedir. Bu nedenle Tasarı ile bu konu mutlaka düzenlenmelidir kanaatindeyiz.

Gündemde bulunan Adalet Bakanlığının hazırlamış olduğu Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısında yeni olarak phishing yöntemiyle işlenen dolandırıcılık suçlarına cezai müeyyide getirilmektedir. Tasarının 21. Maddesi; "Bilişim sistemi aracılığı ile kendisi veya başkası için yarar temin etmek veya başkasına zarar vermek amacıyla kişileri yanıltarak bilgi toplayan kişiye, fiili başka bir suç oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası

verilir" hükmünü getirmektedir. Tasarının 22. Maddesinin 1. Fıkrası da; "Halkı yanıltacak şekilde, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin bilişim ağındaki hizmetlerini veya kimliklerini taklit eden kişiye" cezai yaptırım öngörmektedir. Bu Kanundaki düzenleme ile bilişim ağları ile işlenen phishing suçlarına ayrı bir müeyyide getirilmekte, eğer phishing suçun işlenmesi ile menfaat elde edilmiş ise TCK:158/1-f bendi hükümlerinin uygulanması söz konusu olacaktır.

Tasarı kamuoyunda yeterince tartışmaya açılmaması, STK'ların yeterince görüşüne başvurulmaması, Ulaştırma bakanlığı ile Adalet Bakanlığının aynı konularda değişik düzenlemeler içermesi ve İnternet'e sansür getirdiği gibi değişik açılardan eleştirilere maruz kalmıştır[156]

3.16.2 Ulaştırma Bakanlığının Hazırlamış olduğu "İnternet Ortamında İşlenen Suçlarla Mücadele Kanun Tasarısı"

Kamuoyunda yakın geçmişte yoğun şekilde çocuk pornografisi üzerinde durulmuş ve çeşitli yetkililer tarafından çocuk pornografisi üzerinde yasal düzenlemeler yapılacağı konusunda açıklamalar yapılmıştır. Bu açıklamalardan hareketle oluşan kamuoyunun da etkisi ile Ulaştırma Bakanlığı İnternet ortamındaki suçlarla, suç oluşmadan önceki aşama bağlamında, önleme amacıyla bir düzenleme yapılmasını kaçınılmaz görerek harekete geçmiş ve "**İnternet Ortamında İşlenen Suçlarla Mücadele Kanun Tasarısı"**nı hazırlamıştır[157].

Bu haberler kamuoyunda bir hayli yer bulmuş ve kamuoyunda çocuk pornografisinin cezalandırılmadığı, bu konuda yasal düzenlemenin bulunmadığı şeklinde fikir ve yayınlara da rastlanmıştır. Öncelikle şunu ifade etmek gerekir ki çocuk pornografisi ile ilgili olarak Türk Ceza Kanunun 226. maddesinde düzenleme mevcut olup bu maddeye göre çocuk pornografisi ile ilgili suç işleyen kişilere on yıla kadar hapis cezası verilebilmektedir[158]. Diğer yandan yine Türk Ceza Kanunu 103. maddesinde çocukların cinsel istismarı ile ilgili fiilleri işleyenlere 20 yıla varan hapis cezaları öngörülmüştür. Doç. Dr. Adem Sözüer'in de belirttiği gibi mevcut durum bu iken bu konuda yasal düzenleme bulunmamaktadır şeklinde iddialarda bulunmak hatalı

---

[156] http://www.btnet.com.tr/haber.phtml?yazi_id=590000230; "Bilişim Suçları Yasa Tasarısı Kafa Karıştırıyor", Levent Uyanıker**;** Birgün Gazetesi, "İnternet'in Yıldönümü Sansür Tartışmaların Gölgesinde Geçiyor"(12.04.2007)**;** Cumhuriyet Gazetesi, (20.02.2007), "Küresel Gözaltı ve Sansür Girişimi, Mehmet Sucu"**;** IT Business Dergisi (12.02.2007), "AB Değil Şangay Kriterleri", Eylem Cülcüoğlu; Birgün Gazetesi, (22.02.2007), "Bilişim Suçları Kargaşası", Haluk Geray; "Hükümetten İnternet'e büyük gözaltı" http://www.hurriyet.com.tr/gundem/5640581.asp (19.12.2007); İnternet'e "Büyük Gözaltı" Geliyor" Nokta Dergisi, 18-24 Ocak 2007, Yıl:1, Sayı: 12;

[157] Vatan Gazatesi, "İnternet'te Çocuk Pornosu ve Kumara Önlem Geliyor!"(10.02.2007)

[158] Milliyet Gazetesi,"Çocuk Pornosuna 4 Yıl Hapis" (26.01.2007); "Çocuk pornocusuna dört yıl hapis cezası" http://www.sabah.com.tr/2007/01/26/gun107.html (15.04.2007); "Kanadalı öğretmene çocuk pornosundan 1,5 yıl hapis" http://www.hurriyet.com.tr/gundem/5752846.asp?sd=2 (15.04.2007)

bir tutum olarak değerlendirilmelidir. [159] Kaldı ki sırf cezaların arttırılması suçun işlenmesinde tek başına engel olamayacaktır. Nasıl ki idam cezası olan ülkelerde suçların artış hızları ABD'de olduğu gibi önemli oranda düşmüyorsa, İnternet'le ilgili çocuk pornografisi gibi suçların engellenmesi için sadece yüksek cezalar yeterli olmayacaktır. Bu tür suçların engellenebilmesi için ülkemizde bilişim suçları ile ilgili delillerin ne şekilde tespit edileceği konusunda bir an önce temel ilkeler belirlenmeli ve bu konuda daha kapsamlı yasal düzenlemeler yapılmalı, uygulayıcılar bu konuda eğitilmeli ve yeterli teknik donanımla teçhiz edilmelidirler. Bu fikrimizi desteklemek bakımından şu örnek verilebilir; İstanbul Emniyet Müdürlüğünün kurmuş olduğu bilişim suçları bürosu faaliyete geçtikten sonra basına da yansıyan önemli oranda suçun tespitine yönelik çalışmalar yapılmış ve failler hakkında yasal işlemler başlatılmıştır.

Tasarının 1. maddesinde amaç ve kapsam düzenlenmiş ve yasa tasarısının amacının İnternet ortamında işlenen belirli suçların içerik yer ve erişim sağlayıcıları üzerinden önlenmesine ilişkin esas ve usulleri düzenlemek olduğu belirtilmiştir. Adalet Bakanlığının hazırlamış olduğu bilişim suçları ile ilgili yasa tasarısı da İnternet servis sağlayıcıları ile ilgili hukuki ve cezai düzenlemeler içermektedir. Böyle bir yasa tasarı var iken aynı konuyu düzenleyen Ulaştırma Bakanlığı tarafından hazırlanan yasa tasarısı uygulamada karışıklıklara neden olabilecektir. Tasarının 2. maddesinin h bendinde izleme teriminin tanımı yapılmış ve İnternet ortamına sunulan haberleşme dışındaki verileri etki etmeksizin bilgi ve verilerin takip edilmesi şeklinde tanımlanmıştır. Taslağın 4. maddesinin 5. fıkrasının e bendinde ise servis sağlayıcılarında uygulanacak olan filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılması gerektiği hususunda elektronik haberleşme ve İnternet sektörünü yönlendirmek şeklinde bilişim güvenliği başkanlığına görev verilmiştir.

Yine Taslağın 4. maddesinin 5. fıkrasının b bendinde yine başkanlığa İnternet ortamına sunulan haberleşme dışındaki yayınları izleyerek bu kanun kapsamına giren suçların işlendiğinin tespiti halinde bu yayınların erişilmesine yönelik olarak gerekli tedbirleri almakta sayılmıştır. B ve e bendi birlikte değerlendirildiğinde İnternet ortamındaki sohbet, mesaj, form ve benzer ortamların da başkanlık tarafından izleneceği sonucu çıkarılabilecektir. Anayasamızın 22. maddesinin 1. fıkrasına göre herkes haberleşme hürriyetine sahiptir ve haberleşmenin gizliliği esastır. Yine 22. maddesinin 2. fıkrasına göre milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya bir kaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça, yine bu sebeplerle bağlı olarak gecikmesinde sakına bulunan

[159] Sözüer, Doç. Dr. Adem, "TCK, CMK ve Kabahatler Kanunundaki son değişiklikler ne getiriyor." HPD Aralık 2006, Sayı:9

hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı 24 saat içinde görevli hâkimin onayına sunulur. Hâkim kararını 48 saat içinde açıklar, aksi halde karar kendiliğinden kalkar. Anayasanın bu hükümleri nazara alındığında İnternet ortamındaki sohbet mesaj veya diğer kişisel haberleşmelerin ancak istisnai durumlarda ve hâkim kararı ile sınırlandırılabileceği, izlenebileceği veya engellenebileceği açıktır. Taslakta kurulacak olan başkanlığın ne şekilde izleme yapılacağı, hangi durumlarda izlemenin yapılacağı açıkça belirtilmemiştir. Taslağın içerisine anayasanın 22. maddesinin 2. fıkrasındaki istisnalar sayılarak ve hâkim kararı ile izlemenin yapılabileceği açıkça yazılmalıdır. Aksi halde taslak Anayasaya aykırı bir düzenleme olacaktır.

H bendindeki izleme tanımındaki "haberleşme dışındaki" ibaresi kişisel haberleşme olarak değiştirilmesi yerinde olacaktır.

Taslağın 3. maddesinin 2. fıkrasında 1. fıkrada yazılı suçların işlenmesini önlemeye yönelik yurt içindeki içerik ve yer sağlayıcısının ne şekilde engelleneceği hususu düzenlenmiş ve bu yöndeki kararların hâkim kararı ile verilebileceğini özellikle belirtilmiş ve gecikmesinde sakınca bulanan hallerde ise Cumhuriyet Savcısına yetki verilmiştir. Yine 3. maddenin 3. fıkrasında 1. fıkrada düzenlenen çocukların cinsel istismarı, devlet sırlarına karşı suçlar, casusluk gibi suçlarda yayınlarla ilgili erişimin engellenmesi kararının başkanlık tarafından verileceği belirtilmiştir. Kanaatimizce yurt içi veya yurt dışında içerik ve yer sağlayıcıları bakımından erişimin engellenmesi açısından iki ayrı düzenleme yapılmasında pratik bir fayda bulunmamaktadır. Yurt dışında bulunan içerik ve yer sağlayıcısının da bir Türk Vatandaşı olarak anayasanın 22. maddesindeki haberleşme özgürlüğü ve dokunulmazlığı hakkı göz önünde tutulmalıdır. Ayrıca yurt dışında bulanan içerik ve yer sağlayıcısının da 2. fıkrada olduğu gibi hâkim kararı ile erişimin engellenmesi karar verilebilir ve Türkiye'deki erişim sağlayıcılarına bu karar tebliğ edilerek, erişimin engellenmesi mümkündür. Dolayısıyla 3. fıkra doğrultusunda yurt dışında bulanan içerik ve yer sağlayıcıları için ayrı bir düzenleme yapılması anayasanın 10. maddesinde düzenlenen eşitlik ilkesine de aykırıdır kanaatindeyiz.

Taslak kanunda erişimin engellenmesi konusunda başkanlığın aktif olarak görev yapacağı düzenlenmiş iken, erişimin engellenmesi kararı verilen yayınlar hakkında bu karar kaldırıldığı takdirde bütün yer, ortam ve erişim sağlayıcılara ne şekilde gereğinin yapılacağı düzenlenmemiştir. Buda haksız olarak kapatılan yayınların yargı kararı ile yeniden yayınlarına izin verilse bile, servis sağlayıcılarına verilen erişimin engellenmesi kararının kaldırılmasına ilişkin karar gönderilmediğinden, hukuken yasak kalkmış olmasına rağmen servis sağlayıcılarına bu karar ulaşmadığından dolayı fiili olarak

yasak devam edecektir. Buda mağduriyetlere ve devletimizin tazminatlar ödemesine neden olabilecektir.

Taslak kanunun 4. maddesinde bilişim güvenliği dairesi başkanlığının ne şekilde teşekkül edeceği düzenlenmiş olup başkanlıkta çalışacak olan personelin memur olarak istihdam edilecekleri anlaşılmaktadır. İnternet gibi özgürlükçü ve bütün kamuyu ilgilendiren hassas bir konuda demokratik devlet yapısı içerisinde servis sağlayıcıların da bir şekilde alınacak kararlarda söz sahibi olabilmeleri, kendilerini ilgilendiren düzenlemelerde görüşlerini bildirebilmeleri ve yapılacak işlemlerde etkin olabilmeleri bakımından onlarında yapılanma içerisinde yer alması uygun ve gerekli bir düzenleme olacaktır.

Taslak kanunun 4. maddesinin 5. fıkrasının ç bendinde kurum tarafından işletmecilerin yetkilendirilmeleri ibaresi geçmekte olup bu ibareden kurum tarafından yetki belgesi verilmeyen işletmecilerin servis sağlayıcı hizmeti yapamayacakları sonucu çıkmaktadır. Oysaki 2000/31 sayılı e-ticaret ile ilgili AB direktifinin 4. maddesinde üye devletler bir bilgi toplumu hizmeti sunucusunun bu faaliyete başlamasının ve icrasının devam ettirilmesinin önceden izin şartına veya eş etki doğuran başka bir şarta tabi tutulamaz hükmünü getirmiştir. AB müktesebatına uyum açısından da dikkate alınması gereken bu hüküm karşısında 4. maddenin 5. fıkrasının ç bendindeki işletmecilerin yetkilendirilmesi ibaresinin gözden geçirilmesi gerekmektedir.

Taslak kanunun 3. maddesinin 8. fıkrasında, 4. fıkra uyarınca erişimin engellenmesi kararını yerine getirmeyen kişilere bir yıldan üç yıla hapis cezası öngörmektedir. Kamu görevlisi sorumlu servis sağlayıcı kim olduğu yasada açıkça belirtilmediğinden bu cezanın muhatabının kimler olacağı belirlenmemiştir. Ayrıca erişimin engellenmesi kararı teknik bir imkânsızlık sebebi veya benzer bir sebeple yerine getirilemediyse durum ne olacaktır. Bu konuda da taslakta açık hüküm konulması yerinde olacaktır.

Diğer taraftan parelel yürüyen ve halen TBMM'de olan ve Adalet Komisyonunda kabul edilen Ulaştırma Bakanlığı tarafından hazırlanan "İnternet Ortamında İşlenen Suçlarla Mücadele Kanun Tasarısı" adı Komisyon çalışmaları sırasında , **"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Kanunu Tasarısı"** olarak değiştirilmesine karar verildiği ve sadece erişimin engellenmesi değil bunun yanı sıra Tasarının kapsamının genişletilirek Adalet Bakanlığının hazırlamış olduğu İnternet Servis Sağlayıcılarla ilgili bazı hükümlerin Ulaştırma Bakanlığı Tasarısına alındığı anlaşılmaktadır. Bu bağlamda Ulaştırma Bakanlığının hazırlamış olduğu Yasa Tasarısının içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile İnternet

ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri de kapsayacak şekilde yasalaştırılacağı haber verilmektedir[160].

Aynı haberde Tasarıya yeni eklenen maddelere göre içerik, yer ve erişim sağlayıcıları, tanıtıcı bilgilerini kendilerine ait İnternet ortamında güncel olarak bulundurmakla yükümlü olacaklar ve kendilerine ait bilgileri İnternet ortamında bulundurmayanlara, 2 bin YTL ile 10 bin YTL arasında para cezası verilecek.

Adalet Bakanlığı Tasarısında olduğu gibi bu Tasarıda da İnternet ortamında kullanıcılara sunulan her türlü bilgi veya veriyi üreten içerik sağlayıcıları, İnternet ortamında yayınladıkları her türlü yayından sorumlu olacaklar. İçerik sağlayıcı, bir başkasına ait İnternet sitesinden sağladığı içerikten, kural olarak sorumlu tutulmayacak. Ancak bağlantı sağladığı, içeriği benimsediği ve kullanıcının ulaşmasını amaçladığının anlaşılması halinde, aynı içerikten dolayı sorumlu tutulacak. Bağlantı sağlanan içeriğin suç oluşturması halinde, bu içeriğe bağlantı sağlayan içerik sağlayıcısı, işlenen suça katılmaktan dolayı sorumlu tutulacak.

Yine yapılan değişikliğe göre İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten yer sağlayıcıları, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü tutulmayacaklar. Yer sağlayıcı, hukuka aykırı içerikte suç unsuru bulunduğundan haberdar edilmesi ve engelleme yeteneği bulunması durumunda, hukuka aykırı içeriği yayından kaldırmakla yükümlü olacak.

Yeni düzenlemeyle, erişimi engellenecek suçlara ilişkin katalogda da değişiklik yapılıyor. Katologdan artık çocukların cinsel istismarı ve sağlık için tehlikeli madde temini suçları, erişimi engellenecek suçlar arasından çıkarılacak. Suçu ve suçluyu övmenin eklendiği katalog, müstehcenlik, fuhuş, intihara yönlendirme, kumar oynanması için yer ve imkân sağlama suçlarından oluşturulacak.

Tasarıya eklenen yeni bir maddeye göre ise İnternet erişim sağlayıcılarına yükümlülük getiriliyor. Buna göre; erişim sağlayıcısı, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten haberdar edilmesi halinde erişimi engelleyecek. Ancak bu noktada hangi yayının hukuka aykırı olduğunun tespiti sorun teşkil edecektir. Bu da hak kayıplarına veya aslen hukukçu olmayan ISSlerin mağduriyetine sebep olacaktır. Özellikle günümüzde erişimin engellemesi konusunda açıkça bir hüküm bulunmamasına rağmen mahkemeler tarafından değişik iş kararları olarak erişimin engellenmesi kararları verilmekte ve değişik iş kararlarının alınması birçok kez

[160] Sabah Gazetesi, (27.03.2007);
http://www.sabah.com.tr/tek100-20070327.html (03.05.2008)

duruşma yapılmaksızın evrak üzerinden verilmekte olması nedeniyle ve seri çıkmaktadır. Hatta bu nokta da bile birçok eleştiri mevcut iken erişimin engellenmesi kararaının idari makamlara verilmesi ülke olarak değil sadece iç kamuoyunda, dünya kamuoyunda da daha da çok eleştiri almamıza neden olacak gibi gözükmektedir. Bu durum nazara alındığında tüm erişimin engellenmesi kararlarının acele hallerde Cumhuriyet savcısı, diğer zamanlarda ise hâkimler tarafından alınması daha baştan temel hak ve özgürlükler bağlamında birçok mağduriyeti engelleyecektir.

Yine Tasarıya eklenen yeni maddlerle erişim sağlayıcısı, sağladığı hizmetlere ilişkin her türlü bilgi, veri tabanı ve ulaşım kayıtlarını 6 aydan 2 yıla kadar saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü olacak. İnternet kafeler veya tasarıda geçen hali ile ticari amaçlı toplu kullanım sağlayıcıları, mahalli mülki amirden izin belgesi alacak. İzne ilişkin bilgi ve belgeler yetkili makama 30 gün içinde bildirilecek.

Ticari amaçla olup olmadığına bakılmaksızın bütün toplu kullanım sağlayıcıları, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlü olacak. Bu koşulları yerine getirmeyenlere 10 bin YTL'den 50 bin YTL'ye kadar ceza verilecek.

Asıl Tasarının en çok eleştirilen kısmı ise içerik veya yer sağlayıcısının yurtdışında bulunması halinde, erişimin engellenmesi kararı, Telekomünikasyon İletişim Başkanlığı tarafından verilecek. Bu karar, erişim sağlayıcısına bildirilerek, gereğinin yerine getirilmesi istenecek. Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren 24 saat içinde yerine getirilecek. İdari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde erişim sağlayıcılarına 10 bin YTL'den 100 bin YTL'ye kadar idari para cezası verilecek.

Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, 6 aydan 2 yıla kadar hapisle cezalandırılacak.

İnternet'te kişilik haklarına saldırıda bulunanların, bu nitelikteki içeriğin yayından çıkarılması ve buna karşı cevap hakkının kullanılması, Basın Kanununun ilgili hükümleri doğrultusunda sağlanacak[161].

Raporun yayınlandığı günlerde adı geçen tasarı "Elektronik Ortamda İşlenen Suçların Önlenmesi Kanunu Tasarısı" kabul edilerek yasalaşmıştır[162].

---

[161] http://www.sabah.com.tr/tek100-20070327.html (03.05.2008); http://www.sabah.com.tr/haber,0C6FA86207934AC2B0B8935B22919611.html (13.04.2007) Bugün Gazetesi, (14.04.2007); Cumhuriyet Dergi, (15.04.2007)

[162] **"**İnternet yayıncılarının …. Yasa, Meclisten Geçti " http://www.nethaber.com/NewsDetails.aspx?id=20579 (07.05.2007)

3.16.3 Almanya'da Bilişim Suçları İle Mücadele için Hazırlanan Yasa Taslağı

Bilişimin ilerlemesi sadece ülkemizde değil diğer bir çok ülkenin de bu alanda mevzuatlarında zaman zaman değişiklik yapılmasını gündeme getirmiş ve bu konuda çalışmalar yapılmasını gerekli kılmıştır.

Almanya'da yasa değişikliği çalışmaları, özellikle ülkemizdeki bilişim suçları yasa değişiliklikleri ile parelellik arzetmesi nedeniyle konuyu biraz daha ilginç kılmıştır. Bu durum aynı zamanda grubumuzda acaba konu orada nasıl ele alınıyor ve inceleniyor şeklinde merak ve ilgiye neden olmuştur.

Almanya'da ilk kez 15 Mayıs 1986 tarihinde kabul edilen Ekonomik Suçlarla Mücadele Yasası ile bilişim suçlarına ilişkin hükümler ACK'na eklenmiştir. Bu ekleme ACK'da ayrı bir bölüm halinde ekleme olmamış ve işlenen suçta korunan değer ne ise o değerin korunduğu kısımlara ekleme yapılmıştır. Böylece özel ceza hukukunda düzenelenen suçlar bakımından ACK'nun genel hükümlerine ilişkin uygulamasında bir parelellik, bir adalet tesis edilmeye çalışılmıştır ki kanaatimizce bu yöntem daha adil uygulamalara da yol açacak, aksi durumlarda benzer suçlar değişik kanunlarda düzenlendiği için uygulamada haksız sonuçlar ortaya çıkabilecektir. Ayrıca ortaya konulmaya çalışılan tek bir ceza hukuku sistemi daha iyi işleyecektir.

Almanya'da da bizde olduğu gibi uzun zamandan beri ACK'da bilişim suçları bakımından bir düzenleme ve ACK'na eklemeler yapılması gerektiği konusunda tartışmalar sürmekte ve bu konudaki ACKdaki eksiklikler konusunda tezler, araştırma yazıları ve makaleler yazılmakta idi[163].

Bu tartışmalar ve bir taraftan 23 Kasım 2001 tarihinde Almanya'nın SSS imzalaması ve 1 Temmuz 2004 yılında bu andlaşmanın yürülüğe girmesi, diğer taraftan ise AB Konseyinin 24 Şubat 2005 tarihli "Bilişim Sistemlerine Karşı Saldırılar"[164] başlıklı çerçeve kararının tüm üye ülkeleri bilişim suçlarının ağı ortaya çıkış şekillerine karşı cezai yaptırım koymaları yolunda yükümlü hale getirmesi ve bilişim suçları ile mücadelede adalet ve güvenlik güçlerinin ortak çalışması için daha fazla işbirliği istemesi sonucu bir yasa değişikliği yapılması yolunda çalışma başlatılması ile sonuçlanmış ve "Bilgisayar Suçaları ile Mücadele için Ceza Kanununda Değişiklik Yapan Kanun Tasarısı" hazırlanmıştır[165]. AB Konseyinin 24 Şubat 2005 tarihli Bilişim Sistemlerine Karşı Saldırılar başlıklı Çerçeve Kararının 12. Maddesine göre AB üyesi

---

[163] Fassbender, Marcel; "Angriffe auf Datenangebotene im İnternet und deren starftrechliche Relevanz", (DS),Hamburg, 2003, s.132, 133;
"Beitrag: Denial-of-Service-Attacken straffrei?" http://www.rechtsanwalt.de/dos.html (21.04.2007)
Tanrıkulu, Cengiz; "Rechtsvergleich; İnternet'kriminalität in türkischen und deutschen Starfgesetzbüchern" Seminararbeit, Rostock, 2004

[164] AB Konsey'inin 2005/222/ JI Çerçeve Kararı için bakınız;
http://eur-lex.europa.eu/LexUriServ/site/de/oj/2005/l_069/l_06920050316de00670071.pdf , (21.04.2007)

[165] Tasarının tamamı için bakınız; http://www.bmj.bund.de/media/archive/1317.pdf , (21.04.2007)

ülkeler 16 Mayıs 2007 tarihine kadar bu karardaki yükümlülüklerini yerine getirmek ile yükümlüdürler.

Almanya bu yükümlülüklerini yerine getirme bağlamında içerik bağlantılı bilişim suçları ile ilgili olarak bu Tasarıda hükümlere yer vermemiş ve örneğin SSS 3. Maddesi ile çocuk pornografisi ile ilgili 9. Maddeleri için ayrı bir tasarı yolunu seçmiş gözükmektedir. Çocuk pornografisi konusunda AB tarafından çıkarılan Çocukların Cinsel Yönden Suistimali ve Çocuk Pornografisi ile Mücadele Çerçeve Kararı gereği Almanya, bizdeki değişiklik çalışmalarının aksine, özellikle çocuk pornografisi konusunda ceza usul hukuku alanında bir yasa tasarısı çalışması yapmaktadır[166].

ACK'nun 202a maddesi, bir bilişim sistemine hukuka aykırı girme ve oradan verileri ele geçirme suçunu düzenlemekte ve fakat sadece yalnız başına sisteme girme suçunu, yani yetkisiz erişimi düzenlememekte idi. Hatta bu yetkisiz erişim ve verilerin ele geçirilmesi suçunun belirli bir şifre ile girişi engellenmiş sistemlere karşı yapılması gerekiyor ve fakat korumasız sistemlere girme suç kapsamında değildi[167].

Tasarı ACK 202a maddesini artık sadece yetkisiz erişimi de ceza kapsama alınacak şekilde değiştirmektedir. Buna göre madde; "Her kim kendisine veya başkalarına, erişimine yetki verilmeyen, kendisince bilinmeyen ve hukuka aykırı girişlere karşı özel olarak güvenli hale getirilmiş (şifrelenmiş) verilere ulaşmak için, giriş güvenliğini aşarsa 3 yıla kadar hapis veya para cezası ile cezalandırılır." halini almıştır. Alman Yasa Koyucu burada düzenleme yaparken elektromanyetik alanlarda yapılanlar da dahil olamak üzere yetkisiz erişim eylemlerinin cezalandırılmasını isteyen SSS'nin 3. Maddesinin gereğinin yerine getirildiğini düşünmektedir[168].

Tasarı ACK 202a maddesinden sonra gelmek üzere ayrıca iki madde daha eklemiştir. Eklenen 202b maddesi ile "Verilerin Ele Geçirilmesi"nin değişik versiyonalrını yaptırım altına almıştır. Buna göre artı kamuya açık olmayan veri iletişimini ve veya elektromanyetik veri iletimi, sırasında yapılan verilere tecavüz böylece cezalandırılmak istenmiştir. Zira 202a maddesi sadece belirli bir güvenlik önlemi olan bilişim sistemlerini korumakta, örneğin şifrelenmemiş bir sitemden ele geçirilen veriler için bir yaptırım öngörmemekte idi. Bu yeni düzenleme ile artık özellikle kablolu veya wireless ortamlarda iletilen verilerin ele geçirilmesi halinde, bu veriler güvenli bir şekilde nakledilmiyor olsa bile ACK'nun 202b maddesi uygulanacaktır.

ACK'na Tasarı ile getirilen önemli bir değişilik ise 202c maddesidir. Bu madde ile 202a ve 202b maddelerinde tanımlanan suçları işlemek üzere yapılan hazırlık hareketleri de artık cezai yaptırım altına alınmaktadır. Bu maddenin birinci fıkrasına

[166] http://www.bmj.bund.de/media/archive/1317.pdf , (21.04.2007)
[167] http://dejure.org/gesetze/StGB/202a.html (21.04.2007)
[168] http://www.bmj.bund.de/media/archive/1317.pdf , (21.04.2007), s.7

göre; bilişim sistemlerinin girişinde kullanılan parola vb kodların kırılması sağlayan veya bu parola ve kodların üretilmesini sağlayan programları üreten, kendisine veya başkasına tedarik eden, satan, başkasının kullanımına bırakan, yayan veya başka bir şekilde sağlayan bir yıla kadar hapis veya para cezası ile cezalandırılır.

Tasarı ile ayrıca 202a, 202b, 202c maddelerini şikâyete bağlı hale getiren 205. Maddeye de ekleme yapmakta ve yukarıda bahsedilen suçların daha önce ve bizde de olduğu gibi şikâyete bağlı olduğunu belirterek, sadece kolluk görevlileri kamu yararı nedeniyle, ceza usul kovuşturma ve soruşturmaları sırasında görevini yerine getirirken sınırını aşarsa bu suçun şikâyete bağlı olmayacağını hükme bağlamaktadır.

Tasarı aynı şekilde verilerin değiştirilmesini, kullanılmaz hale getrilmesini, silinmesini, gizlenmesini veya erişilmez kılınmasını düzenleyen 303a maddesinde[169] de hazırlık hareketlerini yaptırım altına almış, buradada bu möaddedeki suçların işlenmesi için programlar üreten, yayan satan vb. hareketlerde bulunan failler için ceza öngörmüştür.

Tasarı ile önemli bir ek de 303b maddesine yapılmıştır. 303b maddesi halen bilgisayar sabotajı suçunu düzenlemekte ve sadece işletmelerin, ticari kuruluşların ve kamu kurumlarının bilişim sistemlerine karşı işlenmesi halinde fiili suç saymakta, özel kişilerin bilişim sistemlerini korumamaktadır. Ayrıca suçun oluşması için meydana gelen zararın önemli zarar olması gerekmektedir[170].

Tasarıda yapılan değişiklikle artık sabotaj kimin bilişim sistemine yapılırsa yapılsın koruma altına alınmakta ve 3 yıla kdar hapis veya para cezası öngörülmektedir. Maddeye eklenen ikinci fıkra ile de daha önce olduğu gibi sabotaj fiili, ticari kuruluşların ve kamu kurumlarının bilişim sistemlerine karşı işlenmesi halinde ceza 5 seneye kadar hapis veya para cezası olarak düzenlenmiştir.

Tasarıda ayrıca 303b ile ilgili olarak Maddedeki 2. Fıkra 3. Fıkra haline getirilmiş ve daha sonra da 4. Fıkra ile; sabotaj fiili, ticari kuruluşların ve kamu kurumlarının bilişim sistemlerine karşı işlenmesi halinde özellikle ağır bir durum ortaya çıkarsa bu kez cezanın 6 aydan 10 yıla kadar hapis cezası olacağı ilave edilmiştir. Özellikle ağır bir durumun ne olduğu hemen fıkranın devamında düzenlenmiş ve suç büyük bir servet kaybına neden olur, bilgisayar suçu işlemek üzere oluşturulmuş bir örgütün üyesi olarak veya bilgisayar suçu meslek edinilerek işlenirse veya fail halkın iaşe temin ettiği hayati maddelere, hizmetlere ve Almanya'nın güvenliğine zarar verirse, yerinde bir düzenleme ile verilecek ceza önemli oranda artırılmaktadır.

[169] http://dejure.org/gesetze/StGB/303a.html (21.04.2007)
[170] http://dejure.org/gesetze/StGB/303b.html (21.04.2007)

Tasarın ile eklenen 303b maddesinin 5.fıkrası ile de yine önceki değişikliklerde olduğu gibi bu maddede belirtilen suç için yapılan hazırlık hareketleri de cezai yaptırım altına alınmaktadır.

Alman Yasa Koyucu 303b maddesine ek düzenleme yaparken elektromanyetik alanlarda yapılanlar da dâhil olamak üzere hukuka aykırı saldırılarla ilgili eylemlerinin cezalandırılmasını isteyen SSS'nin 5. Maddesinin gereğinin yerine getirildiğini düşünmektedir[171]. Bunun yanın da özellikle hassa bilişim sistemlerine yapılacak saldırıları özel olarak düzenlemiş verilecek cezaları önemli oranda arttırmış bulunmaktadır.

3.17 *Bilişim Suçları İle Ulusal ve Uluslararası Boyutta Mücadele*

Avrupa Konseyi bilişim suçlarında bir ülkenin tek başına bu suçla mücadele edemeyeceğini öngörerek özellikle uluslararası platformda bir adli yardımlaşmanın şart olduğunu göz önünde bulundurarak bu konuda SSS özel bir düzenleme yapmıştır.

Bilişim alanındaki suçlarla mücadelede özellikle adli yardımlaşma konusunda SSS'nin iç hukuka uyumlulaştırma ihtiyacı kaçınılmaz bir ihtiyaç olarak kendini göstermektedir. Özellikle çocuk pornografisi ve phishing suçları ile etkin mücadele için en azından benzer özellikler taşıyan yasalara ihtiyaç var. İnternet saldırıları çok çabuk ve yaygın gelişmektedir. İnternet üzerinden en çok iletişim ABD-Avrupa-Asya arasında gerçekleşmekte. Bu suçlarda soruşturmanın başarısı genellikle diğer uluslararası makamlarla işbirliğine bağlıdır. Ulusal egemenlik ilkesi, uluslararası araştırma ve soruşturmaları sınırlamakta birçok suçun takipsiz kalmasına neden olmaktadır. Suç her yerden işlenebildiği için failler oradaki yasal durumu öğrenip hiç veya az ceza alacakları ülkeleri seçmektedirler. Arada aracı olarak başka bilgisayarları kullanarak asıl fail kendisini gizleyebilmektedir. İşbirliği için global anlamda uygulanabilecek ortak veya benzer mevzuatın varlığı gereği suçluların iadesinde en çok ihtiyaç duyulan konudur. Ülkeler eğer SSS taraf değil veya onaylamamışlarsa örneğin bu eylem benim ülkemde suç değil o zaman iadeyi reddederim diyebilmektedir. Bu noktada uluslararası adli yardımlaşmanın önemi ortaya çıkmaktadır. Çünkü bu yardımlaşma yeterli değil ise o zaman bu suçla mücadele çoğu kez sonuçsuz kalmaktadır. Burada SSS öngördüğü 7/24 temas noktaları devreye girmektedir. İstediğiniz zaman bu büroları arayıp bu bürolar yardımı ile herhangi başka bir ülkenin adli makamlarından bilişim suçları ile ilgili konularda adli yardım talebinde bulunulabilinir.

Bu konuda SSS'yi onayalayan ülkeler ve bu kapsamda andlaşmayı imzalamasa bile işbirliği yapan ülkeler mevcuttur. Bunlardan Meksika, Brezilya ve Hindistan'ı

[171] http://www.bmj.bund.de/media/archive/1317.pdf , (21.04.2007), s.7

sayabiliriz. Burada anahtar kelime “implementation” yani uygulama kelimesidir. Şu ana kadar 19 ülke bu sözleşmeyi onaylamış ve iç hukukuna katmıştır. Bu alanda kamu-özel sektör işbirliğinin önemine de vurgu yapmak gerekir. 7 gün 24 saat temas noktalarının (contact points) oluşturulması da yine SSS'nin bir bölümü ve ilgi alanı olarak Avrupa Konseyinin önem verdiği bir kurum olmuştur.

19-21 Mart 2007 tarihleri arasında Belgrad/Sırbistan'da yapılan “Sanal Ortamda İşlenen Suçlar Bölgesel Konferansı”nda ülkesindeki uygulamaları anlatan Romanyalı savcı Iona Albani ilgili şubeleri şu şekilde kurduklarını anlatmıştır; Albani SSS kapsamında 7/24 temas noktalarının yararlarından söz ederek, başlıca amaçlarının SSS'nin ülke iç hukuku ile uyumlulaştırma olduğunu, bu kapsamda bilişim suçları ile uluslararası boyutta mücadele zeminini hazırlamak istediklerinin altını çizmiştir. Bu bağlamda Sözleşme'nin kendi iç hukuklarına adapte edebilmek için özel bir yasa çıkararak SSS'nin madde 35'[172]de düzenlenen 7/24 sistemini kurduklarını belirtmiştir. Romanya'da 7/24temas noktası biriminde 6 savcı çalışmakta ve bu savcılar bilişim alanında donanımlı ve yabancı dil bilgisine sahip kişilerden seçilmişlerdir. Bu birimin Romanya'da Bükreş'te özel yerleri bulunmakta ve özal yasaca tanınmış özel yetkiler ile donatılmışlardır. Savcılar talep geldiğinde harekete geçmekte ve istek üzerine ilgili birimlerle irtibata geçerek bilişim ağlarındaki bilgi ve trafik takibini yetkileri çerçevesinde yapmaktadırlar. Birim ilk taleple gereken önlemleri alarak harekete geçmekte ancak daha sonra resmi adli yardım talebinin gelmesini beklemektedir. Ancak bu resmi talep gelirse talepte bulunan ülkeye istenilen ve temin edilen bilgiler gönderilmektedir. SSS 35. Madde gereği kurulan 7/24 sisteminin İtalya'da da başarılı uygulamaları olmakta ve bürokratik olmayan acil cevap vermeye odaklı bi yaplanma gerçekleştirildiği bilinmektedir. O kadar ki yakın bir geçmişte Rusya bağlantılı büyük bir çetenin bu sistem sayesinde kredi kartlarının kötüye kullanımı ile ilgili bir olayın açığa çıkarıldığı söylenmektdir.

---

[172] SSS, Başlık 3 – 24 saat 7 gün boyunca elverişli ağ
Madde 35 – 24/7 Ağı;

- Taraflardan her biri, bilgisayar sistemleri ve verileriyle ilgili cezaî suçlar konusundaki soruşturma ve davaların yürütülmesi ya da cezaî bir suça ilişkin olarak elektronik ortamda delil toplanabilmesi işlemlerine ilişkin olarak en kısa sürede yardım temin edilmesini sağlamak üzere haftanın 7 günü 24 saat boyunca elverişli olan bir irtibat noktası belirleyecektir. Söz konusu yardım, aşağıdakilerin kolaylaştırılması ya da ulusal yasa ve uygulamaların uygun görmesi halinde doğrudan yapılması ile olacaktır:

1. Teknik görüş verilmesi;
2. Madde 29 ve 30 uyarınca verilerin korunması ve
3. Delil toplanması, yasal bilgilerin verilmesi, şüphelilerin yerlerinin bulunması.

- a. Tarafların irtibat noktaları hızlı iletişim sağlanmasına elverişli nitelikte olacaktır.

b. Herhangi bir Tarafın belirlediği irtibat noktasının, ilgili Tarafın uluslararası yardımlardan ya da iadeden sorumlu merciinin ya da mercilerinin bir parçası olmaması durumunda, söz konusu irtibat noktasının ilgili merci ya da mercilerle hızlı bir şekilde koordinasyon sağlayabilecek nitelikte olması gerekmektedir.

- Taraflardan her biri, ağın rahat biçimde işletilmesini sağlayacak eğitimi ve teçhizatı haiz personel bulunmasını temin edecektir.

Özellikle kamuoyunda uluslararası boyutta işlenen bilişim suçlarında diğer ülkelerin ülkemize yardımcı olmadıkları yönündeki yaygın inanış da dikkate alındığında, ülke olarak bir an önce SSS en azından adli yardımlaşma boyutundan en geniş biçimde yararlanabilmek için bile olsa bu Sözleşmeyi imzalamamız gerekmektedir. Çünkü SSS ile kapsamlı bir uluslararası ve milli yaklaşımlar arasında temas noktası ve sistemi getirmekte, elektronik delil toplama kolaylaştırmakta, araştırma imkânları genişletmekte, milli hukuklar arasında uyumlulaştırma sağlamakta, uluslararası karşılıklı adli yardımlaşmayı kolaylaşmakta, sözleşme tarafların karşılıklı danışmalarına zemin sağlamaktadır.

Özetle 24/7 temas noktası esasen G–8 ülkeleri tarafından oluşturulan, acil ve hızlı adli yardımlaşmayı amaçlayan bir iletişim ağıdır. Bunun yanı sıra yukarıda bahsettiğimiz gibi Sözleşmenin de 35. maddesinde de aynı mekanizma düzenlenmiştir. Ancak 24/7 sistemine dâhil olmak için sözleşmeye taraf olmak gerekmemektedir. Diğer taraftan, Sözleşmeye taraf olunduğunda ise 24/7 temas noktasını bildirmek Sözleşme çerçevesinde bir zorunluluk halini almaktadır. Bu sistem, sisteme dahil olan ülkeler arasında 24 saat cevap verecek şekilde çalışmaktadır. Bu temas noktası, diğer iade, adli yardımlaşma ve emniyetin sanal suçlarla mücadele birimleri ile doğrudan temas kuracak yetenekte olması gerekmektedir. Bunun tesis edilmesi için ise yasal dayanağa ihtiyaç duyulmaktadır. Sisteme taraf ülkelerde bu 24/7 sistemi, daha çok İçişleri Bakanlığına, bazı ülkelerde Yüksek Mahkemelere, bazı ülkelerde ise Adalet Bakanlığına bağlı olarak çalışmaktadır. Bununla beraber, hali hazırda Sözleşmeyi onaylayan ülkeler de bile tam olarak 24/7 sistemini oluşturulup Konsey'e bildirimlerini tamamlamamışlardır. Önümüzdeki dönemde ise, Sözleşme kapsamında taraf ülke iç hukuklarının uyumlulaştırılması ve Sözleşmenin uygulamaya konulması, hayata geçirilmesi ve 24/7 sisteminin işleyişini izlemek üzere bir komite oluşturulup, izleme mekanizmalarının kurumsallaştırılması planlanmaktadır.

Halen Avrupa Konseyi (AK) üyesi, AB ile ise müzakereleri sürdüren aday ülke konumunda olan ve Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne taraf olmayı değerlendiren Ülkemizin bu Sözleşme çerçevesinde düzenlenen ve Avrupa Konseyi ile AB tarafından desteklenen toplantıya katılmasının söz konusu Sözleşmenin gerektirdiği alt yapı çalışmalarının hazırlığı ve iç mevzuatımızın daha taraf olmadan uyumlaştırılması çalışmalarını başlatması yerinde olacaktır. Avrupa Konseyi kapsamındaki bu gibi toplantıların içinde bulunulmasının mukayeseli mevzuat değerlendirmelerinde bilgi değişimine zemin oluşturması ve burada oluşacak inisiyatiflerin Ülkemize hazırlık yapılmadan ve önlem alınmadan dayatılmasının bu sayede daha baştan önüne geçilebilmesini temin etmesi açısından uygun olacağı değerlendirilmektedir.

Yine bu bağlamda Sözleşme kapsamında oluşturulacak ve Sözleşme hükümlerinin iç hukuka aktarılması ve uygulama seviyesinin izlenmesi mekanizmalarının takip edilmesi ve bu kapsamda Sözleşme hükümlerinin tatbiki için önemli ölçüde uluslararası adli yardımlaşma araçlarına başvurulacak olması ve Sözleşme'nin adli yardımlaşmaya ilişkin yeni hükümler taşıması nedeniyle, Sözleşme ile ilgili konferans ve toplantıların dikkatle takip edilmesi ve bu konferanslarda Sözleşme kapsamında alınacak kararların daha alınması aşamasında izlenmesi ile Ülkemiz yararlarına uygun tecelli etmesi için gerekli girişimlerde bulunmak üzere bundan sonraki aşamalarında da faal olarak ülkemizden akademik ve uygulama seviyesinden araştırmacıların katılımının sağlanmasının yararlı olacağı düşünülmektedir.

3.18 *Adli Bilişim (COMPUTER FORENSICS)*

Adli bilişim; temelde özel verileri kurtarma teknikleri kullanarak, kimlik denetimi, analiz, fiil ile bilgisayar kullanıcısı ve data arasında ne gibi bağlantıların bulunduğu analiz ve izah etme sanatıdır. Adli bilişimde alanında uzman olan kişinin amacı bir kısım teknikler kullanmak suretiyle normal data ile bu dataları üreten son kullanıcıya veya destek veren personele ulaşmak ve aralarındaki bağlantıyı çözmektir. Kısaca dijital durum ile olay arasındaki bağlantıyı çözmektir. Bu araştırmanın içeriği yöntem bilgisayar sisteminde yasa dışı ya da izinsiz olarak kullanılmayı tanımlamaktır. Uzmanların genelde çalışma alanlarını harddisk, CD, DVD, flash Bellek, vb. depolama aygıtları oluşturmaktadır.[173]

Kısaca adli bilişim; bir bilgisayarda, yan bileşenlerinde veya bilişim sisteminde bulunan dijital delillerin araştırma ve analiz teknikleri kullanılarak incelenip irdelenmesi sonucu ortaya çıkartılan verilerin mahkemede suçluluğun veya suçsuzluğun ispatında ya da hukuk davalarındaki anlaşmazlıkları gidermek üzere incelenmesidir"[174] Bir başka tanımda, "Adli bilişim, bir yargılama esnasında kullanılabilecek potansiyel delillerin belirlenmesi için bilgisayar nin kullanılmasıdır" (Adli Bilişim, 2005). Adli bilişim, bilgisayar kullanılarak ne, kim, nerede, ne zaman ve nasıl sorularına cevap bulunmaya çalışılan yeni bir bilim dalıdır. "Dijital delil" kavramı; bilgisayardan elde edilen deliller, dijital sesler, dijital videolar, mobil telefonlar, dijital fotograf makineları, dijital faks makineları vb. nitelikteki bütün delilleri kapsadığından adli bilişimle ilgili bu çalışmada bilgisayardan elde edilen adli delil"[175] kavramı yerine "dijital delil" kavramı kullanılacaktır.

---

[173] http://en.wikipedia.org/wiki/Computer_forensics (14.04.2007)
[174] Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime Gary R. Gordon; Chet D. Hosmer; Christine Siedsma; Don Rebovich, http://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf, (17.03.2007)
[175] Carrie Morgan Whitcomb., An Historical Perspective of Digital Evidence: A Forensic Scientist's View,

Adli bilimler; tıp, fen ve sosyal bilimler alanındaki bilgilerin adaletin hizmetine sunulması ile ilgilenen bilim dallarının tümüdür.[176] Adli bilimler de; bilim ve teknolojideki gelişmelerin sosyal hayatı etkilemesi sonucu toplumların sosyal hayatlarında oluşan problemleri çözme, suçları önleme ve suçluları cezalandırma adına yasa koyucu daima yeni düzenlemeler yapmak zorundadır. Bu yeni yasal düzenlemeler neticesinde ceza hukukuna yeni kavramlar ve yeni terimler girmektedir. Yasa uygulayıcısı yapılan yeni kanunları uyguladığı sırada suçun unsurlarının oluşup oluşmadığını tespit ederken teknik konularda adli bilimlere müracaat etmektedir. Gün geçtikçe hukuk biliminin teknik konularda yardımını talep ettiği bilim dallarının sayısı artarak adli bilimlere yeni bilim dalları dâhil olmaktadır.

Adli bilimlerin başlıca çalışama alanlarını; adli patoloji, adli psikoloji, adli toksikoloji, adli seroloji, adli travmatoloji, adli hemogenetik, adli otomotiv, balistik, adli belge incelemesi, adli odontoloji, adli osteoloji, adli entomoloji ve adli mikrobiyoloji, adli arkeoloji, adli sosyoloji, adli genetik, adli mühendislik ve adli antropoloji olarak saymak mümkündür[177]. Son zamalarda hızlı bir şekilde gelişen diğer bir adli bilim dalı da adli bilişimdir. Adli bilişimi şimdilik kendi alanında bilgisayar, yazıcı, tarayıcı, dijital video, dijital fotograf, mobil telefon, depolama aygıtları, e-posta, İnternet vb. şeklinde ayırmak mümkündür. Bu alandaki teknolojinin hızla gelişmesinden dolayı bu alt bilim dallarını sınırlamak mümkün olmayacaktır.

Adli bilimlerde, uzmanlığı olmayan tıp doktorları ile Adli Tıp Kurumu'nda ya da üniversitelere bağlı Adli Tıp Ana Bilim Dallarından uzmanlık almış olan adli tıp uzmanlarından faydalanılmaktadır. Adli Tıp Kurumu Kanunu'nda yapılan değişiklikle 04.03.2003 de yürürlüğe giren 4810 sayılı "Adli Tıp Kurumu Kanununda Değişiklik Yapılmasına Dair" kanunun birinci maddesinde Adli Tıp Kurumuna adalet işlerinde bilirkişilik görevi yapmanın yanında ayrıca "adli tıp uzmanlığı ve yan dal uzmanlığı programlan ile görev alanına giren konularda sempozyum, konferans vb. etkinliklere düzenlemek ve bunlara ilişkin eğitim programı uygulamak" hususunda yetki vererek adli bilimlerin geliştirilmesi ve uzman yetiştirilmesi adına önemli bir düzenleme yapılmıştır. Bütün bu düzenlemelerin mazisi çok yeni olmasına rağmen adli bilişim ile ilgili herhangi bir kanuni düzenleme mevcut değildir.

Öncelikle bu konu ile ilgişli bir düzenleme yapılmak suretiyle Adli Tıp Kurumu Kanunu'nda köklü bir değişikliğin yapılmasına gerek bulunmaktadır. Kanunda yapılacak değişiklikle öncelikle kanunun adı "Adli Bilimler Kanunu" şeklinde olmalıdır. Adli Tıp

---

http://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf, (15.03.2007)

[176] Hamit, İ. Hancı, (20/04/2004) "Adli Tıp ve Adli Bilimler Analiz Raporu" http://home.tiscalinet.en/s.alcinkaya/hamidhanci.htm

[177] Hamit, İ. Hancı, (20/04/2004), "Adli Tıp ve Adli Bilimler Analiz Raporu" http://home.ti scalinet.ch/s.alcinkaya/hamidhanci.htm

Kurumu Kanunu'nun ilk düzenlemesinde sadece tıbbi alanlarda bilirkişilik ihtiyaçlarının giderilmesi amacıyla Adalet Bakanlığına bağlı bir kurum olarak kurulmuş iken daha sonra birimin ana yapısı içinde yer alan ihtisas Kurullarına İhtisas Daireleri de eklenerek morg, fizik, kimya, gözlem, trafik, biyooji vb. Ihtisasa daireleri kurulmak suretiyle kurum sadace tıbbi alanlarda bilirkişilik yapma fonksiyonunundan hızla uzaklaşmış olmasına rağmen birimin adının değiştirlmesi gerektiği yönünde bir girişimde bulunulmamıştır. Diğer ihtisas dairelerinde olduğu gibi şimdi de dijital delillerin sağlıklı bir şekilde toplanması amacıyla kanunun adı da değiştirilmek suretiyle Adli Bilişimi bütün boyutları ile içine alacak bir Adli Bilişim İhtisas Kurulunun kurulması gerekmektedir.

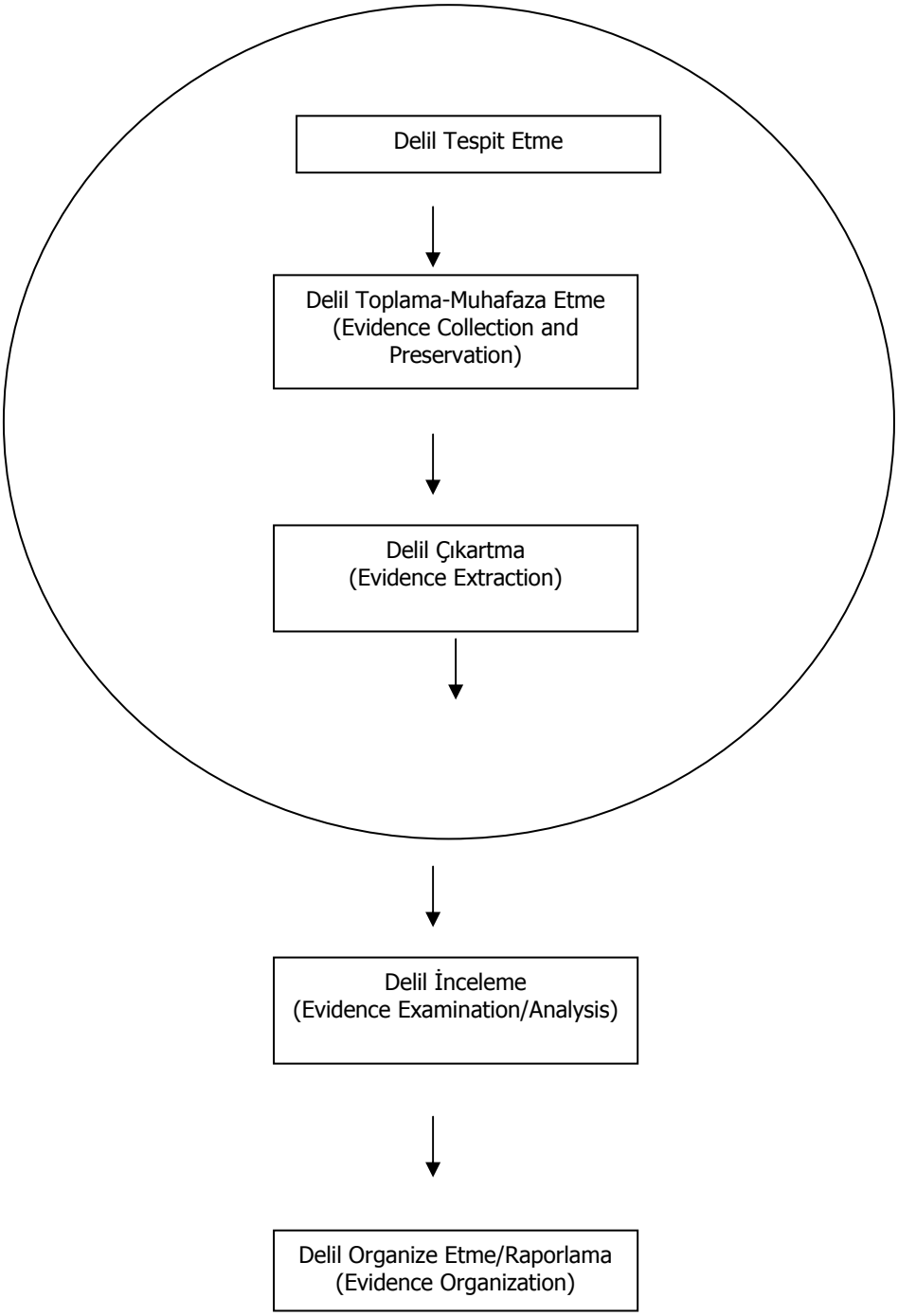
Kurulacak olan bu birimde çalışacak olan adli bilişim uzmanları belli bir sertifika proğramına dâhil edilmek suretiyle bu alanda uzmanlıklarını kanıtlamış olan kişler tarafından bilirkişilik faaliyetleri yürütülmelidir. Burada uzmanlık yapacak olan bilişim uzmanlarına ilk aşamada klasik delil toplama yöntemleri öğretildikten sonra adli bilişim alanında gerekli eğitimler verilmelidir. Bilgisayar teknolojilernin hızla gelişmesinden dolayı dijitital delillerin niteliklerinin artması söz konusu olduğundan burada çalışacak olan adli bilişim uzmanları devamlı surette gelişen teknolojilere uygun olarak tekamül eğitimlerine tabi tutulmalıdırlar. Bu birimde çalışacak olan uzmanlar özellikle fizik ihtisas dairesi ile yakın temas içinde olmadırlar. Yine bu birimde çalışacak olan uzmanları adli olayaların çözümünde istifade edeceleri son derece ileri düzey labarotuarlarının bulunması gereklidir. Dijital delillerin niteliği itibariyle alınan imaj ve yedeklerin uzun zaman diliminde saklanması gerekeceğinden yine bu ihtiyaçları giderici mahiyette yedekleme ünitelerinin bulunması gereklidir.

Adli Tıp İhtisas kurullarında olduğu gibi Adli Bilişim İhtisas Kurulunda da, yazılımdan, donanımdan, veri tabanı yönetiminden ve network yönetiminden anlayan uzman kişiler olmalıdır.

Bilgisayarlar ve diğer dijital cihazlarda adli bilişim işlemleri, bu cihazların hem suçlular tarafından suçu işlemede araç olarak kullanıldığında hem de herhangi bir suçun işlenmesinde direkt olarak kullanılmasa dahi suçluların bilgisayarları kendi aralarındaki iletişimde veya işlemlerini kolaylaştırmak ve bilgileri yedeklemek için kullanmaları durumunda yapılmaktadır. Günümüzde hemen herkes tarafından her türlü iş yapılırken bilgisayarlar veya diğer elektronik cihazlar kullanıldığı düşünülürse, sadece bilişim suçlarının araştırması ve soruşturmasında değil belki birçok suç türünün araştırma ve soruşturmasında adli bilişim tekniklerinden istifade etmek gerekmektedir. Bilgisayar teknolojileri; işlenen suçların araştırılmasında kullanılan aygıtlar olabileceği gibi bu cihazların kullanılması ile de birçok suç işlenebilmektedir. Adam öldürme eyleminin silahla işlenmesi ile dolandırıcılık eyleminin bilişimin vasıta kılınmak suretiyle

işlenmesi arasındafarklılık bulunmamaktadır. Adli bilişimin aşamalarını; delil tespit etme, delil toplama-muhafaza etme, delil çıkartma, delil inceleme ve delil organize etme/raporlama olarak saymak mümkündür.

Adli bilişim aşamaları:



Olay Yerinin, Dijital Delillerin Güvenliği ve Dijital Delil Tespit Etme Yöntemlerine bakıldığında; Olay yerine giden ilk müdahale grubu öncelikle delil toplamada kullanacakları aygıtları hazır etmeli, kendi güvenliğinden emin olmalı, ardından olay yerinin güvenliğini sağlamalı ve akabinde olay yerindeki dijital olan ve olmayan bütün delillerin sağlamlığını ve bütünlüğünü koruma altına almalıdırlar. Olay yeri incelemesinde aşağıdaki işlemler dikkatli bir şekilde yerine getirilmelidir;[178]

Olay yerinin güvenliği sağlanmalı, dijital delillerin değiştirilip bozulmasına izin verilmemelidir,

Fiziksel ve dijital bozulabilir deliller koruma altına alınmalıdır; ilk müdahale grubu olay yerinde bozulabilir verilerin varlığını her zaman düşünmeli bunların hemen çevre güvenliğini sağlamalı, dokümante etmeli ve fotoğraflamalıdır.

Modemler, çağrı kutuları gibi bilgisayara telefonla bağlanan cihazlar tespit edilmelidir. Bu tür cihazlar dokümante edilmeli, sökülmemeli sadece etiketlenmelidir.

Ayrıca LAN/Ethernet, kablosuz, kızılötesi, firewire bağlantı varsa bunlar da aynı şekilde tespit edilip etiketlenmelidir.

Klavyede, farede, disketlerde, cd ve dvd'lerde ve diğer bilgisayar bilişenlerinde parmak izi veya diğer fiziksel deliller muhafaza edilmelidir.

Kimyasal madde kullanımı cihaz ve verilere zarar verebilir. Dolayısıyla gizli izler dijital deliller kurtarıldıktan sonra toplanmalıdır.

Once varsa fiziksel delillerin tespiti yapılmalıdır, olay mahalline mümkün ise fiziksel delil toplama ekipleri de hazır bulunmalıdır.

Daha sona çalışan sistemler üzerinde delil toplama işlemleri yapılmalıdır. Kullanılan lisanslardan, çevre birimlerinden ve bilgisayar parçalarından fatura bilgilerine ulaşma yöntemleri araştırılmalıdır.

Elde edilen deliller tehlikeli virüsler, elektromanyetik yahut mekanik zarara uğramış olabilir, yâda tuzak içerebilir. Dijital delillerin araştırılması sırasında bu hususlara dikkat edilmelidir.

Bir kısım araştırmalarda dijital delillerin araştırılacağı yer sahipleri delilleri araştırılmasına izin vermeyecektir, bu delillilerin araştırılmasında hukuki prosedürlerin zamanında yerine getirilmesi sağlanmalıdır.

[178] Carrier, Brian., Spafford, Eugene H.,Getting Physical with the Digital Investigation Process, https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2003-29.pdf, (16.03.2007)

Olay yerinde elde edilen notlar dikkatli bir şekilde incelenmelidir, bunların arasına şifreler yahut planlar gizlenmiş olabilir.

Araştırılacak dijital delilin çalışmakta olduğu aygıt halen aktif ise son açılan uygulamalar kaydedilmelidir. Şayet makinada illagal suç örgütleri ile haberleşme yapılıyorsa bu bilgiler donanımda kayıtlı olmayabilir. Bilgiler sadece RAM de tutulduğundan RAM deki işlemlere son verildikten sonra bu son verme işlemi öncesi kullanılan verilere ulaşmak mümkün olmayacaktır. Temel amaç RAM kapatılmadan önce çalışan uygulamaların tespitine yönelik olmalıdır. Bir kısım donanımlar kendiliğinde kapatıldığında önceki verileri silmeye ayarlanmış olabilir, ideal olan uygulamaları kapatmadan önce gerekli çalışmalar yapılarak delil toplama işleminin yapılmasıdır, örneğin çalışan uygulamalar, uygulamalarda yapılan faaliyetler, en son girilen İnternet siteleri vb. gibi tespitleri yapılmalıdır.179

Ram'ler güçlerini kaybettikten sonra da her ne kadar besleme zamanındaki kadar olmasa da içerikleri analiz edilebilir. Ram'deki datalar uzun bir periyotta statik bir alanda durduklarından bir kısım metodlar kullanılarak algılanabilir. İşletim sisteminin sıcaklığı ve sürekliliği bu dataların kurtarılmasını artıran faktörlerdendir. Besleme olmadan -60C den daha aşağı bir muhafaza edilen RAM'lerden başarılı bir şekilde data kurtarılma şansı vardır.180

Açık olarak yakalanan bilgisayarlar kapatılırken bu aşamada bir kısım verilerin kaybına sebebiyet verecek scripler kapatma aşamasında çalışacak şekilde ayarlanmış olabilir bu durumda da hazfızadaki bilgiler yada harddiskteki bilgiler zarara uğrayabilir, bu değişik işletim sistemlerin değişik yöntemler kullanılarak yapılıyor olabilir, yada "volatile data" uçucu datalar olabilir, ayrıca beslemenin kapatılması durumunda dosya sistemi zarar görebileceği gibi bir kısım hayati dataların kaybına da sebebiyet verilebilecektir.181

Sisteme izinsiz girmeye karşı kendiliğinden çalışan ve kendisini yok eden mekanizmalara kurulmuş olabilir. Bu durumda da bir kısın veriler zarar görbilir, bu verilerden de bir kısm kurtarılabilir, bu makinelarda özellikle capasitorlere, bataryalara, alışılmışın dışında bilgisayar yanında bulunan aygıtlara dikkate etmek gerekiyor, bunlar patlayıcı olabilir, aksi takdirde korkulacak bir durum olmayacaktır, ayrıca kablosuz bağlantılara dikkat edilmelidir. CMOS (Bütünleyici Metal Oksit Yarıiletken) bataryaların kullanılması durumund anakartın kendiliğinden bilgi depolama durumu sözkonusu olabilir, bu bataryaların kaldırılmasından kaçınılmalıdır.182

---

179 http://en.wikipedia.org/wiki/Computer_forensics
180 http://en.wikipedia.org/wiki/Computer_forensics
181 http://en.wikipedia.org/wiki/Computer_forensics
182 http://en.wikipedia.org/wiki/Computer_forensics

Donanımlar vb. aygıtların imajı alınırken bağımsız başka bir bilgisayar kullanılmalı ve harddisk vb.aygıtların tamamıyla suretleri çıkartılmalıdır, imajları alınmalıdır. Dosya sisteminin suretini almadan ziyade bölüm bzalı kullanım mevcut ise kullanıcı erişim alanları ayrı ayrı alınmalıdır. Alınan imajlar sürücülerle eşleştirilmeli ve biribirine karıştırılmamalıdır. Orijinal sürücüler güvenli bir ortamda saklanmaldır.

İmaj alma durumunda orijinal sürücüler kullanılmasızın imajlar alınmalıdır, imajlar diğer bir harddiske, tape ünütesine yada başka araçlara yüklenebilir, tape ünüteleri tercih edilmelidir, bunlar saldırılara daha az maruz kalırlar, uzun sürede bilgileri muhafaza edebilirler.

Delilleri tespit etme sırasında; dijital delillerin tanımlanması ve belirlenmesi, belirlenen tüm dijital delillerin fotoğraflanarak üzerine ilgili tanımlayıcı bilgilerin yazılarak etiketlenmesi ve fiziksel olmayan delil sayılabilecek bilgilerin not edilmesi, dijital deliller tespit edilirken, olay yerinde bulunan potansiyel bilgi bulunabilecek bütün dijital cihazlar; bilgisayarlar, cep telefonları, el bilgisayarları, dijital fotoğraf makinaları, dijital kameralar, flash kartlar, usb ürünler, modemler, ağ cihazları, ağ sunucuları, disk alanları, çıkarılabilir depolama araçları, tarayıcılar, printerlar, ses kayıt cihazları, fax makinaları, vb. gözönünde bulundurulmalıdır.

Olay yerinde hemen her şey çok dikkatle incelenmelidir. İlk bakıldığında farklı gözüken birçok cihaz bilgisayar veya bilgisayar çevre birimi olabileceği hatırdan çıkartılmamalıdır. Dijital deliller, diğer klasik deliller gibi dikkatle toplanmalı ve gerçek değerini koruyacak şekilde hareket edilmelidir. Bu hareket sadece öğelerin fiziksel bütünlüğü için değil, bunların içinde bulunan veriler içinde aynı hassasiyet gösterilmelidir. Delillerin bozulmasına sebep olacak toplama teknikleri (parmak izi alınması için kimyasal madde kullanımı gibi) dijital delillerin kurtarılmasından sonraya bırakılmalıdır.

Dijital deliller toplanırken araştırmada ve incelemede faydası olacak dijital olmayan diğer delillerin toplanmasına da dikkat edilmelidir. Küçük kâğıtlara yazılmış sistem bilgileri, kullanıcı adları, şifreler, el yazması notlar, baskılı yazılmış boş kâğıtlar, donanım ve yazılım kullanıcı belgeleri, ajandalar, eserler, yazılı veya grafiksel yazıcı çıktıları, fotoğraflar, IP adresleri, vb. bu türden bilgilerdir. Sisteme/sistemlere ait aşağıdaki bireysel bilgiler alınmalıdır. Dijital delillerin sahipleri ve/veya kullanıcıları, şifreleri, kullanıcı adları ve İnternet servis sağlayıcıları sistemdeki yazılım ve verilere ulaşabilecek şifreler (bireysel şifreler, BIOS, sistem login, network veya ISP, uygulama dosyaları, kriptolu veriler, mailler vb.) dikkatli bir şekilde araştırılmaldır.

Üzerinde delil araştırması yapılan sistemin amacı, sistemin herhangi bir güvenlik planı veya cihazları yıkıcı tedbirlerle korunup korunmadığı, gizli bir veri

depolama aygıtlarının bulunup bulunmadığı, sistemde bulunan donanım ve yazılımı açıklayıcı herhangi bir dokümanın olup olmadığı araştırılmaldır.

Dijital Delillerin Toplanması aslında bağımsız masaüstü ve dizüstü bilgisayarlardan delil toplama sadece bir bilgisayardan veya bir dizüztü bilgisayardan delil toplamadır. Kompleks sistemlerdeki bilgisayarlardan delil toplama, iş yerleri ve kurumlardaki bilişim sistemlerinden delil toplamadır. Bu tür sistemlerden delil toplanırken sistemlerin ayakta kalmaları sağlanmalıdır. İşletmelerin durumuna göre genelde sistemler çalışırken delil toplamak gerekmektedir.

Masaüstü bilgisayarlarından, dizüztü bilgisayarlarından, karmaşık ağ bilgisayarlarından yukarıda belirtilen yol ve yöntemlerle toplanan hard diskler ve diğer medyalar (CD-ROM, DVD-ROM, disket, vb.) adli bilişim standartlarına uygun olarak imaj alınmak suretiyle yedeklenmelidir.

Bu delillerin toplanması sırasında aşağıdaki hususlara dikkat edilmelidir.

- Imaj alma, donanımsal (hard disk kopyalama cihazları kullanılmak suretiyle) ve yazılımsal (çeşitli programlar kullanılarak) imaj alma olarak iki tür olabilmektedir.
- Delillerin değiştirilme ihtimaline binaen elle dokunulmaktan kaçınılmalıdır.
- Denetleme ve gözetleme zinciri kurulmalı ve takip edilmelidir.
- Hiç bir zaman orjinal delil (hard disk, cd, disket, vb.) üzerinde çalışma yapılmamalıdır. Şartların gerektirmesi sonucu orjinal delil (çalışan sistemler) üzerinde inceleme yapılacaksa bunun konunun uzmanı kişiler tarafından yapılması ve yapılan bütün işlemlerin dokümante edilmesi gerekmektedir.
- İmaj, orjinal delilin birebir (bit-to-bit, sector-by-sector) kopyası olmalıdır. İmaj alma işlemi adli bilişim standartlarına uygun programlar tarafından alınmalıdır.
- İmaj alma işleminde geçerli asgari adli bilişim standartları; kullanılan program orjinal medyada herhangi bir değişiklik yapmamalıdır, program orjinal diskin birebir (bit-to-bit, sector-by-sector) kopyasını almalıdır (raw image) veya birebir kopya ve ek bilgileri (tarih-saat, imajı alan kişinin ismi, olayın ismi, vb.) beraberce alabilmelidir (bit-plus image) program her türlü disk arabirimi (IDE, SCSI, ATA, vb.) ile çalışabilmelidir, program orjinal diske ait imajı bir başka diske alabileceği gibi usb disk veya benzeri harici medyaya alabilmeli ve alınan imajı bir dosya halinde tutabileceği gibi kullanıcının belirteceği ve teknolojinin müsaade edeceği büyüklükte parçalar halinde alabilmelidir, program arızalı disklere ait imajı alabilmelidir ve program imaj alma esnasında meydana gelen bütün hata mesajlarını loglayabilmelidir.

• Bir bilgisayarın hard diskinin yedeği alınırken bilgisayardaki mevcut işletim sistemi mümkün mertebe kullanılmamalı, temiz bir açılış disketi ve CD'si kullanılarak işlemler yapılmalıdır.

• Bir bilgisayar çalışırken dijital delil toplama durumunda bazı konulara dikkat etmek gerekmektedir. İlk olarak çalışan sistemlerde toplanacak bütün deliller toplanmadan sistem kapatılmamalıdır. Çalışan sistemlerde mevcut olan programlara güvenmemek temel bir ilkedir; bu yüzden CD ile güvenilir programları kullanmak gerekmektedir. CD'den çalıştırılan programlar, sisteme kurulmadan çalıştırılabiliyor olmalıdır. Çalışan bilgisayalardan toplanan veriler şunlardır: bellek (memory) içeriği, registry içeriği, ağ bağlantıları, çalışan programlar, sistemin tarih ve saati, açık portlar, sistem bilgileri, sisteme girmiş kullanıcılar, dosya sistemi ve benzerleridir. Yapılacak araştırmada şüpheli dosyalara en son ulaşım zamanları, karşılaştırılmalı, İnternet'e en son giriş çıkış saatleri, en son erişilen İnternet siteleri, çerezler ve alışılmışın dışında hatları belirsiz beklenene ters düşen tuhaf ve uygunsuz e-posta trafiklerinin incelenmesi ile sonuç çıkartılması incelenmelidir.[183][184]

Dijital Delillerin Muhafaza Edilmesi delillerin kullanabilirliği açısındançok önemlidir. Dijital delillerin yapısı gereği, özel toplama, paketleme ve taşıma sistemi gerekmektedir. Statik elektrik, manyetik, radyo vericileri ve bu gibi diğer cihazların oluşturduğu manyetik alandan zarar görme veya bozulma ihtimaline karşı veriler önemle korunmalıdır.

Bütün toplanan delillerin paketlenmeden önce dokümante edildiğinden, etiketlendiğinden ve kaydı yapıldığından emin olunmalıdır.

Hassas veya örtülü/gizli delillere özel dikkat gösterilmeli ve korumaya yönelik tedbirler alınmalıdır.

Manyetik medyaları anti statik paketlerle veya statik plastik çantalarla paketlemeli, standart plastik çantalar gibi statik elektrik üreten materyallerin kullanımından kaçınılmalıdır.

Disket, CD-ROM ve manyetik bantlar gibi bilgisayar medyalarını kazımaktan, bükmekten ve katlamaktan kaçınılmlalıdır.

---

[183] Carrier, Brian., Spafford, Eugene H.,Getting Physical with the Digital Investigation Process, https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2003-29.pdf , (16.03.2007)

183 Lim, Mark Jyn-Huey., Negnevitsky, Michael., Hartnett, Jacky, http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Lim%20et%20al%20-%20A%20Fuzzy%20Approach%20For%20Detecting%20Anomalous%20Behaviour%20in%20E-mail%20Traffic.pdf , (15.03.2007)

184 Lim, Mark Jyn-Huey., Negnevitsky, Michael., Hartnett, Jacky, http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Lim%20et%20al%20-%20A%20Fuzzy%20Approach%20For%20Detecting%20Anomalous%20Behaviour%20in%20E-mail%20Traffic.pdf , (15.03.2007)

Elde edilen delillerin konduğu kutuların hepsinin etiketlendiğinden emin olunmalıdır.

İmajı alınan verilerin hash değerleri SHA veya MD5185 hesaplama yöntemleri İle tespit edilmelidir. Buradaki amaç incelenen imajların dğiştirilme olasılığının bulunması ve ilerde meydana gelebilecek olan itirazların ortadan kaldırılmasıdır.

Eğer çoklu bilgisayar sistemleri toplandıysa her bir sistem kendi içerisinde etiketlenmelidir. Çünkü sistem o bilgiler ile tekrar ayağa kaldırılabilmelidir (A sistemine ait kasa, monitör, fare, klavye, B sistemine ait vb..

Diğer önemli bir konuda Dijital Delillerden Bilgiler Çıkartmadır. Delil çıkartma, imaj alma programları ile alınan imaj dosyalarından delil olabilecek verilerin bulmunmasıdır. Delil çıkartma esnasında, mevcut dosyaların çeşitli programlarla aranması ve listelenmesi yapıldığı gibi, silinmiş ve gizlenmiş dosyalar bulunmakta veya işletim sisteminden birçok bilgi toplanmaktadır. Delil çıkartma işlemleri aşağıdaki başlıklarda sıralanabilir;

- Mevcut dosya araması,
- Silinmiş dosya araması,
- Unallocated alandan dosya araması,
- Kelime araması,
- İnternet işlemleri,
- Link dosyaları,
- Print spool dosyaları,
- Registry incelemesi,
- Dosya imza analizi,
- Hash analizi,
- Geri dönüşüm kutusu kurtarma,
- Swap dosyası,
- Unused disk area,
- Windows açılışında otomatik çalışan programlar,

[185] Şifreleme algoritmalarına yardımcı olmak amacıyla kullanılabilecek bir HASHING / FINGERPRINTING algoritmasıdır ve yalnızca 128-bit'lik (16-bayt) bir çıktı üretir. Bu öncelikle bir verinin (dosyanın) doğru transfer edilip edilmediği veya değiştirilip değiştirilmediğini kontrol etmek için kullanılan bir yöntemdir. (Md5 Nedir?, http://www.supermeydan.net/forum/forum439/thread3935.html, (15.03.2007)

- Saklanmış bölümler (hidden partitions),

Dijital Delil İnceleme farklı bir ihtisas gerektirir. Adli bilişim uzmanları bilgisayardaki her dosyayı teker teker inceleyemeye zaman bulamayabilirler. Günümüzde disk boyutları sürekli büyümekte ve diskler içerisinde on binlerce hatta yüz binlerce dosya bulunmaktadır. Bu dosyalar çeşitli türlerde (resim, görüntü, yazı, vb.) dosyalar olabilmektedir. Adli bilişim uzmanları dosya inceleme işlemini hızlandıracak ve uzmanlara yardımcı olacak programlar kullanma ihtiyacı hissetmektedirler. Delil inceleme programları bu ihtiyacı karşılamak üzere hazırlanmış programlardır. Delil inceleme programlarını üç ayrı kategoride incelemek mümkündür. Bunlar:

1. Dosya listeleme programları,
2. Kelime arama programları,
3. Dosya tanımlama/görüntüleme programlarıdır.
4. Dijital delillerin araştırılmasına hataya sebebiyet vermemek için birden fazla delil inceleme yöntemi kullanılmak suretiyle ortaya çıkartılan delilleri doğrulanmalıdır.[186]

Dejital delillerin sırasında her zaman imajı alınan yedeklenen deliller üzerinde çalışma yapılmalıdır. Kesinlikle orijinal deliller üzerinde çalışma yapılmamalıdır.

Dijital Delil Organize Edip Raporlama adli bilişimin en önemli ayaklarından biridir. Suç araştırmalarında delillerin iyi organize edilmesi (raporlanması) her zaman önemlidir. Delil organize işlemi hem dijital olmayan deliller hem de dijital deliller için geçerlidir. Dijital deliller organize edilirken çoğu zaman dijital olmayan delillere de ihtiyaç duyulmaktadır. Deliller organize edilirken bunun gözönünde bulundurulması ve hangi delilin hangi konuyla ilgili olduğu çok iyi belirlenmesi gerekmektedir. Konunun gelişimi çoğu zaman hem dijital hem de dijital olmayan delillerin doğru sıraya konması ile anlaşılabilmektedir. Özellikle dijital delillerin yoğunluğu ve iyi organize edilmemiş deliller günümüzde araştırmacıların delil inceleme safhasında boğulmalarına ve doğruyu bulamamalarına veya geç bulmalarına sebep olmaktadır. Adli bilişim aşamalarının etkin yapılması iyi organize edilmiş ve mahkemede tatmin edici raporların hazırlanması olmadan sonuca varılmaz.

Araştırma sonucu hazırlanacak raporda aşağıdaki bilgilerin bulunması gereklidir:

a. Araştırmayı yapan kurumla ilgili bilgiler,

b. Olayla ilgili bilgiler,

[186] Michael R., Anderson., Defending Against Junk Science Attacks, http://www.forensics-intl.com/art20.html, (16.03.2007)

c. Araştırmaya başlanma tarihi ve bitiş tarihi,

d. El konan ve inceleme yapılan dijital delillerle ilgili bilgiler,

e. Araştırmada kullanılan donanım ve yazılımla ilgili bilgiler,

f. Araştırmada izlenen yol ve kullanılan metod ve taktikler,

g. Gözetim zinciri (hangi delil ahngi tarihte kimden kime aktarıldı),

h. Araştırma sonucu bulunanlar, nereden ve nasıl bulundukları rapor edilmelidir.

Suçluların Tespiti bilişim sistemlerinde nasıl yapılmaktadır? Bu sorunun cevabını bulabilmek için bilişim suçu araştırmalarında ilk olarak adli bilişim yöntemleri doğru olarak uygulanmalıdır. Bu yöntemlerin bazılarını sıralarsak;

- Delillerin güvenliği sağlanmalıdır.
- Deliller doğru tespit edilmelidir.
- Uygun imaj alma programları kullanılmalıdır.
- Saklanmış, gizlenmiş ve silinmiş veriler bulunmalıdır.
- Çıkarılan veriler iyi incelenmelidir.

Suçluları tespit edebilmek için yukarıda sayılan bilgilere ilave olarak klasik polis çalışması da yapılmalıdır. Dijital-dijital olmayan deliller beraberce zamana göre incelenmelidir. Sadece bilgisayar ortamında yapılan incelemelerle sonuca varmak çoğu zaman mümkün olmamaktadır.

Sonuç olarak öncelikle Adli Tıp Kurumu Kanununda gerekli düzenlemeler yapılarak kanunun adı Adli Bilimler Kanunu olarak değiştirilmeli veya Adalet Bakanlığı ile ilgili bağımsız bir kurum kurularak bu bilişim suçlarının delillendirilmesi konusunda uzmanlaştırılmalı,

Bu kanunla İhtisas Kurullarındaki yapılanmaya benzer bir yapılanma ile adli bilişim suçlarında incelemede bulunacak yeni bir ihtisas kurulunun kurulması, bu kurulda yeterli sayıda ve uzmanlık alanında uzmanın görevlendirilmesi, bu birimlerin nitelikli ve standartlara uygun yazılımlar ve donamımlarla desteklenmesi, delillerin bu birimde muhafaza edileceği süre ve şartların kanun ile çerçevesinin tayin edilmesi,

Adli Bişilim alanında uzmanlık yapacak uzmanlar kurulacak yada yetkilendirilecek bir sertifikasyon merkezi tarafından gerekli eğitim çalışmaları tamamlanarak bu kişilere gerekli olan yeterlilik sertifikası verilmeli,

Bilişimim doğrudan ya da dolaylı olarak kullanılması ile işlenen suçlarda diğital delillerin toplanması muhafazası ve değerlenedirilmesi, elektronik verilerin delil olarak

hukuki niteliği, yardımcı delil, ana delil olması, delil vb. hususlarında yargılama faaliyetine katılan kişilere gerekli eğitimlerin verilmesi,

Dijital delillerin ortadan kaldırılması veya değiştirilmesi çok kısa zamanda olabildiğinden bu delillerin toplanmasın uygulanacak usulü yöntemlerin kişi hak ve özgürlüklerini de kısıtlmayacak şekilde Ceza ve Hukuk Yargılama usulü yasalarında gerekli düzenlemelerin yapılması, ayrıca telefon dinleme yöntemlerinde olduğu gibi bilişim teknolojileri üzerindeki hareketlerin takip altına alınması usul ve yöntemleri ile ilgili düzenlemelerin yapılması temel sorun olarak karşımıza çıkmaktadır.

4 BİLGİ GÜVENLİĞİ

4.1 Genel Olarak Bilgi Güvenliği

Bilgi önceki zamanlarda söylendiği gibi güç olmaktan çıkmış günümüzde bir varlık halini almıştır. Bilgi ve destek süreçleri, sistemler ve bilgisayar ağları önemli ticari varlıklardır. Bilginin gizliliği, güvenilirliği ve elverişliliği; rekabet gücünü, nakit akışını, karlılığı, yasal yükümlülükleri ve ticari imajı korumak ve sürdürmek için zorunlu ve gerekli olabilir. Giderek işletmeler ve sahip oldukları bilgi sistemleri ve ağları bilgisayar destekli sahtekârlık, casusluk, sabotaj, yıkıcılık, yangın ve sel gibi çok geniş kaynaklardan gelen tehdit ve tehlikelerle karşı karşıyadırlar. İş dünyasında bilişim teknolojilerinin yoğunlukla kullanılmasıyla birlikte bilgisayar virüsleri, bilgisayar korsanları ve hizmet saldırıları gibi yıkıcı kaynaklar daha yaygın, daha hırslı ve daha karmaşık hale gelmeye başlamıştır. Bilgi sistemlerine ve hizmetlerine bağımlılık, işletmelerin güvenlik tehditlerine karşı daha savunmasız olduğu anlamına gelmektedir. Genel ve özel ağların birbiriyle bağlantısı ve bilgi kaynaklarının paylaşımı, erişim denetimini oluşturmadaki zorlukları arttırmaktadır. Dağıtılmış bilgi işleme olan eğilim, merkezi, uzman denetimin etkinliğini zayıflatmıştır.

Bilgi sistemleri henüz yeterli güvenlik seviyesinde tasarlanmamıştır. Teknik olanaklar aracılığıyla ulaşılabilen güvenlik sınırlıdır ve uygun yönetim ve yöntemlerle desteklenmelidir. Hangi denetimlerin yer alacağının tanımlanması, özenli planlamayı ve detaylara dikkati gerektirir. Bilgi güvenliği yönetimi en az, tüm işletme çalışanlarının katılımını gerektirir. Aynı zamanda tedarikçilerin, müşterilerin ve ortakların da katılımına gereksinim duyulur. İşletme dışından uzman tavsiyelere gerek duyulabilir. Bilgi güvenliği denetimleri, eğer şartların ve tasarım aşamasının gereklerinde birleştirilirse çok daha ucuz ve etkili olur.

Günümüz sadece çalışanlarıyla değil, müşteri, iş ortakları ve hissedarlarıyla birlikte tanımlanan organizasyonlarda, bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine ilişkin güven ortamının yaratılması, stratejik bir önem taşımaktadır. Bu konuyu biraz daha açığa kavuşturmak için Amerika Birleşik Devletlerinde Computer Security Institute

(CSI) ve Federal Bureau of Investigation (FBI) tarafından her yıl hazırlanan “Bilgisayar Suçları ve Güvenlik Gözlemi” (Computer Crime and Security Survey) nin 2005 yılı raporu incelendiğinde:

ABD de firmaların çalışan başına yaptıkları bilgi güvenliği harcamalarına bakıldığında yıllık gelirlerine göre;

Yıllık Gelir	İşletme Giderleri	Sabit Giderler	Toplam
< 10 mio. $	358$	285$	643$
10–99 mio. $	89$	52$	141$
100–1000 mio. $	216$	109$	325$
> 1 milyar $	170$	77$	247$

Kullanılan bilgi güvenliği teknolojileri incelendiğinde firmaların;

- % 97 si firewalls,
- % 96 sı Anti-virus software,
- % 72 si Intrusion Detection Systems,
- % 70 i Server-Based Acces Control Lists,
- % 68 i Encryption for data in transit,
- % 52 si Reusable account/login passwords,
- % 46 sı Encypted files,
- % 42 i Smart cards / other one-time password tokens,
- % 35 i Public key infrastructure,
- % 35 i Intrusion Prevention Systems,
- % 15 i Biometrics

Çözümler kullandığı tespit edilmiştir.

Kullanılan güvenlik teknolojilerine rağmen bu firmaların 2005 yılında değişik bilgi güvenliği açıklarından kaynaklanan maddi kayıplarının toplamı 130,1 milyon $ gibi çok büyük bir meblağdır.

Bu firmaların % 87 si güvenlik denetimi yaptırmakta, % 70 i de çalışanlarının güvenlik bilinci eğitimi almalarına inanmaktadır.

Aslında bilgi güvenliğini sağlamak çalışmaları 90'lı yıllara dayanmaktadır. Bilgi güvenliğinin teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sisteminin kurulması ile mümkün olabileceğinin anlaşılmasıyla birlikte tüm dünyada farklı gruplar tarafından çalışmalar başlamıştır. Avrupa da 1990 lı yılların sonunda bir grup İngiliz bilişim güvenliği uzmanı tarafından küçük, orta ve büyük firmalar tarafından benimsenip kullanabilecekleri ISO/IEC 17799:2000 Bilgi Güvenliği Yönetim adıyla bir standart hazırlandı. BS 7799 Parti 2,2002 Bilgi Güvenliği Yönetim Sistemi Özellikleri (Specification for information security management systems) British Standard Institude (BSI) veya akredite belgelendirme kuruluşları tarafından BS 7799 adıyla belgelendirmeye esas bir standart halini almıştır. 15 Ekim 2005 tarihinde ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi (Information security management systems) standardı uluslararası bir standart olarak yayınlandı. Bilgi Güvenliği Yönetim Sistemi konusunda yayınlanmış olan bu standart yayım tarihinden itibaren, BS 7799–2,2002'nin yerini almıştır.

Dünya ölçeğinde önde gelen bilişim şirketinin sahibi yakınlarda basında yayınlanan yazısında bilişim dünyasının birinci ve en önemli meselelelerinden birinin bilgi güvenliği olduğuna işaret etmişti[187]. 2007 yılı ve sonrasında nda giderek bilgi güvenliği açısından daha akıllı ve kompleks saldırılar beklenmekte ve özellikle kişisel verilerin ele geçirilmesi odaklı faaliyetlere ağırlık verilmektedir. Önde gelen bilgi güvenliği şirketleri raporlarında bu konuya dikkat çekmektedirler. Gerçekten de yine bir şirketin raporuna göre 2006 yılında 7247 adet yeni bilgi güvenliği açığı ortaya çıkmış ve her gün de ortalama 20 adet güvenlik açığı ortaya çıkmaktadır. Rapora göre dikkat çeken bir başka konu ise ortaya çıkan güvenlik açıklarının % 88 inin uzaktan gerçekleştirilmiş olması. İyi haber ise 2005 yılında meydana gelen zararı büyük saldırıların toplamdaki payı %28 paya sahip iken, 2006 da bu oran alınan önlemlerle %18 düşmüş olması[188].

Tüm bu gelişmeler ve güvenlik ihtiyacının artması, standartlarla başlayan çalışmaların zamanla standartların temel ve ana çatı yasalara ve daha alt mevzuatta yer bulması zorunluluğu ile sonuçlanmış olması sonucunu doğurmaktadır.

4.2 Almanya'da Bilgi Güvenliği ile İlgili Mevzuat

Almanya'da 1 Ocak 1991 tarihinde federal Almanya İç İşleri Bakanlığına bağlı, Almanya'daki bilgi güvenliğinden sorumlu bir kurum oluşturulmuştur. Bu kurulun adı "Bundesamt für Sicherheit in der Informationstechnik" (BSI) yani Bilişim Teknolojileri için Bilgi Güvenliği kurumudur. Bu Kurum Bilişim Teknolojilerinde Güvenlik İçin Federal

[187] "**Güven ve güvenlik ,….'un en çok önem verdiği öncelikler arasında yer alır."** **http://www.belestr.com/konu-13547.html (30.04.2007)**

[188] Sektörsel Bilgi Teknolojileri, "İnternet korsanları 'kişiye özel saldırıyor'"(26.04.2007 tarihli nüsha)

Bir Kurum Kurulması Hakkında Kanun[189] ile kurulmuş ve en son 25 Kasım 2003 tarihli Kararnamenin 11. Maddesi ile değişiklik yapılmıştır.

Kurumun başlıca görevleri Avrupa'da ki benzer kuruluşların aksine ve onlardan daha farklı olarak Bilişim Teknolojileri konusundaki Bilgi Güvenliği ile ilgili her türlü konuyu bünyesinde toplayarak Bilgi Güvenliği ile ilgili her türlü sorumluluğu üstlenmektir. BSI'nin en önemli görevlerinden birisi enformasyon teknolojilerindeki hızlı gelişmeye ayak uydurarak sürekli ortaya çıkan güvenlik ihtiyacını tespit etmek ve meydana gelen boşlukları doldurmaya çalışmaktır. Kuruluş Kanunun 3. Maddesinde kurumun görevleri sayılmıştır. Bunlar;

- Uygulamalardaki güvenlik rizikolarını araştırmak, Devletin (Federal Bazda) görevlerini yerine getirme bağlamında, görev gerektiriyorsa gelişen güvenlik (tedbirleri) önlemleri gibi konuları ve özellikle BT alanındaki güvenlik süreçlerini (Usullerini) ve araç-gereçlerini takip etmek,

- BT sistemleri veya bileşenlerinin test edilmesi ve değerlendirilmesi için Kriterleri, usulleri ve araç-gereçleri geliştirmek,

- BT Sistemlerinin veya bileşenlerinin test edilmesi ve değerlendirilmesi ve güvenlik sertifikalarının dağıtılması,

- Gizli resmi bilgilerin işlenmesi veya iletimi için (şifreli veya kilitli veriler) Federal veya işletmelerde (ruhsatlı şifreleme aletlerinin ihtiyaç duyduğu şifreli verilerin üretilmesinde olduğu gibi Devletin görevlerinin özel sektöre devredilmesi halinde bu işletmelerde) BT Sistemlerine veya bileşenlerine onay (ruhsat) verilmesi,

- Yetkili Federal Kurumları, BT güvenliği için desteklemek, (özellikle danışma ve kontrol görevi ölçüsünde Kişisel verilerin Korunması Yetkilisinin Kişisel Verilerin Korunması Kanununda bulunan görevlerini yerine getirme bağlamında ve bağımsızlığı çerçevesinde, öncelikli olduğuna dikkat edilir)

- Polis ve Kolluk Güçlerinin yasal görevlerinin yerine getirilmesinde destek verilmesi,

- Anayasayı koruma yetkilileri, Federal veya Federe Anayasayı Koruma Kanunlarına göre yasal yetkileri ve görevleri dâhilinde, terörist gözleme faaliyetlerinde veya istihbarat çalışmalarında bilgilerden faydalanma ve değerlendirmede destek sağlamak. Destek sadece BT Güvenliğine yönelmiş veya BT kullanılarak meydana gelmiş belirli olayları önleme veya araştırma için ve gerekli ise sağlanır. Destek talepleri kayıt altına alınarak yapılır.

[189] http://www.bsi.de/bsi/gesetz.htm (21.04.2007)

- Üreticilere, işletmelere ve uygulamacılara BT güvenliği sorunları konusunda danışma ve destek olmada, eksik veya yetersiz güvenlik tedbirleri konusunda dikkat edilmesi istenir.

- 1. Fıkranın 2. Bendinde belirtilen, güvenlik sertifikalarının madde 4'e göre dağıtılmasının temel ilkelerini belirlemeye hizmet etmek üzere, kriterler ve usuller konusunda ekonomi ve iş bakanlığı ile anlaşılarak karar vermek.

BSI'nin kuruluş felsefelerinden birisi İnternet'in bilgi toplumunun bir sembolü olarak bilginin global ağ haline dönüşmüş olması ve bunun sonucu olarak da sadece kamu kurumlarında veya sadece ticari hayatta değil ülkede bulunan tüm sektörlerin vazgeçilmez bir parçası haline gelen İnternet ve BT uygulamaları için bilgi güvenliği konusunun bütüncül bir yaklaşım ile ele alınması gerektiğinin ortaya çıkmış olmasıdır. Artık e-ticaret giderek yaygınlaşmakta ve hatta bazı alanlarda klasik yöntemlerle yapılan alışverişlerin ötesinde bir işlem hacmine erişmiş bulunmakta ve bu trend giderek de e- ticaret lehine artacak gözükmektedir.

Aynı şekilde tüketicilerle ilgili uygulamalarda giderek elektronik ortama taşınmakta ve 2000–31 sayılı AB Direktifinde de belirtildiği gibi tüketicilerin e-ticaret yolu ile karşılaştıkları hukuksal anlaşmazlıklarında yine elektronik ortamda çözülmesi yönünde eğilimler belirmektedir.

Bu nedenlerle BSI artan elektronik ortam kullanımına paralel olarak bu ortamın duyduğu güvenlik ihtiyacının arttığını ve bu ihtiyacın nasıl karşılanacağı konusunda sürekli bir araştırma, uygulama ve çözüm bulma sorumluluğu ile oluşturulmuştur.

Bunun için BSI öncelikle BT teknolojileri uygulamalarının ne kadar güvenilir ve emniyetli olduklarının tespitine yönelik çalışmalar yapma ikinci olarak kullanıcıların ve uygulayıcıların hangi tehdit ve tehlikelerle karşı karşıya oldukları ve bu tehlikelerden nasıl korunacakları konusunda araştırma yapıp tavsiyede bulunma görevleri yanı sıra ani güvenlik boşluklarında potansiyel zararın minimuma indirilmesi için risk analizleri yaparak önlemler almak ve uzman müdahalesi reaksiyon planları yapmakla yükümlü hale getirmiştir.

Yine BSI acil durumlarda yine Alman İç İşleri Bakanlığına bağlı olarak görev yapmakta olan BT suçları ile mücadele merkezine yardımcı olma görevini de üzerine almıştır. Bunun yanı sıra BSI genel anlamda İnternet suçları ile mücadeleye katkı sağlama görevini de üstlenmiştir. Bunun için BSI geniş halk kitlelerine farkındalık yaratmaya yönelik BT teknolojileri üzerine işlenebilecek suçlar hakkında hassasiyet kazandırma çalışmaları da yapacaktır.

BSI'nin görevi bunlarla da sınırlı değildir. Ek olarak BT kullanılarak üretilen cihaz ve ekipmanları test etmek, testi geçen cihazlara onay vermek ve güvenlik sertifikaları dağıtmak, kripto sistemleri geliştirmek, enformasyon teknolojilerindeki gelişme ve eğilimleri takip etmek, e-imza ve sertifika merkezlerinin yapılandırılmasını sağlamak, BT teknolojileri ve güvenliği konusunda resmi kurumlara danışmanlık yapmak, isteğe bağlı olarak güvenlik açıklarını tespit etmek ve son olarak da üreticilere, işletmelere, tüketicilere danışmanlık yapmaktır.

Özetle BSI genel olarak bilgilendirme, planlama, koordinasyon, sertifikasyon yapan, yaptırımdan çok gönüllülük esasına göre çalışan danışman merkezi niteliğinde bilgi güvenliği ile ilgili önemli bir örnek kuruluş olarak önümüzde durmaktadır.[190]

H.Yıldırım, V. Kaplan, T. Çakmak, C. C. Üstün tarafından kısmen belirtildiği üzere ülkemizde de İçişleri Bakanlığı, Adalet Bakanlığı ve TÜBİTAK kurumları tarafından oluşturulacak ve buna TSE'nin de dâhil edilerek bir üst kurum veya yapı oluşturulması ve kuruluna bu kurulun ülkemizin ulusal alt yapı networklerini, İnternet', uydu, radyo ve televizyon gibi telekomünikasyon şebekelerinin yanı sıra elektrik, ulaşım, gaz, su gibi şebekelere ileri teknoloji kullanılarak yapılacak her türlü saldırıyı engellemek, bu yönde kamu kurumları ve diğer kurumlar için yol gösterici ve bağlayıcı kurallar oluşturmak ve bilgi güvenliği konusunda danışmanlık ve denetleme işlemlerini yerine getirmesi yerinde bir önlem olacaktır. Bu arada halen Telekomünikasyon Kurumuna bağlı birimler tarafından yerine getirilen iletişim araçlarının teknik dinleme ve izleme konuları da yine bu kurulacak birimle koordinasyon içersinde işbirliği ile yeniden yapılandırılması düşünülmelidir. [191]

4.3 ABD'de Bilgi Güvenliği Yasaları

ABD'de de değişik sektörleri ilgilendiren birçok yasal düzenleme göze çarpmaktadır. Bunlardan bazıları şunlardır; Sarbane-Oxley Act: 2002 Enron olayından sonra ABD'de ivedilikle 30 Temmuz 2002 tarihinde çıkarılmış bir yasadır. Yasa ismini katkılarından dolayı Senator Paul Sarbanes ve Temsiler Meclisi Üyesi Michael G. Oxley isimlerinden almıştır. Bu yasanın amacı borsaya açık şirketlerin açıkladıkları bilgilerin doğruluğu ve güvenilirliğini sağlayarak yatırımcıları korumaktır. Bu kanuna göre şirket yöneticileri ve yönetim kurulu üyeleri finansal raporlar hazırlanırken, yeterli iç denetimleri ve prosedürleri oluşturduklarını ve uyguladıklarını belgelendirmeleri gerekmektedir. Bu konulara uymayan şirket yöneticilerine yasa, hapis cezası öngörmektedir[192].

---

[190] Bu kısımın oluşturulması sırasında temel kaynak H.Yıldırım, V. Kaplan, T. Çakmak, C. C. Üstün tarafından yazılan e-Devlet Başa isimli kitabın 2. Baskı , Ankara 2006 , s.110-111'dan yararlanılmıştır.
[191] H.Yıldırım, V. Kaplan, T. Çakmak, C. C. Üstün ; "e-Devlet Başa" , s.108-109
[192] http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf (15.04.2007)

Finansal kuruluşların müşteri bilgilerinin güvenliği, bütünlüğü ve kişiye özel olmasını korunmak için düzenlemiş bir başka Yasa da Gramm-Leach-Bliley Act (GLBA)'dır**.** Bu Yasa Finansal kuruluşların yüksek güvenlik bilincinin diğer endüstri kuruluşlarından daha fazla olması tarihten beri bilinmektedir. GLBA, bankalar, sigorta şirketleri, güvenlik firmaları, mali müşavirleri ve kredi kartı şirketlerini ilgilendirmektedir. GLBA 'e göre bu şirketler Temmuz 2002 den önce bu kanuna uyumluluklarını tamamlamak ve yürütmeden sorumlu tarafça denetlenip uyumluluklarını belgelendirmek zorundadırlar. GLBA'e göre finans kuruluşları, yönetici ve yönetim kurulunun da dahil bulunduğu risk temelli bilgi güvenliği programı geliştirmeli, tehditlerin risk değerlendirmesi yapılmalı, risk yönetimi ve kontrolleri yöneterek gerekli önlemleri almalı ve yönetim kuruluna rapor etmelidir[193].

Sağlık alanındaki bilgi güvenliği ile ilgili Yasa ise **Health Insurance Portability and Accountability (HIPAA)'dir.** HIPAA sağlık hizmeti sağlayan kuruluşların uyması gereken kuralları açıklar. Bu kurallar sağlık hizmeti veren kuruluşların kanunun istediği raporları oluşturan bilgilerin sağlanması ve bu bilgilerin korunmasını zorunlu kılmaktadır. HIPAA uyumluluğunu sağlamak için şirketler bilgilerini muhtemel tehditlere karşı korumak, bütünlüğünü sağlamak, yetkisiz kullanılmalarını, ortaya çıkmalarını önlemek zorundadırlar. Bunun yanında kurum çalışanlarının yetkin ve güvenli olduklarının sağlanması gereklidir. Sağlık hizmeti veren kuruluşlar bütün bunları gerçekleştirebilmek için; erişim kontrolü, konfigürasyon kontrolü, zararlı yazılım tespiti, politika yaptırımı, kullanıcı takibi ve yönetimi, çevre ve haberleşme güvenliği sağlamakla yükümlüdürler[194].

4.4 Türkiye'de Bilgi Güvenliği Mevzuatı

Türkiye'de değişik bazı Kanunlarda bilgi güvenliğini ilgilendiren kimi yasal düzenlemeler mevcuttur. Örneğin TCK'da bulunan madde 243, 244, 245'de yer alan bilişim suçları, kişisel verilerin hukuka aykırı kullanılmasını düzenleyen TCK 135. ve devamı maddeler gibi.

Ancak kamu ve özel kurum ve kuruluşları bilgi güvenliği konusunda bağlayan veya onlara yol gösteren veya yol gösterme veya standartları belirlemeyi belli bir kuruma veya kuruluşa bir görev olarak veren bir yasal düzenleme bulunmamaktadır. Bu noktadan hareketle DPT'nin hazırlatmış olduğu ve 2010 yılını hedefleyen Stratejik Planiçersinde bu konuya özel önem verilmiş ve 87 nolu strateji programı olarak eylem planına konulmuştur. Strateji Planının Program Tanımlama Dokümanının 87 nolu

[193] http://banking.senate.gov/conf/ (15.04.2007)
[194] http://www.legalarchiver.org/hipaa.htm (15.04.2007)

Eylemi "Bilgi Güvenliği İle İlgili Yasal Düzenlemelerin Yapılması"dır[195]. Bu görev Adalet Bakanlığına verilmiş ve Milli Savunma Bakanlığı, İç İşleri bakanlığı, DPT, TÜBİTAK ve ilgili diğer kurum ve kuruluşlar Proje ile ilişkilendirilmiştir. Dokümana göre Projenin bitiş takvimi Ocak 2007 olarak öngörülmüş olup henüz kamuoyuna Adalet Bakanlığının hazırlamış olduğu Bilgi Güvenliği Yasa Taslağı hakkında bir bilgi paylaşılmamıştır.

Ancak bu konuda Milli Savunma Bakanlığı tarafından mazisi eskiye dayanan bir yasa çalışması bulunduğu bilinmektedir. 2000'li yılların başında hazırlanan, ancak kamuoyunun tepkisiyle geri çekilen Tasarı 2007 ortalarına doğru yeniden dizayn edilerek kurumların görüşüne sunuldu[196]

Tasarının incelenmesinden hemen göze çarpan konulardan bazıları şu şekildedir; Öncelikle Tasarıda "Ulusal bilgi güvenliğini sağlamaya ilişkin bilginin" tanımı belirli ve net değildir. Bu belirsiz tanım nedeniyle, kamu ve özel kurumlarda her türlü bilgiye Tasarı kapsamında "Ulusal Bilgi Güvenliği Teşkilatı" tarafından erişme hakkı tanınmış olur ki bilgi güvenliğinden beklenen bu olmasa gerektir.

Yine Tasarıda "Anahtarlama materyalinin üretim esaslarını" hangi durumlar ve koşullar altında belirlenmesinin geçerli olduğu açık değildir. Burada "kişilerin gizli anahtarlarının" kişisel verilerin gizliliği gereği Yasa kapsamı dışında olduğu açıkça belirtilmelidir.

Tasarıda "Ulusal Bilgi Güvenliği Teşkilatının" işlevleri ve ilgi alanı net değildir. Bu teşkilatın asıl amacının ne olduğu ve hangi çerçeveler içinde kalacağı net olarak belirtilmelidir.

Bu bağlamda yine "ulusal bilgi güvenliği", "ulusal güvenliği ilgilendiren bilgi" tanımları belirsizlikten kurtarılmalıdır.

Yasa haksız rekabet ve tekelci uygulamalara yol açabilecek, teknolojik açık rekabet ortamını zedeleyecek bir yapılanmadan arındırılmalıdır. Ticari politikalar, kişisel ve ticari gizlilik hakları tümüyle ulusal politikalar düzeyinde ele alınabilecek konulardır. Bu bağlamda kararlar "siyasi otoriteye" bırakılmalıdırlar. Kurumsal yapı, ancak talep olduğunda danışmanlık veren bir kurum statüsünde olmalıdır. Yasanın bu konudaki ilgili maddeleri değiştirilmelidir.

Bilgi güvenliğinin sivil uygulamaları dünyada henüz çok yenidir. Ülkemizde de bilgi teknolojilerinin gelişmişlik düzeyi üretim, tüketim ve içerik açısından gelişmiş ülkelerin çok altındadır ve henüz gelişmektedir. Bu bir yana, bu düzenlemeleri yukarıda

[195] http://www.bilgitoplumu.gov.tr/btstrateji/Program%20Tanımlama%20Dokumani_Temmuz%202006%20Nihai.pdf (15.04.2007)

[196] **Uyanıker, Levent;** "**Ulusal Bilgi Güvenliği Tasarısı yeniden gündemde**"; http://www.btnet.com.tr/haber.phtml?kategori_id=7&yazi_id=590000272 (23.01.07)

da ifade edilmeye çalışıldığı gibi kapsamı ve işlevleri tam olarak belirlenmemiş bir kurum aracılığı ile yapmaya çalışmak, ekonomik ve toplumsal yaşamımızı önemli ölçüde kısıtlar altına sokacaktır.

Tasarının 29'uncu maddesi birinci fıkrasında, "kamu kurum, kurul ve kuruluşları ile özel kuruluşlar, ulusal güvenliği ilgilendiren ulusal bilginin korunması için kendi idari yapıları içerisinde gereken organizasyonu kurmak veya değişiklikleri yapmak ve gerekli tedbirleri almaktan sorumludur" ifadesi kullanılmaktadır. "Ulusal bilgi, ya da "gizlilik gerektiren ulusal bilginin" ne olduğu ise net olarak tanımlanmamış bulunmaktadır. Tasarının 34'üncü maddesinde, 29'uncu maddedeki yükümlülükleri yerine getirmeyenler hakkında 4 milyar TL'lik ceza kesileceği belirtilmektedir. 2002 yılındaki Tasarıda ise cezai hüküm olarak 1 yıldan 5 yıla kadar hapis öngörülmüştü. Bu hüküm kanunsuz suç ve ceza olmaz hükmünü ihlal etmektedir [197]. Suç olarak tanımlanan eylemin sınırları net çizilmeli ki Tasarının bu maddesi net ve sınırları kesin değildir. İdareye ceza koyma sonucunu doğurabilecek yanlış yorumlara neden olabilecek gözükmektedir.

Ulusal Bilgi Güvenliği Yasa Tasarısı sonuç olarak biraz daha üzerinde çalışılmaya ve bilgi ve belge isteyen bir Yasa'dan daha çok veya var olan verilerin içeriklerinden çok, onların bulundukları ortamlarının güvenliğine odaklanmış bir Tasarı haline getirilmedir. Yine özellikle bilgi güvenliği konusunda standartları uygulayan, sertifika dağıtan TSE ve bilgi güvenliği konusunda teknik alt yapısı olan ve bu konuda değişik alanlarda faaliyetlerde bulunan TÜBİTAK gibi kuruluşların bu Tasarıda daha çok öne çıkarılması yerinde olacaktır kanaatindeyiz.

Türkiyede'de bilgi güvenliği ile ilgili olmak üzere finans sektörü açısından yasa boyutunda olmasa da yönetmelik seviyesinde üzerinde durulması gereken bir düzenleme yapılmıştır. Bu çalışmadan kısaca da olsa burada bahsetmek yerinde olacaktır. Bu Yönetmelik "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" olup** 16 Mayıs 2006 tarih ve 26170 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir[198]. Yönetmeliğin amacı 1. Maddede; "Bu Yönetmeliğin amacı, bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesiyle ilgili usul ve esasları düzenlemektir şeklinde tarif edilmiştir." Yönetmeliğin 3. Maddesine göre bu Yönetmelik, 19.10.2005 tarihli ve 5411

[197] **Uyanıker, Levent;** "**Ulusal Bilgi Güvenliği Tasarısı yeniden gündemde**"; http://www.btnet.com.tr/haber.phtml?kategori_id=7&yazi_id=590000272 (23.01.07)
[198] http://www.bddk.org.tr/turkce/anasayfa/ (15.04.2007)

sayılı Bankacılık Kanununun 15 inci maddesi[199] ve 93 üncü maddesinin dördüncü fıkrası hükümlerine[200] dayanılarak hazırlanmıştır.

4.4.1 Uluslararası Bilgi Güvenliği Standartları ve Yasal Mevzuata Etkileri

100 milyondan fazla İnternet'sayfasının olduğu günümüzde, kişiler, resmi ve özel kurumlar işlerini artık çok büyük oranda bilgisayarlar ve ağlar üzerinde gerçekleştirmektedir. İnternet kullanımının en yüksek olduğu bu zamanda verilerin resmi ya da gayri resmi olarak başkaları tarafından kullanılması, çoğatılması veya üstünde değişiklik yapılması söz konusudur. Kişiler ve kurumların sahip oldukları veriler elektronik ortamda izinsiz olarak elde edilmesi ve değiştirilmesi konusunda giderek daha riskli bir duruma gelinmektedir.

İnternet ve bilgisayarın yaygın olmadığı dönemlerde yapılan bir çok hizmet (pasaport başvuruları, bankacılık, alış-veriş v.b.), İnternet ortamında sunulmaya başlanmıştır. Bu tür hizmetler, işlerin hızlı ve rahat yapılmasını sağlamakta, iş süreci bakımından zaman kazandırmakta, iş takibini kolaylaştırmakta ve gereksiz yazışmaları ortadan kaldırmaktadır.

Bilgisayar korsanları elektronik saldırılarda bulunarak kişilerin ve kurumların gizli ve özel verilerini ele geçirerek çok büyük zararlar verebilmektedir.

İşte bu tehlikelerden sakınabilmek ve bilgi güvenliğini sağlayarak elektronik ortamı daha kullanılır bir hale getirmek için güvenliğin farkında olan BT sektörü daha işin başından bu yana sürekli uluslararası düzeyde bilişim teknolojileri alanında özellikle güvenlikle ilgili olarak belgelendirme ve standartlaşma çalışmalarını yürütülegelmiştir. İşte bu belgelendirme ve standartlaşma çalışmaları genel olarak ISO/IEC 17799, ISO/IEC 15408–1, ISO/IEC 15408–2 ve ISO/IEC 15408–3 standartları göz önüne alınarak yapılmaktadır.

Bu standartların tümü TSE (Türk Standartları Enstitüsü) tarafından Türk Standardı olarak kabul edilmiş ve yayınlanmıştır.

İngiliz Standartlar Enstitüsü (BSI, British Standards Instute) ve İngiltere'deki bazı kuruluşların talepleri doğrutusunda 1990'lı yılların ortasında, Bilgi Güvenliği Standartları BS 7799 altında ortaya çıkmıştır. İlk 1995 yılında BS 7799 olarak

---

[199] 5411 S.K. MADDE 15 - Bankaların bağımsız denetim, değerleme, derecelendirme ve destek hizmeti faaliyetlerini gerçekleştirecek olan kuruluşların yetkilendirilmesine, yetkilerinin geçici veya sürekli olarak kaldırılmasına Kurulca karar verilir. Buna ilişkin usûl ve esaslar ilgili meslek birliklerinin görüşü alınarak Kurulca belirlenir.

[200] 5411 S.K. MADDE 93 Fıkra 4; (Değişik cümle: 08.03.2006–5472 S.K./1.mad) Kurum, bu Kanun ve ilgili diğer mevzuat hükümleri çerçevesinde kendisine verilen yetkilerini, Kurulca tesis edilecek düzenleyici işlemler veya alınacak özel nitelikli kararlar ile kullanır. Kurum, Kurul kararıyla bu Kanunun uygulanmasına ilişkin yönetmelikler ve tebliğler çıkarmaya yetkilidir. (Fıkranın Değişmeden önceki Hali; "Kurum, bu Kanun ve ilgili diğer mevzuat hükümleri çerçevesinde kendisine verilen yetkilerini, düzenleyici işlemler tesis ederek veya özel nitelikli kararlar alarak kullanır. Kurum, Kurul kararıyla bu Kanunun uygulanmasına ilişkin yönetmelikler ve tebliğler çıkarmaya yetkilidir.")

yayınlanan standart, BS 7799–2,1998 ve BS 7799–1:199 iki kısıma ayrılarak yayınlanmıştır.

Daha sonra Kurumsal bilgi güvenliği olarak bilinen ve kabul edilen en iyi yöntemlerin sıralandığı Uluslararası Standartlar Komitesi (ISO, International Organization for Standardization) standartları Aralık 2000'de Bilgi Güvenliği ile standardın birinci bölümü ISO 17799 olarak yayınlanmıştır. Bu BS 7799-1'in aynısıdır. ISO 17799 revize edilerek 2005 sonlarında ISO 17799:2005 adını almıştır. Ayrıca ISO tarafından Bilgi Teknolojileri Güvenlik Standartları ile ilgili çalışmalar JTC 1 (Joint Technical Committee) Bilişim Teknolojileri Komitesine bağlı SC 27: IT Güvenlik Teknikleri alt komisyonunda ele alınmaktadır. Bu komisyon üç ayrı alt çalışma grubuna ayrılarak, her biri farklı standartlar hazırlamaktadır (Güvenlik Yönetimi, Kriptografi Teknikleri, Ürünleri ve Sistemleri için Güvenlik Değerlendirme).

Türk Standartları Enstitüsü (TSE) tarafından TS ISO/IEC 17799 Kasım 2002'de yayınlanmıştır. Tekkiklerde kullanılan BS 7799–2 "Bilgi Güvenliği Yönetim Sistemleri Özellikler ve Kullanım Kılavuzu" Şubat 2005'de yayınlanmıştır.

15 Ekim 2005 tarihinde ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi (Information security management systems) standardı uluslararası bir standart olarak yayınlandı. Bilgi Güvenliği Yönetim Sistemi konusunda yayınlanmış olan bu standart yayım tarihinden itibaren, BS 7799–2,2002'nin yerini almıştır. Türk Standartları Enstitüsü de 2 Mart 2006 tarihinde söz konusu standardı Türkçeleştirerek TS ISO/IEC 27001 "Bilgi teknolojisi – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler" standardı olarak yayımlayarak yürürlüğü koydu.

ISO/IEC 27001 standardında "Elektronik Ticaret Güvenliği, Elektronik Posta Güvenliği, Mesaj Kimliğinin Doğrulanması, Şifreleme, Sayısal İmzalar, İnkâr Edememe Servisleri ve Verinin Korunması ve Kişisel Bilgilerin Gizliliği" maddelerinde kişisel verilerin korunmasıyla ilgili tedbirlerden söz edilmiştir.

Çeşitli ulusal güvenlik ve standart organizasyonları tarafından, kendi güvenlik kıstaslarını ortak bir standartla değiştirebilmek için CC (Common Criteria) hazırlanmıştır. Bu ISO'nun da kabul ettiği (ISO/IEC 15408 1-2-3 Ağustos 1999) uluslararası bilgi güvenliği garanti düzeyi belirleme ölçütleridir.

Güvenlik gereksinimi, ülkelerin kabul ettiği güvenlik ölçütlere uygun olarak testler yapan laboratuarların kurulmasını sağlamıştır. Bu test laboratuarları önceleri her ülkede o ülkenin kabul ettiği güvenlik ölçütlerini kullanarak testler yapmaktaydılar. Amerika'da Savunma Bakanlığının hazırladığı TCSEC'yi (Trusted Computer Security Evaluation Criteria) kullanılırken, Avrupa ülkeleri TCSEC'i temel alarak ITSEC'i (Information Technology Security Evaluation Criteria) kullanmaya başladılar. Bu iki

standart devletlerin kullanacakları IT (Information Technology – Bilgi Teknolojisi) ürünler için yeterli görülmekteydi. Ancak, IT ürünlerin alım-satımında artış olduğundan ortak ölçütlere ihtiyaç duyuldu. Bu sebeplerden ülkeler ortak bir standart geliştirmek için çalışmaya başladılar. CC (Common Criterion) bu çalışmalar sonucunda geliştirildi.

CC'nin temelini, Amerika'nın geliştirdiği TCSEC, Avrupa'nın geliştirdiği ITSEC ve Kanada'nın geliştirdiği CTCPEC oluşturmaktadır. Ocak-1996 yılında CC Yayın Kurulunun çalışmaları sona erdi ve CC standardının ilk sürümü çıkarttıldı. CC'nin oluşumunda ABD (NIST – National Security Agency, NIST – National Institute of Standards and Technology), İngiltere (CESG – Communications – Electronics Security Group), Almanya (BSI – Bundesamt für Sicherheit in der Informationstechnik), Fransa (DCSSI – Direction Centrale de la Securite des Systemes d'Information) ve Kanada'nın (CSE – Communications Security Establishment) yanı sıra Avustralya (DSD – Defence Signals Directorate) ve Yeni Zellanda da bulunmuştur. 1998 yılının Mayısında CC Uygulama Kurulu CC'nin 2.0 sürümünü hazırladı ve piyasaya çıktı. Bu sürüm 1999 yılında Uluslararası Standartlar Organizasyonu tarafından ISO 15408 referans numarasıyla kabul edildi. 1999 yılının Ağustosunda CC Açıklama Yönetim Kurulunun yaptığı eklemelerin ardından sürüm 2,1 çıkartıldı. Şu anda hala geliştirilmektedir. CC, ISO'nun da kabul ettiği uluslararası bilgi güvenliği garanti düzeyi belirleme ölçütleridir.

CCRA'yı (Common Criteria Recognition Arrangement) imzalamış ülkeler "Sertifika Üreticileri" ve "Sertifika Müşterileri" olarak ikiye ayrılır.

Sertifika Üreticileri, ABD, Kanada, Fransa, Almanya, İngiltere, Avustralya, Yeni Zelanda (Mayıs – 2000) ve Japonya (Eylül - 2004).

Sertifika Müşterileri, Finlandiya, Yunanistan, İtalya, Hollanda, Norveç, İspanya, Avusturya (Mayıs – 2000), İsrail (Temmuz – 2001), İsveç, Macaristan, Hindistan, Singapur (Mayıs - 2002), Türkiye (Ağustos - 2003) ve Çek Cumhuriyeti (Eyül - 2004).

Kısaca CC, belli başlıca güvenlik denetimi, şifreleme desteği, kullanıcı verilerinin korunması, tanıma ve kimlik doğrulama ve gizlilik gibi konuları içermektedir.

Bu standartların yanı sıra "Elektronik sertifikanın veri yapısını (ITU X.509)", "Kimlik, kredi kartları ve akıllı kartların özelliklerini (ISO/IEC 7816) ", "Sertifika ilkeleri ve sertifika uygulama esasları dokümanlarının nasıl yazılacağını (RFC 3647)" ve "Elektronik imzalı ve/veya şifreli e-posta mesajlarının yapısını (RFC 3851)" tarif eden birçok standart vardır. Ayrıca, ISO/IEC 15504 (SPICE) gibi standartlarda tasarı aşamasındadır.

Bilgi güvenliğini ilgilendiren doğrudan ya da dolaylı olarak daha birçok standart vardır. Yapılan bu standartlar, denetim çalışmasının nasıl olması ve karşılaşılan

durumlarda nasıl davranılması gerektiği konularında denetçiye yol gösterici olup, denetim uygulamalarında birlik sağlamaktadır. Bunun yanında, bağımsız denetimin kamu çıkarını koruyup kollama işlevi göz önünde tutulursa, standartlar denetim çalışmalarında kaliteyi sağlayarak veya mevcut kaliteyi artırarak denetimin sonucuna olan güveni artıracaktır.

4.4.1.1 Standartların Yasal Mevzuata Etkisi

Bilgi güvenliği konusunda mevzuat hazırlayan ülkeler genelde mevcut bir standartı yasalarına esas olarak almamakta, yasalarda daha çok bilgi güvenliği ile ilgili temel kuralları, kurumları ve ilkeleri belirlemektedirler. Standartaların seçimi, oluşturulması ve uygulamasını denetlenmesi bu kurum kuruluşlar tarafından yapılmaktadır. Almanya'da BSI'nin görevi budur. BSI'yi kuran yasal mevzuat sadece genel ilke, yetki ve görevleri belirlemekte, ortaya ayrıntılı kurallar koymamaktadır.

Bu konuda dünya ülkelerinde yapılan çalışmalar incelendiğinde her ülke kendi yapısına uygun olarak belli başlı organizasyonlar tarafından kabul görmüş standartları yasalarına dahil etmişler ve uygulayıcılara yol göstermekle beraber uygulamalarda standartlık sağlamışlardır. Yasalara en çok dahil edilen standartlara göz attığımızda Avrupa Birliğine üye ülkelerde International Standardization Organization (ISO) standartları yaygın olarak karşımıza çıkmaktadır. Özellikle ISO 27001 Information Security Management System Standardı Ingiltere nin başını çektiği ülkeler tarafından bilgi güvenliği yasalarında referans edilen standart halini almıştır. ISO standartlarının yanında Comite Europeen de Normalisation (CEN) Workshop Agreement (CWA) standartları, European Telecommunications Standards Institute (ETSI) standartları, İnternet Enginering Task Force (IETF) standartları da Avrupa Birliği ülkelerinin yasalarında yer almıştır.

4.4.1.2 Türkiye'de Durum

Ulusal Güvenliği ilgilendiren bilginin örgütlenmesi açısından, "gizlilik dereceli" bilginin ne olduğu, nasıl üretileceği, korunacağı, nakledileceği, kullanılacağı ve imha edileceği konusunda T.C. Devleti'nin yasal hazırlığı ve düzenlemesi henüz bulunmamaktadır. Bu yasal düzenlemeler ise geçici olarak kurulup sonra dağıtılan birtakım platformların üstesinden gelebileceği gibi basit bir yasa ya da mevzuat çalışmasına değil, çok karmaşık bir yasalar zincirlerine ve gelişen teknoloji nedeni ile sürekli güncellenmek ve teknolojiye uygun hale getirilme ihtiyacı mevcuttur.

Ülkemizin henüz Ulusal bir bilgi güvenliği politikasının olmayışı ülkenin ulusal güvenliğini hassas hale getirmektedir. Bakanlıklar, kamu kurum ve kuruluşları arasında ulusal güvenlik ihtiyaçları doğrultusunda bilgi güvenliğini koordine edecek, yönlendirecek ve ulusal bilgi güvenlik sistemini işletecek bir yapı bulunmamaktadır.

Bu nedenle de ulusal bilgi güvenliği gibi karmaşık ve konunun nasıl çözülebileceği hususunu müzakere etmek için ortak anlayışı kolaylaştıracak, üzerinde mutabakata varılmış tanımlar mevcut değildir.

Hassas bilgi altyapısına bağımlılık ve bu altyapıya tehdit ve riskler, kurum ve kuruluşlarca iyi henüz tam olarak analiz edilip gerekli tedbirler alınamamıştır. Kripto grafik ürünlerin ithalatı ve ihracatı ile ilgili kontrol esasları net olarak belirlenmemiş olup kontrol mekanizması tam olarak tesis edilememiştir.

4.4.1.3 Kamu Otoritesi

Kişisel özgürlüklerin ve verilerin dokunulmazlığının zedelenmemesi prensibinin neredeyse anane haline geldiği ABD'de, devlet, yurttaşlarının haberleşmenin mahremiyeti konusunda hakları ile terörizm, kaçakçılık ve devlete karşı islenen diğer suçların önlenmesi konusunda son dönemlerde terör tehdidi nedeniyle kabul edilen yasalar akımından bazı eleştiriler olsa da dengeleri en azından mevzuat açısından kurmuş gözükmektedir. ABD'de 1952 yılında kurulan "Ulusal Güvenlik Teşkilatı (National Security Agency) bu dengenin içinde kendine özgü bir yere sahiptir. NSA, ABD çıkarları doğrultusunda bir yanda uluslararası elektronik istihbarat yapmak ve öte yanda Amerikan devletinin bilgi güvenliğini sağlamaktan sorumludur.

NSA, uzman teknik fonksiyonları sağlamaktan sorumlu kılınan Savunma Bakanı'nın yetki, kontrol ve yönlendirmesinde ve Savunma Bakanlığı bünyesinde bağımsız bir teşkilat olarak kurulmuştur. NSA'nın günümüzde aldığı biçim hakkında şu noktalar önemlidir: NSA, tam olarak bir "elektronik istihbarat" örgütüdür. Hatta bu öyledir ki; NSA "ABD Istihbarat Topluluğu (US Intelligence Community)" içinde, CIA, FBI, "Ordu İstihbarat (Army Intelligence)" ve Savunma Bakanlığı gibi toplam 13 federal kurumdan birisidir ve bu kuruluşundan beri değişmemiştir. Ayrıca, 1972 yılında kurulan "Merkezi Güvenlik Birimiyle (Central Security Service) NSA ve ordu istihbarat birimleri arasında tam bir işbirliği sağlanarak Savunma Bakanlığının kripto grafik çalışmaları tek bir bünyede verilmeye başlanmıştır.

Ancak özellikle vurgulanmalıdır ki NSA diğer uluslar ve onların vatandaşları için istihbarat ve karsı istihbarat toplamak yetkisi ile sınırlıdır. Amerika'da oturma izni olan yabancılar, Amerikan vatandaşları ve Amerikan özel sektör kurumlarının gizlilik haklarına aykırı yasadışı istihbarat yürütmesi Anayasa ve NSA'in kuruluş yasasıyla kesinlikle yasaklanmıştır. Bunun ötesinde, gizlilik ve haberleşme özgürlüğü yasalarıyla kişiler kendileri hakkında NSA gizlilik Yasasında tanımlanan "kimlik bilgilerine" erisme hakkına sahiptirler. Haberleşme özgürlüğü kapsamına giren "hükümet kayıtlarının" NSA tarafından tutulması yasayla engellenmiştir.

NSA "ithalat ve ihracat politikalarının" belirlenmesinde görevli değildir ve kendi dışında oluşan politikalara tabiidir. ABD'de bu politikalar "Başkanlık" düzeyinde saptanır.

NSA'in ABD'deki "kriptografi üretimini" kontrol altında tutmak, söz konusu ürünleri sertifikalandırmak türünden hiçbir işlevi ve görevi yoktur. Hatta özel üreticiler kamuya ürünlerini satarlarken dahi, NSA'in onayını almak zorunda değildirler. Tam aksine, NSA, gelişmiş yeteneklerinden ABD özel sektörünün de yararlanmasını sağlamak amacıyla, özel sektörün isteğine bağlı olarak danışmanlık vermektedir.

Kamuda bilgi güvenliği standartlarının belirlenmesi ve uygulanması da NSA'in görevleri arasında değildir. ABD'de bu islevi, Amerika Standartlar Enstitüsü (National Institute of Standarts and Technology) "Federal Bilgi İşleme Standartları (Federal Information Processing Standarts)" yayınlarıyla yerine getirmektedir. Bu bağlamda standardın çeşitli bentlerinde ve farklı biçimlerde tekrar edilen "usuller ve yöntemler belirlemek, altyapıları korumak" fiilleriyle ifade edilen ve temelde kamuda bilgi güvenliği standartlarının altyapılar, ürünler ve uygulamalar açısından saptanmasına dönük olduğu anlaşılan işlevler bu kapsama girmektedir.

1993 yılı Nisan ayında Clinton yönetimi NSA tarafından hazırlanan/önerilen yeni bir kriptoloji politikasını ortaya koymuştur. Başkan Bush zamanından başlayarak yürütülen bu çalışmaların odak noktası hükümet tarafından geliştirilen Clipper adlı bir kripto çipidir. Özel sektör tarafından üretilen her türlü güvenli iletişim ürünlerine yerleştirilmesi önerilen bu çipe karşı çok büyük bir tepki oluşmuştur. Bu tepkilerin kaynağında, her çip için özel olarak üretilen anahtarların bir kopyasının hükümet tarafından tutulması ve tamamen yasal olmayan hiçbir nedene dayanarak bu çipler üzerinden geçen trafiğin dinlenmeyeceğinin hükümet tarafından garanti edilmesine rağmen, yeterli güvenin oluşturulamaması bulunmaktadır. Ayrıca, hükümet tarafından geliştirilen anahtar algoritmasının açıklanmaması sonucunda algoritmanın denenmesinin ve güvenilirliğinin kanıtlanamayacak olması, bunun sonucunda tüketicilerin bu ürünlere rağbet etmeyeceğinin ortaya çıkması, gittikçe önem kazanan kriptoloji sanayinde dünya pazarlarında rekabet şansının kapalı bir algoritma kullanılarak üretilen ürünlere dayanarak korunamayacağı gibi endişeler ortaya çıkmış ve bu çip istenen kullanım yaygınlığına ulaşamamıştır.

Öte yandan "yaşamsal altyapıların korunması" (critical infrastructure protection) yeni bir kavram olarak dünya ülkelerinin gündemine girmiştir. Yaşamsal altyapıların korunması kavramı, ekonominin ve devletin minimum düzeyde isleyişi için gerekli fiziksel ve ağsal sistemleri kapsamaktadır. Amaç, ülkenin düşmanlarının, bunlar ister

baksa ülkeler, ister ülke içindeki gruplar ve bireysel olsun, "geleneksel olmayan" yöntemlerle yapacakları saldırıların engellenmesidir.

Açıktır ki, bu tehditler, devletin elektronikleşmesi ve açık ağları kullanmasının yaygınlığıyla doğru orantılıdır. Yaşamsal altyapıların korunması için ABD Başkanı Bill Clinton, 1998 yılında bir Beyaz Belge direktifleri yayınlamıştır. Bu belgede dikkat çeken unsurlar şunlardır:

Devlet içinde öncü kurumlar tespit edilmiştir. Her öncü kurum çeşitli sektörleri paylaşmışlardır. Örneğin, Ticaret Bakanlığı iletişim ve enformasyon sektörüne; Hazine Bakanlığı bankacılık ve finans sektörüne, FBI polis, acil durum ve adalet konularına; CIA dış istihbarata; Dışişleri Bakanlığı dışişleri sektörüne; Savunma Bakanlığı savunma sektörüne liderlik edecek kurumlar olarak belirlenmişlerdir. Ayrıcı, Bilim ve Teknoloji Politika Genel Müdürlüğü, Ulusal Bilim ve Teknoloji Konseyi'nin programları aracılığıyla araştırma ve geliştirme çalışmalarını eşgüdümleşmekle görevlendirilmiştir. Öncü kurumların seçilmesinin nedeni, bu konuda, özel sektör/kamu sektörü işbirliğini gerektirmesi ve gereksiz hükümet düzenlemeleri yaratmaktan kaçınılmasıdır.

Ulusal Eşgüdümcü: Güvenlik, Altyapı Koruma ve Karsı−terörizm Ulusal Koordinatörü bu direktifin eşgüdümünden sorumludur. Uyarma ve Bilgi Merkezleri: Başkan, bu görevle FBI'yı sorumlu kılmıştır.

National Infrastructure Protection Center (NIIPC): Bu heyet, FBI, bilgisayar suç uzmanları, Savunma Bakanlığı, İstihbarat topluluğu ve önder kurumların temsilcilerinden oluşur.

ABD'de kriptografik teçhizat Wassenauer ilkeleri gereğinde "mühimmat" gibi görmektedir. "Mühimmat kavramı" askeri bir terim olarak, kriptografik ürünlerin, 1998 Wassenaar düzenlemesinde, "askeri ve ticari olmak üzere çift kullanımlı" teknolojilerden sayılmaya başlanmasıyla ilgilidir. Bunun anlamı, bu düzenlemeye imza koyan ülkelerin, kriptografi ürünlerinin ithalat ve ihracında "uyumlu" politikalar izleme niyetinde olduklarıdır. Ancak Wassenaar bir anlamsa değildir ve yaptırımı yoktur. Nitekim İsviçre hükümeti 1998 düzenlemesinin "liberal politikalarında" bir değişikliğe neden olmayacağını ve İsviçre firmalarının dünya pazarından en yüksek payı almaları konusundaki desteğinin devam edeceğini açıklamıştır. Wassenaar üyesi İrlanda ise, en başından beri ABD ve İngiltere'nin aksi yönünde politikalar izlemiştir. İrlanda'nın bir firması olan "Baltimore Inc." bugün dünyanın en önde gelen bilgi güvenliği firmalarından birisidir.

ABD, 1998 Wassenaar düzenlemesinin aksi yönünde, ihraç politikalarını 2000 yılıyla beraber değiştirmiştir. Wassenaar 1998 açık bir biçimde İnternet tarayıcılarında 56 bit anahtar uzunluğunda kriptoya izin verirken, ABD bu yılın basından itibaren 128

bit anahtar uzunlugunu ihraç etmeye başlamıştır. ABD kökenli İnternet'sunucuları da paralel bir biçimde 128 bit SSL destekler bir biçimde ihraç edilmeye başlanmıştır. Ülkemizde bazı bankaların İnternet sayfalarında bu konunun uygulaması görülmektedir.

Bu değişimde, "ticari çıkarların" ağır bastığı vurgulanmaktadır. Değişiklik, tümüyle liberal bir politika değilse de, geçmiş uygulamalara göre liberalleşme anlamına gelmektedir NSA dışında gelişmiş ülkelerden anılan iki diğer örnek kurum İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters) ve Almanya'daki Enformasyon Teknolojileri Güvenlik Kurumudur (Bundesamt für Sicherheit in der Informationstechnik). İngiltere'deki Kamu Haberleşmesi Koordinasyonu (Government Communications Headquarters), NSA'ya çok yakın işlevler yürütmektedir. GCHQ'nun da oluşumu Soğuk Savaş dönemine dayandırılmaktadır.

Enformasyon Teknolojileri Güvenlik Kurumu (BSI) ise NSA ve GCHQ örneklerinden farklı olarak, istihbarat işlevi olmayan bir kurumdur. BSI bir Alman kamu kurumu olarak, 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 verebilmektedir.

Alman Hükümeti de söz konusu teknolojiyi yasaklamak üzere girişimlerde bulunmaya başlamıştır. 4 Mayıs 1995 tarihinde Alman Parlamentosu "Telekomünikasyon İzleme Kanunu" adı altında ülkede tasarlanan ve kullanılan telefon, GSM, ISDN ve bilgisayar şebekesi tarayıcılarının, devlet birimleri tarafından gerektiğinde dinlenmesini sağlamak için standart bir ara bağlantı sağlamaları konusunda bir kanun teklifini onaylamıştır. Kanunun özünü, güçlü delillere dayanarak bağımsız bir yargıç kararı olmadan özel haberleşmenin dinlenememesi oluşturmaktadır. Yargıcın gerekli gördüğü durumlarda, bu kanuna göre çağrı oluşturma bilgilerine ve GSM kullanıcılarının hücreler arasında izlenmesini sağlayacak bilgilere erişilmesi mümkün hale gelmektedir. Almanya, bu düzenlemesiyle, Avrupa ülkeleri arasında bireyi devlete karsı üst düzeyde güvenceye alan bir ülkelerin öncülüğünü yapmaktadır.

Bir ilginç notta OECD'nin 1998 yılında gerçekleştirdiği "Kriptografi Teknolojilerindeki Kontroller" baslıklı envanter çalışmasının raporu 1999 yılında yayınlanmıştır. Bu envantere göre kriptografik ürünlerin ihracat ve ithalatından sorumlu kurumlar büyük çoğunlukla ekonomiden ya da sanayi ve ticaretten sorumlu bakanlıklardır. Envantere göre yalnızca Avustralya ve Türkiye'de sorumlu bakanlıklar

olarak Savunma Bakanlıkları belirtilmiştir. Türkiye'de ayrıca Dış Ticaret Müsteşarlığı da sorumlu kurum olarak belirtilmektedir.

5 KİŞİSEL VERİLERİN KORUNMASI

5.1 Giriş

Eğer kurumlar her zaman;

Nereye seyahat ettiğinizi,

O anda dünyanın neresinde olduğunuzu,

Kiminle telefonla konuştuğunuzu,

Hangi bilgisayarla çalıştığınızı,

Hangi kuruluşlara veya örgütlere üye olduğunuzu,

Ne satın aldığınızı,

Servetinizin veya borçlarınızın durumunu,

Sağlık durumunuzu,

Bilselerdi hoşunuza gider miydi?

Bu soruya Canavarın İnternet'teki sayısı 666 – Kutsal Kitap'ın gözüyle İnternet adıyla Türkçeye çevrilen kitabında Frank Sunn "Hep Yüce Tanrı her şeyi bilir deriz ama galiba başkası da aynı şeyleri yapmaya çalışıyor" diye cevaplıyor. Frank Sunn bilişime yönelik eleştirel bakışını son derece ustaca kaleme aldığı bu kitabında bilgi edinme özgürlüğüne sözde geçişi, bilgiye giden yolların açılmasını, küresel bilgiye herkesin ulaşabilmesini, yöneticilerin önceden hesapladığı ve tüm insanlığı kontrol altına alabilmeleri için gerekli bir adım olarak tanımlıyor.

Tüm dünyada otoriteler tarafından kişisel bilgilerin sistematik bir şekilde toplanması çalışmalarına yönelik tepkiler artadursun günümüzde bu tip bir çalışmayı yapmayan bir kuruma hemen hemen rastlamak artık imkânsız gibidir.

Durum böyle olmakla birlikte bilgi teknolojileri uygulamalarında temelin rakamlar üzerine kurulduğu, harflerin ikinci planda kaldığı yadsınamaz bir gerçektir. Sayısal bilgilerin veritabanı mantığı ile çalışan sistemlerin hızını ve güvenilirliğini sağlayan en önemli etkenlerden biri olduğu ise her türlü izahtan varestedir. Nasıl ki günlük hayatımızda isimler ile bir birbirimizi tanımlıyorsak bilgi teknolojileri ortamında da bu tanımlamalar sayısal anlamda yapılmaktadır. Bu durum da kişilere "bir numara" yani konumuz itibariyle TC kimlik no'sunun verilmesi ve bunun adres kayıt sistemi ile entegrasyonunu sağlanmasını zorunlu kılmaktadır.

"Kişisel Verilerin Korunması Kanun Tasarısı"nın gerekçe kısmında da belirtildiği üzere kişisel verilerin elektronik olarak işlenmesi, kişilere olduğu kadar özel ve kamu sektörüne de büyük yararlar sağlamaktadır. Bu şekilde mal ve hizmetler, daha kolay üretilebildiği gibi kişilerin veri işleme yoluyla tespit edilmiş tercihlerine bakılarak, bireylere ucuz ve sür'atle sunulabilmektedir. Elektronik veri işleme sistemleri keza, sağlık, sosyal güvenlik, eğitim, vergi, kamu düzeni ve güvenliği gibi alanlarda da benzer yararlar sağlamaktadır. Bu nedenle, mal ve hizmetlerin daha iyi, ucuz ve sür'atle sunulabilmesi için, verileri elektronik ortamlarda işleyen sistemler, gerek özel ve gerek kamu sektöründe hızla yaygınlaşmıştır.

Kişisel veri kütüğü sistemleri iki grup açısından önem arz etmektedir:

Bunlardan birincisini kişisel veri sicillerini kullananlar oluşturmaktadır. Yukarıda da belirtildiği gibi, mal ve hizmetlerin ihtiyaca uygun bir şekilde üretimi ve dağıtımı için bu tür sicillerden yararlanılması zorunlu hale gelmiştir. Bu sicillerden yararlananların, ihtiyaçları olan kişisel verileri işlemeleri engellenmemeli, aksine kolaylaştırılmalı, ancak ilkelere bağlanmalıdır.

- Diğer grubu ise, hakkında kişisel veri işlenen gerçek ve tüzel kişiler oluşturmaktadır. Elektronik bilgi işlem sistemlerinde zorunlu olarak kişiler hakkında kişisel veriler işlenmektedir. Kişisel veriler sınırsız olarak gelişigüzel toplandığı, denetimsiz olarak açıklandığı, yetkisiz kişilerin eline geçtiği takdirde kötüye kullanılarak kişilik hakları ihlal edilebilecektir. Bu nedenle kişisel veri sicillerinin bu tür sakıncaları giderecek şekilde kurulması, faaliyet göstermesi ve denetim altına alınması zorunlu hale gelmiştir.

Tasarı, bu iki grubun çıkarlarını koruyarak dengelemek ve kişilik hakları ile temel hak ve hürriyetleri korumak amacıyla hazırlanmıştır.

5.1.1 Mahremiyet

Tüm İnsan hakları içinde mahremiyet[201] belki de kavranması ve tanımlanması en zor alandır. Westin (1967, s.7)'e göre, "mahremiyet bireylerin, grupların veya kurumların kendilerine dair bilgilerin ne zaman, nasıl ve ne ölçüde diğerlerine aktarılabileceğini kendilerinin belirleme hakkıdır". Amerikalı hakim Louis Brandeis'in meşhur tanımında mahrumiyet "yalnız bırakılma hakkıdır-hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak" (Diffie ve Landau, 1998, s.132). Bu devletler, ekonomik kurumlar veya diğer bireyler gibi herhangi bir dışsal aktör

[201] www.icisleri.gov.tr/_Icisleri/WPX/tezler_İnternet'suclari.doc (15.04.2007)

tarafından yalnız bırakılma hakkıdır (Lyon, 1994). Profesör Arthur Miller (1971, s.40)'ın ifadesi ile bu "bireyin kendisiyle ilgili bilginin dolaşımını kontrol yeteneğidir"[202].

Mahremiyet otonomi hakkıdır ve yalnız bırakılma hakkını kapsar. Mahremiyet kendimiz hakkındaki bilgiyi -bu bilgiye girişi sınırlama hakkı dahil- kontrol hakkını içerir. Mahrumiyet hakkı sırları gizli tutma hakkını ve onları ancak özel konuşmalarda paylaşmayı kapsar. En önemlisi, mahremiyet hakkı yalnızlık, samimiyet ve anonimliği yaşama hakkı demektir. Fischer-Hubner (2000) mahremiyet kavramının üç özelliğe sahip olduğunu ifade eder. Bunlar mekânsal mahremiyet, kişi mahremiyeti ve bilgi mahremiyetidir. Birincisi, kişiyi çevreleyen yakın fiziksel alanı korumayı, ikincisi kişiyi haksız müdahalelere karşı korumayı, üçüncüsü kişisel verilerin toplanma, saklanma, işlenme ve dağıtımının nasıl yapılacağını veya yapılmayacağını kontrol etmeyi gerektirir.

Bireysel mahremiyet ise; toplumların ahlaki, manevi, sosyal, ekonomik ve hukuki kurallarının ayrılmaz bir parçası olup mahremiyetin ihlali bu kurallardan sapma sayılır ve suç oluşturur. Örneğin, bir şahsın evine zorla girmek ceza hukukunun ihlali demektir.

Bilgi ve iletişim teknolojisindeki gelişim bir yandan sosyal düzene bir meydan okuma yaratırken öte yandan bireysel özgürlüklere daha fazla sınırlamaların getirilmesi girişimlerine sebep olmaktadır. Başka bir deyişle İnternet sosyal düzene ve bireysel mahremiyete yeni meydan okumalar yaratmaktadır. Onun özellikleri düzen, kural koyma ve denetim açısından problemler doğurmaktadır. Sosyal düzenin çelişkili karakteri nedeniyle çözüm arayışları sonsuzdur ve dünya döndüğü müddetçe arayış ta devam edecektir.

Gittikçe artan miktarda hassas bireysel, tıbbi ve ticari veriler gibi kişisel veriler toplanmakta, işlenmekte ve ulusal sınırları aşan şebekeler yoluyla el değiştirmektedir. Bilginin dijitalizasyonu hükümetlere ve iş dünyasına ilgili bireylerin bilgi ve rızası olmadan bile, yurttaşlara ait bireysel verilere sahip olma, işleme, denetleme, kullanma ve değiş tokuş yapma konusunda eskisinden daha çok imkân sağlamaktadır. Bu mahremiyete yönelik bir tehdittir ve gizli takibe de zemin sağlar. Bu, bilgi mahremiyetinin istismarıdır.

Foley (1999) İnternet'in insan hakları ile ilişkili olduğu üç spesifik alan olduğunu ifade eder: bilgi özgürlüğü, ifade özgürlüğü ve mahremiyet. İnternet'in kullanıcılarına sağladığı özgürlük aynı zamanda bu haklara yönelik tehdidin de sebebi olmuştur. İnternet'in istismarı ve suistimalinden iki büyük tehdit doğmaktadır:

[202] Tanılır, M.Niyazi; "İnternet Suçları ve Bireysel Mahremiyet" Ankara, 2002

1. İfade hürriyetine karşı hükümet sansürü,

2. Mahremiyetin ihlali. Mahremiyetin ihlali iki şekilde ortaya çıkar:

   a. Hükümet veya iş dünyasınca toplanan kişisel verilerin istismarı,

   b. Bireysel haberleşmeye izinsiz giriş.

Mahremiyet insan özgürlüğünün bir parçası olduğundan mahremiyetin ihlali aynı zamanda özgürlüğün de ihlalidir. Mahremiyetin bihakkın korunmadığı yerde özgürlük yaşayamaz. Eğer güvenli bilgi ve iletişim ortamına sahip değilseniz, özgür bir biçimde haberleşemez ve özgür ifade hakkınızı koruyamazsınız. Kontrol edilme duygusu birey üzerinde engelleyici bir etkiye sahip olabilir. Batı Alman Anayasa Mahkemesi yeni bir Nüfus Sayımı Yasası'nın Anayasaya aykırı olduğuna dair 1983 tarihli kararında:

"Eğer bir kişi belli alanlarda kendisi hakkında hangi bilgilerin sosyal çevresince bilindiğine dair yeterli kesinlikte tahminde bulunamıyorsa ve iletişimin muhtemel taraflarına dair yeterli bir şekilde kestirimde bulunamıyorsa, o her hangi bir baskıya/etkiye konu olmaksızın özgür bir biçimde plan yapma ve karar verme özgürlüğünden (self-determinasyon) can alıcı bir biçimde alıkonuyordur. Bilgi ile ilintili olarak self-determinasyon hakkı, vatandaşların kendileri hakkında kimin, neyi, ne zaman ve hangi münasebetle bildiğini artık bilemediği bir sosyal düzeni ve onu sağlayan hukuk düzenini dışarıda bırakır. Eğer bir kişi aykırı davranışlarının kaydedilip bilgi olarak sürekli saklanıp saklanmadığı veya başkalarına aktarılıp aktarılmadığı konusunda emin değilse, o bu gibi davranışlarla dikkat çekmemeye çalışacaktır. Eğer o bir derneğe veya vatandaş girişimine katılımın resmi olarak kaydedildiğini ve bundan belirtilen şahsi risklerin doğduğunu düşünüyorsa, muhtemelen kendi haklarının tatbikatını terkedecektir. Bu sadece onun gelişim şansını sakatlamakla kalmayacak, ayrıca ortak yararı da sakatlayacaktır, çünkü self-determinasyon, davranmak ve işbirliği yapmak konusunda yurttaşlarının kapasitesine dayanan özgür demokratik toplumun bir temel fonksiyonel şartıdır"[203]

Diğer taraftan 1980 yılında OECD tarafından belirlenen “Adil Bilgi Uygulama Kuralları” özünde kişisel verilerle ilgili olarak şu ilkelere yer vermiştir:

- Bilgi toplanmasına belli kısıtlamalar getirerek, sadece gerekli bilgilerin toplanmasına izin verilmesini,

- Mümkün olabilen durumlarda bilginin doğrudan kişinin kendisinden alınmasını, bilgi alınmasının sebebinin açıklanmasını ve neden bu bilgiye gereksinim duyulduğunun açıklanmasını,

[203] Michael, 1994, s.4

- Toplanan bilginin sadece bildirilen neden için kullanılmasını,
- Bilgi veren kişiye, kişisel bilgilerine girme ve yanlış ise düzeltme olanağı verilmesini ister.

Avrupa Parlamentosu ve Konseyi de çıkardığı 1995 tarih ve 95/46/EC sayılı yönergesi ile verilerin ancak yasal çerçevede toplanabileceğini ve verinin öznesine sistem hakkında bilgilendirilme yapılacağını hükme bağlamıştır. Veriler, verinin öznesine açıktır, veri sahibinin verilere itiraz ve yanlış olan verilere karşı düzeltme hakkı vardır. Yönerge de asıl önemli olan Verinin gizliliği ve güvenliğini koruma ilkesidir. 2001 tarihli (CE) 45/2001 sayılı Avrupa Parlementosu ve Konseyi'nin Topluluk Kurum ve Organlarına Yönelik Verilerin Korunmasına İlişkin Düzenlemesine göre de kişisel veriler; adil ve yasal olarak, belirlenen, açık ve yasal olan amaçlar için toplanmalı ve ancak bu amaçlar doğrultusunda kullanılmalı, toplanma amacıyla ilgili ve yeterli ölçüde olmalı, bu amacı aşmamalı, doğru ve güncel olmalı (yanlış ya da eksik olan verinin silinmesi ya da düzeltilmesi için gereken yapılmalı) ve ancak amaca uygun olarak gerektiği sürece saklanmalıdır.

Mahremiyetin korunması mevzuatın yanı sıra mahremiyet koruma teknolojilerini gerektirir. Fischer-Hubner (2000)'in dediği gibi, tamamen bilgisayarlaşmış bir toplumda, mahremiyet ciddi bir şekilde tehlikededir ve sadece mahremiyet mevzuatı ile etkili bir şekilde korunamaz. Mahremiyetin gerekleri teknik olarak yerine getirilmeli ve mahremiyet enformasyon sistemleri için bir tasarım kriteri olmalıdır. Sistemler için yüksek mahremiyet gerekleri ile genişletilmiş güvenlik kıstasları çeşitli mahremiyet artırıcı güvenlik türlerini kapsamalıdır. Bunlar; anonimlik, takma isimlik (pseudonymity), bağlanamazlık (unlinkabilty), kullanıcıların gözlenemezliği (unobservability of users) ve giriş kontrolü veya şifreleme gibi güvenlik mekanizmaları dahil saklanacak, işlenecek veya transfer edilecek kişisel verilerin bütünlük ve gizliliğini korumak için zorunludurlar.[204]

5.1.2 Anonimlik Hakkı

"Anonimlik hakkı" özellikle İnternet'in gelişimiyle ortaya çıkmış, yasalar üstü bir haktır. İnternet üzerinde iletişim deklarasyonuna göre, bilgi ve düşüncelerin özgür ifadesini çoğaltmak için kişilerin kimliklerini ifşa etmeme hakkına saygı gösterilmelidir. Bir yandan kişilerin içerikten zarar görmesini engellemeye çalışmak, diğer yandan anonimlik hakkına saygı göstermeye çalışmak çok hassas bir ayar gerektirmektedir. Dengenin bozulması egemen olanın lehine işler ve fikirler özgürce çoğalamaz.

[204] İnternet Suçları ve Bireysel Mahremiyet - M.Niyazi Tanılır Ocak 2002- Liberte Yayınları

5.1.3 Pseudonym

Müstear, takma isimle yazmak. Çağdaş Yunanca'daki "yalan, yalancı, uydurma" anlamlarına gelen "pseud" önekinin "isim" anlamina gelen "onoma" kelimesiyle birleşmesiyle ortaya çıkan ve "takma ad, rumuz, mahlas" anlamlarına gelen “pseudonym” kelimesi Ortaçağ’da özellikle dini tekstler üzerine çalışan düşünürler, yazarlar tarafından kullanılmıştır. Pseudonym kalma günümüzde İnternet ortamında; bir taklit kimlikle, lakapla ortaya çıkma anlamında kullanılmaktadır. Bir görüşe göre kalabalığın içinde örneğin bir küfür sallayıp kaybolan bir birey aslına bir anlamda bir anonim kalma hakkı kullanmaktadır. Belki o an için kısa bir tepkisini belli etmektedir. Bu, bireyin kimliğini öğreneceğinizi anladığında gerçek fikirlerini artık konuşamaz ve iletemez bir hale geleceği, kabul edilmektedir [205].

5.2 Kurumların Bilgi Toplama Nedenleri

Kurumlar yasal olsun olmasın bilgilerini toplamak için kendilerince muhakkak geçerli bir sebep bulurlar. Ülkemize yakın bir zamanda gerçekleşmiş büyük bir süpermarket zincirinde meydana gelen olay buna çarpıcı bir örnektir. 10000 kadar kredi kartı bilgisini kendi sisteminde tutan süpermarket zincirine, e-ticaret sistemine sızan bir hacker bu verilerin tamamına yakınını elde etmişti. Bu süpermarket zinciri, kredi kartlarının kopyalanmasıyla ilgili sahtecilik olayının müşterilerine verebileceği muhtemel zarardan ötürü üzüntü duyduğunu, ancak hiçbir müşterisinin bu olayın sonuçlarına katlanmak zorunda kalmayacağını taahhüt ettiğini de aşağıdaki şekilde resmen duyurmuştu.

Yapılan açıklamada, şunlar kaydedildi: "… Yönetimi, … Mağazalarının kredi kartı işlemleri yönetim sistemine yapılmış olduğu tahmin edilen bir korsan saldırıdan dolayı, … 2006 günü sahte kredi kartı işlemleri tespit edildiğini doğrulamaktadırlar. … Yönetimi derhal, bankalarla işbirliği içinde kredi kartı işlemleri yönetim sistemi ile ilgili bir denetim başlatmış ve korsan saldırının gerçekleştiği sistem süratle ve tamamen kullanıma kapatılmıştır.

Yönetimi kullanılan yeni kredi kartı yönetim sisteminin tamamen güvenli olduğunu vurgulamak istemektedir. Bu çerçevede, … Yönetimi… 2006 tarihinde… Cumhuriyet Başsavcılığı nezdinde suç duyurusunda bulunmuş, olaydan zarar gören bankalar ilgili dosyaya müdahil olacaklarını bildirmişlerdir.

[205] İnternet Ve Hukuk, Yeşim M. Atamer, s.632

Yönetimi, bu sahtecilik olayının müşterilerine verebileceği muhtemel zarardan ötürü üzüntü duymaktadır ve hiçbir müşterisinin bu sahteciliğin muhtemel sonuçlarına katlanmak zorunda kalmayacağını taahhüt etmektedir."[206]

Görüldüğü üzere bu yapılan açıklamadan bile bu bilgilerin ilgili firma tarafından neden tutulduğu açıklanmamaktadır. Market alışverişlerinde kredi kartının banka pos cihazından geçirilmesi banka ile market arasında bağlantı kurulması ve ödeme işleminin gerçekleşmesi için yeterlidir. Kredi kartının teknik olarak ayrıca markete ait bir bilişim sistemden geçirilmesi zorunluluğu yoktur. Ancak buna rağmen bu bilgiler uygulamada özellikle muhasebeleştirme işlemlerindeki kolaylık açısından ilgili firmalarca kayıt altına alınmaktadır. Öyle ki bazı marketlerde kredi kartının ayrıca bu sistemden geçirilmemesi durumunda kasa dahi açılmamaktadır[207].

5.3 Toplanan Bilgilerin Güvenliği

Son derece önemli bilgilerin depolandığı alanların yetkisiz ve kötü niyetli kişilerin eline geçebileceği muhakkaktır. Türkiye'de yaşayan tüm vatandaşların kimlik bilgilerinin text ortamında tutulduğu veri dosyasının anahtarlıklarımızdaki flash disklere, cep telefonlarımızdaki hafıza kartlarına veya yolda müzik dinlediğimiz i-podlara yüklenebilir türden küçük dosyalar olduğu gerçeğini görmek durumun ne kadar önemli olduğuna işaret etmektedir.

En emniyetli bilgisayarın kapalı bir bilgisayar olduğuna dair yaygın bir söz vardır. Bu sözü akıllıca ama yanlış diye nitelendiriyor dünyanın ilk ve en büyük hackerı olarak tabir edilen Kevin Mitnick "Aldatma Sanatı" adlı kitabında. Art niyetli bir kişi ofise gidip bilgisayarı açması için birini ikna ederek işi bitirir. Elinizdeki bilgiye sahip olmak isteyen bir rakibiniz çoğu zaman var olan pek çok farklı yoldan birini kullanarak onu elde edebilir. Bu iş yalnızca zamana, sabırlı olmaya, kişiliğe ve ısrarcılığa bakar. İşte bu noktada aldatma sanatı devreye girer diye gerekçelendiriyor bu görüşünü kitabında Kevin Mitnick[208].

5.4 İlgili Uluslararası Düzenlemeler

OECD Kriptografi Politika Rehberi (OECD, 1999) tarafından tasarlandığı gibi yurttaşların kendi meşru mahremiyet hakkını korumak amacı ile her hangi bir sınırlama olmaksızın şifreleme teknolojisini kullanma bireysel hakkını içermelidir: "Mahremiyete dair temel birey haklarına, haberleşmenin gizliliği ve kişisel verilerin korunması dahil,

[206] http://www.dunyagazetesi.com.tr/news_display.asp?upsale_id=264914 (15.04.2007)

[207] http://www.milliyet.com.tr/2006/05/30/son/soneko09.asp (30.05.07)

[208] Mitnick,Kevin D./Simon,William L., "Aldatma Sanatı" Çeviren; Nejat Eralp Tezcan, Ankara,2006

ulusal kriptografi politikalarında ve kriptografik yöntemlerin kullanım ve uygulamasında saygı gösterilmelidir".

Mahremiyet uluslararası topluluk tarafından bir temel insan hakkı olarak tanınmıştır ve uluslararası insan hakları hukukunda mahremiyet açık ve muğlak olmayan bir şekilde, korunması gereken bir temel hak olarak vazedilmiştir. 1948 Evrensel İnsan Hakları Bildirgesi'nin 12. maddesi "Hiç kimsenin mahremiyeti, ailesi, evi veya haberleşmesi keyfi müdahalelere konu olamaz ve şeref ve itibarına saldırıda bulunulamaz. Herkes bu gibi müdahale ve saldırılara karşı kanun tarafından korunma hakkına sahiptir" demektedir. (Academy on Human Rights, 1993, s.3)

1967 Uluslararası İnsan Hakları Sözleşmesi'nin 17. maddesi aynı hususu düzenler : "1. Hiç kimsenin mahremiyeti, ailesi, evi veya haberleşmesi keyfi veya hukuk dışı müdahalelere konu olamaz ve şeref ve itibarına hukuk dışı saldırılar yapılamaz. 2. Herkes bu gibi müdahale ve saldırılara karşı kanun tarafından korunma hakkına sahiptir. " (United Nations, 1985, s.149)

"Mahremiyet" kelimesini zikretmemesine rağmen 1950 Avrupa İnsan Hakları Sözleşmesi (Council of Europe, 1950)'nin 8. maddesi özel hayata, meskene ve haberleşmeye saygı hakkını deklare eder ve kamu otoritesinin müdahalesini gerektiren şartlara dikkat çeker: "Herkes özel ve aile hayatına, evine ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bu hakkın uygulanmasında kargaşa veya suçu önleme, sağlık veya ahlakı koruma, veya diğerlerinin haklarını ve özgürlüklerini koruma amacı ile bir demokratik toplumda ulusal güvenlik çıkarları, kamu güvenliği veya ülkenin ekonomik refahı açısından zorunlu olan ve kanun ile düzenlenmiş durumlar hariç kamu otoritesinin hiçbir müdahalesi olmamalıdır".

Mahremiyet insan özgürlüğünün bir parçası olduğundan mahremiyetin ihlali aynı zamanda özgürlüğün de ihlalidir. Mahremiyetin bihakkın korunmadığı yerde özgürlük yaşayamaz. Eğer güvenli bilgi ve iletişim ortamına sahip değilseniz, özgür bir biçimde haberleşemez ve özgür ifade hakkınızı koruyamazsınız. Kontrol edilme duygusu birey üzerinde engelleyici bir etkiye sahip olabilir.

Batı Alman Anayasa Mahkemesi yeni bir Nüfus Sayımı Yasası'nın Anayasaya aykırı olduğuna dair 1983 tarihli kararında: "Eğer bir kişi belli alanlarda kendisi hakkında hangi bilgilerin sosyal çevresince bilindiğine dair yeterli kesinlikte tahminde bulunamıyorsa ve iletişimin muhtemel taraflarına dair yeterli bir şekilde kestirimde bulunamıyorsa, o her hangi bir baskıya/etkiye konu olmaksızın özgür bir biçimde plan yapma ve karar verme özgürlüğünden (self-determinasyon) can alıcı bir biçimde alıkonuyordur. Bilgi ile ilintili olarak self-determinasyon hakkı, vatandaşların kendileri hakkında kimin, neyi, ne zaman ve hangi münasebetle bildiğini artık bilemediği bir

sosyal düzeni ve onu sağlayan hukuk düzenini dışarıda bırakır. Eğer bir kişi aykırı davranışlarının kaydedilip bilgi olarak sürekli saklanıp saklanmadığı veya başkalarına aktarılıp aktarılmadığı konusunda emin değilse, o bu gibi davranışlarla dikkat çekmemeye çalışacaktır. Eğer o bir derneğe veya vatandaş girişimine katılımın resmi olarak kaydedildiğini ve bundan belirtilen şahsi risklerin doğduğunu düşünüyorsa, muhtemelen kendi haklarının tatbikatını terkedecektir. Bu sadece onun gelişim şansını sakatlamakla kalmayacak, ayrıca ortak yararı da sakatlayacaktır, çünkü self-determinasyon, davranmak ve işbirliği yapmak konusunda yurttaşlarının kapasitesine dayanan özgür demokratik toplumun bir temel fonksiyonel şartıdır" (Michael, 1994, s.4).

1980 yılında OECD tarafından belirlenen “Adil Bilgi Uygulama Kuralları” özünde de yine benzer dürtülerle hareket edildiğini görüyoruz:

- Bilgi toplanmasına belli kısıtlamalar getirerek, sadece gerekli bilgilerin toplanmasına izin verilmesini,
- Mümkün olabilen durumlarda bilginin doğrudan kişinin kendisinden alınmasını, bilgi alınmasının sebebinin açıklanmasını ve neden bu bilgiye gereksinim duyulduğunun açıklanmasını,
- Toplanan bilginin sadece bildirilen neden için kullanılmasını,
- Bilgi veren kişiye, kişisel bilgilerine girme ve yanlış ise düzeltme olanağı verilmesini ister.

Avrupa Parlamentosu ve Konseyi’nin 1995 yılı tarihli 95/46/EC sayılı yönergesine göre veriler yasal çerçevede toplanabilir ve verinin öznesine sistem hakkında bilgilendirilme yapılır. Veriler, verinin öznesine açıktır, veri sahibinin verilere itiraz ve yanlış olan verilere karşı düzeltme hakkı vardır. Yönerge de asıl önemli olan Verinin gizliliği ve güvenliğini koruma ilkesidir. 2001 tarihli (CE) 45/2001 sayılı Avrupa Parlementosu ve Konseyi’nin Topluluk Kurum ve Organlarına Yönelik Verilerin Korunmasına İlişkin Düzenlemesine göre de kişisel veriler; adil ve yasal olarak, belirlenen, açık ve yasal olan amaçlar için toplanmalı ve ancak bu amaçlar doğrultusunda kullanılmalı, toplanma amacıyla ilgili ve yeterli ölçüde olmalı, bu amacı aşmamalı, doğru ve güncel olmalı (yanlış ya da eksik olan verinin silinmesi ya da düzeltilmesi için gereken yapılmalı) ve ancak amaca uygun olarak gerektiği sürece saklanmalıdır.

Mahremiyetin korunması mevzuatın yanı sıra mahremiyet koruma teknolojilerini gerektirir. Fischer-Hubner (2000)'in dediği gibi, tamamen bilgisayarlaşmış bir toplumda, mahremiyet ciddi bir şekilde tehlikededir ve sadece mahremiyet mevzuatı ile etkili bir şekilde korunamaz. Mahremiyetin gerekleri teknik olarak yerine getirilmeli ve

mahremiyet enformasyon sistemleri için bir tasarım kriteri olmalıdır. Sistemler için yüksek mahremiyet gerekleri ile genişletilmiş güvenlik kıstasları çeşitli mahremiyet artırıcı güvenlik türlerini kapsamalıdır. Bunlar; anonimlik, takma isimlik (pseudonymity), bağlanamazlık (unlinkabilty), kullanıcıların gözlenemezliği (unobservability of users) ve giriş kontrolü veya şifreleme gibi güvenlik mekanizmaları dahil saklanacak, işlenecek veya transfer edilecek kişisel verilerin bütünlük ve gizliliğini korumak için zorunludurlar[209].

5.5 Ülkemizdeki Mevcut Düzenlemeler

Ülkemizde, Özel Hayatın Gizliliği, Haberleşme Hürriyeti ve Haberleşmenin Gizliliği Anayasa ile korunmuştur. (T.C.Anayasası Madde 20, Madde 22). Türkiye ayrıca; (8.maddesiyle) "Herkesin Özel ve Aile Hayatına, Konutuna ve Haberleşmesine Saygı Gösterilmesini" hükme bağlayan Avrupa İnsan Hakları Sözleşmesi'ni 1954 yılında onaylamış; "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması"'na ilişkin 108 sayılı Avrupa Konseyi Sözleşmesi'ni de 1981 yılında imzalamıştır. Bunların yanı sıra Türkiye, veri koruması ve sınır-ötesi bilgi akışı konusundaki OECD Yönlendirici İlkeleri'ni de imzalamıştır.

5237 Sayılı Türk Ceza Kanunu'nun Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlıklı dokuzuncu bölümündeki maddelerle 5271 Sayılı Ceza Muhakemesi Kanunu'nun İletişimin tespiti, dinlenmesi ve kayda alınması başlıklı 135.maddesi ve Teknik Araçlarla izleme başlıklı 140.maddelerinde ise ilgi çekici düzenlemeler mevcuttur.

Kişisel verilerin korunmasına ilişkin en somut ve özel düzenleme olan "Kişisel Verilerin Korunması Kanun Tasarısı" 09.11.2005 tarihinde Başbakanlığa sevk edilmiştir.

Sonuç olarak belirtmek gerekir ise Kişilere bir numara verilmesi ve bu numaralar aracılığıyla işlemlerin gerçekleştirilmesi gelişen teknolojinin zorunlu bir sonucudur. Elbette ki; bir şekilde elde edilmiş toplu verilerin de denetiminin belli ilkelere bağlanması gerekmektedir. "Kişisel Verilerin Korunması Kanun Tasarısı"nın kanunlaşması ile de bu tür sorunların çözümünde önemli bir yol aşılmış olacaktır.

5.6 Kişisel Verilerin Koruması Konusunda AB Müktesebatı

Avrupa Birliği Ülkelerinde kişisel verilerin korunması ve gizliliğinin sağlanması önemli bir konu olarak ele alınmaktadır.

[209] Tanılır, M.Niyazi, "İnternet Suçları ve Bireysel Mahremiyet" Ankara, 2002

Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme, 28.1.1981 tarihinde Strasbourg' da imzalanmıştır. Türkiye Avrupa Birliği Konseyinin kabul ettiği 108 sayılı bu sözleşmeyi imzalayarak gerekli düzenlemelerin yapılması için çalışmalar başlatmıştır.

Günümüze kadar Avrupa Birliği Strazburg sözleşmesini tamamlayıcı nitelikte 2002/58/EC ve 95/46EC sayılı iki adet direktif yayınlamıştır[210]. Sözkonusu direktiflere sırasıyla adreslerinden erişilebilmektedir.

5.6.1.1 Almanya

Federal Data Protection Act (Bundesdatenschutzgesetz,211 BDSG): 20 Aralık 1990 tarihinde halen yürürlükte olan halini almıştır. Almanya da veri koruması bilgi teknolojilerinin gelişmesine paralel olarak 1970 lerin başında Hessen Eyaletinde başlamıştır. 1977 yılında ilk Federal Kanun olarak çıkmıştı. 1983 yılında Alman Yargıtay'ı bilgi güvenliği konusunda önemli bir adım atarak Kurumlarında bulunan kişisel bilgilerin kurumlar tarafından kullanılmasının kişinin bireysel hakkı olduğuna karar verdi. Bu durumda kişisel verilerin toplanabilmesi için anahtar kriter zorunluluk ve maksatla sınırlı prensibi olarak belirlendi. Bu da şahsın kendi bilgilerini takip edebilmesini mümkün kıldı.

1990 tarihli veri koruması yasası aynı zamanda kişisel bilgilerin korunmasını zorunlu kılmıştır. Kişiler kendi bilgilerinin toplanmasına veya saklanmasına rıza göstermezlerse kurumlar buna göre düzenlemelerde yapmak zorundadırlar. Öncelikle devlet kişinin rızası olmadan kişisel bilgileri toplamamakta ve saklamamaktadır. Polis soruşturmaları, istihbarat servisleri ve savunma konuları bu kapsamdan muaf tutulmuşlardır. Kamu ve özel sektör kuruluşları kişileri şahsi bilgilerini aldıkları konusunda bilgi sahibi yapmak ve rızalarını almak zorundadırlar.

Veri koruma yasası birçok güvenlik kısıtlamalarını zorunlu kılmaktadır. Örneğin veriye erişim yetkileri, veri saklamadan sakınma ve verinin gereksiz kullanımını düzenler.

Yasa, yasa ihlalleriyle ve şikâyetleriyle doğrudan ilgilenen ve Alman devleti tarafından görevlendirilmiş bir Federal Veri Koruma Komseri (Federal Data Protection Commissioner) tanımlamıştır. Veri Koruma Komiseri aynı zamanda yasanın düzgün işlemesiyle ilgili olarak parlamentoya ve hükümete tavsiyelerde bulunur.

Yasa veri koruma yasası ihlallerine bir ile beş yıl arasında hapis cezası öngörmektedir.

---

[210] http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf (15.04.2007)
http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (15.04.2007)
[211] : http://www.gesetze-im-İnternet'.de/ bundesrecht/bdsg_1990/gesamt.pdf (15.04.2007)

Belirtilen Kişisel Verilerin Korunması Yasasının yanısıra Almanya'da 2006 tarihinde kamuoyunda çok tartışılan AntiterörYasası kabul edildi. Bu Kanun aslında 11 Eylül 2001 tarihinde kabul edilen Terörle Mücadale Kanununun uzatılmasına ilişkin bir Kanun idi. Bu Kanuna göre merkezi federal ve eyalet verileri index veriler ve gelişmiş (ayrıntılı veriler) şeklinde ikiye ayrılmıştır. **İndex veri**ler ve bu verileri paylaşan 38 kurum tarafından her an sorgulama yapılabilmektedir. İndex veriler yasaya göre isim, cinsiyet, doğum tarihi,doğum yeri, tabiiyet, adresler, diller, fotograflar ve özel alameti farikalardan oluşmaktadır.

Ayrıntılı veriler ise kaynakları korumak amacıyla talep üzerine verilebilir ve sadece acil durumlarda geçici bir tehlikeden sakınmak amacıyla istenebilir. Ayrıntılı veriler bağlamına yasanın kabul ettiği veriler telefon ve banka bağlantıları, motorlu taşıtlar bilgileri, aile durumuna ilişkin veriler, kişilerin dinlerine ilişkin bilgiler, ruhsat veya izinlerine ilişkin bilgiler, silah ve patlayıcı madde ilişkin bilgiler, ziyaret edilen yer ve ziyaret yeri bilgileridir (belli gruplar için). Beş yıldan beri geçerli olan kanun Parlemanto tarafından 5 yıl daha uzatıldı. Yeni yasaya göre istihbarat örgütleri motorlu taşıtlar ve motorlu taşıt aidiyet bilgilerine direkt ulaşabileceklerdir. Alman İç İşleri Bakanı Wolfgang Schauble yaptığı açıklamaya göre eğer bu Kanun olmasaydı yakın geçmişte ortaya çıkarılan bavullu bomba patlatma organizasyonu ortaya çıkarılamayacaktı[212]. Bu açıklama bu Anti Terör Yasasının belirtilen hükümlerine kişisel verilerin korunması taraftarlarının eleştirileri üzerine yapılmış olsa gerek.

Almanya'da mevcut olan bir başka kişisel verilerin korunması ile ilgili kanun da İletişim Verilerinin Korunması Hakkında Kanundur (Teledienstdatenschutzgesetzes). Temmuz 1997 yılında yürürlüğe giren Tele Hizmetler Veri Koruma Yasası belirtilen koşullar sanal ortamda kişisel verilerin kullanılmasında uyulması gereken kuralları belirlemiştir. Yasaya göre kişisel verilerin korunması koşulları veri kullanılmasa dahi geçerlidir. Yasada tele servis sağlayıcı ile kullanıcını uymaları gereken kurallar açıklanmıştır. Kurallar incelendiğinde kişisel verilerin tele servislerde kullanılması konusunda kişinin rızası esastır ve tele servis sağlayıcı bu konu hakkında kullanıcıyı bilgilendirmek zorundadır. Yasanın ihlalleri konusunda Kişisel Verilerin Korunması Hakkındaki Kanuna (Bundesdatenschutzgesetz, BDSG) atıfta bulunmuştur213.

5.6.1.2 İngiltere

İngiltere'de kişisel verilerin korunmasını sağlayan kanun Data Protection Act'dir214.Temmuz 1998 yılında yürürlüğe giren veri koruma yasası UK

[212] http://www.faz.net/s/Rub28FC768942F34C5B8297CC6E16FFC8B4/Doc~E1913C07215D34C0CB3179A134EAC523C~ATpl~Ecommon~Scontent.html (03.12.2006)
[213] http://bundesrecht.juris.de/ bundesrecht/tddsg/gesamt.pdf (Almanca) (15.04.2007)
http://www.iuscomp.org/ gla/statutes/TDDSG.htm(İngilizce) (15.04.2007)
[214] http://www.opsi.gov.uk/acts/acts1998/19980029.htm (15.04.2007)

vatandaşlarının kişisel bilgilerini ve kişisel verilerini korunması maksadıyla yapılmıştır. Yasa yaşayan kişileri tanımlamaya yarayan verileri toplayan ve barındıran tüm kurum ve kuruluşların uymaları gereken kuralları belirler. Yasaya göre kişisel bilgiyi toplayan kurum veya kuruluş bu veriyi sadece hizmet ettikleri belirli bir amaca yönelik kullanmalarına olanak verir. Kişisel veriler sadece belirli bir süre saklanabilirler ve kişinin izni olmadan hiçbir şekilde başka birileriyle paylaşılamaz. Yasa devletten bağımsız bir Bilgi Komiseri Bürosu (Office of the Information Commissioner) tarafından denetlenmeyi zorunlu kılmıştır. Kişisel bilgi toplayan veya barındıran tüm kurum ve kuruluşlar bilgi komiserliğine kayıt olmalıdırlar. Yasanın tamamına İnternet'adresinden erişilebilir.

5.6.1.3 Fransa

Fransa'da 6 Ocak 1978 tarih ve 78-17 sayılı kanunu değiştiren 6 Ağustos 2004 ve 2004-801 sayılı Kişisel Verilerin Kulanılması Ve Korunması İle İlgili Kanun [215] kabul edilerek kişisel verilerin korunması mevzuata girmiştir.: Kanun 1978 yılında çıkarılmış olan kanunun Avrupa Birliğinin 95/46/EC sayılı direktifine uygun olarak düzenlenmiştir.

Avrupa Birliği Müktesebatına ve belli başlı AB ülkelerinin kanunlarına baktığımızda öncelikle kişisel verilerin korunması yolunda somut kanun maddeleri bulunmakta, kanun ihlallerinde hapis cezası öngörülmekte ve bağımsız veri koruma denetmenliği (komiserliği) gibi bir yapı öngörülmektedir.

5.7 İdare Hukuku Açısından Kişisel Verilerin Korunması Hukuku

5.7.1 Genel Olarak İdare Hukuku ve Kişisel Verilerin Korunması

Bu Rapor kapsamında AB uyum sürecinde yaşadığımız bu yeniden yapılanma anlayışı içinde önemli bir yer tutacağı anlaşılan ve idareyi oldukça ilgilendiren kişisel verilerin korunması konusunda "Kişisel Verilerin Korunması ve Saklanması" konusunu ele alacak ve özellikle konunun idareyi ilgilendiren yönü üzerinde durmaya çalışacağız. Ancak öncelikle idareyi diğer kurum ve kuruluşlardan ayıran temel kavramlar üzerinde duracak ve daha sonra kişisel verilerin AB Müktesebatı ve Hukukumuz açısından ele alacağız.

AB'nin Türkiye için hazırladığı 2005 Yılı İlerleme Raporunda veri koruması hukuku açısından, yeni Ceza Kanunundaki, kişinin siyasi, felsefi ve dini fikirleri, ırksal kökenleri, yasadışı ahlaki eğilimleri, cinsel hayatı veya başkalarının sağlık durumu veya sendikalarla ilişkisi hakkında yasadışı bilgi toplayan kişilerin hapis cezasına çarptırılmasını öngören hüküm içerdiği övgüyle vurgulanmıştır. Öte yandan Ceza

[215] (LOI n° 2004–801 du 6 août 2004 relative à la prot ection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Kanununda ayrıca, kişisel verilerin dağıtımı ve yasal süre çerçevesinde imhasına ilişkin maddeler bulunduğu belirtilmiştir. Ayrıca Türkiye'nin Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunması Sözleşmesini imzaladığı özellikle belirtilerek Türkiye'nin bu antlaşmayı henüz onaylamadığına vurgu yapılmıştır. Son olarak ta Türkiye'de, kişisel verilerin korunmasına ilişkin kuralların uygulanmasını sağlayacak kurumsal çerçevenin kilit bir unsuru olarak veri muhafazasını denetleyecek bağımsız bir kurum oluşturması tavsiye edilmiştir.[216]

Diğer taraftan ise Kişisel Verilerin Korunması Hukuku aracılığı ile AB 'nin yeni ekonomik bir silaha sahip olduğu, "özellikle AB Kişisel Verilerin Korunmasına ilişkin bu Yönergenin kendisinin öngördüğü korumaya eşdeğer yasaları yoksa Avrupalıların kişisel bilgilerinin üçüncü ülkelere transferlerini yasaklamaktadır. Bu durum ABD hukukçularının çoğunluğu ile yeni ekonomiye yön vermeye alışık iş çevrelerini teoride ve pratikte Avrupa'ya karşı tavır almaya itmektedir. Onlar Avrupa'yı pederşahi bir tavırla değişime karşı durmakla bilgiye erişim özgürlüğünü engellemek ile pahalı yeni bürokratik kurumlar yaratmakla en önemlisi Avrupalı tüketiciye kötü ve niteliksiz ürünlere pahalıya almaya mahkum etmekle suçlarken süzülmüş ve demokrasi ve insan hakları yaklaşımı ve küresel bilgi trafiğine kırmızı ışıklar koyan Avrupa yoksa zaman mı kazanıyor?"[217] diye eleştirilmektedir.

5.7.2 Kamu İdaresi Ve Hizmeti Kavramı

Kamu Hizmetlerini yasalar gereğince yürütmekle görevli yapı kamu idaresidir. Dar anlamda kamu idaresi, politika kararlarını yasalara uygun bir biçimde yerine getiren hiyerarşik bir düzendir. [218] Kamu yönetimi, yasama ve yürütme organlarının vazgeçilmez ortağıdır. Kamu yönetiminin yaptığı işlerin büyük kısmı günlük işlerin yürütülmesi ile ilgilidir. Bu işler de teknik ve yönetsel beceriye ihtiyaç göstermektedir.[219] Geniş anlamda idare, düzenli toplumlarda kamu gücünün örgütlenmesini ve işleyişini içerir. Bu her türlü devlet görevlerini ve örgütlerini içine alan bir tanımlamadır.[220]

Kamu idaresi özel idareden bazı yönleri ile ayrılır ve farklı amaçları gerçekleştirmek üzere kurulurlar. Bu farklar kısaca şunlardır; **birinci** fark amaçtadır. Kamu idaresinin amacı kamu yararının gerçekleştirilmesidir. Özel idareler ise özel çıkarlarını gerçekleştirmek için kurulular. Kâr etmek gibi. **İkinci** olarak kamu idareleri kamu yararını gerçekleştirmek için kamu gücüyle donatılırlar. **Üçüncü** olarak kamu idareleri özel idarelere oranla kamu gücüne dayandıklarından dolayı özel kişiler

---

[216] 2005 AB Komisyonu Tarafından Türkiye İçin Yayınlanan İlerleme Raporu , http://www.abgm.adalet.gov.tr/ (12.05.06)

[217] Tansuğ, Avniye, AB'nin Yeni Ekonomik Silahı Veri Saklama Hukuku, Güncel Hukuk Dergisi, Nisan 2005, Sayı; 16, s. 54

[218] Doğan Canman, **İnsan Kaynakları Yönetimi,** Yargı Yayınevi, Ankara, 2000, s.1.

[219] Bilal Eryılmaz, **Kamu Yönetimi,** 2.Baskı, İzmir,1995,s.37

[220] Gözübüyük, A.Şeref, **Yönetim Hukuku**, 13.Baskı, Turhan Kitapevi, Ankara,1999, s.2

karşısında üstün konumdadırlar. **Dördüncü** ve son önemli farkta kamu idaresinin kuruluşu ve işleyişi kanunlarla düzenlenmesidir. Yani Kamu idareleri özel idarelere oranla "**kanuna bağlılık**" ilkesi çerçevesinde çalışırlar. [221]

Kamu idaresini ilk olarak kuruluşu, personeli ve teşkilatı söz konusu olduğunda organik idare, yaptığı eylem ve işlemleri söz konusu olduğunda ise işlevsel idare gündeme gelmektedir.[222] Kamu idaresi "organik olarak" devletin yürütme organının Cumhurbaşkanı, Başbakan, Bakanlar ve Bakanlar Kurulu dışında kalan kısmı ile devlet dışında kalan kamu tüzel kişilerdir. Devlet dışındaki kamu tüzel kişiler ise İl Özel İdaresi, Belediyeler, Köyler, Üniversiteler, KİT'ler, TRT, Barolar ve diğer Meslek kuruluşları gibi tüzel kişilerdir. Kamu idaresi fonksiyonel olarak kısaca devletin yasama ve yargı fonksiyonları dışında kalan fonksiyonları ifade etmektedir.[223] Duguit'e göre idari fonksiyon yasama fonksiyonuna göre bünyesinde açık bazı farklar ihtiva eder. Bu farkların başlıcası yasamanın daima soyut ve genel, idari işlemlerin ise somut ve özele has olmasıdır.[224] İdari fonksiyon yürütme fonksiyonundan da farklılıklar arz eder. Yürütme fonksiyonu ya da hükümet fonksiyonu idari fonksiyona göre daha genel ve kapsayıcı bir özelliği içinde barındırır. Hükümet fonksiyonu ülkenin genel siyasetini belirleme, ülkenin yüksek yönetimini sağlama, ülkenin kısa, orta ve uzun vadeli hedeflerini belirleme ve uygulama gibi fonksiyonları içerir. İdari fonksiyon ise daha çok tekniktir ve kamu hizmetleri ile ilgilidir.

Anayasamızın 123. maddesi İdarenin kuruluş ve görevlerinin bir bütün olduğunu ve kanunla düzenleneceğini, öte yandan İdarenin kuruluş ve görevleri bakımından birincisi merkezden yönetim ve ikinci olarak ta yerinden yönetim esaslarına dayandığını belirtmektedir. Kamu tüzelkişiliği ise ancak kanunla veya kanunun açıkça verdiği yetkiye dayanılarak kurulabilir.

İdarenin önemli bir kısmını oluşturan Merkezî Yönetim vatandaşlara sunulacak olan kamu hizmetlerinin belediye, köy, üniversite, KİT, TRT gibi devletten ayrı kamu kuruluşları aracılığı değil de doğrudan doğruya devlet tarafından yürütülmesi anlamına gelmektedir.[225] Bu hizmetleri örnek olarak eğitim hizmetlerini Milli Eğitim Bakanlığı, sağlık işlerini Sağlık Bakanlığı, cezaevleri ile ilgili işleri ise Adalet Bakanlığı merkezden yönetmekte ve vatandaşlarla ilgili verileri işlemekte ve transfer etmektedir.

Yerel yönetimler ise il, belediye veya köy gibi belirli yerlerde ikamet edenlerin yerel ihtiyaçlarının karşılanması için, merkezi idarenin dışında kurulan, ayrı tüzel kişilikleri bulunan, belirli bir oranda merkezden özerk, karar organları seçmenler

[221] Gözler, Kemal, **İdare Hukuku**, C.1, Ekin Yayınevi, Bursa, 2003, s.20
[222] Gözler, a.g.e., C.1, s.21
[223] Gözler, a.g.e., C.1, s.25
[224] Özbudun, Ergun, Türk Anayasa Hukuku, 7. Baskı, Yetkin Yayınları, Ankara, 2002, s.172
[225] Gözler, a.g.e., C.1, s.115

tarafından seçilen kamu tüzel kişilerdir.[226] Bu kamu tüzel kişileri de bu kamu hizmetlerin sunulması sırasında hizmet sunulan vatandaşlarla ilgili birçok veriyi toplamakta, işlemekte ve gerekirse transfer etmektedirler.

Yerel yönetimlerin dışında hizmet yönünden merkezden ayrı işlem yapan, kamu hizmeti gören kurumlar da bulunmaktadır. "**Hizmet Yönünden Yerinden Yönetim Kuruluşları**" da denen bu kurumlar merkezi idare tarafından yürütülmesi uygun görülmeyen, uzmanlık isteyen bazı kamu hizmetlerinin yürütülmesinden sorumlu, devletten ayrı tüzel kişilikleri bulunan ve belirli oranda özerk yapıları bulunmaktadır.[227] Bu kurumlar devletin hiyerarşik değil ve fakat vesayet denetimi altındadırlar.[228]

Yer yönünden Yerinden Yönetim ile Hizmet Yönünden Yerinden Yönetim Kuruluşları arasında ise yer yönünden Yerel Yönetimlerde tüzel kişilik insanlara tanınırken, hizmet yönünden yerel yönetimlerde tüzel kişilikler hizmete tanınmakta, birincisi kişi topluluğu olarak oluşurken, ikincisi mal topluluğu olarak oluşmakta, birincisinde organlar seçimle işbaşına gelmekte, ikincisinde ise atama ile gelmektedirler. Faaliyet konuları bakımından ise birincisinde genel yetki mevcut olup, ikincisinde ise uzmanlık konusu ile ilgili olmak üzere faaliyet alanları sınırlıdır.[229]

Hizmet Yönünden Yerinden Yönetim Kuruluşlarına örnek olarak TRT, Üniversiteler, Barolar, Meslek Odaları, SSK ve KİT'leri verebiliriz.[230]

Genel olarak kamu tüzel kişilerini kamu hukukuna tabi olan tüzel kişiler olarak tanımlayabiliriz. Yukarıda da bahsettiğimiz gibi kamu tüzel kişileri "kişi topluluğu" ve "mal topluluğu" olmak üzere iki kısma ayrılmaktadır. [231] Kişi toplulukları olan kamu tüzel kişileri Devlet, il özel idareleri, belediyeler ve köylerdir. Mal toplulukları şeklideki kamu tüzel kişilerine ise üniversiteler, TRT, KİT'ler örnek verilebilir. Konumuz açısında bu tüzel kişiler hizmetleri ile ilgili konularda sürekli olarak kişisel verileri toplamakta ve işleme tabi tutmaktadırlar.

Kamu hizmeti, bir kamu kurumunun ya kendisi tarafından ya da yakın gözetimi altında özel girişim eliyle kamuya sağlanan hizmet olarak tanımlanabilir.[232]

Kamu hizmeti "devlet veya diğer kamu tüzel kişileri tarafından veya bunların gözetim ve denetimleri altında genel, kolektif ihtiyaçlarını karşılamak, kamu yararını sağlamak için kamuya sunulmuş devamlı ve muntazam faaliyetlerdir" denilmektedir.[233]

---

[226] Gözler, a.g.e., C.1, s.125
[227] Gözler, a.g.e., C.1, s.127
[228] Danıştay'ın 1. Dairesinin 1988/107 E, 1988/108 K. Sayılı Kararı; "Merkezi idarenin ve Danıştay'ın bu maddeye göre yaptığı denetimin, yerinden yönetim organlarının işlem ve kararlarının mevzuata aykırı olmamasının sağlanması amacıyla öngörülen bir tür vesayet denetimi olduğu kuşkusuzdur."
[229] Gözler, a.g.e., C.1, s.129
[230] Gözler, a.g.e., C.1, s.128, 134
[231] Gözler, a.g.e., C.1, s.133
[232] Gözübüyük, a.g.e., s.235

İdarenin faaliyetleri genel olarak iki alanda toplanmakta ve bunlar kamu hizmetleri faaliyetleri ve kolluk faaliyetleri olarak ikiye ayrılmaktadır. Doğaldır ki idarenin hem kolluk, hem de kamu hizmetleri alanlarında kişisel verilerin korunmasına ilişkin hükümler uygulama konusu olacaktır. Kolluk faaliyetleri ilk olarak amaç bakımından kamu hizmetlerinden ayrılır. Kamu hizmetlerinin amacı kamu yararıdır. Kolluk faaliyetlerinin amacı ise kamu düzenini korumaktır. Kolluk faaliyetleri kamu gücüne dayanan idarenin tek yanlı düzenleyici ve bireysel özellik gösteren emir ve yasaklarının tek yanlı uygulanması ile tezahür eder.[234] Buna karşılık kamu hizmeti vatandaşlara bir hizmet sunmak biçiminde ortaya çıkar. Bazen her iki tür hizmet ve kolluk faaliyeti birlikte söz konusu olabilir. Örneğin umumi helâları kamu idareleri hem temizler ve aynı zamanda temiz tutmayanlar hakkında bazı kurallar koyarak, ihlal halinde bu kuralların öngördüğü cezaları uygular.[235]

Kişisel verilerin toplanmasında önemli aktörlerden biri de şüphesiz kamu görevlileri olacaktır. O halde kamu görevlileri kimlerdir. Geniş anlamda kamu görevlisi deyimini kamu kesiminde görev yapan, hukuksal durumları birbirinden farklı olan tüm görevlileri kapsar. Özetle kamu kesiminde çalışan herkes kamu görevlisidir.[236]

Dar anlamda kamu görevlisi ise Anayasamızın 128. maddesinde yer alan kamu kurum ve kuruluşların genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği asli ve sürekli görevleri yürüten kişileri ifade etmektedir. Dar anlamda kamu görevlisi kavramının içinde özel hukuka tabi kamu idareleri çalışanları ile devletin siyasal yapısı içersinde yer alan çalışanlar kamu görevlisi değildir.[237]

İdare açısından kişisel verilerin genel olarak idari işleme konu olması nedeniyle burada idari işleminde ne olduğu ve bu kavramdan ne anlaşılması gerektiği üzerinde kısaca durmakta yarar bulunmaktadır. İdari işlem idarenin hukuki sonuç doğurmaya yönelik bir irade açıklaması olarak tanımlamak yerinde olacaktır.[238] İdari işlemin bu tanımdan çıkan bir irade açıklaması ve ikincisi de bu açıklamanın maddi olarak tezahürü bulunacaktır. Konumuz açısında ele aldığımızda örneğin nüfus sayımı için idarenin değişik nedenlerden dolayı vatandaşların nüfusunu öğrenmek için bir irade beyanında bulunmakta ve bunun sonucu olarak da bu iradenin tezahürü olarak görevlileri aracılığı ile sayım işlemi yaptırmaktadır. Bu işlem sırasında da tek tek vatandaşların kişisel verileri toplanmakta ve işlenmektedir.

---

[233] Birsen Çırakman, **"Kamu Hizmeti",** Amme İdaresi Dergisi, Cilt: 9, Sayı:4,Ankara, Aralık,1976,s.75
[234] Gözler, Kemal, C.2, s.216
[235] Gözler, Kemal, C.2, s.216
[236] Gözübüyük, a.g.e., 116
[237] Gözübüyük, a.g.e., 117
[238] Gözler, Kemal, İdare Hukuku Dersleri, Ekin Kitabevi, 3. Baskı, Bursa 2005, s.198

Ancak Devletin yaptığı tüm işlemler idari işlem olarak ele alınmaz. Anayasanın 40. maddesinde bu anlamda yanlış bir düzenleme yapılmış ve idari işlemler devlet işlemleri olarak düzenlenmiştir. Devlet işlemi devletin her türlü kurumunun yaptığı işlemlerdir. Örneğin yasama işlemleri, yargı işlemleri de devlet işlemleri arasındadır.[239]

Kamusal örgütlerin vatandaşların ihtiyaçlarını karşılamaya yönelik hizmet sunumu yöntemlerine geçmeleri kaçınılmaz duruma gelmiştir. Kamu yönetimi etkililiğe, verimliliğe ve yurttaşların insan olarak gereksinmelerini sağlamaya yönelik, yönetsel uygulamalara başvurmalıdır. Sekizinci Beş Yıllık Kalkınma Planının Dokuzuncu Bölümünde yer alan Madde 1836'da "kamu hizmetlerinin sunumunda vatandaşın memnuniyeti esas alınmak suretiyle, hizmet kalitesine ve sonuçlara odaklanarak, kamu yönetiminin etkinliğini ve halk nezdinde güvenirliğini geliştirmek esas olacaktır"[240] ifadesi de bu çerçeveyi desteklemektedir.

Yönetim anlayışının, kamu yönetim reformları ya da yeniden yapılandırma girişimleri için taşıdığı anlam açıktır. Kamu yönetiminde egemen olan klasik yönetim anlayışı, yerine giderek iş dünyasının toplam kalite ve müşteri memnuniyeti hedefleriyle iş gören paydaşların katılımına dayanan bir anlayışa bırakmış, beklentileri artan vatandaş memnuniyeti "müşteri memnuniyeti" olarak görülmeye başlanılmıştır. Kamu idarelerinin faaliyetleri kalite standartlarının sürekli olarak arttırılması gereken "hizmetler" olarak kabul edilmeye başlanılmıştır. Kamu politikalarının üretim süreçlerine yurttaş katılımından başlayarak kamu yönetiminde etkili ve verimli hizmeti sosyal adalet ve eşitlik kıstaslarıyla buluşturacak bir yeniden yapılanmada vatandaşla devleti buluşturan elektronik devlet ve bunun hukuk altyapısı ve merkezi veri tabanları önemli rol oynamaktadır. e-Devlet, elektronik idare özü itibariyle bir ağ yönetişimidir.

Kamu yönetiminde ortaya çıkan yeni arayışlarda yönetimde etkinliği ve verimliliği sağlamak temel belirleyici unsurdur. Yönetime sonuca yönelme ve performans değerlendirmesinin bir diğer nedeni de, etkin ve verimli bir yönetim yapısı oluşturmaktır. [241] Sanayi toplumu yapısından bilgi toplumu aşamasına geçişte önemli işlevler üstlenen yeni teknolojiler, kamu yönetiminin yeniden yapılanmasında ve kamu hizmetlerinin etkin ve verimli şekilde yürütülmesinde önemli rol üstlenmişlerdir. Bilgi teknolojiler, organizasyonların yapısını, kurum içi ilişkileri değiştirmekte ve bu durum kişisel verilerin büyük networkler aracılığı ile sürekli alış veriş trafiğine muhatap olmasına neden olmaktadır.[242]

---

[239] Atay, Ethem, **Genel İdari Usul Kanunu Tasarısı Sempozyumu**, Türk Hukuk Dergisi, Mayıs 2004, Özel 87. Sayı, s. 20
[240] www.dpt.gov.tr./http//e.kutup.dpt.gov.tr. (01.11.2005)
[241] Al, Hamza **Bilgi Toplumu ve Kamu Yönetiminde Paradigma Değişimi,** Bilim Adamı Yayınları, Ankara,2002, s.253
[242] Al, **a.g.e.,** s-256-257

E-Devlet, kamunun hizmet verdiği alanlarda bilgi ve iletişim teknolojileri kullanılması yoluyla daha şeffaf, vatandaşa daha yakın, daha ucuz ve daha iyi çalışan bir idari yapı olarak düşünülmekte ve geleceğin devleti olarak ön plana çıkmaktadır. "Bilgisayar ve iletişim teknolojilerinin kamu yönetiminde kullanımının artışına koşut olarak, devlet etkinliklerinin boyutları da giderek genişlemektedir."[243] Diğer taraftan da bu husus vatandaşların kişisel verilerinin daha çok işlenmesi ve kayıt altına alınmasına yol açmakta ve bu verilere daha kolay ve hızlı bir şekilde ulaşılabilmenin imkanı ortaya çıkmaktadır.

E-Devlet kavramının tanımı "iç ve dış iş süreçlerinin yeni iletişim teknolojilerinin (İnternet'tabanlı teknolojiler gibi) hükümet işlevini daha etkin ve verimli olarak adalet ve eşitlik prensipleri çerçevesinde yerine getirerek vatandaş odaklı hale dönüştürme işlemidir." Yine " Bir vatandaşın herhangi bir kamu birimiyle olan herhangi bir etkileşiminin İnternet (world wide web) kullanılarak hizmet alımını bu yolla gerçekleştirmesi" veya " kamu hizmetlerinin mümkün olanlarının İnternet üzerinden vatandaşa sunma, evdeki bilgisayarlar aracılığı ile vatandaşların kamu hizmetleri hakkında bilgi sahibi olması, belli işlemler için müracaat edebilmesi, formları doldurabilmesi" diğer iki tanımdır. "Devletin vatandaşlara karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesidir" şeklinde de tanımlanmaktadır. [244].

5.7.3 AB'de Kamu İdareleri Tarafından Kişisel Verileri İşlenmesi

1960'lı yıllardan itibaren Amerika'da kişisel mahremiyet konusunda özel bir hassasiyet ortaya çıkmaya başlamış ve kişilerin yalnız kalma hakları olduğu ve bu haklarından dolayı özel hukuklarına ilişkin alanın hukuk düzeni tarafından daha sıkı bir şekilde korunması gereği üzerinde durularak ortaya ilk kişisel verilerle ilgili düzenlemeler çıkmaya başlamıştır.

1970'li yıllarda ortaya çıkan bu kişisel veriler hukuku veya kişisel mahremiyet hukuku Avrupa kıtasında da gündeme gelmeye başlamış ve hukuki düzenlemelerin konusu olmuştur.

Özellikle son on'lu yıllarda teknolojinin hızla ilerlemesi, kitle iletişim araçlarının yaygınlaşması ve yaygınlaşan bu araçlar sayesinde kişilerle ilgili bilgilerin yaygınlaşması ve erişiminin çok kolaylaşması bu verilerin hukuka aykırı olarak yetkisiz ve çoğu zaman kötü niyetli kişilerin eline geçmesine neden olmaya başlamıştır. Kişisel verilerin üzerindeki hâkimiyet konusunda o kadar çok hassasiyet ve korku ortaya

[243] Ergun, a.g.e., s.137
[244] http://www.milliemlak.gov.tr/_projelerimiz/e_devlet/e_devlet_yazi.htm (01.02.2006)

çıkmıştır ki, bu korku romanlara konu olmuştur. George Orwell 1949 yılında yayınlanan 1984 isimli romanında gelişen bilgi teknolojileri sayesinde Big Brother'ın herkesi gözetlediği ve kişiler hakkında her türlü bilgileri toplayarak bu kişiler üzerinde hâkimiyet kurduğu teması işlenmiş ve özel hayatın gizliliği gibi temel hakların ihlali karşısında toplumu bilinçlendirme yolunda yayınlar yapılamaya başlanmıştır.[245]

Bu şekilde serüvenine başlayan kişisel verilerin korunması hukuku, bilişim teknolojilerinin hızla ilerlemesi sayesinde sürekli değişen dinamik ve gelişen bir alan olarak karşımıza çıkmıştır. [246]

Diğer taraftan idare hukuku diğer hukuk dallarından ayrı olarak iki usul alanına sahip olduğu ve bunların birincisi idari usul ki "olaydan önce" uyulması ve dikkat edilmesi gereken bir usul dalıdır ve daha ziyade idari işlem sırasında kişisel verilerin korunması ve işlenmesi süreçleri ile alakalıdır. Daha çok bilinen usul ise idari yargıla usulüdür ki bu da "olaydan sonra" konumundadır.[247]

Kişisel verilerin koruması hukukunun ortaya çıkıp hızla gelişmesinin bir sebebi de özellikle batı kültüründeki bireyin toplum karşısındaki öne çıkışı ve ferdiyetçiliğin giderek etkisini artırmasıdır.

AB elektronik çağa geçmeye çalışırken ABD tıpkı e-ticaret alanında olduğu gibi çoktan yol almış ve yasal düzenleme gerektiren alanlarda çok tan yol almıştı. Örneğin bilgi çağının önemli öğesi kamu sektörünün elindeki bilgilere erişiminin ve ekonomik amaçlarla yeniden kullanımını önceliğe alarak bilgi özgürlüğü alanındaki düzenlemelerini gerektiği kadarıyla uygulamaya sokmuştu.[248]

Diğer taraftan Kişisel Verilerin Korunması Hukuku bakımından 1980 tarihinde OECD tarafından kabul edilen bağlayıcı olmayan kişisel verilerle ilkeleri de burada anmak gerekir.[249] Aynı şekilde Avrupa Konseyinin 28 Ocak 1981 tarihli 108 no'lu sözleşmesi "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" üye devletlerin hâkimiyet alanında kişisel alanın korunmasın hedefleyerek kişisel verilerle ilgili yeknesak bir hukuk düzeni ortaya koymak üzere bir sözleşme addedilmiş[250] ve bu sözleşmeyi Türkiye de 28.01.1981

[245] Başalp, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayımevi, Ankara 2004, s.21
[246] Başalp, a.g.m., s..7
[247] Akıllıoğlu, Tekin, İdari Usul ve Kişisel Verilerin Korunması, www.idare.gen.tr/akkillioglu-idariusul.htm (11.04.06)
[248] Tansuğ, Avniye, **a.g.m.,**.55
[249] Akıllıoğlu, Tekin, İdari Usul ve Kişisel Verilerin Korunması, www.idare.gen.tr/akkillioglu-idariusul.htm (11.04.06)
[250] Tansuğ, a.g.m., s.56

tarihinde imzalamıştır. Fakat ne varki bu tarihten bu yana Türkiye bu sözleşmeyi onaylayarak yürürlüğe sokmamıştır.[251]

Aynı şekilde Birleşmiş Milletler 1990 yılında kişisel verilerle ilgili "Bilgisayarla İşlenmiş Kişisel Veri Dosyalarıyla İlgili Rehber İlkeler" adlı düzenlemeyi kabul ederek bu konuda asgari bir standart getirmeye çalışmıştır.

5.7.4 Genel Olarak Kişisel Verilerin İşlenmesi Konusundaki AB'deki Gelişmeler

AB sürecinde özellikle AB anlaşmasının 6. maddesinin ikinci fıkrasıyla üye devletlerin ortak anayasal geleneklerinden kaynaklanan ve topluluk hukukunun genel prensiplerinden temel haklara saygı özel bir yere sahiptir. Bu anlamda AİHS'nin 8. maddesi gereğince özel ve aile hayatı özel bir koruma altına alınmıştır.

AİHS'nin Avrupa Toplulukları Mahkemesi de bu temelden hareketle çeşitli kararlarında kişisel verilerle ilgili kararlar vererek bu hukuku ve verilerin gizliliği, özel hayatın korunması kavramını kabul ederek bu konuda mevzuat düzenlemesi karşısında önde gitmiştir. 90'lı yıllarda ise kişisel verilerin korunması konusunda Avrupa Birliği'nde ilk tasarılar ortaya çıkmaya başlamış ve uzun çalışmalar sonunda 24 Ekim 1995 tarihinde Avrupa Parlamentosu ve Konseyi "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi" ni kabul etmiştir.[252] Kabul edilen bu Yönerge ancak 1998 yılında yürürlüğe girebilmiştir. Böylece AB'de serbestçe dolaşan hizmet, sermaye ve malların aksine kişisel veriler serbestçe dolaşamaz olmuştur.[253] Bu yönergelerle birlikte de artık özel hayatın gizliliği ile kişisel bilgilerin gizliliği arasında kalın bir duvar örülerek birbirlerinden ayrılmışlardır.

Bu direktifi desteklemek maksadıyla eksik kalan alanlarda Avrupa Parlamentosu ve Konseyi 1997 yılında "Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesini" yürürlüğe koymuştur. Bu yönerge 97/66/EG nolu yönerge ismini almıştır.[254] Daha sonra da AB bu Yönergeyi tamamlayan 2002/58/EC Sayılı "Özel Hayatın Korunması ve Elektronik İletişim Yönergesi"ni de ileri teknolojik ortamlardaki ilişkileri de kapsayan yeni bir veri saklama hukuku olarak ortaya koydu.[255]

AB'nin sıkı takibi ve ısrarı ve nihayet AB ile ABD arasında imzalanan "Safe Harbours" sözleşmelerinin uygulanmasında yaşanan sıkıntılar nihayet ABD'yi de harekete geçirdi ve Senatoya Başkanlık OPPA (Online Privacy Protection Act, 2005)

---

[251] Başalp, a.g.m., s..24, Akıllıoğlu, Tekin, İdari Usul ve Kişisel Verilerin Korunması, www.idare.gen.tr/akkillioglu-idariusul.htm (11.04.06)
[252] Tansuğ, Avniye, **a.g.m.,**.s.55
[253] Tansuğ, a.g.m., s.55
[254] Başalp, a.g.m., s..27
[255] Tansuğ, a.g.m., s.55

adında bir kanun taslağını gönderdi.[256] ABD ile arasında olan mevcut ilişkilere rağmen bu kadar sıkıntı çıkaran AB, Türkiye ile de arasında devam eden üyelik müzakerelerinde hayli hayli sıkıntı çıkarması beklenmelidir.

2001 yılında ise yine Avrupa Birliğinde kişisel verilerin korunması hakkı bir temel hak olarak Temel haklar ve hürriyetler şartının 8. maddesinde yerini almıştır. Ancak Avrupa Birliğine ısrarla kişisel verilerden ve bu verilerin korunmasından bahseden müktesebatın sanki amaç sadece verilerin korunmasıymış gibi bizi tehlikeli bir sonuca götürebileceği gözetilerek asıl amacın kişilerin korunması olduğu ve vurgunun da buna yapılması gerektiği belirtilmiştir.

5.7.5 Genel Olarak Kişisel Verilerin İşlenmesi Konusundaki Türkiye'deki Gelişmeler

Hukukumuzda Kişisel Verilerin Korunması Hukuku yakın zamanlarda giderek artan bir şekilde yerini almaktadır. Türk Medeni Kanunun 24 -27 maddeleri arasında kişilerin özel hayatı Medeni Hukuk açısından da koruma altına alınması, yeni Ceza Kanunumuzda kişisel verilerle ilgili maddelere yer verilmesi, 06 Şubat 2004 tarihinde yayınlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi Ve Korunması Hakkında Yönetmelik ve Adalet Bakanlığı tarafından hazırlanan Kişisel Verilerin Korunması Hakkında Kanun Tasarısı da göstermektedir ki bu etki giderek daha hızlı bir şekilde kendini gösterecektir.

Türkiye'de kişisel verilerin korunması hukuku daha çok Avrupa Birliği müktesebatına uyum sürecinde gündeme gelmiş ve bu konudaki çalışmalar sık sık Avrupa Birliği izleme raporlarında yer almaya başlamıştır.

Türkiye'deki kişisel verilerle ilgili bir başka kanun da Avrupa Birliği müktesebatına uyum kapsamında kişisel verilerin korunmasıyla yakından ilgili ve hatta bir madalyonun iki yüzü olarak tanımlanan Bilgi Edinme Kanunu olarak 4982 sayılı İdari Usül ve Bilgi Edinme Hakkında Kanun 09.10.2003 tarihinde Mecliste kabul edilmiş ve 24.04.2004 tarihinde yürürlüğe girmiştir. Bu kanuna göre kişiler kendileriyle ilgili her türlü idarenin tutmuş olduğu kişisel verilere ulaşabileceklerdir. Hatta bu kanuna dayanarak ülkemizde memurlar gizli sicil fişlerine dahi ulaşabilmektedirler.

Türkiye'de bazı Danıştay kararları da dikkate değer şekilde konuyu ele almışlardır. Örneğin Danıştay'ın Birinci Dairesi bir kararında kamu yönetimlerinin vergi sırrı bağlamında elde ettiği bazı kişisel verileri diğer kamu birimlerine iletmesini, kamu idaresinin bir bütün olduğundan bahisle verip veremeyeceği tartışılmış ve sonuç olarak bu veri gizliliğinin kişilerin buna duyduğu güven sayesinde vergi gelirlerini artırdığını

[256] Tansuğ, a.g.m., s.56; http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.84: (21.04.2007)

belirtmiştir. Ayrıca gizli belge ve bilgilerin sırf bu nedenle açıklanmaması gerektiğine karar vermiştir.[257] İdare İşleri Kurulundaki azınlıkta kalan bu görüşe göre vergi gizliliği Anayasanın 20. maddesindeki özel hayatın gizliliği kapsamında koruma görmelidir.[258]

Yine ilginç bir kararda Danıştay Avukatın müvekkiline ait istediği sicil dosyasını vermeyen idarenin İYUK madde 20/3 e göre haklı olduğunu ve fakat idarenin vermediği bu belgeye dayanarak savunma yapamayacağına ve yapsa bile hükme esas alınmayacağına karar vermiştir. Burada Danıştay'ın kişi lehine sicil raporunun, yani kişisel verilerin, ilgili şahsa verilemesi yönünde yorum yapmamasından dolayı eleştirilmiştir.[259]

Yine kişisel verilerle ilgili olarak Danıştay'ın özellikle güvenlik soruşturmalarıyla ilgili idarenin uygulamaları ile ilgili yasal bir düzenleme olmamasına rağmen isabetli kararlar verdiği ileri sürülmüştür.

5.7.6 AB Kişisel Veriler Koruma Mevzuatının Temel Özellikleri

Avrupa Birliği'nde yukarda da belirttiğimiz gibi Kişisel Verilerin korunması konusunda tüm üye ülkelerde yeknesak bir uygulamaya gitme konusunda özel bir gayret ve çaba görüyoruz. Zira ilk zamanlar üye ülkelerdeki kişisel verilerle ilgili farklı yasal mevzuat koruma düzeyi yüksel aleyhine bir gelişme göstermiş örneğin Almanya'daki bir takım masraflı ve zorlu yükümlülüklerin İtalyan Müktesebatındayer almaması nedeniyle Alman şirketlerinin İtalya'ya kayması gibi bazı haksız neticeler ortaya çıkarabilmekte idi. Bunu gören Avrupa Birliği çözümü AT anlaşmasının 7/a maddesi ve aynı anlaşmasının 94. maddesine dayanarak üye ülkeler arasında bir uyumlaştırma ve yeknesaklaştırmada aramıştır.

Avrupa birliğinin 95/46/EG direktifi temel olarak kişisel verilere gerek kamudan ve gerekse özel kişi ve kuruluşlardan gelecek saldırılara karşı önlem almak ve saldırı öncesi sistemli bir koruma ortaya koymak amacındadır.

Kural olarak 95/46/EG direktifi Türk Kişisel Verileri Koruma Kanun Tasarısı, Alman ve İsviçre Veri Koruma Kanunlarının aksine, kişisel verilerin korunması hususunda, özel ve kamu kesimi diyerek bir ayrıma gitmemiştir.

Almanya'da özellikle 1983 tarihinde Alman Anayasa Mahkemesinin nüfus sayımı kararında kamu idarelerine karşı kişilerin kişisel verilerini koruma haklarına sahip olmaları konusunda önemli ilkeler ortaya koyduğu göze çarpmaktadır. Bu kararı önemli kılan da kişilerin verileri bakımından kendi kaderlerini belirleme haklarına sahip

[257] Danıştay Birinci Daire, 20. 12 1984 tarih ve E. 1984/291, K. 1984/294 Sayılı Karar
[258] Akıllıoğlu, Tekin, İdari Usul ve Kişisel Verilerin Korunması, www.idare.gen.tr/akkillioglu-idariusul.htm (11.04.06)
[259] Akıllıoğlu, Tekin, İdari Usul ve Kişisel Verilerin Korunması, www.idare.gen.tr/akkillioglu-idariusul.htm (11.04.06)

olmaları ve Alman Anayasasının 2. maddesinde belirtilen bu hususun dayanak yapılarak Avrupa Hukukunda ilk kez kişisel verilerin korunması hukukunda idareye karşı bir takım kuralları ortaya konduğu ve kişinin devlete karşı korunduğunu görüyoruz. Artık idare gerekli gereksiz, belki ilerde lazım olabilir diye verileri toplayamayacak, ancak gerekli ve yeteri kadar veri toplayacaktır.[260]

Kişisel Verilerin Korunması Hukukunun gelişimine baktığımızda özellikle Amerika'da kişisel verilerin daha çok özel sektör alanında düzenlemelere ihtiyaç duyduğu ve fakat kamu sektörünün parlamentoya karşı sorumlu olması ve bu kurum tarafından denetleniyor olması karşısında daha az düzenlemeye muhatap olduğu ileri sürülmüştür. Ancak Avrupa Parlamentosu özelikle ABD'de ortaya çıkan bu gelişmenin aksine kişisel verilerin işlenmesi bakımından kamu idaresiyle özel sektör arasında herhangi bir ayrıma gitmeyerek her iki kesimi de aynı mevzuata tabi kılmıştır. Avrupa Birliğindeki bu süreçle birlikte gittikçe kabul edilen düşünce de artık kişisel verilerin korunması konusunda ihlali işleyenin kimliğine bakılmaksızın aynı kurallara tabi olması düşüncesidir.

Yine Avrupa Birliğinde kişisel verilerin korunması konusunda kamu kurumlarıyla özel kurumlar ve kişiler arasında herhangi bir ayrım yapılmamış ise de kişisel verilerin işlenmesindeki hukuka uygunluk sebepleri sayılırken bir istisna da kamu menfaati veya kamu düzeni gereği kişilerin kişisel verilerini herhangi bir izin alınmaksızın işlenebileceği kabul edilmiştir. Bu da bize her ne kadar kamu özel ayrımı yapılmasa da doğal olarak kamu idaresinin doğasından kaynaklanan ihtiyaçlar nedeniyle genel kuraldan ayrılmaların olduğunu göstermektedir.

5.7.7 AB Kişisel Veriler Koruma Müktesebatında Kamu İdareleri İçin Tanınan İstisnalar

Avrupa Birliği kişisel verilerin korunması hukukunda özel kamu kesimi arasındaki bir fark da hassas veriler konusundadır. 95/46/EG sayılı direktifin 8. maddesinin birinci fıkrasında düşünce özgürlüğüne ilişkin, sağlık, politik görüş, cinsel tercih gibi sayılan hassas kişisel verilerin işlenmesi kesinlikle yasaktır. Ancak yine aynı direktifin 7. maddesinde hassas kişisel verilerin bazı durumlarda idare veya kişiler tarafından işlenebileceği belirtilmiş ve tek tek sayılarak istisnaları sayılmıştır.

Bu istisnalardan bazıları yine kamu idaresi için öngörülmüş olup kamuya yararlı kurum ve kuruluşlar tarafından bazı kişisel veriler işlenebilecektir. Yine direktifin 8. maddesinin ikinci fıkrasında belirtildiği üzere kişinin kendisi tarafından açıklanan hassas kişisel veriler idare tarafından işlenebilecektir. Yine idareyle ilgili özel bir istisna direktifin 8. maddesinin dördüncü fıkrasında üye devletlere yeterli garantinin tanınmış

[260] Garstka, Hansjürgen, 25 Jahre Datenschutz 5 Jahre Informationsfreiheit in Berlin, Berlin, 2004, s.14

olması şartıyla yapılacak bir düzenlemeyle önemli kamusal yararların korunması amacıyla ve gerekçesi belirtilmek şartıyla kişisel verileri işleyebilecektir. Yine idare Avrupa Birliği 95/46/EG sayılı direktifinin 8. maddesinin beşinci fıkrası gereğince suçlara verilen cezalara ve emniyet tedbirlerine ilişkin hassas kişisel verileri işleyebilecek ve gerektiğinde kullanabilecektir.

Yine idare hassas kişisel verilerle ilgili vatandaşların ulusal kimlik numaralarıyla birlikte bazı kişisel verilerin düzenlenecek olan kurallar çerçevesinde kullanması hukuken mümkün olacaktır. Yine yargılama nedeniyle işlenen hassas kişisel veriler, tıbbi tedbirler çerçevesinde işlenen kişisel veriler, iş hukuku çerçevesinde işlenen bazı veriler ve kişinin rızası doğrultusunda işlenen hassas kişisel veriler bu istisnanın diğer kapsamı içinde olan hususlardandır.

Direktifin 10. maddesi gereğince bu istisnalar kapsamında işlenen kişisel veriler konusunda ilgili kişilere bildirilecek ve bu bilgiler soyut bir bilgiden ziyade kaynağıyla birlikte somut olarak zikredilecektir.[261]

Avrupa Birliğinde anılan direktifin 12. maddesiyle kişilerin kendileri hakkında tutular kişisel verileri öğrenme hakları güvence altına alınmıştır.

Yine Avrupa Birliği direktifinde idare kişisel verilerin üçüncü kişilere transferi konusu olan veri veya veri kategorilerinin yani iş tecrübesi, yabancı dil bilgisi veya ailevi ilişkiler gibi, yanısıra bunların kime verildiği de açıkça belirtilmelidir. Buna verileri ayırt etme zorunluluğu da denilmektedir. Ayrıca idare veri kütüklerinde bilginin kimden alındığını da açıkça ifade etmelidir.[262]

Avrupa Birliği direktifinin 14. maddesinde üye devletlere vatandaşların kendileri hakkında tutulan kişisel verilerin işlenmesine itiraz haklarının tanınmasını da bir yükümlülük olarak ortaya koymuştur. Ancak direktifin 7. maddesinin b, e ve f maddelerindeki gerekçelerle ulusal hukukta aksi açıkça öngörülmediği sürece korumaya değer nedenlerden dolayı verilerin işlenmesine itiraz edebileceklerdir. Ancak değindiğimiz gibi ulusal hukuklarda bunun aksi hükümler mevzuatta yer alabilir, fakat direktifin 8. maddesinin altıncı fıkrası gereğince bu istisnalara Avrupa Birliği Komisyonuna bildirme yükümlülüğü üye ülkelere getirilmiştir.

Yine Avrupa Birliği direktifinin 6. , 10., 11., 12. ve 21. maddelerinde devlet güvenliği ve ülke savunması, kamusal güvenlik, mesleki kurallara riayetsizlik ve suçların önlenmesi, Avrupa Birliğinin ya da üye ülkenin ekonomik çıkarlarının zedelenmesi veya son üç halden dolayı sürekli veya süreli kamusal gücün kullanılmasını gerektiren hallerin varlığı, ilgilinin ve kişilerin hak ve özgürlüklerinin

[261] Başalp, a.g.m., s..48
[262] Başalp, a.g.m., s..49

korunması ve son olarak da bilimsel araştırma ve istatistik çalışmaları nedeniyle kişisel verilerin işlenmesinde sınırlayıcı tedbirler ulusal düzenlemelerde yer alabileceği direktifin 13. maddesinde açıkça tanınmıştır. Bu konu doktrinde bilgi edinme hakkının kişisel verilerin öğrenilmesi açısından bazı sınırlamalara neden olabileceği ve hukuka karşı hile amacıyla kullanılabileceği dile getirilmiştir.[263] Kanaatimizce belirli amaçlar için idareye tanınan bu tür istisnalar, idarenin doğası gereği geniş kullanması gereken yetkileri ile ilgilidir.

5.7.8 AB Kişisel Veriler Koruma Müktesebatında İşlem Gizliliği ve Güvenliği

AB Kişisel Verilerin Korunmasına ilişkin Direktifin 16. maddesi her türlü kişisel verilerle ilgili kayıtları ve işlemleri gizli olarak tutulmasını ve kural olarak açıklanmamasını emretmektedir. İdare kişilerle ilgili verileri mevzuat ve talimatlara uygun olarak gizli olarak işlemeli, işlem gizliliğine riayet etmelidir. Ancak iç hukuk gereği bir kişisel verinin yetkili makam veya kişiler tarafından istendiğinde verilmesi hadisesinde işlem gizliliği ileri sürülerek bilginin verilememesi yoluna gidilemeyecektir. Bu durumda idare yasadaki düzenlemeye istinaden istenen veriyi ilgili kişi veya kuruma vermesi yasal bir ödev haline gelecektir ki bu durum işlem gizliliği ilkesinin nitelikli bir istisnası sayılmalıdır.[264]

Kişisel veriler idareler tarafından işlenirken aynı zamanda muhtemel ihlal durumlarına karşı da her türlü tedbiri almakla yükümlüdürler. Bu tedbirler maddi olabileceği gibi, teknik te olabilir.[265] Verilerin saklandığı disklerin özel şifreli hale getirilerek üçüncü kişilerin erişimine kapalı hale getirilmesi bu duruma örnek olarak verilebilir. Alınan tedbirler ilgili kişi veya kurumlar tarafından kontrol edilmeli ve varsa eksiklikler giderilmelidir. Öte yandan alınacak tedbirlerin sınırının tayininde idareye yüklenecek olan külfetin de göz önünde bulundurulması gerekmektedir. Bu aynı zamanda Direktifin 17. maddesinin de bir gereğidir.

5.7.9 AB Kişisel Veriler Koruma Müktesebatında İş Görme Yoluyla Verilerin İşlenmesi

Daha önce de bahsettiğimiz gibi kamu hizmetleri, bir kamu kurumunun ya kendisi tarafından ya da yakın gözetimi altında özel girişim eliyle yerine getirilebilir[266] İşte bu durumda yani bir idare adına özel bir teşebbüs kişisel verileri toplama veya işleme işlemini yerine getiriyorsa o takdirde; ilk olarak sorumlu idare ile iş görme yoluyla verileri işleyen kişi veya kurumlar ararsında hukuki bir işlem çerçevesinde bir yetkilendirme olmalıdır**.** İkinci olarak da iş görme yoluyla verileri işleyen kişi işi veren idarenin talimatlarına uygun davranmalıdır. Üçüncüsü ise iş görme yoluyla verileri

[263] Başalp, a.g.e, s.54
[264] Başalp, a.g.e ,s.55
[265] Başalp, a.g.e ,s.55
[266] Gözübüyük, a.g.e., s.235

işleyen kişiler bulundukları ülkenin iç hukuklarına göre Direktifin 17. maddesinde sayılan tedbirleri almalıdır.[267] Son olarak ise sorumlu idare ile iş görme yoluyla verileri işleyen kişi veya kurumlar arasında verilerin ne şekilde işleneceğine ilişkin bir mutabakat belgesi olmalıdır. [268]

5.7.10 AB Kişisel Veriler Koruma Müktesebatında İdarenin Bildirim Yükümlüğü

Veri Koruma Direktifinin 18 maddesine göre kişisel verileri toplayan veya işleyen idare veya onun temsilcisi verilerin kısmen veya tamamen otomatik işlenmesinden veya belirli bir amaca yönelik birçok işlemin gerçekleştirilmesinden önce Direktifin 28. maddesinde düzenlenen kontrol birimine bir bildirimde bulunmak zorundadır. Bu bildirimin amaçlarını hem kontrol hem de açık bir görev yapma ortamını sağlamak olarak sayabiliriz[269].

Direktifin 18. maddesinin 2. fıkrasına göre idarelerin belli şartlarda ilgili kontrol örgütüne otomatik olmayan veri toplama işlemlerinde bildirimde bulunma zorunluluğunu ortadan kaldırabileceklerdir.

İdare Direktifin 19. maddesine göre ilgili kontrol birimine idarenin sorumlusunun adı ve soyadını, işlemin gerçekleştirilmesinde güdülen amaç, ilgililerin dâhil olduğu kategoriler ve buna ilişkin veriler ve bu verilerin dâhil olduğu kategoriler bulunmalıdır. Ayrıca verilerin verileceği kişi veya kurumlar ile bunların kategorileri, varsa üçüncü ülkelere yapılacak veri transferleri, işlemlerin güvenliği için alınan tedbirler kontrol makamına mutlaka iletilmelidir.

İdarenin topladığı verilerde bir değişiklik bulunması halinde bu değişikliklerin ne şekilde kontrol birimine bildirileceği üye ülkeler tarafından belirlenecektir. Bu konuda Direktif yetkiyi üye ülkelere bırakmıştır. Burada üye ülkeler genelde bürokratik yükten kaçınmakta ve yılda bir kez değişen verilerin ilgili yerlere bildirilmesini istemektedirler.[270]

5.7.11 AB Kişisel Veriler Koruma Müktesebatında İdarenin Bildirim Yükümlüğünün Muafiyet Halleri

Direktif bazı hallerde bütün veri toplayanların yanı sıra idarelere de **Bildirim Yükümlüğüne** özel bazı istisna hükümleri getirmiştir. Zararsız kişisel verileri toplayan idare örneğin bunun için kontrol birimine bildirimde bulunmak zorunda olamayacaktır. Yine işin mahiyeti icabı etraflıca korunan veriler yine bildirim yükümlülüğünün kapsamı dışındadır. Mesela müşterilerinin bilgilerini meslek sırrı icabı korumak zorunda olan avukatın bu mecburiyeti yasal bir zorunluluk olduğu ve ihlali halinde ceza kanuna göre

[267] Başalp, a.g.e., 56
[268] Başalp, a.g.e., 57
[269] Başalp, a.g.e., 57
[270] Başalp, a.g.e., 58

suç teşkil edebileceğinden ayrıca bunun bildirim yolu ile korunmasına çok gerek görülmemiştir.[271] Üye ülkelerde genelde kontrol birimleri her sene ne tür bilgilerin zararsız veriler olduğu ve bildirim yükümlüğünden muaf olduğu ilan edilmektedir. Örneğin Fransa'da elektrik, su faturaları için toplanan verilerin zararsız veriler olduğuna kontrol birimi karar vermiştir. Aynı şekilde hesap sahiplerinin kişisel verilerinin banka tarafından işlenmesi zararsız işlem olarak görülmüştür.

Kişisel veri işleyen idarelerin veri koruma görevlisi ataması da oto kontrol sistemin kurulması nedeniyle o kurumu bildirim yükümlülüğünden kurtarmaktadır. Örneğin Alman Verilerin Korunması Kanunun 4. maddesine göre kurularında veri koruma memuru atayan idareler artık kontrol ve denetimleri bu kontrolörler tarafından yapmakta ve bildirim yükümlüğünden muaf olmaktadırlar.[272]

Yine tapu sicilleri gibi umuma açık sicillerle ilgili veriler ayrıca kontrol birimine bildirilmesine gerek yoktur.[273]

5.7.12 AB Kişisel Verileri Koruma Müktesebatında Veri Koruması Denetim Organları

AB Kişisel Verilerin Korunması Direktifinin 28. maddesinde üye devletlerden yeni bağımsız bir kontrol biriminin kurulmasını istemektedir. Bu birimin genel görevi kişisel verilerle ilgili mevzuatın uygulamasını takip etmek ve zaman zaman bu konularda rapor yayımlamak olacaktır. KVK Direktifini iç hukukuna aktaran tüm üye ülkeler bu maddenin öngördüğü kontrol birimini kurmuşlardır.[274]

5.8 Türkiye'de Kamu İdareleri Tarafından Kişisel Verileri İşlenmesi

5.8.1 Türkiye' Kişisel Veriler Müktesebatı İle İlgili Yapılan Çalışmalar

Yukarıda da belirttiğimiz gibi Avrupa Konseyinin 28 Ocak 1981 tarihli 108 no'lu sözleşmesi "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" üye devletlerin hâkimiyet alanında kişisel alanın korunmasın hedefleyerek kişisel verilerle ilgili yeknesak bir hukuk düzeni ortaya koymak üzere bir sözleşme addedilmiş[275] ve bu sözleşmeyi Türkiye de 28.01.1981 tarihinde imzalamıştır. Fakat ne var ki bu tarihten bu yana Türkiye bu sözleşmeyi onaylayarak yürürlüğe sokmamıştır.[276]

Ancak AB üyelik sürecinde kişisel verilerle ilgili düzenlemelerin iç hukukumuza aktarılması konusunda ülkemiz giderek yoğunlaşan bir talep ile karşı karşıya kalmaktadır. Nitekim AB'nin Türkiye için hazırladığı 2005 Yılı İlerleme Raporunda veri

[271] Başalp, a.g.e., 58
[272] Başalp, a.g.e., 59
[273] Başalp, a.g.e., 60
[274] Bu konuda üye devletlerin kurdukları kontrol birimlerinin adı için bkz. Başalp, a.g.e., s.78
[275] Tansuğ, a.g.m., s.56
[276] Başalp, a.g.m., s..24, Akıllıoğlu, Tekin, İdari Usul ve Kişisel Verilerin Korunması, www.idare.gen.tr/akkillioglu-idariusul.htm (11.04.06)

koruması hukuku açısından, yeni Ceza Kanunundaki, kişinin siyasi, felsefi ve dini fikirleri, ırksal kökenleri, yasadışı ahlaki eğilimleri, cinsel hayatı veya başkalarının sağlık durumu veya sendikalarla ilişkisi hakkında yasadışı bilgi toplayan kişilerin hapis cezasına çarptırılmasını öngören hüküm içerdiği övgüyle vurgulanmıştır.

Öte yandan Ceza Kanununda ayrıca, kişisel verilerin dağıtımı ve yasal süre çerçevesinde imhasına ilişkin maddeler bulunduğu belirtilmiştir. Ayrıca Türkiye'nin Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunması Sözleşmesini imzaladığı özellikle belirtilerek Türkiye'nin bu antlaşmayı henüz onaylamadığına vurgu yapılmıştır. Son olarak ta Türkiye'de, kişisel verilerin korunmasına ilişkin kuralların uygulanmasını sağlayacak kurumsal çerçevenin kilit bir unsuru olarak veri muhafazasını denetleyecek bağımsız bir kurum oluşturması tavsiye edilmiştir.[277]

Bu tavsiyeler dikkate alınarak Adalet Bakanlığı tarafından 13.09.2005 tarihinde Kişisel Verilerle ilgili bir komisyon kurmuştur. Zaman zaman çalışmalarına ara veren bu komisyon dağıtılarak yeniden 18 Eylül 2000 tarihinde yeni bir komisyon oluşturulmuştur. Daha sonra üç sene çalışsan bu komisyon nihayet 2003 yılında "Kişisel Verilerin Korunması Kanunu Tasarısı" adı altında bir tasarı kabul ederek kamuoyunun huzuruna çıkarmıştır.[278] O yıldan bu yana birkaç kez Adalet Bakanlığı ile Başbakanlık arasında gidip gelen bu tasarı son olarak Adalet Bakanlığında bazı değişiklikler yapılarak TBMM sevk için 09.11.2005 tarihinde Başbakanlığa gönderilmiştir[279].

Tasarı AB Direktifini izlemeyerek Almanya örneğini esas alarak, kamu ile özel kişilerin veri işlemesinde farklılık yaparak ayrı ayrı başlıklarda düzenleme yapmıştır. Tasarı 13. maddesinden itibaren Gerçek ve Özel Hukuk Tüzel Kişilerin kişisel verileri işlemesini düzenlemiş, 16. maddeden itibaren de Kişisel verilerin kamu kurum ve kuruluşları tarafından işlenmesini ele almıştır. Bu maddelerde Tasarı hassas kişisel verilerin ne hallerde kamu tarafından işlenebileceğini düzenlemiştir. Yine maddenin devamında 17. maddede kamu kurum ve kuruluşlarının ne şekilde başka kurum veya kişilere aktarabileceği özel olarak düzenlenmiştir.[280]

Tasarı kamu kurum ve kuruluşları ayrı bir başlık altında düzenlemekle birlikte bu kurum ve kuruluşların neler olduğunu açıkça belirtmemiş ve tanımlamamıştır. Oysa örnek alınan Alman Verilerin Korunması Hakkındaki Kanunun 2. maddesinde hangi kurum ve kuruluşların adı geçen kanun anlamında kamu kurumu sayılacağı teker teker

[277] 2005 AB Komisyonu Tarafından Türkiye İçin Yayınlanan İlerleme Raporu , http://www.abgm.adalet.gov.tr/ (12.05.06)
[278] Başalp, a.g.e., s.108
[279] http://www.kgm.adalet.gov.tr/kisiselveriler.htm (21.04.2007)
[280] http://www.kgm.adalet.gov.tr/kisiselveriler.htm (21.04.2007)

sayılmıştır. 27. maddede ise Alman Yasa Koyucu kamu kuruluşu olmakla birlikte işletme sahibi kamu kurum ve kuruluşları bu işletmeleri nedeniyle işledikleri verilerde özel kurum ve kişilerin tabi olduğu hükümlere tabi kılınmıştır.[281]

Türk Kişisel Verilerin Korunması Yasa Tasarısında hangi kamu kurumlarının ve kuruluşlarının bu Kanun Tasarısı anlamında kamu kurumu sayılacağı belirtilmediği için kanaatimizce bu konuda yukarıda birinci bölümde açıklamaya çalıştığımız kamu kurum ve kuruluşları tanımı içinde yer alan tüm kamu kurum ve kuruluşları, kamu kurum statüsünde bu kanuna tabi olacaklar özellikle verilerin işlenmesinde daha geniş bir yetkiye sahip olacaklardır.

5.8.2 Türk Kişisel Verilerin Korunması Kanuna Yapılan Eleştiriler

Hazırlanan Tasarıya yapılan ilk eleştirilerden biri hassas verilerin özellikle idare tarafından işlenmesinin kural olarak yasaklanmış olduğunun özellikle vurgulanmamış olmasıdır. Zira Direktif bu konuda açık bir hüküm taşımaktadır.[282]

Aynı şekilde Alman Verilerin Korunması Kanununda da 13. madde de kural olarak hassas verilerin idare tarafından işlenmesinin yasak olduğunu ve ancak kanunun özel izin verdiği hallerde ki bu haller teker teker sayılmıştır; Bunlar önemli bir kamu yararının mevcudiyeti, ilgilinin rızası, ilgilinin veya üçüncü bir kişinin hayati çıkarlarının mevzubahis olması, veri sahibinin bu verileri alenen açıklamış olması, kamu güvenliği için önemli bir saldırının defi için, sağlık gerekleri nedeniyle, bilimsel araştırmalar yapılması, ülke savunması için kaçınılmaz hale gelmesi halleridir.[283] Türk Kanun Tasarısında hassas veriler konusunda sayılan eleştirilerin eksik olması, Direktifte ve Alman Kişisel verilerin Korunması Kanununda sayılan istisnaların tam olarak Tasarıya alınmamış olması sonucu ortaya çıkmaktadır.[284] Tasarının 16. maddesine göre sayılan istisnalar sadece dört adettir ve bunar kişinin rızası, alenen zaten kişi tarafından açıklanmış olması, Bakanlar Kurulunun iznidir. Bu da ilerde idare açısından yapılan işlemler sırasında sıkıntı çıkarabilecek özelliktedir.[285]

Yine tasarıya yöneltilen eleştirilerden bir başka önemlisi de ilgilinin AB Direktifinin aksine sadece özel hukuk tüzel kişisi ise itiraz hakkının tanınmış olmasıdır.[286] Yani Tasarıya kişi idareye karşı kişisel verilerle ilgili bir itirazda bulunmayacaktır. Kaldı ki Direktif kamu ile özel kuruluşlar ve kişiler arasında bir ayırım yapmamaktadır.[287]

---

[281] Bundesdatenschutzgesetz, 5. Baskı, Berlin, 2004
[282] Başalp, a.g.e., s.138
[283] Bundesdatenschutzgesetz, Berlin, 5. Baskı, Druckerei Conrad, Eylül, 2004
[284] Başalp, a.g.e., s.138
[285] Bilgi Toplumuna Doğru, Türkiye 2. Bilişim Şurası Sonuç Raporu, Ankara 2004, s.297
[286] Bilgi Toplumuna Doğru, Türkiye 2. Bilişim Şurası Sonuç Raporu, Ankara 2004, s.297
[287] Başalp, a.g.e., s. 138

Yine Tasarı ile kurulması öngörülen Kontrol birimi bağımsız ve tam mesai ile çalışanlarının çalışması gerekirken, bu düzenlemeden sapmış ve kurumun tam bir bağımsız kuruluş olarak düzenlememiştir. Bunun da giderilmesi ve kontrol kurumunun idareden bağımsız bir yapı arz etmesi için tasarının yeniden ele alınması istenmiştir.[288]

Kişisel verilerin korunması konusu anlaşılmaktadır ki önümüz dönemde daha sık karşımıza çıkacak ve Türk hukuk sisteminde yerini alacaktır. Bir taraftan kişisel verilerle çok sıkı yeni kurallar getirmenin birçok bürokrasiyi de beraberinde getirdiği ve işleri daha da karmaşıklaştırdığı, o nedenle daha esnek bir yapı öneren ABD hukukçuları bir tarafta durmaktadır. Ancak diğer yandan AB'nin istek ve baskılarına dayanamayarak bu konuda Türkiye gibi AB ile uyumlu bir yasa taslağı hazırlayarak Senatoya sunan ABD gerçeği ise diğer tarafta durmaktadır.

Özellikle bilişim sistemlerinin kullanımının yaygınlaşması, her şeyin elektronik ortamda, İnternet vasıtasıyla halledilemeye çalışılması da ister istemez kişisel verilerin istek dışı global dünyaya hızla yayılması ve kişilerin özel hayatına müdahale imkanlarının ve kolaylığının gittikçe çeşitlenmesi, kişisel verilerin belli kurallar çerçevesinde işlenmesi ve nakli zorunluluğunu da birlikte getirmektedir.

Yoksa örneğin kötü niyetli kişilerin eline geçen mail hesabınız nedeniyle binlerce spam mailin posta kutunuzu devre dışı bırakması, ya da İnternet'te takip ettiğiniz trafiğin takip edilerek her türlü zaaf ve açıklarınızın bir şantaj olarak önünüze çıkarılması içten bile olmayacaktır.

Gerçi bunu Amerikanın gerek işletim sistemlerindeki bazı açık kapılar veya Truva atları ile yaptığı, hepimizin bilgisayardaki her işlemi veya izi big brother olarak izlediği ve artık özel hayatımızın sandığımızdan çok daha az bir alana münhasır kaldığı da iddia edilmektedir. Ancak her türlü sakıncasına rağmen giderek kullanımı artan elektronik ortamı güvenilir bir hale getirmenin bir şartı kişisel veriler ile birlikte bunun ayrılmaz bir parçası olan bilgi güvenliği çalışmalarıdır.

6 BİLİŞİM VE HUKUK USULÜ MUHAKEMELERİ HUKUKU

6.1 E-Belge Ve Elektronik İmzalı Belgelerin Delil ve Hukuki Niteliği

6.1.1 Giriş

Bu bölümde[289] genel olarak dünya ve Türk hukuk sisteminde elektronik imza uygulamaları üzerinde durulacak[290], Türk Hukuk sisteminde benimsenen güvenli

[288] Başalp, a.g.e., s.139

[289] e-İmza Konusunda daha geniş bilgi için bkz. TBD Kamu –BİB Kamu Bilişim Platformu VII, 26-29 Mayıs 2005 Antalya, Çalışma Grubu Raporları 1. Çalışma Grubu Nitelikli Sertifikasyon Alt Yapısı ve Yetkilendirme, s. 11 vd.

[290] "Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı" Ankara, 2006;7–8 Aralık 2006 tarihinde Ankarada yapılan Ulusal Elektronik Sempozyumu Elektronik İmza enine boyuna tartışılmış ve e-İmzanın hukuki boyutuna güvenli elektronik imzanın inkârı başlıklı makale ile katkıda bulunulmuştur. Yine Hukuksal

elektronik imza kavramı ve servis sağlayıcıları ile hukuki alt yapısı üzerinde durulacaktır. Ayrıca e-Belgenin ne olduğu, uygulamaları, Türk maddi ve ispat hukukundaki yeri üzerinde durulduktan sonra, e-imzanın ve güvenli e-imzalı belgelerin ispat hukuku açısından değerlendirmesi yapılacaktır.

İmza[291], bir yazının kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla metnin altına konulan isim veya işarettir. İmza, bir yandan kişinin hüviyetini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece imzalayanın metni okuyup anladığı ya da belgeyi bizzat hazırlayan kişi olduğu ve bağlanma iradesinin varlığı anlaşılır.

Borçlar Kanunu'nun 14'üncü maddesine göre imza, üzerine borç alan kimsenin el yazısıyla olmak zorundadır. İmza, kural olarak metnin altına atılmalıdır. Çıkıntılar, ilâveler varsa, bunlar da imzalanmalıdır. Aksi halde bunlar geçerli olmayacaktır.

Ancak teknoloji, hız ve sınır tanımayan bir olgu olduğu için, bütün dünya insanlarını 20. yüzyılda ilk önce " İnternet " adı verilen global ağ ile, daha sonra ise bu ağ üzerinden kendisinden kilometrelerce uzakta bulunan diğer bir kişi ile haberleşmek veya sözleşme yapmak için can atan kişilerin, bu işlemlerini bağlayıcı kılmalarını sağlayacak, kimliklerini ispata yarayacak " dijital imza " adı verilen bir imza türü ile tanıştırmıştır.

Elektronik imza altyapısı, bize, kimlik tespiti, bütünlük kontrolü ve inkâr edilemezlik gibi ıslak imza ile sağlanan fonksiyonların elektronik ortamda temin edilmesi için geliştirilen bir yöntemdir. Elektronik imzanın yakın bir zamanda günlük yaşamımıza gireceği ve yaşamın ayrılmaz bir parçası olacağı konusunda yalnız uzmanlar değil; pekçok kişi görüş birliği içindedir. Çünkü, güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden söz etmek mümkün değildir. Bu gereksinim, yalnızca şirketler, kurum veya kuruluşlar için değil, aksine elektronik ortamda hukuken bağlayıcı işlemler yapmak isteyen herkes bakımından söz konusudur.

Elektronik imza kanunu güvenli elektronik imzayı kabul etmiş ve bu çerçevede düzenlemeler yapmıştır.

---

bakımdan "e-İmza Uygulamalarında AB ve Türkiye'de mevcut durum ve öneriler başlıklı yazılar özellikle ilgi çekici olmuştur.

[291] İmza, genel olarak, bir belgenin doğruluğunu gösterme niyetiyle yapılan her türlü işaret olarak tanımlanabilir. İmza çok eski çağlardan beri değişik şekillerde kullanılmıştır. Örneğin Roma Hukukunda, bir sözleşmenin oluşturulabilmesi için, sözleşme yapan kişilerin mühür yüzüklerini balmumuna basarak metni mühürlemeleri gerekiyordu. Orta çağ boyunca Avrupa'da, belgeler, topraktan yapılmış mühürlerle mühürlenerek doğrulukları/güvenilirlikleri ispat edilmiştir. Daha sonraları, taraflar, el yazısı ile atılmış imzaları, sözleşmenin geçerliliğini ispat vasıtası olarak kullanmaya başlamışlardır.

Elektronik imzanın hukuk hayatımıza girmesiyle birlikte konuyla ilgili tartışmaların bittiğini söylemek mümkün değildir. Artık kanunun uygulanmasına ve uygulamada karşılaşılan sorunların çözümüne ilişkin tartışmalar başlamıştır.

Hukuk kuralları sosyal vakıanın ortaya çıkıp tamamlanmasını, hukuki problemin ortaya çıkmasını, teşkil ve teşhisini beklemek zorunda[292] olmasına rağmen, elektronik imzaya ilişkin yasal düzenlemeye bakıldığında, elektronik imzaya dair sosyal vakıa ortaya çıkmadan düzenleme yapıldığını görüyoruz. Elektronik imza kanunu düzenlemesi, bizim dışımızda gelişen sürecin kendimize uyarlamasından ibarettir. Böyle olunca da uyarlama sürecinde birtakım eksiklik ve yanlışlıkların ortaya çıkması kaçınılmaz olmuştur. Dahası uygulamanın sonuçlarını görmeden elektronik imza ile imzalanmış verilere hüküm ve sonuçlar bağlanmıştır[293].Uygulamanın ve getirdiği sorunları görmeden bir düzenleme yapmak tartışmaları ve uygulamda karşılaşılan sıkıntıları artıracaktır.

Teknik ve sayısal boyutu fazla olan elektronik imza, bir zorunluluk olarak ortaya çıkmasına rağmen henüz tam olarak anlaşılamamış ve kısa vadede anlaşılamayacaktır.

Teknolojinin gereği olarak ticaret hayatının da elektronik ortama taşınması ile birlikte birçok ülkenin mevzuatında, elektronik ticaretin benimsenebilmesi için açık ağ sistemine kullanıcıların güven duymasını sağlamak amacı ile hukuki düzenlemelerin yapılması gereği doğmuştur. Bu nedenle taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğunu, kurulacak olan teknik ve yasal alt yapı ile garanti edebilmek amacı ile elektronik imza kavramı ortaya çıkmıştır.

Bu gerekçelerle ülkemizde, kamusal alanda elektronik ticaret ile ilgili çalışmalar, Bilim ve Teknoloji Yüksek Kurulu'nun 25.08.1997 tarihli kararıyla Dış Ticaret Müsteşarlığı'nın koordinasyonunda Elektronik Ticaret Koordinasyon Kurulunun (ETKK) oluşturulmasıyla başlamıştır[294.] Yapılan çalışmalar neticesinde oluşturulan yasa tasarısı, 15 Ocak 2004 tarihinde kabul edilmiş ve 24 Temmuz 2004 tarihinde yürürlüğe girmiştir. e-imza uygulaması ise 18 Temmuz 2005 günü Telekomünikasyon Kurumu tarafından düzenlenen bir toplantı ile resmen başlamıştır[295].

---

[292] Kalpsüz,Turgut, Noterlik Hukuku Sempozyumu: III-IV-V (Noterlik Hukuku ile İlgili Bazı Sorunlar, Türk Hukuk Dili, Noterlik ve Tebligat Hukuku), Notev, Ankara 1999, s. 60-61.

[293] Deliduman,Seyithan,Elektronik Verilerin Delil Değeri, II.Türkiye Bilişim Hukuku Sempozyumu,28.05.2004,

[294] 8 Mayıs 1998 tarihli Dış Ticaret Müsteşarlığı, Elektronik Ticaret Koordinasyon Kurulu, Elektronik Ticaret Hukuk Çalışma Grubu Raporu

[295] Üney, s.1 www.bakernet.com/ecommerce

6.1.2 E-İmzanın Hukuksal Boyutu

Hukuk düzeni bir yandan belirli sembolleri imza değerinde görürken, genel kural olarak, geçerli bir imzanın, kâğıt üzerine elle yapılmış bir işaretleme olduğunu kabul etmektedir[296]. Mevcut hukuk düzenimizde, yazılı olması gereken akitlerde, borçlunun imzasının olması gerektiği Borçlar Kanununun amir hükmüdür. Aynı Kanunun 12-15. maddeleri, imzanın 'el yazısı ile' olması gerektiğini belirtmektedir. Sadece bu açıdan değerlendirildiğinde, kâğıt, mürekkep ve elle atılmış olma şartlarını taşımayan elektronik imza hukuksal bir geçerliliğe sahip olamayacaktır.

Ancak elektronik haberleşme teknolojilerinin yaygın şekilde kullanılması ve elektronik ticaretin tam bir hukuksal güvene kavuşturulabilmesi için, bu teknikler kullanılarak yapılan şifrelemenin veya kodlamanın geçerli bir imza sayılıp sayılmayacağı konusunun yeniden ele alınması gerekmektedir[297].

Bir belge, bir şahsın el yazısı ile imzasını taşıyorsa, bu, belgenin onun tarafından oluşturulduğuna karine teşkil eder. Aksinin ispatı imzalayana aittir. Burada kişinin imzasının bir başkası tarafından kolayca taklit edilemeyeceği ve kullanılamayacağı unsurlarına dayanılmaktadır. İkinci olarak imza, belge içeriğine ilişkin, imzalayanın niyetini ortaya koyar. Belgenin altında imzası bulunan kişinin belgenin içeriğine razı olduğu kabul edilir. Üçüncü özellik ise silinti ve kazıntı gibi bozulmalar olmadığı sürece, bu şekilde bir belgenin oluşturulmasını, imzalayanın istediğini ve belgenin gerçeklik ve doğruluğunu(bütünlüğünü) göstermesidir.

Elektronik imzalar, kriptografinin ve imzanın en son halkaları olarak günümüz hukuksal sorunları arasında, çözüm bulunmak üzere yerini almışlardır**.**

Elektronik imzaya ihtiyaç duyulmasının en önemli sebebi, hukuki işlemlerde güvenlik, kimlik tespiti, inkar edilmeme gibi özelliklerin sağlanmak istenmesidir.

6.1.3 Elektronik İmza

Elektronik imza, konuyla ilgili birçok çalışmada ve Avrupa Birliği Direktifi ve pek çok ülkelerin kanunlarında tanımlanmıştır. Elektronik imza bir üst kavramdır. Her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul edilebilir[298]. Ancak "sayısal imza,dijital imza" kavramı yerine kullanımına rastlamak da mümkündür[299]. Sayısal imzanın işlevi, elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal dokümanların olduğu şekilde, herhangi bir tahrip ve tahrife uğramaksızın iletilmesini

[296] Soydan Billur Y., E-İmza ve E-Belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk-1, Vergi Sorunları Dergisi, s.151, Nisan 2001, s.132
[297] Küçükközyiğit, Galip H; Elektronik Ticaret, Elektronik İmza ve Hukuk,2004.
[298] Alkan, Mustafa,İnalöz;Telekom Regülasyonları ve Elektronik İmzanın Elektronik Ticaret Üzerindeki Etkileri,TBD 21.Ulusal Bilişim Kurultayı Bildiriler Kitabı, Ankara 2004, s.111.
[299] www.turkpoint.com/e-yasam/sayisal imza.asp (01.12.2003)

sağlamaktır[300]. Bu nedenle sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir denilebilir.

Çeşitli ülkelerde yürürlüğe girmiş bulunan, yada girmek üzere olan yasa metinleri incelendiğinde dijital imza veya elektronik imza terimlerinden birinin seçildiği görülmektedir. Dijital imza aynı zamanda elektronik imzanın bir çeşididir. Elektronik imza kavramı içerisine el yazısı imzanın yerini, elektronik ortamda alabilecek bütün teknolojiler girmektedir. Örneğin, el yazısı imzanın orijinalinin scaner ile taranarak elde edilen kopyası bilgisayarda kullanılabileceği gibi , pin kodu ve dijital kalemle atılmış imzalarda elektronik imza kapsamına girmektedir[301.]

Yukarıda da anlatmaya çalıştığımız gibi elektronik imza da, şu yöntemler kullanılabilir: Doğrudan elektronik bir kalemle ekrana atılan imza kullanılabileceği gibi, sadece kullanıcı adı ve şifre de elektronik imza sayılabilir; çünkü kimliği doğrulamaya yarar ve aynı zamanda işlemle ilgili bir veriye eklenir. Bütün bunların dışında , yüz tanıma, ses tanıma, biyometrik yöntemler, genetik yöntemler, vs. elektronik imza olarak kullanılabilmektedir. İşte elektronik imza denildiğinde bunlar ifade edilebileceği gibi , şu anda aklımıza gelmeyen veya ileride ortaya çıkacak teknolojik gelişmelerde bu tanım içerisine çok rahat bir şekilde girebilmektedir[302,303,304,305].

13 Aralık 1999 tarihli Avrupa Birliği Direktifinde elektronik imza, , "**başka bir elektronik veriye eklenen veya onunla mantıksal bağlantısı bulunan, kimlik teşhisine yarayan elektronik formda bulunan veriler**" olarak tanımlanmıştır.

---

[300] Keser, Berber, "İmzalıyorum O Halde Varım, Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri",TBB Dergisi,2000/2 s.503

[301] Ergün,Ömer; Dijital İmza-İnternet Hukuku,www.law.ankara.edu.tr,2005.

[302] Erturgut M., Elektronik İmza Kanunu, e-Belge ve e-İmza (Hukuki açıdan tanıtım ve değerlendirme : http://www.tbb.org.tr/turkce/konferans.htm), Deliduman,Seyithan,Elektronik Verilerin Delil Değeri, II.Türkiye Bilişim Hukuku Sempozyumu,28.05.2004, Orta, Mesut; Elektronik İmza ve Uygulaması, Ankara 2005,s.36.; Diğer bir tanıma göre elektronik imza, kişilerin biyometrik özelliklerine dayalı (ses, göz retinası taraması, parmak izi taraması gibi) biyometrik yöntemler, kredi kartlarında kullanılan PIN kodları, elle atılmış imzanın tarayıcıdan geçirilerek elektronik ortama aktarılmış hali, bilgisayar ekranında bu amaçla yapılmış bir kalemle atılan imza tekniği veya çift anahtarlı kriptografiyle oluşturulan dijital (sayısal) imzayı da içeren bir üst kavramdır

[303] Bir tanıma göre elektronik imza, kişinin el yazısı ile attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştirmeye yarayan matematiksel formüllere veya şifreleme programlarına verilen bir isimdir. Keser Berber, L., Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi,www.hukukcu.com, Yazar kanımca da isabetli olarak "dijital imza" tabirinin kullanılması gerektiğini ifade etmektedir. Ancak şu an için kanunun tabiri "elektronik imza" olduğundan biz de bu tabiri kullanıyor ve olması gereken bakımından "dijital imza" tabirini yerinde buluyoruz.

[304] Başka bir tanıma göre elektronik imza, ıslak imzanın fonksiyonlarını da kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır. Arıkan, Saadet., *"Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım"*, Ankara 1999, s.151. Orta, Mesut,s.36.

[305] Elektronik imzanın bir diğer tanımı, bir bilginin üçüncü kişilerin erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karater veya sembollerden oluşmuş bir settir[305]. Genel olarak elektronik imza; elektronik ortamda oluşturulan, iletilen ve saklanabilen özel bir elektronik belgeyi ifade etmektedir, Sevimli, Ahmet: Elektronik Sözleşmeler ve ABD. Elektronik İmza Yasa Tasarısı, Prof.Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı, C.2, Beta Yayınları, İstanbul, 2001, s.1029; Ayrıca Amerika Birleşik Devletlerinde kanunlaşan E-Sıgn Act diye de adlandırılan dijital imza kanunundaki tanım için bkz. http://tansug.com/dijitalimzayasasi.htm (21.04.2007)

Türk hukukunda da, elektronik imza Avrupa Birliği Direktifi esas alınarak tanımlanmıştır. Buna göre, elektronik imza, "**başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri**" şeklinde tanımlanmıştır (EİK m.3, b).Elektronik İmza Kanunu (m. 3) elektronik verinin ise, elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar (m. 3/a) olarak tanımlamıştır.Böylece Elektronik İmza Kanunu ile yalnızca şu anda bilinen elektronik yöntemler değil de yeni geliştirilecek teknolojiler de kapsama alınmak istenmiştir[306].

Elektronik imza için de Kanunun elektronik veri tabirini kullanmış olması, elektronik veri ile elektronik imzanın karıştırılmasına sebebiyet verici nitelikte olmakla birlikte, böylesi bir düzenlemenin bir zorunluluktan kaynaklandığını ve bunu ifade için farklı bir tabirin bulunamamış olmasından kaynaklanmaktadır.

Kanun (m. 5, I) güvenli elektronik imzanın elle atılan imza ile aynı hukuki sonucu doğuracağını düzenlediğinden elektronik imzanın tanımında, elle atılan imzanın tanımından yararlanılabilir.

İmza, kişinin kimliğini, hüviyetini gösteren, onu belirleyen ve diğer kişilerden ayıran bir işaret[307] olarak tanımlandığına göre, elektronik imzanın da, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik işaret şeklinde tanımlanması mümkündür.

Elektronik imza tanımlarında herhangi bir teknolojiye üstünlük tanınmadan, sadece ondan beklenen fonksiyonlar dikkate alınarak tanım yapılması "teknolojik tarafsızlık" kavramıyla açıklanabilir[308]. Böylece elektronik imza alanında gerçekleşen değişikliklerin kanun değişikliğine gerek kalmaksızın uygulanabilmesi sağlanmış olmaktadır. Kanuni düzenlemeler, bu anlamda teknolojinin gerisinde kalmamış ve her değişikliğe uygulanabilir bir duruma getirilmiştir. Elektronik imza, şimdiye kadar imzalamada kullanılan ve ileride kullanılabilecek tüm yöntemleri kapsar bir şekilde hukuki düzenlemeye kavuşmuştur.

6.1.4 Sayısal İmza (Dijital İmza) Tanımları

Elektronik imza ile ilgili yapılan tanımlarda, yazarlar farklı isimler kullanmışlardır[309]. Ancak bu tanımlar incelendiğinde çoğunun da benzer olduğu

[306] Toplaoğlu,M.;s.127.
[307] Eren, F., Borçlar Hukuku Genel Hükümler, s. Tekinay/Akman/Burcuoğlu/Altop S. 149.
[308]Erturgut M., Elektronik İmza Kanunu, e-Belge ve e-İmza (Hukuki açıdan tanıtım ve değerlendirme : http://www.tbb.org.tr/turkce/konferans.htm),
[309] Dış Ticaret Müsteşarlığı bünyesinde kurulmuş Elektronik Ticaret Koordinasyon Kurulu Hukuk Raporu'na göre: sayısal imza; "Elektronik imzanın özel bir çeşidi olup, bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühürdür. Sayısal imzalar göndericinin kimliğinin açık ve net bir biçimde teyidini, elektronik dokümanın orijinalliğini ve güvenilirliğini mümkün kılar. Gönderici için ve

görülecektir. Karışıklığa yol açmamak ve konunun daha iyi anlaşılması için 'sayısal ve dijital imza' tanımları ayrı başlık altında incelenmiştir. Dijital ya da sayısal imza, nitelik olarak, tükenmez kalemle bir kâğıda atılan bildiğimiz imzadan farklı değildir[310]. Yani hukuki bakımdan aynı sonucu doğururlar. Aralarındaki tek fark, birinin bir kağıt üzerinde olması, diğerinin de elektronik ortamda bulunmasıdır.

Hemen belirtelim ki, sayısal imza, elektronik imza çeşitlerinden sadece birisidir. Elektronik imza, günümüz teknolojisinde çeşitli şekillerde olabilmektedir. Halen kullanılan imza dosyaları, biyometri tekniği (kullanıcının parmak ya da el izi, göz retinası vb. kişiye has özellikler) ile oluşturulan imzalar ve sayısal imzalar en çok bilinen ve tartışılan elektronik imza çeşitleridir. Hatta çoğu kişi ve kurumların, fiziki ortamda imzaladıkları belgeleri tarayıp bilgisayara aktarmak ve sonra da karşı tarafa göndermek şeklinde elektronik imza uygulaması yaptıkları da sıkça görülmektedir.

Elektronik ortamda yapılacak her tür sözleşme, mektup veya başka tür belgelerin hukuki korunması ancak ve ancak sayısal imza ile mümkün olmaktadır.

Sayısal imza, elektronik ortamda üretilen bilgilerin gönderilmesi sırasında göndericinin kimliğini kesinlikle teyit edecek, verinin başkası tarafından gönderilmediğini garanti edecek ve bu verilerin güvenliğini sağlamak amacıyla gizli olarak ve başkası tarafından değiştirilemeyecek bir uygulamadır[311].

Sayısal imza, bir imzacının imzalanacak metni şifreleme ve sıkıştırma mantığıyla çalışan, açık ve gizli iki anahtarlı kriptoloji tekniği ile sayısal karakterlere dönüşmüş özetini şifreli olarak belge altına eklemesidir. Ancak, bu işlem tek başına yeterli olmamakta, bir de arada onay makamı denilen ve kimlik doğrulaması yapan bir kuruluş bulunmaktadır. Bu kuruluşun diğer bir görevi de gönderilen belgelerin bir kopyasını kimsenin ulaşamayacağı şekilde saklamasıdır. Onay makamı, önceden kişinin kimlik bilgilerini teyit edip kayıt altına almaktadır.

Mesaj gönderici ve alıcılarının kimliklerinin belirlenmesi için üçüncü kişi veya kurumlarca sayısal sertifika düzenlenmesi gereklidir. Bu sertifikaları düzenleyen kurumlar, "Sertifikasyon Otoritesi", "Onay Makamı" ya da "Onay Kurumu" olarak adlandırılmaktadır. Sertifika, Onay Makamı tarafından düzenlenerek, sayısal olarak imzalanır. Sertifika; kullanıcı ismi ile onun açık anahtarını ihtiva eden ve gizli anahtarının kullanıcıya ait olduğunu doğrulayan elektronik dokümandır.

---

mesajın gönderildiği taraf için tek olan sayısal imzalar doğrulanabilir ve inkar edilemez." diye tanımlanmaktadır.

[310] Ahi,Gökhan; "Hukuki Bakımdan Dijital(Sayısal) İmza", www.bilisimhukuku.net,27.10.2004.

[311] Keser Berber, "İmzalıyorum O Halde Varım" s.503

Dijital imza şifreleme teknikleriyle oluşturulmuş bir elektronik imza türüdür[312]. Bir elektronik veriye eklenen veya veri ile mantıksal bağlantısı bulunan ve imzalayanın kimliğini belirleme aracı olarak kullanılan veriye elektronik imza denilmektedir[313]. Dijital imza ise bir bilginin, üçüncü kişilerin erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir settir[314].. Pekcanıtez[315], bu şekildeki dijital imzayı elektronik ortamda iletilen veriye vurulmuş bir mühür gibi nitelendirmektedir Elektronik imza çok çeşitli olmakla birlikte şu an için en güvenilir olanı ve güvenilirliği nedeniyle en yaygın olarak kullanılanı dijital imzadır[316].

Kavramları tekrar düzenleyip tanımlayacak olursak, elektronik imza, elektronik ortamda oluşturulmuş bir mesajın bütünlüğünü ve değiştirilmediğini ifade eden her türlü elektronik işaret olarak tanımlanabilir[317].Sayısal imza ise, bir kullanıcı ya da sunucu'dan gönderilen bilgilerin kesinlikle o kuruma ya da kişiye ait olduğunu doğrulayarak, verinin başkası tarafından yollanmadığını garanti eden, bilginin içeriğini koruyup, bir başka kişinin eline geçmesini ya da değiştirilmesini engelleyen, bilginin sadece alıcıya gittiğini ve sadece alıcı tarafından okunacağını garanti eden ve veriyi gönderen ve alanın kim olduğunu kanıtlamaya yarayan şifrelenmiş özel bir sayısal bilgidir.

Sayısal imzalar, asimetrik şifreleme olarak adlandırılan teknoloji yani elektronik bir dokümanın sahibinin dokümanı gizli şifreleme anahtarı kullanarak mühürleyebilmesi temeline dayanır. Bu şifre her zaman gizlidir, genellikle bir akıllı kart ya da diğer bir donanım üzerinde yazılı olarak verilir, bu şifre bilinmeden doküman üzerinde değişiklik yapılması mümkün değildir veya teknik olarak çok zordur. Elektronik İmza Kanunu'nun dijital imzayı esas aldığı savunulmaktadır[318].

---

[312] Diğer elektronik imzalara parmak izi, retina, yüz veya ses taraması gibi biometrik yöntemlerle oluşturulan veya PIN(Personal Identıfıcatıon Number) numarası verilerek oluşturulan elektronik imzalar örnek verilebilir. Bkz. **Ekşi**, Nuray: Elektronik İmzalara İlişkin Uncıtral Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme, Yasa Hukuk Dergisi, S.3, Mart, 2001, s.336

[313] Şenocak, Zarife: Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması, AÜHFD, 2001/2, s.98; Pekcanıtez, Hakan: Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, Uluslarası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002, s.395; Benzer bir tanım da Uncıtral Model Kanun Tasarısı 2. maddesinin a bendinde yer almaktadır. Buna göre elektronik imza ; veri mesajı ile ilintili olarak imza sahibini teşhis etmede kullanılabilen ve veri mesajında yer alan bilginin imza sahibi tarafından onaylandığını gösteren, veri mesajı ile mantıklı bir şekilde ilişkilendirilmiş veya veri mesajına eklenmiş olan elektronik biçimdeki veridir. Bkz. **Ekşi**, s.337

[314] www.etkk.gov.tr/hukuk.htm: Elektronik Ticaret Koordinasyon Kurulu Raporları, Hukuk Çalışma Gurubu Raporu, s.8; Diğer bir tanım: Elektronik ortamdaki yazışmalara eklenen, yazıyı gönderenin kimliğini ve gönderilen yazının iletim sırasında bozulmadığını kanıtlamaya yarayan bölüm. Bkz. Elektronik Ticaret Terimler Sözlüğü, (TÜBİTAK-BİLTEN), http://www.etkk.gov.tr

[315] Pekcanıtez, s.395

[316] Ekşi, s.336vd.

[317] Uslu,İzzet;Sayısal İmza ve Türkiye, Beykent Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası Ekonomi Politik Ve İşletmecilik Anabilim Dalı,www.bilgiyonetimi.org,07.06.2004.

[318] Topaloğlu, Mustafa:Bilişim Hukuku,Adana 2005,s.127.

6.1.5 Elektronik İmza Çeşitleri

6.1.5.1 Genel Olarak

Gerek kıta Avrupasındaki hukuksal düzenlemelerde, gerekse Türk hukukundaki düzenlemelerde elektronik imza taşıdığı özelliklere göre ayırımlara tabi tutulmuştur. Elektronik imzaya mevcut yasal düzenlemeler çerçevesinde çeşitli sebeplerle ve en önemlisi hukuki işlem güvenliğinin sağlanması bakımından çeşitli şartlar getirilmiştir. Getirilen şartlara göre elektronik imzalar, basit elektronik imza, gelişmiş elektronik imza, güvenli (nitelikli) elektronik imza ve akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilmiş elektronik imza şeklinde ayrıma tabi tutulmaktadır.Ancak tüm bu ayrımlar basit elektronik imza esası üzerinden getirilen ek şartlara göre yapılmıştır.Bu tür bir düzenleme tarzı, teknikteki gelişmelerin dikkate alınmasına olanak vermesi bakımından uygun bir tutumdur. Böylece, kanun koyucu, bilimin ve tekniğin, kanunun yapıldığı o günkü durumuyla kendini sınırlamaksızın gelecekteki elektronik imza alanındaki teknolojik gelişmelere de uyarlanabilir bir yol izlemek amacındadır.

Yabancı mevzuatta bu hukuki etkiye sahip elektronik imzalar çeşitli adlarla (kalifiye, üniversal e-İmza gibi) ve farklı teknik gereksinimlerle tanımlanmıştır. Ancak bütün bu imzaların ortak noktası, nitelikli sertifikaya dayanarak ve güvenli elektronik imza oluşturma aracıyla oluşturulmuş olmalarıdır. Kanunda yapılan tanım, Direktif md.2/2-a da yer alan ileri elektronik imza tanımında belirtilen bazı gereksinimler ile md.5/1 de belirtilen gereksinimlerin birleştirilmesi sonucu oluşturulmuştur. Böylece Direktifin ortaya koyduğu elektronik imza sınıflandırılmasından [elektronik imza,ileri elektronik imza, elle atılmış imza ile aynı hukuki etkiye sahip imza (nitelikli imza)] ayrı bir sınıflandırılmaya gidilmiştir. Kanunumuzda sadece elektronik imza ve güvenli elektronik imza ayrımı vardır.

6.1.5.2 Basit Elektronik İmza ve Gelişmiş Elektronik İmza

Basit elektronik imza başlığı altında bilgisayar ekranına kalemle atılan imza, biyometrik imza, dijital imza ve el yazısıyla imzanın tarayıcıdan geçirilerek elektronik belgelere eklenmesi durumları incelenebilir.

Basit elektronik imza ve özellikle basit dijital imza, sadece verinin bütünlüğünün korunduğunu göstermektedir. Bu sebeple basit elektronik imzalar hukuki işlerde şekil şartını yerine getirmeye elverişli olmadıkları gibi yargılamada geçerli delil olarak kullanılamazlar[319].Oysa Avrupa Ancak, Avrupa Birliği Direktifine göre, bir elektronik imzanın,

- Sadece elektronik formda olması

[319] Orta, Mesut;s.106;Erturgut M., Elektronik İmza Kanunu, e-Belge ve e-İmza (Hukuki açıdan tanıtım ve değerlendirme : http://www.tbb.org.tr/turkce/konferans.htm).

- Veya nitelikli bir sertifikaya dayanmaması
- Ya da akredite edilmiş bir sertifika hizmet sağlayıcısı tarafından verilmiş nitelikli bir sertifikaya dayanmaması
- Yahut güvenli bir imza oluşturma aracıyla üretilmemiş olması

Gerekçeleriyle hukuki etki doğurmasına veya yargılamada caiz delil olarak kullanılmasına engel olunmaması düzenlenmiştir (Direktif m.5).

Gelişmiş elektronik imza ise, genel olarak elektronik imza tanımından yola çıkılarak, bu tanıma çeşitli unsurların eklenmesi suretiyle tanımlanmaktadır.

Gelişmiş elektronik imza, verinin bütünlüğünün korunduğunu göstermesi yanında, imzalayanın kimliğinin tespitini de sağlar[320].

Avrupa Birliği Direktifine göre (Art. 2) gelişmiş elektronik imza, sadece imzalayana bağlı olan; imzalayanın kimliğini belirlemeye imkan veren; sadece imzalayanın kontrolü altında tutabileceği araçlarla yaratılan ve verilerde sonradan yapılacak değişikliklerin bilinmesini sağlayan elektronik imza olarak tanımlanmıştır.

Buna karşılık, Türk hukukunda gelişmiş elektronik imza tanımına yer verilmemiştir. Ancak gelişmiş elektronik imzanın unsurları, güvenli elektronik imza tanımındaki unsurlarda yer almaktadır (EİK m.4).

6.1.5.3 Güvenli Elektronik İmza

Avrupa Birliği Direktifinde, güvenli (nitelikli) elektronik imza tanımı yapılmamış, bunun yerine, üye ülkelerin el yazısı ile imzaya eşdeğer kabul edecekleri ve yargılamada delil olarak kullanılmasını temin edecekleri imzanın unsurları bakımından güvenli elektronik imza kabul edilmiştir. Bunun için gerekli şartlar, gelişmiş elektronik imzanın unsurlarını taşıyan bir elektronik imzanın, nitelikli elektronik sertifikaya dayanması ve güvenli imza oluşturma araçları ile oluşturulmuş olmasıdır. Bu unsurların varlığı halinde üye ülkeler bu imzanın el yazısı ile imzaya eşdeğerliğini ve yargılamada delil olarak kullanılmasını sağlayacaklardır (Art. 5).

Türk hukukunda, “nitelikli elektronik imza” kavramı yerine “güvenli elektronik imza” kavramı tercih edilmiştir. Elektronik imza kanunu sadece “güvenli elektronik” imzayı düzenleyerek bunun oluşturulmasının hüküm ve sonuçlarını düzenlemiştir. Kanun elektronik imzayı, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri, elektronik veriyi ise, elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar diye tanımladığını yukarıda belirtmiştik.(E.İ.K.m.3)

[320] Orta, Mesut;s.106-107;Erturgut M., Elektronik İmza Kanunu, e-Belge ve e-İmza (Hukuki açıdan tanıtım ve değerlendirme : http://www.tbb.org.tr/turkce/konferans.htm).

6.1.5.4 Güvenli Elektronik İmza

Teknolojinin kaydettiği hızlı gelişme ve İnternet'in küresel nitelikte kullanımı, sözleşmelerin de İnternet üzerinden kurulmasına yol açmış ve elektronik ticaret büyük bir gelişme göstermiştir. Artık insanlar bilgisayar başına oturup İnternet ortamında alışveriş yapmakta ve sözleşme oluşturmaktadırlar. Ancak bu şekilde kurulan hukuki ilişkilerde tarafların birbirleri ile hiç karşılaşmadıkları ve muhtemelen ileride de karşılaşmayacakları bir gerçektir. Böyle olunca İnternet ortamında hazırlanan bu belgelerin senet niteliği taşıyıp taşımadığı, sözleşmeci tarafların belirlenmesi, kimliklerinin doğrulanması ve kimliklerinin sözleşme ile ilişkilendirilmesi önemli bir problem olarak karşımıza çıkmaktadır.[321]

Bir başka problem herkese açık olan İnternet ortamında karşı tarafa gönderilen mesajın içeriğinin değiştirilip değiştirilmediğidir. Bundan daha da önemlisi sözleşme ile borç altına giren tarafların sözleşme metninde imzasının bulunması gerekir. Sanal ortamda bu nasıl yapılacaktır. Bilgisayara takılı bir çizim kalemi veya tarayıcı vasıtasıyla kişinin imzasının metne eklenmesi halinde, bu imzanın gerçek olup olmadığının ve sahteliğinin denetlenmesi mümkün olamamaktadır. Bu nedenle diyebiliriz ki; İnternet üzerinde yapılan işlemlerde, özellikle elektronik ticaret uygulamalarında, en çok ihtiyaç duyulan şeylerin başında güvenlik gelmektedir.

İşte bu ihtiyaca çözüm bulmak için el yazısı ile atılan imza yerine elektronik ortamda kullanılabilecek güvenilir bir mekanizma arayışına gidilmiştir. Böylece İnternet üzerinden yollanan bilgilerin güvenilirliğinin sağlanması, bilgilerin, güvenli ve değişmeden, aynı zamanda hukuki koruma sağlayıcı nitelik kazanarak yerine ulaşması gibi amaçlarla teknik çalışmalara başlanılmış ve tüm bu sorunların çözümü amacına yönelik olarak "güvenli elektronik imza" ortaya çıkmıştır.

Elektronik imza altyapısı, elektronik belgenin şifrelenmesini mümkün kılmakta, değiştirilmesini önlemekte ve ayrıca birden çok kişi ile, mesajın şifrelendiği anahtar kelimeyi öğrenmelerine gerek kalmadan, elektronik yoldan haberleşmeyi kolaylaştırmakta, kısacası elektronik ortamda zorunluluk arz eden güvenli bir ortam ihtiyacını karşılamayı amaçlamaktadır.[322]

1997 yılından beri birçok ülkede sayısal imzanın hukuki çerçevesi hakkında çalışmalar yapılmıştır. Yine çoğu ülkenin sayısal imza düzenlemelerinde UNCITRAL[323] model yasaları ve Avrupa Birliği direktifleri rol oynamıştır[324]. AB üyesi ülkelerin yanı sıra, ABD, Kanada, Arjantin, Brezilya, Japonya, Singapur, Hindistan, Rusya, Çin,

[321] Altınışık, s.77
[322] Orta, s.35
[323] UNCITRAL: Birleşmiş Milletler Uluslararası Ticaret Komisyonu
[324] 13 Aralık 1999 tarihli Avrupa Konseyi Elektronik İmza Direktifi ile Birleşmiş Milletlerin 14 Haziran 1996 tarihli Elektronik Ticarete İlişkin Model Kanunu

Tayvan, İsrail ve Avustralya'da sayısal imza kanunlaşmıştır ve elektronik ticarete hız ve güvenilirlik kazandırılmıştır.

Ülkemizde, bu konuda çalışmalar Dış Ticaret Müsteşarlığı'na bağlı Elektronik Ticaret Koordinasyon Kurulu ve Adalet Bakanlığı tarafından çalışmalar başlatılmış, hazırlanan yasa tasarısı tartışmaya açılmış ve 5070 sayılı Elektronik İmza Kanunu 23/01/2004 tarihinde resmi gazete yayınlanarak 23/07/2004 itibariyle yürürlüğe girmiştir. Kanun hazırlanırken yabancı mevzuattaki benzer düzenlemeler ve Avrupa Komisyonu'nun 99/93/EC sayılı elektronik imzalara ilişkin direktifi baz alınmıştır.[325]

Bu kanun Adalet Bakanlığı ve bağlı kuruluşların bünyesinde yürütülen faaliyetlerin ve yargı sistemi ile ilgili işlevlerin bilgisayar yardımı ile tam entegre bir şekilde otomasyona geçirilesi için çalışmaları devam eden Ulusal Yargı Ağı Projesi çalışmasının bir sonucudur[326].

5070 sayılı yasadan önce mevzuatımızda bu yönde bir düzenleme olmadığından, elektronik ortamda işlemlerin güvenle yapılması sorunu söz konusu olduğu gibi; bu nitelikteki belgelerin, ispat hukuku açısından senet niteliğinde kabul edilmediği gibi, yazılı delil başlangıcı dahi kabul edilmediğinden ve bu tür bir belge hakkında taraflar delil sözleşmesi yapmamış iseler, bu belge ancak ses bandı yada manyetik bandlar gibi kanunda sayılmayan ve özel hüküm sebepleri olarak belirtilen takdiri delil sayılacağından[327]; HUMK'nun 288 ve 290. maddeleri dikkate alındığında bu nitelikteki belgelerle ispat işlevini gerçekleştirmek neredeyse imkansız bulunmaktaydı. 5070 sayılı yasa ile elektronik işlem ve uygulamalardaki güven sorunu, elektronik işlemlerden kaynaklanan ihtilafların ve bunun gibi pek çok muhtemel sorunun çözümü mümkün hale gelmiştir.

Elektronik İmza Kanununun 4.maddesine göre güvenli elektronik imza: Münhasıran imza sahibine bağlı olan, Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan, Elektronik imzadır. Bu nitelikleri taşımayan elektronik imzalar hakkında kanunda hüküm bulunmamaktadır. Ayrıca bu şartların hepsinin birlikte gerçekleşmesi gerekmektedir.

Avrupa Birliği Direktifinde gelişmiş elektronik imza tanımının unsurları olan dört unsur, hukukumuzda güvenli elektronik imzanın unsurları arasında belirtilmiştir. Bu şekilde hukukumuzda gelişmiş elektronik imza şeklinde bir ayırım yapılmamıştır. Güvenli elektronik imza, Avrupa Birliği Direktifinde belirtildiği üzere el yazısıyla imzaya

[325] Sevim, s.1
[326] Biçkin, s.351
[327] Pekcanıtez, s.425

eşdeğer sayılacak ve yargılamada caiz delil olarak kullanılacaktır. Hukukumuz açısından bu hususların gerçekleştiği söylenmelidir. Zira Elektronik İmza Kanununda, güvenli elektronik imza, el yazısıyla imzaya eşdeğer kabul edilmiş (m.22) ve elektronik imza ile oluşturulmuş verilerin senet hükmünde olacağı belirtilmiştir (m.23).

Elektronik imzanın unsurları ise şunlardır; İmza sahibi, Kanunda imza sahibi "Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi"dir. Direktifte ve yabancı mevzuatlarda da bu tanımla örtüşen tanımlar mevcuttur. Burada dikkat edilmesi gereken husus, imza sahibinin ancak gerçek kişi olabileceğidir.

Güvenli imza oluşturma verisi, "İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler"dir. Uygulamada imza oluşturma verisi hem hizmet sağlayıcı tarafından hem de sertifika sahibi tarafından oluşturulabilmektedir[328].

Güvenli imza doğrulama verisi, "Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler"dir. Bu tanım uygulamada "public key" olarak bilinen açık anahtarı belirtmektedir. Tanım Direktifin çevirisi şeklindedir ve yabancı mevzuatta da aynı şekilde tanımlanmıştır.

Güvenli imza oluşturma aracı, "Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı"dır. Uygulamada imza oluşturma araçları smart kartlar veya bilgisayar yazılımları olarak karşımıza çıkabilmektedir

Güvenli imza doğrulama aracı, "Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı"dır.

Elektronik sertifika, elektronik imzanın doğrulanması için gerekli olan veriyi ve imza sahibinin kimlik bilgilerini içeren elektronik kaydı ifade etmektedir. Kanunun (a) bendinde geçen "münhasıran imza sahibine bağlı olan" ifadesi elektronik sertifikaya işaret etmektedir. Elektronik sertifikalar, kanuna uygun olarak faaliyette bulunacak elektronik sertifika hizmet sağlayıcılarından belirli bir ücret karşılığında temin edilecektir.

Elektronik sertifika hizmet sağlayıcısının sertifika üzerindeki elektronik imzası, sertifikanın bütünlüğünü ve doğruluğunu garanti edecektir. Elektronik sertifikalar, atılan imzanın doğruluğunun teyit edilebilmesi için gereklidir.

Nitelikli elektronik sertifikalar; Kanunun 9 uncu maddesinde belirtildiği şekilde "nitelikli sertifika" olduğuna dair bir ibareyi, sertifika hizmet sağlayıcısının kimlik bilgilerini ve kurulduğu ülke adını, imza sahibinin teşhis edilebileceği kimlik bilgilerini,

[328] Orta, Mesut; s.97–98.

sertifikanın geçerli olduğu süreyi ve sertifikanın seri numarasını barındıran elektronik sertifikalardır.

Güvenli elektronik imza, açık anahtar altyapısını kullanarak hem imzalama hemde şifreleme işlemlerini güvenli bir şekilde yerine getirmektedir. Açık anahtar altyapısı mimarisinde biri imza doğrulama işlevi gerçekleştiren "açık anahtar[329]", diğeri imza oluşturmaya yarayan "özel anahtar[330]" olmak üzere iki anahtar kullanılmaktadır. Açık anahtar, kamunun erişimine açıktır. İstenilmesi halinde öğrenilebilir. Özel anahtar ise kişiye özeldir. Anahtar, imzayı şifrelemek veya deşifre etmek için kullanılan sayısal karakterler dizisine denmektedir[331]. Bu dizi şu anki uygulamada 256 bit uzunluğunda dahi bulunmaktadır. Hangi anahtarın kime ait olduğu elektronik ortamda kimlik teşhisi açısından önem arz etmektedir. Bu görev sertifika otoriteleri tarafından yerine getirilmektedir. Sertifika otoriteleri kişinin açık anahtarı ile kimlik bilgilerini bir araya getirerek adeta elektronik ortamda nüfus kağıdı çıkarırlar. Bu sertifikaları her an ulaşılabilecek şekilde tutarlar. Sertifikaların yaşam döngülerini sağlar, gerektiğinde iptal ederek bunlara ilişkin bilgileri de saklarlar[332].

Güvenli elektronik imza teknik olarak bir yazılımdır. Genel anlamıyla kimliğini ve ekli bilgiye onay verildiğini göstermek niyetiyle bir kimse tarafından (veya onun namına) kullanılan herhangi bir işaret veya kabul edilen herhangi bir güvenlik usulüdür. Bir mesajın; imzalayanın açık anahtarına karşılık gelen bir özel anahtar kullanılarak oluşturulup oluşturulmadığı ve başlangıçtaki mesajın dönüşüm esnasında değiştirilip değiştirilmediğinin asimetrik şifreleme sistemi ve başlangıçtaki mesaja sahip olan kişi ve imzalayanın açık anahtarının tam olarak saptanabildiği bir "hash fonksiyon" kullanılarak dönüştürülmesidir[333].

Güvenli elektronik imzanın oluşturulması matematiksel bir süreci gerektirir. Bu süreç insanlara ilk bakışta karmaşık ve zor gibi görünse de, durum zannedildiği kadar zor değildir. Bir metni dijital olarak imzalamak istediğimizde altyapısı çok karmaşık olan algoritmalardan kimsenin haberi olmaz. Çünkü bu işlemlerin hepsini bilgisayarın kendisi gerçekleştirir. Aksini düşünmemiz halinde, bir metni şifrelemek ya da deşifre etmek için birkaç yıl uğraşmamız gerekebilirdi.

Güvenli elektronik imzada, kişinin ıslak imzasının elektronik ortama kopyalanması söz konusu değildir. Aksine, elektronik ortamda oluşturulan belgelerin asimetrik anahtarla şifrelenmesi esasına dayanmaktadır.

---

[329] 5070 sayılı yasada "imza doğrulama verisi" şeklinde tanımlanmıştır.
[330] 5070 sayılı yasada "imza oluşturma verisi" şeklinde tanımlanmıştır.
[331] Altınışık, s.82-83; Özgül, s.4; Orta, s.42
[332] Orta, s.35
[333] Orta, s.37; Erturgut, s.69

Güvenli elektronik imzanın işlevi, elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal dokümanların olduğu şekilde, herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktır[334]. Bu nedenle elektronik imza, elektronik ortamın vazgeçilmez unsurlarından birisidir denilebilir.

Açık anahtar alt yapısı, sayısal imzanın oluşturulmasında, kullanılmasında çok önemli rol oynamaktadır. Aşağıda açıklanacağı üzere, imzanın oluşturulmasında ve doğrulanmasında kullanılan açık ve özel anahtarlar ile açık anahtarın kime ait olduğunun belgesi sayılan elektronik sertifika ve bu sertifikaların üretilmesi, yönetilmesini sağlayan elektronik sertifika hizmet sağlayıcıları (ESHS) sayısal imzanın unsurlarını oluşturmaktadır.

AAA (Açık Anahtar Alt Yapısı "Public Key Infrastructure"), 1978 yılında 3 bilim adamı Rivest, Shamir ve Adleman'ın baş harflerinden oluşan RSA matematik algoritmasının onaylanması ile başlar[335]. Ana amacı; sanal dünyada, herhangi bir bilgi taşınırken gizlilik (confidentiality), bilgi bütünlüğü (Integrity) , kimlik doğrulama (Authentication) ve gönderenin inkar edememesi (Nonrepudiation) güvenlik özelliklerinin sağlanması olan AAA; bu işlemleri sayısal imza ve sayısal şifreleme ile özel ve genel (açık) anahtar kullanarak gerçekleştirmektedir. Sayısal imza; kimlik doğrulama, bilgi bütünlüğü ve gönderenin inkar edememesi; Sayısal şifreleme ise gizlilik ve güvenlik fonksiyonlarını sağlamaktadır.

AAA teknolojisinin kalbi asimetrik kriptolojidir. Asimetrik kripto, private (özel) ve public (genel) key olarak iki farklı anahtarla çalışır ve çapraz şifreleme yöntemi kullanılır. Buna göre karşı tarafa gönderilen mesaj aynı anahtar ile değil kişiye daha önceden verilmiş, özel bir anahtarla açılıp okunabilmektedir. Böylelikle mesaj sadece özel anahtara sahip kişi tarafından açılabilecektir[336]. Her iki anahtar farklı işler için kullanılır. Özel anahtar sayısal imzanın oluşturulmasında açık anahtar ise sayısal imzanın tetkikinde kullanılmaktadır. Başka bir deyişle özel anahtar mesajı şifrelemekte, açık anahtar ise deşifre etmekte kullanılır[337]. Bu yüzden özel anahtar sadece kullanıcıda bulunur ve özenle saklanması gerekir. Bu durumun aksine açık anahtarın üçüncü kişilerce ulaşılabilir olması, onlar tarafından biliniyor olması gerekmektedir. Bu anahtar çiftleri birbirlerine matematiksel bir bağla bağlıdırlar. Ancak birinden diğerini elde etmek imkansız kabul edilmektedir[338]. Söz konusu anahtar çifti ya elektronik sertifika hizmet sağlayıcıları tarafından üretilir ve sahibine teslim edilir, ya da kişiler

[334] Orta, s.38
[335] Yükseliyor, s.1
[336] Orta, s.42; Altınışık, s.82; Erturgut, s.67; Keser Berber, s.25
[337] Orta, s.43; Topaloğlu, s.121
[338] Orta, s.43; Babür, s.2; Altınışık, s.82

tarafından bizzat uygun programlar aracılığıyla elde edilir[339]. Açık anahtara herkesin ulaşabilmesi amacıyla güvenilir üçüncü kişiler, diğer bir deyimle elektronik sertifika hizmet sağlayıcıları elektronik sertifika dizinleri oluştururlar. Sertifika içinde açık anahtarla birlikte kişinin kimliğini yansıtan diğer bilgiler de yer alır.

Asimetrik kriptolojini çalışma şeklini herkes tarafından anlaşılması bakımından bir örnekle açılayalım; diyelim ki ben arkadaşım Mehmet'e başkalarının öğrenmesini ve değiştirmesini istemediğim bir mesaj veya belge göndereceğim; bunun için öncelikle göndereceğim metni bilgisayarda hazırladım. Şimdi bu metni şifreleyeceğim. Yukarıda izah ettiğimiz gibi bu metin ancak bana özel ve kimsenin bilmediği "özel anahtar" ile şifrelenecektir. Ben metni özel anahtarım ile şifreledim diyelim. Şimdi benim genel anahtarım kamuya açık olduğundan isteyen herkes tarafından mesajın deşifre edilmesi söz konusudur. Ancak ben bu mesajın yalnızca Mehmet tarafından deşifre edilebilmesini istiyordum. İşte bu nedenle çapraz şifreleme yapılması gerekmektedir. Yani ben hazırladığım metni önce Mehmet'in kamuya açık olan genel anahtarı ile şifreledikten sonra bu hali ile kendi özel anahtarım ile de şifreliyor ve Mehmet'e gönderiyorum. Mehmet kendisine mesaj ulaştığında, mesajı açabilmek için benim özel anahtarımla şifrelememe karşı kamuya açık genel anahtarımı, Kendisinin genel anahtarı ile şifrelememe karşın da kendi özel anahtarını kullanarak mesajı deşifre edecektir. Yani ne ben ne de Mehmet birbirimizin özel anahtarını öğrenemeyecek ve bu mesajı üçüncü kişiler açamayacaktır. Bu örneği sadeleştirirse; mesajı gönderen, alıcının genel, kendisinin özel anahtarını kullanarak şifreleme yapacak; alıcı da gönderenin genel, kendisinin özel anahtarı ile mesajı deşifre edecektir. İşte bu çapraz şifreleme yöntemidir. Yani özel anahtarla yapılan şifrelemeyi genel anahtar, genel anahtarla yapılan şifrelemeyi ancak özel anahtar açabilir. Şu anki uygulamada üçüncü kişilerin mesajı deşifre etmeleri imkânsız kabul edilmektedir.

Yukarıdaki örnek genel şifreleme şeklini irdelediğinden karmaşık gelebilir. Ancak uygulamada bu işlemi bilgisayar kendisi gerçekleştirdiği için biz kullanıcılara sadece bilgisayar programının bizden istediği genel ve özel anahtar bilgisini girmek yeterli olacaktır.

Bir kişinin özel anahtarının öğrenen üçüncü kişi artık o kişi imiş gibi imzasını kullanabilir. Bu nedenle özel anahtarın güvenliğinin sağlanması gerekmektedir. Özel anahtar üretildikten sonra ya bilgisayarın diskinde ya da harici bir depolama biriminde tutulur. Ancak, erişilmesi kolay olup ataklara maruz kalacağından disk, disket, CD, DVD gibi elektronik ortamlarda tutulması güvenlik açısından tehlikelidir. Özel anahtarın bulunduğu elektronik medya şifre ile korunsa dahi bu şifrelerin bulunması çok zor

[339] Örneğin, PGP – Pretty Good Privacy

değildir. Açık anahtardan yola çıkarak matematiksel yöntemlerle özel anahtarın elde edilmesinin imkânsız kabul edildiğini yukarıda izah etmiştik. Bu nedenle üçüncü kişiler ancak gerekli güvenlik önlemlerinin alınmadığı durumlarda özel anahtarlara ulaşabilirler. Bu durumda, imza özel anahtarla atıldığından ve inkâr edilemeyeceğinden bütün sorumluluk özel anahtar sahibine ait olacaktır.

Bu nedenle özel anahtarın çok iyi korunması gerektiği konusunda kullanıcılar mutlaka bilinçlendirilmeli, kurumsal uygulamalarda özel anahtarın sabit veya geçici disk ortamlarında tutulması yerine akıllı kart gibi güvenlik seviyesi yüksek cihazlar özendirilmelidir[340].

Asimetrik kriptolojide mesajı deşifre etme süreci simetrik yönteme göre daha uzun sürmektedir. Metnin tamamının şifrelenme süresi metnin büyüklüğüne göre uzayacağından kullanışlı olmayacaktır. Bu nedenle 'rivest' tarafından hash fonksiyonu geliştirilmiştir[341].

Bilgisayar terminolojisinde " Hash (= Öz)"; yazılan bir mesajın, kısaltılmış şeklidir. Hash foksiyonu ile matematiksel bir algoritma kullanılarak mesajın özeti çıkartılır ve bu özet şifrelenir[342]. Hash fonksiyonu ile oluşturulan mesaj özeti verilerin parmak izi olarak düşünülebilir.[343] Teknik açıdan dijital imza, imzalanmış belgenin özünü (Hash) içerir[344]. Buradaki algoritma genel olup aynı belgeye kim tarafından uygulanırsa uygulansın aynı hash değeri elde edilir.[345] Çünkü mesaj özeti, metnin karakteristik özelliklerinin tümü dikkate alınarak oluşturulmaktadır. Yapılacak en küçük bir değişiklik mesaj özetinin değişmesine yol açacaktır[346].

Burada bilinmesi gereken husus, sayısal imza denilen olgunun metnin içeriğinde değil mesaj özeti üzerinde uygulandığıdır. Metni imzalayan kişinin özel anahtarı ve asimetrik şifreleme sistemi vasıtasıyla mesaj özeti şifrelenir ve bu şekilde şifrelenen mesaj özeti elektronik metne eklenerek muhataba gönderilir. Şifrelenen mesaj özeti metinden ayrı olarak tutulur. Mesaj özetinden bir şekilde metne ulaşmak mümkün değildir.

Mesaj alındığında öncelikle tekrar mesaj özeti çıkarılır. Gelen mesaj ekinde yer alan şifreli mesaj özeti gönderenin açık anahtarıyla deşifre edilir. Bu işlemle gönderenin kimliği doğrulanmış olur. Gelen mesaj özeti ile yeni hesaplama sonucu bulunan mesaj özeti karşılaştırılır. İkisi de aynı ise mesaj orijinaldir, değişikliğe uğramamış demektir. Böylelikle bütünlük kontrolü gerçekleştirilmiş olmaktadır. Metinde yapılacak en küçük

[340] Orta, s.44
[341] Orta, s. 37; Altınışık, s.83
[342] Keser Berber, s.24; Altınışık, s.83; Erturgut, s.75;
[343] Orta, s. 53
[344] Topaloğlu, s.121
[345] Altınışık, s.83; Orta, s.54
[346] Keser Berber, s.25; Orta, s. 54; Altınışık, s.84

bir değişiklik, muhatap tarafında çıkarılacak mesaj özetinin gönderen tarafta oluşan mesaj özetinden farklı olacağından doğrulama işleminin başarısızlıkla sonuçlanmasına yol açacaktır.

Elektronik bir belgenin ispat gücünü artırmak için, diğer koşulların yanı sıra belgenin düzenlendiği zamanın şüpheye yer bırakmayacak bir şekilde tespit edilmesi gerekir[347]. Zira elektronik ortamda işlemlerin yapıldığı zamanın tayini, işlem güvenliği açısından önemli olup, imzanın doğrulanması ve mesaj bütünlüğünün denetlenmesi açısından vazgeçilmez bir unsurdur. Mesajı alan taraf mesajın geçerli olup olmadığını denetleyebilmek için izanın atıldığı tarihe ihtiyaç duyar. Öte yandan iletişim sırasında mesajın içeriğine müdahale yapılmışsa, en son yapılan işlemin tarihi görüneceğinden bu da anlaşılabilecektir.[348]

Elektronik ortamda zaman tayini fonksiyonunu zaman damgası gerçekleştirir. Zaman damgası; "sertifika hizmet sağlayıcıları tarafından, belirli bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı veya saklandığı zamanı göstermek üzere verilen belgedir"[349]. 5070 sayılı yasada ise "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt" şeklinde tanımı yapılmıştır.

Normal bilgisayarlarda ve işletme sistemlerinde, tarih ve saat ayarı, fazla bir zahmete gerek olmadan, kolaylıkla değiştirilebilmektedir. Normal belgelerdeki gibi, elektronik belgelerde de tarih ve saatin doğru bir şekilde tespit edilmesi gerektiğinden, bunu başarmak için güvenli bir yönteme ihtiyaç vardır.

Bu yüzden şifreleme ve kimlik teşhis etmenin yanı sıra, zaman kaşesi fonksiyonu da önemli bir role sahiptir. Günlük yaşamdaki bir çok işlemlerde, örneğin; sigorta mukaveleleri, hisse senedi ve döviz işlemlerinde tam zamanın açıkça tespit edilmesi gerekir. Bu nedenle onay kurumları talep üzerine dijital tarihleri zaman damgası ile belirtmek zorundadır[350].

Dijital imza, verilerin elektronik ortamda, değişikliğe uğramadan, gizli ve güvenli bir şekilde kullanılmasını ve paylaşılmasını yukarıda anlatıldığı şekilde gerçekleştirmektedir. Dijital imza, sadece gizli anahtarla oluşturulur ve bu anahtara karşılık gelen açık anahtarla doğrulanabilir. Bu sebeple imzalı belgenin alıcısının, dijital imzanın gizli anahtarın sahibi tarafından oluşturulduğuna dair bir güveni vardır. Fakat dijital imza tek başına kişinin kimliğini tespit edici bir fonksiyona sahip değildir.Bu

[347] Keser Berber, s.26; Orta, s. 55
[348] Altınışık, s. 88
[349] e-imza Hukuk Çalışma Grubu Raporu, s.37
[350] Altınışık, s. 88; Keser Berber, s.26

nedenle dijital imza, imza sahibinin kimliğini de güvenilir biçimde tespit etmelidir. Bunu sağlamak için sertifika hizmet sağlayıcılarına ihtiyaç duyulur. Çünkü, tarafsız bir üçüncü kişi tarafından kimlik belirlenmişse bu kişinin kimliğine güvenilebilir[351].

Elektronik sertifika, "onay kurumları[352]" yada "güvenilir üçüncü kişiler[353]" olarak da isimlendirilen Elektronik Sertifika Hizmet Sağlayıcıları tarafından oluşturulur. Buna göre elektronik sertifika hizmet sağlayıcıları sertifikadaki kişinin gerçekten o şahıs olup olmadığını tescil ederler. Yani açık anahtar ve kimlik bilgilerini sertifikaya yerleştirip kendi özel anahtarlarını kullanarak tasdik ederler[354].

Elektronik sertifika günlük hayatta kullanılan ehliyet, pasaport gibi kimlik kartlarının elektronik ortamdaki karşılığıdır denilebilir[355]. Elektronik sertifika, kullanıcı adıyla onun açık anahtarını içeren ve gizli anahtarının kullanıcıya ait olduğunu doğrulayan elektronik dokümandır. Diğer bir deyişle elektronik sertifika imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eder. Elektronik sertifika, kişilerin veya kuruluşların bilgilerinin elektronik ortamda güvenli bir şekilde iletilmesini sağlamaktadır[356].

Elektronik sertifika hizmet sağlayıcısının sertifika üzerindeki elektronik imzası, sertifikanın bütünlüğünü ve doğruluğunu garanti edecektir. Elektronik sertifikalar, atılan imzanın doğruluğunun teyit edilebilmesi için gereklidir.

5070 sayılı Elektronik İmza Kanununa göre ise Elektronik Sertifika; "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı" ifade eder[357]**.**

İmza anahtarı sahibi, imza anahtarını aldıktan sonra, bütün elektronik belgeleri gerek kendi ürettiği veya gerekse sertifika hizmet sağlayıcısı tarafından iletilmiş olan kendi özel anahtarıyla imzalayabilir. İmza anahtarı sahibi, sertifika hizmet sağlayıcısına başvurduktan sonra elde ettiği özel anahtarıyla elektronik belgeleri imzaladığında, imza anahtarı sahibinin sertifikası da imzalı elektronik belgelere eklenir[358].

Ekinde sertifika bulunan dijital imzalı bir elektronik belge alıcıya ulaştığında, alıcı kimlik tespiti yapmak için öncelikle, sertifika hizmet sağlayıcısının açık anahtarı ile sağlayıcının kimliğini kontrol edecektir. İkinci adım olarak sertifika sayesinde imza sahibinin açık anahtarı ile imza sahibinin kimliğini kontrol edecektir. İmza sahibinin

[351] Erturgut, s. 82
[352] Altınışık, s.84, Keser Berber, s. 27
[353] Erturgut, s.83
[354] Orta, s. 45; Altınışık, s. 85; Keser Berber, s.27 ; Erturgut, s.83; Sevimli, s.1030
[355] Orta, s. 45
[356] Orta, s. 45; Keser Berber, s.27
[357] 5070 sayılı yasa, m.3
[358] Erturgut, s. 84

kimliğinin tespiti ise sertifika hizmet sağlayıcısının her zaman ulaşılabilir liste hizmeti sayesinde mümkündür.

Elektronik İmza Kanunu'muzun 9. maddesine göre, nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse mesleki veya diğer kişisel bilgilerinin,

ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının, bulunması zorunludur.

Gönderilecek dijital imzalama prosedürlerinde iki yöntem vardır. Yazılıma (software) dayalı olanlar ve donanıma dayalı olanlar. Yazılıma dayalı olanlarda bir program aracılığıyla özel anahtara ulaşılır ve imzalama prosedürü yerine getirilir. Bu yöntemde giriş kodu yazılarak sisteme girilir ve işlemler başlatılır. Donanım esaslı yöntemde ise, onay kurumunun özel anahtarı kopyaladığı çip kart (smartcard-akıllı kart) bilgisayarın sürücüsüne yerleştirilir. Kullanıcı giriş kodunu yazdıktan sonra özel anahtara ulaşır[359].

Mesaj oluşturulduktan sonra imza sahibi tarafından yukarıda bahsedilen yöntemlerden herhangi biri vasıtasıyla "imzala" komutu verildikten sonra. Bilgisayar tarafından "hash fonksiyonu" denilen matematiksel bir işlemle, gönderilecek metnin bir özeti çıkartılır. Buna "hash değeri" denir. Anahtardan farklı olarak hash değeri belirli bir mesaj için her zaman aynıdır. Yani mesajda tek bir karakterlik bir değişiklik dahi olsa hash değeri farklı olur.

İkinci adım olarak hash değeri göndericinin özel anahtarı ile şifrelenir ve mesaja eklenir. Daha sonra alcının açık (genel) anahtarı, onay kurumundan veya alıcının

[359] Altınışık, s.91; Orta, s.44

kendisinden öğrenilerek mesaj ve dijital imza şifrelenir. Alıcı önce kendi özel anahtarı ile şifreyi deşifre eder. Alıcının yazılım programı mesajın hash değerini hesaplar. Gönderenin genel anahtarını kullanan alıcı şifreli hash değerini açarak kendi bilgisayarının hesapladığı hash değeri ile karşılaştırır. Eğer değerler aynı ise mesaj değiştirilmemiş demektir. Genel anahtarla şifreyi deşifre etmekle mesajın özel anahtar sahibi tarafından şifrelendiği anlaşılır. Mesaja ekli elektronik sertifika sayesinde de gönderenin onay kurumunun ilan ettiği kişi olduğu anlaşılır.[360]

Elektronik imza kullanıcılarına aşağıda belirtilen özellikleri ve fonksiyonları sağlamaktadır[361] Elektronik imza ile uygulamada "ıslak imza" olarak nitelendirilen imzanın hukuki açıdan aynı nitelikte olduğunu yukarıda izah etmiştirk. Islak imzanın işlevlerini ise genel olarak "sonuçlandırma, kalıcılık sağlama, kimlik tespit etme, gerçeklik, tasdik, ispat ve uyarı" işlevleri olarak sıralayabiliriz[362]. Elektronik imza ile ıslak imza aynı nitelikte olduğundan aralarında fonksiyon eşitliği de vardır. Şimdi bu fonksiyonları ve özellikleri ayrı ayı inceleyelim:

aa)Doğrulama**:** Veriyi imzalayanın kişinin kimliğinin doğrulanması yoluyla, işleme katılan tarafın kim olduğunun kesinlik bir şekilde bilinmesi sağlanacaktır. Bu özelliğin mantığı, dijital imzanın sahibinin imzası(gizli anahtarı) üzerinde kontrolü kaybetmedikçe taklidini yapmanın mümkün olmamasına dayanmaktadır.

İmzanın el yazısı ile atılması sayesinde belgeyi düzenleyen kişinin kimliği şüpheye yer vermeyecek şekilde tespit edilebilmektedir[363]. Aynı şekilde dijital imzada kimlik tespit etme işlevi, belirli makamlar (onay makamları) tarafından belirli bir gerçek kişiye bir defa olmak üzere koordine edilen imza anahtarlarının, yine bu makamlar tarafından kontrol edilmesi ile yerine getirilmektedir. Bu koordinasyon, bir imza anahtarı sertifikası ile yapılmaktadır. Anahtar sahibinin açık anahtarını bilen alıcı, herkes tarafından ulaşılabilen imza anahtarı sertifikasının kontrolü sayesinde, tanzim eden kişinin kimliği hakkında bilgi sahibi olabilecektir.

bb)Erişim Kontrolü: Gönderilen bilgilere ve kaynaklara sadece izin verilmiş kişiler tarafından erişilebilmesi garanti edilecektir.

cc)Bütünlük: Verinin bütünlüğü korunacaktır ve bu yol ile gönderildiği andan itibaren mesaj içeriğinin hiç değişmemiş olduğu, mesajın hangi amaç ile olursa olsun hiçbir şekilde alıcının gizili anahtarına sahip olmayan biri tarafından açılamayacak olduğu ve göndericinin de mesajı değiştiremeyeceği garanti altına alınmıştır. Asimetrik kriptografi teknolojisi ve açık anahtar altyapısı(PKI), İnternet ve diğer açık ağlar

[360] Altınışık, s.83-92; Keser Berber, s.27; Özgül, s.8
[361] Küçükközyiğit,Galip H; Elektronik Ticaret, Elektronik İmza ve Hukuk,www.ceterispapirus.net,2004. www.bakernet.com/ecommerce
[362] Keser Berber, s.6; Altınışık, s.92
[363] Keser Berber, s.39; Altınışık, s.93

üzerinde gerçekleşin elektronik haberleşme ve işlemlerde çok üst düzeyde bir güvenlik ve güvenilirliği olanaklı kılmaktadır.

dd)İnkâr edilememe: İnkâr edilememe, hukuksal bir anlaşmazlık ortaya çıktığında, gönderici tarafın mesajdan sorumlu tutulabilmesini sağlamaktadır. Karşı tarafın bir mesaja, sözleşmeye ya da ödemeye ilişkin isteği, bu mesajın karşı tarafın tek taraflı iradesiyle reddedilemeyeceğine güvenebilmesi ile yakından ilişkilidir. Gönderilen mesajın, gönderen tarafından reddedilememesi ve bu yolla işlemi gerçekleştiren açısından hukuksal yükümlülük oluşturması sağlanacaktır. Bu fonksiyon, için hayatsal öneme sahip uzaktan iletişime güvenilebilmesini sağlayarak, elektronik ticaretin gelişimini olumlu yönde etkileyecektir.

İrade beyanının yapıldığı belgede yer alan imzanın, bu belge ile olan lokal ilişkisi, belge ve imza arasında bir bağlantı meydana getirecektir. Bu suretle beyanın içerik olarak imza sahibi tarafından kabul edildiği garanti edilmiş olacaktır. Dijital imzada da metin ve imza arasındaki matematiksel-mantıki bağlantı nedeniyle, beyan ve imzalama arasında da sıkı bir bağlantı ortaya çıkmaktadır. Bu suretle beyanın içerik olarak imzalayan tarafından hazırlandığı ve sonradan değiştirilmediği garanti edilmektedir[364].

ee)Verimlilik ve Lojistik: Dijital imzalar, işlemlere kolaylık, ucuzluk ve hız kazandıracaktır.

ff) Sonuçlandırma İşlevi: El yazısı ile atılan imza, bir metnin içerik itibariyle sona erdirilmesidir. Dijital imzada ise, öncelikle elektronik ortamda hazırlanan metnin tümünün, gizli imza anahtarı ile imzalanacak olan bir hash değerinin oluşturulması gerektiği için, dijital imzalama süreci belgenin tümüne ilişkindir. Bu şekilde hazırlanan belgeye ilişkin olan imza, ancak metnin hazırlanmasından sonra oluşturulabilecektir. İmzalanan metin ve imza arasındaki bu mantıki bağlantı, sonuçlandırma işlevini yerine getirmektedir.[365]

gg) Kalıcılık Sağlama İşlevi:Yazılı şekil zorunluluğu, imzanın ve imzalanacak olan metnin okunabilir bir şekilde bir belgede yer almasını ve sürekli bir kontrole elverişli olması gerekir. Bu sayede yapılan beyan hakkındaki bilginin bir belgede tespit edilerek kalıcı olması sağlanmış olacaktır. Elektronik olarak imzalanan bir belge de, bu elektronik metnin istenildiği zaman okunabilmesini ve kontrol edilebilmesini mümkün kılmaktadır366. Örneğin; bilgisayarın hafızasına veya ayrıca bir de diskete veya CD'ye kopyalanan bir metnin her zaman için okunabilmesi mümkün olmaktadır.

[364] Keser Berber, s.39; Altınışık, s.93
[365] Keser Berber, s.39; Altınışık, s.93
[366] Keser Berber, s.39

hh) Tasdik İşlevi: Tasdik işlevi, gerçeklik ve kimlik tespiti fonksiyonları ile yakından bağlantılıdır. Tasdik işlevi sayesinde belgenin alıcısı, imza karşılaştırması yapmak suretiyle, imzanın gerçek olup olmadığını kontrol etmek olanağına sahiptir. Elektronik belgede de güvenilir ve sağlam bir dijital imza tekniği sayesinde alıcı, imzanın, imza anahtarı sahibi tarafından atılıp atılmadığını ve imzalanan metnin sonradan değiştirilip değiştirilmediği kolay bir şekilde kontrol etmek edebilmektedir[367].

jj) İspat İşlevi: Bir metnin altına el yazısı ile atılan imza, delil ikamesine ve hukuki işlemin içeriğinin açıklanmasına ve bu sayede taraflar arasındaki işlem bakımından sürekli bir şeffaflığa hizmet etmektedir. Yazılı şekil, ispatla yükümlü olan tarafın delil ileri sürmesini kolaylaştıracaktır. Yasanın aradığı özellikleri taşıyan bir dijital imza, bu imza ile imzalanan elektronik belgeye kesin delil olan "senet" niteliği kazandırmaktadır. Böylece elektronik şekilde yapılan bir irade beyanının alıcısı bakımından, klasik yazılı şekilde hazırlanmış bir belgeye verilen delil değerine sahip olacaktır.

kk) Uyarı İşlevi: İmza sayesinde beyanda bulunan kişi, imzalanan beyanın hukuki bağlayıcılığını ve sonuçlarını hesaba katmak zorundadır. Böylece kişiler, hukuki işlemler bakımından aceleci davranmaktan, düşüncesizce hareket etmekten korunmuş olacaklardır. Elektronik belgede de, imza atacak olan kişinin öncelikle ilgili metni bilgisayarda hazırlaması gerekmektedir. Daha sonra chip kartını kart okuyucuya takması ve PIN kodunu girmesi veya ayrıca bir de biyometrik bir yöntem kullanarak imza anahtarı sahibi olduğunu ispat etmesi için yaklaşık bir dakikaya ihtiyacı olduğu için, bu zaman zarfında hazırladığı metni göndermeden önce istediği değişiklikleri yapabilir. Sadece bu prosedür bile, işin ne kadar bağlayıcı olduğu konusunda imza atacak olan kişinin dikkatini çekmektedir[368].

Görüldüğü gibi elektronik (dijital) imza el yazısı ile atılan imza ile işlevsel eşitliğe sahiptir. Bunların yanında dijital imzanın başkaca avantajları da vardır. Bunları aşağıdaki, şekilde sıralayabiliriz[369].

1- Bir kullanıcı tarafından gönderilen bilgilerin veya verilerin kesinlikle o kişi tarafından gönderildiği teyit eder. Kısacası, başkası tarafından gönderilmediğini garanti eder. Dolayısıyla, klasik imzadaki gibi taklit edilme olasılığı da ortadan kalkar. Gönderici göndermediğini, alıcı da almadığını iddia edemez.

2- Bir kullanıcı tarafından gönderilen bilgilerin veya verilerin bir başkasının eline geçmesini veya değiştirilmesini engeller.

[367] Keser Berber, s.39; Altınışık, s.93
[368] Keser Berber, s.40; Altınışık, s.93
[369] Keser Berber, s.17; Altınışık, s.94; Ahi, s.2-3

3- Gönderilen bilgi ve verilerin içeriği, gönderici tarafından veya alıcı tarafından inkâr edilemez. Çünkü değil başkası, kendileri dahi gönderimden sonra içeriğini değiştiremez. Kaldı ki, bir uyuşmazlık halinde elektronik belgenin bir kopyası da onay kurumundadır.

4- Gönderilen verilerin tarih açısından damgalanmasını sağladığı gibi, arşivleme kolaylığı sağlar.

5- Gönderilen verilerin çabuk ulaşmasını sağlar, baskı, kağıt, posta ve arşivleme maliyetlerini en aza indirger.

6- Dijital imzanın hazırlanması kullanımı kolaydır,

7- Her yeni mesajda dijital imzanın farklı bir " bit " örneği ortaya çıktığı için, taklit edilmesi son derece güçtür ve gizli anahtara imza üzerinden ulaşılması mümkün olmadığı için, bilgi ağı üzerinden dijital imzanın elde edilmesi zordur,

8- Dijital imza ile fikri haklar ve telif hakları da imzalanabilir (örneğin; dijital resimler, besteler, yazılımlar gibi). Bu durumda diğer imza türlerinde olmayan verinin korunması ve izinsiz kullanılamaması güvencesini verir.

6.1.5.5 Güvenli Elektronik İmzanın Türk Hukukundaki Yeri

Ülkemizde elektronik imzanın kullanımı için gerekli yasal çalışmalar, ilk kez Sermaya Piyasası Kanunu Yönetmeliğinde "kendisine bağlı çalışan kurum ve e-imza dahil elektronik işlem usul ve esasları belirlenir" hükmüdür. Bu hükümden hareketle SPK, e-ticaret için pilot bir proje hazırlamıştır.[370] Daha sonra 29 Haziran 2001 tarihinde Hazine Dış Ticaret Müsteşarlığı koordinasyonunda oluşturulan Hukuk Alt Çalışma Grubu oluşturulmuştur[371]. Adalet Bakanlığı, 14 Ocak 2002 tarihli yazısı yeni bir çalışma komisyonu kurarak kısa sürede "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" taslağını hazırlamış, söz konusu tasarı taslağı, 10 Eylül 2002 tarihli yazı ile kurumların görüşüne sunulmuş ve 19 Şubat 2003 tarihinde Başbakanlığa gönderilmiştir.

Elektronik İmza Kanun Tasarısı, 15 Ocak 2004 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş, Kanun, 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmıştır. Yasanın gerekçesinde, "Günümüzde geleneksel ve alışılmış iletişim yöntemlerinden elektronik iletişim yöntemine doğru hızlı bir değişim ve gelişim yaşanmaktadır. Bilgi ve iletişim teknolojilerinin bu değişimi ve hızlı gelişimi, ekonomik faaliyet alanlarında ve sosyal yaşamda yeni olanaklar yaratmaktadır Bilgisayar ve İnternet'in sosyal ve ekonomik yaşama girmesi, bu alandaki gelişim ve

[370] http://www.turk.İnternet'.com, Topaloğlu, Mustafa:Bilişim Hukuku,Adana 2005,s.126.
[371] Çamurdan, Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme, 2003, http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm (21.04.2007)

değişimi hızlandırmıştır. Özellikle elektronik imzanın çeşitli alanlarda kullanılır olması sonucu bazı düzenlemelerin yapılması ihtiyacı ortaya çıkmıştır" denilmiştir.

İkincil düzenleme çalışmaları Telekomünikasyon Kurumuna verildiğinden Kanunun verdiği 6 aylık zamandan önce ikincil mevzuat çalışmaları tamamlanarak yürürlüğe girmiştir. Mevzuat çalışmalarının ardından elektronik imzanın uygulamaya girmesi için gerekli çalışmalar başlamıştır.

Kanun güvenli e-imzanın hukuki sonucu ve uygulama alanını bir yandan doğrudan 5. madde ile öte yandan ise 20 ve 21. maddelerinde yapılan değişikliklerle BK m. 14[372] ve HUMK m. 295A[373] maddeleriyle düzenlemeye yönelmiştir.

Şimdi kanunlarımızdaki elektronik imzanın düzenlenişini inceleyelim.

Kanuna göre "Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur". Bu hüküm Direktif md.5/1'e uygundur. Md.5/1'e göre nitelikli sertifikaya dayanan ve güvenli imza oluşturma aracı ile oluşturulan imzaların hukuki etkisi kağıda elle atılmış imza ile aynı olmalıdır ayrıca bu imzanın delil niteliği inkar edilmemelidir.

Direktif md. 5/2'ye göre üye devletler elektronik imzanın;

1. Elektronik formda olması,
2. Nitelikli sertifikaya dayanmaması,
3. Akredite edilmiş bir sertifika hizmet sağlayıcının sağladığı sertifikaya dayanmaması,
4. Güvenli elektronik imza oluşturma aracı ile oluşturulmamış olması,

Nedenlerinden biriyle delil niteliğini yadsıyamazlar. Direktifin bu hükmü Kanunumuza alınmamıştır. Oysa Direktifin ve dünyadaki diğer elektronik imza kanunlarının amacı elektronik imzalara hukuki bir çerçeve çizmek ve elektronik imzanın delil değerini ortaya koymaktır. Bu sebeplerden dolayı Avusturya'da olduğu gibi hukuki sonuç kısmına yukarıda sayılan sebeplerden birinin bulunmasına rağmen elektronik imzanın delil niteliği inkar edilemez kısmı eklenmelidir[374].

Kanuna göre "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez". Bu düzenleme ile teminat sözleşmeleri kapsam dışı bırakılmak suretiyle, elektronik

[372] Madde 22. 22.4.1926 tarihli ve 818 sayılı Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına aşağıdaki cümle eklenmiştir. "Güvenlikli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir".

[373] Madde 23. 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere aşağıdaki 295/A maddesi eklenmiştir. Madde 295/A- Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.

[374] Bilişim Şurası, Elektronik İmza,www.bilisimsurası.org.

imzanın kullanımının çabukluğu dolayısıyla doğması muhtemel zararların önlenmesi amaçlanmıştır[375]. Buna göre noterlerin yapacağı işlemler, noterlerin huzurunda yapılan işlemler, tescil zorunluluğu olan işlemler (gayrimenkul, motorlu araç alım satımı), evlenme gibi resmi memur önünde yapılması zorunlu olan işlemler elektronik imza ile yapılamazlar. .Dolayısıyla kanunların resmi şekle bağladığı, Örneğin, , araç satışları, mal rejimi sözleşmeleri, evlilik akti, tapuda yapılan taşınmaz tescilleri, resmi vasiyetname, kefalet sözleşmeleri vb. hukuksal işlemler de güvenli elektronik imza kullanılamayacaktır. Ancak kanun metninde elektronik imza ile yapılamayacak işlerin genel bir tanımla anlatılması bazı karışıklıklara sebebiyet verebilir.

Elektronik imzanın kullanımına işlerlik kazandırmak amacıyla, el ürünü imza ile eşdeğerde görülmüş ve Elektronik İmza Kanunu, el ürünü imza ile düzenlemenin yapıldığı 818 sayılı Borçlar Kanununda[376] değişiklik yapılmıştır.

Bu amaçla 5070 sayılı Kanunun 22. maddesi ile 818 sayılı Borçlar Kanunu'nun 14. maddesine bir cümle eklenmiştir. Bu şekilde, el ürünü imza ile ilgili düzenleme yapan mevcut yasal düzenleme gelişen teknolojinin doğurduğu ihtiyaçlara cevap verebilecek hale getirilmiştir. Düzenlemede, güvenli elektronik imzanın elle atılan imza ile aynı ispat gücüne sahip olacağı belirtilmiştir. Bu durum elektronik imzanın kullanımını yaygınlaştıracak ve güvenilirliğini artıracaktır. İstisnası 5070 sayılı kanunun 5. maddesinde belirtilen özel merasimi gerektiren işlemlerde elektronik imza kullanılamayacak, kullanılması durumunda işlem 5070 sayılı yasanın 22. maddesine rağmen geçersiz olacaktır[377].

5070 sayılı Elektronik İmza Kanununun 22. maddesine göre, Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına eklenen cümle şöyledir: "Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir" diyerek güvenli elektronik imza ile imzalanmış bir metnin mahkemelerde, delil niteliğinde olacağını ve bunun klasik elle atılmış olan bir imzadan farkının olmadığını belirtmiştir.

Türk İspat Hukuku sisteminde, "Kanuni Delil sistemi" mevcuttur. Bu sisteme göre Hâkim, Hukuk Usulü Muhakemeleri Kanunu'nda sayılan ve "Kesin Delil" olarak da adlandırılan, ikrar (HUMK m. 236), kesin hüküm (HUMK m. 237), senet (HUMK m. 286 vd.) ve yemin (HUMK m. 377 vd.) delillerinden biri ile ispat edilen bir vakıayı, doğru olarak kabul etmek zorundadır. Yani hakim, bu delillerle bağlıdır ve bu delilleri takdir yetkisi yoktur.[378]

[375] TBMM Adalet Komisyon Raporları,22.Dönem,2.Yasama Yılı, S.Sayısı:333.
[376] . Bkz. 22.4.1926 tarih ve 366 sayılı Resmi Gazete , 818 Sayılı Borçlar Kanunu, madde 14.
[377] Biçkin, İ., "Elektronik İmza Kanunu ve Getirdiği Düzenlemeler", Yargıtay Dergisi, C. 30, S.3, 351-361.
[378] Kuru, s. 1398;

Hukuk Usulü Muhakemeleri Kanunumuz, kesin deliller kategorisi yanında, ayrıca "Takdiri Delilleri" de düzenlemektedir. Takdiri deliller ile hakim, kesin delillerin aksine bağlı değildir. Bu delillerle ispatlanan bir vakıanın doğru olup olmadığını serbestçe takdir eder. Bunlar; tanık (HUMK m. 245 vd.), bilirkişi (HUMK m. 275 vd.), keşif (HUMK m. 363 vd.) ve özel hüküm sebepleridir (HUMK m. 367)[379]

Hukuk Usulü Muhakemeleri Kanunu m. 288/f.1'e göre; "Bir hakkın doğumu, düşürülmesi, devri, değiştirilmesi, yenilenmesi, ertelenmesi, ikrar ve itfası amacıyla yapılan hukuki işlemlerin, yapıldıkları zamanki miktar veya değeri 400 YTL' nı geçtiği takdirde senetle ispat olunması gerekir." Senetle (veya kesin delille) ispat zorunluluğu olarak adlandırılan bu kurala göre; yapıldıkları zamanki miktar veya değeri 430 YTL'nı geçen hukuki işlemlerin kanunda sayılan istisnalar saklı kalmak koşuluyla, kesin delillerden biri ile ispatlanması zorunludur. Bu hukuki işlemler, kural olarak tanıkla ispat edilemez. Senetle (veya kesin delille) ispat zorunluluğu hakkındaki ikinci ana kural ise, "senede karşı senetle ispat zorunluluğudur." Bu kurala göre; senede bağlı olan her çeşit iddiaya karşı savunma olarak ileri sürülen ve senedin hüküm ve kuvvetini ortadan kaldıracak veya azaltacak nitelikte bulunan hukuki işlemler, 430 YTL' dan az miktara ilişkin olsa bile, tanıkla ispat olunamaz.

Elektronik imza ile imzalanmış belgelerin uygulamada ispat vasıtası olarak kullanılması durumunda hangi delil kategorisinde olacağı konusunda doktrinde çok tartışmalar yapılmıştır. Kimi zaman özel hüküm sebeplerinde takdiri delil olarak değerlendirilebileceği söylenmiş, kimi zamanda el ürünü imza ile aynı hukuki güvenceyi sağlayabilmesi nedeniyle kesin delil olarak değerlendirilebileceği belirtilmiştir[380]. Bu tartışmalar 5070 sayılı Kanunda 1086 sayılı Kanunun 295 maddesine ek olarak bir madde getirilmiştir. Elektronik İmza Kanunu'nun 23. maddesinin 2. fıkrasında Hukuk Usulü Muhakemeleri Kanunu'nun 295. maddesine ek olmak üzere 295/A maddesi eklenmiş ve bu maddeye göre, " Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar " denilmiştir[381].. Yukarıdaki açıklamalar da göz önüne alındığında; senetle ispat zorunluluğu olan, 430 YTL'nı aşan her türlü hukuki işlemin ispatında, elektronik olarak imzalanmış belgeler kullanılabilecektir. Yine bu miktarın altında dahi olsa, senede veya bu niteliği haiz elektronik belgeye dayanan hukuki işlemlerin aksi ancak bu nitelikteki başka bir belge ile ispatlanabilecektir.[382]

---

[379] Kuru, s. 1399;
[380] Değişik görüşler için bkz.Pekcanıtez, Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, s. 390, Uluslar arası İnternet Hukuku Sempozyumu, İzmir 2002; ARIKAN, Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım, Ankara 1999, s. 134-135.
[381] 5070 Sayılı Elektronik İmza Kanunu, 239 sayılı Yargı Mevzuatı Bülteni.
[382] Keser Berber, s.12; Sevinç, s.1; Pekcanıtez, s. 398; Orta, s33

Elektronik imza ile tanzim edilen elektronik veriler, senet hükmünde sayılmaktadır. Bunun sonucu ispat hukuku bakımından aksi ispat edilinceye kadar kesin delil olarak kabul edilmesi gerekir. İkinci fıkrada ise güvenli elektronik imza ile oluşturulmuş verinin inkârı durumunda nasıl bir inceleme yapılması gerektiği konusunda Hukuk Usulü Muhakemeleri kanununun 308. maddesine kıyas yoluyla uygulanmak üzere atıf yapılmıştır. Bu fıkraya göre, "Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır."

Yukarıdaki düzenlemelerden anlaşılacağı üzere her elektronik imza, klasik imza ile eş değerde tutulmamaktadır[383]. Yani, e-mail kullanırken kendimize göre, oluşturduğumuz imzalar veya ilgili sitenin oluşturulmasına imkan verdiği imzalar veya bazı sitelerin güvenirliği artırmak için kendilerine göre oluşturdukları imza niteliğindeki şekiller, rakamlar, şifreler vs. bütün bunlar elektronik imza kanununun kapsamı dışındaki uygulamalardır ve bu tür atılan imzalar hukuksal koruma altında olmayıp, klasik imza ile elbette eş tutulamaz. Kanunun bir elektronik imzayı, klasik imzayla eş değerde tutabilmesi için, öncelikle elektronik imzanın kanunda tanımlanan nitelikte olması gerekir. Yani kanunda belirtilen sertifika vermeye yetkili kurumlar tarafından verilmiş güvenli elektronik imza olması gerekir.

6.1.5.5.1 Güvenli Elektronik imza ile imzalanmış verilerin delil değeri

Bilindiği üzere, bir hukuk normunun uygulanması, o normla düzenlenen, yani kendisine hukuksal sonuç bağlanan, olumlu veya olumsuz vakıaların somut olarak gerçekleşmiş bulunmasına bağlıdır[384].Dava konusu hakkın ve buna karşı yapılan savunmanın dayandığı vakıaların var olup olmadıkları hakkında mahkemeye kanaat verilmesi işlemine ispat denir[385].

Hukukumuz bakımından kanuni ve takdiri ispata birlikte yer veren karma bir sistemin geçerli olduğu söylenebilir. Zira, her ne kadar hukuki işlemler alanında kesin delillerle ispat geçerli ise de, bu düzenleme kamu düzenine ilişkin değildir ve ayrıca kanuni ispat sistemine, kanun tarafından geniş ölçüde istisnalar tanınmıştır (HUMK m. 289, 293 ve 294)[386].

---

[383] Ergün,Ömer; Dijital İmza ve İnternet Hukuku,www.law.ankara.edu.tr,03.02.2005.

[384] Bir başka ifade ile, hukuk normunun soyut olarak düzenlediği ve kendilerine hukuksal sonuç bağladığ vakıalar, somut olarak gerçekleşmiş bulunmadıkça, o norm uygulanamaz; o normda öngörülen hukuksal sonuç doğmuş sayılamaz (Umar, B/Yılmaz, E., İsbat Yükü, Ankara 1980, s. 1).

[385] Kuru, B/Arslan, R/Yılmaz, E., Medeni Usul Hukuku, Ankara 2003, s. 423. Davada ispata ilişkin olarak doktrinde yapılan bir diğer tanım ise, "taraflarca iddia edilen talebin dayandığı hukuk kuralının koşul vakıalarının somut olarak, iddia edildiği gibi gerçekleştiği konusunda hakimde kanaat uyandırmak üzere yapılan inandırma faaliyetidir" şeklindedir (bkz. Pekcanıtez, H/Atalay, O/Özekes, M., Medeni Usul Hukuku, Ankara 2001, s. 356; Atalay, O., Medeni Usul Hukukunda Menfi Vakıaların İspatı, İzmir 2001, s. 5).

[386] Türk hukuku bakımından senetle ispat zorunluluğuna ilişkin kuralın kamu düzenine ilişkin bulunmadığı ilişkin olarak bkz. 18.3.1959 günlü İBK (RG. 22.6.1959, S. 10237). Postacıoğlu, İ. E., 18.3.1959 gün ve

Hukuk Usulü Muhakemeleri Kanunu m. 288 vd. hükümleri ile hukuki işlemler bakımından senetle (kesin delille) ispat zorunluluğu kabul edilmiştir. Bu hükümlerde açıkça düzenlenen kanuni ispat halleri dışında delil serbestisi esası geçerlidir.

Delil, Hukuk Usulü Muhakemeleri Kanunumuzda, "davanın halline tesir edebilecek münazaalı hususların ispatı için başvurulan vakıalar" şeklinde tarif edilmiştir (m. 238, I)[387].

Kanun bir yandan güvenli elektronik imzanın elle atılan imza ile aynı hukuki sonucu doğuracağını düzenlemişken (m. 5, I), diğer yandan m. 22 ve m. 23'te konuya ilişkin açık düzenleme getirmiştir.

Hukuk Usulü Muhakemeleri Kanununun 295/A maddesine göre, güvenli elektronik imza ile imzalanmış verilerin senet hükmünde olduğu belirtilmiştir. Buna göre, yargılamada taraflarca, güvenli elektronik imzalı bir belge ibraz edildiği takdirde, bu belge "kesin delil" olarak hâkimi bağlayacaktır. Bu belgelere, resmi senetlere yaklaşır bir nitelik verildiği belirtilmelidir. Nitekim bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.

Hâkimin, yargılamada ibraz edilen elektronik belgenin, güvenli elektronik imza ile imzalanıp imzalanmadığı hususunun kendiliğinden araştırması gerekir. Aksi halde sadece tarafın beyanı üzerine, ibraz edilen herhangi bir elektronik belgeye senet niteliği atfedilmiş olacaktır. Hakim keşif ve bilirkişi incelemesine re'sen karar verebileceği için, ibraz edilen elektronik belgedeki imzanın güvenli elektronik imza olup olmadığı bu suretle incelenecektir.

Hâkimin kâğıda dayalı senetlerde bu şekilde bir inceleme yapmasına gerek yoktur. Çünkü senedin, senet niteliği gözle görülebilir. İbraz edilen senet, ispat edilmek istenen hukuki işlem hakkında tam bir bilgiyi içeriyorsa ve kendisine karşı senet ileri süren tarafından imzalanmış ise hakim, bu belgeyi senet olarak kabul edecektir. Böylece iddianın ispatı konusunda ibraz edilen kesin delil sebebiyle kanaate varacaktır.

Buna karşılık, elektronik belgelerde durum farklıdır. İbraz edilen bir elektronik belgenin, kanunun saydığı şartları haiz bir belge ve dolayısıyla senet olup olmadığı hakim tarafından gözle görülebilir ve değerlendirilebilir durumda değildir. Bundan başka, hakimin bu konudaki teknik bilgi eksikliği de söz konusudur.

Kanun yaptığı düzenleye ile elektronik imza ile imzalanmış verilerin senet değil senet hükmünde olduğunu düzenlemiştir. Bu düzenleme isabetlidir. Çünkü veri o anda senet halinde değil de elektronik belge halinde de olabilir[388].

18/21 sayılı İçtihadı Birleştirme Kararının Tahlili, (İÜHFM 1959/1-4), s. 380 vd; Konuralp-Delil Başlangıcı, s. 33.

[387] Bu yönde tanımlar için bkz. Umar/Yılmaz, s. 2; Kuru/Arslan/Yılmaz, s. 424.

Doktrinde Konuralp[389], HUMK m. 295/A hükmünün dolaylı olarak elektronik senedi düzenlediğini, elektronik senedin tanımının ise yapılmadığını, ancak elektronik senedin tanımının "bir kimsenin kendi güvenli e-imzası ile meydana getirdiği ve aleyhine delil olarak kullanılma amacı taşıyan ve bilgisayar ortamında varlığını sürdürebilen elektronik veriler" şeklinde yapılabileceği görüşündedir.

Kanımca, kanun koyucu elektronik senet tabirini bilinçli olarak kullanmaktan kaçınmış ve sadece, elektronik verilerin senet hükmünde" olduğunu kabul etmekle yetinmiştir. Böyle bir durumda kanun koyucunun elektronik verilere vermek istemediği senet vasfının kendilerine tanınamayacağını kabul etmekteyiz[390]. Kanun koyucunun böyle bir kabulündeki sebep, elektronik imzanın, senetteki imza kadar müşahhas olmamasıdır. Hemen belirtelim ki, müşahhaslıktan kastettiğimiz imazının kişiye aidiyeti, gerçekliği konusundaki ihtimaliyet derecesi olmayıp, imzanın somut olarak algılanabilir olmasıdır.

Burada belki tartışılması gereken husus elektronik imzalı olduğu için senet hükmünde sayılan belgelerin adi senetlerin mi yoksa resmi senetlerin mi hüküm ve sonuçlarını doğuracağıdır.

Resmi senetler, resmi bir makamın katılımı ile düzenlenen senetlerdir. Resmi makamların katılımı düzenleme biçiminde olabileceği gibi onaylama biçiminde de olabilir. O halde resmi makamın katılımı yalnızca imza ve tarih onaylaması suretiyle de olsa, senet ispat hukuku anlamında resmi bir senettir[391].

Elektronik imzalı verilerin adi senet mi yoksa resmi senet mi sayılacağı büyük oranda elektronik sertifika hizmek sağlayıcılarına atfedilecek niteliğe göre belirlenecektir. Kanundaki düzenleme bu konuda kolayca karar verilebilecek nitelikte değildir.

Kanımca elektronik imza ile imzalanmış verilerin senet hükmünde sayılmasının onaylama biçiminde düzenlenmiş resmi senetler olarak kabul edilmesi ve elektronik imza ile imzalanmış verilerin içeriğinin aksinin, elektronik imzanın ve tarihin ise ise sahteliğinin ispat edilebilmesi gerekir.

---

[388] Deliduman, Seyithan, Elektronik Verilerin Delil Değeri, II. Türkiye Bilişim Hukuku Sempozyumu,28.05.2004,

[389] Genel Hatlarıyla Elektronik İmza Kanunu, s. 5 (http://www.tbb.org.tr/turkce/konferans.htm).

[390] Tam bir benzerlik olmamasına rağmen benzetmek gerekirse, tıpkı ilam niteliğinde sayılan belgelerin ilamlardan farklı olmasında olduğu gibi. Örneğin ilam hükmünde sayılan noter senetlerini noter ilamı olarak nitelendiremeyiz.

[391] Deliduman-Noter Senetleri, s. 16.

6.1.5.5.2 Elektronik İmza İle İmzalanmamış Verilerin Delil Değeri

Elektronik İmza Kanunu sadece güvenli elektronik imzanın unsurlarını ve hukuki sonuçlarını düzenlemiş olup güvenli olmayan, başka bir ifade ile, güvenli elektronik imzanın dışında kalan elektronik imzanın hukuki niteliğini düzenlememiştir.

Kanunun güvenli olmayan elektronik imzayı ve hukuki sonuçlarını düzenlememiş, olması bilinçli olarak bırakılmış bir boşluktur. Çünkü Avrupa Birliğinin 93 sayılı Direktifinin 5. maddesinin 2. Bendine göre, üye ülkeler her türlü elektronik imzanın delil olarak kullanılabilmesine olanak sağlamayı üstlenmişlerdir. Buna göre, güvenli olmayan elektronik imzaya da, güvenli elektronik imza kadar olmasa bile, bir ölçüde caiz delil sayılma özelliği tanınmak istenmiştir[392]. Bunda çıkan sonuç güvenli elektronik imza dışında kalan, başka bir ifade ile, güvenli olmayan elektronik imzalarla imzalanmış veya hiç imzalanmamış elektronik veriler de delil olarak kullanılabilecektir.

Güvenli olmayan elektronik imzalar kanuni (kesin) delil olmayacağından takdiri delil olarak değerlendirilebilir. O halde, güvenli olmayan elektronik imza ile imzalanmış veya elektronik imza ile imzalanmamış elektronik veriler kanunda düzenlenmemiş deliller kapsamına girer[393].

Güvenli elektronik imza ile imzalanmamış elektronik veriler takdiri delil olarak kabul edilebileceğine göre, bu konudaki usul kuralı dayanağımız hangisi olacaktır. İlk akla gelen HUMK m. 367'de düzenlenmiş olan "özel hüküm sebepleri"dir. HUMK m. 367 hükmü şu şekildedir: "Tahkikat hâkimi senetsiz ispatı caiz olan davalarda re'sen veya talep üzerine bu kanunda düzenlenmemiş olan diğer hüküm sebeplerinin istima ve tetkikatına karar verebilir ve bu husus hakkında iki tarafı istima ettikten sonra tebeyyün edecek hale göre iktiza eden tedbirleri ittihaz eder".O halde açıkça görülmektedir ki, güvenli elektronik imza ile imzalanmamış elektronik verilerin HUMK m. 367 kapsamında değerlendirilmesi mümkündür.

Sorunun çözümünde bir diğer çıkış yolu olarak da Hukuk Usulü Muhakemeleri Kanunu m. 287, II ve m. 289 hükümlerinde düzenlenmiş olan delil sözleşmesine ilişkin düzenleme görülebilir[394]. Ancak hemen belirtelim ki, tarafların elektronik verilerin delil

---

[392] Konuralp, s. 4.

[393] Aynı yönde, Pekcanıtez, H., Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri (Uluslar arası İnternet Hukuku Sempozyumu, İzmir 2002), s. 424.

[394] Kanuni delil sisteminin sonucu olarak, kanunun belli bir delille ispatı aradığı vakıaların ispatı için başka delillerin kullanılması mümkün olmadığından kanun, taraflara, belli vakıaların belli delillerle ispatı konusunda anlaşma yapabilme imkanı vermiştir. Bu durumda tarafların arasındaki delil sözleşmesine göre sözleşme konusu vakıanın ispatında başka delillerin kullanılamayacağı hükme bağlanmıştır (HUMK m. 287, II). Delil sözleşmesi belli vakıanın, belli bir delil veya diğer deliller yanında kararlaştırılan türdeki deliller ile ispat edilebileceği konusunda taraflar arasında davadan önce veya dava sırasında yapılan usuli bir sözleşmedir (Alangoya, s. 373; Pekcanıtez/Atalay/Özekes, s. 396; Pekcanıtez, s. 420. Karş. Taşpınar, s. 184).

olarak kullanılabileceğine ilişkin olarak yaptıkları delil sözleşmesi de çoğunlukla elektronik ortamda gerçekleşeceğine göre, burada artık elektronik imza ile imzalanmış elektronik verilerdeki elektronik imzanın güvenli elektronik imza olup olmamasına göre getirilecek çözüm de farklı olacaktır.

Galiba bu konuda en kolay çözüm sunan husus, güvenli olmayan elektronik imza ile imzalanmış olan verilerin delil olarak kullanılmasına karşı tarafça muvafakat edilmesidir.

Güvenli elektronik imza ile oluşturulmuş veriyi, imzaladığı iddia edilen taraf, imza inkârında bulunursa, Hukuk Usulü Muhakemeleri Kanununun 308. maddesi kıyas yoluyla uygulanacaktır. Bu maddenin kıyas yoluyla uygulanması için, yine öncelikle elektronik belgenin güvenli elektronik imza ile imzalanmış olup olmadığının tespiti gerekir. Zira güvenli elektronik imza dışında kalan imzalar bakımından, bu belgeler senet sayılmadığı için, imza incelemesine ilişkin Kanunun 308. maddesinin uygulanması mümkün olmayacaktır. İmza kontrolünde hem belgenin değiştirilip değiştirilmediğinin hem de imzaladığı iddia edilen kişiden sadır olup olmadığının incelenmesi gerekir. Bu sebeple hem imzanın kontrolü hem de sertifikanın kontrolü gerekecektir.

6.1.5.5.3 Elektronik Belge

Hukuk Usulü Muhakemeleri Kanununda senedin tanımı yapılmamıştır.Ancak doktrinde hukuki anlamda senet, bir kimse tarafından bir vakıanın gelecekteki delilini teşkil etmek üzere yazıp veya yazdırılıp imzalanan ve imzalayan aleyhine delil teşkil eden yazılı belgedir[395]. Buna göre, senet yazılı bir belgede açıklanan irade beyanıdır[396].

Elektronik belge ise dediğimizde, en basit ifadeyle elektronik ortamda sayısal olarak kodlanmış şekilde bulunan elektronik veriler kastedilmektedir. Bu anlamda İnternet üzerinden yapılan hukuki işlemler, e-mail yoluyla gönderilen irade beyanları, çeşitli veri taşıyıcılarına kaydedilmiş ve irade açıklaması içeren elektronik veriler aklımıza gelmektedir.

Elektronik belge veya elektronik kayıt gibi terimler, elektronik ortamda yaratılan bir bilgiyi ifade etmek üzere kullanılmaktadır.

---

[395] Postacıoğlu İ. E., Medeni Usul Hukuku Dersleri, İstanbul 1975. Benzer tanımlar için bkz. Berkin-Senetler, s. 9; Üstündağ, Medeni Yargılama Hukuku, İstanbul 1997, s. 637.

[396] Kuru, B., Hukuk Muhakemeleri Usulü, C. II, İstanbul 1990, s. 1427.

Belge, medeni usul hukukundaki senet kavramından geniş bir anlama sahiptir. Her senet bir belgedir, fakat her belge medeni usul hukuku anlamında senet özelliklerini taşımaz.

Elektronik imzalı belge teriminden hukuki işlemlerde, elektronik (irade) açıklamaları ve imzanın anlaşılması gerekir.

Elektronik belgeler üç şekilde karşımıza çıkmaktadır.

- Bilgisayarın belleğinde veya veri taşıyıcısında kayıtlı veriler: (Bilgisayarın Ana Belleğinde Kayıtlı veya Disket, CD Gibi Taşıyıcılarda Kayıtlı Veriler) Dış bellek birimleri, verilerin kalıcı olarak saklandığı yerdir. Bunlar, sabit diskler (hard disk), disketler, CD ler ve teyplerdir.
- Bilgisayar Ekranında Görülen Veriler (İnternet Aracılığıyla Görülen Veriler): Kişinin e-mail adresinde saklı bulunan elektronik belgeler veya bir İnternet'teki İnternet'sitesinde yayınlanan veriler örnektir.
- Bilgisayar Çıktısı ve Bilgisayar Faks: Bilgisayar çıktısı, elektronik ortamda bulunan bir verinin yazıcı (yardımcı araç) vasıtasıyla kağıtta vücut bulmuş halidir. Böylece, elektronik ortamdaki veri, elektrik mevcut olduğu sürece gözle görülebilir olan durumundan, elle tutulabilir ve her zaman görülebilir bir duruma geçmiş olmaktadır. Bilgisayar çıktısı için yazıcıya ihtiyaç bulunmaktadır. Bilgisayara bağlı yazıcı sayesinde, bilgisayar ekranında görülebilen herhangi bir veri, kağıt yüzeye aktarılmış olmaktadır.

Elektronik imzalı belge, elektronik bir usul yardımıyla imzalanmış bir elektronik belgedir. Elektronik imzalı belgeler de, irade açıklaması içerir ve düzenleyici tarafından imzalanmıştır. Elektronik imzalı belgeyle "imzalanmış verinin teknik durumu" anlatılmak istenir. Elektronik imzalı belgeler, sesler ve resimler de içerebilir. Bir elektronik imzalı belgede teknik olarak bir veya daha fazla veri söz konusu olabilir. Çünkü elektronik imza sadece bir veri üzerinde olabilir (gönderilen metnin imzalanmış ve imzalanmamış kısımları). Hukuki işlemlerde elektronik imzalı belgelerde, belgenin elektronik irade açıklaması taşıyıcısı olması ön planda bulunur. Elektronik imzalı belgelerin, imzanın taşıdığı özelliklere göre senet sayılması mümkündür (HUMK m.295A).

Elektronik İmza Kanunu'nda; güvenli elektronik imza, elle atılan imzaya eşdeğer kabul edilmiş ve elektronik imza ile oluşturulmuş verilerin senet hükmünde olacağı belirtilmiştir.

5070 sayılı Elektronik İmza Kanununun 22. maddesine göre, Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına eklenen cümle şöyledir: "Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir".

5070 sayılı Elektronik İmza Kanununun 23. maddesiyle Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere 295/A maddesi eklenmiştir. Bu maddenin birinci fıkrasına göre, "Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar."

Elektronik imzanın kullanılması ile taraflar, bir araya gelmeden sözleşme imzalayabilecekler ve belgeler oluşturabileceklerdir. Bu sözleşme ve belgeler el ürünü imza ile oluşturulan sözleşmeler ve belgeler ile aynı hukuki geçerliliğe sahip olacaktır. Böyle bir imkan, zaman tasarrufu ve hız yanında tarafları kırtasiye giderlerinden de kurtaracaktır.

Elektronik İmza Kanunu ile el ürünü imza ile elektronik imza eşdeğerde kabul edilmiş ve elektronik imza ile tanzim edilen belgelerin senet hükmünde olacağı açıkça belirtilmiştir. 5070 sayılı Kanun bu eşitliği güvenli elektronik imza için kabul etmiş ve bunu da açıkça ifade etmiştir[397]. Kanunda güvenli elektronik imzanın yapılacak hukuki işlemler açısından geçerlilik ve ispat şartını sağlayacağının belirtilmesi, elektronik imzaların güvenli elektronik imza kavramı ile sınırlandırılması sonucunu beraberinde getirecektir[398].

Güvenli elektronik imza kullanılarak yapılan hukuki işlemlerin şekil açısından geçerli olacağının 5070 sayılı Kanunda belirtilmesi nedeniyle, Kanunda belirtilen şekilde oluşturulmayan yani güvenli elektronik imza özelliğini göstermeyen, fakat elektronik imza özelliğini taşıyan imza ile düzenlenen sözleşmeler veya yapılan hukuki işlemler, şekil açısından gerekli şartları yerine getirmemiş kabul edip, geçersiz sayılacaktır.

Kanunların özel bir merasimi ya da üçüncü tarafların şahitliğini gerek gördüğü gayrimenkul satımı, gayrimenkul satış vaadi, vefa ve iştira sözleşmeleri, gayrimenkul bağışlanması vaadi, ölünceye kadar bakma akdi, vakıf senedi, evlenme, boşanma, evlat edinme, tanıma, aile şirketi emvali, resmi vasiyetname, miras sözleşmesi, irtifak hakkı tesisi, gayrimenkul rehnine ilişkin sözleşmeler, ipotekli borç senedi, noterlerce düzenleme yoluyla yapılacak işlemler(tapuda işlem yapılmasını gerektiren vekâletnameler, mülkiyeti muhafaza kaydıyla satış, vasiyetname, mirasın taksimi sözleşmesi gibi) elektronik imza kullanılarak yapılamamaktadır. Resmi şekle veya özel merasime tabi hukuki işlemlerde, hukuki işlem iradesi kanunda belirtilen şekil ve usulde noter, tapu memuru ve sulh hâkimi gibi resmi memur önünde açıklanır. Kanunda özel

[397] Bkz. 5070 Sayılı Elektronik İmza Kanunu, madde 5, 239 sayılı Yargı Mevzuatı Bülteni.
[398] FALCIOĞLU, 96.

merasim öngörülmüş, ancak resmi memur veya makam açıkça belirtilmemiş ise, her türlü resmi şekilde yapılması gereken sözleşmeleri yapmaya noterler yetkilidir[399].

Elektronik İmza Kanunu'nun 5. maddesinde böyle bir sınırlamaya gidilmesinin nedeni olarak hukuki işlem güvenliğinin sağlanması, kanuni şekil şartlarının tam olarak yerine getirilmesinin ve devamının sağlanması, hukuki işlemin taraflarının etraflıca düşünmesine imkân verilmesi gibi nedenler gösterilebilir[400]. Bu nedenle resmi şekle tabi sözleşmelerin elektronik imza ile geçerli olarak yapılabilmesi için açık bir yasal düzenlemeye ihtiyaç vardır. Elektronik İmza ile ilgili kanun hazırlayıp, bizden önce uygulamaya koyan İngiltere'de böyle bir sınırlama, elektronik imza kanunda öngörülmemiştir. Hatta tapu kayıtlarını elektronik ortama aktaran İngiltere, taşınmaz satım sözleşmelerinin elektronik ortamda ve elektronik imza kullanılarak yapılması için gerekli teknik ve hukuki alt yapı çalışmalarını tamamlamıştır[401].

5070 sayılı Elektronik İmza Kanunu sadece elektronik imza ile ilgili teknik, idari ve kısmen hukuki düzenlemeler getirmiştir. Elektronik sözleşme ve elektronik verilerle ilgili henüz ayrı bir yasal düzenleme yapılmamıştır. Elektronik sözleşmelerle ilgili olarak ayrı bir hukuki düzenleme yapılıncaya kadar, 5070 sayılı Kanun'da belirtilen şekilde bazı hukuki işlemlerin ayrık tutulması yerinde bir düzenlemedir[402]. Ancak Kanun, şekle bağlı kanuni işlemlerden resmi şekilde olanları ayrı tutmakla birlikte, adi yazılı şekle tabi (alacağın temliki gibi) sözleşmelerle nitelikli yazılı şekle tabi sözleşmelerde (el yazısı ile vasiyetname, kefalet gibi) elektronik imzanın kullanılıp kullanılmayacağı konusunda açık bir düzenleme öngörmemektedir.[403]. Bu durumda elektronik imzanın kullanılması yaygınlaştıkça ve ortaya çıkacak sorunlar netleştikçe ya Elektronik İmza Kanunu'nun 5. maddesinde değişiklik yapılmalı yada ayrıntılı düzenlemeler getiren elektronik sözleşmeler ve elektronik veriler ile ilgili yeni bir hukuki düzenleme yapılmalıdır.

İmza ile tamamlanması halinde geçerlilik kazanacak hukuki işlemler ve diğer sözleşmelerin elektronik ortamda yapılması halinde elektronik imza kullanılarak geçerlilik kazandırılacaktır. Yani elektronik ortamda yapılan işlemlerde ve sözleşmelerde şekil elektronik imza ile sağlanmaktadır[404].

Resmi şekle, özel merasime tabi sözleşmeler ile teminat sözleşmeleri, elektronik imza ile yapılamamaktadır. Bu sözleşmelerin hangi sözleşmeler olduğu

---

[399] Bkz.1512 Sayılı Noterlik Kanunu, Resmi Gazete, Sayı 14090.
[400] ORTA, 139.
[401] Elektronik İmza Semineri, 19-20 Ekim, Ankara, European Commission, TAIEX, http://taiex.cec.eu.int/images/carte/htm.
[402] Bkz. Tacidar Seyhan, Türkiye Büyük Millet Meclisi Genel Kurul Konuşması, 22. Dönem 2. Yasama Yılı, 43. Birleşim, http://www.tbmm.gov.tr.
[403] Coşkun Koçak, Yargıtay 19. Hukuk Dairesi Başkanı, Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Görüşü, 3.
[404] SAVAŞ, 320.

Elektronik İmza Kanunu'nda sayılmadığı gibi, mevzuatımızda da dağınık olarak düzenlenmiştir. Bir kısmı 818 sayılı Borçlar Kanununda, bir kısmı 1512 sayılı Noterlik Kanununda ve bir kısmı da 4721 sayılı Türk Medeni Kanununda düzenlenmiştir. Güvenli elektronik imza kullanacak olan kişilerin bu sözleşmeleri bilmesi pek mümkün değildir. Bu nedenle bu sözleşmelerin genel çerçevesinin çizilmesi yerine Kanunda açıkça sayılmasının daha doğru olacağı kanaatindeyiz. Kanunda sınırlayıcı bir düzenlemeye gidilmek istenmemesi amacıyla böyle bir düzenleme yapıldı ise, daha sonradan çıkarılan elektronik imza ile ilgili yönetmelikte örnekleme yolu ile bu sözleşmelerden bahsedilmesi, kullanıcı ve uygulayıcılar için yol gösterici olması açısından büyük bir kolaylık sağlardı.

Bir başka açıdan, 5070 sayılı Kanunun 5. maddesinde, geçerlilik açısından elektronik imza ile düzenlenemeyen sözleşmelerin teknolojik gelişmeler göz ardı edilerek genel çerçevesinin sınırlayıcı bir şekilde belirlenmesi, doğru değildir. Alt yapı çalışmaları tamamlandıkça, teknolojik gelişmelere hızla uyum sağlandıkça, yapılmaması öngörülen sözleşmeler ileride yapılabilir hale gelecektir. Örneğin, Amerika Birleşik Devletlerinde yürürlükte olan, Eyaletlerarası veya Dış Ticarette Elektronik Kayıtların Kullanılmasını Kolaylaştıracak Kanunun 103. bölümünde tüketicilerin korunması amacıyla elektronik imzanın kullanılmayacağı alanlar belirtilmiştir. Ancak aynı kanunun 103/c'de Ticaret Bakanlığına 3 yıllık süre içerisinde bu yasaklamanın gerekli olmaya devam edip etmediğini kontrol görevi vermiştir. Bu da getirilen bu kısıtlamanın mutlak olmadığını gerekirse kaldırılıp, bu alanlarda da elektronik imza kullanılmasına izin verilebileceğini göstermektedir[405].

Medeni usul hukukumuzda, ispat kuralının genel çerçevesi Neuchatel sistemine göre belirlenmiş, hukuki işlemlerin ispatı ise Alman hukukundan da etkilenerek Fransız sistemine göre belirlenmiştir[406].

Hukuk Usulü Muhakemeleri Kanunu madde 288 ve devamı hükümlerinde, hukuki işlemler bakımından senetle ispat zorunluluğunu getirirken, açıkça düzenlenen kanuni ispat halleri dışında delil serbestîsi esasını benimsemiştir[407].

İddianın ispatı için kullanılan deliller, kesin deliller ve takdiri deliller olarak ikiye ayrılmaktadır. İkrar, kesin hüküm, yemin ve senet kesin delil grubu içerisinde yer alır. Bu deliller üzerinde hakimin serbestçe takdir yetkisini kullanması söz konusu değildir. Hakim sunulan kesin deliller ile bağlı olup, bu delilleri sunan taraf iddiasını ispatlamış sayılmaktadır[408] . Takdiri deliller ise; tanık, bilirkişi, keşif ve özel hüküm sebebidir.

[405] KESER, L.,Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi,s. 3
[406] YILDIRIM, 118.
[407] DELİDUMAN, 1.
[408] KONURALP,H., Yazılı Delil Başlangıcı, s . 26.

Takdiri deliler konusunda hakimin geniş bir takdir yetkisi olup, bu delilleri serbestçe değerlendirir.

Elektronik imza ile imzalanmış belgelerin, medeni usul hukukumuzda yer alan delil sistemi içerisinde hangi delil grubuna dahil olacağına ilişkin olarak doğacak tereddütleri gidermek açısından, 5070 sayılı Elektronik İmza Kanunu madde 23 ile 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295. maddeden sonra gelmek üzere 295/A maddesi eklenmiştir[409]. Bu maddeye göre; " güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu verilen aksi ispat edilinceye kadar kesin delil sayılır " denilmiştir. Görüldüğü gibi Kanun, sadece güvenli elektronik imza ile oluşturulan belgelerin kesin delil hükmünü haiz olduğunu belirtmiştir. Ayrıca elektronik imza ile imzalanmış belgenin senet değil senet hükmünde olması yerinde bir ifade olup, elektronik veri şeklen senet halinde değil belge halinde de olabilir.

5070 sayılı Kanunun 23. maddesi ve 1086 sayılı Kanunun 295/A maddesinin birlikte değerlendirildiğinde, güvenli elektronik imza ile imzalanmış her türlü elektronik veri ve hatta elektronik sözleşmelerin, mahkemelerde senetlerin haiz oldukları ispat özelliklerine haiz olarak değerlendirileceği sonucuna varılmaktadır. Bu durum elektronik sözleşmeler ile diğer sözleşmelerin eşit olarak değerlendirilmesi açısından olumlu bir adımdır. Bu eşitlik için güvenli elektronik imzanın kullanılması şartının getirilmesi sınırlayıcıdır[410].

ABD'nin bir çok eyaletinde elektronik imzanın kullanımını yaygınlaştırmak amacıyla, elektronik imza ile imzalanmış belgeler kesin delil olarak kabul edilmiş hatta elektronik imzanın inkar edilmezlik özelliği nedeniyle kesin delil olarak sayılan diğer delillerden daha üstün tutulmuştur[411]. Avusturya'da ise, güvenli elektronik imza dışında diğer elektronik imzaların da, delil niteliğinin inkâr edilemeyeceği Elektronik İmza Kanununa eklenmiştir[412].

Güvenli elektronik imza dışındaki diğer elektronik imzalar bakımından, Elektronik İmza Kanunda açık bir düzenle yapılmamıştır. Bu durumda güvenli elektronik imza dışında diğer elektronik imza ile düzenlenmiş belgeler, 1086 sayılı Kanunun 367. maddesi kapsamında değerlendirilerek, senetle ispatın zorunlu olmadığı davalarda özel hüküm sebepleri içinde değerlendirilerek, takdiri delil olarak kabul edilebilir[413]. Güvenli elektronik imza içermemekle birlikte karşı tarafça gönderilen e-mailler, bilgisayar ortamında saklanan diğer veriler, bunlardan alınan çıktılar yazılı delil

[409] Bkz. 5070 Sayılı Elektronik İmza Kanunu, madde 23, 239 sayılı Yargı Mevzuatı Bülteni; 18.6.1927 tarih ve
622.623.624 sayılı Resmi Gazete, 1086 Sayılı Hukuk Usulü Muhakemeleri Kanunu, madde 295/A.
[410] FALCIOĞLU, 98.
[411] ORTA, 136.
[412] Bkz. Avusturya Elektronik İmza Kanunu, madde 3, http://www.tk.gov.tr/eimza/yabanci_mevzuat.htm.
[413] KONURALP, H. Genel Hatları İle Elektronik İmza Kanunu. s . 6.

başlangıcı olarak değerlendirilebilir. Hatta manipüle edilme ihtimallerinin az olduğu daha güvenli elektronik ortamlarda yazılı delil olarak dahi kabul edilebilir[414].

Ayrıca sözleşme serbestîsi kuralları çerçevesinde, taraflar delil sözleşmesi yaparak güvenli elektronik imza haricindeki diğer elektronik imzalar ile düzenlenmiş elektronik verilerin, anlaşmazlık halinde mahkemelere delil olarak sunulabileceğini öngörebilirler. Kesin deliller ile ispatın zorunlu olmadığı davalarda, taraflardan birinin mahkemeye sunacağı güvenli elektronik imza özelliği olmayan elektronik imza ile imzalanmış bir belgeye, diğer taraf itirazda bulunmayarak bu belgenin delil olarak davada kullanılmasına ve değerlendirilmesine zımnen rıza verebilir[415] .

Mahkemece, mahkemeye delil olarak sunulan belgenin güvenli elektronik imza ile imzalanıp imzalanmadığı karşı tarafın itirazı, imzanın inkarı veya gerekli görüldüğü takdirde resen araştırılır. Bu durumda davanın taraflarınca delil olarak gösterilen elektronik belgenin mahkemeye ibrazı, elektronik veri taşıyıcısı olan CD, DVD, disket ve USB gibi araçlarla veya mahkemeye gönderilecek e-mail ile olacaktır[416] .

Elektronik belgelerdeki, kayıtlardaki veya senet hükmünde olan elektronik verilerdeki imzanın inkârı halinde, mahkemece nasıl bir inceleme yapılacağı konusunda sadece güvenli elektronik imza ile oluşturulan belgeler için 1086 sayılı Kanunun 295/A maddesinde ikinci fıkrasında belirtilmiştir. Buna göre, dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkar ederse, 1086 sayılı Kanunun 308. maddesi kıyasen uygulanacaktır. Yani imza inkarı halinde hakim, mahkeme huzurunda imzayı inkar eden tarafın tatbiki imzalarını alacak, imza inkarında bulunan tarafın resmi kurumlarda bulunan tatbik imzalarını dosyaya getirtecek ve bunları üzerinde bilirkişi incelemesi yaptıracaktır. Bu araştırma şeklinin güvenli elektronik imzanın inkârı halinde nasıl uygulanacağı konusunda pek çok tartışma olmakla birlikte henüz somut bir uygulama yoktur.

Güvenli elektronik imzanın özelliği inkâr edilmez olmasıdır. İnkâr edilmesi halinde bu imzanın dayandığı elektronik sertifika ve bu elektronik sertifikayı sağlayan elektronik sertifika hizmet sağlayıcısından belki bir araştırma yapılabilir. Ancak tatbiki imzaları toplayıp bilirkişi incelemesi yaptırmak, bir uygulayıcı olarak kanaatimce istenilen sonuca götürmeyecektir.

---

[414] BOZBEL, 303.

[415] Bkz. 18.6.1927 tarih ve 622.623.624 sayılı Resmi Gazete, 1086 Sayılı Hukuk Usulü Muhakemeleri Kanunu,
madde 287 ve 289.

[416] Ulusal Yargı Ağı Projesi kapsamında, pilot uygulamaları süren adliyelerde elektronik ortamda yargılama yapılmakta ve deliller de elektronik ortamda toplanabilmektedir. Dolayısıyla davada gösterilen bir delilin elektronik ortamda mahkemeye ibrazı mümkündür.

Ancak yine de güvenli elektronik imza veya basit elektronik imza ile kullanılarak düzenlenen kayıtların, belgelerin veya sözleşmelerin delil olarak kabul edilmesi, bu işlemler bakımından hukuki güvenliği tesis edecek ve elektronik ticaretin gelişmesine katkıda bulunacaktır [417].

Elektronik imza kavramı, uygulamaya ve hukuk sistemimize 5070 sayılı Elektronik İmza Kanunu ile birlikte girmiştir. Daha doğrusu güvenli elektronik imza kavramı ilk defa Elektronik İmza Kanunu ile gündeme gelmiştir. Toplumumuzun çoğu tarafından bilinmeyen ancak hem uluslarası ilişkilerde hem de modern toplumlarda günlük hayatta sıkça kullanılan elektronik imza, günlük hayatı ve iş hayatını kolaylaştıran bir vasıtadır.

Teknolojinin gelişmesi ve İnternet ağının yaygınlaşması ile aslında güvenli olarak nitelendirilemeyen elektronik imzalı belgeler, sanal ortamda dolaşmaya başlamıştır. Bu belgelerin değiştirilmesi ihtimalinin olması ve elektronik belge, veri ve kayıtlara hukuki güvence getirilmesi ihtiyacının bir sonucu olarak Elektronik İmza Kanunu çıkarılmıştır

Elektronik imza konusunda düzenleyici ve denetleyici kurum olarak belirlenen Telekomünikasyon Kurumu, bu yöndeki çalışmalarını 5070 sayılı Kanundan aldığı yetki ile devam ettirmektedir. Ayrıca 2004/21 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının çalışanlarıyla birlikte nitelikli elektronik sertifikalarını sağlamak amacıyla kamu sertifikasyon merkezi oluşturulmuştur. Bu merkezin işletimi TÜBİTAK-UEKAE'ye verilmiştir.

Elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik imza, elektronik belgenin kimin tarafından oluşturulduğunu ve belgeyi oluşturma ifadesini doğrulayan elektronik bir kayıttır. Elektronik sözleşmeler ve işlemler açısından ise, şekil şartını sağlayan bir unsurdur.

Güvenli elektronik imza dışında kullanılan bir takım elektronik imzalar da olmakla birlikte, 5070 sayılı Kanun tarafından geçerli kabul edilen ve kesin delil niteliği verilen imza, açık anahtar alt yapısı ve biyometrik tanımlama yöntemleri kullanılarak oluşturulan güvenli elektronik imzadır.

Elektronik İmza Kanunu'nun yürürlüğe girmesi ile BK. da düzenlenen klasik imza ile güvenli elektronik imza aynı bazı istisnalar haricinde aynı hukuki sonuçları doğurmaktadır. Getiren istisnalar 5070 sayılı Kanunun 5. maddesinde sayılmış bulunan ve kanunlarca özel bir merasimin öngörüldüğü, üçüncü kişilerin katılımının istendiği bir

[417] ÇELİKOĞLU, 16.

takım hukuki ilişkilerdir. Elektronik ortamın güvenliğinin artması, teknolojinin gelişmesi ve kullanımının yaygınlaşması ile ayrık tutulan hukuki işlemlerinde ileride güvenli elektronik imza kullanılarak yapılması mümkün olabilecektir.

Güvenli elektronik imza ile imzalanmış belgeler mahkemelerde kesin delil olarak değerlendirilebilmektedir. Hukuk Usulü muhakemeleri Kanununa eklenen 295/A maddesi ile elektronik imza ile oluşturulan elektronik veriler senet hükmünde sayılacak ve aksi ispat edilinceye kadar kesin delil olarak değerlendirip işlem görecektir.

Elektronik ortamlarda bilgi alışverişi üzerine kurulmuş bulunan elektronik ticaretin gelişmesi, elektronik sözleşmelerin yaygınlaşması için elektronik imzaya hukuki bir geçerlilik kazandıracak böyle bir Kanuna olan ihtiyaç Elektronik İmza Kanunu ile giderilmiştir. Bu şekilde ticari değeri olan-olmayan elektronik belgeler, taraflar için hukuki yükümlülük doğurabilecektir. Taraflar bir araya gelmeden belge ve sözleşme oluşturabilecekler ve bu belgeler klasik imzalı belgeler ile aynı hukuki geçerliliğe sahip olacaktır.

Alt yapı çalışmaları ve yasal düzenlemelerin tamamlanması ile elektronik imza uygulamada yaygın olarak kullanılacaktır.

6.2 HUMK'da Yeni Düzenlemeler Öngören Hukuk Muhakemeleri Kanunu Taslağı'nda Bilişim Hukuku

6.2.1 Genel Olarak

Hukuk Muhakemeleri Kanunu Tasarı genel olarak eski Kanunun sistematiğini koruyarak yeniden düzenleme yapmış ve genel olarak başarılı bir çalışma olarak göze çarpmaktadır.

Ancak Tasarıda yapılan hukuki işlemlerin ve usuli muamelelerin genel olarak kâğıt ortamında yapıldığının kabulü ile hareket edildiği ve düzenlemelerin bu ortama göre yapıldığı değerlendirilmiştir. Her ne kadar 154.madde de olduğu gibi zaman zaman Bilişim Teknolojilerinin gelişmelerinden esinlenerek bazı düzenlemeler yapılmış ise de BT teknolojilerinin daha fazla hukuk sistemimizde kullanılabilmesi ve birçok kamu Kurumunda hayata geçen BT kullanıldığı bilişim sistemleri ve Türkiye'de Ağır Ceza Merkezleri bazında büyük çoğunluğunda işletime alınmış olan Ulusal Yargı Ağı Projesi ve elektronik ortamın sağlamış olduğu olanaklar göz önünde bulundurularak kâğıt ortamında yapılan işlemlerin aynı zamanda sadece elektronik ortamda da yapılmasına imkân verecek şekilde yeniden Tasarının baştan sona gözden geçirilmesi yerinde olacaktır.

6.2.2 E-Dava Geliyor

Tasarı da yazılı olarak başvurmanın zorunlu tutulduğu yerlerde aynı zamanda güvenli elektronik imza kullanarak avukatların veya vatandaşların dava açabilmesi için olanak sağlanması gerekmektedir. Bu yönü ile Tasarının Alman Parlamentosunun 2000 yılında Alman Hukuk Usulü Kanununda yaptığı büyük reform sırasındaki değişikliklerde ve Alman Hukuk Usulü Kanunun 130 a maddesinde olduğu gibi elektronik ortamda dava açmaya imkân verecek şekilde yeniden düzenleme yapılması bir ihtiyaçtır. Yine Alman Parlamentosunun 22 Mart 2005 tarihinde kabul ettiği Adalet İletişim Kanunu (Justizkommunikationsgesetz[418]) ile Usul Kanununu baştan sona gözden geçirmiş ve kâğıt ortamında yapılan işlemlerin elektronik ortamda yapılmasına olanak veren düzenlemeleri Usul Kanununa işlemiştir. Bu bağlamda özellikle 130 b maddesini yasaya dâhil ederek mahkemelerde yapılan her türlü yazışma ve resmi işlemleri güvenli imza ile elektronik ortamda da yapılmasına olanak sağlamıştır.

Tasarıda yazılı olarak başvurmayı zorunlu hale getiren maddelerin aynı zamanda elektronik ortamda, kâğıt ortamının kullanılmasına gerek olmadan, elektronik ortamda hazırlanan dokümanların güvenli elektronik imza ile imzalanarak fiziksel olarak avukatın veya başvuranın mahkemeye veya adli birimlere başvurmasına ihtiyaç bırakmayacak şekilde yeniden düzenlenmesi gerekmektedir.

Şu anda UYAP Uygulamalarının mahkemelerde uygulanmasını düzenleyen mevzuat bağlamında Adalet Bakanlığının çıkarmış olduğu 124 nolu genele mevcuttur. Bu genelgenin 4.maddesi UYAP'ın işletime geçtiği birimlerde veri girişleri, soruşturma, kovuşturma, harç, duruşma, karar, infaz ve tüm adli işlemlerin UYAP üzerinden gerçekleştirilmesi, 5. maddesinde UYAP ta veri girişlerinde dosyanın mevcut bilgilerinin sisteme doğru bir şekilde girilmesi gerektiği ve tutarsız bilgi girişinin engellenmesi gerektiği, 9. maddesinde bilgisayar ortamında UYAP sisteminin kullanılarak yapılan işlemlerin kâğıt ortamında tekrar yapılmaması, kalemlerde tutulan eski defter ve kayıtlar yerine elektronik ortamda tutulan kayıt listelerinin alınarak çıktı halinde ıslak imza ile imzalanarak saklanması, 10. maddesinde ise Yargıtay, Bakanlık, C.Başsavcılıkları, Mahkemeler, İcra Daireleri, Ceza ve İnfaz Kurumları, Adli Tıp ve diğer birimlerin kendi aralarındaki adli ve idari yazışma ve işlemlerin UYAP vasıtası ile gerçekleştirilmesi, 11. maddesi tevzi ve vezne birimlerinde banka düzenine geçilerek tevzi işlemlerinin sistem üzerinden yapılarak dosyaların fiziki olarak sistemde tevzi edildiği mahkemelerine verilmesi, 12. maddesi kolluk kuvvetlerinden veya diğer ilgili birimlerden intikal eden soruşturma ve kovuşturma evraklarının ve sair belgelerin

[418] http://www.bmj.bund.de/enid/Justizmodernisierung/Justizkommunikationsgesetz_rp.html (21.04.2007)
Kanuna ulaşmak için bakınız; http://217.160.60.235/BGBL/bgbl1f/bgbl105s0837.pdf (21.04.2007)

mevzuata aykırı olmamak kaydı koşuluyla disket, CD, taşınabilir bellek vb. Elektronik veri cihazlarına kaydedilerek UYAP sistemine aktarılması sağlanması düzenlenmiştir.

UYAP'ın işlemesi ve elektronik ortamdan umulan faydaların sağlanması için asgari düzenlemeleri içeren 124 nolu genelgenin genel hatlarıyla Tasarıya da taşınmasını gerektiğini düşünmekteyiz. Bu düşüncemizi Alman Usul Kanunun 130 b maddesinde yapılan değişikliklerde desteklemektedir.

Kaldı ki ülkemizde de bazı kurumların mevzuatı güvenli elektronik güvenli imza şartı aramaksızın verilerin elektronik ortamda sistemlerde tutulabileceğini, işlenebileceğini hükme bağlamıştır. Buna örnek olarak Türkiye İş Kurumu Kanunun 22 maddesi kurumca bu kanuna göre yapılacak işlemler İnternet'te dâhil her türlü elektronik bilgi iletişim araç ve ortamı benzeri araçlar üzerinden yapılabilir ve arşivlenebilir. Elektronik ortamda bilgi ve belge istenebilir veya bilgi ve belge verilebilir şeklinde düzenleme yapmıştır. Aynı şeklinde 22 maddenin 2. fıkrasında "elektronik veya bilgi işlem ortamında yapılanlar dâhil her türlü işlemlerin ve arşivlenen bilgilerin tespit tevsikinde kurumun kayıtları esas alınır bu bilgi ve belgeler adli ve idari merciler nezdinde geçerlidir. İtiraz edilmesi halinde ispat mükellefiyeti itiraz edene aittir" denmekte ve 22 maddenin 3. fıkrasında ise elektronik ortamda bilgi ve belge alınması ve arşivleme konularına ilişkin usul ve esasların yönetmelikte belirleneceği ayrıca belirtilmiştir. Ayrıca aynı şekilde Sosyal Güvenlik Kurumu Teşkilat Kanunun 3146 sayılı kanunla eklenen ek 1a maddesinde bakanlıkça "bu kanuna göre yapılacak işlemler, İnternet'te dâhil her türlü elektronik bilgi iletişim araç ve imkânı benzer araçlar üzerinden yapılabilir ve arşivlenebilir. Elektronik ortamda bilgi ve belge istenebilir, bilgi ve belge verilebilir. Elektronik ortamda bilgi ve belge alınıp verilmesi, arşivleme konularına ilişkin usul ve esaslar yönetmelikle belirlenir şeklinde bir hüküm mevcuttur." Tasarıda yapılacak düzenlemelerde bu hükümlerden de yararlanılması mümkündür.

6.2.3 HUMK'da Elektronik ortamda Yapılan işlemler Bakımından Süreler

Tasarıda ayrıca süreler yönünden de bir gözden geçirme ihtiyacı kendisini hissettirmektedir. Zira yazılı ortamlarda yapılan klasik başvurularda genel olarak başvurular avukat veya başvuranın fiziksel olarak adliyeye giderek dilekçesini veya evrakını mahkemeye sunması gerektiğinden süreler genel olarak memurların çalıştığı mesai saatleri dikkate alınarak düzenlenmiş bulunmaktadır. Oysaki elektronik ortamda yapılan başvuruları veya sunulan evrakları sistem kabul edeceğinden ve fiziki bir başvuru ve memurun bu başvuruyu kabulü gerekmediğinden sürelerin tespitinde mesai saatlerinin dikkate alınması ihtiyacı da kendiliğinden ortadan kalkacak ve artık gün ile belirtilen süreler günün bitimi olan gece saat 24.00 a kadar yapılabilir olduğundan buna uygun düzenleme ihtiyacı da kendini hissettirecektir. Ya da elektronik ortamda Helen e-

imzalı dilekçe ve evraklar örneğin 16.00 dan sonra ertesi günün kaydını alır şeklinde düzenleme yapılması yerinde olacaktır.

UYAP sisteminde kayıtlar elektronik ortamda sistemin saati dikkate alınarak hesaplanarak yapılacağından evrakların teslim edildikleri veya kayıt edildikleri zamanlarında tespiti kâğıt ortamından daha sağlıklı bir şekilde yapılması mümkün olacaktır. Bu nedenle de Tasarı baştan sona gözden geçirilmesi gerekmektedir.

Davanın açılması zamanı başlıklı 123. maddede dava dilekçesinin yönetmelikte belirtilen şekilde dava dilekçesinin yönetmelikte belirlenen şekilde kaydedildiği tarihte açılmış sayılacağı ve dava dilekçesine davalı sayısı kadar örnek ekleneceği belirtilmiştir. Öncelikle davanın elektronik ortamda açılması halinde hangi aşamada davanın açılmış sayılacağı hususunun da maddede düzenlenmesi gerekmektedir. Örneğin dava harcının elektronik ortamda ödendiği anın sistem tarafından belirlenerek bu anda açılmış sayılabileceği hükme konu yapılabilir. Ayrıca elektronik ortamda açılan davalarda dava dilekçesine davalı sayı kadar örnek eklenmesine gerek yoktur. Zira mahkeme elektronik ortamdaki e-belgeden istenilen kadar kopyayı gerek elektronik ortamda gerekse kâğıt ortamında elde edebilir. Bunun için davalı sayısı kadar örnek ekleme şartının elektronik ortamda açılan davalar için aranmaması yönünde düzenleme yapılması gerekmektedir.

6.2.4 E-Devlet Projelerinde Entegrasyon ve Elektronik Belge Alış Verişi

Belirtilen dilekçelerin, belgelerin yanı sıra dosyaya sunulan ve fiziken mahkeme veya adliyeye teslimi şart olmayan her türlü diğer belgelerinde mahkemelere elektronik ortamdan sunulması mümkündür. Örneğin mahkemelerimiz bilişim sistemleri sayesinde artık MERNİS VERI TABANI kullanarak nüfus kayıtlarını, ADLİ SİCİL VERI TABANINI kullanarak adli sicil kayıtlarını direkt bu veri tabanlarından dosyaya intikal ettirebilmektedirler. Bunun için ayrıca ilgili idarelere yazı yazılmasına ve cevap beklenmesine gerek bulunmamaktadır. Yakın gelecekte benzer entegrasyonlar UYAP ile TAKBİS, UYAP ile Gümrük İdaresi Veri Tabanı, UYAP ile POLNET, UYAP ile Sanayi Bakanlığı Hakem Heyetleri Veri Tabanları gibi birçok resmi kurum ve kuruluşun veri tabanları arasında doğrudan veri alış veriş imkânı sağlanmış olacak ve bu bağlamda mahkemenin bir tapu kaydını, dayanaklarını, polis de mevcut kayıtları, jandarmadaki kayıtları, hakem heyetleri dosyalarını doğrudan ilgili veri tabanlarında sorgulayarak kendi dosyasına aktarabilecektir.

Örnek olarak sayılan bu veri tabanları dışında daha birçok uyum çalışması önümüzdeki yakın gelecekte gündeme gelecek ve bunun için idareler arasında protokol görüşmeleri yapılması kaçınılmaz olacaktır. Bu durumda genel olarak protokol şartları ilgili idarelerin tasarrufunda olacak ve idarecilerin kendi mevzuatlarını yorumlayarak ve

genel de kendi kurumunun bilgisini başkalarıyla paylaşmama geleneğinin etkisiyle bu süreçler uzun sürebilecek ve mümkün olandan daha az bir veri alışverişi sağlanma ihtimali ortaya çıkabilecektir. Bu ihtimallerin azaltılması devletimiz tarafından milyonlarca dolar harcanarak kurulan bilgi sistemlerinden azami faydanın sağlanması bakımından adli teşkilatın her türlü bilgi sisteminden dosyası ile ilgili bilgileri direkt bu veri tabanlarından sağlanmasına olanak sağlayıcı ve emredici bir yasal düzenlemenin Tasarıda yer alması UYAP ve benzeri e-Devlet projeleri için büyük bir getiri sağlayacaktır.

Bu bağlamda Türkiye İstatistik Kurumunun 10.11.2005 tarih 5429 sayılı Türkiye İstatistik Kanunu 6. maddesinde ”Kurum ve Kuruluşlarının resmi istatistiklerine ilişkin veri derleme değerlendirme, yayımlama görev ve yetkisi açıkça belirtilir. Bu kurum ve kuruluşlar, talep edilmesi durumunda, derlenen verileri istenilen zamanda başkanlığı vermekle yükümlüdür. ” 7. maddede ise özellikle konumuz açısından önemli şu madde yer almaktadır, ”Başkanlık (Türkiye İstatistik Kurumu Başkanlığı), kurumun görev alanına giren konularla ilgili sayım ve araştırmalarda istatistik üretimi için gerekli gördüğü her türlü ortamdaki veri ve bilgiyi tüm istatistikî birimlerden, başkanlıkça belirtilen, süre ve standartta doğrudan isteme yetkisine sahiptir. ” 7. maddenin 3. fıkrasında ise başkanlığın ”veri ve bilgi derleme ve yayınlama işlemleri dâhil her türlü işlemleri elektronik ortamda yapabilir, arşivlenebilir ve elektronik imza kullanılabilir.” denmektedir. Yine konumuz açısından çok önemli bir maddede Türkiye İstatistik Kanununun 10. maddesidir. Bu maddede ”Kurum ve kuruluşlar kendi görev alanında Ulusal Kayıt Sistemlerini başkanlığın belirlediği standartlarda oluşturmak, güncellemek ve başkanlığın istatistik amaçlı kullanımına açmakla yükümlüdür. Bu konuda yapılacak her türlü mevzuat çalışmalarında başkanlığın uygun görüşü alınır[419]. ” hükmü yer almaktadır.

Buna benzer bir hükmün Tasarıda yer alarak UYAP’ın ve diğer kamu kuruluşlarının bilgi sistemlerinin ihtiyaç duyduğu elektronik verilerin ilgili sistemlerden karşılıklı alınabilmesi için emredici ve kurumları zorlayıcı bir hüküm bulunmalıdır. 10. maddedeki bu hükmü desteklemek amacıyla yine kanunun 11. maddesi ile kurum ve kuruluşlara İstatistik Başkanlığı tarafından oluşturulan istatistik amaçlı tanım ve sınıfları kullanmakla, kendi ihtiyaçları doğrultusunda belirleyecekleri sınıflamaları kullanmaları halinde ise başkanlığın belirlediği sınıflamalara dönüştürülmesini sağlayacak tedbirleri almakla yükümlü tutmuştur. Bu maddeden hareketle Tasarıya bir madde eklenerek ilgili birimlerden gönderilecek adli verilerin şekil ve sınıflandırılmasının da adliyelere göre yapılması düzenlenebilir ve bu şekilde düzenlemesinde fayda olduğu değerlendirilmektedir.

[419] Kanaatimizce bu hüküm görüşü alınır şeklinde değiştirilmelidir.

Yukarıdaki maddelerde belirtildiği gibi yine Tasarının dilekçelerin, defter ve kayıtların harç ve masrafların tüm tutanak ve yazılı işlemlerin elektronik ortamda yapılmasını sağlamak için gözden geçirilmesi gerekmektedir.

6.2.5 E-Tebligat

Yine Tasarıyla elektronik ortamdan azami fayda sağlanması, kamu kurumlarının ve adliyelerin daha hızlı işlemesi ve UYAP ve diğer bilgi sistemlerinin tam olarak fonksiyonunu yerine getirmesi bakımından düzenlenmesi gereken bir diğer konuda e-tebligat konusudur.

Bunun için e-Tebligatın alt yapısını sağlayacağı bir e-posta sunucusunun kullanılarak ve bu sunucu üzerinde avukatlar başta olmak üzere tüm adliyede işleri olan vatandaşlara e-posta adresleri verilebilir ve bu kişilere yapılacak tebligatlar elektronik ortamda bu sunucu üzerinde verilen mail adreslerine tebliğ amacıyla gönderilebilir. Sunucu üzerinden tebligat yapılan işlemlerin kaydı tutularak ilerde çıkması muhtemel anlaşmazlıklar da bu kayıtlar kullanılarak kişilere tebligatın yapılıp yapılmadığı bir yazılım vasıtasıyla ispatlanabilir. Teknik anlamda bunların yapılması için herhangi bir engel bulunmamaktadır. Teknik bu imkânın UYAP ve diğer kamu e-Devlet Projeleri sayesinde yaygınlaştırılması ve avukatlardan başlayarak hızla kullanılmasının sağlanması çoğu zaman uzun zamanlar alan tebligatların kısa zamanda taraflara yapılarak zamandan tasarruf sağlanması mümkün olacaktır. Aynı zamanda özellikle uygulamada yakınmalara neden olan yurtdışı tebligatların bu sistem kullanılarak yapılması suretiyle harcanacak zaman çok daha kısaltılabilecektir. Bu nedenle Tebligat Kanunun 35. maddesinde yer olan iadeli taahhütlü olarak yapılan tebligat hükmünün elektronik ortamdaki karşılığı olacak bir maddenin tasarıya eklenmesi yargı hizmetlerine sürat katacağı düşünülmektedir.

Sürelerle ilgili Tasarının 96. maddesi ve devamında sürelerin nasıl işlemeye başlayacağı ve ne şekilde biteceği konuları açıklığa kavuşturulmuştur. Bu maddelere e-tebligatların ne zaman taraflara tebliğ edilmiş sayılacağı hususunu düzenleyen bir maddenin eklenmesi yerinde olur. Tebligatların e-posta sunucusuna düştüğü an tebliğ edilmiş sayılacağı gibi bu konuda hazırlanmış bir yazılımın kullanılarak, Outlook programında olduğu gibi kişilerin sadece mail sunucusuna e-postanın düşmesini yeterli görülmeyerek ayrıca e-postayı açması ve sonuna kadar gittiğini tespite yarayan programlar kullanılarak gönderilen e-postanın okunduğunun tespitinin istenmesi de mümkündür. 2000/31 sayılı e-ticaret konulu Avrupa Birliği Direktifinde de öneri bu yöndedir. Özetle tasarıya e-tebligatların ne zaman tebliğ edilmiş sayılacağı bir hüküm konulması isabetli olacaktır.

6.2.6 Kâğıt Ortamında Yapılan İşlemlerin Elektronik Ortama Göçü

Yine Tasarıya bir madde eklenmek suretiyle mahkemelerin ve kamu idareleri ilgili tüm kurumların teknik imkanlarının bulunması halinde, kendi aralarında, ve birbirleriyle olan doküman, dosya ve veri alışverişlerinin uzun süre kesintiye uğramadığı müddetçe var olan bilgi sistemleri üzerinden yapılması zorunlu hale getirilmesi gerekmektedir.

Tasarının usul ekonomisi başlıklı 36. maddesi hâkime yargılamanın makul süre içerisinde yürütülmesini ve gereksiz gider yapılmamasını sağlamakla yükümlü tutmaktadır. Tam da bu noktada UYAP sisteminin nihai hedefinin yargılamaların makul süre içinde, düzenli bir şekilde yürütülmesini ve gereksiz gider yapılmamasını ve bu arada tutarlı bir veri tabanı ile sağlıklı istatistiksel raporlar alınmasına imkân tanıyarak sağlamak olduğundan UYAP kullanımının sistemin işler durumda olduğu sürece zorunlu hale getirilmesi ve bu halde maddeye ekleme yapılması yerinde olacaktır. Bu konuda Tasarıya aşağıdaki şekilde ekleme yapılması uygun olacaktır; **Eklenmesi teklif edilen Madde:** "Bakanlık tarafından bilişim alt yapısı tamamlanarak UYAP a bağlandığı tespit olunan adli ve idari işler UYAP üzerinden gerçekleştirilir. İşletime alınan yerlerde aksi mevzuatta belirtilmedikçe dilekçeler UYAP sistemine katılır. Harç ve masraflar sistem üzerinden alınır, tutanak ve defterler sistem üzerinden tutulur, diğer veriler elektronik ortamda sisteme girilir, işlenir, alış verişi bu sistem kullanılarak yapılır ve arşivlenir. Teknik bir engel bulunmadıkça bakanlıkça elektronik imza temin edilen kullanıcılar imzalarını elektronik imza ile atarlar.

Tutanak, belge veya kayıtlarda imzası bulanacak kişilerin bazılarının elektronik imzası bulunmaması durumunda tutanak veya kayıt sistem üzerinde elektronik imzası bulunanlar tarafından imzalanır ve ayrıca bu belgenin çıktısı alınarak belgenin altına elektronik imzası olmayanlar tarafından ıslak imza ile imzalanır.

Sistemde olağanüstü kesilmeler veya arızalar meydana gelmesinde birimler durumu tutanak ile imza altına alarak tutanağı başkanlığa gönderirler.

Bu durumda sistem dışı sistemin kesik olduğu sürece işlemler kâğıt ortamında yapılarak sistem tekrar geldiğinde veriler sistem dışında tutulan kayıtlar UYAP sistemine aktarılır.

Doğası gereği veya teknik imkânsızlıklar nedeniyle elektronik ortamda yapılamayan usulü işlemler mümkünse, oluşturulan belgeler daha sonra elektronik ortama artırılır. Kanun gereği tutanak altına alınması gerekli evrak elektronik ortamda güvenli elektronik imza ile imzalanmış ise ayrıca kâğıt ortamında tutulmaz."

6.2.7 E-Noter

Tasarının Vekâletnamenin ibrazı başlıklı 82. maddesinde avukat açtığı ve takip ettiği dava ve işlerde noter tarafından onaylanan ya da düzenlenen vekâlet aslı veya avukat tarafından onaylanmış aslına uygun örneğini dava veya takip dosyasına konulmak üzere ibraz etmek zorundadır. Hükmü yer almaktadır. Ancak UYAP sistemiyle Noterler Birliği bilgi sistemi arasında entegrasyon çalışmalarına devam edilmektedir. Bu çalışmalar kapsamında yakın bir gelecekte noterler tarafından hazırlanan vekâletnameler elektronik ortamda sorgulanabilir olacak ve hâkim veya diğer bir adliye görevlisi bu veri tabanına bağlanarak ilgili vekâletnameyi buradan sorgulayabileceği gibi, noterler ve avukatlar bu vekâletnameleri elektronik ortamda güvenli elektronik imza ile imzalayarak mahkemelere UYAP sistemini kullanarak elektronik ortamda gönderebileceklerdir. Maddenin mevcut haliyle kalması durumunda entegrasyonun sağlanması halinde avukatlar ve noterler vekâletnameleri elektronik ortamda ibrazı imkânından veya mahkemelerin bu veri tabanından sorgulayarak elde ettikleri vekâletnameleri dosyasına çekerek ibrazı sağlamaları imkânı olmayacaktır. Bu nedenle bu yönde maddeye ek yapılması uygun olacaktır.

6.2.8 T.C. Vatandaşlık Numarasının Kullanımı

Dava dilekçesinin içeriği başlıklı Tasarının 124. maddesinin 1. fıkrasının c bendinde belirtilen davacının T.C.Kimlik Numarasının dava dilekçesinde bulunmasını zorunlu hale getirmesini çok yerinde ve gerekli bir düzenlemedir. Çünkü UYAP sistemi ve diğer birçok e-Devlet projeleri T.C. Kimlik Numarası üzerine kurulu bir sistemdir. Sağlıklı istatistiksel sonuçlar alınması için olabildiğince T.C. kimlik numarasının zorunlu tutulması yerinde bir düzenlemedir. 29.04.2006 tarih ve 26153 sayılı Resmi Gazetede yayınlanan 25.04.2006 tarih ve 5490 sayılı kanunun 47. maddesi ile kişiler adına düzenlenecek olan her türlü form, beyanname, kimlik kartı, vergi kimlik kartı, pasaport gibi tüm tanıtıcı belgelerde T.C. Kimlik numarasına yer verileceği, T.C. kimlik numarası ile kurumlar ile diğer tüzel ve gerçek kişilerin diğer tüm işlemlerde esas alınacağı açıkça belirtilmiştir. Tasarı bu haliyle de 5490 sayılı kanun ile uyum içerisindedir. Bu nedenle bu hükmün korunması ve davayı açan vekilinde T.C. Kimlik Numarasının dava dilekçesinde bulunmasının sağlanması yerinde bir düzenleme olacaktır.

6.2.9 Video Konferans ve Ses Kayıt Sitemlerinin Yeni Kullanım Alanları

Tasarının 154. maddesinin birinci fıkrasında ses ve görüntü nakledilmesi yoluyla oturum icrası düzenlenmiş olup, tarafların rızası olması şartı ile aynı anda görüntü ve ses nakledilmesi yoluyla bulundukları yerden oturuma katılmalarına ve usul işlemleri yapabilmelerine izin verileceği, maddenin 2. fıkrasında ise aynı yöntem ile tanıkların bilirkişilerin veya bir tarafın ifadelerinde bu yolla alınabileceği ve duruşmalara imkân verilebileceği hükme bağlanmıştır. Her ne kadar Alman Usul Kanun'un da benzer

usuller mevcut ise de Türkiye'deki mevcut durum ve zaman zaman rıza olsa bile duruşma sonrası karşı taraftaki kişinin gerçek davalı ya da davacı olmadığı yönünde bazı itirazların olması kuvvetle muhtemeldir. Bu nedenle başka tarafta herhangi bir tarafın tanık ya da bilirkişinin ses ve görüntü nakli yoluyla ifadesinin alınmasına karar verildiğinde, ifadesi alınan karşı tarafın veya bilirkişi veya tarafın bulunduğu yerde mutlaka yapılan duruşmanın ve duruşma sırasındaki ses ve görüntü nakli yoluyla ifadesi alınan kişinin kimliğini bir şekilde tutanağa geçmesinde yarar bulunduğu düşünülmektedir. Böylece bu tür teknolojinin kullanılarak yapıldığı duruşmaların hem sayısı arta bilir hem de daha güvenilir yargılama süreci yerine getirilmiş olabilir. "Better Access to Justice" Projesi kapsamında 225 ağır ceza merkezine 2006 sonu veya 2007 başlarında ses ve görüntü nakil ve kayıt sistemleri kurulacak olup, bu sistemlerin kullanılmasıyla mahkemeden mahkemeye ses ve görüntü nakli mümkün olacak, bunun yanı sıra duruşmadaki ses ve görüntüler kaydedilerek anlık veya duruşmanın hemen sonrasında tutanaklara geçirilmesi mümkün hale gelecektir. Bu sistemlerin kullanılmasıyla Tasarının 176. maddesinde belirtilen bizzat isticvap edilme de dâhil olmak üzere tüm istinabeler elektronik ortamda, ses ve görüntü nakli yoluyla bir mahkemeden diğer mahkemeye aktarılabilecektir. Hukuk mahkemeleri de ağır ceza mahkemelerinin duruşmalarının olmadığı günlerde bu sistemden ücretleri mukabilinde yararlanmaları mümkündür.

Tasarının kayıt ve yayın yasağı başlıklı 157. maddesinde duruşma sırasında fotograf çekilemeyecek ve hiç bir şekilde ses ve görüntü kaydı yapılamayacağı ve ancak dava dosyasında saklı kalmak kaydıyla yargılamanın zorunlu kıldığı hallerde, mahkemece çekim yapılabileceği ve kayıt alınabileceği hükme bağlanmıştır. Her ne kadar hukuk muhakemeleri kanunu tasarısının Adalet Bakanlığı tarafından Mayıs 2006 tarihinde bastırılan kitabının 229. sayfasında 157. maddenin gerekçesinde daha çok bu yasağın basına karşı ve yargı süreçlerine adil yargılama ve kişilik hakları ile basın özgürlüğü ve haber alma hakkı arasında bir denge kurulmasına yönelik getirildiği, ileri sürülmüş ise de kanaatimizce maddenin lafzı sadece basına karşı bir yasak getirmediği, getirilen kayıt yasağının mahkeme içinde söz konusu edildiği izlenimi ortaya çıkmaktadır. Bu şekildeki düzenleme sanıyoruz uygulamada mahkemelerin zorunlu olmadıkça duruşma işlemlerini ve safahatını ses ve görüntü kayıt sistemleri ile kayıt altına alınmasını bu haliyle engeldir ve engel olarak yorumlayacaktır. Bu da hukuk mahkemelerinin ses ve görüntü kaydı sistemlerini kullanarak kayıt yapabilmeleri için mutlaka zorunlu bir sebep aramaları anlamına gelecektir. Bu sistemlerin kullanılması hukuk mahkemeleri açısından neredeyse imkânsız veya istisnai durumlarla sınırlı olacaktır. Bu nedenle maddenin yeniden gözden geçirilerek kayıt ve yayın yasağının basın ve 3.kişilere yönelik olduğunun ve mahkemenin ses ve görüntü kayıtlarını her

halükarda kaydedip bunları saklayabileceğinin açıkça maddede yer verilmesi gerekmektedir. Kaldı ki 158. maddenin 5.fıkrasında tahkikat ve yargılama sırasında yapılan işlemler teknik araçlarla kayda alınacak olursa bu durum bir tutanakla tespit olunur demek suretiyle 157. madde ile çelişkili bir düzenleme getirmektedir. Ayrıca 158. maddenin 5.fıkrası bağlamında eğer duruşma safahatı teknik araçlarla kayda alınmışsa bunların ayrıca bir tutanakla tespiti kanaatimizce gerekli değildir. Zaten kayda alınan işlemler ve duruşma tutanağa geçirileceği için, hazırlanan tutanağın içine duruşmanın teknik araçlar vasıtasıyla ses ve görüntü kaydı sistemleri kullanılarak kayıt yapıldığı eklenebilir. İlerleyen aşamalarda bütün hâkim ve savcılara ve kâtiplere e-imza sertifikası dağıtıldığında, yapılan görüntülerin ve kayıtların elektronik imza ile imzalanarak e-arşivlerde saklanması da mümkün hale gelecek ve herhangi bir tutanak tutmaya da gerek kalmayabilecektir.

6.2.10 Resmi Tutanakların Elektronik Ortamda Tutulması

Tutanağın imzalanması ve imza atamayanların durumu başlıklı Tasarının 159. maddesinde tutanağın hâkim ve kâtip tarafından derhal imzalanacağı emredici bir şekilde ifade edilmiştir. Bu düzenleme 1086 sayılı kanunun 152. maddesine tekabül etmekte ve orada olmayan imza bilmeyenler için ne gibi işlem yapılacağı açıklığı kavuşturulmakta ve eski sistem devam ettirilmektedir. Eğer duruşma safahatı 158. maddenin 5. fıkrası ve 154. madde kapsamında kayıt altına alınması halinde tutanaklar duruşmanın sonrasında da yazılabilecektir. Nitekim bu ihtimali göz önünde bulunduran mülga 1412 sayılı Ceza Muhakemeleri Usulü Kanunun 264.maddesi 1985 yılında değiştirilerek mahkemece gerekli bulunduğunda duruşma safahatı mahkemenin uygun ve lüzumlu göreceği teknik araçlarla tespit olunabileceği ve bu tespite dayanılarak SONRADAN düzenlenecek duruşma tutanaklarının duruşma safahatına uygun olduğu ve mahkeme başkanı ve tutanağı düzenleyen zabıt kâtibi tarafından tasdik edilir şeklinde idi ve amaca daha uygun bir düzenleme idi. Bu düzenleme daha sonra 5271 sayılı ceza muhakemesi kanunu 219 maddesinin 1.fıkrasının 3. cümlesiyle duruşmada yapılan işlemlerin teknik araçlarla kayda alınması halinde bu kayıtlar vakit geçirilmeksizin yazı tutanak dönüştürülerek mahkeme başkanı veya hâkim ile zabıt kâtibi tarafından imzalanır hükmü getirilmiştir. Görüldüğü üzere daha önceki 264. maddede tespitlerin sonradan düzenlenecek duruşma tutanaklarına geçirileceği belirtilirken 219. madde ile vakit geçirilmeksizin yazılı tutanağa geçirileceği hükme bağlanmıştır. “Better Access to Justice” Projesiyle kurulacak 225 ağır ceza mahkemesindeki ses ve görüntü kayıt sistemlerini hukuk mahkemelerinin de kullanabilme ihtimalleri ve ayrıca ilerde benzer bir sistemin hukuk mahkemeleri içinde kurulmaları halinde hâkimler duruşmaları o an zapta geçirmeyerek ses ve görüntü kayıt sistemleri ile duruşmaları kaydedebilecek ve duruşmalar bittikten sonra kayıtları zapta

geçirebileceklerdir. Bu da onlara duruşmadaki ifadelerin ayrıca özetlenerek tutanağa geçirilmesi işinden kurtarmış olacak ve hâkimler daha çok kendilerini duruşma sırasındaki beyanlara ve ifadelere odaklanabilecekler ve duruşmalar daha kısa süre içinde bitebilecektir. Bu imkânın kullanılması için Tasarıdaki 159. maddeye eğer teknik aletler kullanılarak duruşmanın kayda alınması halinde bu kayıtların vakit geçirilmeksizin veya duruşma sonrasında yazılı tutanağa dönüştürülme imkânın yaratılması gerekmektedir.

Dosyaya belge konulması ve dosyanın başka yere gönderilmesi başlıklı Tasarının 163. maddesinde dava ile ilgili belgelerin ne şekilde dosyasına konulacağı açıkça ifade edilmiş ve ayrıca ikinci fıkrada başka bir resmi merciice dosyanın gönderilmesi gerektiğinde Hâkimin belgenin aslı yerine onaylı bir örneğinin gönderilmesine karar verebileceği hükme bağlanmıştır. Maddede görüldüğü üzere kâğıt ortamında dosyaya belge konulması veya dosyanın başka yere gönderilmesi bakımından düzenleme yapılmış olup, elektronik ortamda belge ve dosyanın başka yere gönderilmesi konusunda herhangi bir düzenleme mevcut değildir. Oysaki UYAP sistemi içerisinde milyonlarca dava dosyası veya takip dosyası mevcut olup bu dosyalar C. Savcılıklarından mahkemelere, mahkemelerden Yargıtay'a, Yargıtay'dan mahkeme ve savcılıklara ve daha sonra Cezaevlerine gönderilip tekrar geri alınmaktadır. Özetle artık elektronik ortamda milyonlarca dolaşan dava ve takip dosyası vardır. Yine icra takip dosyaları icra mahkemelerine UYAP üzerinden gidip gelmektedir. Bu dosya trafiğinin hukuki altyapısına kavuşturulması için maddeye ek yapılması zorunludur.

Belge başlıklı Tasarının 203. maddesinde elektronik ortamdaki verilerin de kapsama alınarak yerinde bir düzenleme yapıldığı değerlendirilmektedir. Ancak elektronik ortamdaki veriler tabirinin sınırlayıcı olmamak kaydıyla her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletişim sistemlerinin vasıtasıyla iletilebilen, gönderilip alınabilen veriler olarak örnek kabilinden maddede sayılması uygun olacaktır.

Adi senetlerin ispat gücü başlıklı Tasarının 209. maddesinin ikinci fıkrasında usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir ibaresi 5070 sayılı kanun ile uyumlu olup, ancak yeterli olmadığı değerlendirilmektedir. Alman Usul Kanunun 130b maddesinde olduğu gibi güvenli elektronik imza ile imzalanan her türlü dilekçe, tutanak, belge ve diğer dokümanların geçerli ve tek başlarına yeterli olduğuna ilişkin maddeye ek yapılması uygun olacaktır.

6.2.11 Mahkemeye E-Posta İle Tanık, Bilirkişi Daveti ve Dinlenmesi

Tanığın davet edilmesi başlıklı Tasarının 246. maddesinin son fıkrasında e-posta ile tebligat yapılabileceği düzenlenmiş olup, ancak davete rağmen gelmemeye bağlanan sonuçların bu durumda uygulanmayacağı öngörülmüştür. UYAP sistemi içerisinde tüm adli işlemlerin elektronik ortamda yapılması hedeflenmiş olup, bu cümleden olmak üzere tebligatın da elektronik ortamda yapılmasında hem sürat hem de pratiklik bakımından birçok yararları bulunduğu veya yararlı olacağı tartışmadan varestedir. E-tebligatların geçerli hale gelmesi için örneğin Adalet Bakanlığı tarafından sağlanan e-posta sunucusu üzerinde taraflara ve öncelikli olarak da taraflara e-posta hesabı tanımlanarak, adli tebligatlar bu e-posta hesaplarına yapılabilir ve bakanlık bu e-postaların açılıp açılmadığını, okunup okunmadığını bir yazılım vasıtasıyla tespit ederek bu hesapların kayıtlarını tutabilir. Bunun için gerekli olan teknik altyapı Bakanlığımızda mevcuttur. Bu hazır altyapının kullanılarak ve Tebligat Kanunun 35. maddesine de ek yapılarak tebligatların elektronik ortamda yapılması ve bunun bağlayıcı olarak tasarıya yansıtılması gerekmektedir.

Tanığın dinlenme şekli başlıklı Tasarının 264. maddesinin beşinci fıkrasında tanığın sözleri tutanağa yazılarak önünde okunacağına ve tutanağının altının kendisi tarafından imzalanacağına amirdir. Güvenli e-imza kullanan tanıkların bu imzalarını kullanmak suretiyle tutanak altına elektronik imzalarının alınması dosyanın tamamının elektronik ortamda tutulmasını temin bakımından gerekli ve önemli bir ihtiyaç olduğu düşünülmektedir. Her ne kadar günümüzde elektronik imzanın kullanımı çok yaygın olmasa da yakın gelecekte bu kullanım şeklinin hızla yaygınlaşacağı ve böylece elektronik ortamın daha fazla kullanılacağı öngörülmektedir. Bu nedenle yakın gelecekte bu ihtiyaca yönelik tasarıda düzenleme yapılması, aynı şekilde tutanağın da Alman Usul Kanunun 130b maddesine benzer bir madde tasarıya eklenerek, elektronik ortamda tutulmasına olanak sağlanması faydalı olacaktır.

Bilirkişilerin görevlendirilmesi başlıklı Tasarının 272. maddesinde genel olarak bilirkişilerin ne şekilde görevlendirileceği tespit edilmiş olup genel olarak Ceza Muhakemesi Kanunundaki yapıya benzer bir yapının öngörüldüğü anlaşılmaktadır. UYAP sisteminde bilirkişilerin listesinin komisyonlar tarafından belirlendikten sonra merkezi bir veritabanında tek bir tabloda tutulması ve oradan bilirkişilerin takip edilmesi, hem uygulamada hem de pratik olarak birçok yararlar sağlayacağı kanaati Başkanlığımızda mevcuttur. Böylece mahkemeler kendi mahkemeleriyle ilgili ekranlardan bilirkişi listelerine erişebilecekler, atayabilecekler, gerekirse yenileyip listeleri sürekli canlı tutabileceklerdir. Aynı zamanda tüm Türkiye'deki bilirkişi listelerine ulaşarak komşu illerden ve Büyükşehirlerdeki bilirkişi listelerinden de haberdar

olabileceklerdir. Bu nedenlerle bilirkişi listesinin merkezi veritabanında tutulması ve bu tablo üzerinden işlemlerin yapılması için maddeye fıkra eklenmesi uygun olacaktır.

Bilirkişilerin merkezi veritabanında bilgilerinin tutulması halinde sağlanacak bir fayda da, bilirkişilerin gelirlerden elde ettikleri paralardan yapılacak gelir vergisi kesintilerinin daha sağlıklı bir şekilde takip edilmesine imkân verecek olmasıdır. Mevcut UYAP sisteminde herhangi bir bilirkişi Türkiye'nin herhangi bir adli biriminden yapmış olduğu bilirkişilik hizmeti karşılığında aldığı paraların toplamı hesaplanarak ödeyeceği gelir vergisi bu toplam üzerinden hesaplanmaktadır. Uyak'tan önce çok farklı yerlerde bilirkişilik yapan kişiye ödenen bilirkişili ücreti üzerinden en düşük gelir vergisi diliminden kesinti yapılırken, artık sistem toplam geliri otomatik hesapladığından kesintiyi de otomatik olarak gelir vergisine tabi kazanç daha üst dilimlerden kesintiyi gerektiriyorsa bu kesinti sistem tarafından otomatik olarak hesaplanmakta ve tahsil edilmektedir.

7 FİKRİ SINAÎ HAKLAR VE BİLİŞİM

7.1 Giriş

İnternet kullanımının artması ile birlikte fikri haklar ile ilgili düzenlemeler de bir kere daha gündeme gelmektedir. İnternet üzerinde bilgilerin yayılması, İnternet kültürünün artması ile birlikte fikri haklar için bir taraftan avantaj sağlarken diğer taraftan da şimdiye kadar mevcut olmayan bir başka tehlikeyi de beraberinde getirmektedir420.

Eser hakkı sahibine İnternet yeni imkânlar sunmaktadır. İnternet telif hakları için iyi bir reklâm yolu sağlamaktadır. Eser hakkı sahibi, eserini üçüncü ve ilgili kimselere daha çabuk ve daha ucuz bir reklâmla tanıtabilme imkânına kavuştuğu gibi, eserini dijital ortamda yayınlayabilme imkânına da kavuşmuştur. Ayrıca eserler dijital ortamda satışa da sunulabilmektedir.

İnternet yoluyla dünyanın her tarafından esere ulaşanların çokluğu ve kullanıcıların çeşitliliği, eserin haksız ve izinsiz kullanılması ihtimalini de artırmıştır. Herhangi bir kişisel bilgisayara ve İnternet bağlantısına sahip olan kimse, İnternet üzerinde bulunan bir eseri kalite kaybı olmaksızın kopyalayabilmekte ve çoğaltabilmektedir.

7.2 Tanım Sorunu

Türk Dil Kurumu Sözlüğü'nde bilişim "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle

420 Thoman, F.H., Rechtsprobleme des Online-Datenverkehrs(1996-1997), www.rzmw.ch/docs/thom01.rtf, s. 25.

elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi olarak tanımlanmaktadır[421]. Fikri ve sınaî haklar ile bilişimin kesiştiği nokta ise bilgisayar programları ve veri tabanları olup, raporda bilgisayar programları ve veri tabanlarının fikri mülkiyet hukukundaki yeri, hukuki niteliği, koruma koşulları ve bu konudaki tartışmalar üzerinde durulacaktır.

Örneğin; Gümrük Müsteşarlığınca fikri ve sınaî mülkiyet hakları ile ilgili olarak hazırlanan ve yakın bir zamanda işlerlik kazanacak olan bir bilgisayar programı oluşturulmuştur. Bu şekilde başlatılan çalışmaların tamamlanmasını müteakip fikri ve sınaî mülkiyet mevzuatı kapsamındaki hakların korunması için gümrüğe başvuru yapan ve gümrük tarafından başvurusu kabul edilen hak sahiplerine ilişkin irtibat bilgilerinin ve firma bazında orijinal ve sahte ürün mukayeselerine ilişkin bilgi ve resimlerin yer aldığı bir veri tabanı sisteminin oluşturulması ve söz konusu veri tabanına dijital olarak yüklenen bilgi ve belgelerin en hızlı ve doğru şekilde Türkiye'nin her yerindeki gümrük muayene memurlarının ulaşımına açılması planlanmaktadır.

Buna göre herhangi bir sahtecilikten şüphelenen gümrük memuru Gümrük Müsteşarlığı intranetinde yer alan söz konusu veri tabanında "arama" yapmak suretiyle şüpheli eşyanın orijinaline ilişkin bilgilere, resimlere, vs. (hak sahibi tarafından verilen ve sahte eşya ile orijinal eşya arasındaki farkı ortaya koyan bütün detaylara) ulaşmak suretiyle hızlı bir şekilde karar verebilecek ve yine veri tabanında yer alan erişim bilgileri vasıtasıyla hak sahibine ulaşarak şüphesi ile ilgili bilgi verebilecektir.

Ayrıca, yine söz konusu veri tabanına gümrük memurları tarafından gerçekleştirilen yakalamalar kaydedileceğinden belli bir süre sonra Müsteşarlığın elinde fikri ve sınaî mülkiyet haklarının korunması konusunda fiziki muayeneye gerek kalmadan sadece belge kontrolü sonucunda hedefleme yapmaya imkân verecek çok detaylı bir istatistikî bilgi kaynağı oluşacaktır.

7.3 Bilişim Hukuku Bakımından Fikir ve Sanat Eserlerinin Niteliği

7.3.1 Ülkemizde Bilgisayar Programlarının Niteliği

Ülkemizde bilgisayar programları, bir fikri eser olarak kabul edilmekte Fikir ve Sanat Eserleri Kanunu ile korunmaktadır. 551 Sayılı Patent haklarının Korunması Hakkında KHK. nın md.6/c hükmü ise buluş niteliğinde olmadıkları için bilgisayar yazılımlarına patent verilemeyeceğini düzenlemiştir. Ülkemizdeki bu hukuki düzenlemeler, tarafı olduğumuz uluslararası antlaşmaların gereğidir. Türkiye, 1886 tarihli Bern Sözleşmesi'nin (Edebiyat ve Sanat Eserlerinin Korunmasına İlişkin Sözleşme) 1948'de Brüksel'de değiştirilen metnine 1951 tarihinde katılmış, Sözleşmenin 1979 tarihli Paris metnini de 1995 tarihinde 4117 sayılı Kanun ile kabul

[421] http://www.tdk.gov.tr

etmiştir. Keza 1995 tarihinde Dünya Ticaret Örgütü'nün ayrılmaz parçası kabul edilen TRIPS Sözleşmesi'ni (Sahte Mal Ticareti Dâhil Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması) kabul etmiştir. Anayasa'nın 90 md. hükmü gereği uluslararası antlaşmalar kanun hükmündedir ve uluslararası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda uluslararası antlaşma hükümleri esas alınır. Nitekim mahkemeler ve Yargıtay da kararlarında fikri ve sınaî haklara ilişkin uluslararası sözleşme hükümlerine doğrudan dayanmaktadır. (Yargıtay 11.HD.13.11.2006 tarih ve E.2005/10856;K.2006/11671; 11.HD. 05.12.2006 tarih ve E.2005/9994,K.2006/12852; 11.HD.13.11.2006 tarih ve E.2005/10821, K.2006/11633) Böylece ulusal hukukumuzda en azından şimdilik "olan hukuk" açısından bir belirsizlik yaşanmamaktadır. Ülkemizde fikir ve sanat eserleri, 1951 tarihli 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) ile düzenlenmiş ve koruma altına alınmıştır. FSEK, 1983 tarihli 2936 sayılı, 1995 tarihli 4110 sayılı, 2001 tarihli 4630 sayılı ve 2004 tarihli 5101 sayılı Kanunlar ile önemli değişiklikler geçirmiştir. FSEK'in amacı, 1.md. hükmünde açıklandığı üzere fikir ve sanat eserlerini meydana getiren eser sahipleri ile bu eserleri icra eden veya yorumlayan icracı sanatçıların, seslerin ilk tespitini yapan fonograf yapımcıları ile filmlerin ilk tespitini gerçekleştiren yapımcıların ve radyo-televizyon kuruluşlarının ürünleri üzerindeki manevi ve mali haklarını belirlemek, korumak, bu ürünlerden yararlanma şartlarını düzenlemek, öngörülen esas ve usullere aykırı yararlanma halinde yaptırımları tespit etmektir.

FSEK. Md.1/B-a gereğince eser, sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat ürünleri olarak ve FSEK: md.1/B-g'de bilgisayar programı ise "bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları" olarak tanımlanmıştır.1995 tarihli 4110 sayılı Kanun ile FSEK de önemli değişiklikler yapılmış ve FSEK. Md 2'de bilgisayar programı, ilim ve edebiyat eseri olarak ilk kez açıkça düzenlemiştir. Bu açık düzenlemeden önce de bilgisayar programları, FSEK. Md.2 "herhangi bir şekilde dil ile ifade olunan bütün eserler" hükmü gereği ilim ve edebiyat eseri olarak kabul edilerek korunmaktaydı.

7.3.2 Bilgisayar Programlarının Fikir Ve Sanat Eseri Olup Olmayacağı Tartışmaları

Bilgisayar programlarının hukuki niteliği ile korunmalarında hangi hukuki rejimin uygulanacağı konusundaki tartışmalar devam etmektedir.

1. Bilgisayar programlarının dil ve yazı ile ifade edilen bir fikri eser olduğu ve bu nedenle eser sahibinin hakları kapsamında korunması gerektiği [422],

2. Bilgisayar programlarının işlevsellik nitelikleri yönünden patent hukuku kapsamında korunması gerektiği[423],

3. Eser sahibinin hakları veya patent hukuku dışında sui generis düzenlemeler yapılarak korunması gerektiği[424],

4. Ticari sır ya da haksız rekabet hukuku kapsamında korunması gerektiği[425],

5. Yeni düşünceler ve teknolojiler, herkesin serbestçe faydalanabileceği kamu mallarıdır, yaratıcılığın asıl uyarıcısı ya da motivasyonu maddi kazançtan çok kültürel saygınlık ve itibardır düşüncesiyle hiç korunmaması gerektiği[426] savunulmaktadır.

Genelde kabul gören görüş, bilgisayar programlarının eser sahibi hakkının konusu olduğu yönündedir. Bu görüşe göre, bilgisayar programları, yazılarak hazırlanması, kaynak kodlarının belirli kurallara ve formlara uyularak hazırlanmış olması nedeniyle ilim ve edebiyat eseri olarak kabul edilmelidir. Eser sahibinin hakkı kapsamındaki korumanın herhangi bir tescil zorunluluğu gerektirmemesi, korumanın eserin yaratılıp herhangi bir şekilde kaydedildiği andan itibaren başlaması ve koruma sürelerinin uzun olması nedeniyle, bu görüş özellikle A.B.D menşeli yazılım sanayinin lider kuruluşları tarafından desteklenmektedir.

Bilgisayar programlarının patent hukuku kapsamında korunması, patent hakkı kapsamındaki korumanın eser sahibinin hakkına kıyasla daha güçlü bir tekel hakkı sağlaması nedeniyle savunulmaktadır. Eser sahibinin hakkı kapsamındaki korumada, kopyalanmadan, tamamen özgün çalışmalarla aynı işlevlere sahip ve aynı sonuçları veren ikinci bir programın piyasaya sürülmesi mümkünken, patentle korunan bir programın kopyalama ve esinlenme hiç söz konusu olmasa dahi geliştirilip kullanıma sunulması olanaksızdır[427]. Diğer yandan, patent hukuku ile korumada bilgisayar programının sahibi, inceleme merciine buluşunun tekniğin bilinen durumunu aşan, sanayiye uygulanabilir bir buluş olduğunu kanıtlamak zorundadır. Ayrıca koruma süresi de, inceleme sonucu verilen patentler için 20 yıl ve incelemesiz verilen patentler için 7 yıldır ki, telif hukukundaki eser sahibinin yaşadığı sürece ve ölümünden itibaren 70 yıllık koruma süresi ile karşılaştırıldığında daha kısadır.

[422] Kaypakoğlu,S.;Bilgisayar Programlarının Hukuki Korunması, İzmir, 1997; s.25
[423] Kaypakoğlu,S; s.29
[424] Kaypakoğlu,S; s.38
[425] Kaypakoğlu,S; 34,36
[426] Yüksel,M.; Hukuk ve Adalet Dergisi,Ekim-Aralık 2004; İstanbul, 2005; s.39
[427] Kaypakoğlu, s.33

7.3.3 Fikri Haklar ile İlgili Ana Kavramlar

Fikri hukuk kavramlarında ülkemizde henüz bir terim birliğinin sağlanmamış olduğu gözlenmektedir. “Fikir ve sanat eserleri” yerine “telif hakları” , “Fikir ve Sanat Eserleri Kanunu” yerine “Telif Hakları Kanunu” terimlerinin kullanıldığı sıkça gözlenmektedir.

Fikri mülkiyet kavramı, 1967 yılında kurulan Dünya Fikri Mülkiyet Örgütü (WIPO-World Intellectual Property Organization) tarafından ana kavram olarak kullanılmış ve bu kavram konuları itibariyle de “sınaî mülkiyet” (Industrial Property) ve “eser sahibinin hakları” (copyright) olarak iki bölümde değerlendirilmiştir.

Kavramlar, 1995 yılından itibaren “sınaî mülkiyet” ve “eser sahibinin hakları ve komşu haklar” olarak kullanılmıştır. Kavramlardaki karışıklığı önleme amacıyla, sınıflandırma, aşağıda sistematik olarak sunulmuştur.

Fikri Haklar:
Fikri Mülkiyet

- **Eser Sahibinin Hakları**

- Bilim ve Edebiyat Eserleri
- Müzik Eserleri
- Güzel Sanat Eserleri
- Sinema Eserleri
- İşlenmeler ve Derlemeler

- **Eser Sahibinin Hakları ile Bağlantılı Haklar**

  - **Komşu Haklar**

  - İcracı sanatçıların hakları
  - Fonograf yapımcılarının hakları
  - Radyo-televizyon kuruluşlarının hakları

Film Yapımcısının Hakları

- **Sınaî Mülkiyet**

  - Patent ve Faydalı Modeller
  - Endüstriyel Tasarımlar
  - Markalar
  - Coğrafi İşaretler
  - Ticaret Unvanı

- İşletme Adı
- Entegre Devre Topografyaları
- Yeni Bitki Çeşitleri

Raporumuzda fikri mülkiyet kavramı, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'ndaki eser sahibi hakları ile sınırlı olarak kullanılmıştır.

7.3.4 Fikri Hakların Niteliği ve Gerekliliği

Fikri hakların niteliği ve gerekliliğine ilişkin tartışmalar mevcuttur. Bir görüş, yaratıcılığın teşvik edilmesi ve kamu yararı için yaratıcılığın korunması gerektiği savunmakta olup, bir başka görüş fikri haklar ile getirilen korumaların yaratıcıların haklarından çok tekel yaratmak suretiyle bilgi ve iletişim teknolojilerinde meydana gelen ilerlemeler sonucu, çok büyük kuruluş ve şirketlerin haklarını korumakta olduğu, gerçek yaratıcıların artık pek ortada görünmediğini iddia ederek fikri haklar kavramını tartışmaya açmaktadır.

"Ekonomistlerin bakış açısıyla, fikri haklar, temel olarak ekonominin enformasyon ve kitle iletişim araçları sektörlerinde sermaye ile emek arasındaki ilişkiyi düzenlemektedir. Fikri yaratımlar, araziler, menkul eşyalar, lisanslar, isim hakları, değerli madenler gibi sermayeye dahi yatırım araçları haline gelmiştir. Rekabet halinde kar peşinde koşan firmalar, Pazar ekonomisinde gerçekleşen teknik değişimin başat aktörleridir. Teknolojik gelişmeler, yeni icatlar ve yaratımlar, yalıtılmış bir ortamda değil, sosyal, ekonomik ve kültürel bir çerçeve içerisinde gerçekleşebilmektedir. Hukuki çerçeve, kültürel şartlar ve kamusal bilimsel bilgi olmadan yeni icatlar yapılamamaktadır. Bu durumda ortaya çıkan fikir ürünlerinden ne kadarının kamuya, ne kadarının da özel şahıslar ait olacağına yanıt aranmalıdır. Ekonomistlerin aksine sosyologlar ve tarihçiler, firmalar arasındaki rekabet unsurunu kabul etmekte beraber, teknik ilerlemenin sosyal ve mesleki yanlarını vurgulama eğilimindedirler. Geniş bir teknik ve bilimsel bilgi temeline sahip uygulama yönelimli bilim adamları veya mühendisler bu sürecin anahtar aktörleridir.

Fikri haklar üzerinde, günümüzde gerçek kişi yaratıcıların mı yoksa tüzel kişilerin, büyük şirketlerin mi çok söz sahibi olduğu araştırılmalıdır. Günümüzde fikri haklar korumasında, bireysel yaratıcılardan ziyade çokuluslu şirketlerin, çok büyük film ve müzik yapımcıları ile bilgisayar programları üreticilerinin yararlandığı gözlenmektedir. Bu durumda, fikri haklar koruma düzeni ile iletişim özgürlüğü, düşünce ve ifade özgürlüğü bilgi ve haber alma hakkı arasındaki yakın ilişki ve hassas denge, hukuki düzenlemelerde dikkate alınmalıdır.

Toplum yaşamı bakımından bu kadar önemli olan, ekonominin günümüzde temel girdisi ve temel bir üretim faktörü olarak görülen bilgi ve enformasyonun böylesine önemli olduğu bir çağda, fikri ürünlerin bu kadar önem taşıdığı bir çağda elbette fikri mülkiyet korunmalıdır"[428]

Bununla birlikte, fikri haklar, sahibine tekel konumu sağlayan haklardır ve fikri hak sahibi hem yarattığı ürün ya da eserinde münhasıran bir hakka sahip olmakta hem de başkalarını bunları çoğaltma, yararlanma hakkından yoksun bırakabilmektedir. Fikri hak sahiplerinin böyle bir yetkiye ya da hakka ne kadar süreyle sahip olması gerektiği, sınırsız olup olmaması gerektiği tartışmalıdır.

7.3.5 Eserin Niteliği Olarak Dijitalleşme

Fakat raporda fikri haklarla birlikte eserin dijital hale gelmesinden de bahsetmek gerekmektedir. Eser ortaya çıktıktan sonra başka ortamlarda sunulabilmesi için veri mesajları, sayısal bilgiler haline dönüştürülmektedir.

Fikri haklar için dijitalleşme, bir eserin ortaya çıkarılmasından sonra onun radyo ve televizyon mesajları veya fotoğraf şekline dönüştürülmesinden, yeni bir teknolojinin ortaya konulmasından başka bir şey değildir[429]. Teknik bir yenilenmenin mevcut olmasına rağmen telif hakları bakımından olaya bakıldığında yeni bir nitelik değişmesi söz konusu değildir. Eser sahibi ile kullanıcı arasındaki menfaat çekişmesi ve hukuki araçlar aynı kalmaktadır[430]. Fikri hakların temel problemleri, dijital hale getirilmiş olan eserler için de mevcuttur. Ortaya çıkarılan eser, mülkiyet hakkı dolayısıyla iktisadi faydanın sağlanabilmesi için uygun bir koruma ile teminat altına alınmalıdır[431].

Eserlerin dijitalleşmesinde gözden kaçırılmaması gereken husus, bir eserin dijitalleşmesi ile telif hakkının ihlalinin kolaylaşmasıdır. Birkaç tuş yardımı ile İnternet'te dolaşan eserler izinsiz olarak sınır ötesinde kopyalanabilmekte ve çoğaltılabilmektedir[432]. Kolayca taklit edilebilme ve yanıltılabilme, kopyalanabilmeye karşı yeni hukuki enstrümanlar aranmakta ve yeni teknolojiler geliştirilmeye çalışılmaktadır. Özellikle günümüz teknolojisinde dijital eserlerin "su üzerine yazı" gibi kopyalanamaz bir hale getirilmesine çalışılmakta ve Serial Copy Manegement System (SCMS) "Seri Kopya Yönetim Sistemi" ile dijital haldeki eserlerin sadece bir defa kopyalanmasıyla sınırlanmaktadır[433].

Ayrıca İnternet'e mahsus eser görünümleri olarak Multimedya Eserler kavramı üzerinde de durmak gerekmektedir.

---

[428] Yüksel,M., Hukuk ve Adalet Dergisi,Ekim-Aralık 2004; İstanbul, 2005; s.40 vd.

[429] Lehmann, M., Digitalisierung und UrhR, Internet und Multimdiarecht (Cyberlaw), Stutgart 1997, s. 27.

[430] Rehbinder, Urheberrecht (Kommentar) § 18i Rn. 162.

[431] Lehmann, Digitalisierung und UrhR, s. 27.

[432] Lehmann, Digitalisierung und UrhR, s. 28.

[433] Koeve, D., Urheberrecht im Internet', www.raekoeve.de/Urheb.html, s. 7.

Bir kavram olarak multimedya kavramı aslında tam olarak tanımlanmış bir kavram değildir. Multimedya kavramının değişik tanımlamalarına burada işaret etmek gerekir. Multimedya, sinema filmi, müzik ve resmi içeren değişik medya ürünleridir. Ancak bu tanımlamanın son bir tanımlama olmadığını da burada belirtmek gerekmektedir. Çünkü enformasyon teknolojisinin hızlı gelişimi sayesinde multimedya kavramı sürekli bir değişim içindedir[434].

İnternet üzerinden fikri haklara konu olan eserlerin ikinci özelliği bu eserlerin multimedya özelliği taşımasıdır. Yani eserler, İnternet üzerinde yazı, görüntü, ses, film ve müzik eserleri ile karışık olarak sunulmaktadır. Dijitalleşme dolayısıyla hem zamana bağlı video ve ses kaydı gibi medya, hem de zamana bağlı olmayan kalıcı resim ve metinler gibi medyanın karışımı ile eserler İnternet ortamına verilmektedir. Bu ortamda kullanıcıya yeni imkânlar verilmekte ve onun isteğine göre bir ortam hazırlanmaktadır. Burada multimedyanın bir diğer özelliği de karşımıza çıkmaktadır ki bu da etkileşimdir. Multimedya ürünleri, tamamen kullanıcı ile iletişime dayanan bir dijital ortamda gerçekleşmektedir. Artık kullanıcılar daha önceki ürünlerdeki gibi sadece programı açmak veya kapamak gibi iki seçenek arasında sıkışmamışlardır. Burada artık kendileri de programa katkıda bulunabilmekte enformasyon gönderebilmektedirler[435].

Multimedya ürünleri offline-kullanım ve online kullanım olarak öncelikle ikiye ayrılabilir. Offline-kullanım, CD gibi veri taşıyıcılarla kullanımı anlatırken, online-kullanım radyo, kablolu yayın ve İnternet ortamındaki kullanımı anlatmaktadır. Online ve offline kullanım yanında sunulan hizmetin enteraktif olup olmamasına göre bir ayrım da yapılabilmektedir. Online kullanım da senkron ve asenkron kullanım olarak kendi arasında ikiye ayrılmaktadır. Senkron kullanımda, radyo yayınlarında olduğu gibi eş zamanlı bir tüketim söz konusu iken asenkron kullanımda İnternet ortamında olduğu gibi eş zamanlı bir tüketim şart değildir. İnternet kullanıcıları, birbirinden farklı zamanlarda sunulanlara erişme ve onları tüketme imkânına sahiptir[436].

Tablo1: Multimedya Kullanımın Tasnifi[437]

Senkron ve asenkron kullanımlarda fikri haklar bakımından ilginç farklılıklar oluşmaktadır. Örneğin yeniden yayınlama kavramı (FSEK. M. 25) asenkron kullanımlara her zaman uygun düşmemektedir[438] . Ancak İnternet ortamında yapılan multimedya sunumlar çok çeşitlidir ve hem senkron hem de asenkron sunumlar

434 Zscherpe, Urheberrechtsschutz digitalisierter Werke im Internet, MMR 1998, s. 404.

435 Schwarz, M., Merkmale, Entwicklungstendenzen und Problemstellungen des nternet, http://www.jura.uni-münchen.de/Institute/İnternet_I.html 3. Das İnternet ist interaktiv, s. 4; Saacke, A., *Saacke*, Astrid - "Schutzgegenstand und Rechtsinhaberschaft bei Multimediaprodukten - Grundfragen des Rechtsschutzes und der Lizenzierung", in: *Götting*, Horst-Peter (Editor) - "Multimedia, İnternet und Urheberrecht", 1998, s. 21; Zscherpe, s. 404.

436 Federrath, H., “Multimediale Inhalte und technischer Urheberrechtsschutz im İnternet”, ZUM, 2000, s. 805.

437 Tablo Federrath’dan alınmıştır. Bkz. s. 805.

438 Federrath, s. 805.

yapılabilmektedir. Örneğin İnternet radyoda yapılan yayınlar, aynı zamanda senkron yayınların bütün özelliklerine sahiptir.

7.3.6 Fikri Mülkiyet ve Bilgisayar Programlarının Hukuki Korunması

Yukarıda da belirtildiği gibi, ülkemizde bilgisayar programları, bir fikri eser olarak kabul edilmekte Fikir ve Sanat Eserleri Kanunu ile korunmaktadır. 551 Sayılı Patent haklarının Korunması Hakkında KHK. nın md.6/c hükmü ise buluş niteliğinde olmadıkları için bilgisayar yazılımlarına patent verilemeyeceğini düzenlemiştir.

1995 tarih ve 4110 sayılı kanunla FSEK'de yapılan değişikliğe kadar bilgisayar programları Türk özel hukuk mevzuatında yer almıyordu. Bununla birlikte, bilgisayar programları ister nesne kodu isterse kaynak kodu ile yazılmış olsun, FSEK. Md. 2 anlamında "dil ile ifade olunan eser" kabul edilmekteydi. 1995 yılındaki değişikle FSEK.2 maddesi 1.fıkra, 1.bendindeki "her biçim altında ifade edilen bilgisayar programları ile bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları" ilim ve edebiyat eserleri arasında ayrı bir kategori olarak kabul edilmiştir. FSEK.2.maddesi 2.fıkrası bilgisayar programlarının hangi unsurlarının koruma kapsamı dışında tutulduğunu düzenlemektedir. Buna göre ara yüzene temel oluşturan düşünce ilkeleri de içine almak üzere, bir bilgisayar programının herhangi bir öğesine temel oluşturan düşünce ve ilkeler eser olarak kabul edilmemektedir ve bu nedenle koruma kapsamı dışındadır.

1995 tarihli değişikle FSEK'in "işlenmeler" başlıklı maddesine "işlenme niteliğindeki bilgisayar programları ve veri tabanları eklenmiştir." FSEK. Md. 6/10 " bir bilgisayar programının uyarlanması, düzenlenmesi veya herhangi bir değişim yapılması" ve FSEK. Md.6/11 " Belli bir maksada göre ve hususi bir plan dâhilinde verilerin ve materyallerin seçilip derlenmesi sonucu ortaya çıkan ve bir araç ile okunabilir veya diğer biçimdeki veri tabanları" hükümleri ile işlenme niteliğindeki bilgisayar programları ve veri tabanlarına sağlanan koruma açıkça düzenlenmiştir.

FSEK tarafından bilgisayar programları açısından eser sahibine tanınan mali haklar, işleme hakkı (FSEK. Md.21), çoğaltma hakkı (FSEK. Md.22) , yayma hakkı (FSEK. Md. 23) , manevi haklar ise kamuya sunma yetkisi (FSEK. Md.14), adım belirtilmesi yetkisi (FSEK. Md.15), eserde değişiklik yapılmasını men etme yetkisi (FSEK. Md. 16) ve eser sahibinin zilyet ve malike karşı hakları (FSEK. Md. 17) dır dır.

Şahsen kullanma başlıklı FSEK. Md. 38 hükmü ile bilgisayar programlarına özgün düzenlenmeler de getirilmiştir.

7.3.7 İnternet'te Fikri Hukuk Bakımından Özellik Arz eden Uygulamalar

İnternet ortamında özellik arz eden ve yeni ve zorluk arz eden bir takım uygulamalar bulunmaktadır.

7.3.7.1 İnternet (Web) Sayfalarının Korunması

İnternet sayfasının fikri hukuk bakımından nasıl korunacağı konusunda bir fikir beyan etmeden önce İnternet sayfasının özelliklerinin ele alınması gerekmektedir. İnternet sayfası, multimedya ürün niteliği arz eden ve bir eser türü olarak nitelenemeyen çoklu eser türleri arasında yer almaktadır. Bir İnternet sayfasında İnternet öncesinde kitap, resim, grafik, fotoğraflar gibi analog eser türleri bulunabileceği gibi, İnternet'e özgü tasarımlar da bulunmaktadır. Ancak İnternet sayfası denildiğinde eser türleri ayrı ayrı değil de hepsinin bütünleşmiş olduğu toplu ve ayrı bir birleşik bütün anlaşılmaktadır.

Aslında birden fazla eser türünün birbiri içinde bütünleştirilerek bulunduğu bazı eser bileşimleri fikri hukukumuzda ayrı bir eser kategorisi olarak korunmaktadır. Eser türünün belirlenmesi elbette kanun koyucunun bir tercihidir. Bu nedenle henüz kanun koyucuların İnternet sayfalarını bağımsız bir eser türü olarak kabul etmediği görülmektedir. Eğer bir gün kanun koyucu İnternet sayfalarını aynen sinema eserlerinde olduğu gibi ayrı ve bağımsız bir eser türü olarak kabul ederse bu durumda İnternet sayfasının bütünü itibariyle ayrı ve bağımsız bir eserin varlığından bahsedildiğinde bu eser türüne göre koruma sağlanacaktır; ancak bu şekilde bir bütün olarak "eser" niteliğine haiz değilse bu durumda hâlihazırdaki eser türlerine göre koruma sağlanır[439].

Bilindiği gibi Fikir ve Sanat Eserleri Kanunu'na göre bir fikri ürünün eser sayılabilmesi için objektif ve sübjektif şartın yerine gelmesi gerekir. Eserin sahibinin hususiyetini taşıması, sübjektif şartı oluşturur iken; söz konusu fikri ürünün kanunda sayılan eser türlerinden biri olması da objektif şartı oluşturmaktadır. Hal böyle olunca İnternet sayfası multimedya bir ürün olarak, yani çoklu ortam ürünü olarak karşımıza çıkmaktadır. Ancak bununla birlikte Kanunda sayılan eser tiplerinden herhangi birine girmemektedir.

Bu halde İnternet sayfasının münferit unsurlarına ayrılarak korunması gündeme gelmektedir. İnternet sayfası, resimlerden, seslerden ve birbirine geçişi sağlayan teknik süreçten ve bazı hallerde bilgisayar yazılımlarından oluşan bir bütün olarak karşımıza çıkmaktadır. İnternet sayfasının unsurlarının ayrı ayrı korumaya mazhar olacağı tabiidir. Yani İnternet sayfasında kullanılan metinlerin şartları varsa ilmi ya da edebi

[439] Schwarz, M., Recht im İnternet, Bd. 1, Loseblattsammlung, Maerz 2000, s. 31.

eser, bir müzik eserinin kullanıldığı hallerde müzik eseri olarak yine resim kullanılıyorsa güzel sanat eseri ya da sinema eseri olarak, arkasında bir veri bankası varsa veri bankası olarak korunması mümkün olabilir. Ya da bir bilgisayar programı kullanılmış ise bilgisayar programı olarak korunabilir. Şu ana kadar bu şekilde kombine eserlerin yeni bir eser türü olarak tanınması ve korunması, sadece sinema eserlerinde mümkün olmuştur[440].

İnternet sayfasında bulunabilecek eser türlerine bakıldığında ilmi ve edebi eserler, güzel sanat eserleri, musiki eserler ve sinema eserleri İnternet sayfasında yer alabilen klasik eser türleridir. Bunların FSEK kapsamında korunmasında herhangi bir problem bulunmamaktadır.

İnternet sayfalarında ayrıca HTML-kodları dediğimiz kodlar bulunmaktadır. Bunlar aslında FSEK bakımından yazılım olarak kabul edilebilir[441]. Özellikle son zamanlarda enteraktif yazılımların gelişmesi ile birlikte İnternet sayfaları, artık klasik HTML-kodlarından daha karmaşık yazılımlara doğru gidiş seyri izlemektedir.

İnternet sayfası, "asp" tekniği kullanılarak da hazırlanabilir. Bu teknikte, İnternet sayfası her seferinde yeniden kullanıcının talebine göre üretilmektedir. Yani İnternet sayfasının arkasında artık bir yazılım çalışmaktadır. Bu durumda yazılımı koruma altına alan hükümlere göre bir eserin varlığından bahsedilmelidir. Yine İnternet sayfaları, Javascript denilen programlarla da yapılabilir. Java programlama dilinin İnternet sayfaları için özelleştirilmiş biçimidir. Script dilleri ile hazırlanan kodlar programlardan farklı olarak satır satır işletilirler. Bu programlar ise bir bütün olarak ele alınır ve değerlendirilirler. Ancak, klasik anlamda, İnternet sayfası hazırlamak için kullanılan HTML dilinden farklı olarak statik bir sayfa ortaya çıkmaz, kodlara bağlı olarak farklı sayfalar ortaya çıkar.

İnternet sayfalarının arkasında bazı zamanlar işleyen bir veri bankası da bulunabilir. FSEK. nun 6/11. maddesinde veri tabanı tanımlanmıştır: "Belli bir maksada göre ve hususi bir plan dâhilinde verilerin ve materyallerin seçilip derlenmesi sonucu ortaya çıkan ve bir araç ile okunabilir veya diğer biçimdeki" veri tabanları (Ancak, burada sağlanan koruma, veri tabanı içinde bulunan veri ve materyalin korunması için genişletilemez)". Burada veri tabanından bahsedebilmek için iki tane unsur sıralanmıştır. Bunlardan ilki belirli bir maksada yönelik materyallerin derlenmesi, ikincisi ise bu materyallerin bir araç ile okunabilmesidir.

Bazı hallerde kopyalanan İnternet sayfalarında tescilli logoların bir başka ifadesi ile markaların ya da tescilli tasarımların bulunması mümkündür. Bu logoların izinsiz

440 Lehmann, M./v. Tucher, T., "Urheberrechtlicher Schutz von multimedialen Webseiten" CR1999, 700 vd.
441 *Bechthold* ZUM 1997, 427(428).

kullanımı, marka hakkına tecavüz olarak değerlendirilebilir. Bunlar da ilgili mevzuata göre incelenmelidir. İnternet sayfalarında alan adlarının kullanılması ise bazı hallerde marka hakkına tecavüz teşkil eder iken bazı hallerde de ticaret unvanının haksız kullanımını oluşturabilir[442].

7.3.7.2 Link ve Frame Kullanılması

7.3.7.2.1 Link (Çengel-Bağlantı)

Link, Türkçede "çengel" veya bağlantı olarak adlandırılmaktadır. Link verme veya çengel atma, özel bir bilgisayar programı ile gerçekleştirilen ve bir İnternet sayfasından diğerine geçişi mümkün kılan tekniğin ismidir[443]. Aslında link verme, normal bir metin üzerinde de yapılabilmektedir. Zira günümüz editör tabanlı yazılımlarda bugün akıllı sayfa dediğimiz tanıma olayı gerçekleştirilmektedir. Yani Word metninde yazılan bir İnternet adresi, otomatik olarak geçişe uygun hale getirilmektedir[444]. İnternet bağlantısının mevcut olması ve adrese tıklanması halinde İnternet sayfalarına geçiş mümkün olmaktadır. Link veya hyperlink, İnternet sayfasından İnternet kullanıcısını, yabancı İnternet sayfasına aktaran bir program kodudur[445].

Bir linkte (çengel) iki esas unsur bulunmaktadır. Bunlardan ilki, ağda herhangi bir yerde bulunan bir içeriğe işaret, diğeri ise bu içeriğe ulaşabilme imkânıdır[446]. Link verilme halinde işaret edilen İnternet sayfaları veya bilgiler, link veren veya ziyaret edilen sayfanın sunucusunda tutulmamakta, link verilen sayfanın veya atıf yapılan İnternet sayfasının kendi sunucusunda bulunmaktadır.

Linkler, uygulanan tekniklere göre farklı isimler alabilmektedir[447]. Öncelikle linkler, deeplinks, surfece links ve inline link olarak adlandırılmaktadır. "surfece link"in verilmesi halinde İnternet sayfası ziyaretçisi, bu linki seçmesi ile birlikte bir başka sayfayı açmaya başlayacaktır. Bu tür linklerde link verilen sayfa bağımsız bir sayfa

---

442 Bu konuda bkz. Tekin Memiş, Alan İsmi Etrafında Ortaya Çıkan Hukuki Sorunlar, **Bilişim Toplumuna Giderken Psikoloji, Sosyoloji ve Hukukta Etkiler Sempozyumu**, Ankara 2001.

443 Link, terim ve sistematiği ilk olarak Jean Armour Polly'nin 1992 tarihli "Surfing the Internet'" isimli kitabında kullanılmıştır.

444 Word metninde çalışmış olan kimseler için yazılan İnternet'adreslerinin mavi hale gelmesi bilinen bir olaydır.

445 Link vermek için İnternet'sayfasının HTML-kodları arasına <a>-Tag yazılması ile gerçekleştirilmektedir (bu konuda ayrıntılı bilgi için bkz. Fröhlich, M.: "Zentrale Institionen des deutschen Urheberrechts und des fransözischen Droit d'autteur auf dem Prüfstand der elektronischen Netzwerke", Frankfurt am Main 2001, s. 131; Bechtold, S.: "Schutz des Anbieter von Information Urheberrecht und Gewerblicher Rechtsschutz im İnternet'", www.jura.uni-tuebingen.de/ri/96ws/bechtold/seminar.htm); Völker, S./Lührig, N.: "Abwehr unerwünschter Inline-Links", K&R 2000/1, s. 21.

446 Sosnitza, O.: "Das İnternet im Gravitationsfeld des Rechts: Zur rechtlichen Beurteilung so genannter Deep Links", CR 10/2001, s. 694.

447 Burada link verme her ne kadar genel olarak iki ana başlıkta incelenecek ise de ayrıca "surface-link" veya "deep-link", "embedding links", "inline images" olarak diğer tür linklerden de bahsedilmektedir (bkz. Plass, G.: "Hyperlinks im Spannungsfeld von Urheber-, Wettbewerbs- und Haftungsrecht", WRP 2000/6, 599, 600.

olarak kullanıcının karşısına gelecektir[448]. Buna karşılık "Deeplinks"te kullanıcı, doğrudan ziyaret ettiği sayfa üzerinden bir diğer kimsenin sayfasındaki bilgilere giriş sayfasını kullanmaksızın ulaşabilme imkânına kavuşmuştur[449]. Nihayetinde aslında "deeplinks" bir dâhili link olarak kabul edilmektedir[450].

Konunun fikri hukuk bakımından ele alınacağı bu çalışmada temelde linkler, İnternet (dâhili) ve ekstern (harici) link olarak ikiye ayrılmaktadır[451]. Harici (ekstern) linklerde İnternet kullanıcısı, link verilen sayfada bulunan linklerin tıklanması ile diğer sayfaya ulaşmaktadır. Bu doğrudan diğer İnternet sitesinin ana sayfası olabileceği gibi, o site içinde bulunan bir diğer sayfa da olabilir. Dâhili (intern) linklerde ise İnternet kullanıcısı, bir başka sayfaya aktarılmamaktadır. Burada kullanıcı link veren sayfada kalmakta, ancak linkin verildiği sayfa, bu sayfa içinde görülebilmektedir. Dâhili (intern) linkler sayesinde, yüzlerce grafik ve büyük hacimli veriler, link veren kimsenin serveri meşgul edilmeksizin kullanılmaktadır. Bu tür linkler, bir eserin sahibinin link veren kimse olduğu görünümü verilerek kötüye kullanılabilmektedir[452].

7.3.7.2.2 Çerçeve (Frame)

Frame verme halinde ise bir İnternet sayfasında birbirinden bağımsız bölümlerde birden çok doküman görülmektedir. Burada frame veren ile frame verilen yabancı İnternet sayfası, İnternet kullanıcısının ekranında birleşik olarak görülmektedir. Modern İnternet browserları, kullanıcının ekranının bölünebilmesini sağlamaya elverişlidir. Frame tekniği ile İnternet sayfası yapımcısı, bir başkasına ait İnternet sayfasını kendi sayfası içine monte etme imkânını elde etmektedir. Her frame verilmesinde, İnternet kullanıcısının ekranında yabancı İnternet sayfaları görüntülenebilmektedir[453]. Frame, intern link vermeden farklıdır. İntern linklerde bir İnternet sayfasının sadece belirli bir metni veya grafiği görüntülenmekte iken frame vermede link verilen tüm sayfa görüntülenmektedir[454].

Bir Frame Görüntüsü[455]

---

448 Plass, s. 600; Sosnitza, s. 694.

449 Leistner, M./Bettinger, T.: "Immaterialgüterrechtlicher und wettbewerbsrechtlicher Schutzdes Web-Designers", CR 1999, s. 926; Sosnitza, s. 694.

450 Bosmann, W.: Onlinerecht - Recht der eigenen Homepage, http://www.dr-bosman.de/seiten/ratgeber/onlinerecht.htm#gestaltung-links.

451 Kreuzer, P. A.: "Urheberrecht im Internet'", s. 250, 252; Fröhlich, s. 131, 135; Leupold, A./ Demisch, D.: "Bereithalten von Musikwerken yum Abruf in digitalen Netzen", ZUM 2000, s. 385.

452 Fröhlich, s. 135.

453 Burmeister, K.: "Urheberrechtsschutz gegen Framing im Internet'-eine rechtsvergleichende Untersuchung des deutschen und US-amerikanischen Urheberrechts", Köln 2000, s. 22, 23; Laga, G.: "Neue Techniken im World Wide Internet'- Eine Spielwiese für Juristen?", JurPC Web-Dok. 25/1998, Abs. 1 – 50 (www.jurpc.de), p. 23 (Eine Spielwiese für Juristen). Frame verilen İnternet'sayfası örneği için bkz. www.netbul.com.

454 Laga, Eine Spielwiese für Juristen, p. 24.

455 Bkz. www.janko.at/webmaster/index.

B'nin Frame'i	
B'nin Framesi	A'nın Sayfası

7.4 Link ve Frame Vermeye Eser Sahibinin Rızası Sorunu

Link atmanın değerlendirilmesinde öncelikle İnternet sayfalarının özellikleri göz önünde bulundurulmalıdır. Link atma, ilk anlamda çoğaltma olarak düşünülebilir. Zira bir İnternet sayfasının çağrılması, tipik bir çoğaltma olarak kabul edilmektedir. Fakat sadece bir link atmanın eser sahibinin çoğaltma hakkının ihlali olduğu söylenemez. Çünkü link atma, sadece sayfanın adresinin verilmesi veya o sayfaya İnternet kullanıcılarının ulaşmasının kolaylaştırılmasıdır[456]. Ayrıca link aktif hale getirildiğinde işlemler link verilen sayfanın üzerinde gerçekleşmektedir. Bu, özellikle ekstern link atma hallerinde söz konusudur.

Bir İnternet sayfasının işleticisinin yani bir anlamda eser sahibinin bir İnternet sayfasında sunum yapması halinde onun en azından kendi İnternet sayfasına başkalarının link vermesini zımni olarak kabul ettiği varsayılmaktadır[457]. Çünkü link atma, İnternet sayfasında sunulan imkânlardan biridir ve link atılan sayfaya da ulaşılabilme imkânı eser sahibi tarafından sağlanmaktadır. İnternet'in temel felsefesini oluşturan bir tür bilgi bankası olması da bu görüşü haklı kılmaktadır. Eser sahibi tarafından başkaca bir hakkın ihlali söz konusu değilse link atma yasaklanamaz[458].

Doktrinde ekstern link atma, kural olarak atıf hakkı ve kaynak gösterme hakkı ile karşılaştırılmaktadır. Bu nedenle doktrine hâkim olan görüşe göre de link atma yasaklanamamalıdır[459]. Amerikan hukukunda link atma hakkı tanınmıştır[460]. Mahkeme içtihatlarında da İnternet'te bir İnternet sayfası kuran kimsenin kendisine bu şekilde linkler verilmesine rıza gösterdiği sonucuna ulaşılmıştır[461].

Hemen burada söylenmesi gereken bir husus da link veren kimseler arasındaki özel ilişkilerdir. İki rakip arasında verilen linkler ayrıca değerlendirilmeye tabi tutulmalıdır. Buna İskoç adalarında yaşanan bir çekişmezlik örnek olarak verilebilir: Ekstern linklerin kullanılmasında ilk hukuki problem, İskoç adalarında 1996 yılında yaşanmıştır. "Shetland Times" günlük haberlerinin bir kısmını İnternet sayfasında da yayınlayan günlük bir gazetedir. "Shetland News" de İnternet sayfasında yayınlanan bir

456 Strömer, T. H.: "Online Recht, Rechtsfragen im İnternet'", 2. Auflage, Heidelberg 1999, s. 198.
457 Ihde, R.: "Hyperlinks", www.graefe-partner.de/ecom/hyperlinks.html; Ernst, NJW-CoR, s. 242.
458 Bechtold, Schutz des Anbieters, dn. 52.
459 Schuster, F./Müller, U.: "Entwicklung des İnternet'- und Multimediarechts von Januar 1999 bis Juni 2000", MMR-Beilage 2000/10, s. 16.
460 Schuster /Müller, s. 17.
461 OLG Düsseldorf, 29.06.1999; Jurpc Web-Dok. 42/2000, Abs. 39 (www.jurpc.de/20000042.htm); BGH 27.01.1998, VI ZR 72/97 (GRUR, 1998, s. 504).

haber gazetesidir. Bu gazete, kendi İnternet sayfasında "Shetland Times"den bir habere kendi sayfasından link vermiştir. Bu link nitelik itibariyle bir ekstern linktir. İnternet kullanıcısı, söz konusu linki tıklayarak "Shetland Times" gazetesinin haberine ulaşabilmektedir. Bunun üzerine "Shetland Times" yöneticileri, İskoç mahkemelerinde bir dava açmıştır. Dava bir ara karardan sonra 1997 yılında mahkeme dışı bir anlaşma ile sonuçlandırılmıştır. Buna göre verilen linklerin her biri için logo ile birlikte "A Shetland Times Story" ilavesi ve ayrıca "Shetland Times"in ana sayfası için ayrı bir link konulacaktır[462].

Dâhili (İntern) linklerin ve framelerin konulması halinde eser sahibinin bu duruma ekstern linklerde olduğu gibi zımnen izin vermesinden söz edilemez[463]. Çünkü burada eser sahibinin İnternet sayfasından ummakta olduğu haklı menfaatler ihlal edilebilmektedir. Zira İnternet kullanıcısı, eser sahibinin sayfasına ulaşmamakta, geçiş yapmamakta, link veya frame veren kimsenin sayfasında kalmakta ve eserin link veren kimseye ait olduğunu düşünebilmektedir. Zira frame veren İnternet sayfası ile frame verilen İnternet sayfası arasında bağlantı kurulmakta; frame veren kişinin İnternet sayfasına monte edilerek kullanıcının karşısına çıkmaktadır([464]). Amerika'da TotalNews firması, frame verme yolu ile 1100 adet radyo, televizyon ve gazeteyi sayfalarına monte etmiştir([465]).Kaldı ki link verilen İnternet sayfası sahibinin eserinin sadece belirli formatta görülmesini isteme hakkı, asıl olarak kabul edilmelidir.

Deeplink verilmesi halinde de eser sahibinin rızasının alınması gerekmektedir. Bir görüşe göre eser sahibi İnternet'te bulundurduğu sayfada herhangi bir sınırlama getirmemiş ise bu durumda deeplink verilmesine rıza göstermiş sayılmalıdır[466]. Bir başka görüşe göre ise eser sahibinin bu durumda açık rızası aranmalıdır[467]. Kanaatimce eser sahibinin adının belirtilmesi hakkı, manevi haklardan olduğu ve bunlardan vazgeçmenin bile mümkün olmadığı düşünüldüğünde, sadece zımni bir rızanın varlığından bahsedilememeli, eser sahibinin açık bir rızası aranmalıdır. Dâhili link ve frame verilmesi halinde mahkeme içtihatları, eser sahibinin zımni bir rızasından bahsedilemeyeceğini kabul etmiştir[468].

7.4.1 Link ve Frame Verilmesi Ve Eser Sahibinin Hakları

Link ve frame verilmesinde ortaya çıkacak sorunlara genel bir bakıştan önce link türleri arasında başlangıçta bir ayrım yapmak gerekmektedir. Fikri hukuk açısından

462 Fröhlich, s. 133. (Karar için bkz. www.shetland-times.co.uk/st/daily/dispute.htm).
463 Kreuzer, s. 252.
464 Burmeister, s. 25.
465 Klett, A.: "Urheberrecht im İnternet aus deutscher und amerikanischer Sicht", Baden-Baden 1998, s. 189.
466 Sosnitza, s. 701.
467 Plass, 604.
468 LG Hamburg, 12.07.200, 308 O 205/00 (MMR 2000, s. 762); OLG Hamburg, 22.02.2001, 3 U 247/00 (MMR 2001, s. 534).

problem olabilecek link türleri dâhili linklerdir. Zira harici linkler, İnternet'in kalbi olarak nitelendirilmekte ve atıf hakkına benzetilmektedir. Burada sadece eser sahibinin sayfasına bir geçiş sağlanmaktadır. Zaten eser sahibinin söz konusu sayfasına İnternet ağında ulaşmak mümkündür. Dâhili link ve framelerde ise eser sahibinin ihlal edilebilen haklarının tek tek ele alınması ve incelenmesi gerekmektedir.

Eser sahibinin hakları manevi ve mali haklar olarak ikiye ayrılabilir. Birbirinden farklı olan bu haklar demetinin kendine ait özellikleri ile konu alt başlıklar halinde incelenecektir.

Bern Sözleşmesi 6 bis) 1'e uygun olarak, eser sahibinin bu sıfatının, yani eserin sahibi olduğunun belirtilmesi, Fikir ve Sanat Eserleri Kanunu'nun 15. maddesinde belirtilmiştir. Eser sahibinin adının belirtilmesi hakkı, eser sahibinin adının eserde yer almasını kapsadığı gibi, eserin kullanıldığı her yer ve durumda açıkça belirtilmesini de kapsamaktadır. Bu hak, bir taraftan eseri sahibine bağlar, diğer taraftan da eser sahibini eser hırsızlarına karşı (intihal) korur[469]. Bu hak, eserin kullanıldığı her tür ve bütün boyutlarda her halde mevcuttur, kullanmanın nitelik ve çapı önemli değildir[470].

"Eser sahibinin adının eser yayımlanırken yazılması gerekir. Aksi halde maddi ve manevi tazminat istenebilir"[471]. Eser sahibinin isminin yazılmaması hali bir kusur olarak kabul edilmektedir ve manevi tazminatı gerektirmektedir[472].

İntern (inline-dâhili) link verme halinde ise eser sahibinin ihlal edilen bir takım haklarından bahsetmek mümkündür. Zira bu link türünde link verilen sayfa (eser) bağımsız bir sayfa olarak açılmamakta, link veren sayfanın içinde görüntülenmekte; link veren sayfanın adeta bir parçası görünümü verilmektedir. Bu durumda eser sahibinin korunmaya değer menfaatlerinden bahsetmek gerekmektedir. Öncelikle eser sahibinin manevi haklarından adının belirtilmesi hakkının çiğnenmesi söz konusu olabilir (FSEK m. 15) [473].

Deeplink verilmesi halinde genellikle eser sahibi tanınabilmektedir. Burada kullanıcı, içeriğin gerçek eser sahibini tanımlayabilmektedir. Deeplinkte, link verilen sayfa, bazen İnternet sitesinin ilk sayfası olabilmektedir. Bu durumda eser sahibinin tanınabilmesi daha kolaydır. Ancak deeplink'le hedefteki İnternet sayfasının giriş sayfasından başka bir sayfaya bağlanılıyor ise bu durumda eser sahipliğinin karıştırılma ihtimali ortaya çıkmaktadır. Zira İnternet kullanıcısının linkle bağlandığı

469 Tekinalp, Ü.: "Fikrî Mülkiyet Hukuku", İstanbul 1999, s. 157, p. 24.
470 Tekinalp, s. 157, p. 25.
471 11.HD. 3.4.1978, E. 1183, K. 1979/1704 (Çevik, O.N.: "İçtihatlı Notlu Fikri Hukuk Mevzuatı", Ankara 1988, s. 21, 22).
472 11. HD. 23.3.1978, E. 78/687, K. 78/1437 (Yargıtay Kararları Dergisi, Temmuz 1979, s. 1012, 1013).
473 Ihde, R., "Hyperlinks" s. 2 (www.graefe-partner.de/ecom/hyperlinks.html).

sayfadan İnternet sayfasının diğer içeriğine geçmesi beklenemez. Bu durumda deeplink verilen sayfanın sahibinin rızası alınmalıdır.

Frame vermede birbirinden farklı iki teknik kullanılabilmektedir. Bunlardan ilkinde İnternet kullanıcısı, hangi sayfanın verilerini ekranda gördüğünü bilmemektedir. Diğerinde ise bu sayfanın URL adresi belirtilmektedir([474]). Kullanıcının hangi sayfanın görüntülendiğini bilmediği hallerde eser sahibinin adının belirtilmesi hakkı ihlal edilmektedir.

Fikir ve sanat eserleri, eser sahibinin adı, eserin adı ve muhteva ile şekil olarak bir bütün teşkil eder. Bu bütünlüğün korunmasında eser sahibinin manevi bir menfaati bulunmaktadır. Eser sahibinin eserinde zorunlu hallerde değişiklik yapılabilmektedir. Bu zorunluluk halleri, onarım, ihtiyaca uygun hale getirmek, halkın ve çevrenin güvenliği zorunlu hallere örnek olarak verilebilir[475]. Eser sahibinin zorunlu haller dışında eserinde değişikliklere izin verme yetkisi sadece onun tarafından kullanılabilmektedir ve miras yolu ile intikale yahut üçüncü şahıslara devredilmeye elverişli bulunmamaktadır[476].

Normal olarak hangi tür olursa olsun linklerde ve framelerde eserin değiştirilmesi söz konusu değildir[477]. Ancak bazı hallerde eserin belirli bir parçasının frame ve dâhili linklerle bir başka sayfaya bitiştirilmesi halinde eser sahibinin eserinin bütünü veya parçasında belirli bir değişiklik yapıldığının kabul edilmesi gerekmektedir[478].

Fikir ve Sanat Eserleri Kanunu anlamında bir işlemeden bahsedilebilmesi için eseri dönüştüren kimsenin de esere katkısının bulunması gerekmektedir[479]. İşleme eserde iki unsurun bulunması gerekir. Birincisi işleme eser, orijinal eserden bağımsız değildir, ikincisi ise onu işleyen kişilerin de esere bir katkısını taşımaktadır[480].

Eserin kısaltılması veya genişletilmesi işlenme sayılmaz. Bir roman veya hikâyenin kısaltılması, bir tablodan belirli bir kısmın çıkarılması, senaryonun rejisör tarafından kısaltılması birer işlenme değildir. Eserin büyüklüğünde veya buutlarında değişiklik yapılması işleme değil, çoğaltmadır[481]. Hatta mekanik vasıtaların kullanımı ile de bunun yapılması sonucu değiştirmez. Eserde meydana getirilen dış değişiklikler, ona bir yaratıcı emeğin katkısı değil de sadece bir sunumun, nâkilin sonucu ise yine

474 Decker, U.: "Urheberpersönlichkeitsrecht im Internet'", (Hoeren, T./ Sieber, U.: Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschaeftsverkehrs", München 1999), 7.6, p. 51

475 Tekinalp, s. 161, p. 44.

476 Erel, Ş.: "Türk Fikir ve Sanat Hukuku", Ankara 1998, s. 123

477 Sosnitza, s. 701.

478 Farklı örnekler için bkz. Plass, s. 603.

479 Gahrau, E.: "Einleitende Überlegungen", (Hoeren, T./ Sieber, U.: Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschaeftsverkehrs", München 1999), 7.1, Rdnr. 28.

480 Schack, H.: "Urheber- und Urhebervertragsrecht", 2. Aufl. Tübingen 2001, Rdnr. 237.

481 Geniş Bilgi için bkz. Öztan, F.: Fikir ve Sanat Eserleri Hukukunda İşlenme Eserler, s. 229 vd; EREL'de "eserin başka bir sesle nakli"ni işleme eser olarak kabul etmemektedir (bkz. EREL, Fikir ve Sanat Hukuku, s. 59).

ortada bir işlenme eserin varlığından bahsetmek mümkün olmayacaktır. Mesela bir tablonun değişik ışıklandırılmalar altında sergilenmesi gibi. Esere bir başka buut kazandırılması durumlarında da işlenme eser mevcut değildir[482]. Bir müzik parçasına yeni bir güftenin yazılması da işlenme eser olarak kabul edilemez. Böyle bir durumda eserin metni değişmemekte, ilave ve ikame bir metin daha esere bitiştirilmektedir. Burada işlenme eserden değil, bir eser beraberliğinden bahsedilmektedir[483]. Eser beraberliğinde ortada yeni bir eser mevcut olmadığından her eser bağımsız bir eser olarak değerlendirilir. Bir müzik eserinin operada kullanılması, bir şiirin tiyatro temsilinde okunmasında da ortada işlenme eserden bahsedilemez[484].

İntern linklerde eser sahibinin yani link verilen sitenin sadece belirli kısımları ile yeni bir görünümün elde edilebilmesi de mümkündür. Bu durumda ise eser sahibinin işleme hakkının ihlali söz konusudur. İşleme hakkı da münhasıran eser sahibine aittir (FSEK m. 21). Özellikle dâhili linklerde ve framelerde link verilen sayfalar, adeta kullanıcının ziyaret ettiği ve aynı zamanda link ve frameyi veren sayfanın bir parçası olarak gösterilebilmektedir. Burada bir başkasının yaptığı İnternet sayfasının değiştirilmesi, bir başka görünüme kavuşturulması söz konusudur. Ancak işlemenin var olup olmadığı her somut olayda ayrıca araştırılmalıdır.

Frame veya link verilmesi halinde aslında sadece link ve frame verilen sayfa ile teknik bir bağlantının yapıldığı, dolayısıyla eserin aslına bir müdahalede bulunulmadığı doktrinde savunulmaktadır[485]. Ancak eserin kullanıcının ekranına yansıyan halinde şayet esere katkıda bulunulmuş ise ortada bir işlemenin varlığından bahsetmek gerekmektedir. Fakat kullanıcının sadece linki seçmesi ile onun ekranına gelen görüntünün frame veya link veren kimsenin işlemesi olarak nasıl kabul edileceği de şüpheli bulunmaktadır[486]. Ancak kanaatimizce bu kullanıcının bir eylemi olmayıp, İnternet sayfasını düzenleyen yani linki veya frameyi veren kimsenin eylemi olarak düşünülmelidir[487].

Amerika'da dava konusu olan bir olayda da mahkeme, fikri hukuk bakımından korunan fotoğrafların ortaya yeni bir eser konulmamasına rağmen işleme hakkı ile ilgili olduğuna karar vermiştir[488]. Fakat benzeri bir olayda bir başka mahkeme haklı olarak,

---

482 Öztan, s. 229.
483 Öztan, s. 231.
484 Schack, s. 140-141, p. 291.
485 Gabel, D.: "Anmerkung zum Urteil des LG Düsseldorf vom 29.4.1998," K&R 1988, s. 556.
486 Burmeister, K.: "Urheberrechtsschutz gegen Framing im nternet': eine rechtsvergleichende Untersuchung des deutschen und US-amerikanischen Urheberrechts", Köln 2000, s. 171.
487 Krş. Burmeister, s. 25; Klett, s. 190.
488 Burmeister, s. 170.

işleme hakkının ihlali için frame verilen sayfanın yeni biçiminin yaratıcı ve özgün bir formda olması şartını aramıştır[489].

FSEK 22. maddesinin I. fıkrasına göre, bir eserin aslının veya kopyalarının herhangi bir şekil veya yöntemle, tamamen veya kısmen, doğrudan veya dolaylı, geçici veya sürekli olarak çoğaltılmasıdır. Ayrıca çoğaltma kavramının kapsamı II. fıkrada genişletilmiştir: "Eserlerin aslından ikinci bir kopyasının çıkarılması ya da eserin işaret, ses ve görüntü nakil ve tekrarına yarayan, bilinen ya da ileride geliştirilecek olan her türlü araca kayıt edilmesi, her türlü müzik ve ses kayıtları ile mimarlık eserlerine ait plan, proje krokilerin uygulanması da çoğaltma sayılır".

Çoğaltma kavramının içeriği her gün genişlemektedir. Özellikle bilgisayar teknolojisinin gelişmesi ile birlikte çoğaltma kavramı da oldukça gelişmiştir. Bir bilgisayar disketine kayıt edilmiş bulunan eserin, bilgisayarda görünmesi anında bile "geçici" de olsa bir çoğaltma bulunmaktadır. Çünkü bilgisayar ekranına getirilen görüntüler, bilgisayar RAM'larında geçici olarak kaydedilen bilgilerdir[490]. Bilgisayarın hard diskine kayıt ve gönderme de çoğaltma sayılmaktadır[491]. Kanunun kullanmış olduğu ifadeler de sınırlayıcı olmadığından teknolojinin gelişmesi ile birlikte çoğaltma kavramı da gün geçtikçe genişleyecektir.

Bir eserin aslından veya kopyasından taklitin çıkarılması ise çoğaltma değildir. Çoğaltma, eserin herhangi bir yolla aynen kopyalanmasıdır[492].

Çoğaltma, günlük dilde geniş halk kitlelerinin yararlanmasını sağlayacak kadar çok nüshanın çıkarılmasını ifade etmektedir. Ancak fikri hukukta aslının yerine ondan yararlanmayı sağlayan tek bir nüshanın çıkarılması da çoğaltma sayılmaktadır[493]. FSEK. m.22/II' de "ikinci bir kopyasının çıkarılması" ifadesi ile de bu durum açıkça ortaya konmuştur.

Çoğaltma hakkı münhasıran eser sahibine verilen bir haktır. Fakat kanun koyucu, bazı hallerde çoğaltma hakkına bazı sınırlamalar getirilmiştir. Örneğin FSEK m. 38'de belirtilen şahsen kullanım amacı ile çoğaltma, bu hakkın bir istisnasını oluşturmaktadır.

İnternet ve bilgisayar ortamında eserlerin sunumunda birden fazla çoğaltma süreci bulunmaktadır[494]. Önbelleğe kayıt, eserin görülebilmesi için zorunlu olan teknik

489 Burmeister, s. 171.
490 Bu konuda bkz. Schack, Rdnr. 378.
491 Leupold/Demisch, s. 383; Tekinalp, s. 176, p. 91.
492 Tekinalp, s. 176, p. 91; Erel, Fikir ve Sanat Hukuku, s. 140.
493 Erel, Fikir ve Sanat Hukuku, s. 141.
494 Bu aşamalar içinde yabancı literatürde tartışılan fakat bir çoğaltma olarak kabul edilmeyen bilgisayar ekran görüntüsü ele alınmamaktadır. Çünkü bu konuda herhangi bir aksi görüş bulunmamaktadır ve isabetli bir şekilde ekrandaki görüntü bir çoğaltma olarak kabul edilmemektedir (bu konuda bkz. NORDEMANN; s. 181, § 16, p. 2; Fröhlich, s. 106).

bir çoğaltma işlemidir[495].Yine bir bilginin İnternet'ten kullanıcının bilgisayarına gelene kadar değişik duraklarda kaydedilmesi de bir çoğaltma işlemidir (routing). World Wide Web, birbirine bağlı milyonlarca bilgisayardan oluşmaktadır. Bu bilgisayarlar arasında İnternet erişiminde bir bilgi, diğer bilgisayara giderken birden fazla yol takip etmektedir. Takip edilen bu yolda bilgisayarlardan oluşan birçok durak bulunmaktadır. Bu duraklardaki bilgisayarlar "router" ismini almaktadır ve kendisine gelen bilgileri gideceği hedef bilgisayara aktarmaktadır.

Bu aşamalardan her birinde ayrıca bilgiler kayıt edilmekte ve gönderilmektedir. İstenilen bilgiler, İnternet ağında küçük parçalara ayrılmaktadır. Bu bilgiler hedef bilgisayarda birleştirilmektedir. Bu kayıtlar bir başka bilgisayara "transfer için yapılan kayıtlar"dır[496]. Bu nedenle bu süreçteki kayıtlar da çoğaltma kavramı içinde değerlendirilmelidir[497]. Kanaatimizce, bu aşamadaki çoğaltma da, fikri hukuk anlamında çoğaltma kavramı içinde değerlendirilmelidir. Ancak bu çoğaltma hali, klasik çoğaltma hallerinden farklı olarak müeyyidelendirilememelidir. Zira bu süreçteki çoğaltmalar, nihai çoğaltmanın zorunlu parçalarıdır. Bir başka çoğaltma süreci de ana bellekte gerçekleşmektedir. Önbellekte yapılan kayıt işlemine göre kalıcı bir kayıt işlemi olarak adlandırılabilir ve fikri hukuk bakımından tartışmasız bir şekilde çoğaltma olarak kabul edilir[498]. Dijital hale getirilmiş olan bir eserin İnternet'ten veya bilgisayarın hard diskinden bir CD veya diskete kaydedilmesi de fikri hukuk bakımından bir çoğaltma sayılmaktadır[499]. CD veya diskete kayıt, sürekli bir kayıttır. FSEK m. 22/III, bir bilgisayar programının görüntülenmesini de geçici çoğaltmayı gerektirdiği ölçüde çoğaltma olarak kabul etmiştir. Fakat doktrin sadece ekranda görüntülemeyi, çoğaltma olarak kabul etmemektedir[500].

Link ve frame verilmesinde eser sahibinin çoğaltma hakkının ihlal edilip edilmediği de burada ayrıca araştırılmaya değer bir konu olarak karşımıza çıkmaktadır. Bir linkin aktif hale getirilmesi halinde, çoğaltma bizzat link veren kimsenin eylemi olarak gerçekleşmemektedir. Çoğaltma üçüncü kişinin, yani İnternet sayfası

---

495 Fröhlich, s. 105; Bosak, V.M.: "Urheberrechtliche Zulaessigkeit privaten Downloadings von Musikdateien", CR 2001/3, s. 178; Nordemann, W.: "Urheberrecht, Kommentar zum Urheberrecht und zum Urheberrechtswahrnehmungsgesetz", Stuttgart 1998, s. 181, § 16, p. 2; Freitag (Kröger/Gimmy), s. 315; Lowenheim (Lowenheim /Koch), "Praxis des Online-Rechts, 1998", s. 306; Bosak, s. 178; Hoeren, CR 1988, s. 912. Burada belirtilmelidir ki, eserin bilgisyarda görülebilmesine dair bu açıklamalar şu anda yaygın olarak kullanılan teknoloji içindir. PC=Personel Computer/bilgisayarları karşısında bugün piyasaya sürülmeye başlanan NC=Net Computer/Ağ bilgisayarlarında ön bellek dediğimiz RAM'ler bulunmamaktadır. Bu durumda yukarda söylenen kayıt aşamaları tamamen daha farklı bir şekilde ele alınmalıdır.

496 Eichhorn, B.: "Internet'-Recht, Ein Lehrbuch für das Recht im World-Wide-Web", Köln 2000,. 18.

497 Bosak, s. 178.

498 Nordemann, s. 181, § 16, p. 2; Schack, s. 195, p. 417; Fröhlich, s. 100 vd.

499 Nordemann; s. 181, § 16, p. 2.

500 Nordemann, s. 181, § 16, p. 2; Fröhlich, s. 106.

ziyaretçisinin bilgisayarında meydana gelmektedir[501]. Bu nedenle link ve frame veren kimse, doğrudan eser sahibinin çoğaltma hakkını ihlal etmemektedir[502].

Frame verme de doğrudan bir çoğaltma değildir. Zira burada ilgili bir program yardımı ile iki İnternet sayfası arasında bir bağlantı kurulmaktadır. Bu durumun aynısı link türleri için de söz konusu olmaktadır. Böyle bir durumda link ve frame veren kimse eser sahibinin çoğaltma hakkını ihlal etmemiş kabul edilmelidir[503].

Fakat doktrinde savunulan bir görüşe göre dâhili linklerde ve framelerde İnternet sayfası ziyaretçisi olan üçüncü kişi, şayet link veya frame ile ulaştığı sayfanın kime ait olduğunu anlayamıyorsa bu durumda eser sahibinin çoğaltma hakkı ihlal edilmektedir[504].

İntern linklerin kullanımı ile ilgili olarak 1996 yılının yazında Amerika'da meydana gelen bir çekişmezlik incelemeye değerdir. Burada "Dilbert" adı verilen popüler komik figür, intern link yoluyla özel bir İnternet sayfasında kullanılmıştır. Bu figürü günlük olarak "United Medya" firması, kendi İnternet sayfasında yenilemekte ve sunmaktadır. Fakat aynı figürleri intern linklerle bu özel şahıs kendi sayfasına eklemektedir. Mahkeme, bu durumda, eser sahiplerinin haklarının ihlal edildiğine karar vermiştir[505].

Almanya'da uyuşmazlık konusu bir olayda online ortamda sunulan bir sözlüğe link verilmekte, bu sözlük kişinin İnternet sayfasında görüntülenmektedir (framing). Bu durum mahkeme tarafından söz konusu bilgi bankasının kısmen çoğaltılması olarak kabul edilmiştir ki, bu durum eser sahibinin münhasır haklarının bir ihlalidir. Bilgi bankasını sunan kimsenin link verilmesine zımni rızasından da bahsedilememektedir. Zira bu rıza sadece link verilmesine gösterilen bir rıza olup, bir yabancı İnternet sayfasında görüntülenmesine verilen rıza değildir[506].

Konunun Türk hukuku bakımından değerlendirmesine gelince; normal linklerde, yani harici linklerde ve hangi sayfanın görüntülendiğinin bilindiği dâhili link ve framelerde çoğaltma hakkının ihlal edilmediği sonucuna varılmalıdır. Ancak kullanıcı tarafından hangi sayfanın link ve frame sonucu kullanıldığı bilinemiyorsa bu takdirde çoğaltma hakkının ihlal edildiği sonucuna ulaşılmalıdır. FSEK m. 22 metni son derece geniş ve ayrıntılı düzenlenmiştir[507]. Buna göre her ne kadar çoğaltma, link veya frame

501 Junker, M.: "Anwendbares Recht und internationale Zustaendigkeit bei Urheberrechtsverletzungen im Internet'", Kassel 2002, s. 122.
502 Schricker/Lowenheim, § 16, p. 22; Ernst, s. 224; Sosnitza, s. 698; Plass, s. 601.
503 Burmeister, s. 83; Lowenheim/Koch, s. 306.
504 Junker, s. 132, 133.
505 Fröhlich, s. 137.
506 OLG Hamburg, 22.02.2001, 3 U 247/00, JurPC Web-Dok. 147/2001 (www.jurpc.de).
507 FSEK.m. 22/I metni şu şekildedir: "Bir eserin aslını veya kopyalarını herhangi bir şekil veya yöntemle, tamamen veya kısmen, doğrudan veya dolaylı, geçici veya sürekli olarak çoğaltma hakkı münhasıran eser sahibine aittir".

veren kimsenin kendi severinde meydana gelmese de burada uygulanan teknik, dolaylı bir çoğaltma olarak kabul edilmelidir. Dolayısıyla bu şekilde bir link veya frame verecek kimsenin mutlaka eser sahibinin iznini alması gerekmektedir. Hakkaniyet ilkesi de burada bir çoğaltmanın varlığının kabulünü, eser sahibinin izninin alınmasını gerektirmektedir. Herhangi bir çoğaltma işlemini kendi sayfasında yasal olarak yapamayan kimse bunu link ve frameler yolu ile de gerçekleştirememelidir[508].

FSEK m. 25'in yeni düzenlemesi ile umuma iletim, bir eserin veya çoğaltılmış nüshalarının radyo, televizyon veya herhangi diğer bir teknik usulle umumun yararlanmasına sunulmasıdır. Umuma arz kavramında önem taşıyan kavram "umum" kavramına yüklenecek anlamdır. Fikir ve Sanat Eserleri Kanunumuzda umum kavramı tanımlanmamıştır. Buna karşın Alman Telif Hakları Yasası'nın UrhG § 15/III de tanımlanmıştır. Bu tanımlamaya göre belirli bir çevre ile sınırlı olmayan, birbirine karşılıklı ilişkiler içinde bağlı bulunmayan veya bir organizasyonla birbirine bağlanmayan birden fazla kimse, umum kavramını oluşturmaktadır[509].

Umuma iletim hakkının ihlal edilip edilmediği sorununda da dikkate alınması gereken husus, umuma iletimin nasıl gerçekleştiğidir. Zira burada fikri hakka konu teşkil eden eser, yine sahibinin severinde bulunmakta, erişim oradan sağlanmaktadır.

Herhangi bir teknik usulle umumun yararlanmasına sunulma tanımı, dâhili link veya frame veren kimsenin dolaylı da olsa yapmış olduğu sunumları da kapsayıp kapsamadığı sorunu gündeme gelmektedir. Fakat kanaatimizce dâhili link ve frame verilmesi halinde umuma iletim hakkının link veya frame veren tarafından ihlal edilmediği sonucuna ulaşılmalıdır. Zira burada yine umuma iletim, eser sahibinin sayfasından gerçekleştirilmektedir. Umuma iletimi düzenleyen FSEK m. 25 de eser sahibinin çoğaltma hakkını düzenleyen FSEK m. 22 genişliğinde değildir ve "dolaylı da olsa umuma arz", madde kapsamına alınmamıştır.

7.4.2 Link Veren Kimselerin Sorumluluğu

Link veren kimsenin sorumluluğunu tespit etmek için öncelikle bu kimselerin sorumluluk esaslarının ve link vermenin hukuki niteliğinin belirlenmesi gerekmektedir.

Link veren kimsenin sorumluluğunun kendi sayfasını hazırlayan kimse sorumluluğuna mı yoksa bir başkasının sayfasına aracılık yapan kimsenin sorumluluğuna mı tabi olacağı sorusunun da cevaplandırılması gerekmektedir[510].

---

508 Junker, s. 133.

509 Alman UrhG § 15/III'ün metni şu şekildedir: "Die Wiedergabe eines Werkes ist öffentlich, wenn sie für eine Mehrzahl von Personen bestimmt ist, es sei denn, dass der Kreis dieser Personen bestimmt abgegrenzt ist und sie durch gegenseitige Beziehungen oder durch Beziehung zum Veranstalter persönlich untereinander verbunden sind".

510 Bu konuda geniş açıklama ve tartışmalar için bkz. Freytag, s. 229 vd.

Bir görüşe göre İnternet sayfasına link yerleştirilmesi hali bir hazır bulundurmadır. Link tesis edilmesi, kısmen İnternet girişine aracılık olarak kabul edilebilir[511]. Fakat bu görüş kabul edilmemektedir. Zira ekstern link atma halinde sadece link verilen siteye işaret edilmektedir[512]. Bir başka görüşe göre ise, link tesis edilmesi, yabancı bir kimsenin içeriğinin bulundurulması olarak düşünülmelidir (host-provider)[513]. Ancak bu görüş de isabetli değildir. Çünkü burada link veya frame veren kimse link ve frame verilen sayfanın içeriğini kendi severinde tutmamaktadır. İçerik yine link veya frame verilen sayfanın hazırlayıcısının severinde tutulmaktadır[514].

Amerika'da film endüstrisi temsilcisi olan MPAA, Hacker-dergisi çıkaran Eric Corley'e karşı bir dava açmıştır. Davanın sebebi ise, Corley'in kendi İnternet sayfasında DVD üzerine kaydedilmiş olan sinema eserlerinin çoğaltma ve seyretmeye karşı esere ilave edilmiş bulunan şifreleri etkisiz kılan kodların yayınlaması veya bu şifreleri yayınlayan sitelere link vermesidir[515]. Bu davada mahkeme, Corley'in hem şifrelerin kendi İnternet sayfasında açılmasını hem de şifrelerin kırıldığı başka sitelere link verilmesini yasaklamıştır. Hâkim, söz konusu eylemleri Dijital Milineum Copyright Act'a da[516] aykırı bulunmuştur. DMCA bölüm 1201 (a) (2) hükmü, fikrî hakların korunmasını hedefleyen bir teknik sistemin "ilk planda" aşılmasını hedefleyen teknolojileri yasaklamaktadır[517]. Burada getirilen ölçülere göre link verilen sayfanın içeriğinin suç teşkil etmesi ve link veren kimsenin bu sayfanın içeriğini bilmesi gerekmektedir.

Türk hukukunda link ve frame veren kimsenin sorumluluğu genel hükümlere göre belirlenmelidir[518]. Link verilen sayfada eser sahibinin hakları ihlal ediliyorsa bu durumda link veren kişi, yardım ve teşvik etmekten dolayı sorumlu olacaktır.

Burada müteselsil sorumluluk düşünülebilir. Müteselsil sorumluluk, taraf iradelerinden ya da kanunun öngördüğü durumlarda kanundan doğar. Kanunen öngörülen müteselsil sorumluluk hallerinden birisi haksız fiiller alanındadır. Türk/İsviçre kanun koyucusu birden fazla kimselerin aynı zarardan sorumlu olmalarının iki türünü düzenlemiştir. Bunlardan ilki, "birden fazla kimselerin müşterek kusurlarıyla sebebiyet

511 Koch, CR. 1997, s. 200.
512 Freytag, s. 229.
513 Von Bonin, A./Köster O.: "Internet im Lichte neuer Gesetze", ZUM 1997, s. 823
514 Schack, H.: "Urheberrechtliche Gestaltung von Webseiten unter Einsatz von Links und Frames", MMR 2001, s. 15; Junker, s. 131.
515 www.heise.de, 8.09.2000., Ayrıca bkz. www.jura.uni-sb.de.
516 Bu kanun 1998 yılında yürürlüğe girmiştir. Bu kanun ve etkileri hakkında bkz. www.loc.gov/copyright/reports/studies/dmca/dmca_study.html.
517 Madde metni şu şekildedir: "No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title".
518 Alman hukukunda da link ve frame veren kimselerin sorumluluğu genel hükümlere göre çözümlenmektedir (bkz. Junker, s. 132).

verdikleri zarardan sorumluluk (tam teselsül, BK. m. 50)", diğeri, "birden fazla kimselerin muhtelif sebeplerden dolayı sorumlulukları (eksik teselsül BK. m. 51)"dır.

Borçlar Kanunu'nun 50. maddesine göre "birden ziyade kimseler birlikte bir zarar ika ettikleri takdirde müşevvikle asıl fail ve fer'an methali olanlar, tefrik edilmeksizin müteselsilin mesul olurlar. Hâkim bunların her biri aleyhine rücu hakları olup olmadığını takdir ve icabında bu rücuun şümulünün derecesini tayin eder. Yataklık eden kimse, vaki olan kardan hisse almadıkça yahut iştirakiyle bir zarara sebebiyet vermedikçe mesul olmaz". Maddede sözü geçen "asil fail" ifadesinden, bizzat kendi fiili ile zararlı neticenin doğmasına sebebiyet veren, yani zarar verici fiili maddi anlamda işleyen kişi; "müşevvik" ifadesinden bir kimseyi bir haksız fiil işlemeye teşvik eden, onda teşvik edici söz ve davranışlarıyla haksız fiili işleme fikrini yaratan kimse anlaşılmalıdır. Kusurlu davranışlarıyla başkasının haksız fiil işlemesini kolaylaştıran, onun neticeye ulaşmasında yardımda bulunan kişiler "fer'an methaldar"; haksız fiil işlendikten sonra bundan yararlanmak için faile yardım eden, delillerin ortaya çıkmasına engel olan kişi ise "yataklık edendir[519].

Ekstern link veren kimsenin yaptığı eylem, aracılık olarak nitelenmelidir. Zira onun diğer sayfanın içeriğine herhangi bir etkisi bulunmamaktadır. Ayrıca link verdiği sayfanın içeriğinin kendi sunucusu üzerinden sunulması da söz konusu değildir. Bu nedenle link veren İnternet sayfası işleticilerine aracılık yapan kimselere dair bir sorumluluk türünün uygulanması gerekmektedir.

Yasal olmayan bir şekilde eser sahibinin sitesine intern link veren kimsenin durumu ise aracılık yapmaktan daha farklı bir niteliğe kavuşmaktadır. Bir başkasının hazırlamış olduğu içeriği kendi İnternet sayfasından sunmakla içeriği bilmediği savını ortadan kaldırdığı gibi, link veren yasal olmayan içeriğe sahiplenerek bunu kendi içeriği gibi sahiplenmektedir.

7.4.3 Widget Programlarının Kullanımı

İnternet kullanıcılarının, sürekli olarak İnternet'te ziyaret ettikleri sayfalar vardır. Bu sayfalar, değişik sayfalar oldukları için bunların tek tek aranması ve ziyaret edilmesi oldukça uzun bir vakit almaktadır. İnternet kullanıcılarını ziyaret ettiği bu sayfaları tek tek arayıp bulmaktan kurtaran yeni programlar geliştirildi. Bu programlar, widget programları olarak adlandırılmaktadır. Bu programlar, İnternet'e giren kişinin istediği sayfaları onun sayfasına getiren küçük programcıklardır[520].

---

519 Eren, F. : "Borçlar Hukuku Genel Hükümleri" 6. Bası, C. I, İstanbul 1998, 806 vd.

520 Bu konuda bkz. Gökcan, H., Widget'lar sizin yerinize sörf yapacak, Zaman Gazetesi, 14.1.2007 Pazar, Gençlik-Teknoloji, s. 10; Bu programların indirilebileceği site örneği iöin bkz. http://widgets.yahoo.com/win/. http://gezgindunyasi.blogcu.com/1731689

Bu tür programların kullanılması halinde ortaya birçok hukuki sorunun çıkacağı en azından İnternet sayfasının sahipleri tarafından çıkmasının arzulanacağı aşikârdır. Zira bu durumda programa kayıtlı İnternet sayfaları artık ziyaret edilmeyecek, yani bir diğer deyişle reytingi düşecektir. Haksız rekabet açısından bunların ayrıca ele alınması gerekir.

Bu programlar, İnternet sayfalarını, kullanıcının sadece kendi özel sayfasında görüntülemesine hizmet etmekte ve sadece kullanıcı tarafından görüntülenmektedir. FSEK bakımından değerlendirildiğinde kullanıcının bu sayfayı şahsi kullanım çerçevesinde bu şekilde arzusuna göre kullanabilmesinin önünde bir engelin bulunmadığı sonucuna ulaşılmalıdır (m.38).

7.4.4 Değişim Programları[521]

Yukarıda eserin dijitalleşmesinden bahsetmiştik. Burada eserin İnternet ortamında daha rahat nakledilebilmesi için geliştirilen diğer teknolojilerin incelenmesi gerekmektedir.

7.4.4.1 Sıkıştırma Teknikleri-Mp3, DivX vb.

Dijitalleşme sonrasında, özellikle büyük hacimli müzik ve sinema eserlerinin İnternet ortamında nakledilmesi yine de çok zordu ve nakli ve download edilmesi saatler, hatta günler sürebiliyordu. Fakat geliştirilen sıkıştırma teknolojileriyle büyük hacimli müzik ve sinema eserleri de İnternet'te kolaylıkla nakledilebilmeye başlandı. Alman Frauenhofen Enstitüsünde geliştirilen ve Mp3 adı verilen bir teknoloji ile eserler 10–12 kat küçültülmeye başlandı. Böylece bir CD'ye daha önceleri 10–12 müzik parçası kaydedilebilirken, bu teknoloji ile 100–150 müzik parçası kaydedilmeye başlandı. Benzeri teknoloji film eserleri alanında DivX veya DVD teknolojileri ile gerçekleştirildi. Bir müzik eseri artık kalite kaybı olmadan İnternet'te yayılabilmekte ve birkaç dakika içinde kopyalanabilmektedir.

7.4.4.2 Müzik Değişim Programları-Filesharing-P2P

İnternet ortamında eser ve bağlantılı hak sahiplerinin haklarının ihlalinde en fazla kullanılan ve çözümsüzlük arz eden problem "peer to peer" veya "Filesharing" olarak adlandırılan müzik değişim programlarıdır. Bu programlar, İnternet ortamında ücretsiz olarak sunulmaktadır. Bu yazılımların esası, arama motoru, elektronik posta ve Windows'un dosya paylaşım fonksiyonlarının birleştirilmesine dayanmaktadır. Merkezi ve merkezi olmayanlar olarak ikiye ayrılmaktadır. Napster, kapatılmadan önce 70 milyon kullanıcıya sahip olmuştu. Böylece dünya adeta her gün genişleyen bir dijital müzik kütüphanesine dönüşmektedir.

[521] Bu bölümde anlatılan konularda geniş bilgi için bkz. Tekin Memiş, Fikri Hukuk Bakımından İnternet ortamında Müzik Sunumları, Ankara 2003.

7.4.5 Fikri Hak İhlalleri

Yukarda sıralanan İnternet ortamında müzik sunumlarında bir İnternet sayfasında sunum yapılmaya dayanan ilk beşinde ihlallere karşı daha etkin bir mücadelenin yapılması mümkündür. Bununla birlikte bu tür ihlallerle mücadelenin de kendine özgü sorunları bulunmaktadır. Bu zorluklar şu şekilde sıralanabilir. Öncelikle sayısı milyonlara varan İnternet sayfalarında bu tür ihlallerin tespiti nasıl yapılacaktır? Örneğin AB ile ilgili bir İnternet sayfasında bile müzik sunumları yapılabilmektedir. İkincisi sınır ötesi sunumlarda kime karşı ve nasıl dava açılacaktır?

Daha da zor olanı müzik değişim programları yoluyla fikri hukuk ihlalleridir.

7.4.6 İhlal Örnekleri

Müzik alanında ihlalin boyutlarına örnekler vermek gerekirse:

- Arama motorlarında en fazla aranan kavram “Mp3” kavramıdır, hatta “sex” kavramını dahi geçmiş ve onu ikinci sıraya itmiştir.

- Bugün net rakamlar bilinmemekle birlikte 1988 yılında 30 ayrı ülkede 2 binin üzerinde sitede 200 bin müzik parçası sunulmuştur. IFPI’nin son rakamlarına göre illegal müzik sunumu yapan 700 bin İnternet sayfası bulunmaktadır.

- IFPI’ye göre bir güne 1 milyon 100 bin müzik verisi sunuculardan alınmaktadır. Sadece 2001 Ağustos ayında 3 milyar müzik verisi transfer edilmiştir.

- 2003’de sadece müzik değişim platformlarından biri olan Kazaa’da 2,6 milyar müzik verisi değiş-tokuş edilmiştir.

- Bir tahmine göre dünya müzik piyasasının İnternet’te yasal olmayan müzik sunumları dolayısıyla kayıpları 32,6 milyar dolara ulaşmaktadır.

7.4.7 Hukuki Nitelemeler

1. Bir İnternet sayfasına müzik yükleme (upload), müzik değişim programı için hazır bulundurma bir çoğaltmadır ve bu eser sahibinin münhasır haklarındandır (FSEK m.22). FSEK. m.38 anlamında şahsi kullanım amacıyla bir çoğaltma kabul edilemez. Zira şahsi kullanım amacıyla çoğaltma ilişkinin bulunduğu tabii ve dar bir alanı kapsar. Sınırları belli olmayan ve adeta bütün bir dünyaya kopyalama imkânı veren bir çoğaltma FSEK m.38 anlamında bir çoğaltma sayılamaz.

2. Bu tür eylemler, FSEK m.25 anlamında bir “umuma iletim” olarak kabul edilmelidir. Umum, belirli bir çevre ile sınırlı olmayan, birbirine karşılıklı ilişkiler içinde bağlı bulunmayan veya bir organizasyonla birbirine bağlanmayan birden fazla kimse olarak tanımlanmaktadır. Müzik değişim platformlarında oluşan kullanıcı çevresi ise bu anlamda “umum” kavramını oluşturur ve eser sahibini “umuma iletim” hakkını ihlal eder.

7.5 Açılan Davalardan Örnekler

7.5.1.1 RIAAA-Mp3.com Davası

Mp3.com, İnternet'te yayın yapan bir sitedir ve 80 bin müzik parçası, kullanıcıların bir ücret karşılığında dinlemesi veya kopyalaması (download) edebilmesi için hazır bulundurulmaktadır. Bu İnternet sayfasında bulundurulan eserlerin 45 bini, hak sahiplerinin izni olmaksızın kullanılmaktadır. RIAA tarafından açılan davada toplam 6,75 milyar dolarlık tazminat istenmiştir. Mahkeme, mp3 formatında hak sahiplerinin izni olmaksızın eserlerin kullanımını Fikri Haklar Yasasının açık bir ihlalidir ve eserlerin "online" kullanımı "fair use" kavramı altında da mütalaa edilemez.

Almanya'da ise IFPI çalışma grubu ve meslek birlikleri, illegal müzik sunumu yapan İnternet sayfalarına önce uyarıda bulunmakta, uyarılarına riayet edilmezse dava açılacağı belirtilmektedir. Bu çalışmalar sonucu sadece 1999 yılında 500'ün üzerinde İnternet sayfasında illegal müzik sunumu engellenmiştir.

7.5.1.2 Napster Davası

Napster, merkezi sunucusu olan ve kullanıcılarına müzik değişim imkânı sağlayan bir yazılımdır. Müzik değişim platformları arasında en fazla meşhur olmuş ve 70 milyona varan kullanıcı sayısına ulaşmıştır.

Napster'in ilk derece ve temyiz merci aşamalarında mahkeme, Napster'in fikri hakların ihlalinde iki aşamalı bir sorumluluğunun bulunduğuna karar vermiştir. Bu sorumlulukların ilk aşamasını fikri hakların müşterek ihlali, ikinci aşamasını ise dolaylı ihlal oluşturmaktadır. Napster, kurmuş olduğu müzik değişim sistemi ile telif hakkı bakımından korunan eserlerin izinsiz olarak kullanılabileceğini, yayılabileceğini biliyordu ve kurduğu sistemle de buna yardımcı olmuştur. İkinci aşamada ise Napster, sistemi üzerinden yapılan değişimlerde fikri hukuk bakımından korunan eserlerin değişimine engel olmayarak, kontrol yapmayarak gözetim görevini yerine getirmemiştir. Dava aşamalarının devamında mahkeme filtre sistemini öngörmüş, ancak bu meslek birlikleri ve hak sahiplerini tatmin etmemiş, nihayet Napster sistemini paralı hale getirerek ve meslek birliklerine değişimler karşılığını ödeyerek mahkeme aşamaları sonuçlandırılmıştır.

7.5.1.3 Kazaa Davası

Merkezi olmayan müzik değişim platformlarından en ünlüsü olan Kazaa'ya karşı Hollanda'da dava açılmıştır. Hollandalı Hâkim, müzik değişim platformu olan Kazaa'nın iki hafta içinde kapalı kalmasını ve bu süre içinde fikri hukuk bakımından korunan eserlerin değişiminin teknik olarak imkânsız kılınmasını kararlaştırdı. Aksi takdirde P2P servisi, hizmetlerini bitirmek zorunda kalacaktır.

Bu süre sonrasında fikri hukuk bakımından korunan eserlerin değişimi halinde Kazaa, günlük 40 bin–80 bin Dolar ceza ödemek zorunda kalacaktır. Kazaa teknolojisi, Fast Track Şirketinden kaynaklanmaktadır ve MusicCty ve Grokster tarafından da kullanılmaktadır. Bu üç P2P platform kullanıcısı kendi verilerinin platform sınırlarını aşarak dolaşmaktadır. MusicCty ve Grokster, ABD'de Film ve Müzik meslek birlikleri ile bir davada karşı karşıya gelmiştir.

Webnoize-Araştırma Direktörü Lee Black'in görüşüne göre hâkimin bu kararı ağır bir teknolojik yoksunluğu ile izah edilebilir, zira Kazaa, değişim platformunu kontrol edememektedir. Olsa olsa Fast Track Şirketi, Danimarka, İsveç ve Hollanda şubeleri ile bu veri akışına etki edebilir[522]. Kazaa, bu karara karşı temyize gitmiş ve temyiz merciinde verilen kararda hem ihtiyati tedbir kararı kaldırılmış hem de Kazaa'nın kullanıcılarının fikri hak ihlallerinden sistem işleticisinin sorumlu olmayacağına karar verilmiştir.

7.5.1.4 RIAA/MPAA-Grokster, Morpheus, Streamcast Davası

Amerikan Meslek Birlikleri olan Recording Industry Association of America (RIAA) ve Motion Picture Association of America (MPAA) 2003 yılının Nisanında reddedilen dava karşısında Müzik Değişim Platformları olan "Grokster" ve "Morpheus"un işleticilerine karşı temyize başvurdu. Bu haber 20.8.2003 tarihinde BBC'nin Online baskısında yer alıyordu. Karar, müzik değişim borsalarının işleticilerinin kullanıcıların fikri hakları ihlal eden eylemlerinden sorumlu tutulamayacağı gerekçesine dayanıyordu. Temyiz başvurusu yapan davacıların görüşüne göre her şeyden önce işleticiler de bizzat fikri hakları fikri hukuk bakımından korunan müzik ve filmleri kendi alanlarında sağlamakla ihlal ediyorlardı.

Cary Sherman, onların çalışma şeklinin ilgilileri bu sunumlarla yemleyerek borsa ve reklâm amaçlı çalışmaya yönelik olduğunu açıkladı. Davacılar, temyiz başvurularında Grokster ve Streamcast Networks Inc. (Streamcast)'in bir anlamda müzik ve video işletmecilerinin kapılarını kırdıklarını ve insanları istedikleri kadar kopya yapmaya davet ettiklerini belirtmişlerdir.

Nisan'ın sonunda Meslek Birliklerinin ABD-Temyiz Mercii önünde Grokster ve Streamcast karşısında yenilgiye uğradılar. RIAA ve MPAA'nın İnternet değişim platformlarının kapatılması talepleri reddedildi. Burada Mahkeme, ilk olarak video kaydedicilerle ilgili Betemax-kararını İnternet değişim yazılımlarına uygulamıştır. Video kaydedicilerde olduğu gibi yazılımların yapımcıları ve işleticileri, yazılımların kullanıcılarının eylemlerinden sorumlu olmaz, zira yazılım yasal olarak da olmayarak da

[522] Bkz. "Kazaa muss binnen 14 Tagen geschlossen werden" www.e-media.at

kullanılabilmektedir. Merkezi bir serverın olmayışı dolayısıyla değişim platformunun işleticisinin neyin değiştirildiğini bilmesine de imkân tanımamaktadır[523].

Hâkim, müzik değişim platformu işleticilerinin kendi sistemleri üzerinden değişilen materyallerin kontrolünü yapmadığını, illegal müzik değişiminde bulunan kullanıcının eylemlerinden işleticinin sorumlu tutulamayacağına karar vermiştir. Değişim platformlarının yasal amaçlarla kullanılabilmesi dolayısıyla video kaydedicilerin kötüye kullanılma imkânı dolayısıyla yasaklanamayacağı kararına benzemektedir. Bu karar müzik endüstrisinin İnternet değişim platformlarına karşı ilk yenilgisidir.

Olaya bakan hâkim, 1984 yılında ABD Yüksek Mahkemesinin video kaydedicilerle ilgili Sony-kararına atıf yapmaktadır. O zamanlar film endüstrisi, video kaydedicilerin fikri hakları ihlal edebilme tehlikesi dolayısıyla yasaklanmasını istemişti. Film endüstrisi temsilcilerinden Jack Valenti, video kaydedicilerin film stüdyoları üzerindeki etkisini seri katillerin tahribatına benzetilen o dönemi hatırlatarak hâkimin kararını eleştirmişti. Burada ise değişim platformlarının dijital teknolojisi, analog kaydedicilerle karşılaştırıldığında sonsuz ve kusursuz kopyalar anlamına gelmektedir. “Dijital kayıtla analog kayıt arasındaki fark, yıldırımla ateş böceği arasındaki fark gibidir” nitelemesini yapmaktadır[524].

8 SONUÇ

Raporumuzda ele alınan konu başlıkları çerçevesinde yaptığımız araştırmalar sonucunda grubumuz içinde yapılan tartışmalar ve görüş alışverişleri sonucunda raporun sonuç kısmında aşağıdaki konulara değinilmesinin yararlı olacağı değerlendirilmiştir. Diğer taraftan grubumuz yapılan çalışmalar sonucunda bazı önerilerde bulunması bazı konularda ise tartışma başlatmak üzere konunun bilişimcilerin ve bilişim hukukçularının dikkatine sunulmasının uygun olacağı düşünülmüştür.

Her ne kadar raporun başlangıcında bu raporda yer almayan e-Devletin Hukuki Alt Yapısı, Elektronik Arşiv ve Doküman Yönetim Sistemleri, İdare Hukukunun Bilişim Açısından İncelenmesi, Servis Sağlayıcıların Hukuksal Alt Yapısı, Türkiye’de halen uygulanmakta olan e-Devlet ile ilgili önemli projelerin hukuksal açıdan irdelenmesi, birlikte çalışabilirliğin hukuksal alt yapısı, e-Devlet konusundaki bilişim konusunda önemli gelişmeler kaydetmiş ülkelerin yasal alt yapılarının incelenmesi, ülkemizdeki e-Devletin uygulanmasında rol alan önemli kurum ve kuruluşların hukuksal yapısının incelenmesi ve Avrupa Birliği Müktesebatında yer alan BT’ yi ilgilendiren hukuksal düzenlemelerin incelenmesi ve ülkemiz mevzuatı ile karşılaştırılması gibi

523 Bkz. www.urheberrecht.org.
524 Bkz. “Industrie gegen Tauschbörsen Klage abgewiesen” 26. April 2003, www.n-tv.de.

konular ya diğer konularla bağlantıları oranında ele alınmış ya da hiç ele alınamayarak daha sonra yapılacak çalışmalara bırakılmıştır.

Yukarıdaki paragrafta belirtilen konu başlıkları aslında bir an önce uzman kişiler tarafından ele alınarak gündeme taşınması konusunda ihtiyaç duyulduğu açıktır. Bu konuların her biri ayrı bir grup tarafından ele alınarak, enine boyuna tartışılması, yabancı ülke uygulamaları da göz önünde bulundurularak evrensel kurallara uygun bir şekilde yeniden düzenlenmesi ülkemizin BT kullanılmasının hukuksal boyutunun sağlıklı oluşması açısından mutlaka yapılması gereken çalışmalardır.

Grubumuzun ilk bölümde ele aldığı etik veya bilişimde etik konusunda sonuç olarak şunu söyleyebiliriz ki hukukun tek başına tüm bilişim suçlarını önlemesi veya önemli oranda engellemesinde yeterli gözükmemektedir. Tarihte de ahlak hep sürekli hukukun yanında vicdanların hukuku olarak var olagelmiş ve toplumların hayatlarında evrensel değerlerin korunup yaşatılmasında önemli bir işlev üstlenmiştir.

Bu kabulden hareketle şunu söyleyebiliriz ki etik bilişim alanında da hukuk ile başat var olmalıdır ve bu bağlamda gerekli olan kurumsal yapılanmalar oluşturulmalıdır. Bu konuda uluslararası deneyimler de dikkate alınabilir ve yapının oluşturulmasında yol gösterici olabilir. Özellikle Basın Konseyi gibi örneklerden dersler alınarak oluşturulacak etik kurulların bilişim alanında işlenecek olan suçların ve hak ihlallerinin önüne proaktif olarak geçilmesi bakımından çok can alıcı bir öneme sahiptir.

Ancak burada özellikle belirtilmesi gerekir ki bu kurulların oluşturulması sırasında STK'ların bu kurullarda yeterince temsil edilmesi ve fonksiyonel olarak görev yapmaları gerekmektedir. Bu husus etik kurallarının tüm sektör tarafından içselleştirilmesi ve uygulanması bakımından olmazsa olmaz bir unsurdur.

İkinci bölüm olarak ele aldığımız bilişim suçları konusunda yakın geçmişte ülkemizde gerek bu suçların kamuoyuna yansıtılması konusunda ve gerekse bu gündemle paralel olmak üzere mevzuat çalışmaları konusu gündemi fazlası ile işgal etmektedir. Bilişim suçlarının görülme sıklığının artması, elektronik ortama veri göçünün hızlanması, doğal olarak bilişim alanındaki güvenlik sorunlarını da ortaya çıkarmıştır. Şifreleme uzmanı Bruce Schiner'in de belirttiği gibi; "Eğer teknolojinin tek başına güvenlik problemlerini çözeceğini düşünülüyorsa güvenlik problemi ve güvenlik teknolojileri tam anlaşılmamış demektir." Bu sözden hareketle bilişim suçları ile mücadele de sadece teknolojik önlemler almak yeterli değildir. Elbette teknolojik önlemler bilişim suçlarının önlenmesi konusunda önemli bir araç olmakla birlikte bunun yanı sıra farkındalık ve hukuksal alt yapıda önemli diğer iki unsurdur. Aslında bu üç unsur sıkça dile getirildiği gibi bir sacayağının üçayağını teşkil etmektedir ve birisinin

bulunmaması halinde denge sağlanamayacak ve bu konuda işe yarar politikalar üretilemeyecektir.

İncelediğimiz bilişim alanında ilerlemiş ülke mevzuatları da göstermektedir ki genel olarak bilişim hukuku özelde ise her gün yeni suç türlerinin ortaya çıktığı bilişim suçları alanlarında daha detaylı ve sürekli bir çalışmaya ihtiyaç vardır. Örneğin ABD'nin bilişim suçları ile ilgili yasalarının oldukça ayrıntılı olduğu hemen göze çarpmaktadır. Ülkemize göre bilişim suçları ile daha erken karşılaşan ve bunlarla mücadele etmek zorunda kalan ABD ve bilişim konusunda önde olan diğer ülkelerin bilişim alanında ki yapmış olduğu mevzuat çalışmalarının da eleştirel bir gözle masaya yatırılarak daha önce yaşanmış tecrübeler sonucu oluşan bu birikimden ülkemizin ihtiyaçları doğrultusunda yararlanılması Amerika'yı yeniden keşfetmeme bağlamında yerinde olacağı kanaatindeyiz. Aksi takdirde daha önce tartışılmış ve bir şekilde çözüme kavuşturulmuş sorunlarla boş yere vakit kaybedilmesi ve emek ve zamanın asıl harcanması gereken alanlardan başka alanlara kayması sonucu ortaya çıkacaktır. Çünkü bilişim suçları gelişen teknolojiye paralel olarak hızla artmakta, sürekli ve inatçı bir mücadele yöntemi belirlenmesi, bu alanda yapılan uluslararası çalışmalara daha fazla katkı sağlanması yerinde bir yöntem olacaktır.

Ülkemizdeki bilişim suçlarına karşı mücadelenin hukuksal boyutunda yukarda da belirttiğimiz gibi bir takım mevzuat çalışmaları halen gündemdedir. Bu çalışmalar yapılırken İnternet'in doğası gereği özgürlük alanı olduğu unutulmamalı, yapılan yasalar da bu özgürlük alanının mümkün olduğu kadar az daraltılmasına hassasiyet gösterilmesi gerekmektedir. Bu çalışmalar yapılırken uluslararası hukuksal düzenlemeler mutlaka göz önünde bulundurulmalı ve örnek çalışmalardan yararlanılmalıdır. Bunun yanı sıra bu konuda tepki niteliğindeki yasal düzenlemelerden çok ihtiyaçlar önceden tespit edilmeye çalışılarak hukuksal bağlamda gelişmeleri öngörerek yasal çalışmalar için problemlerin içinden çıkılmaz hale gelmesi beklenmemeli, konuyu inceleyen kurum ve kuruluşlar oluşturulmalı ve aynı zamanda konu akademik bağlamda uygulama ile ilişkili olarak enstitüler vb. yapılanmalar vasıtası ile ele alınmalıdır. Bu konuda kamuoyuna yansıyan yasalar ancak meydana gelen gelişmelere tepki olarak düzenlenir şekildeki yaygın kanaate katılmamaktayız. Çünkü bugün gündemimizde olan birçok problem elektronik ortamın kullanılmaya başlandığı ilk zamanlardan bu yana vardı ve artarak var olmaya devam etmektedir. Kaldı ki bilişim suçları konusundaki birçok mevzuat düzenlemesi gelişmiş olan ülkelerde 90'lı yıllarda mevcut idi. Hatta bizim mevzuatımıza bile 1990'lı yılların başında girdiği düşünüldüğünde aslında konunun ülkemiz açısından çok yeni olmadığı görülmektedir.

Konuya bu açılardan yaklaşıldığında bilişim suçları konusundaki yasal düzenlemeler yapılırken daha geniş katılımlı tartışma zeminleri oluşturulmalı ve konunun uzmanı tüm bireylerden bir şekilde katkı sağlanması gerekmektedir.

Raporumuzun 4. bölümünde yer alan bilgi güvenliği konusu da yine gündemi işgal eden ve değişik adli olaylarla gündeme taşınan önemli konulardan birisidir. Aslında bilgi güvenliği uluslararası alanda çok gündemde olan bir konu olup genelde uluslararası birçok standardı ve kuralları ortaya çıkmış bulunmaktadır. Ancak bu standartların ülkeler bazında uygulamaya sokulabilmesi, uyulması zorunlu hale getirilmesi için bunları yasal anlamda iç hukukta bağlayıcı hale getirmeye ihtiyaç bulunmaktadır. Bilişim alanında gelişmiş ülkeler de bilgi güvenliği konusunda yasal düzenlemelerini yaparken genel de oluşmuş uluslar arası standartları göz önünde bulundurularak genel ilkeleri belirlemekte ve detayları daha alt mevzuat düzenlemelerine bırakarak, bilgi güvenliğinin kurumsal alt yapılarını oluşturdukları görülmektedir. Ülkemizde bilgi güvenliği alanında finans sektöründe ve diğer bazı yasal düzenlemelerde kısmi hükümler ortaya konulmuş olmakla birlikte, gerek kamu gerekse özel sektörü bağlayıcı sırf bilgi güvenliği konusunu ve kurumsal yapısını düzenleyen bir yasal mevzuat bulunmamaktadır. Bu konu da Milli Savunma Bakanlığı tarafından bir Yasa Tasarısı hazırlanmış ve uzun süreden beri tartışılmaktadır. Bu yasa tasarısının veya yeni hazırlanacak başka bir tasarının tüm bilgi güvenliğinin temel ilkelerini ve kurumsal yapısını kapsayacak şekilde ve uluslararası düzenlemeler dikkate alınarak yeniden gözden geçirilmesi ve yürürlüğe konulması bir ihtiyaç haline gelmiştir. Ancak burada dikkat edilmesi gereken konu bu yasanın bilginin içeriği ile ilgili düzenleme yapmaması, asıl bilginin bulunduğu yerde fiziksel ve sistem içersinde ki güvenliğini ilgilendiren konularda düzenleme yapmasıdır. Bilgi güvenliğinin amacı bilgiye sadece yetkili olan kişilerin yasalarla belirtilen amaçlar doğrultusunda ve bu amaçla sınırlı olmak üzere sadece bu kişiler tarafından erişilmesine olanak sağlamaktadır.

5. Bölümde kişisel verilerin korunması konusuna değinilmiş ve kişisel verilerin korunması ile ilgili genel kavramlar üzerinde durulmuştur. Daha sonra uygulamada en çok veri işleyen İdarenin kişisel verileri işlemesi üzerinde durularak konu ayrıntılı olarak tartışılmış ve Kişisel Verilerin Korunması Yasa Tasarısı eleştirel bağlamda ele alınmıştır.

6. Bölümde ele aldığımız Medeni Usul Hukuku bağlamında önemli bir konu da elektronik imzadır. Elektronik imza kavramı, uygulamaya ve hukuk sistemimize 5070 sayılı Elektronik İmza Kanunu ile birlikte girmiştir. Daha doğrusu güvenli elektronik imza kavramı ilk defa Elektronik İmza Kanunu ile gündeme gelmiştir. Toplumumuzun çoğu tarafından bilinmeyen ancak hem Uluslarası ilişkilerde hem de modern toplumlarda

günlük hayatta sıkça kullanılan elektronik imza, günlük hayatı ve iş hayatını kolaylaştıran bir vasıtadır.

Teknolojinin gelişmesi ve İnternet ağının yaygınlaşması ile aslında güvenli olarak nitelendirilemeyen elektronik imzalı belgeler, sanal ortamda dolaşmaya başlamıştır. Bu belgelerin değiştirilmesi ihtimalinin olması ve elektronik belge, veri ve kayıtlara hukuki güvence getirilmesi ihtiyacının bir sonucu olarak Elektronik İmza Kanunu çıkarılmıştır.

Avrupa Birliğine girme çabalarımızın devam ettiği bir süreçte Avrupa Birliğine üye ülkelerin uygulamaları da bize yol göstermiş, elektronik imzalar için topluluk çerçevesi konusunda 13 Aralık 1999 tarihli 1999/93/AT sayılı Avrupa Parlamentosu ve Konsey Direktifi temel alınarak 5070 sayılı Kanun hazırlanmıştır.

15 Ocak 2004 tarihinde Türkiye Büyük Millet Meclisinde kabul edilerek resmi gazetede yayımlanan Kanun, 24 Temmuz 2004 tarihinde yürürlüğe girmiştir. Bu tarihten sonra Kanunda yetkilendirilen Telekomünikasyon Kurumu ikincil mevzuat çalışmalarına başlamış ve ilgili yönetmelik çıkarılmıştır. Ardından yönetmeliğe dayalı tebliğler ve genelgeler ayrıntıları ile uygulamayı belirlemek açısından düzenlenmiş ve yayımlanmıştır.

Elektronik imza konusunda düzenleyici ve denetleyici kurum olarak belirlenen Telekomünikasyon Kurumu, bu yöndeki çalışmalarını 5070 sayılı Kanundan aldığı yetki ile devam ettirmektedir. Ayrıca 2004/21 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının çalışanlarıyla birlikte nitelikli elektronik sertifikalarını sağlamak amacıyla kamu sertifikasyon merkezi oluşturulmuştur. Bu merkezin işletimi TÜBİTAK-UEKAE'ye verilmiştir.

Elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik imza, elektronik belgenin kimin tarafından oluşturulduğunu ve belgeyi oluşturma ifadesini doğrulayan elektronik bir kayıttır. Elektronik sözleşmeler ve işlemler açısından ise, şekil şartını sağlayan bir unsurdur.

Güvenli elektronik imza dışında kullanılan bir takım elektronik imzalar da olmakla birlikte, 5070 sayılı Kanun tarafından geçerli kabul edilen ve kesin delil niteliği verilen imza, açık anahtar alt yapısı ve biyometrik tanımlama yöntemleri kullanılarak oluşturulan güvenli elektronik imzadır.

Elektronik İmza Kanunu'nun yürürlüğe girmesi ile BK. da düzenlenen klasik imza ile güvenli elektronik imza aynı bazı istisnalar haricinde aynı hukuki sonuçları doğurmaktadır. Getiren istisnalar 5070 sayılı Kanunun 5. maddesinde sayılmış bulunan

ve kanunlarca özel bir merasimin öngörüldüğü, üçüncü kişilerin katılımının istendiği bir takım hukuki ilişkilerdir. Elektronik ortamın güvenliğinin artması, teknolojinin gelişmesi ve kullanımının yaygınlaşması ile ayrık tutulan hukuki işlemlerinde ileride güvenli elektronik imza kullanılarak yapılması mümkün olabilecektir.

Güvenli elektronik imza ile imzalanmış belgeler mahkemelerde kesin delil olarak değerlendirilebilmektedir. Hukuk Usulü muhakemeleri Kanununa eklenen 295/A maddesi ile elektronik imza ile oluşturulan elektronik veriler senet hükmünde sayılacak ve aksi ispat edilinceye kadar kesin delil olarak değerlendirip işlem görecektir.

Elektronik ortamlarda bilgi alışverişi üzerine kurulmuş bulunan elektronik ticaretin gelişmesi, elektronik sözleşmelerin yaygınlaşması için elektronik imzaya hukuki bir geçerlilik kazandıracak böyle bir Kanuna olan ihtiyaç Elektronik İmza Kanunu ile giderilmiştir. Bu şekilde ticari değeri olan-olmayan elektronik belgeler, taraflar için hukuki yükümlülük doğurabilecektir. Taraflar bir araya gelmeden belge ve sözleşme oluşturabilecekler ve bu belgeler klasik imzalı belgeler ile aynı hukuki geçerliliğe sahip olacaktır.

Alt yapı çalışmaları ve yasal düzenlemelerin tamamlanması ile elektronik imza uygulamada yaygın olarak kullanılacaktır

Medeni Usul Hukuku alanında temel yasa olan HUMK'u baştan sona değiştiren HMK tasarısı BT bakımından baştan sona yeniden gözden geçirilmeli özellikle sadece elektronik ortamda işlem yapma, elektronik dava, elektronik tebligat gibi konular da yasal mevzuat oluşturularak bu alandaki teknolojik olanakların kullanılması yönündeki engeller kaldırılmalıdır.

Son bölümde ele aldığımız BT bakımından fikri ve sınaî haklar ve bu hakların takipleri ve korunması konusunda sonuç olarak şu konuların altını çizmekte yarar olduğunu görmekteyiz.

Öncelikle artık fikri ve sınaî hakların bilişim alanında korunması mekanizması mahkemelerden, araştırma enstitülerine ve meslek örgütlerine kaymaktadır. Bu nedenle ülkemizde de dünyadaki bu genel gidişata uygun olarak teknoloji ve fikri hukuk ağırlıklı enstitülere ihtiyaç vardır.

Yurtdışı örneklerinde Meslek Birliklerinin bu tür enstitüleri kurdukları ve destekledikleri örnekler pek çoktur. Gema, Institüt für Urheber- und Medienrecht gibi.

Bunun yanı sıra bu alanda teknik koruma ve işbirliğine dayanan sistemlerin Türkiye'de de geliştirilmesi, kurulması gerekmektedir.

Servis sağlayıcılar, meslek birlikleri, Telekom ve İnternet'in kamusal bir erk tarafından sağlandığı kuruluşlar arasında işbirliğine ihtiyaç vardır. Kültür Bakanlığının

bu yönde çalışmalar yapması gerekir. Ayrıca uluslararası işbirliklerine de ihtiyaç duyulacaktır.

Bu alanda bir takip komisyonu kurulmalıdır. Bu komisyonun görevi,

- Yeni ihlal tiplerinin tespiti,
- Bunlar için teknik koruma yöntem ve usullerinin belirlenmesi,
- Hukuki mücadelenin altyapısını hazırlamak olmalıdır.

Toplu kullanım alanlarında müzik değişim programlarına karşı filtre sistemi uygulanmalıdır. Bu özellikle Türkiye'de daha bir önem kazanmaktadır.

Nihayet, Avusturyalı Hukukçu Anton Kolb'un ifadesi ile "Günümüzde gelişen teknoloji ile birlikte çokluortam (multimedya) suçluluğu ortaya çıkmıştır. Disiplinler arası çalışmaya ihtiyaç vardır. Bu nedenle, bilişim, ekonomi, kültür, politika ve hukukun işbirliği içinde mücadelesine ihtiyaç vardır".

9 EKLER

9.1 E-Devlet Yasalarına Örnek bir Yasa ABD e-Devlet Kanunu

ABD'de E-Devlet çalışmaları Clinton döneminde Başkan Yardımcısı Algore'un yürüttüğü "devleti yeniden icat etmek" çalışmaları ile başlamıştır. Bu dönemde 1998 de çıkarılan "Devlet İşlerinde Kâğıt Kullanımının Kaldırılması Kanunu" 2002 e-Devlet kanununa temel teşkil etmiştir.

Genel bir bakış açısıyla, ABD E-Devlet Kanunu devlet hizmetlerinin elektronik ortama taşınmasını ve devlet-vatandaş arasındaki iletişimin kâğıtsız bir ortamda yapılmasını hedeflemektedir. En geniş anlamda kanunun amacı, bilgi teknolojilerinin tüm olanaklarını kullanarak devlette verimliliğin, etkinliğin ve hizmet kalitesinin arttırılması ve vatandaşların devletçe sunulan bilgi ve hizmetlere erişiminin en üst düzeye çıkarılmasıdır.

Kanun devlet politikası adına, İnternet tabanlı bilgi teknolojilerinin kullanılmasını zorunlu kılan genel bir çerçeve çizmiştir. Kurumsal yapı açısından bakıldığında ise, e-Devlet kanunu ABD Federal Hükümeti'nde Başkanlığa bağlı İdare ve Bütçe Ofisi'ne bağlı e-Devlet Ofisi kurulmasını öngörmüştür. Ayrıca kanun, bilgi-işlem başkanları konseyinin oluşturulmasını öngörmüştür. Kanun, e-Devlet Ofisi yöneticisinin görev ve sorumluluklarını belirtmiş ve bilgi başkanları konseyinin üyelerini, konseyin görevlerini ve çalışma şekillerini belirlemiştir. Mali olarak da hazinede e-Devlet fonu oluşturulmasını öngörmüş, fonun idare makamını ve idare şeklini belirlemiş ve fon kapsamında desteklenecek projelerin genel çerçevesini çizmiş ve 2003–2006 mali yılları için fon miktarını belirlemiştir. Bu miktar, 2003 yılı için $45 milyon, 2004 yılı için $50 milyon, 2005 yılı için $100 milyon ve 2006 için $150 milyon olarak saptanmıştır. Kanun, idarenin kongreye bu fonun işletilmesine ilişkin yıllık rapor sunmasını öngörmüştür.

E-Devlet Ofisi yöneticisinin başlıca görevleri şu şekilde sıralanmıştır:

- Bilgi-İşlem stratejileri konusunda İdare ve Bütçe Ofisine tavsiyelerde bulunmak
- E-Devletin devlet genelinde önderliğini yapmak ve yönünü belirlemek
- Özellikle kurumlar arası yürütülecek projeler yolu ile devlet kurumlarının bilgi teknolojilerini etkin ve yenilikçi bir biçimde kullanmalarını sağlamak
- E-Devlet fonunu idare etmek ve kullanmak
- E-Devleti teşvik etmek ve kurumlarca etkili kullanımını sağlamak

- Bilgi teknolojileri politikasının geliştirilmesinde İdare ve Bütçe Ofisi Müdürüne yardımcı olmak

Denetime yönelik olarak E-Devlet Kanunu, idarenin kongreye yıllık olarak E-Devlet Raporu sunmasını öngörmüştür. Bu raporda, e-Devlet fonu durum raporu, idari birimlere ilişkin e-Devlet raporları ve Federal Devletin kanunun gereklerini yerini getirmesine ilişkin uygulama raporunu içermesi öngörülmüştür.

Kanun E-Devlet hizmetlerinin teşviki ve geliştirilmesi adına idari birimlerin sorumluluklarını belirlemiştir. Bu bağlamda, kanunun uygulama sorumluluğunu bakanlara ve kurumların bilgi-işlem müdürlerine yüklemiştir. Her kurumun, kurum hedeflerine ve amaçlarına ulaşmada ve kanunların gereklerini yerine getirmede e-Devlet uygulamalarının katkısını gösterir nitelikte performans ölçütleri geliştirmesini gerekli kılmıştır. Bu performans ölçütlerinin müşteri hizmetleri, kurum üretkenliği ve özel sektörde kullanılan örnek uygulamaları da içerir yeni bilgi teknolojilerinin benimsenip kullanılma düzeyini kapsaması öngörülmüştür. Ayrıca, kurumların e-Devlet hizmetlerini planlarken toplumun İnternet erişimindeki farklılıklarını ve bireylerin bedensel engellilik durumlarını göz önünde bulundurmalarını ve İnternet'e erişimi olmayanların devlet hizmetlerine ulaşmasının kısıtlanmamasını öngörmüştür. Kurumların idareye yıllık olarak e-Devlet uygulamalarının ilerleme durumunu ve e-Devlet kanununun uygulanmasını gösterir E-Devlet raporları hazırlayıp sunmalarını zorunlu kılınmıştır.

Elektronik imza kullanımında idari birimler arasında verimliliğin artırılması için bir çerçeve geliştirilmesini ve elektronik imza için bir yetkili sertifikasyon otoritesi oluşturulmasını öngörmüştür. Düzenleyici idari birimlerin, vatandaşların yönetime katılımını artırmak için kuralların oluşturulmasına ilişkin tüm bilgilerin İnternet üzerinden yayınlanmasını ve vatandaşların İnternet üzerinden fikir beyan etmelerine imkân tanıyacak on-line kanun yapma sisteminin geliştirilmesi gerekli kılınmıştır.

Vatandaşların devletçe sunulan hizmetlere ve yayınlanan bilgilere ulaşımını kolaylaştırmak için federal bir E-Devlet portalı oluşturulmasını ve bu portalın hizmet birimlerine göre değil hizmet başlıklarına göre düzenlenmesini öngörmüştür. Bunun yanında, Federal mahkemelerin vatandaşları bilgilendirmeleri için İnternet siteleri oluşturmalarını ve bu sitelerin güncel tutulmasını gerekli kılmıştır.

İnternet üzerinden yayınlanacak bilgiler dâhil, devlete ait bilgilerin saklanması, bu bilgilere erişim ve kullanım kriterleri ve standartları belirlenmiştir. Ayrıca, devletin vatandaşlardan bilgi toplama standartları belirlenmiş ve kişisel gizliliğe ait hususlar belirtilmiştir.

Bilgi teknolojileri alanında devletin personel politikası belirlenmiş ve bu bağlamda bir eğitim merkezi kurulması öngörülmüştür. Bilgi teknolojileri alanında

düzenli olarak personel ihtiyaç analizi yapılması, eğitim programı oluşturulması ve tüm devlet personelinin bilgi teknolojileri ve kaynak yönetimi konularında eğitimi gerekli kılınmıştır.

Kanun coğrafik bilgilerin geliştirilmesi ve çeşitli birimlerde mevcut bilgilerin koordinasyonu görevini İçişleri Bakanlığına vermiştir. Verilerin oluşturulmasında öncelikle standartların geliştirilmesi öngörülmüş, özel sektör ve ilgili kurum ve kuruluşlar ile işbirliği yapılması gerekli kılınmıştır. Buna ek olarak, bilgi teknolojilerinin doğal afetler ve diğer tehlikelere karşı önlem almada ve gerektiğinde bunlara müdahalede kullanılması için bir araştırma ve uygulama stratejisi geliştirilmesi öngörülmüştür.

Bu kanun ABD hükümetinin İnternet'in sunduğu olanaklardan en iyi şekilde yararlanmasını ve yeni bilgi teknolojilerinin verimliliği artıracak şekilde kullanılmasını sağlamak amacı ile çıkarılmıştır. Kökleri Clinton dönemine dayanmakla birlikte, bu kanun, Bush yönetimi tarafından hedeflenen "vatandaş merkezli, endüstri tabanlı ve sonuç odaklı" bir kamu yönetimini gerçekleştirmek için atılan önemli adımlardan birisidir.

Kanunun en önemli özelliği, E-Devlete ilişkin yapısal alanda getirdiği yeniliktir. İdare ve Bütçe ofisine bağlı E-Devlet Ofisi kurulmuş ve hükümet genelinde E-Devletin yönetimi ve denetimi bu ofise verilmiştir. Kanun bu ofisin yetki ve sorumluluklarını belirlemiş ve kanunun uygulanması için E-Devlet fonu oluşturulmasını öngörmüştür.

Devlet kurumları açısından bakıldığında kanun, her kurumun E-Devleti kurumun amaçlarını ve stratejik hedeflerini destekleyecek şekilde planlamasını öngörmüştür. Bunun için geliştirilecek performans ölçütlerinin, E-Devletin kurumların hedeflerini gerçekleştirme adına sağladığı katkıyı göstermesini zorunlu kılmıştır. Denetime yönelik olarak da kanun, yıllık olarak kurumların idareye idarenin de kongreye E-Devlet raporları sunmasını gerekli kılmıştır.

Kanunun bir diğer önemli özelliği de, elektronik ortamda güvenlik ve şeffaflık konularına ışık tutmasıdır. Devlete ait verilerin düzenlenmesi, korunması, kullanılması ve vatandaşlara sunulması konuları düzenleme altına alınmıştır. Ayrıca, kanun Federal devlete ait İnternet sitelerinin içeriği ve yapısı hakkında düzenlemeler getirmiştir. Bu sitelerin, ait olduğu kurumun misyonu ve kanuni yetki alanı, kurumla ilgili tüm bilgi ve belgelerin görülebileceği elektronik okuma odası, kurumun örgütsel yapısı ve kurumun stratejik planını içermeleri öngörülmüştür.

Kamu kurum ve kuruluşlarının yanında yenilikçiliğin öncüsü olan özel sektöre de kamu desteği öngörülmüştür. Kanun, E-Devlet hizmetlerinin ve işlevlerinin geliştirilmesi için devlet genelinde hazırlanacak bir program ile özel sektörde yeniliğin ve mükemmeliyetçiliğin teşvikini öngörmüştür.

Özetle 2002 e-Devlet Kanunu ABD için şu yenilikleri getirmiştir: E-Devlet hizmetlerinin hukuki temellerinin oluşturulması, uygulamaya yönelik performans ölçütlerinin oluşturulması, E-Devlet hizmetlerinin planlanması ve koordinesinin kanun ile kurulan E-Devlet ofisine verilmesi, elektronik imzanın kurumlar tarafından kullanılması, mahkemelerin İnternet siteleri aracılığı ile işleyişleri ve kararları hakkında kamuyu bilgilendirmeleri, devlet tarafından toplanan kişisel verilerin güvenliği ve gizliliği konusunda çerçeve oluşturulması, elektronik ortamda veri yönetimi ve güvenliği politikalarının oluşturulması.

Hukuk devletinin tüm etkinlikleri anayasa, kanunlar ve diğer kurallar ile sınırlı olduğundan, e-Devletin gelişmesine imkân tanıyacak hukuki düzenlemenin oluşturulması büyük önem arz etmektedir. Modern bilgi teknolojilerinin ve iletişim araçlarının kullanıldığı günümüzde, kamu hizmetlerinin elektronik ortamda üretilmesi ve sunulması e-Devlet çözümlerini hukuken bağlayıcı kılacak kanunların varlığına bağlıdır. Bu bağlamda, elektronik imza, elektronik doküman, devlet birimleri ve vatandaşlar arasında elektronik haberleşme, veri güvenliği ve verinin korunması gibi konuların hukuki düzenleme altına alınması gerekmektedir. Ancak, e-Devlet konusunda düzenleme gerektiren konuların çokluğu nedeni ile e-Devletin gelişimini etkileyecek ilgili tüm konuları kapsayacak bir çerçeve çizilerek gerekli idari ve hukuki altyapının bir bütünlük içerisinde oluşturulması gerekmektedir. Aksi takdirde, bu konuların ayrı ayrı ele alınarak düzenlemeye tabi tutulması, uygulama aşamasında sorunlara yol açacaktır.

Çıkarılacak bir e-Devlet kanunu, öncelikle e-Devletin gelişimine temel teşkil edecek nitelikte olmalı ve gelişim aşamalarını düzenlemelidir. Bu kanunun temel amacı e-Devletin etkin gelişimi için genel bir hukuki çerçeve çizerek daha sonra çıkarılacak ilgili kanunlara temel teşkil etmek olmalıdır. Böyle bir kanun, e-Devletin oluşumunda hukuki bütünlüğü ve devlet politikasının sürekliliğini sağlayacaktır.

Kanun, e-Devletin gelişimine ilişkin devletin temel görevlerini ve sorumlu devlet birimlerini yükümlülükleri ile birlikte açıkça belirtmelidir. Ayrıca, kanunun uygulanması için gerekli mali kaynak sağlanmalı ve uygulamanın takibi için performans ölçütleri konulmalıdır. Örnek olarak, “2010 yılında tüm kamu kurum ve kuruluşları hizmetlerinin en az %80ini İnternet üzerinden sunmalıdır” şeklinde bir ölçüt konulmalı ve bunun yıllık bazda takibi yapılmalıdır.

Kanun elektronik idareye toplumun tüm kesimlerinin ve sivil toplum kuruluşlarının katılabilmesini garanti altına almalı, devlet-toplum işbirliğini geliştirmeli ve etkin bir idare mekanizması oluşturmalıdır. Kanun ile temel hak ve hürriyetlerin tamamı elektronik ortamda da geçerli kılınmalı ve elektronik ortamın sağladığı İnternet’e erişim

hakkı ve elektronik bilgi hakkı gibi ek haklar garanti altına alınmalıdır. Ayrıca İnternet üzerinde veri iletişiminin gizlilik ve güvenlik esasları belirlenmelidir. Ulusal ve uluslararası entegrasyonun sağlanması için, elektronik verilerin oluşturulması, kullanımı ve paylaşımı gibi tüm e-Devlet hizmetleri için standartlar oluşturulmalı ve bu standartların oluşturulmasında öncelikle uluslararası standartlar temel alınmalıdır.[525]

9.2 Bilişim Suçlarının Karşılaştırılması

Suç	SSS[526]	765 MTCK	5237 YTCK	Tasarı
Yetkisiz Erişim	2	☹	243/1	15/1
Verinin Ele Geçirilmesi	3	525a/1,2	244/2	15/2
BS'nin donanım kısmına zarar verme suçu	5	525b/1	244/1	
BS' de verilere yönelik zarar verme suçu"	4	525a/1–2	244/2	16
Sisteme Müdahale Engelleme	5	525b/1	244/1	
BS ile haksız yarar sağlama suçu (BS ye karşı dolandırıcılık)	8	525b/2	244/4[527]	19
BS'de Sahtecilik	7	525c	☹	18/1–2

[525] Bu Bölümün oluşturulmasında DPT'da Uzman olarak çalışan Sayın Ramazan Altınok'un çalışması esas alınmıştır.

[526] Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte 23.11.2001) Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte 23.11.2001) m.2: "Her bir taraf Devlet bir bilgisayar sisteminin tamamı veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanunî düzenlemeyi yapmalı gerekli önlemleri almalıdır. Taraf Devlet bu suçun oluşması için erişimin güvenlik önlemleri ihlâl edilerek ya da bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla bilgisayar verisini almak ya da başka kötü niyetlerle kullanmak şartına bağlayabilir".

[527] "Bilindiği üzere, dolandırıcılık suçunun oluşabilmesi için suç mağduru kişinin iradesinin hile ve desise sonucu kandırılması, etkilenmesi gerekmektedir, halbuki eylem bir bilgisayara, bir bilişim sistemine karşı gerçekleştirildiğinde bilgisayarın iradesi diye bir şey söz konusu olamayacağından yani ortada etkilenen bir irade bulunmayacağından eylem dolandırıcılık suçunu değil ve fakat bilgisayar marifetiyle haksız menfaat sağlaması suçunu oluşturacaktır. Fiil, eğer, banka kartı veya kredi kartı kullanmak suretiyle bir bilişim sistemi kullanılmaksızın, örneğin slip makinelerinin kullanılması gibi, mağdurun iradesini etkileyecek surette hile ve desise söz konusu olursa, bu takdirde fiil bir bilişim sistemine karşı işlenmiş olamaz, zira daha henüz bir bilgisayara veri yüklemek veya mevcut verileri manipüle etmek söz konusu olmamıştır bu sebeple burada sadece mağdurun iradesi etkilendiğinden dolandırıcılık suçu söz konusu olacaktır." MEDA kapsamında yürütülen "Yargının Modernizasyonu ve Cezaevi Reformu Projesi " çerçevesinde Adalet Akademisi tarafından düzenlenen 5-6-7 Şubat 2007 Tarihinde İstanbul Dedeman Otelinde gerçekleştirilen Adalet ve Bilişim Teknolojileri Sempozyumunda Doç. Dr. Yılmaz YAZICIOGLU tarafından yapılan "AB Uyum Komisyonu Çalışması Türk Mevzuatında Bilişim Suçları" başlıklı konuşmadan alıntı yapılmıştır konuşmanın tamamı için tıklayınız;
http://www.taa.gov.tr/duyurularana/130606/bilisimsempozyum/sunum/makale.pdf (03.05.2008)

Suç	SSS[526]	765 MTCK	5237 YTCK	Tasarı
Şifrelerin dağıtımını veya hukuk dışı olarak bir BS veya programının hizmetlerinden istifadeyi sağlayacak cihaz veya programları satma veya tedarik etme suçu[528]	6	☹	☹	17
Başkasına ait kredi veya banka kartının haksız olarak ele geçirilmesi sonucu haksız menfaat temini suçu	8	504/3[529] 525b2[530]	245/1	20/1
Sahte kredi veya banka kredi kartı üretme, satma, devretme, satın alma veya kabul etme suçu	8	☹	245/2	20/2
Sahte kredi veya banka kartı marifetiyle haksız menfaat edimi suçu	8	504/3	245/3	20/3
Çocuk Pornografisi	9	☹ 426, 427, 428 [531]	226/3	23
Kişisel Verilerin	[532]	☹	135, 137	☹

[528] SSS Madde 6 – Cihazların Kötüye Kullanımı

- Taraflardan her biri, söz konusu hakkın 1(a) ve 2 numaralı paragraflarda belirtilen unsurların satışına, dağıtımına ve başka suretle kullanıma sunulmasına ilişkin durumlarda kullanılmaması şartıyla, işbu maddenin 1 numaralı paragrafını uygulamama haklarını saklı tutmaktadır.

[529] Kredi kartını ele geçirip daha sonra pos cihazından kendisinin gibi alış verişi yapması halinde uygulanır.

[530] ATMden nakit para çalınırsa

[531] 765 S. Mülga TCK'de müstehcenlikle ilgili genel bir düzenleme var, çocuklara özgü özel bir düzenleme yok, http://www.hukukcu.com/bilimsel/kitaplar/mustehcenlik.htm, (03.05.2008)
http://turk.İnternet.com/haber/yazigoster.php3?yaziid=13182 (03.05.2008)

Suç	SSS[526]	765 MTCK	5237 YTCK	Tasarı
Hukuka Aykırı Kaydedilmesi	3, 4			
Kişisel verileri verme, yayma veya ele geçirme	[533] 3, 4	☹	136, 137	☹
BS Vasıtasıyla Dolandırıcılık	8	☹525b/2504/3[534]	158/1, f bendi[535]	☹
BS Vasıtasıyla Hırsızlık	☹	☹	142/2, e bendi	☹
Yanıltarak bilgi toplamak (Phising)	☹	☹	☹	21
Taklit yoluyla yanıltmak	☹	☹	☹	22

[532] SSS'de 1981 Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Konusunda Avrupa Konvansiyonu tarafından da belirtilen kişisel bilgilerin korunmasına hususuna da gerekli önem verilerek hazırlandığı sözleşmenin giriş kısmında belirtilmiştir.
[533] SSS'de 1981 Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Konusunda Avrupa Konvansiyonu tarafından da belirtilen kişisel bilgilerin korunmasına hususuna da gerekli önem verilerek hazırlandığı sözleşmenin giriş kısmında belirtilmiştir.
[534] Gerçek kredi kartı ile alış verişi yapılırsa TCK 765 504/1, Sahte kimlik ile bankadan kredi kartı çıkartması halinde sanki bankadan haksız kredi almış gibi değerlendiriliyordu.
[535] TCK Madde 157 - (1) Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beş bin güne kadar adlî para cezası verilir.

9.3 5237 S. TCK'da Basın Yayın Yolu ile İşlenen Bilişim Suçları

5237 S. TCK' da[536] **Basın Yayın Yolu ile İşlenen Bilişim Suçları**	
6. m/g bendinde; "Basın ve yayın yolu ile deyiminden; her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar" anlaşılır	
Hakaret ve sövme	125/4
Müstehcenlik	226/2–5
Suç işlemeye tahrik	214, 218
İntihar suçu	84/3
Haberleşmenin gizliliğini ihlal suçu	132/4
Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu	133/3
Özel hayatın gizliliğini ihlal suçu	134/2
Halk arasında korku ve panik yaratmak amacıyla tehdit	213, 218
Suç işlemeye tahrik	214, 218
Suçu ve suçluyu övme	215, 218
Halkı kin ve düşmanlığa tahrik veya aşağılama	216, 218

[536] Tasarıda İçerikle ilgili Yeni Düzenlemeler;
Devletin güvenliğine ve kamu barışına karşı işlenen suçlar
MADDE 24- (1) Bilişim ortamında aleni olarak;
a) Türk Ceza Kanununun 222 (25.11.1925 tarihli ve 671 sayılı Şapka İktisası Hakkında Kanunla, 1.11.1928 tarihli ve 1353 sayılı Türk Harflerinin Kabul ve Tatbiki Hakkında Kanunun koyduğu yasaklara veya yükümlülüklere aykırı hareket edenlere iki aydan altı aya kadar hapis cezası verilir.), 258 (Görevi nedeniyle kendisine verilen veya aynı nedenle bilgi edindiği ve gizli kalması gereken belgeleri, kararları ve emirleri ve diğer tebligatı açıklayan veya yayınlayan veya ne suretle olursa olsun başkalarının bilgi edinmesini kolaylaştıran kamu görevlisine, bir yıldan dört yıla kadar hapis cezası verilir.), 299 (Cumhurbaşkanına hakaret), 300 (Türk Bayrağını yırtarak, yakarak veya sair surette ve alenen aşağılayan kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu hüküm, Anayasada belirlenen beyaz ay yıldızlı al bayrak özelliklerini taşıyan ve Türkiye Cumhuriyeti Devletinin egemenlik alâmeti olarak kullanılan her türlü işaret hakkında uygulanır.) (İstiklal Marşını alenen aşağılayan kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.), 301 (Türklüğü, Cumhuriyeti veya Türkiye Büyük Millet Meclisini alenen aşağılayan kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. 2. Fıkra; Türkiye Cumhuriyeti Hükûmetini, Devletin yargı organlarını, askerî veya emniyet teşkilatını alenen aşağılayan kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.), 304, 306, 307, 308, 313, 316, 319, 320, 323, 326, 327, 328, 329, 330, 331, 333, 334, 335, 336, 337, 338 ve 339 uncu maddelerinde,
b) 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda,
Yer alan ve bilişim sistemi veya bilişim ağı kullanılarak işlenen suçlara ilişkin içeriği üreten, tanıtan veya sunanlar hakkında hükmedilecek cezalar yarı oranında arttırılır.

5237 S. TCK' da[536] Basın Yayın Yolu ile İşlenen Bilişim Suçları	
6. m/g bendinde; "Basın ve yayın yolu ile deyiminden; her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar" anlaşılır	
Kanunlara uymamaya tahrik	217, 218
Örgütün veya amacının propagandasını yapma suçu	220/8
İftira suçu	267/1
Soruşturmanın gizliliğini ihlal suçu	285/3
Adil yargılamayı etkilemeye teşebbüs	288/2
Cumhurbaşkanına hakaret suçu	299/2
Devlete karşı savaşa tahrik suçu	304/1
Temel milli yararlara karşı hareket suç	305/2
Halkı askerlikten soğutma suçu	318/2

Devletin güvenliğine ve kamu barışına karşı işlenen suçlar

MADDE 24- (1) Bilişim ortamında aleni olarak;

a) Türk Ceza Kanununun 222, 258, 299, 300, 301, 304, 306, 307, 308, 313, 316, 319, 320, 323, 326, 327, 328, 329, 330, 331, 333, 334, 335, 336, 337, 338 ve 339 uncu maddelerinde,

b) 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda,

c)Yer alan ve bilişim sistemi veya bilişim ağı kullanılarak işlenen suçlara ilişkin içeriği üreten, tanıtan veya sunanlar hakkında hükmedilecek cezalar yarı oranında arttırılır.

10 KAYNAKÇA

1. Akbulut, Berrin, “Türk Ceza Hukukunda Bilişim Suçları”, Konya 1999
2. Al, Hamza **Bilgi Toplumu ve Kamu Yönetiminde Paradigma Değişimi,** Bilim Adamı Yayınları, Ankara,2002
3. Alkan, Mustafa, İnalöz; Telekom Regülâsyonları ve Elektronik İmzanın Elektronik Ticaret Üzerindeki Etkileri, TBD 21.Ulusal Bilişim Kurultayı Bildiriler Kitabı, Ankara 2004
4. Atalay, O. Medeni Usul Hukukunda Menfi Vakıaların İspatı, İzmir 2001
5. Atay, Ethem, **Genel İdari Usul Kanunu Tasarısı Sempozyumu**, Türk Hukuk Dergisi, Mayıs 2004, Özel 87. Sayı
6. Başalp, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayımevi,
7. Ankara 2004,
8. Biçkin, İnci “Elektronik İmza Kanunu ve Getirdiği Düzenlemeler”, Yargıtay Dergisi
9. Bilal Eryılmaz, **Kamu Yönetimi,** 2.Baskı, İzmir,1995,
10. Birsen Çırakman, **“Kamu Hizmeti”,** Amme İdaresi Dergisi, Cilt: 9, Sayı:4,Ankara, Aralık,1976
11. Bilgi Toplumuna Doğru, Türkiye 2. Bilişim Şurası Sonuç Raporu, Ankara 2004,
12. Bundesdatenschutzgesetz, Berlin, 5. Baskı, Druckerei Conrad, Eylül, 2004
13. Child Pornography: Model Legistation&Global Review 2006; İnternational Centre for Missing and Exploited Children; 2. Baskı
14. Çamurdan, Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme, 2003,http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm(21.04.2007)
15. Doğan Canman, **İnsan Kaynakları Yönetimi,** Yargı Yayınevi, Ankara, 2000,
16. Dülger, Murat Volkan, “Bilişim Suçları”, Seçkin Kitabevi, Ankara 2004,
17. Eichhorn, B. “İnternet-Recht, Ein Lehrbuch für das Recht im World-Wide-Web”, Köln 2000
18. **Ekşi**, Nuray: Elektronik İmzalara İlişkin Uncıtral Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme,
19. Yasa Hukuk Dergisi, S.3, Mart, 2001
20. Erdağ, Ali İhsan, Kırıkkale Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Öğretim Üyesi, Bilişim Alanında Suçlar Makalesi,2005
21. Erel, Ş. “Türk Fikir ve Sanat Hukuku”, Ankara 1998
22. Eren, F. : “Borçlar Hukuku Genel Hükümleri” 6. Bası, C. I, İstanbul 1998
23. ERMAN, Sahir, “ Kamu Güvenine Karşı İşlenen Suçlar”,Dünya Yayıncılık, İstanbul 1996,
24. Fassbender, Marcel; “Angriffe auf Datenangebotene im İnternet und deren starftrechliche Relevanz”, (DS), Hamburg, 2003,
25. Federrath, H. “Multimediale Inhalte und technischer Urheberrechtsschutz im İnternet”, ZUM, 2000

26. Funk, A. „Wettbewerbliche Grenzen von Werbung per E-Mail“, CR, 1998/7, s. 413, 414; Rosenthal, D:
27. Unverlangte Werbe E-Mail ohne Rechtsfolgen“, Media Lex, 4/99,
28. Garstka, Hansjürgen, 25 Jahre Datenschutz 5 Jahre Informationsfreiheit in Berlin, Berlin, 2004,
29. Gözler, Kemal, İdare Hukuku, C.1, Ekin Yayınevi, Bursa, 2003,
30. Gözübüyük, A.Şeref, Yönetim Hukuku, 13.Baskı, Turhan Kitapevi, Ankara,1999,
31. H.Yıldırım, V. Kaplan, T. Çakmak, C. C. Üstün tarafından yazılan e-Devlet Başa isimli kitabın 2. Baskı, Ankara 2006,
32. Hilgendorf, Jus, 1996, 509 (512), Schönke/Schröder-Lenckner, § 202a, Par.6
33. İnanıcı, Haluk, ”Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü”, İstanbul Barosu Dergisi, Cilt:70, Sayı:7–8–9
34. Tanılır, M.Niyazi; İnternet Suçları ve Bireysel Mahremiyet - Ocak 2002- Liberte Yayınları
35. Junker, M. “Anwendbares Recht und internationale Zustaendigkeit bei Urheberrechtsverletzungen im İnternet”, Kassel 2002
36. Kalpsüz, Turgut, Noterlik Hukuku Sempozyumu: III-IV-V (Noterlik Hukuku ile İlgili Bazı Sorunlar, Türk Hukuk Dili, Noterlik ve Tebligat Hukuku), Notev, Ankara 1999,
37. Karagülmez, Ali, Dr. Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, (2005)
38. Kaypakoğlu,S.;Bilgisayar Programlarının Hukuki Korunması, İzmir, 1997
39. Kerem Ertan, “Banka Kredi Açma Sözleşmelerinin Hukuki Niteliği ve Özellikle Çerçeve Anlaşma Olma Özelliği”, Legal Hukuk Dergisi, Sayı:7, 2003
40. Keser, Berber, “İmzalıyorum O Halde Varım, Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri”,TBB Dergisi,2000/2
41. Küçükközyiğit, Galip H; Elektronik Ticaret, Elektronik İmza ve Hukuk,2004.
42. Kurt, Levent. Tüm Yönleriyle Bilişim Suçları, Seçkin Yayınevi , (2005),
43. Kurt, Levent; Tüm Yönleri ile Bilişim Suçları ve TCK’da Uygulaması; Ankara 2005,
44. Kuru, B. Hukuk Muhakemeleri Usulü, C. II, İstanbul 1990
45. Kuru, B/Arslan, R/Yılmaz, E. Medeni Usul Hukuku, Ankara 2003
46. Lehmann, M. Digitalisierung und UrhR, İnternet und Multimdiarecht (Cyberlaw), Stutgart 1997
47. Lehmann, M./v. Tucher, T. “Urheberrechtlicher Schutz von multimedialen Webseiten” CR1999
48. Lettl, T. „Rechtsfragen des Direktmarketings per Telefon und E-Mail“, GRUR, 2000, s. 982, 983.
49. Mitnick,Kevin D./Simon,William L., “Aldatma Sanatı” Çeviren; Nejat Eralp Tezcan, Ankara,2006
50. Orta, Mesut; “Elektronik İmza ve Uygulaması”, Seçkin Yayınları, 2005 Ankara
51. Özbudun, Ergun, Türk Anayasa Hukuku, 7. Baskı, Yetkin Yayınları, Ankara, 2002,

52. Özgenç, İzzet; Türk Ceza Hukuku Genel Hükümler Ankara, 2006
53. Pekcanıtez, Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, s. 390,
54. Uluslar arası İnternet Hukuku Sempozyumu, İzmir 2002
55. Postacıoğlu İ. E. Medeni Usul Hukuku Dersleri, İstanbul 1975
56. Schack, H. "Urheber- und Urhebervertragsrecht", 2. Aufl. Tübingen 2001
57. Schwarz, M., Recht im İnternet, Bd. 1, Loseblattsammlung, Maerz 2000
58. Soydan Billur Y. E-İmza ve E-Belge: Kâğıtsız ve Mürekkepsiz Dünyada Hukuk–1, Vergi Sorunları Dergisi, s.151, Nisan 2001,
59. Sözüer, Doç. Dr. Âdem, "TCK, CMK ve Kabahatler Kanunundaki son değişiklikler ne getiriyor." HPD Aralık 2006, Sayı:9
60. Strömer, T. H. "Online Recht, Rechtsfragen im İnternet", 2. Auflage, Heidelberg 1999
61. Şenocak, Zarife: Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması, AÜHFD, 2001/2
62. Tanılır, M.Niyazi, "İnternet Suçları ve Bireysel Mahremiyet" Ankara, 2002
63. Topaloğlu, Mustafa: Bilişim Hukuku, Adana 2005,
64. Yazıcıoğlu, Yılmaz, "Bilgisayar Suçları: Krminolojik, Sosyolojik ve Hukuki Boyutları ile", Alfa Yayınevi, İstanbul 1997,
65. Yenidünya Dr. Caner; Değirmenci, Olgun; "Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları", İstanbul 2003,
66. Yüksel, M. Hukuk ve Adalet Dergisi, Ekim-Aralık 2004; İstanbul, 2005