**BİLİŞİM HUKUKU**

**UNITE -1**

Özellikle son çeyrek asırda tüm dünyayı etkileyen ve baş döndürücü bir hızla ilerleyen teknolojik gelişmeler, bilişim hukukunun ortaya çıkış sürecinin nedeni olarak kabul edilmektedir; Teknoloji alanındaki gelişmeler tarafların yüz yüze yaptıkları hukuksal işlemleri konu alan klasik yasal düzenlemelerin gözden geçirilmesini gerekli kılmıştır. Bilişim Hukuku teknolojilerindeki gelişmeler ve yenilikler sebebiyle mevcut yasal düzenlemelerin yetersiz kalması ile ortaya çıkmıştır. E-ticaretin gelişmesi, devletin vatandaşlarıyla olan ilişkilerinde e-devlet gibi bilişim sistemlerini kullanması sonucun da bilişim hukuku denilen yeni bir hukuk dalı ortaya çıkmıştır. Bu hukuk dalını oluşturan normların oluşturulması ve yürürlüğe konulması yetkilerinin devletlere bırakılması, diğer bir ifadeyle bu normları düzenleme hakkının devletlerin egemenlik yetkisinden doğduğunun kabulü, devletlere bilişim sistemlerinin çeşitli hukuki işlemlerde kullanılmasından doğan sorunların çözümlenmesi hususunda süratle hareket etmesi yönünde görev yüklemektedir. Ülkelerin gelişmişlik düzeyleri, ulusal ekonomileri, bilim ve teknolojiyi hayata geçirme istemleri ile yakından ilgilidir, çeşitli biçimlerdeki bilgiyi oluşturmak, saklamak, düzenlemek, yönetmek, taşımak, görüntülemek, aktarmak, değiştirmek, iletmek veya almak için kullanılan bütün teknolojileri içeren her türlü donanım ya da bağlantı sistemi olarak kabul edilen ve “bilgi teknolojileri” (BT) veya “bilgi ve iletişim teknolojileri” (BİT) olarak adlandırılan sistemleri yaygın biçimde kullanan, büyük miktarlarda bilgi ve iletişim ürünleri ve hizmetleri üreten, çeşitlendirilmiş içerik endüstrisine sahip “bilgi toplumunun” oluşturulması ve geliştirilmesi yönünde devletlere yüklenen pozitif ödevdir.

**Bilişim Hukukunun Yapısı**

Bünyesinde birçok farklı hukuk dalını barındırması ve/veya birçok hukuk dalıyla iç içe geçmesi nedeniyle, multi-disipliner bir hukuk dalı olarak tanımlanmaktadır. Kamu kurum ve kuruluşlarında bilgisayarların kullanılmasına ilişkin sorunlar veya e-devlet, Ulusal Yargı Ağı Projesi (UYAP) gibi yazılımlardan doğan problemler idare hukukunun alanına girmektedir. Yine genel olarak internetin yönetiminde hangi kurumların yetkili ve görevli olduğunun belirlenmesi temelde idare hukukunun konusu olmakla birlikte, bu kurumların yapmış oldukları idari tasarrufların temel hak ve özgürlükler çerçevesinde değerlendirilmesi ise insan hakları hukuku ve anayasa hukuku ile ilintilidir. Devletlerin siber savaşa karşı hazırlıklı olduklarını bildirmeleri ve siber saldırıyı savaş nedeni sayacaklarını açıklamaları göstermiştir ki, bilişim hukukunun uluslararası hukukla da bağlantısı vardır Bu tip örnekler kişilik hakları, özel hayatın gizliliği, kişisel verilerin korunması, rekabet hukuku, adli yardımlaşma hukuku v.b. verilebilir.

**BİLİŞİM HUKUKU MEVZUATINA GENEL BAKIŞ**

Bilişim hukukunu oluşturan mevzuat, birçok kanunun içinde dağınık bir görüntü sergilemektedir. Yine de bu dağınık görüntüyü “*bünyesinde bilişim hukukunu ilgilendiren normlar bulunduran mevzuat* ”ve “*bünyesinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulunduran mevzuat*” olarak iki alt başlık altında toplamak mümkündür.

**Bünyesinde Bilişim Hukukunu İlgilendiren Normlar Bulunduran Mevzuat**

6533 Sy Avrupa Siber Suç Sözleşmesini İç Hukuka >>Sanal Ortamda İşlenen Suçlar Sözleşmesinin Uygun Bulunduğuna Dair Kanun;

5237 Sy Türk Ceza Kanunu;

5271 Sy Ceza Muhakemesi Kanunu;

2803 Sy Jandarma Teşkilat ve Yetkileri Kanunu;

2559 Sy Polis Vazife ve Salahiyet Kanunu;

2937 Sy Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu;

4721 Sy Türk Medeni Kanunu;

6098 Sy Türk Borçlar Kanunu;

6502 Sy Tüketicinin Korunması Hakkında Kanun;

6698 Sy Kişisel Verilerin Korunması Kanunu;

4982 Sy Bilgi Edinme Hakkı Kanunu;

6102 Sy Türk Ticaret Kanunu;

6563 Sy Elektronik Ticaretin Düzenlenmesi Hakkında Kanun;

5070 Sy Elektronik İmza Kanunu;

5846 Sy Fikir ve Sanat Eserleri Kanunu;

6279 Sy Çoğaltılmış Fikir ve Sanat Eserlerini Derleme Kanunu;

5411 Sy Bankacılık Kanunu;

 5464 Sy Banka Kartları ve Kredi Kartları Kanunu;

6362 Sy Sermaye Piyasası Kanunu;

6493 Sy Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hk Kanun;

213 Sy Vergi Usul Kanunu;

488 Sy Damga Vergisi Kanunu;

5147 Sy Entegre Devre Topoğraflarının Korunması Hakkında Kanun;

4734 Sy Kamu İhale Kanunu;

5018 Sy Kamu Mali Yönetimi Kontrol Kanunu;

5300 Sy Tarım Ürünleri Lisanslı Depoculuk Kanunu;

6100 Sy Hukuk Muhakemeleri Kanunu;

2004 Sy İcra ve İflas Kanunu;

6112 Sy Radyo ve Televizyon Kuruluş ve Yayın Hizmetleri Hakkında Kanun;

7201 Sy Tebligat Kanunu;

406 Sy Telgraf ve Telefon Kanunu;

4691 Sy Teknoloji Geliştirme Bölgeleri Kanunu.

**Bünyesinde Doğrudan İnternet Ortamını Veya Bilişim Alanını Düzenlemeye Yönelik Normlar**

5651 Sy İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Kanun’un 1. maddesine göre bu yasanın amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülükle sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir.

Kanun’un 2. maddesinde tanımlar başlığı altında yasada yer alan bazı kavramların tanımlarına yer verilmiştir.

**Bakanlık:** Ulaştırma, Denizcilik ve Haberleşme Bakanlığını,

**Başkan:** Bilgi Teknolojileri ve İletişim Kurumu Başkanını,

**Bilgi:** Verilerin anlam kazanmış biçimini,

**Erişim:** Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

**Erişim sağlayıcı:** Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

**İçerik sağlayıcı:** İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

**İnternet ortamı:** Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

**İnternet ortamında yapılan yayın:** İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,

**İzleme:** İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,

**Kurum:** Bilgi Teknolojileri ve İletişim Kurumunu,

**Toplu kullanım sağlayıcı:** Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

**Trafik bilgisi:** Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,

**Veri:** Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

**Yayın:** İnternet ortamında yapılan yayını,

**Yer sağlayıcı:** Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,

**Birlik:** Erişim Sağlayıcıları Birliğini,

**Erişimin engellenmesi:** Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,

**İçeriğin yayından çıkartılması:** İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkartılmasını,

**URL adresi:** İlgili içeriğin internette bulunduğu tam internet adresini,

**Uyarı yöntemi:** İnternet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınmaması halinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini ifade eder. Kanun’un ilerleyen maddelerinde ise internet süjeleri olarak adlandırılan içerik, yer ve erişim sağlayıcılarının uymaları gereken kurallar, bu süjelerin sorumlulukları ve hangi durumlarda erişimin engelleneceği ve engelleme kararının verilmesinde kimlerin yetkili ve görevli olduğu düzenlenmiştir.

***Dikkat: İçerik, yer ve erişim sağlayıcılarına genel olarak internet süjeleri denilmektedir.***

Kanun’un 3. maddesine göre içerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür. 5651 Madde 5. Ticari veya ekonomik amaçlı içerik sağlayıcıları, yer sağlayıcıları ve erişim sağlayıcıları, gerçek kişi ise adı ve soyadı, tüzel kişi ise unvanı ve sorumlu kişiler, vergi kimlik numarası veya ticaret sicil numarasını, yerleşim yeri, tüzelkişi ise merkezinin bulunduğu yeri, elektronik iletişim adresi ve telefon numarasını, sunduğu hizmet, bir merciin iznine veya denetimine tabi bir faaliyet çerçevesinde yapılıyor ise, yetkili denetim merciine ilişkin bilgileri, kendilerine ait internet ortamında, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve iletişim başlığı altında, doğru, eksiksiz ve güncel olarak bulundurmakla yükümlüdür. Kanun’un 4 ve devamı maddeleri içerik, yer ve erişim sağlayıcılarının sorumluluklarını düzenlemektedir. İçerik sağlayıcı (m. 2/f), internet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur. İçerik sağlayıcı, Kurum’un bu kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Kuruma teslim eder ve Kurum tarafından bildirilen tedbirleri alır Yer sağlayıcı (m. 2/m), yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanun’un 8. ve 9. maddelerine göre haberdar edilmesi halinde yayından çıkarmakla yükümlüdür. Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla (İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik’in 7. maddesine göre altı ay) ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. Yer sağlayıcı, Kurum’un talep ettiği bilgileri talep edilen şekilde Kurum’a teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla yükümlüdür (md. 5). Erişim sağlayıcı (m. 2/e), kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir. Buna karşın erişim sağlayıcı herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde erişimi engellemekle; sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla (İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik’in 8. maddesine göre bir yıl) ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla; faaliyetine son vereceği tarihten en az üç ay önce durumu Kurum’a, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usullere uygun olarak Kurum’a teslim etmekle; erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla; Kurum’un talep ettiği bilgileri talep edilen şekilde Kurum’a teslim etmekle ve Kurum tarafından bildirilen tedbirleri almakla, yükümlüdür (md. 6). Kanun’un 7. maddesi klasik anlamda bir internet süjesi olmayan ticari amaçla toplu kullanım sağlayıcılarını (örneğin internet kafeleri) düzenlemektedir. Bu hükme göre bunlar, mahalli mülki amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahalli mülki amir tarafından Kurum’a bildirilir. Ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında belirlenen tedbirleri almakla yükümlüdür. Ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında tedbirleri almakla yükümlüdür. Kanun 8 ve devamı maddelerinde ise 4 farklı kapsamda erişimin engellenmesini düzenlemektedir.

1. Koruma tedbiri olarak öngörülen erişimin engellenmesi
2. Önleme amaçlı olarak erişimin engellenmesi
3. Kişilik haklarının internet yoluyla ihlaline bağlı olarak ilgililerin başvurusu üzerine erişimin engellenmesi
4. Özel hayatın gizliliğinin ihlaline yönelik yayınların erişiminin engellenmesi

Koruma tedbiri olarak öngörülen erişimin engellenmesi 8. maddede düzenlenmiştir. Buna göre internet ortamında yapılan ve içeriği katalog suçlardan birini 5237 Sy Türk Ceza Kanununda düzenlenmiş olan intihara yönlendirme (md. 84), çocukların cinsel istismarı (md. 103/1), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (md. 190), sağlık için tehlikeli madde temini (md. 194), müstehcenlik (md. 226), fuhuş (md. 227), kumar oynanması için yer ve imkân sağlama (md. 228) suçları ve 25.7.1951 tarihli ve 5816 Sy Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlardırı oluşturduğu yönünde yeterli şüphe bulunan bir internet sitesine erişim, hakim veya mahkeme tarafından engellenebilir. 5651 Sy Kanunun 8.maddesinin 4. fıkrasında erişimin engellenmesi Kararı için aranan şartların var olduğu takdirde, idari bir makam tarafından da yerine getirilebileceği hüküm altına alınmıştır. İnternet yayını katalog halinde sunulan suçlardan birini oluşturduğu ve ilgili yayının içerik veya yer sağlayıcısı yurt dışında bulunması durumunda veyahut yer sağlayıcısı yurt içinde bulunsa bile, internet yayını çocukların cinsel istismarı, müstehcenlik veya fuhuş suçlarını oluşturduğu durumlarında, erişimin engellenmesi kararı re ’sen Bilgi Teknolojileri ve İletişim Kurumu Başkanı tarafından verilmektedir. Alınan karar erişim sağlayıcısına kendisinden gereğini yapmasını istenmesi koşuluyla bildirilir. Buna idari tedbir olarak erişimin engellenmesi de denilmektedir. Önleme amaçlı olarak erişimin engellenmesi ise 8/A maddesinde düzenlenmiştir. Bu hükme göre yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hakim veya gecikmesinde sakınca bulunan hallerde, Başbakanlık veya milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından internet ortamında yer alan yayınla ilgili olarak erişimin engellenmesi kararı verilebilir. Başbakanlık veya ilgili Bakanlıkların talebi üzerine Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkan tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hakim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. Kanun’un 9. maddesine göre internet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişilerle kurum ve kuruluşlar, içerik sağlayıcısına ve/veya yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hakimine başvurarak içeriğe erişimin engel lenmesini de isteyebilir. İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda Hakim erişimin engellenmesine karar verebilir. Hakim zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar vermez, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak verir. Ancak hâkim bunun mümkün olmaması halinde internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir. Özel hayatın gizliliğinin ihlaline yönelik yayınların erişiminin engellenmesi ise Kanun’un 9/A maddesinde yer almaktadır. İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir. Kanun erişimin engellenmesi kararının yerine getirilmesi için de bazı düzenlemeler öngörmüştür. Kanun’un 6/A maddesi ile Erişim Sağlayıcıları Birliği kurulmuştur. Birlik özel hukuk tüzel kişiliğini haizdir. Birliğin merkezi Ankara’dır. Birliğin gelirleri, üyeleri tarafından ödenecek ücretlerden oluşur. Ücret, Birliğin giderlerini karşılayacak miktarda belirlenir. Birliğe üye olmayan internet servis sağlayıcıları faaliyette bulunamaz.

Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilen koruma tedbiri olarak öngörülen erişimin engellenmesi kararları hariç olmak üzere, diğer erişimin engellenmesi kararları erişim sağlayıcılar tarafından yerine getirilir. Kararların uygulanması amacıyla gerekli her türlü donanım ve yazılım erişim sağlayıcıların kendileri tarafından sağlanır. Erişim engellenme kararları Birliğe gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır. Kanun’un 10. maddesi Bilgi Teknolojileri ve İletişim Kurumu’nun görev ve yetkilerini düzenlemiştir. ***5651 sayılı Kanun’a 671 sayılı Kanun Hükmünde Kararname (KHK) ile eklenen ek madde 3 ile Telekomünikasyon İletişim Başkanlığı (TİB) 2016 Yılında kapatılmıştır.*** Diğer mevzuatta Telekomünikasyon İletişim Başkanlığına yapılan atıflar Bilgi Teknolojileri ve İletişim Kurumuna, Telekomünikasyon İletişim Başkanına yapılan atıflar Bilgi Teknolojileri ve İletişim Kurumu Başkanına yapılmış sayılır.

**5369 Sayılı Evrensel Hizmet Kanunu**

Kanun’un 1. maddesine göre, Amac; Kamu hizmeti niteliğini haiz, ancak işletmeciler tarafından karşılanmasında mali güçlük bulunan evrensel hizmetin sağlanması, yürütülmesi ve elektronik haberleşme sektörü ile bu Kanun kapsamında belirlenen diğer alanlarda evrensel hizmet yükümlülüğünün yerine getirilmesine ilişkin usul ve esasları belirlemektir.

**Bilişim Hukuku:**

Kanun’un 2. maddesinde tanımlar başlığı altında yasada yer alan bazı kavramların tanımlarına yer verilmiştir.

**Bakanlık:** Ulaştırma, Denizcilik ve Haberleşme Bakanlığını,

**Kurum:** Bilgi Teknolojileri ve İletişim Kurumunu,

**Elektronik haberleşme:** İşaret, sembol, ses, görüntü ve elektrik işaretlerine dönüştürülebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını,

**Evrensel hizmet:** Türkiye Cumhuriyeti sınırları içinde coğrafi konumlarından bağımsız olarak herkes tarafından erişilebilir, önceden belirlenmiş kalitede ve herkesin karşılayabileceği makul bir bedel karşılığında asgari standartlarda sunulacak olan, internet erişimi de dahil elektronik haberleşme hizmetleri ile bu Kanun kapsamında belirlenecek olan diğer hizmetleri,

**Evrensel hizmet yükümlüsü:** Elektronik haberleşme sektöründe, ilgili mevzuatına göre Kurumca yetkilendirilmiş ve bu Kanun kapsamındaki hizmetleri sağlamakla yükümlü kılınan işletmeciyi,

**Evrensel hizmetin net maliyeti:** Bir işletmecinin, evrensel hizmet yükümlülüğünün gereklerini yerine getirmek için sağladığı durum ile hiç yükümlü olmasaydı içinde bulunacağı durum arasındaki net maliyet farkını,

**İşletmeci:** İlgili mevzuatına göre Kurumca veya bu Kanun kapsamına alınmış hizmetler bakımından ilgili diğer mercilerce yetkilendirilmiş olan işletmecileri,

**Alt yapı:** Evrensel hizmetin sağlanmasını temînen hizmetin verilebilmesi için gerektiğinde öncelikle fiziki ortamın oluşturulmasına yönelik her türlü teçhizat, ekipman, bilgisayar, yazılım ve donanımı ifade eder.

Kanun’un 3. maddesinde ise evrensel hizmetin sağlanmasında ve bu hususta yapılacak düzenlemelerde hangi ilkelerin göz önüne alınacağı belirtilmiştir.

a. Evrensel hizmetten, Türkiye Cumhuriyeti sınırları içerisinde yaşayan herkes, bölge ve yaşadığı yer ayırımı gözetilmeksizin yararlanır.

b. Evrensel hizmet, fert başına gayrisafi yurt içi hasıla tutarı da göz önünde bulundurularak karşılanabilir ve makul fiyat seviyesinde sunulur.

c. Düşük gelirliler, engelliler ve sosyal desteğe ihtiyacı olan grupların da evrensel hizmetten yararlanabilmesi için uygun fiyatlandırma ve teknoloji seçeneklerinin uygulanabilmesine yönelik tedbirler alınır.

d. Evrensel hizmet, önceden belirlenmiş hizmet kalitesi standartlarında sunulur.

e. Evrensel hizmetin sunulmasında ve ulaşılmasında devamlılık esastır.

**5809 sayılı Elektronik Haberleşme Kanunu**

Kanun’un 1. maddesine göre, bu yasanın amacı elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımlarınteşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesidir.

Kanun’un 2. maddesine göre elektronik haberleşme hizmetlerinin yürütülmesi ve elektronik haberleşme alt yapı ve şebekesinin tesisi ve işletilmesi ile her türlü elektronik haberleşme cihaz ve sistemlerinin imali, ithali, satışı, kurulması, işletilmesi, frekans dahil kıt kaynakların planlaması ve tahsisi ile bu konulara ilişkin düzenleme, yetkilendirme, denetleme ve uzlaştırma faaliyetlerinin yürütülmesi bu Kanun’a tabidir.

Kanun’un 3. maddesinde tanımlar başlığı altında yasada yer alan bazı kavramların tanımlarına yer verilmiştir.

**Elektronik haberleşme:** Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını,

**Elektronik haberleşme alt yapısı:** Elektronik haberleşmenin, üzerinden veya aracılığıyla gerçekleştirildiği anahtarlama ekipmanları, donanım ve yazılımlar, terminaller ve hatlarda dahil olmak üzere her türlü şebeke birimlerini, ilgili tesisleri ve bunların bütünleyici parçalarını,

**Elektronik haberleşme alt yapısı işletimi:** İlgili alt yapıya ilişkin gerekli elektronik haberleşme tesislerinin kurulması, kurdurulması, kiralanması veya herhangi bir surette temin edilmesiyle bu tesisin diğer işletmecilerin veya talep eden gerçek veya tüzel kişilerin kullanımına sunulmasını,

**Elektronik haberleşme hizmeti:** Elektronik haberleşme tanımına giren faaliyetlerin bir kısmının veya tamamının hizmet olarak sunulmasını,

**Elektronik haberleşme şebekesi:** Bir veya daha fazla nokta arasında elektronik haberleşmeyi sağlamak için bu noktalar arası bağlantıyı teşkil eden anahtarlama ekipmanları ve hatlar da dahil olmak üzere her türlü iletim sistemleri ağını,

**Elektronik haberleşme sektörü:** Elektronik haberleşme hizmeti verilmesi, elektronik haberleşme şebekesi sağlanması, elektronik haberleşme cihaz ve sistemlerine yönelik üretim, ithal, satış ve bakım-onarım hizmetlerinin yürütülmesi ile ilgili sektörü,

**Elektronik haberleşme şebekesi sağlanması:** Elektronik haberleşme şebekesi kurulması, işletilmesi, kullanıma sunulması ve kontrolünü,

**Elektronik kimlik bilgisi:** Elektronik haberleşme cihazlarına tek ve benzersiz olarak tahsis edilmiş kimlik tanımını,

**Erişim:** Bu Kanunda belirtilen koşullarla, elektronik haberleşme şebekesi, alt yapısı ve/veya hizmetlerinin, diğer işletmecilere sunulmasını,

**Erişim yükümlüsü:** Erişim sağlama yükümlülüğü getirilen işletmeciyi,

**İnternet alan adı:** İnternet üzerinde bulunan bilgisayar veya internet sitelerinin adresini belirlemek için kullanılan internet protokol numarasını tanımlayan adları,

**İnternet alan adı sistemi:** Okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simge sel isimlerle yapılan adreslemede, karşılığı olan internet protokolü numarasını bulan ve kullanıcıya veren sistemi ifade eder.

Kanun’un 4. maddesine göre her türlü elektronik haberleşme cihaz, sistem ve şebekelerinin kurulması ve işletilmesine müsaade edilmesi, gerekli frekans, numara, uydu pozisyonu ve benzeri kaynak tahsislerinin yapılması ile bunların düzenlenmesi Devletin yetki ve sorumluluğu altındadır. İlgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde aşağıdaki ilkeler göz önüne alınır

a. Serbest ve etkin rekabet ortamının sağlanması ve korunması.

b. Tüketici hak ve menfaatlerinin gözetilmesi.

c. Kalkınma planları ve Hükümet programlarındaki hedefler ile Bakanlık tarafından belirlenen strateji ve politikaların gözetilmesi.

ç. Herkesin, makul bir ücret karşılığında elektronik haberleşme şebeke ve hizmetlerinden yararlanmasını sağlayacak uygulamaların teşvik edilmesi.

d. Aksini gerektiren objektif nedenler bulunmadıkça veya toplumdaki ihtiyaç sahibi kesimlere özel, kapsamı açık ve sınırları belirlenmiş kolaylıklar sağlanması halleri dışında, eşit şartlardaki aboneler, kullanıcılar ve işletmeciler arasında ayrım gözetilmemesi ve hizmetlerin benzer konumdaki kişiler tarafından eşit şartlarla ulaşılabilir olması.

e. Bu Kanunda aksi belirtilmedikçe ya da objektif nedenler aksini gerektirmedikçe, niteliksel ve niceliksel devamlılık, düzenlilik, güvenilirlik, verimlilik, açıklık, şeffaflık ve kaynakların verimli kullanılmasının gözetilmesi.

f. Elektronik haberleşme sistemlerinin uluslararası normlara uygun olması.

g. Teknolojik yeniliklerin uygulanması ile araştırma-geliştirme faaliyet ve yatırımlarının teşvik edilmesi.

ğ. Hizmet kalitesi artırımının teşvik edilmesi.

h. Milli güvenlik ile kamu düzeni gereklerin eve acil durum ihtiyaçlarına öncelik verilmesi.

ı. Bu Kanunda, ilgili mevzuatta ve yetkilendirmelerde açıkça belirlenen durumlar haricinde, işletmecilerin, ara bağlantı da dahil olmak üzere erişim ücretleri ile hat ve devre kiralarını da kapsayacak biçimde, elektronik haberleşme hizmeti sunulması karşılığı alacakları ücretleri serbestçe belirlemesi.

i. Elektronik haberleşme cihaz ve sistemlerinin kurulması, kullanılması ve işletilmesinde insan sağlığı, can ve mal güvenliği, çevre ve tüketicinin korunması açısından asgarî uluslararası normların dikkate alınması.

j. Elektronik haberleşme hizmetlerinin sunulmasında ve bu hususlarda yapılacak düzenlemelerde tarafsızlığın sağlanması.

k. Teknolojik yeniliklerin kullanılması da dahil olmak üzere engelli, yaşlı ve sosyal açıdan korunmaya muhtaç diğer kesimlerin özel ihtiyaçlarının dikkate alınması.

l. Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi.

Kanun, 5 ve 6. maddelerinde bu ilkeler ışığında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı’na ve Bilgi Teknolojileri ve İletişim Kurumu’na çeşitli görevler ve yetkiler vermekte; sonraki maddelerde ise bu görev ve yetkileri somutlaştırmaktadır.

**BİLİŞİM, BİLİŞİM SİSTEMLERİ VE İNTERNET**

**Bilişim**

Bilgi ve iletişim sözcüklerinin bir araya getirilerek kullanılmasıyla ortaya çıkan “bilişim” terimi, Türk Dil Kurumu’nca “*insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi*” olarak tanımlamıştır. Bilişim terimi “enformasyon” ve “otomasyon” kelimelerinin bir araya getirilmesinden türetilmiş olan Fransızca kökenli “enformatik” terimine karşılık gelmektedir ve genel olarak enformasyonun otomatik makineler aracılığıyla işlenmesi anlamında kullanılmıştır.

Bilgisayar ve bilişim sözcükleri zaman zaman birbirleri yerine kullanıla gelmişlerdir. Fakat her ikisi de farklı anlamlara sahiptirler. Zira bilişim bir bilim dalını, bilgisayar ise ana işlemci, salt okunur bellek, rasgele erişilen bellek, çevre giriş çıkış birimleri, işletim yazılımı ve uygulama yazılımı gibi donanımlardan oluşan bir makineyi ifade eder. Bilgisayar, kullanıcılardan aldığı bilgi ve komutlarla aritmetik ve mantıksal işlemleri yapabilen ve yaptığı işlemlerin sonuçlarını saklayabilen, saklanan bilgilere istenildiğinde ulaşılabilen elektronik bir makinedir. Bu bilgilere genel olarak “veri ”adı verilmektedir. Veri, bilgisayar tarafından üzerinde işlem yapılan her türlü değeri ifade etmektedir. Bir bilgisayarda ya da bilgisayarlar tarafından okunabilen araçlarda saklanabilen, üzerinde işlem yapılabilen her şey veridir. Bu saklama ve sonradan okuma işlemini yapabilmek için verilerin uygun şekilde sayısal kodlara dönüştürülmesine ve gerektiğinde eski haline getirilip okunabilmesine yardımcı olacak alfabeye de “yazılım dili” denilmektedir. Bilgisayar, her türlü bilgiyi veri denilen sayısal kodlar aracılığıyla işleyen ve yazılım diliyle bunu kullanıcılara aktaran makinedir. Bilişim sözcüğü ise bilgisayara göre daha üst bir kavramı ifade etmek için kullanılmaktadır. Bilişim hem verilerin işlenmesini, yani “bilgi işlemi”, hem de bilgi işlemin sonucunun aktarılmasını, yani “veri iletişimini” ifade eden bir kavramdır. Teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması kavram olarak bilişimin konusudur. Dolayısıyla her bilgisayarın bir bilişim sistemi olduğu ancak herhangi bir bilişim sisteminin zorunlu olarak bir bilgisayar olmadığı kabul edilmelidir.

**İnternetin Tanımı**

İnternet kelimesi, “interconnected networks”(kendi aralarında bağlantılı ağlar) kelimesinin kısaltması olarak kullanılmaktadır. İnternet, kişilerin dünya üzerinde birbirleri ile çok geniş amaç ve içerikte iletişim kurmalarını, bilgi alışverişinde bulunmalarını sağlayan ortak iletişimin adıdır. İnternet birden fazla haberleşme ağının birlikte meydana getirdiği metin, resim, müzik, grafik, yazılı metin gibi dosyalar ile bilgisayarlar yazılımlarının, kısacası insanlar tarafından oluşturulmuş her türlü bilginin veri halinde paylaşıldığı ve iletildiği bilişim sistemleri arasındaki ağ olarak tanımlanabilir. Diğer bir ifadeyle internet, birden fazla haberleşme ağının, birlikte meydana getirdikleri bir haberleşme ağıdır. İnternete merkezi olmayan, küresel seviyede planlanmış, hiyerarşik bir yapısı bulunmayan “ağlar arası ağ” da denilmektedir.

**İnternetin Teknik Alt Yapısı**

**Backbone:** İnternet üzerindeki veri iletişimi omurga olarak adlandırılan ana iletişim hatları üzerinden sağlanır. Bu ana hatlardan çıkan veri iletişim hatları ile çeşitli merkezlere giderler ve oradan da dağılarak tek tek bilgisayarlara ulaşırlar. İnternet üzerindeki ilk omurga, Amerika’da ARPANET tarafından kurulmuştur. İnternetin ortaya çıkışının ilk yıllarında bu omurgalar kamusal kuruluşlar tarafından yapılmaktaysa da, bu yapıların kurulması bugün için özel sektör tarafından sağlanmaktadır.

**TCP/IP Protokolü:** Bilişim sistemlerinin birbirleriyle iletişim kurabilmeleri ve veri aktarımında bulunabilmeleri için birtakım kurallara uygun hareket etmeleri gerekir. Bu kurallar, iletişimdeki eşler arasında veri trafiğinin kurallarını oluşturup daha etkin bir iletişim sağlanmasını gerçekleştirirler. Bu kurallara, TCP/IP (Transmission Control Protocol/Internet Protocol) protokoller ailesi denir. Bu protokoller birbirleriyle iletişim kuran bir ağda yer alan farklı yapıdaki bilgisayarların birbirleriyle iletişim kurabilmeleri için oluşturulan bir anlaşma dilidir. IP adresi, internetin teknik alt yapısını kuran internet servis sağlayıcıları tarafından internet kullanıcılarına verilen kimlik numarasıdır. Bunlar 0 ile 255 sayıları arasında değişen, onluk (decimal) formatta gösterilen sayılardır (örneğin 155.212.56.73). IP adresleri “dinamik” ve “statik” olmak üzere ikiye ayrılır. İnternet servis sağlayıcısı (ISS) tarafından internete bağlanmak isteyen bilgisayara geçici olarak atanan IP adresleri dinamiktir. Statik IP adresleri ise, değişmeyen adreslerdir. Sunucu bilgisayarda statik IP kullanılır. Bu nedenle genellikle bir web sayfasının statik IP’si bulunurken, bu sayfayı ziyaret eden son kullanıcının internete bağlanırken kullandığı IP dinamiktir. DNS (Domain Name System/alan adı sistemi) de bir TCP/IP servis protokolüdür. DNS bu alan adı adreslerini kişilerin anlayabileceği hale getirir. Örn. tarayıcıya anadolu.edu.tr yazıldığında aslında bir IP adresine bağlanılır. DNS, kolay anlaşılabilir ve kullanılabilir makine ve alan isimleri ile makine IP adresleri arasında çift taraflı dönüşümü sağlar. IP adreslerinin gündelik hayatta kullanımı ve hatırlanması pek pratik olmadığı için domain isimlendirme sistemi kullanılır. Zira bir internet adresine 4 haneli bir numara karşılık gelir, a.b.c.d şeklindeki bu numaralara IP numaraları denir. Burada, a,b,c ve d 0-255 arasında değişen bir tam sayıdır. DNS sistemi isim sunucuları ve çözümleyicilerinden oluşur. Örn. Google’a bağlanmak istediklerinde Google’ın şu anda internetteki adresi olan

74.125.224.83 adresini tarayıcılarına yazmalarına gerek kalmaz. Bunun yerine tarayıcısına [www.google.com](http://www.google.com) yazar ve DNS sunucusu, onu bu IP adresine yönlendirir. DNS kavramı ile yakından ilintili olan “alan adı” (domain name) kavramı İnternet adresleri, IP ve alan adı denilen kısaltmalardan meydana gelmektedir (örneğin şirket adı). Alan adları ülkelere göre ayrılır (ccTLD/country code top level domain). Adreslerin sonundaki tr, de, uk gibi ifadeler adresin bulunduğu ülkeyi gösterir. Örneğin tr Türkiye’yi de Almanya’yı, uk İngiltere’yi gösterir. ABD adresleri için bir ülke takısı kullanılmaz. Bunun nedeni DNS ve benzeri uygulamaları oluşturan ülke ABD’dir. İnternet adresleri ülkelere ayrıldıktan sonra .com, .edu, .gov, .biz, .tv, .org gibi daha alt bölüme ayrılırlar. (gTLD/generik top level doma- in). Böylece alan isimleri bir yandan .com, .net gibi birinci derece alan isimlerinden (TLD) diğer yandan kişilerin sanal adresini oluşturan ikinci derece alan isimlerinden (SLD/second level domain) oluşan ve son kullanıcılara bir anlam ifade eden internet adresinin adıdır. TLD ve SLD’den oluşan ifadeler DNS de üst düzey (top-level) domainlere karşılık gelir

**World Wide Web (www):** Sözcük anlamı olarak dünyayı saran ağ anlamına gelen world wide web’e kısaca web denilmektedir. Web, dünyanın her yerindeki yüzbinlerce sunucuda kayıtlı, milyarlarca dosyadan oluşan bir bütündür. Birçok internet hizmetini birleştiren bir araç olarak; yazı, resim, ses, video, animasyon gibi pek çok farklı nitelikteki verilere etkileşimli olarak ulaşmamızı sağlayan çoklu bir hiper ortam sistemidir. Hiper ortam, bir dokümandan başka bir dokümanın çağırılmasına imkân verir (iç içe dokümanlar). Bu ortamdaki her veri, bir fare (mouse) yardımıyla başka bir veriyi çağırabilir. Buna “hiper link” yada kısaca “link” denir. Link, aynı doküman (aynı internet sayfası/web sayfası) içinde başka bir yerde olabildiği gibi, fiziksel olarak başka bir yerde de (internet üzerindeki herhangi bir makinada ya da başka bir web sayfasında) olabilir. Bütün bu farklı yapıdaki veriler uygun bir standart ile bir arada kullanılıp bir “web tarayıcısında” (web browser) görüntülenebilir. Bir Macintosh (Mac), PC ya da Unix Web web sayfalarını aynı şekilde alırlar. Kısacası web açık bir sistemdir; platform, bilgisayar, işletim sistemi vb. ile bağımlı değildir. Web üzerinden pek çok bilgi kaynağına kolayca erişilebilir. Web uygulamaları geliştirmek ve bunları kullanıma sunmak çok kolaydır. Bu anlatımlardan anlaşılacağı üzere web, web browser (web tarayıcısı/ağ tarayıcısı) olarak adlandırılan ve internet üzerinde web sayfalarında yer alan tüm bilgilere bakabilmek ve bu bilgilerle etkileşim halinde olabilme imkanı veren bir uygulama programı (örneğin Microsoft İnternet Explorer, Mozilla, Firefox, ve Safari) ve web sayfası ya da web sitesi olarak adlandırılan, istenilen verilerin görüntülenmesini sağlayan ve HTML (HyperTextMarkup Language) adı verilen işaretleme dili kullanılarak oluşturulan uygulama yazılımlarının bir araya gelmesinden oluşmaktadır.

**İnternetin Tarihçesi**

İnternetin ortaya çıkışı soğuk savaş döneminde ABD ve Sovyetler Birliği arasında yaşanan rekabete dayanmaktadır. Sovyetler Birliği’nin, 1957 yılında Sputnik uydusunu uzaya göndermesinden sonra ABD’de bulunan ve Amerikalıların “think-tank” olarak adlandırdıkları askeri ve politik strateji geliştirme düşünce kuruluşu RAND Corporation tarafından tek bilgisayardan bağımsız olarak çalışabilen bir ağ kurma fikri ulusal güvenlik gerekçesiyle ortaya atılmıştır. Bunun üzerine ABD Hükümeti olası bir savaş durumunda hem ülke yöneticilerinin birbirleriyle hem de askeri kaynakların kendileriyle iletişimlerinin güvenli ve kesintisiz bir biçimde devamını sağlayacak olan bir ağ sisteminin oluşturulması için harekete geçmiştir. Bunun için de Savunma Bakanlığı’na bağlı olan ve birbirinden uzakta olan bazı askeri birliklerin geliştirdiği projelerin ortak bir ağ üzerinden birleştirilmesi temeline dayanan ARPA (Advanced Research Project Agency) adlı bir birim oluşturulmuştur. Buradaki çalışmalar sonucunda da farklı sistemleri birbirine bağlamak için ARPANET adlı bir askeri bilgisayar ağı kurulmuştur. Bu sistemden önce ordu daha sonra da üniversiteler faydalanmıştır. 1980 yılında ARPANET’in yalnızca askeri birlikler için kullanılmasından vazgeçilmiş ve sistem sivil kuruluşlarında kullanımına sunulmuştur. İlerleyen zamanlarda web teknolojisinin ve bunun dayandığı en temel dosya transfer protokolü olan http protokolünün geliştirilmesiyle ARPANET tamamen ortadan kalkmış ve bilinen anlamda internet ortaya çıkmıştır. Türkiye’de ilk internet bağlantısını **12 Nisan 1993** tarihinde Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) destekli bir proje ile Orta Doğu Teknik Üniversitesi (ODTÜ) gerçekleştirmiştir.

**İnternetin Yönetimi**

İnternet ağının tamamını kontrol eden tek bir yetkili otorite yoktur. Ancak bu durum, internetin küresel ağ niteliğinin korunabilmesi için bazı politikaların merkezi bir sistemden yürütülmediği anlamına da gelmez. Gerçekten de temel internet mekanizmalarının yönetimi ve düzenlenmesi için küresel düzeyde ticari kaygı gütmeyen bazı kurumlar bulunmaktadır. Bunlardan ilki internetin yönetim ve gelişme politikalarını belirleyen Internet Corporation for Assigned Names and Numbers (ICANN/İnternet Tahsisli Sayılar ve İsimler Kurumu) kurumudur. ICANN 1998 yılında kurulmuştur ve merkezi Marina Del Rey, Kaliforniya’dadır. ICANN, internet ağının yaygınlaşmasıyla birlikte alan adı sisteminin özelleştirilmesi için özerk olarak faaliyet göstermek üzere ABD tarafından yetkilendirilmiştir. ICANN, alan adları sisteminin teknik yönetimi, protokol parametrelerinin belirlenmesi ve kök sunucu sistemi yönetimi işlevlerini koordine etmekle görevlendirilmiştir. Daha teknik bir ifadeyle bu Kurum, IP tahsisi, protokol tanıtıcı ataması, genel (gTLD) ve ülke kodu (ccTLD) üst düzey alan ismi sistemi yönetimi ve kök sunucu sistemi yönetimi işlevlerinden sorumludur. ICANN, tüm İnternet kullanıcılarının geçerli adresler bulabilmelerini sağlamak üzere evrensel çözüle bilirlikten emin olunması için DNS’in teknik unsurlarının yönetiminin koordinasyonundan da sorumludur. Teknik tanıtıcıların dağıtımını ve üst düzey alan isimlerinin (.com, .info, aero, .biz, .coop, museum, .name, pro, gov. vb.) kullanılma yetkilerinin dağıtılmasını gözlemleyerek yapar. Mali işlemler, internet içeriğinin kontrolü, istenmeyen ticari e-postaları (spam) ve veri korumasıyla ilgili kurallar gibi internet kullanıcılarını ilgilendiren diğer sorunlar, ICANN’ın teknik koordinasyon görevinin dışında kalmaktadır. Diğer bir kurum Internet Assigned Numbers Authority (IANA/İnternet Tahsisli Sayılar Otoritesi kurumudur. Bu kurum ICANN ile koordinasyon içerisinde IP adreslerinin yönetimini gerçekleştirmek amacıyla ABD tarafından yetkilen dirilmiştir. IANA’nın yetkisi, IP yönetimi için politikalar belirlemekten ziyade ICANN tarafından önceden belirlenmiş politikaları tarafsız biçimde uygulamaktan ibarettir. Her iki kurumun altında dünyanın beş bölgesi için internet kaynaklarını ICANN’nın belirlediği politikalara göre yöneten kuruluşlar vardır. Bunlara Regional Internet Registry (RIR/Bölgesel Internet Kayıt Merkezi) denir. Bu kuruluşlar ticari amaç gütmez ve hükümetlerin organı değildir. Dünyada 5 adet RIR bölgesi bulunmaktadır.

1-Afrika bölgesi için AfriNIC (African Region Internet Registry),

2-Asya ve Pasifik bölgesi için APNIC (Asia Pacific Network Information Centre),

3-Kuzey Amerika için ARIN (American Registry for Internet Numbers),

4-Latin Amerika ve Karayipler bölgesi için LACNIC (Latin America and Caraibbean Adresses Registry)

5-Avrupa Bölgesi RIPE NCC (Réseaux IP Europens NetworkCoordination Centre).

Türkiye RIPE NCC bölgesindedir. RIPE NCC’nin merkezi Hollanda’dadır. RIR merkezleri altında son kullanıcıya IP adresi veren internet servis sağlayıcıları vardır. Bunlara Local Internet Registry (LIR/Yerel Internet Kayıt Merkezi) denilir. İsteyen her kişi, şirket veya kuruluş LIR olabilir. Bunun için giriş aidatı ve yıllık servis ücreti ödemek gerekir. LIR olan her kişi veya kurum, RIR toplantı larına katılabilir, politikaları için önerilerde bulunabilir. Genel olarak internetin teknik alt yapısını ve internet servis sağlayıcısı olarak adlandırılan her gerçek veya tüzel kişi LIR’dir. Örn: TürkTelekom bir LIR’dır.

Bunların dışında internet trafiğini düzenleyen ve ICANN tarafından akredite edilen kurumlarca yönetilen on üç adet kök sunucu bulunmaktadır. Ayrıca Internet Engineering Task Force, Internet Research Task Force, Internet Society, World Wide Web Consortium gibi kurumlarda internet ile ilgili temel politikaların belirlenmesinde yardımcı olmakta ve bu alanda araştırma geliştirme (ar-ge) çalışmaları sürdürmektedir. İnternet üzerindeki ABD yetkisinin kırılması için ise çeşitli zamanlarda girişimler olmuştur. Buna neden olarak ABD’nin ulusal güvenlik tanımını diğer birçok ülkeye göre farklı tanımlaması ve bundan dolayı ABD’nin zaman zaman interneti top yekûn denetlemek için girişimlerde bulunmasıdır. Örneğin ABD 2000 yılında Federal Bureau of Investigation’ın (FBI) kullanımına “Carnivore” adlı bir sistemi sunmuş ve böylece bireylerin internet iletişimini denetlemeye başlamıştır. Sistem, bireylerin özel yaşamına ve iletişim özgürlüğüne müdahale ettiği gerekçesiyle ABD’de çok tartışılmış ve tepkiler üzerine FBI bu sistemden vazgeçme durumunda kalmıştır. İnternetin devlet kurumlarınca denetlenmesi ve gözetlenmesi amacıyla ortaya atılan diğer bir proje ise “Echelon” projesidir. Bu proje, ABD, Kanada, İngiltere, Avusturalya ve Yeni Zelanda tarafından ortaya atılmış olan ve dünyadaki iletişimin denetlenmesini amaçlayan, varlığını ABD’nin kabul etmediği, buna karşın Avusturalya ve Yeni Zelanda Hükümetlerinin varlığını doğruladığı bir projedir. Sistem aracılığıyla telefon, cep telefonu, e-posta, faks, telefaks gibi veri iletim ağlarıyla yapılan iletişimin tümünün denetlenebilmesi mümkündür. Sistemin dakikada 2 milyon, günde ise 3 milyar telefon görüşmesini denetleyebildiği belirtilmektedir. Veriler, düzenli olarak toplanmakta ve “dictionary” (sözlük) adı verilen şifreleme sisteminden geçirilerek; uzmanlar tarafından anahtar sözcükler yardımıyla izlenmektedir. İşte bu gelişmelere tepki olarak da 2005 yılında Tunus’ta gerçekleştirilen Dünya Bilgi Toplumu Zirvesi’nde Avrupa Birliği temsilcileri ICANN’ın yetkilerinin Birleşmiş Milletler çatısı altında faaliyet gösterecek bir uzmanlar kuruluna devredilmesini istemişlerdir. ABD ise bu teklifi kabul etmemiş ve mevcut tepkileri dindirmek için devletlerin internetle ile ilgili görüşlerini doğrudan beyan edebilecekleri Internet Governance Forum adlı uluslararası platformu faaliyete sokacağını belirtmekle yetinmiştir. Ancak bütün bu gelişmelerden sonra NSA Skandalı patlak vermiştir. Edward Snowden tarafından 2013 yılında ortaya konan belgelere göre ABD Ulusal Güvenlik Ajansı (National Security Agency/NSA) başta Google, Facebook, Apple ve diğer büyük internet aktörlerinin kullanıcılarının pek çok kişisel verisini geniş kapsamlı ve derinlikli gözetimlere tabi tutmuştur.

**TÜRKİYE’DE İNTERNETİN YÖNETİMİNDE YER ALAN YETKİLİ VE SORUMLU KURUMLAR**

**Ulaştırma, Denizcilik ve Haberleşme Bakanlığı**

655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname’ye göre haberleşme hizmetlerinin geliştirilmesi, kurulması, kurdurulması, işletilmesi ve işlettirilmesi hususlarında, ilgili kurum ve kuruluşlarla koordinasyon içerisinde, milli politika, strateji ve hedefleri belirlemek ve uygulamak, gerektiğinde güncellemek; evrensel hizmet politikalarını ilgili kanunların hükümleri dahilinde ülkenin sosyal, kültürel, ekonomik ve teknolojik şartlarına göre belirlemek, evrensel hizmetin yürütülmesini sağlayacak esasları tespit etmek, uygulanmasını takip etmek ve net maliyetiyle ilgili hesapları onaylamak; bilgi toplumu politika, hedef ve stratejileri çerçevesinde ilgili kamu kurum ve kuruluşlarıyla gerekli işbirliği ve koordinasyo nu sağlayarak e-Devlet hizmetlerinin kapsamı ve yürütülmesine ilişkin usul ve esasları belirlemek, bu hizmetlere ilişkin eylem planları yapmak, koordinasyon ve izleme faaliyetlerini yürütmek, gerekli düzenlemeleri yapmak ve bu kapsamda ilgili faaliyetleri koordine etmek; haberleşme, posta, havacılık ve uzay teknolojileri iş ve hizmetlerinin gerektirdiği uluslararası ilişkileri yürütmek, anlaşmalar yapmak ve bu alanlarda uluslararası mevzuatın gerektirmesi halinde mevzuat uyumunu sağlamak görevleri bakanlık tarafından yerine getirilecektir (md. 2). Bu kapsamda Bakanlık teşkilatında Haberleşme Genel Müdürlüğü kurulmuştur (md. 13). Yine 5809 sayılı Elektronik Haberleşme Kanunu md. 5, Bakanlığın elektronik haberleşme sektörü ile ilgili görev ve yetkilerini belirtmiştir

a. Numaralandırma, internet alan adları, uydu pozisyonu, frekans tahsisi gibi kıt kaynaklara dayalı elektronik haberleşme hizmetlerine ilişkin strateji ve politikaları belirlemek.

b. Elektronik haberleşme sektörünün serbest rekabet ortamında gelişimini teşvik etmeye ve bilgi toplumuna dönüşümün desteklenmesini sağlamaya yönelik hedef, ilke ve politikaları belirlemek ve bu amaçla teşvik edici tedbirleri almak.

c. Elektronik haberleşme alt yapı, şebeke ve hizmetlerinin teknik, ekonomik ve sosyal ihtiyaçlara, kamu yararına ve milli güvenlik amaçlarına uygun olarak kurulması, geliştirilmesi ve birbirlerini tamamlayıcı şekilde yürütülmesini sağlamaya yönelik politikaları belirlemek.

ç. Elektronik haberleşme cihazları sanayisinin gelişmesine ilişkin politikaların oluşumuna ve elektronik haberleşme cihazları bakımından yerli üretimi özendirici tedbirleri almaya yönelik politikaları belirlemeye katkıda bulunmak.

d. Ülkemizin üyesi bulunduğu elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşlar nezdinde 5.5.1969 tarihli ve 1173 sayılı Milletlerarası Münasebetlerin Yürütülmesi ve Koordinasyonu Hakkında Kanun hükümleri saklı kalmak üzere Devleti temsil etmek veya temsile yetkilendirmek, çalışmalara katılım ve kararların uygulanması konusunda koordinasyonu sağlamak.

e. Elektronik haberleşme politikalarının tespiti ve uygulanması amacıyla gerekli araştırmaları yapmak ve yaptırmak.

f. Elektronik haberleşmenin doğal afetler ve olağanüstü haller nedeniyle aksamamasını temînen gerekli tedbirleri almak ve koordinasyonu sağlamak. Haberleşmenin aksaması riskine karşı önceden haberleşmenin kesintisiz bir biçimde sağlanmasına yönelik alternatif haberleşme alt yapısını kurmak, kurdurmak ve ihtiyaç durumunda söz konusu sistemi devreye sokmak.

g. Olağanüstü hâl ve savaşta elektronik haberleşme hizmetlerini, 16.7.1965 tarihli ve 697 sayılı Kanun hükümleri dahilinde planlamak, gerekli işleri yapmak ve yaptırmak.

ğ. Elektronik haberleşme sistemlerinin yerli tasarım ve üretimini, bu amaçla sektöre ilişkin araştırma, geliştirme ve eğitim faaliyetlerini teknik ve maddi destek de dahil olmak üzere teşvik etmek.

h. Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, Siber Güvenlik Kurulunun sekretaryasını yapmak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.

ı. Ulusal kamu entegre veri merkezlerine yönelik politika, strateji ve hedefleri belirlemek, eylem planlarını hazırlamak, eylem planlarını izlemek,

e-Devlet hizmetlerinde kullanılan verilerin ve sistemlerin barındırıldığı veri merkezlerini kamu entegre veri merkezlerinde toplamak amacıyla verilerin transferi de dahil gerekli altyapıları kurmak, kurdurmak, işletmek, işlettirmek ve tüm bu faaliyetlere yönelik uygulama usul ve esaslarını belirlemek, kurulum, uygulama ve işletim süreçlerini planlamak, yürütmek ve koordine etmek.

**İnternet Geliştirme Kurulu**

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı’na bağlı olarak 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname’nin 29. maddesi uyarınca kurulan İnternet Geliştirme Kurulu’nun ana işlevi, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı’na danışmanlık yapmaktır. Kurul’un oluşumu ve yetkileri Ulaştırma, Denizcilik ve Haberleşme Bakanlığı İnternet Geliştirme Kurulu Yönetmeliği’nde düzenlenmiştir. Kurul, internet ortamı ile ilgili çalışmalarda bulunmak, araştırma, inceleme ve değerlendirme yapmak üzere Bakanlık, kurum ve kuruluş, üniversite, sivil toplum kuruluşları temsilcileri ve konuyla ilgili çalışmalarıyla temayüz etmiş kişiler arasından Bakan tarafından seçilecek toplam yedi üyeden oluşur. Kurul’un Yönetmelik md. 6’da belirtilen görevleri şunlardır:

a. İnternet ortamının ekonomik, ticari ve sosyal hayat ile bilim, eğitim ve kültür alanında etkin, yaygın, kolay erişilebilir olarak kullanımını teşvik edecek politika ve strateji önerileri hazırlamak ve Bakana sunmak.

b. Türk Kültürü, Türk Tarihi ve Türk Dünyasıyla ilgili bilgilerin internet ortamında daha fazla yer alması ve bunların tanıtılması hususunda çalışmalar yapmak, yaptırmak ve öneriler hazırlamak ve Bakana sunmak.

c. İnternet ortamının güvenli, serbest, özgür ve faydalı kullanımı ile katma değer üretmesine yönelik öneriler hazırlamak ve Bakana sunmak.

ç. İnternet kullanımının faydaları konusunda toplumsal farkındalığın oluşturulmasını sağlamak.

d. İnternete ilişkin etkinliklere katılmak, etkinliğin ve verimliliğin sağlanabilmesini teminen üniversite, kamu, özel ve sivil toplum kuruluşlarıyla iş birliği yapmak.

e. İnternet üzerinden yapılan yayınlar ve hizmetlerle ilgili olarak toplumu bilgilendirmek için yöntemler tespit etmek, yapılacak projeler hakkında görüş bildirmek ve Bakana önerilerde bulunmak.

f. Devlet uygulamalarının yaygınlaştırılması, kamu kuruluşlarının birbirleri ile olan ilişkilerinde ve vatandaşa sundukları hizmetlerde internet ortamının daha yaygın kullanımı konusunda çalışmalar yaparak önerilerde bulunmak.

g. İnternetin güvenli kullanımı ve güvenli internet hizmeti konusunda araştırmalar yaparak uygun politikaların belirlenmesi, bu konuda Bilgi Teknolojileri ve İletişim Kurumu ile koordineli bir çalışma içerisinde uygulamaya esas alınacak güvenlik kriterlerinin tespiti ve benzeri konularda önerilerde bulunmak.

ğ. İnternet ortamının güvenli, serbest, özgür ve faydalı kullanımı ile katma değer üretmesine yönelik eğitim etkinliklerini desteklemek.

h. Çocuklar ve gençler başta olmak üzere bireylerin ve toplumun internet üzerinden yapılan zararlı yayınlardan korunmasına yönelik olarak ulusal bazda yazılım programları hazırlanması konusunda çalışmalar yapmak ve önerilerde bulunmak.

ı. Çocuklar ve ailelerde internet kültürünün artırılması, internet üzerinden istismar ve şiddet içerikli oyunların etkileri ve derecelendirilmesi gibi konularda ilgili kurumlarla ve sivil toplum kuruluşlarıyla iş birliği içerisinde toplumsal bilincin artırılması yönünde gerekli çalışmalar yapmak, yaptırmak ve önerilerde bulunmak.

i. İnternet içerik ve yer sağlayıcılığının yaygınlaştırılması ve ulusal arama motoru teşkili konusunda gerekli çalışmalar yapmak üzere önerilerde bulunmak.

j. Bilgi ve iletişim teknolojilerinde kullanılan tüm ürünler için araştırma ve geliştirme desteği ile yerli üretimin artırılmasına yönelik önerilerde bulunmak.

k. Ulusal ve uluslararası sayısal uçurum olarak adlandırılan farklılıkların giderilmesi ve bilgi toplumu ve bilgi ekonomisi oluşumuna katkıda bulunmak amacıyla projeler ve öneriler belirlemek, uygulanabilirliklerini değerlendirmek, risk analizlerinin yapılması ve kabul gören tekliflerin gerçekleştirilmesine katkıda bulunmak ve uygulama planlarının oluşturulması için Bakana öneride bulunmak.

l. İnternet ile ilgili mevzuat için, uluslararası kuruluşlarca kabul gören uygulamaları ve Avrupa Birliği’nin bu alandaki mevzuatı ile uyumlu olmasına özen gösterilmesi için önerilerde bulunmak.

m. İnternete erişim sağlayan işletmeciler arasında birlikte veya ayrı ayrı olarak görüşmek, sektörel sorunları tespit etmek, sorunların çözümü hususunda tavsiyelerde bulunmak.

n. Görev alanına giren konularla ilgili olarak çalışmalarda bulunmak üzere kamu kurum ve kuruluşları, meslek odaları, sivil toplum kuruluşları, özel sektör temsilcileri ve konuyla ilgili uzmanların katılımıyla çalıştay yapmak, çalışma grupları ve geçici komisyonlar oluşturmak.

o. Kamu ile internete erişim sağlayan işletmecilerle görüşmek, sektörel sorunları tespit etmek ve sorunların çözümü hususunda tavsiyelerde bulunmak.

ö. Siber güvenliğin sağlanması için internet üzerinden alınması gereken tedbirlere iliş- kin önerilerde bulunmak.

p. Bakanlık politikalarının belirlenmesine katkı sağlamak amacıyla, Bakan tarafından talep edilen benzer konularda çalışma ve araştırmalar yapmak.

**Bilgi Teknolojileri ve İletişim Kurumu**

Bilgi Teknolojileri ve İletişim Kurumu 4502 sayılı Kanun ile 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun’un 5. maddesinde yapılan değişiklikle kurulmuştur. 5809 sayılı Elektronik Haberleşme Kanunu’nun 67. maddesinin 2. fıkrası gereğince, o güne dek Telekomünikasyon Kurumu olan kurumun adı Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir. Elektronik haberleşme alanında en önemli kurumdur. Kurum’un internet içeriğine de müdahale yetkisi vardır. Zira Kurum, internet içeriğinin takip ve gerektiğinde engellenmesi, içerik, yer, erişim ve toplu kullanım sağlayıcılara ilişkin yetkilendirme, gözetim ve denetim faaliyetlerinin gerçekleştirilmesi ve filtreleme yazılımlarının standartlarının belirlenmesi gibi yetkilerle donatılmıştır. Kurum’un ayrıca internet hizmet sağlayıcılara ilişkin idari yaptırım uygulama hakkı da bulunmaktadır. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile ilişkilidir. Kurum, idari ve mali özerkliğe sahip bir kamu tüzel kişiliğidir. Görevlerini yerine getirirken bağımsızdır. Hiçbir organ, makam, merci veya kişi Kuruma emir ve talimat veremez. Kurum, Bilgi Teknolojileri ve İletişim Kurulu ile Başkanlık teşkilatından oluşur. Bilgi Teknolojileri ve İletişim Kurulu, Kurumun karar organıdır. Kurul, biri başkan olmak üzere toplam yedi üyeden oluşur. Kurul Başkanı Kurumun da başkanıdır. Kurul Başkanı Kurumun en üst idari amiridir. Kurumun yönetim ve temsil yetkisi başkana aittir. Kurul başkanı ve üyeler, Bakanlar kurulu tarafından beş yıllık süre için atanır. Görevi biten Kurul başkanı ve üyelerin yeniden aynı göreve atanmaları mümkündür. Kurul başkan ve üyeleri atanmaları için gerekli şartları kaybetmeleri halinde Bakanlar Kurulu kararıyla süresi dolmadan görevden alınabilir. Kurul üyeliklerine atanacakların; mühendislik alanında elektronik, elektrik-elektronik, elektronik ve haberleşme, endüstri, fizik, matematik, bilgisayar, telekomünikasyon ve işletme mühendisliği fakültelerinden veya bölümlerinden, sosyal bilimler alanında siyasal bilgiler (bilimler), iktisadi ve idari bilimler, iktisat, hukuk, işletme fakülteleri veya bölümlerinden ya da fakültelerden fizikçi veya matematikçi unvanıyla veya sayılan fakülte ve bölümlere denkliği yetkili makamlarca kabul edilmiş yurt dışındaki yükseköğretim kurumlarından mezun olmaları ya da belirtilen bölümlerden mezun olmamakla birlikte sayılan alanlarda yüksek lisans veya doktora yapmış olmaları, mesleki ve elektronik haberleşme veya posta hizmetleri alanında yeterli bilgi ve deneyime sahip, kamu veya özel sektörde en az 10 çalışmış olmaları ve herhangi bir siyasi partinin yönetim ve denetim organlarında görev almamış veya bu görevlerinden ayrılmış olmaları gerekir.

Kurul, Başkanın daveti veya üyelerden en az 3 talebi üzerine toplanır. Kurul toplantılarını Kurul Başkanı, yokluğunda ikinci başkan yönetir. Toplantının gündemi Başkan tarafından belirlenir, gündeme yeni madde eklenebilmesi için bir üyenin öneride bulunması ve en az 3 üyenin kabul etmesi gerekir. Kurul en az 5 üyenin hazır bulunması ile toplanır ve en az 4 üyenin aynı yöndeki oyuyla karar alır. Üyeler çekimser oy kullanamaz. Toplantıda bir konuda karar yeter sayısı sağlanamadığı durumda, izleyen toplantılarda aynı konuda oylarda eşitlik olması halinde Başkanın bulunduğu tarafın oyu üstün sayılarak karar alınır. Kurul kararı tutanakla tespit edilir. Kurulun kararları Kurumun idari denetimi sırasında yerindelik denetimine tabi tutulamaz. Kurul toplantıları gizlidir. İhtiyaç duyulması halinde Uzman kişiler kurul toplantılarına davet edilebilir. Kurul uygun gördüğü kararlarını internet ortamı başta olmak üzere uygun vasıtalarla kamuoyuna duyurur. Kurulun düzenleyici kararları ilişkili Bakanlığa ve Resmî Gazete ’de yayımlanmak üzere Başbakanlığa gönderilir. Kurum’un 5369 sayılı Evrensel Hizmet Kanun gereğince Türkiye Cumhuriyeti sınırları içinde coğrafi konumlarından bağımsız olarak herkes tarafından erişilebilir, önceden belirlenmiş kalitede ve herkesin karşılayabileceği makul bir bedel karşılığında asgari standartlarda sunulacak olan, internet erişimi de dahil elektronik haberleşme hizmetlerinin sağlanmasına yönelik yetki ve görevleri bulunmaktadır.

5809 sayılı Elektronik Haberleşme Kanunu ise Kurum’a şu yetki ve görevleri vermiştir:

a. Elektronik haberleşme sektöründe; rekabeti tesis etmeye ve korumaya, rekabeti engelleyici, bozucu veya kısıtlayıcı uygulamaların giderilmesine yönelik düzenlemeleri yapmak, bu amaçla ilgili pazarlarda etkin piyasa gücüne sahip işletmecilere ve gerekli hallerde diğer işletmecilere yükümlülükler getirmek ve mevzuatın öngördüğü tedbirleri almak.

b. Bu Kanun ve bu Kanuna dayanılarak yapılan düzenlemelere aykırı olarak, elektronik haberleşme sektöründe ortaya çıkan rekabet ihlallerini denetlemek, yaptırım uygulamak, mevzuatın öngördüğü hallerde elektronik haberleşme sektöründe rekabet ihlallerine ilişkin konularda Rekabet Kurumundan görüş almak.

c. Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.

ç. İşletmeciler ile tüketicileri ilgilendiren Kurul kararlarını gerekçe ve süreçleri ile kamuoyuna açık tutmak.

d. Bu Kanun çerçevesinde gerektiğinde işletmeciler arasında uzlaştırma prosedürünü işletmek, uzlaşma sağlanamadığı takdirde ilgili taraflar arasında aksi kararlaştırılıncaya kadar geçerli olmak üzere gerekli tedbirleri almak.

e. Elektronik haberleşme sektöründeki gelişmeleri takip etmek, sektörün gelişimini teşvik etmek amacıyla gerekli araştırmaları yapmak veya yaptırmak ve bu konularda ilgili kurum ve kuruluşlarla iş birliği halinde çalışmak.

f. Elektronik haberleşme hizmetlerinin sunulması ve elektronik haberleşme şebeke ve altyapılarının tesis ve işletilmesi için gerekli olan frekans, uydu pozisyonu ve numaralandırma planlamasını ve tahsisini yapmak.

g. Elektronik haberleşme ile ilgili olarak Bakanlığın strateji ve politikalarını dikkate alarak, yetkilendirme, tarifeler, erişim, geçiş hakkı, numaralandırma, spektrum yönetimi, telsiz cihaz ve sistemlerine kurma ve kullanma izni verilmesi, spektrumun izlenmesi ve denetimi, piyasa gözetimi ve denetimi de dahil gerekli düzenlemeler ile denetlemeleri yapmak.

ğ. Telsiz sistemlerinin belirlenen tekniklere ve usullere uygun olarak kurulmasının ve çalıştırılmasının kontrolünü yapmak, elektromanyetik girişimleri tespit etmek ve giderilmesini sağlamak.

h. İşletmecilerin ticari sırları ile kamuoyuna açıklanabilecek bilgilerinin kapsamını belirlemek, işletmecilerin ticari sırları ile yatırım ve iş planlarının gizliliğini korumak ve bunları adli makamların talepleri dışında muhafaza etmek.

ı. Elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak, Bakanlık tarafından elektronik haberleşme sektörüne yönelik strateji ve politikaların belirlenmesinde ihtiyaç duyulanları, talebi üzerine Bakanlığa iletmek.

i. Bakanlıkça yapılacak düzenlemeler çerçevesinde, elektronik haberleşme sektörüne ilişkin araştırma, geliştirme ve eğitim faaliyetlerine ilişkin olarak, mevcut Kurum gelirlerini göz önünde bulundurarak gelirlerinin %20’sini aşmamak kaydıyla ayıracağı kaynağı Bakanlığa aktarmak.

j. Kullanıcılara ve erişim kapsamında diğer işletmecilere uygulanacak tarifelere, sözleşme hükümlerine, teknik hususlara ve görev alanına giren diğer konulara ilişkin genel kriterler ile uygulama usul ve esaslarını belirlemek, tarifeleri onaylamak, tarifelerin denetlenmesine ilişkin düzenlemeleri yapmak.

k. İşletmeciler tarafından hazırlanan referans erişim tekliflerini onaylamak.

l. Yürütülecek elektronik haberleşme hizmetleri, şebeke ve/veya alt yapısı ile ilgili olarak yapılacak yetkilendirmelere ilişkin hüküm ve şartları belirlemek, uygulanmasını ve yetkilendirmeye uygunluğu denetlemek, bu hususta gereken iş ve işlemleri yürütmek ve mevzuatın öngördüğü tedbirleri almak.

m. Radyo ve televizyon yayıncılığına ilişkin ilgili kanununda belirtilen hükümler saklı kalmak kaydıyla, frekans planlama, tahsis ve tescil işlemlerini, güç ve yayın sürelerini de göz önünde tutarak uluslararası kuruluşlarla iş birliği de yapmak suretiyle yürütmek.

n. Elektronik haberleşme sektöründe kullanılacak her çeşit sistem ve cihazların, uyumlaştırılmış ulusal standartlarını yayımlatmak ve uygulanmasını sağlamak, teknik düzenlemelerini yapmak, piyasa denetimini yapmak ve/veya yaptırmak, bu amaçla laboratuvarlar kurup işletebilmek ve bu laboratuvarlarda verebileceği eğitim ve danışmanlık hizmetleri karşılığında alınacak ücretleri belirlemek.

o. Elektronik haberleşme sektöründe tesis, ölçüm ve bakım-onarım yapacak kuruluşların yetkilendirmesini bu konuda görevli kuruluşlarla koordine etmek.

ö. Elektronik haberleşme sektörüne yönelik pazar analizleri yapmak, ilgili pazarı ve ilgili pazarda etkin piyasa gücüne sahip işletmeci veya işletmecileri belirlemek.

p. Elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşların çalışmalarına katılmak, kararların uygulanmasını takip etmek ve gerekli koordinasyonu sağlamak.

r. Kurumun yıllık bütçesini, gelir-gider kesin hesabını, yıllık çalışma programını onamak, gerekirse bütçede hesaplar arasında aktarma yapmak veya gelir fazlasını mevzuat çerçevesinde genel bütçeye devretmek.

s. Elektronik haberleşme sektöründe faaliyet gösterenlerin mevzuata uymasını denetlemek ve/veya denetlettirmek, konu ile ilgili usul ve esasları belirlemek, aykırılık halinde mevzuatın öngördüğü işlemleri yapmak ve yaptırımları uygulamak.

ş. Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak.

t. Ara bağlantı ve ulusal dolaşım da dahil erişim ile ilgili uygulanacak usul ve esasları belirlemek ve mevzuatın ön gördüğü düzenlemeleri yapmak, elektronik haberleşme sağlanması amacıyla imzalanan anlaşmaların rekabeti kısıtlayan, mevzuata ve/veya tüketici menfaatlerine aykırı hükümler içermemesi amacıyla mevzuatın öngördüğü tedbirleri almak.

u. İlgili kanun hükümleri dahilinde, evrensel hizmetlere ilişkin hizmet kalitesi ve standartları da dahil olmak üzere, gerektiğinde her türlü elektronik haberleşme hizmetine yönelik hizmet kalitesi ve standartlarını belirlemek, denetlemek, denetlettirmek ve buna ilişkin usul ve esasları belirlemek.

ü. Elektronik haberleşme sektöründe, bağımsız denetim faaliyetine ilişkin esasları, bağımsız denetleme faaliyetlerinde bulunacak kuruluşların kuruluş şartlarını, çalışma esaslarını ve çalıştıracağı personelin niteliklerini belirlemek.

v. Siber güvenlik ve internet alan adları konularında Bakanlar Kurulu, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri ilgili birimleri marifetiyle yerine getirmek.

y. Bu Kanunla verilen görevlere ilişkin yönetmelik, tebliğ ve diğer ikincil düzenlemeleri çıkarmak.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Bilgi Teknolojileri ve İletişim Kurumu’na birçok görev ve yetki vermiştir. Madde 10 Fıkra 4

a. Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu Kanun kapsamına giren suçları oluş- turan içeriğe sahip faaliyet ve yayınları önlemeye, internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usuller dâhilinde Kurumca karşılanacak çalışma kurulları oluşturmak.

b. İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen gerekli tedbirleri almak.

c. İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek.

ç. Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülki idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usulleri belirlemek.

d. İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8. maddesi ile 8/A maddesinde sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak.

e. İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek.

f. Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla iş birliği ve koordinasyonu sağlamak.

g. Bu Kanunun 8. maddesinin birinci fıkrasında sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini temînen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkanları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

h. 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümleri uyarınca oluşturulan İnternet Geliştirme Kurulunca internetin yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli kullanılması gibi konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları almak.

ı. Ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlamak, gerekli tedbirlerin aldırılması konusunda faaliyet yürütmek ve ihtiyaç duyulan çalışmaları yapmak

**İNTERNET SÜJELERİNİN SORUMLULUĞU**

İnternette yer alan kişilerin farklı işlevleri olduğu için sorumluluklarının da aynı olması beklenemez. Dolayısıyla içerik sağlayan, yer sağlayan ve erişim sağlayanların hukuki statülerinin ve sorumluluklarının ayrı ayrı belirlenmesi gerekir. İçerik Sağlayıcı (Content Provider) İnternet kullanıcılarınca herhangi bir internet içeriğini hazırlayan veya bilgiyi, veriyi bizzat üreten internet süjesine içerik sağlayıcı denir. Bu itibarla içerik sağlayıcılar çok uluslu şirketlerden, kamu kurumlarına, özel işletmelerden, bireylere kadar çok geniş bir kategoriyi oluşturmaktadır. 5651 sayılı Kanun’un 4. maddesi, içerik sağlayıcının sorumluluğunu düzenlemiştir. Buna göre içerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur. Bu sorumluluğun gerek özel hukuk ve gerekse de ceza hukuku sorumluğu olduğuna şüphe yoktur. İçerik sağlayıcının link şeklinde bağlantı vermesi halinde sorumluluğunun belirlenmesi uygulamada bazen tereddütler yaratmaktadır. Ancak 5651 sayılı Kanun bu konuda açık bir düzenleme içermektedir. Kanun’un 4. Maddesine göre, içerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Buna göre içerik sağlayıcıların, bağlantı verdiği ve ulaşılmasını sağladığı başkasına ait içerikten sorumlu olmayacağı kabul edilmektedir. Ancak bu kuralın bir istisnası bulunmaktadır. 4. maddeye göre sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise link veren içerik sağlayıcının bu durumda genel hükümlere göre sorumlu olduğu belirtilmiştir. İçerik sağlayıcının sadece verilen linkin içeriğinden sorumlu olacağı, buna karşın verilen linkin bulunduğu sitenin tamamının içeriğinden sorumlu olmayacağı kabul edilmelidir. 5651 sayılı Kanun’un 4. maddesi uyarınca, içerik sağlayıcının internet ortamında kullanıma sunduğu her türlü içerikten sorumlu tutulmasının önemli bir sonucu vardır: adı sıkça duyulan “bilişim suçlarının” faili genelde içerik sağlayıcıdır. Sosyal medya, medyanın içeriğini üretenler ile medyayı izleyenler arasındaki katı ayrımı kaldırmıştır. Bilindiği üzere internetin ilk çıktığı zamanlarda web siteleri yalnızca bunların sahipleri veya idarecileri tarafından siteye yüklenen içeriklerle sınırlıydı. Yani tek taraflı bir bilgi, veri iletimi söz konusuydu. Web 2.0 teknolojisi, tek yönlü bilgi akışından, çift taraflı ve eş zamanlı bilgi paylaşımına ulaşılmasına izin veren medya sistemidir. Bu teknolojinin hizmete sunulmasıyla, web 2.0 teknolojisi üstüne üzerine inşa edilmiş ve kullanıcı merkezli yaratım ve değişikliklere izin veren “grup internet tabanlı uygulamalar” bütünü, kısaca sosyal medya denen olgu gerçekleşmiştir. Bugün için internet ansiklopedileri, bloglar, mikro bloglar (Twitter), içerik toplulukları (Youtube), sosyal ağ siteleri (Facebook), sanal oyun dünyaları (örneğin World of Warcraft) ve sanal sosyal dünyalar (örneğin Second Life) bilinen sosyal medya türleridir. Bulut bilişim ise ağırlıklı olarak kurumsal çözümlerde kullanılan bir “büyük veri” (big data) teknolojisidir. Bulut bilişim, hizmet sağlayıcısı aracılığıyla hızlı bir şekilde erişilebilen ve daha sonra da serbest bırakılabilen, bilgisayar ağları, sunucular, depolama alanları, uygulamalar ve hizmetler gibi bilişim kaynaklarının ortak havuzuna her yerden istenildiğinde erişim sağlayabilen bir model olarak ifade edilmektedir. Bulut bilişim genel olarak kaynakların birleştirilmesi esasına dayanmaktadır. Geleneksel veri işleme yöntemleri ile değerlendirilemeyecek kadar çok büyük hacimli, oldukça karmaşık, hızlı değişebilen verinin (büyük veri), birden çok bilişim ağında depolanması ve kullanıcıların da bu büyük veriye her yerden güvenli bir şekilde ulaşabilmesi düşüncesine dayanmaktadır. Bu noktada “dar anlamda bilişim suçları” ve “geniş anlamda bilişim suçları” ayrımı yapılmaktadır. Buna göre sadece bilişim ortamında işlenebilen, bilgisayar ve internete özgü suçlar dar anlamda bilişim suçlarıdır. Örneğin bilişim sistemine hukuka aykırı şekilde girme (TCK m. 243) veya bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçları (TCK m. 244) bu kapsamda değerlendirilmektedir. Buna karşın geniş anlamda bilişim suçları ise bilişim sistemleri kullanılarak veya bilişim sistemlerinden yararlanılarak işlenen klasik suçlardır. Birçok klasik suçun bilişim sistemlerinde veya bilişim sistemlerinden yararlanılarak işlenmesi mümkündür. Bu suçlara örnek olarak; tehdit ve şantaj, hakaret ve sövme, taciz, röntgencilik, dolandırıcılık, terörizm gösterilebilir.

Bilişim suçları, özellikle dar anlamda bilişim suçları, “yıkıcı yazılım” olarak adlandırılan tekniklerle işlenmektedir. Örn: sistem güvenliğinin kırılıp içeri girilmesi (hacking); yararlı bir yazılımın içine fark edilmeyecek küçüklükte zararlı yazılımlar konulmasıyla bilişim sistemine girilmesi (Truva atı/Trojen horse); çok fazla kaynaktan kaynak başına çok az toplamda ise çok miktarda hukuka aykırı yarar sağlanması (salam tekniği); bilişim sisteminin içinde işlemciye sürekli anlamsız komutlar vererek bilişim sisteminin çökertilmesi (tavşanlar/rabbits); sistemin bakım için geçici bir süre kapatılması uyarısından sonra sistemden kullanıcı adları, şifreler gibi bilgilerin çalınması (bukalemunlar/chameleon); sistemi çökertmek için tasarlanan mantık bombaları ve bilişim virüsleri; DoS ve DDoS saldırıları ile hedef bilgisayarın kimseye hizmet veremez hale getirilmesi; phising denilen yöntemlerle kişilerin kredi kartları numaralarının çalınması verilebilir. ***Bilinen ilk bilişim suçu 18.10.1966 tarihinde Minneapolis Tribune gazetesinde yayınlanan “bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor” başlıklı haber ile kamuoyuna yansımıştır.***

Bilişim suçlarında şüpheliye ulaşmak için kullanılan yöntem, IP numarasının tespit edilerek, IP numarasının tahsis edildiği internet abonesini belirlemektir. Ancak sadece IP numarasının tespiti ile şüpheli hakkında mahkûmiyet kararı verilememektedir. Bazı olaylarda bilgisayar Truva atları ile “zombi” bilgisayara dönüştürülmekte ve böylece IP numarası belirlenen kişinin aslında gerçekleştirilen hukuka aykırı eylemden haberinin dahi olmadığı belirlenmektedir. Bu nedenle suçun kesin şekilde ispat edilmesi için, adreste arama yapılması, bilgisayar veya bilgisayar özelliği taşıyan tablet, akıllı telefon gibi cihazların tespit edilmesi ve Ceza Muhakemesi Kanunu’nun 134. maddesi gereğince bu cihazlarda içerik araması yapılması gerekmektedir. Tüm bu süreç, “adli bilişimin” (computer forensics) konusudur. Adli bilişim, bilişim sistemlerinin ve üzerinde bulunan depolama ünitelerinin, herhangi bir suçu işlemede kullanılıp kullanılmadığını tespiti amacıyla yapılan çalışmaların tümü olarak adlandırılmaktadır. Burada en önemli aşamalar bilişim sistemindeki tüm verilerin özel yazılımlarla kopyalanması (imaj alma) ve kopyalanan veri ile depolanan delil arasında herhangi bir farklılığın olup olmadığını kontrol edilmesidir (hash değeri kontrolü) ve hash değerinin doğru olması üzerine imajı alınmış bilginin çözümlenmesidir. Bu gibi durumlarda ulusal makamların, gerekli bilgilere ilişkin taleplerini firma merkezinin bulunduğu ülkenin adli makamlarına gönderecekleri adli yardımlaşma talebiyle istemeleri gerekmektedir Ülkemizde adli yardımlaşma hususunda yetkili makam Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü’dür. Adli yardımlaşma 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu çerçevesinde yapılmaktadır. Ancak Kanun’un 1. maddesinin 3. fıkrasına göre Türkiye’nin taraf olduğu adli iş birliğine ilişkin milletlerarası antlaşmalar saklıdır. Buna göre uluslararası adli yardımlaşma talepleri, diğer devletin sözleşmeye taraf olması durumunda, “Ceza İşlerinde Adli Yardımlaşmaya Dair Avrupa Sözleşmesi” çerçevesinde ya da ABD gibi sözleşmeye taraf olmayan bir devlet ise ikili antlaşmalar çerçevesinde eğer bu da yoksa 6706 sayılı Kanun çerçevesinde yapılmaktadır. Ancak bu durumun bazı istisnaları mevcuttur. Facebook bazı durumlarda IP veya trafik bilgisini doğrudan vermektedir. Facebook; intihara teşebbüs, öldürmeye teşebbüs, kayıp bir şahsın bulunması veya çocukların cinsel istismarı suçlarını acil husus kabul ederek soruşturma makamları tarafından doğrudan talep edildiğinde IP ve trafik bilgilerini vermektedir. Bu tür delillerin kimler tarafından hangi şartlar altında elde edileceği ve şüpheliye karşı kullanılabileceği hususları Ceza Muhakemesi Kanunu’na tabidir.

**Yer Sağlayıcı (Host Provider)**

“Host” kelime anlamı olarak “barındırmak” anlamına gelmektedir. İnternetin aktif bir elemanı olan host’un internet ortamındaki anlamı da tam olarak budur. Host, internet yoluyla erişilebilen dijital bir depolama birimidir. Hostlar kendi materyallerini depolayabildikleri gibi başkası yararına ücretli veya ücretsiz olarak da materyal depolayabilmektedirler. Bu materyaller kısa ömürlü veya devamlı materyal olabilir. Host sahibi materyalin hostta depolanmasında aktif rol üstlenebilir veya depolama alanı tedarik etme dışında hiçbir kontrol imkânına sahip olmayabilir. Yer sağlayıcısı, 5651 sayılı Kanun’un 2. maddesinde, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler olarak tanımlanmıştır. İçerik sağlayıcısının sorumluluğu aynı Kanun’un 5. maddesinde düzenlenmiştir. Host ile günlük hayatta çok sık şekilde karşılaşılır. Örn: ebay, youtube, gittigidiyor, sahibinden gibi siteler bunlara örnektir. Bu siteler, kullanıcılarına (içerik sağlayıcılarına) kendi içeriklerinin internette yayınlanması için yer temin etmektedirler. Yine yukarıdaki örnekte forum sitesinin işleteni de yer sağlayıcısıdır, zira forumda kullanıcılarının düşüncelerini açıklamaları için onlara, kendi sayfasında yer temin etmektedir. Yer sağlayıcılarının kural olarak sorumluluğu bulunmamaktadır. 5651 sayılı Kanun’un 5. maddesine göre yer sağlayıcı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Ancak bu sorumsuzluk sınırsız değildir. Yer sağlayıcı hukuka aykırı içerikten Kanun’da belirtilen usuller çerçevesinde haberdar edilmesi durumunda içeriği çıkarmakla yükümlüdür. Bu yükümlülüğe aykırı davranılması halinde içerik sağlayıcının da sorumluluğu doğar. Bunun için öncelikle hostun ana bilgisayarda depoladığı başkasına ait hukuka aykırı içerikten kesin olarak haberdar olması ve daha sonra da bu bilgilerin kaldırılmasının teknik olarak mümkün olması gerekir. Yer sağlayıcının teknik olarak böyle bir imkâna sahip olduğu kabul edilmelidir. Bu şartlar gerçekleştiği halde içerik kaldırılmıyorsa, yer sağlayıcısının da sorumluluğunun bulunduğu kabul edilebilecektir. (5651 sayılı Kanun madde 9). Bu aşamadan itibaren yer sağlayıcısı kendisine Kanun tarafından yüklenen yükümlülüklerini ihlal ederse, kişilik hakları ihlal edilen kişi yer sağlayıcısına karşı da tıpkı içerik sağlayıcısına olduğu gibi, tazminat davası açabilmektedir. Yer sağlayıcısının 5651 sayılı Kanun’dan doğan yükümlülüğünü ihlal etmesi, tek başına suç işleme iradesiyle hareket ettiğini göstermez. Bu durum, 5651 sayılı Kanun’da yer alan yer sağlayıcısının sorumluluğunu düzenleyen hükmün “ön-filtre” olarak kabul edilmesinin sonucudur. Bu bakımdan yer sağlayıcısının ceza sorumluluğu tartışılırken öncelikle bu süjenin 5651 sayılı Kanun’dan doğan yükümlülüğünü ihlal edip etmediği sorgulanır (ön-filtre), eğer ihlal ettiği kabul edilirse, ikinci aşamada Türk Ceza Kanunu’nda belirtilen suç teorisi ilkeleri çerçevesinde bir suçu işleyip işlemediği araştırılır.

**Erişim Sağlayıcı (Access Provider)**

İnternet erişim sağlayıcıları, internet toplu kullanım sağlayıcılarına ve abone olan kullanıcılara internet ortamına erişim olanağı sağlayan gerçek veya tüzel kişileri ifade eder. İnternet erişim sağlayıcıları iletişimde bulunmamakta, sadece başkasına ait içeriklere ulaşılmasına aracılık etmektedir. İnternet erişim sağlayıcıları başkalarına ait bilgileri kendi sunucularında barındırmaz. Erişim sağlayıcı, 5651 sayılı Kanun’un 2. maddesinde, kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler olarak tanımlanmıştır. Yer sağlayıcısının sorumluluğu aynı Kanun’un 6. maddesinde düzenlenmiştir. İnternet erişim sağlayıcıları, çoğu kez internet servis sağlayıcıları ile aynı anlamda kullanılmaktadır. İnternet servis sağlayıcısı, dial-up (çevirmeli ağ), DSL, ADSL, kablosuz internet, kablolu internet, uydu internet vb. teknoloji kullanarak kullanıcıların internete bağlanmasını sağlayan, yani kullanıcılar ile internet arasında köprü vazifesi gören gerçek veya tüzel kişilerdir. İnternet sistemi içerisinde en önemli aktör internet servis sağlayıcılardır. İnternet servis sağlayıcıları kendi bilgisayarlarını, kullanıcıların internete erişebilmeleri için giriş kapısı olarak kullanırlar. Bu sebeple bir internet kullanıcısı, bir internet servis sağlayıcısının yardımı olmadan internete bağlanamaz. İnternet servis sağlayıcısı internet kullanım hizmeti vermek istediklerinde telefon /telekomünikasyon idareleri ile bir sözleşme imzalayarak kullanım/kullandırma hakkı elde eder ve genellikle ücret karşılığında bu hakkı internet kullanıcılarına kiralar. İnternet servis sağlayıcısı sadece erişim hizmeti veriyor ise yani başkalarına ait bilgileri sunucularında barındırmıyorsa internet erişim sağlayıcısı adını alır. İnternet erişim sağlayıcısı kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir. Dolayısıyla internet erişim sağlayıcısı, kullanıcılarının internete koymuş oldukları içerikten sorumlu değildir, Ancak internet erişim sağlayıcısı bu hukuka aykırı içeriğin erişimini engellemekle yükümlüdür. Zira 5651 sayılı Kanun’un 6. Maddesine göre erişim sağlayıcı, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde erişimi engellemekle yükümlüdür. Erişimin engellenmesinin hukuki yönüyle ilgili detaylı bilgiler ilerleyen bölümlerde verileceğinden, burada bazı teknik bilgilerin verilmesi yeterli olacaktır. Erişimin engellenmesi bazı ayrımlar çerçevesinde ele alınması gereken bir konudur. Bu noktada yapılan ilk ayrım “erişimin genel engellenmesi” ve “erişimin özel engellenmesidir”. Genel engelleme, devletlerin interneti bir filtreye tabi tutularak bazı web sitelerine erişimi henüz bir suç unsuru oluşmadan engellemesidir. Ancak bu yöntemin getirdiği hukuksal sakıncalar yanında teknik olarak da bazı sakıncaları mevcuttur. Genel engellemenin teknik alt yapısı genellikle router programlama sistemleridir. Routerlar verileri parça parça ayırarak en hızlı şekilde son bilgisayara göndermektedir. İşte router programları da bu parçalara ayrılmış veriyi bir filtreye tabi tutarak, veri içerisinde beliren bazı sözcükleri yakalar ve bu sözcükleri içeren verilerin geçişi engeller. Bu programlar sayesinde devletler kendi egemenlik alanlarında, internet ağında bazı sözcükleri bulunduran web sitelerine girişi bütünüyle engellemektedir. Özel engelleme ise, bir ceza normunun ihlali şüphesi olması veya bu ihlalin mahkeme tarafından sabit bulunması ya da suç oluşmasa bile bir hukuka aykırılığın bulunması halinde hukuka aykırılık bulunduran web sitelerine erişimin engellenmesidir. Erişimin özel engellenmesi tedbirine başvurulması için gereken şartlar ülkeden ülkeye değişkenlik gösterse de birçok ülkede mevcuttur. Ülkemizde de erişimin engellenmesi denildiğinde anlaşılan husus genel olarak erişimin özel engellenmesidir. Erişimin özel engellenmesinde birçok teknik kullanılmaktadır. Bunlardan en yaygın olanları IP engellemesi, DNS engellemesi ve URL engellemesidir. En temel erişim engelleme yöntemi web sitelerinin yer aldığı sunucuların IP adreslerinin engellemesidir. IP engellemesinde, ağlar arası iletişimi sağlayan routerlar devreye girer ve engellenmiş olan IP numarasına ait web sitesine dair taleplerin routerlardan internet servis sağlayıcısına iletilmesi engellenir. Böylece web sitesinde yer alan tüm içerik engellenmiş olur. DNS engelleme tekniğinde ise, kullanıcı web sitesine girmeye çalıştığında alan adlarının IP çözümlemesini yapan DNS sunucusu web sitesinin çözümleme isteğini yanıtsız bırakır. IP ve DNS engellemesinin en büyük dezavantajı web sayfasında yer alan içeriğin tümünün engellenmesidir. Kullanılan bir başka yöntem ise Uniform Resource Locator (URL) yöntemiyle erişimin engellenmesidir. URL, internette resim, yazı veya müzik gibi bir kaynağa karşılık gelen standart formatta uygun bir karakter dizinidir. URL, internet üzerindeki bir kaynağın tam bulunduğu yer başka bir deyişle koordinatıdır. Kişinin internette sörf yaparken bir kaynağa tıkladığında adres çubuğunda görünen tam adres URL’dir. URL engellemesi yalnızca hukuka aykırı içeriğe erişimin engellenmesi amacıyla kullanılan bir tekniktir. Dolayısıyla bu yöntemin en önemli avantajının hukuka aykırı bir içerik için tüm web sitesinin erişime engellenmesinin önlenmesi olduğu ifade edilmektedir. URL engellemesi “http” ile başlayan adreslerde uygulanabilmektedir. Buna karşın çoğunlukla hesap oluşturularak kullanılan “facebook.com”, “youtube.com”, “twitter.com” gibi internet adreslerinin “https” protokolünü kullanmalarından dolayı bu sitelere ait URL adreslerine erişimin engellenmesi, en azından şu andaki teknoloji çerçevesinde, teknik olarak mümkün olamamaktadır.

**UNITE 2**

**GİRİS**

20. Yüzyılın 2. Yarısında Bilgisayar teknolojilerinde hızlı gelişim ve ağların ağı İnternet’in ortaya çıkışı insan yaşamını Sanayi Devrimi ile kıyaslanır ölçüde bir dönüşüme uğratmıştır. 20. Yüzyılın sonunda artık bilişim teknolojileri her yerdedir. Akıllı telefonlar, e-posta adresleri, kapalı devre televizyon sistemleri, sosyal paylaşım siteleri, sanal ağlarda sohbet odaları ve saymakla bitmeyecek daha pek çok bilişim ürünü kısa bir süre içinde yaygınlaşmış ve modern insanın yaşamında önemli bir yere kavuşmuştur. Bilişim teknolojilerindeki gelişmeler sosyal, siyasal, ekonomik ve hukuksal alanda yaşanan bir dönüşümü de beraberinde getirmiştir.

**BİLİŞİM TEKNOLOJİLERİ VE İNSAN HAKLARI**

Sosyal yaşam; bilgiye erişim, ekonomik ilişkiler, eğlence ve insan yaşamının neredeyse her alanı dijital koridorlarda kendine yer bulmaktadır. İnternet kullanımı geçen 15 yıl içerisinde (2000-2015) dünya genelinde % 753 oranında artmıştır. Bugün dünyada 3 milyarın üzerinde İnternet kullanıcısı olduğu tahmin edilmektedir. Günümüzde insanlar artan oranda e-posta, İnternet telefonu, görüntülü görüşme siteleri üzerinden iletişim kurmakta, cep telefonlarından İnternet’e bağlanmakta, geleneksel basın yayın kuruluşları yerine çevirim içi alternatif haber alma kaynaklarını tercih etmekte, sosyal paylaşım sitelerinde görüşlerini paylaşmakta, mutfak ihtiyacını internette yapmakta, sohbet odalarında yeni bir sosyal çevre yaratmaktadır. Bu nedenle İnternet yalnızca bir araç değil, insanların yaşamlarında yeni bir alandır. Bu durum eşitlik ve insan onuru gibi insan haklarının eksen kavramlarından, düşünceyi açıklama özgürlüğü, örgütlenme hakkı, özel yaşamın gizliliği hakkı gibi pek çok geleneksel hakka ilişkin de yeni olanakların ve yeni sorunların ortaya çıkmasına neden olmaktadır. İnsan hakları odaklı bir İnternet ortamının yaratılması yönünde talepler artmakta bu konuda çeşitli girişimlerde bulunulmaktadır. 2011 yılında Birleşmiş Milletler İnternet’e erişimi temel bir insan hakkı olarak tanımlamış, Avrupa Konseyi ise İnternet’in evrenselliğini, bütünlüğünü ve açıklığını korumaya ve geliştirmeye yönelik bir tavsiye kararı yayınlamıştır. Her iki metin de günümüzde İnternet’in insan hakları alanında sağladığı olanaklardan yararlanmanın dünya genelinde devletlerin iş birliği içerisinde hareket etmesini gerektirdiğini ve teknik açıdan bu alanın bütünlüğünü koruyucu politikaların geliştirilmesinin önemini ortaya koymaktadır. Öte yandan İnternet, düşüncelerin açıklanmasında ve bilgiye erişimde daha önce hiçbir aracın sunmadığı kadar güçlü olanaklar sunmakta, dünyanın öbür ucunda gerçekleşen bir olay hakkında insanların bilgi almasını, dayanışmasını ve örgütlenmesini olanaklı kılmaktadır. Her ne kadar çeşitli devletler İnternet’te bilgiye erişimi ve bilgi paylaşımını insan haklarının temel ilkelerine aykırı bir şekilde sınırlandırma eğiliminde olsalar da bugün halen bu alanın doğru, güncel, çeşitli bilgilere ulaşma ve demokrasiyi geliştirme açısından önemli olanaklar sunmaya devam ettiğini belirtmek gerekir. İnternet’in denetim ve sınırlama ile değil, insan hak ve özgürlükleri ile anılmaya devam etmesi ise temel insan haklarını merkeze alan bir bakış açısının uluslararası iş birliği içerisinde kabul edilmesine bağlıdır. Birey, devlet ve teknoloji ilişkisinde dengeyi sağlayan hukuksal düzenlemelerin geliştirilmesini gerektirir. Bilişim ile doğrudan ilgili ilk hukuksal düzenleme 1970 yılında Almanya’nın Hessen eyaletinde kişisel verilerin korunmasına ilişkin gerçekleştirilmiştir. Kişisel verilerin korunması hakkı, teknolojinin sağladığı olanakları güçlendirmek ile değil, yarattığı yan etkiler ile ilişkilidir.

**KİŞİSEL VERİ VE KİŞİSEL VERİLERİN İŞLENMESİ**

Bilişim teknolojilerindeki hızlı gelişim her geçen gün artan kaynak ve kanallardan kişisel bilgilerin toplanmasını, kayıt edilmesini, birbiri ile ilişkilendirilmesini, aktarılmasını olanaklı kılmaktadır. 21. Yüzyılda birey kendisine ilişkin bilgilerin kimlerce toplandığı, nerede, hangi amaçlarla kullanıldığı ve kimlerle paylaşıldığı sorularına yanıt aramaktadır. Bu sorulara yanıt bulunması ve bireyin kendisine ilişkin bilgilerle arasındaki bağı kaybetmemesi için ise hukuksal güvencelere gereksinim duyulmaktadır. Bu hukuksal güvenceler, özel yaşamın gizliliği hakkı ile yakından ilişkili olan “kişisel verilerin korunması” çatısı altında toplanmaktadır Kişisel verilerin korunması, veri işleme teknolojileri ile temel hak ve özgürlükler arasında denge kurmayı hedefler. Bu denge veri işlemenin meşru temellerinin ve uyulması gereken ilkelerin hukuksal güvence altına alınmasını gerektirir. Nitekim bu gereksinim, dünyada 100’ ün üzerinde devlette kişisel verilerin korunmasına yönelik hukuksal düzenlemelerin kabul edilmesine neden olmuştur. Kişisel verilerin korunması hakkı, bilişim teknolojilerindeki gelişmeler ile ortaya çıkan bir insan hakkıdır. Bu yeni hak alanının tanımlanmasında “veri” (data) kavramının kullanılmasının nedeni de budur. Ancak “kişisel veri” kavramının doğrudan kişi ile ilgili olduğu unutulmamalıdır. Kişisel verinin ne olduğunu belirlerken aklımızda tutmamız gereken ilk husus, konuya ilişkin ilkelerin benimsenmesindeki temel amacın kişi hak ve özgürlüklerinin korunması olduğudur. Konunun teknik boyutu ve “veri” deyiminin kendisinin teknoloji ile ilişkili bir deyim olması, kimi zaman bu korumanın temel amacının unutulmasına neden olabilmektedir. Bu ilkelerin benimsenmesindeki temel gaye, “veri”lerin, yani herhangi bir rakamın, herhangi bir bilginin, herhangi bir görüntünün, korunması değildir. Burada hedeflenen kişilerin korunmasıdır.

Kişisel veri, en genel tanımıyla, belirli ya da belirlenebilir bir kişiye ilişkin her türlü bilgidir. O halde kişisel veriden söz edebilmek için, verinin (i) bir kişiye ilişkin ve (ii) bu kişinin de belirli ya da belirlenebilir nitelikte olması gerekir. Sayı, yazı, ses ya da görüntüden oluşan bir bilgi bu kapsamda yer alabilir. Her türlü bilgi, mutlaka belirli ya da belirlenebilir bir kişiye ilişkin olmalıdır. Bir başka anlatımla bu bilginin, bir gerçek kişiyle ilişkisinin kurulabiliyor olması gerekir. Bu ilişkinin kurulmasının olanaklı olmadığı bir durumda, tanımda yer alan asgari koşullar gerçekleşmediği için, bu bilgiyi kişisel veri olarak nitelendirmek olanaklı olmayacak, dolayısıyla da kişisel verilerin korunmasında hâkim olan temel ilkeler uygulanmayacaktır. Konuya açıklık getirmek için özel yaşamın gizliliği hakkı açısından da değerlendirme yapılabilir. Nitekim Avrupa İnsan Hakları Mahkemesinin de çeşitli kararlarında belirttiği gibi özel yaşamın gizliliği hakkı, “Bir kişinin kendi kişiliğini geliştirmesi ve gerçekleştirmesi için, özellikle duygusal alanda diğer insanlarla ilişki kurma ve geliştirme hakkını da belirli bir düzeyde içermektedir”. Dolayısıyla kişinin kamusal alandaki etkinliklerinin özel yaşamın gizliliği hakkının dışında olduğunu düşünmek olanaklı değildir. Bu temel hak, belirli düzeyde kamusal etkinlikleri de koruma kapsamına almaktadır. Konuya kamera ile yapılan gözetim açısından yaklaştığımızda ise bir ayrım yapmak gerekir. Buna göre, kamusal alanların kişilerin görüntülerini alan araçlarla izlenmesi ancak bu görüntülerin kayıt edilmemesi durumunda özel yaşama müdahale sayılmaz. Nitekim burada kamera ile yapılan izlemenin, kamusal alanda, örneğin bir meydanda, caddede, otogarda rastlantısal olarak yanımızdan geçip giden insanlarla karşılaşmamızdan bir farkı bulunmamaktadır. Ancak görüntülerin kayıt edilmesi ve bu kaydın sistemli ya da kalıcı olarak yapılması bu durumu değiştirir. Çünkü yapılan kayıt ile o anda görüntülerin belirli bir kişiyle bağlantısı kurulmamış olsa bile ileride bu bağlantının kurulması olanaklı duruma gelmekte, dolayısıyla görüntüsü kayıt edilen kişi “belirlenebilir” olmaktadır. Unutulmamalıdır ki kişiyi doğrudan ya da dolaylı olarak belirlenebilir kılan bütün bilgiler kişisel veridir. Bir kişinin adresi, telefon numarası, pasaport numarası, resmi, ses kaydı, genetik bilgileri, cinsel tercihleri, dini inançları, sabıka kaydı, hobileri, ziyaret ettiği İnternet siteleri gibi bilgiler bu kapsamda değerlendirilecektir. Dolayısıyla bu kapsamdaki bilgiler, kişisel verilerin korunmasında hâkim olan temel ilkelere göre işlenmelidir. AB Yönergesinde “toplama, kaydetme, düzenleme, saklama, uyarlama veya değiştirme, geri alma, danışma, kullanma, ileti ile açığa çıkarma, yayma veya başka bir şekilde oluşturma, sıraya koyma veya birleştirme, engelleme, silme veya yok etme gibi otomatik olan veya olmayan araçlarla kişisel veri üzerinde uygulanan her türlü işlem veya işlem dizisi” veri işleme olarak tanımlanmıştır. Türkiye’de konuya ilişkin hukuksal düzenlemeler kapsamında incelenecek olan Veri Koruma Kanun Tasarısı’nda da benzer bir tanımın benimsendiğini belirtmek gerekir.

**KİŞİSEL VERİLERİN KORUNMASININ ÖNEMİ**

Bir kişiye ilişkin bilgilere ulaşma isteği, belki insanlık tarihinin kendisi kadar eskidir. Eşler, akrabalar, arkadaşlar ya da komşular sosyal ortamda “diğerlerine” ilişkin bilgilere merak duymuşlardır. İşverenler açısından verimliliği arttırmak, ticarî açıdan kârlılığı yükseltmek; idarî açıdan akılcı yönetimi ve güvenliği sağlamak, bu isteğin nedenlerini oluşturan geniş yelpaze içinde ilk akla gelenlerdir. Ancak hangi gerekçeden hareket edilirse edilsin, pek çok cepheden yönelen bu bakışlar, temel hak ve özgürlüklere ilişkin çeşitli sorunlar yaratmaktadır. Bu sorunlara çözüm bulma ve çatışan gereksinimler arasında denge kurma gerekliliği ise tarihsel açıdan daha yakın bir dönemde karşımıza çıkar.

**Bilişim Hukuku**

Kişisel Verilerin Korunması 1960’lardatartışılmaya, 1970’lerde ise hukuksal düzenlemelerinkonusu olmaya başlar. Devletin gözetim isteği,diğer yanda yeni gelişmeler ile bu isteğin eski dönemlerdegörülmeyen ölçüde kapsayıcı bir şekildegerçekleşme olasılığı, bireysel özerkliğe ilişkin kaygılarıngelişmesine neden olmuştur. KişiselVerilerin Korunması Hukukunun ortaya çıkışındatemelde üç etkenin bulunduğu söylenebilir: çeşitliörgütlerce kişisel verilere duyulan gereksinim, teknolojidekigelişmeler, gözetim teknolojilerindekigelişmeler nedeniyle duyulan kaygı.Kişisel verilerin korunması, bireyleri, kendilerineilişkin bilgilerin bilişim teknolojileri ya da dosyalamagibi geleneksel yöntemlerle işlenmesindendoğacak zararlardan koruma amacına yönelmiş vebazı temel ilkelerde somutlaşmış bir dizi önlemiifade eder. Kişisel verilerin korunması hukuku ilkaşamada devlete karşı bireyin korunmasına yönelmiştir. Şirketlerin de veri işlemeyöntemlerini artan oranda ve yaygın bir biçimdekullanmaları özel teşebbüslere karşı da korumasağlanmasını gerekli kılmaktadır. Özellikle sosyalpaylaşım sitelerinde hassas olanbilgilerin paylaşılması özel teşebbüsler tarafındanişletilse de bu alanlarda da korumaya ihtiyaç duyulduğunuaçıkça ortaya koymaktadır.Özellikle son 10 yılda iş yaşamımızın, alışverişyapma şeklimizin, bankacılık faaliyetlerimizin vesosyal ilişkilerimizin teknolojinin sunduğu yeniolanaklarla dönüşüme uğradığına tanık olmaktayız.Bunu görebilmek için cüzdanlarımızdakionlarca indirim ve kredi kartına, e-postalarımızıve cep telefonlarımızın mesaj kutularını dolduranreklamlara, her gün biraz daha sıklıkla karşılaştığımızel izi, parmak izi, retina tarayan sistemlereya da yalnızca en yakın mesai arkadaşımıza, yanibilgisayar(lar)ımıza bakmamız yeterlidir. Bu araçlarıntamamı kişisel verileri içermekte ve yeni veriişleme alanları yaratmaktadır. Bunun yanında ilkaşamada dikkatimizi çekmeyen başka bazı araçlarında izlenmemize hizmet edebileceğini unutmamalıyız.İngilizce bir deyimolan “Radio Frequency Identification”ın kısaltmasıolarak kullanılan RFID’nin tam Türkçe karşılığı:Radyo Frekanslı Tanımlamadır. Bu aracın kullanımıher geçen gün yaygınlaşmaktadır. Bütün bu teknolojilerin bize daha iyi hizmetsunulmasını sağlayan oldukça önemli yararlar sağladığıaçıktır. Öte yandan bu teknolojilerinilk aşamada fark edilemeyen “yan etkileri”, baştaözel yaşamın gizliliği hakkı olmak üzere temel hakve özgürlüklerimize ciddi müdahaleler oluşturabilecekniteliktedir. İşte bu noktada, kişisel verilerinkorunması, teknolojinin kamu kurum ve kuruluşlarına,özel teşebbüslere ve bizlere sunduğu olanaklarla,temel hak ve özgürlüklerimiz arasında birdenge kurmayı hedeflemektedir.Kişisel bilgilerin toplanması, kayıt edilmesi,kullanılması, aktarılması ya da en genel ifadesiyleişlenmesi kaçınılmazdır ve pek çok noktada gereklidir.Ancak bu uygulamaların keyfi olması, kişininsürekli olarak izlenme tehlikesini hissetmesi benzersizkişiliğini özgürce geliştirmesinde engel oluşturacakve bireysel özerkliğin yitimi gibi temeldeinsan onuruna yönelik ciddi bir saldırının oluşmasınaneden olacaktır. Bu noktada kişisel verilerin korunması hakkı,bireye kişisel verilerinin hukuka aykırı olarak sınırsızbir şekilde kaydedilmesi, işlenmesi, paylaşılmasıkarşısında temel bir hak vermektedir. Böyleliklebireye verilerinin kullanılması üzerinde karar vermehakkını tanır. Bu tehlikeleri bertaraf etmek vesözünü ettiğimiz dengeyi sağlayabilmek için kişiselverilerin korumasına ilişkin hukuksal düzenlemelerde, bazı temel ilkelerin kabul edildiğini görüyoruz. Kişisel verilerin hukuka ve dürüstlük kurallarınauygun işlenmesi, verilerin toplanma amacının meşru, açık ve belirli olması, amacın gerektirdiğinden dahauzun süre tutulmaması, ilgilinin rızasının bulunması, veri güvenliği gibi ilkeler bu kapsamda sayılabilir.

**KİŞİSEL VERİLERİN KORUNMASI HAKKI**

Kişisel verilerin korunması özel yaşamın gizliliği yakından ilişkilidir. Ayrıca, kişisel verilerin korunması; düşünceyi açıklama özgürlüğü, bilgi edinme hakkı, haberleşme özgürlüğü gibi başka bazı değerlerle de kimi zaman karşılıklı destekleme, kimi zaman çatışma halindedir. Bireyin özel yaşamının gizliliği hakkının temel amacı, duygusal ve psikolojik yapısını kişisel bilgilerinin istenmeyen şekilde yayılmasını önleyerek korumaktır ve hiçbir zaman, bilginin yasal adını tanımlamak ya da ticarî kullanım hakkına kimin sahip olduğunu belirlemek için bir araç olarak düşünülmemiştir. Oysa bunlar, mülkiyet hukukunun temel işlevlerini oluşturur. Nitekim günümüzde kişisel verilerin korunmasının temel bir insan hakkı olduğu yönünde şüphe bulun mamaktadır. Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi (m.17), BM Bireysel ve Siyasal Haklar Şartı (m.12), Avrupa İnsan Hakları Sözleşmesi (m.8) gibi pek çok önemli insan hakları metninde özel yaşamın gizliliği temel bir insan hakkı olarak kabul edilmiştir. Bunun yanında Avrupa Birliği Temel Haklar Şartı ve başka belgeleri, çeşitli devletlerin anayasaları gibi daha yeni bazı metinlerde kişisel verilerin korunması hakkının, özel yaşamın gizliliği hakkından bağımsız olarak da temel haklar kataloğu içerisinde yer aldığı görülmektedir. Kişisel verilerin korunması hakkı, yalnızca kişisel çıkarların korunması ile ilişkili değildir. Kişisel verilerin korunması hakkı, insan onuru ve temel özgürlükler gibi çok daha geniş bir alana hizmet etmektedir İnsan Onuru, Bireysel Özerklik ve Bilgilerin Geleceğini Belirleme Hakkı Kişisel verilerin korunması, günümüz bilişim teknolojileri karşısında kişisel bilgileri sınırsız bir şekilde toplanan, kullanılan, devredilen bireyin korunmasını amaçlamaktadır. Bu bağlamda kişisel verilerin korunması hakkının ilk olarak insan onuru ve bu kapsamda kişiliğin serbestçe geliştirilmesi hakkına dayandırıldığı görülür. Nitekim Federal Almanya Anayasa Mahkemesi 1983 yılında verdiği ve etkisi ülke sınırlarını aşan, Nüfus Sayımı kararında bu duruma işaret etmiştir. Almanya Anayasa Mahkemesinin henüz veri işleme süreçlerinin yeni yeni geliştiği bir dönemde birey aleyhine bozulan dengeyi saptayarak, bu dengenin yeniden kurulmasının gerekliliklerini titizlikle ortaya koymasıdır. 1983 yılında memurların kapı kapı dolaşarak yapacakları sayımda yurttaşların sayılmasından başka bilgilerin edinilmesi de hedeflenmişti ve yurttaşlara kapsamlı bilgileri açıklama yükümlülüğü getirilmekteydi. Bu yükümlülüğü yerine getirmeyenler için ise yaptırım öngörülmüştü. Alman Anayasa Mahkemesi kararında Alman Temel Yasasının (Grundgesetz) insan onurunun ve kişiliğin korunması hakkına ilişkin hükümlerini temel almıştır. Ayrıca bu hükümlerden hareketle yeni bir hakkı: “bilgilerin geleceğini belirleme hakkı”nı (informationalle Selbstbestimmung) türetmiştir. Özel Yaşamın Gizliliği Hakkı Kişisel verilerin korunması hakkı, çoğunlukla özel yaşamın gizliliği hakkı kapsamında değerlendirilmektedir. Ancak gelişen teknoloji, özel yaşamın gizliliği hakkına geleneksel yaklaşımla ve bu alanda benimsenen ilkelerle verilerimiz korunmasında yetersiz kalmaktadır. Bu nedenle tarihsel süreç içerisinde kendisinden daha köklü bir hak alanı olan özel yaşamın gizliliği hakkından ayrılmaya başlamıştır. ABD, Yeni Zelanda, Avustralya, Kanada gibi ülkelerde konuya ilişkin tartışmaların özel yaşamın gizliliği (privacy) başlığı altında yapılması da bunun bir göstergesidir. Bunun yanında Avrupa’da da konuyu değerlendirirken özel yaşamın gizliliği hakkını dikkate almak gerekmektedir. Bunun önemli bir nedeni 1950 yılında kabul edilen 1953 yılında yürürlüğe giren Avrupa İnsan Hakları Sözleşmesinde kişisel verilerin korunmasından söz edilmemesidir. Aslında bu, Sözleşmenin kabul edildiği tarih dikkate alındığında son derece normaldir. Nitekim önceki açıklamalarda da işaret edildiği üzere kişisel verilerin korunması 1970’li yıllardan sonra hukuksal düzenlemelerin konusu olmuştur. Ancak Avrupa İnsan Hakları Mahkemesi kişisel verilerin korunmasını Sözleşmenin özel yaşamın gizliliği hakkını düzenleyen 8. Maddesi kapsamında değerlendirmektedir. Mahkemenin bu alanda gelişkin bir içtihadı olduğunu şimdiden belirtmek gerekir. Bu bağlamda AİHM, muhtemelen AİHS’nin hazırlayıcılarının aklında olmayan belge eşleştirme, kişisel verilere yetkisiz ulaşım, verilerin gereğinden uzun süre sistemlerde tutulması, DNA profillerinin değerlendirilmesi gibi kişisel verilerin korunması hakkı kapsamında incelenen alanlara özel yaşamın gizliliği hakkına ilişkin ilkeleri uygulamıştır. Benzer şekilde BM İnsan Hakları Komitesi de 1988 yılında yayınlanan yorumunda kişisel verilerin korunması hakkına ilişkin temel ilkelerin BM Bireysel ve Siyasal Haklara İlişkin Uluslararası Sözleşmesinin özel yaşamı korumaya ilişkin 17. maddesi çerçevesinde değerlendirilmesi gerektiğini belirtmiştir. Buna karşılık yine aynı coğrafyada hazırlanmış olan çok önemli, fakat daha yeni bir metinde: Avrupa Birliği Temel Haklar Şartı’nda özel yaşamın gizliliği ile kişisel verilerin korunması farklı maddelerde ayrı ayrı hüküm altına alınmıştır. Şartın 8. Maddesi “Kişisel verilerin korunması” kenar başlığı ile şu düzenlemeyi içermektedir:

(1) Herkes, kendisini ilgilendiren kişisel verilerinin korunması hakkına sahiptir.

(2) Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve düzelttirme hakkına sahiptir.

(3) Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir.

Özel yaşamın gizliliği hakkı, hemen hemen bütün devletlerin anayasalarında temel bir hak olarak belirlenmiştir. Özel yaşamın tanımlanması güç ve hatta olanaksızdır. Konuya ilişkin hemen hemen bütün eserler ve mahkeme kararları bu soruna işaret eder. Pek çok kişi, özel yaşamın ne olduğunu algılayabilir, ancak bunu kelimelere dökmeye zorlanır. Şöyle de ifade edilebilir: özel yaşam, tanınması kolay, tanımlanması güç bir olgudur. Özel yaşam üç grupta toplanabilir. “Genel yaşam alanı” olarak adlandırılabilecek dış çember, kişinin herkesle paylaşabileceği, kamuya açık yaşam alanlarını içerir. İkinci olarak “kişinin özel yaşam alanı”, belirli kimselerle ve belirli ölçüde paylaştığı yaşam parçalarını kapsar. En içte kalan “sır alanı” ise kişinin yalnızca kendine saklamak istediği alanı oluşturur ve özel yaşam içinde değerlendirilir. Nitekim kişinin sır alanı içerisinde yer alan, cinsel yaşamı, dinsel tercihleri, ırksal kökeni gibi konulara ilişkin veriler, hassas veri olarak kabul edilmekte ve daha özel bir korumaya tabi tutulmaktadır. Kişinin özel yaşam alanına müdahale ise ağırlıklı bir kamu yararının varlığı halinde söz konusu olabilir ve bu durumda da belirli ilkelere uygun hareket etmek bir zorunluluktur. Kişinin özel yaşam alanı içerisinde yaptığı konuşmaların kayda alınması ya da telefonlarının dinlenmesi bu kapsamda incelenebilir. Bunun yanında “genel yaşam alanı” olarak adlandırılan dış çemberde de birey korumasız değildir. Kişisel verilerin korunmasına ilişkin temel ilkelere bu alanda da uyulmalıdır. Kişinin kamuya açık yaşam alanında verilerinin toplanması, örneğin video ya da ses kaydının alınması ile söz konusu olabilir. Kapalı devre televizyon (CCTV) sistemleri ile kayıt altına alınan görüntülerin kişisel verilerin korunması açısından önemli tartışmalara neden olması da bundandır. Özel yaşamın gizliliğine duyulan gereksinim, yalnızca kişilerin gizlemek isteyebilecekleri ya da onları utandırabilecek bilgiler çerçevesinde de düşünülmemelidir. Bireylerin, özel olarak utanç duymalarını ya da gizlemelerini gerektirmeyecek durumlarda, bunlar yalnızca “başkalarını ilgilendirmediği” için kişilerin özel yaşamlarını gizli tutma hakları bulunmaktadır. Evli bir çiftin cinsel yaşamına ilişkin son derece sıradan bilgilerin başkaları tarafından öğrenilmesini istememesi ya da mali bazı bilgilerin kendisine herhangi bir şekilde zarar vermeyecek de olsa kendisine saklaması buna örnek olarak gösterilebilir. Rachels’a göre bir “özel yaşamın gizliliği duygusu”na sahibiz ve bu duygu çıkarlarımızın zedelenmesi ya da utanma korkumuzla açıklanamaz. Ona göre, özel yaşamın gizliliğinin asıl değeri, bize ve bizim hakkımızdaki bilgilere kimin ulaşabileceğini denetleyebilmemizle farklı kişilerle farklı ilişkiler kurabilme yeteneğimiz arasındaki ilişkide kendini bulmaktadır. Gerçekten bir kişi, çocuğuyla, eşiyle, patronuyla, çalışanıyla ya da çeşitli arkadaşlarıyla farklı kimliklerle ilişki kurar. Kimileri bunu sosyal ilişkilerde taktığımız çok çeşitli maskelerle “gerçek” kişiliğimizi gizlememizle açıklamaktadır. Ancak Rachels bu düşünceye aslında sosyal ilişkilerde takındığımız bütün rollerin en az diğerleri kadar “gerçek” olduğu düşüncesiyle karşı çıkmaktadır. Görüldüğü gibi özel yaşamın gizliliği hakkı, dolayısıyla kişisel verilerin korunması hakkı kaynağını öncelikle insan onuru, kişilik hakkı ve bireysel özerklikte bulmaktadır. Bunun yanında kişisel verilerin korunması pek çok başka hak ve özgürlükle de ilişkilidir. Bu ilişki kimi zaman çatışma, kimi zaman ise kesişme ve birbirini tamamlama şeklinde kendini gösterir.

**Düşünceyi Açıklama Özgürlüğü**

Düşünceyi açıklama özgürlüğü, “insanınserbestçe düşünce ve bilgilere ulaşabilmesi, edindiğidüşünce ve kanaatlerden dolayı kınanması ve bunlarıtek başına ya da başkalarıyla birlikte (dernek,toplantı, sendika vb.) çeşitli yollarla (söz, basın, sinema,tiyatro vb.) serbestçe açıklayabilmesi, savunabilmesi,başkalarına aktarabilmesi ve yayabilmesianlamına gelir”Düşünceyi açıklamaözgürlüğü, bu kapsamda özgürce yayın yapan kitleiletişim araçları olmadan açık ve aydınlanmış birtoplumdan söz edilemez. Ancak Immanuel Kant’ında belirttiği gibi, sorumlulukla özgürlüğü birbirinebağlamak gerekir. Bu nedenle düşünceyi açıklamaözgürlüğünün belirli sınırları olduğu kabuledilmektedir. Bu sınırlardan biri de kişisel verilerinkorunması hakkının da temel dayanaklarındanolan kişiliğin geliştirilmesine ilişkin ilkelerdir. Nitekimdüşünceyi açıklama özgürlüğü, demokratikbir toplumun eksen özelliklerinden biri olsa da,bu özgürlük, “Bireylerin öğrenmek istedikleri herşeyi bilme hakkı olduğu anlamında yorumlanamaz.”

Kişisel verilerin korunması hakkı, düşünceyi açıklama özgürlüğü ile çatışma potansiyeli taşımaktadır. Böylesine bir çatışma özellikle düşünceyi açıklama özgürlüğü içerisinde değerlendirilen basın özgürlüğü açısından kendini gösterir. Bu durum özellikle magazin basını ya da renkli basın olarak adlandırılan yayınlar açısından söz konusudur. Bu tür yayınların toplum üzerindeki etkileri sosyologlarca araştırılan bir konudur. Amerikan hukukunda “kamusal figür” olarak nitelenen ve kapsamında politikacılardan, eğlence sektöründe çalışanlara, yöneticilerden, sporculara kadar oldukça geniş bir kesimi barındıran kategorinin bu anlamda, özel yaşamın gizliliği hakkını daha sınırlı oranda ileri sürebileceği kabul edilmektedir. Buradaki temel dayanak, bu kişilerin kendi istekleri ile kamunun gözü önünde bulunmalarıdır O halde düşünceyi açıklama ve basın özgürlüklerinin kullanımının kimi zaman kişisel verilerin korunması hakkına bir müdahale yaratabileceği açıktır. Diğer yandan kişisel verilerin korunması hakkının düşünceyi açıklama ve basın özgürlüklerinin gereği gibi kullanımında bir engel oluşturabildiği yönünde eleştiriler de söz konusu olabilir. Bu durumda her bir olayda tartım ve değerlendirme yapılmalı ve somut olayın kendisine özgü koşulları içinde hangisine ağırlık verileceği saptanmalıdır. Kişisel verilerin korunmasına ilişkin çeşitli düzenlemelerde “eğer gerekli” ise düşünceyi açıklama özgürlüğün korumak için istisna getirilebileceğine dair hükümler yer alır. Buradaki “gereklilik” koşulu her devletin olayın kendine özgü koşullarına uygun bir değerlendirme yapması ile açıklık kazanacaktır. Aynı şekilde düşünceyi açıklama özgürlüğüne ilişkin çeşitli düzenlemelerde doğrudan kişisel verilerin korunmasına atıf yapılmasa da kişisel hakların korunmasının hakkın sınırları arasında yer aldığı görülmektedir. Verilerin korunması hakkı ile düşünceyi açıklama özgürlüğü arasında kaçınılmaz bir gerili bulunsa da her iki hakkın bir arada gerçekleşmeyeceğine dair herhangi bir neden bulunmamaktadır. Şöyle söylenebilir; veri koruma ve düşünceyi açıklama özgürlüğü arasında temel bir çatışma yoktur, ancak her iki hakkın da diğeri karşısında dengelenmesi gerekir. Bunun yanında her iki hak ve özgürlüğün birbirlerini desteklediği alanlar da bulunmaktadır. Düşünceyi açıklama özgürlüğü ile bireyin açıklamalarının içeriğini ve muhatabını belirleme hakkı güvence altına almaktadır. Bu ise bireyin kişisel verileri üzerindeki belirleme hakkının bir öğesidir. Aynı durum tam tersi için de söylenebilir. Yani kişisel verilerin korunması hakkı ile düşünceyi açıklama özgürlüğü korunur. Çünkü bu hak kapsamında, insanlar düşüncelerini kiminle ne zaman, nerede, paylaşacaklarını seçebilirler.

**Özel Haberleşmenin Gizliliği**

Özel haberleşmenin gizliliği ile kişilerin telefon, telgraf, mektup, elektronik posta gibi araçlarla gerçekleştirdikleri özel iletişiminin gizliliğini ve güvenilirliğini korumak hedeflenmektedir. Özel haberleşmenin gizliliğinde ilke, bireyin dilediği kişilerle dilediği şekilde haberleşmesinin engellenmemesi ve bu haberleşmelerin ilgilinin onayı ya da yasal gereklilik olmaksızın üçüncü kişilerin müdahalesinden korunmasıdır. Nitekim özel yaşamın korunmasına ilişkin Avrupa İnsan Hakları Sözleşmesi’nin 8. ve Bileşmiş Milleler Evrensel İnsan Hakları Beyannamesi’nin 12. Maddelerinde haberleşmenin gizliliği hakkından da söz edildiği görülür. Ancak önemi nedeniyle pek çok ulusal ve uluslararası düzenlemede haberleşmenin gizliliğine ilişkin özel hükümler de getirilmiştir. Hızla gelişen İnternet ve benzeri teknolojiler sayesinde bireyler, yazdıkları metinleri çok daha hızlı, kolay ve ucuz bir şekilde ilgililerine ulaştırabilmekte, her geçen gün biraz daha yaygınlaşan cep telefonları ile sesli ve hatta görüntülü konuşmaları gerçekleştirebilmektedir. Elektronik posta ve telefon hizmetlerinin yaygınlığı neticesinde telgraf ya da geleneksel yazılı posta ile haberleşme her geçen gün biraz daha az başvurulan yollar olmaktadır. Bu, günümüzde iletişimin büyük oranda sayısal hale geldiğinin de göstergesidir ve sayısal iletişime müdahale, geleneksel iletişim araçları ile karşılaştırıldığında daha kolaydır. Geleneksel posta yoluyla gönderilen bir mektubun içeriğine ulaşmak için üzerinde fiziksel bir müdahalede bulunmak gerekirken, e-postada bu hedef dünyanın öbür ucundan gerçekleştirilebilmektedir. Hukuka aykırı bir şekilde dinleme ya da kaydetme ile kişisel verilerin elde edilmesi hem özel haberleşmenin gizliliğinin, hem de kişisel verilerin korunması hakkının ihlali anlamına gelmektedir. Bu noktada iletişimin doğrudan içeriğinin, bir başka ifade ile “ne” konuşulduğunun değil, telefon aramaları ya da posta gönderimleri kayıtlarının, yani “kiminle”, “ne sıklıkla” ve “ne kadar süreyle” konuşulduğunun merkezi önemde olduğu görülür. Unutulmaması gerekir: Çoğu zaman iletişimin şekli ve bu bağlamda iletişim trafiğinin analizi, en az içeriği kadar önemlidir. Örneğin II. Dünya savaşı sırasında Naziler trafik analizini, gözaltındaki kişilerin telefon faturalarını inceleyerek, iletişim halinde bulundukları kişilerin tespiti için kullanmışlardır. Burada asıl ilgilendikleri, ne konuşulduğu değil, kiminle konuşulduğudur.

**Diğer Bazı Hak ve Özgürlükler**

Özellikle, “hassas kişisel veriler” olarak adlandırılan ve özel koruma gerektiren bazı veri türlerinin, kökenleri oldukça eskiye dayanan bazı ilkelerle korunduğu görülmektedir. Hassas kişisel verilerin özel olarak korunmasında hareket noktası, bu verilerin hukuka aykırı ve keyfi bir şekilde toplanmasının, saklanmasının, işlenmesinin ve yayılmasının doğurabileceği zararın daha büyük olduğu düşüncesidir. Bu noktada ilk akla gelen “ayrımcılık yasağı” dır. Kişilerin ırkları, etnik kökenleri, cinsel tercihleri dolayısıyla bu kimselere ayrımcılık yapılamayacağı ilkesi, insan haklarının eksen kavramlarından “eşitlik”in bir gereğidir. Bu ilke, pek çok devlette anayasal düzeyde korunmaktadır. Özellikle genetik araştırmaların hız kazanması ve kişilerin genetik yapılarına ilişkin bilgilerin toplandığı gen bankalarının kurulması ile ayrımcılık yasağının yeni bir boyutta tartışılmaya başlandığını da belirtmek gerekir. Hassas veriler kapsamında değerlendirilen önemli bir hak kategorisi de kişilerin dinsel inançlarına ilişkin verilerdir. Din ve inanç özgürlüğü, kişisel verilerin korunması hakkının tartışılmaya başlanmasından çok daha eskilere dayanan bir geçmişe sahiptir. Din ve inanç özgürlüğünün kapsamında dinini açıklamaya zorlamama da yer alır. Gerçekten kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağı konuya ilişkin pek çok metinde de belirtilmiştir. Böylece inanç ve kanaate öğrenme biçiminde bile olsa müdahale edilemeyeceği saptanmıştır (Kaboğlu, 2002). Bu bağlamda din ve inanç özgürlüğü ile kişisel verilerin korunması hakkının birbirinin desteklediği söylenebilir. Bunun yanında örneğin sağlık verilerinin gizli tutulması, hekimin sır saklama yükümlülüğü hasta-hekim arasındaki ilişkinin bir gereği olarak binlerce yıldır kabul edilen bir gerekliliktir. Hipokrat yemininde de yer alan bu ilke, sağlık hizmetlerine ilişkin pek çok ülkedeki yasal düzenlemelere de yansımıştır. Ancak bu temel hak ve özgürlüklerin kişisel verilerin korunmasına katkısı oldukça sınırlıdır: Ayrımcılık yasağı, kişilerin hangi etnik kökene, dinsel gruba dahil olduklarının ya da cinsel tercihlerinin, genetik yapılarının ne olduğunun kayıt altına alınmasını değil, bu bilgilerden hareketle farklı işlem görmelerini önlemeyi amaçlamaktadır. Sağlık verilerine ilişkin hekimlerin ulaştıkları bilgileri gizli tutmaları gerekliliği de kişisel verilerin korunması hakkı kapsamında yer alan ilkelerin yalnızca birinin güvencesini oluşturur. Bunun gibi din ve inanç özgürlüğünün getirdiği koruma da bu konudaki verilerin işlenmesi karşısında zayıf kalmaktadır. Kişisel verilerin korunmasına yönelik yasal düzenlemenin yokluğunda bunlar ve benzeri diğer ilkeler sınırlı da olsa bir koruma sağlamaktadır. Ancak tam bir güvence için kişisel verilerin korunması hakkının tanınması gerekir. Ayrıca bu güvence yukarıda belirtilen diğer hak ve özgürlüklerin de etkin bir şekilde sağlanmasına hizmet edecektir.

**KİŞİSEL VERİLERİN KORUNMASINDA HÂKİM OLAN TEMEL İLKELER**

Kişisel verilerin korunması hukukunun normatif temelini oluşturan özel yaşamın gizliliği hakkı, pek çok önemli insan hakları metninde güvence altına alınmıştır. Birleşmiş Milletler Evrensel İnsan Hakları Bildirisi, Birleşmiş Milletler Uluslararası Bireysel ve Siyasal Haklar Sözleşmesi, Avrupa İnsan Hakları Sözleşmesi ve Amerikalılar Arası İnsan Hakları Sözleşmesi gibi metinlerde yer alan özel yaşamın gizliliği hakkı, kişisel verilerin korunmasının hedef ve ilkeleri ile yakından ilişkilidir. Bunun yanında uluslararası alanda doğrudan kişisel verilerin korunmasına hasredilmiş metinler de bulunur. İlk veri koruma düzenlemelerinin yasalaşmasından kısa bir süre sonra, verilerin sınır ötesi aktarımında sorun yaşanmaması için ulusal yasaların uyumlaştırılması gereksinimi ortaya çıkmıştır. Bu doğrultuda 1980’li yılların başından itibaren verilerin korunması açısından yeni bir döneme girildiği söylenebilir. OECD, Birlemiş Milletler, Avrupa Konseyi, APEC gibi uluslararası kuruluşlar, kişisel verilerin korunmasına ilişkin temel ilkeleri ve verilerin sınır ötesi aktarımını düzenleyen metinler kabul etmiştir. Bu metinler, hem ulusal hukuklarda genel olarak geçerli olan veri koruma ilkelerini belirlemektedir, hem de konuya ilişkin ulusal ve uluslararası girişimlerde örnek oluşturarak, veri koruma hukukunun gelişimini etkilemektedir. Kişisel verilerin korunmasında etkili metinler kabul eden bir diğer önemli kuruluş ise Avrupa Birliği (AB) dir. Avrupa’daki düzenlemelerin dünyanın çok çeşitli bölgelerinde konuya yaklaşımı etkilediği söylenebilir. Konuya yönelik gelişkin bir mevzuata sahip olması bir yana, bu etkinin bir diğer nedeni ise AB’nin kişisel verileri “yeterli” oranda korumayan devletlere veri aktarımını yasaklamasıdır. Konuya ilişkin uluslararası metinlerin bir bölümü devletlere, belirlenen ilkeleri iç hukuklarına aktarım hususunda takdir yetkisi tanımaktadır. Örneğin OECD ve Birlemiş Milletler’in Rehber İlkeleri bağlayıcı değildir. Avrupa Konseyi Veri Koruma Sözleşmesine taraf olan devletlerin ise metinde yer alan ilkeleri iç hukuklarının bir parçası haline getirmesi gerekir. Öte yandan AB kişisel verilerin korunmasına ilişkin ilkeleri yönergeler (direktifler) ile belirlemiştir. AB üyesi devletler bu yönergelere uygun ilkeleri iç hukuk sistemlerinde benimsemek zorundadırlar. Hali hazırda gündemde olan AB Veri Koruma Reform Paketi’nin yürürlüğe girmesi halinde bu yaklaşım değişecek ve AB düzenlemeleri-iç hukukta ayrıca bir yasa çıkarmaya gerek kalmaksızın-AB Devletlerinde doğruda uygulama gücüne kavuşacaktır. Kişisel Verilerin Niteliğine İlişkin İlkeler Kişisel verilerin korunmasına ilişkin pek çok hukuksal metinde, işleme sırasında belirli bir niteliğin karşılaması gerektiğine yönelik ilkeler belirlenmiştir. “Verilerin kaliteli olması ilkesi” olarak da ifade edilebilecek bu gerekliliğin içeriği beş alt başlıktan oluşur:

• Hukuka ve dürüstlük kurallarına uygun işleme

• Belirli, açık ve meşru amaçlar için toplanma

• Toplanma ve sonrasında işlenme amaçlarına uygun, ilgili olma, aşırı olmama

• Doğru ve eğer gerekli ise güncel olarak tutulma

• Amacın gerektirdiğinden daha uzun süre tutulmama

Hukuka uygun olma gerekliliği kişisel verilerin işlenmesinde yasalarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade eder. Dürüstlük kuralına uygun olma ilkesi ile veri işleyenleri bu süreç boyunca ilgilinin çıkarlarını ve makul beklentilerini dikkate alma gereğini ifade eder. Bunun yanında kişisel veriler toplanırken amacın açık olması ve hukuk sisteminde benimsenen meşru bir temele dayanması son derece önemlidir. Bu durum daha sonraki aşamalarda verinin başka amaçlarla işlenmesini önleme ve bu noktada bir hukuka aykırılık söz konusu olursa onu saptama açısından da önemlidir. Amacın gerektirdiğinden daha fazla verinin toplanmaması ve gerekli olan süre kadar tutulması ise kişisel verilerin korunması açısından kritik öneme sahiptir. Kişinin Katılımı ve Denetimine Yönelik İlkeler İlgili kişinin katılım ve denetimine yönelik ilkeler çok çeşitlidir. Bu kapsamda kişiye bazı haklar tanındığı, veri işleyenlere ise yükümlülük yüklendiği görülür. Bu hak ve yükümlülüklere örnek olarak şunlar verilebilir:

• İlgilinin bilgilendirilmesi

• İlgilinin kendisine ilişkin bilgilere erişim hakkı

• İlgilinin kendisine ilişkin bilgileri düzeltme hakkı

• İlgilinin veri işlemeye itiraz hakkı

• İlgilinin otomatik kararların konusu olmama hakkı

Kişisel verilerin korunması hukuku kapsamında, ilgili kişiye, sürece çeşitli aşamalarda müdahale etme olanağı tanıyan bazı haklar verilmiştir. Kişisel verilere erişim hakkı, verilerin düzeltilmesini isteme hakkı ve bazı durumlarda veri işlemeye itiraz hakkı bu kapsamda sayılabilir. Bunlar, ilgili kişinin verileri üzerinde denetim sağlamasına hizmet eder. İlgili kişinin katılımı ve denetimine yönelik ilkeler, Alman Anayasa Mahkemesinin ifadesiyle “bilgilerin geleceğini belirleme hakkı”nın sağlanması için gereklidir. Bireyin aktif konumda olduğu bu hakların yanında, yine ilgili kişinin verileri üzerindeki denetimini sağlamak amacıyla veri işleme süreçlerinde yer alan kişilerin de bazı yükümlülükleri bulunur. Bunlardan ilk akla gelen kuşkusuz ilgilinin bilgilendirilmesi zorunluluğudur. İlgilinin otomatik kararların konusu olmama hakkı ise bireysel özerklik ile ilişkilidir. Burada temel olarak, her bireye kendisine yönelik hukuksal sonuçlar yaratan, kendisini önemli ölçüde etkileyen konularda; işindeki performansı, kredi itibarı, güvenilirliği, davranışları gibi kişisel durumların değerlendirilmesi amacıyla yalnızca otomatikleştirilmiş veri işlenmesine dayanan bir karara tabi olmama hakkı tanınmaktadır. Bir başka anlatımla kişinin geleceğine bilgisayarların karar vermesi önlemek istenmektedir.

**Özel Kategorideki Verilerin Nitelikli Korunması**

Bu ilke ile ilgili kişi açısından “hassas” sayılan bazı veri türlerinin daha güçlü bir şekilde korunması hedeflenmektedir. AB Yönergeleri, AK Sözleşmesi, BM Rehber İlkeleri gibi pek çok uluslararası metinde ve ulusal düzenlemelerde hassas verilerin özel olarak korunması yaklaşımı benimsenmiştir. Bu kategoride yer alan veri türleri bazı farklılıklar gösterse de genel olarak ilgili kişinin,

• ırksal veya etnik kökenine,

• siyasal görüşüne,

• dinsel ya da felsefi inancına,

• sendika üyeliğine,

• sağlık ya da cinsel yaşamına ilişkin bilgiler bu kategoride sayılmaktadır.

Bu bilgilerin işlenmesi kural olarak yasaktır, ancak bazı sınırlı durumlarda ve veri koruma ilkelerini güçlü bir biçimde uygulayarak işlenmeleri olanaklıdır. Bu bilgi kategorilerinin diğerlerine göre daha hassas nitelikte olduğu düşünülmektedir. Buradaki temel kaygı ise güçlü veri koruma ilkelerinin uygulanmadığı bir ortamda bu bilgilerin işlenmesi dolayısıyla kişilerin ayrımcılığa uğrama olasılığının diğer bilgi türlerine göre daha yüksek olmasıdır.

**Veri Güvenliğinin Sağlanması**

Kimi yerlerde veri güvenliğinin veri korumayı niteleyecek şekilde, sanki her iki kavram eş anlamlıymış gibi kullanıldığı görülmektedir. Oysa her ikisi arasında açık bir ayrım bulunur. Verilerin korunması, “veri”lerin değil, bu verilerin ilişkili olduğu gerçek kişilerin korunmasına yönelmiştir. Veri güvenliği ise doğrudan verilerin korunmasını hedefler. Bu açıdan amaç, kişilerin değil, verilerin korunmasıdır. Ancak bu veriler, kişilerle ilgili olduğu ölçüde, veri güvenliği, kişisel verilerin korunmasına da hizmet edecektir. Kişisel verilerin korunmasına ilişkin pek çok hukuksal düzenlemede veri güvenliğinin temel ilkeler arasında yer alması da bu nedenledir. Veri güvenliği ilkesi çerçevesinde kişisel verilerin;

• kazara veya hukuka aykırı tahribine,

• kaybolmasına,

• değiştirilmesine,

• yetkisiz yayımı veya erişimine ve bunlara benzer diğer güvenlik açıklarına karşı teknik ve örgütsel önlemleri alması öngörülmektedir.

Bir bankaya parasını yatırmayı, sigorta şirketiyle sözleşme yapmayı ya da tanı ve tedavi için bir sağlık kuruluşuna başvurmayı düşünen kişi verilerinin güvende olduğunu bilmek isteyecektir. Bu konuda endişe duyması halinde ise belirtilen hizmetleri almamayı tercih edebilir. Bunun ilgili kişi açısından yaratacağı sorunlar yanında, kurumun ekonomik kaybına neden olacağıda açıktır. Bu durum, veri güvenliğinin ekonomik olarak ölçülebilir çıkarları da güvence altına aldığını ortaya koymaktadır.

**Bağımsız Organlarca Denetim**

Kişisel verilerin korunması öncelikle bu ilkelerle uyumlu pratiklerin gelişmesiyle olanaklıdır. Bireylerin haklarını, veri işleyenlerin yükümlülüklerini bilmesi gerekir. Ancak pek çok örnek göstermiştir ki bu ilkelerin yalnızca kâğıt üzerinde tanınması hedefe ulaşılabilmesi için yeterli değildir. Belirtilen ilkelere uygun davranmaya zorlayan, bunların ihlal edilmesi durumunda yaptırım öngören ve bireylerin şikâyetlerini dile getirebildikleri, zararlarını tazmin edebildikleri bir sistemin oluşturulması da gerekir. Kişisel verilerin korunmasının uluslararası kaynaklarında genel olarak bu türdeki güvencelere yer verilmediği ya da sınırlı olarak değinildiği görülür. Ancak özellikle AB düzenlemeleri bu ilkelerin yaşama geçmesi konusunda denetim sağlayan bağımsız bir organının varlığını öngörmektedir. Bu bağımsız kurum ve kişilerin ilkelere uygun hareket edip etmediğini denetleyecek ve böylelikle henüz zarar ortaya çıkmadan önleyici koruma sağlayacaktır.

Bağımsız organın bir diğer önemli görevi ise veri koruma alanında farkındalık arttırmaya yönelik çalışmalar geliştirmesidir. İstisnalar ve Sınırlamalar Kişisel verilerin korunması hakkı, sınırsız bir hak alanı değildir. Yukarıda incelenen temel ilkelere belirli durumlarda istisna getirilmesi olanaklıdır. Bu, her şeyden önce buradaki temel hakkın göreceli yapısından kaynaklanır. Hem diğer hak ve özgürlüklerle hem bireysel ya da kolektif olarak başkalarının hak ve özgürlükleriyle dengeli bir yaklaşım benimsenmelidir. Bu denge ise ancak yukarıda incelediğimiz temel ilkelere belirli durumlarda istisna ve sınırlamaların getirilmesi ile olanaklıdır. Nitekim kişisel verilerin korunmasına hâkim olan temel ilkelere yönelik sınırlama ve istisnalar konuya ilişkin bütün belgelerde yer alır. Bu açıdan örneğin kişisel verilerin işlenmesi, yalnızca gazetecilik amacıyla veya sanatsal ya da edebi açıklamalar için söz konusu olduğunda sınırlandırılabilir ve istisnalar getirilebilir. Konuya ilişkin AB Yönergesi uyarınca, bazı durumlarda verinin niteliğine ilişkin ilkelere, ilgili kişinin bilgilendirilme hakkına, erişim hakkına, işleme eyleminin kamuya ilan edilmesine sınırlandırma getirilebilir. Ancak bu yalnızca ulusal güvenlik, savunma; kamu güvenliği, suçların ya da düzenlenmiş etik kuralların ihlalinin önlenmesi, araştırılması, soruşturulması ve kovuşturulması, ilgili kişinin veya diğerlerinin hak ve özgürlüklerinin korunması gibi konular amaçlarla gerçekleştirilebilir. Görüldüğü gibi kamu çıkarının ağır bastığı bazı durumlarda kişisel verilerin korunmasına yönelmiş ilkelere istisna getirilmesi olanaklıdır. İstisnaları oluşturan kavramların sınırları belirsizdir. Bu nedenle istisna ve sınırlamaların geniş yorumlanması kişisel verilerin korunması ilkelerinin özüne zarar verebilir. Ancak temel hak ve özgürlüklere ilişkin bütün metinlerde olduğu gibi burada da sınırlamaların dar yorumlanması gerektiği unutulmamalıdır.

Burada altı çizilmesi gereken husus, kişisel verilerin korunmasının temel bir insan hakkı olduğudur. Bu nedenle temel hak ve özgürlüklerin sınırlanmasına ilişkin ilkeler burada da uygulanacaktır. Avrupa İnsan Hakları Sözleşmesinde ve demokratik devletlerin Anayasalarında temel hak ve özgürlüklerin ancak yasa ile sınırlandırılabileceği ilkesi benimsenmiştir. Bunun yanında ölçülülük ilkesine uygun olarak, meşru amacın gerektirdiğinden daha yüksek oranda sınırlama getirilmemesi gerekir. Kişisel verilerin korunmasına istisna getiren hükümlerin açık ve öngörülebilir olması ve belirlenen amacın aşılmaması da oldukça önemlidir. Aksi takdirde hukuk devleti ile bağdaşmayacak keyfi uygulamalarla karşılaşılabilir.

**UNITE 3**

**GİRİS**

2011 yılında yayınlanan bir araştırma, Kuzey Amerika’dan sonra dünyada İnternet’in en yaygın kullanıldığı bölge olan Avrupa’da yurttaşların veri işleme uygulamaları dolayısıyla endişeli olduklarını ortaya koymuştur. Avrupa Komisyonu tarafından yayınlanan bu araştırma uyarınca Avrupa Birliği yurttaşlarının %74’ü kişisel verilerin açıklanmasını modern yaşamın artan bir parçası olduğunu düşünmektedir. Ayrıca Avrupalıların çoğunluğu davranışlarının ödeme kartları, cep telefonları ya da mobil İnternet aracılığıyla kayıt edildiğinden endişe etmektedir. Türkiye’de kişisel verileri dijital ortamda toplayan, kayıt eden, birbirleri ile ilişkilendiren ve üçüncü kişilere aktaran sistemler yaygın bir biçimde kullanılırken bu kullanımdan kaynaklı önemli “yan etkileri” ortadan kaldırmaya yönelik olan kişisel verilerin korunması alanında hukuksal düzenlemelerin yetersiz olduğu belirtilmelidir. 2013 yılında Türkiye Cumhuriyeti Devlet Denetleme Kurulunun (DDK) yayınladığı bir raporda, artan veri işleme süreçleri karşısında kişisel verilerin korunması ve veri güvenliğinin sağlanmasında önemli eksiklikler bulunduğu çarpıcı bir biçimde ortaya konmuştur. Denetim çalışmaları sırasında ayrıca hassas veri içeren sistemlere erişimde kullanıcılara iki haneli sayısal şifre verilebildiği, 1111, 0000, 1234 gibi kolay tahmin edilebilir şifrelerin kullanıldığı; bazı kurumların çağrı merkezinden sadece ad, soyad ve T.C. kimlik numarası beyan edilerek maaş tutarları, gidilen sağlık kurumu, muayene olunan doktor, alınan ilacın adı, ödenen katılım payı miktarı gibi birçok kişisel bilgiye ulaşılabildiği saptanmıştır. Türkiye’de kişisel veriler “yeterli” düzeyde korunmamaktadır. Bu nedenle kural olarak AB ülkelerinden Türkiye’ye veri gönderilmesi yasaktır.

**TÜRKİYE CUMHURİYETİ ANAYASASI**

Türkiye Cumhuriyeti Anayasası’nda kişisel verilerin korunmasının normatif temelini oluşturacak çeşitli hükümler bulunur. Bu kapsamda ilk olarak kişinin maddi ve manevi varlığını geliştirme hakkı dikkate alınmalıdır. Anayasa’nın başlangıç 6. paragrafında ve 17/1 hükmünde kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı hüküm altına alınmıştır. Bunun yanında Anayasa uyarınca “Devletin temel amaç ve görevleri” arasında “insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak” (m.5) yer alır. Türk Anayasa Mahkemesi bir kararında insan onuru kavramını şu şekilde tanımlamıştır: “İnsanın ne durumda, hangi şartlar altında bulunursa bulunsun sırf insan oluşunun kazandırdığı değerin tanınmasını ve sayılmasını anlatır. Kişisel verilerin korunmasına yönelik Türk hukuk mevzuatındaki en önemli düzenleme yine

Anayasada yer alır. Anayasa’nın 20. Maddesine 2010 Anayasa değişiklikleri ile eklenmiş olan son fıkra şöyledir: “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir”. Belirtilen hüküm ile Türkiye’de kişisel verilerin korunması açıkça anayasal bir hak olarak düzenlenmiştir. Anayasanın 20. Maddesinin 3. fıkrası kapsamında kişisel verilerin korunması hakkından değil, kişisel verilerin korunmasını “isteme” hakkında söz edilmesi anayasa koyucunun bu korumaya ilişkin yeterli güvenceyi sağlamada isteksiz olduğu şeklinde yorumlanabilir. Türk hukuk sisteminde uluslararası antlaşmalar iç hukuk sisteminin bir parçasıdır. Bu antlaşmanın temel hak ve özgürlüklere ilişkin olması durumunda ise, sözleşme hükümlerinin yasaların bile üzerinde yer aldığı söylenebilir. Nitekim 90. maddeye 2004 yılında eklenen bir hüküm uyarınca: “Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır”. Bu düzenleme, konumuz açısından özellikle Avrupa İnsan Hakları Sözleşmesi’nin (AİHS) konumu dolayısıyla önemlidir. Türkiye AİHS’e taraf olan devletlerden biridir. Sözleşmede yer alan hükümlerin içeriğini belirleyen organ ise Avrupa İnsan Hakları Mahkemesidir (AİHM). Mahkemenin içtihadı, özel yaşamın gizliliği hakkını düzenleyen 8. madde çerçevesinde kişisel verilerin korunması hakkının tanınması yönündedir. Bir başka anlatımla kişisel verilerin korunması anayasal temelini 20. maddedeki doğrudan düzenleme yanında, dolaylı olarak Anayasa’nın 90. maddesinde de bulmaktadır. Türkiye’de mahkemelerde konuya ilişkin somut olaylarla karşılaşıldığında AİHS’e ve Sözleşmenin denetim organı olan AİHM’in içtihatlarına da bakmanın önemli bir gereklilik olduğu dikkatten kaçmamalıdır.

**AVRUPA İNSAN HAKLARI SÖZLEŞMESİ**

AİHS’de Anayasa’da olduğu gibi kişisel verilerin korunmasının ayrı bir hak alanı olarak düzenlenmediği görülür. Sözleşme’nin 1950 yılında kabul edildiği düşünüldüğünde bu oldukça doğaldır. Ancak AİHM verdiği kararlarla, kişisel verilerin korunmasında temel ilkelerin büyük bir bölümünü Sözleşme’nin 8. maddesi kapsamında tanımaktadır. Sözleşme hükümlerinin sınır ve kapsamlarını belirleyebilmek için AİHM’in yorumlarının önemi açıktır. O hâlde hem Anayasa’nın 90. madde hükmünün bir gereği olarak hem de bu konuda geliştirilen içtihatlara aykırı uygulamaların AİHM önünde ihlal kararı ile sonuçlanacağı düşünül düğünde bu kararların incelenmesi gerektiği açıktır. AİHS’nin “Özel ve aile yaşamına saygı hakkı” kenar başlıklı 8. maddesi şu hükmü içerir:

*1. Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.*

*2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir.*

AİHM, özellikle 1980’li yılların ortalarından beri ve gittikçe artan bir yoğunlukta, kişisel verilerin korunmasını, Sözleşme’nin sağladığı güvenceler kapsamında değerlendirmiştir. Mahkemenin bireysel özerkliği ve bilgilerin geleceğini belirleme hakkını, 8. madde ile getirilen güvencelerin yorumlanmasında önemli bir temel ilke olarak belirlediği görülür. Bu bağlamda AİHM, bireylerin kişisel verilerinin kullanımı ve kaydı konusunda denetim hakkının bulunduğunu kabul etmektedir. Kişisel verilerin korunması hakkının 8. Madde kapsamında değerlendirilmesi, Sözleşme hükümlerinin yorumlanmasında yeni gelişmelere açık bir bakışın hâkim olduğunun da göstergesidir. Nitekim AİHM’e göre Sözleşme, *“güncel koşullar ışığında* *yorumlanması gereken yaşayan bir enstrüman”*dır

Mahkemenin görevi, Sözleşmeyi yorumlarken sosyal değişimleri de yansıtmaktır AİHM’nin çeşitli kararlarında da belirttiği üzere, Sözleşme ile güdülen amaç, hakların hayali ya da teorik olarak değil, etkili ve elverişli bir şekilde güvence altına alınmasıdır. Ayrıca Mahkemenin çeşitli kararlarında özel yaşamı kişinin mahrem alanı(özel yaşamın iç çemberi) dışında başkaları ile ilişki kurduğu alanları da kapsar şekilde yorumladığı görülmektedir. Bu yorum, kişisel verilerin korunması açısından önemli sonuçlar getirir. Bir örnek sokak ve meydanları izlemek üzere kurulan kapalı devre televizyon sistemlerine (CCTV, Close Circuit Television System) ilişkin olarak verilebilir. Bunun yanında Mahkemenin günün koşullarının gerisinde kalmama düşüncesini koruma alanı açısından kararlarına yansıtmasının olumlu sonuçlarının bulunduğu belirtilmelidir. Örneğin bu yaklaşımla Mahkeme, geleneksel haberleşme araçlarının yanında modern iletişim araçlarını da koruma kapsamında görmektedir. Bu bağlamda kişilerin İnternet aracılığıyla kurdukları iletişimin, e-postalarının izlenmesi ya da içeriklerinin saptanması da 8. Madde çerçevesinde değerlen dirilmektedir. AİHM 8. madde çerçevesinde, kişisel verilerin korunması ile ilişkili ilk önemli kararını Klass ve diğerlerinin Almanya’ya karşı yaptığı başvuru üzerine vermiştir. Bu kararda Mahkeme, gizli telefon dinlemelerini özel yaşam kapsamında değerlendirir. Daha sonra verdiği pek çok kararla Mahkemenin temel olarak konumuza ilişkin önemli bazı ilkeleri Sözleşme’nin 8. maddesi kapsamında değerlendirdiğini görmekteyiz. Bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi, telefon görüşmelerine ilişkin kayıtları izleme, toplanan verilerin toplanma amacı dışında kullanılması, sağlık verilerinin gizliliği, emniyet güçleri tarafından parmak izi ve fotoğrafların alınması, kişisel verilere erişim hakkı, kişisel verilerin gerektiğinden uzun süre tutulması gibi konular Mahkemenin çeşitli kararlarında 8/1 hükmü kapsamında değer lendirilmiştir. AİHS’nin 8. maddesinde düzenlenen özel yaşama saygı hakkının sınırları, aynı maddenin 2. Fıkrasında yer alır. Bu özel yaşama saygı hakkına bir müdahale olduğu saptandığında, Mahkeme bu müdahalenin meşruiyet kazanıp kazanmadığını değerlendirir. Bu değerlendirme 2. fıkrada belirlenen koşul ve ölçütlere uygunluk açısından yapılmaktadır. AİHS 8/2 hükmü uyarınca özel ve aile yaşamına müdahale:

• burada sınırlı sayımla belirtilmiş amaçlardan bir ya da bir kaçına yönelik;

• yasada öngörülmüş ve

• demokratik toplum için gerekli ve öngörülen amaç ile orantılı olması durumunda meşrudur.

Sınırlı sayımla belirlenen ve özel ve aile yaşamına saygı hakkına istisna getiren meşru amaçlar ise şunlardır: “ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının haklarının korunması”.

**TÜRK CEZA KANUNU**

1 Haziran 2005 tarihinde yürürlüğe giren yeni Türk Ceza Kanunu uyarınca kişisel verilerin hukuka aykırı kayıt edilmesi, verileri hukuka aykırı verme, yayma veya ele geçirme ile gereken sürelerin geçmesine karşın verileri yok etmemenin suç olarak düzenlenmesidir. Bu açıdan Türk hukuk sisteminde yasal düzeyde konuya ilişkin en kapsamlı korumanın Türk Ceza Kanunu’nda (TCK) yer aldığı söylenebilir. Öncelikle TCK’nin 135. maddesi uyarınca kişisel verilerin hukuka aykırı olarak kaydedilmesi suçtur.

Buna göre kişisel verileri hukuka aykırı olarak kayıt eden kimseye 1 yıldan 3 yıla kadar hapis cezasının verilmesi öngörülmüştür. Kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ve sendikal bağlantılarına ilişkin bilgileri hukuka aykırı olarak kaydeden kimse de aynı yaptırım ile cezalandırılacaktır. TCK’nin 135. maddesinde yalnızca verilerin işlenmesinin bir türü olan kayıt etmeyi suç olarak belirlenmiştir. Oysa bir önceki bölümde açıklandığı üzere kişisel verilerin işlenmesi yalnızca kayıt etmeyi değil, toplanma, kullanma, aktarma gibi çeşitli eylemleri içeren bir süreçtir. TCK’nin aşağıda incelenecek izleyen hükümlerinde bu eylemlerin bir kısmına ilişkin düzenlemeler bulunmaktadır. Ancak özellikle kişisel verilerin hukuka aykırı olarak kullanılmasına ilişkin düzenlemeye yasada yer verilmediği görülmektedir. Bu durumda hukuka uygun şekilde toplanan ve kayıt altına alınan kişisel verilerin sonraki kullanımlarında oluşabilecek aykırılıklar yaptırımsız kalabilir.

TCK’nin 136. maddesinde ise kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu düzenlenmiştir. Buna göre; “Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, 2 yıldan 4 yıla kadar hapis cezası ile cezalandırılır”.

Belirtilen eylemlerin yaptırıma bağlanmasındaki amaç kişisel verilerin yetkisiz üçüncü kişilere aktarılmasını ve ele geçirilmesini önlemektir. Bu bakımdan verinin kaydedilmesinin hukuka uygun olup olmadığı, suçun oluşması açısından önemli değildir. 136. maddede verme, yayma ve ele geçirme seçimlik hareketler olarak belirlenmiştir. Kişisel verilerin hukuka aykırı olarak verme ve yayma hareketlerinin yaptırıma bağlanmasındaki amaç yetkisiz üçüncü kişilere aktarılmasını önlemektir. Ayrıca kişisel verileri daha önceden kaydedilmiş olsun ya da olmasın hukuka aykırı olarak ele geçiren kişi 136. madde hükmünce cezalandırılacaktır. Daha önceden verinin kaydedilmesinin hukuka uygun olup olmamasının suçun oluşması açısından bir önemi bulunmamaktadır. Nitekim 136. Maddenin gerekçesinde şu ifade yer almaktadır: “Bu madde hükmü ile, hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır”. 136. maddede yer alan düzenleme kişisel verilerin korunmasını sağlayıcı bir niteliktedir. Bu noktada önlenmek istenen eylemler arasında kimlik hırsızlığı örnek olarak gösterilebilir. Konuya ilişkin bir diğer önemli düzenlemenin TCK’nin 138. maddesinde yer aldığı görülür. Buna göre: “Kanunların belirlediği sürenin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde 1 yıldan 2 yıla kadar hapis cezası verilir”. Hükme 2014 yılında eklenen fıkra uyarınca ise “Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.” TCK’nin 138. maddesi ile, kişisel verilerin korunması alanında temel ilkelerden biri olan verilerin süresiz olarak tutulmaması gerekliliğinin karşılandığı söylenebilir. O hâlde bilgileri hukuka aykırı olarak elde eden, kaydeden ve kullanan kişilerin de ilgili mevzuatta belirtilen sürelerin geçmesinin ardından bunları yok etmesi bir zorunluluktur. Bu suçların hiç birinin takibi şikâyete bağlı değildir. Ayrıca Türk Ceza Kanunun 135. ve 136. maddesinde düzenlenen suçların kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hâli ağırlaştırıcı sebep olarak belirlenmiş ve cezanın yarı oranında arttırılacağı hüküm altına alınmıştır. Bunun yanında bu üç maddede yer alan suçların tüzel kişiler tarafından işlenmesi hâlinde bunlara özgü güvenlik tedbirleri uygulanacaktır. TCK’de konuya ilişkin olarak belirtilen suçlara ve yaptırımlara yer verilmiş olmasına karşın, bu eylemlerin tanımlandığı ve kişisel verilerin korunmasında temel ilkelerin belirlendiği bir düzenlemenin bulunmaması önemli bir eksiklik olarak hissedilmektedir. Bu kapsamda özellikle “kişisel veri”nin tanımı konusunda mevzuatımızda açıklayıcı hükümlerin son derece sınırlı olması ve temel ilkelerin düzenlememesi nedeniyle “hukuka aykırılık”ın belirlenmesinde yaşanan güçlükler özellikle dikkat çekicidir.

**TÜRK MEDENİ KANUNU**

Türk hukuk mevzuatında medeni hukukun kişilik haklarına yönelik düzenlemelerinin kişisel verilerin korunmasına açısından bazı olumlu sonuçlar sağlayabileceği söylenebilir. Nitekim kişilik hakları, kişisel değerlerin bütününü kapsayan bir hukuksal alandır. Alman Anayasa Mahkemesi de bir önceki bölümde işaret edilen önemli bir kararında kişisel verilerin korunmasının Alman Anayasası’nda karşılığını bulan genel kişilik hakkı çerçevesinde değerlendirile ceğine kanaat getirmiştir (BverfGE 65,1). Medeni hukukta, kişisel verilerin korunması ile yakından ilişkili olan, kişinin onur ve saygınlığı, adı ve resmi üzerindeki hakları ile sır alanı kişilik haklarının alanı içerisinde değerlendir ilmektedir. Bu doğrultuda konuya ilişkin hukuksal korumanın ise Türk Medeni Kanunu’nun (MK) 24. ve 25.maddelerinde getirildiği görülmektedir. Nitekim MK’nin 24. maddesinde kişiliğe yönelik saldırılara karşı temel ilke, 25. maddede ise başvurulabilecek hukuksal yollar belirlenmiştir. O hâlde MK ve ilgili düzenlemelerin kişisel verilerin

korunmasını belirli oranda sağladığı söylenebilir. Ancak bu düzenlemeler, Türkiye’de kişisel verilerin etkin koruma sını sağlayabilecek içerikten yoksundur. Nitekim kişisel verilerin etkin korumasını sağlayabilmek için önleyici tedbir niteliğinde olan temel ilkelerin yasal düzenlemeler ile belirlenmesi ve zarar meydana gelmeden bu ilkelere uyumlu

pratiklerin geliştirilmesi gerekir. Mehaz hükmün yer aldığı İsviçre Medeni Kanunu’nda hemen hemen aynı düzenle menin bulunmasına karşın, İsviçre’de ayrıca bir kişisel verilerin korunması yasasının da kabul edilmesinin nedeni budur. Kişisel Verilerin Korunması Yasa Tasarısı’nın bu noktada MK ile karşılanamayan bir koruma getireceği ve bir anlamda onu tamamlayacağı söylenebilir.

**TÜRK BORÇLAR KANUNU**

Borçlar Kanunu’nun 419. maddesi uyarınca “İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir”. Belirtmek gerekir ki iş hukuku alanında kişisel verilerin korunması özel ve öncelikli bir konuyu oluşturur. Kişisel öncelikler belirlenirken iş, sağlık ve aile yaşamı sonrasında belki de en önde gelen konudur. İş bulmak, işsiz kalmamak, huzurlu bir iş yaşamı sürdürmek bireysel tatmin açısından oldukça önemlidir. Ayrıca sosyal bir varlık olan insan, başkalarıyla ilişki kurma da önemli bir fırsata iş yaşamında kavuşmaktadır. Bu derece önemli bir alanda kişinin korumasız bırakılması ise düşünülemez. İşe alım sürecinden iş akdinin feshi sonrasına uzanan süreç içerisinde işverenin işçi ile ilgili pek çok bilgiye ulaşabildiği dikkatten kaçmamalıdır. İş ilişkisi niteliği gereği işçinin dezavantajlı olduğu bir durum yaratmaktadır. Bu nedenle işçinin kişisel verilerinin yasal düzenlemeler uyarınca korunması son derece önemlidir. Ayrıca gelişen bilişim ürünlerinin işyerinde artan oranda kullanımı bu gerekliliği daha da artır maktadır. Bütün bunlar, işçinin kişisel verilerinin korunmasının yakından incelenmesine ve kimi yerlerde özel düzenlemelerin konusu olmasına neden olmuştur. Uluslararası düzenlemelere bakıldığında ise Uluslararası Çalışma Örgütünün (International Labour Organization -ILO) konuya ilişkin bir sözleşme kabul etmediği ancak işçinin kişisel verilerinin korunmasına ilişkin uygulama ilkelerini belirlediği görülmekte. Hükmün kişisel verilerin korunması hukukunun temel ilkelerinden olan asgari oranda veri tutulması, bir başka anlatımla gerektiğinden fazla verinin işlenmemesi ilkesi ile de uyumlu olduğu dikkat çekmektedir.

**ELEKTRONİK HABERLEŞME VE ELEKTRONİK TİCARET KANUNLARI**

Elektronik Haberleşme Kanunu 5809 sayılı Elektronik Haberleşme Kanunu’nun 51. maddesi 2014 yılında Anayasa Mahkemesi iptal kararı verinceye kadar kişisel verilerin korunması konusundaki ilkelerin belirlenmesinde Bilgi Teknolojileri ve İletişimi Kurumunu (BTK) yetkili kılan kısa bir hükümdü. Bu hükme dayanarak BTK konuya ilişkin bir yönetmelik çıkarmıştı. Ancak Anayasa Mahkemesi temel hak ve özgürlüklere ilişkin düzenlemelerin ancak yasa ile yapılabileceğine ilişkin açık Anayasa hükmünü işaret ederek bu düzenlemeyi iptal etti (2014). Oluşan boşluğu gidermek amacıyla kanun koyucu 2015 yılında yeni bir düzenlemeyi kabul etti. Böylelikle göre Elektronik Haberleşme Kanunu nun “kişisel verilerin işlenmesi ve gizliliğinin korunması” kenar başlıklı 51. maddesi bu sektörde veri işleme Süreçlerine ilişkin kuralları belirleyen bir hüküm hâlini aldı. 51. madde kapsamında öncelikle bir önceki bölümde üzerinde durulan verilerin kaliteli olması ilkesine işaret edildiği görülmektedir. Buna göre elektronik haberleşme alanında veri işleme süreçlerinde bu ilkenin bileşenlerine uyumlu hareket etmek bir zorunluluktur. Ayrıca elektronik haberleşmenin ve ilgili trafik verisinin gizliliği temel kural olarak benimsenmiştir. Bunun istisnası ilgili mevzuatın ve yargı kararlarının öngördüğü durumlardır. Bunun haricinde haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaklanmıştır. Elektronik Haberleşme Kanunundaki düzenlemenin dikkat çeken bir diğer yönü “çerez”lerin (cookie) kullanımına getirilen sınırlamadır. Çerez kullanıcı bir İnternet sitesini ziyaret ettiğinde bağlantı kurduğu cihazın sabit diskine kaydedilen bir tür tanımlama dosyası olarak tarif edilebilir. Bu dosyalarda kişilerin ziyaret ettiği siteler gibi bazı bilgiler saklanabilmektedir. 51. maddenin 3. Fıkrası uyarınca:

*“Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili aboneleri /kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir”.*

Bu hüküm dolaysıyla telefon operatörleri ancak ilgilinin açık rızasının bulunması halinde çerezleri kullanabilir. Hükmün bir diğer olumlu yanı işletmecilerin veri güvenliğine uygun hareket etmelerini zorunlu kılmasıdır. Bunun yanında kişilerin iletişim trafik verilerinin ve konum bilgilerinin korunmasına yönelik bazı güvenceler de hükümde yer alır. Bu, özellikle cep telefonu aboneleri açısından önemlidir. Elektronik Haberleşme Kanunu’nun 51.maddesi ile bir yandan kişisel verilerin korunmasına yönelik bu kurallar hüküm altına alınırken diğer yandan kişisel verilerin saklanmasına yönelik bazı hükümler getirilmiştir. Kanun kapsamında sunulan hizmetlere ilişkin olarak; soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl, kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince saklanacağı hüküm altına alınmıştır.

**Elektronik Ticaret Kanunu**

6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu 2014 yılında kabul edilmiştir. Kanun’un 6. maddesi uyarınca:

(1) Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay, yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir. Kendisiyle iletişime geçilmesi amacıyla alıcının iletişim bilgilerini vermesi hâlinde, temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz.

(2) Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir.

Burada kastedilen ticari ileti, reklam, pazarlama gibi amaçlarla cep telefonlarına ya da e-posta adreslerine gönderilen mesajlar, e-postalar ya da yapılan aramalardır. Kanun’un 10. maddesi ise doğrudan kişisel verilerin korunmasına yöneliktir.

Buna göre: (1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı:

a)Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur. b)Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz”.

Böylelikle elektronik ticaret etkinlikleri yürüten firmaların, bu süreç içerisinde elde ettikleri kişisel verileri korumaları hüküm altına alınmıştır. Ancak Elektronik Ticaret Kanununda bu yükümlülüğe aykırı hareket edenler için bir yaptırım öngörülmemiş olması bir eksiklik olarak değerlendirilebilir.

**Kişisel Verilerin Korunması Kanunu**

Bankacılık Kanunu, Ceza Muhakemesi Kanunu, Hasta Hakları Yönetmeliği gibi çeşitli düzenlemelerde konuya ilişkin hükümler yer almaktadır. Ancak bu hükümlerin uygulamada sınırlı bir koruma sağladığı dikkat çekmektedir. Bunun bir nedeni, konuya ilişkin temel ilkeleri belirleyen bir yasal düzenlemenin bulunmamasının bu ilkelerin yorumunda zorluklara neden olmasıdır. İkinci olarak yukarıda işaret edilen hükümlerin önemli bir bölümünün kişisel verilerin hukuka aykırı kullanımının ortaya çıkmasından sonra uygulanabilir nitelik taşımaktadır. Bir başka ifadeyle, zarar ortaya çıkmadan önleyici nitelikte ilkelerin belirlenmemiş olması önemli bir eksikliktir. Oysaki Türkiye’de kişisel verilerin korunmasına yönelik temel ilkeleri belirleyerek önleyici koruma sağlayacak Kişisel Verilerin Korunması Kanunu uzun zamandır beklenmektedir. Bu beklentiyi 1981 yılına kadar geriye götürmek olanaklıdır. Nitekim Türkiye, taraf devletlerin metinde yer alan ilkeleri mevzuatlarına yansıtmalarını zorunlu kılan Avrupa Konseyi Kişisel Verilerin Korunması Sözleşmesi’ni 28 Ocak 1981’de imzalamıştır. Belirtmek gerekir ki bu gereklilik hâlen yerine getirilmediği için Türkiye, bugün 46 devletin taraf olduğu bu Sözleşme’yi imzalayıp onaylamayan Avrupa Konseyi üyesi tek devlettir. Geçen süre içerisinde veri koruma alanında temel ilkeleri belirlemeye yönelik yasa hazırlıkları ise 1989 yılında başlamıştır. 2008 yılında TBMM’ye bir tasarı sevk edilmiş, ancak kadük olmuştur. 2010 yılı Anayasa değişiklikleri kapsamında kişisel verilerin korunmasını isteme hakkının anayasal bir hak olarak açıkça düzenlenmesi ile veri koruma alanında çerçeve nitelikte bir yasal düzenleme bir beklenti olmaktan öte anayasal bir zorunluluk hâline gelmiştir. 2012 yılında Adalet Bakanlığı bünyesinde yeni bir komisyon kurulmuş ve bu komisyonun çalışmaları neticesinde şekillenen yeni taslak üzerinde çeşitli değişiklik ve düzenlemelerin yapılmasının ardından 26 Aralık 2014 tarihinde hâlen gündemde bulunan Kişisel Verilerin Korunması Kanun Tasarısı Meclise sevk edilmiştir. Tasarı metninden ve madde gerekçelerinden çıkan bir sonuç, bu metnin hazırlanması aşamasında veri koruma alanında AB’de genel çerçeveyi belirleyen 95/46/AT sayılı Yönergeden yararlanıldığıdır. Ancak tasarıdaki geniş istisna hükümleri ve AB bünyesinde bu yıl yürürlüğe girmesi beklenen ve bütüncül olarak Veri Koruma Reformu olarak adlandırılan yeni düzenlemelerin dikkate alınmadığını belirtmek gerekir. Kişisel Verilerin Korunması Kanun Tasarısı ile geç kalınmış da olsa ihlallerin asgari ve denetlenebilir bir düzeye indirilmesi için yeni bir fırsat doğmuştur. Fırsatın değerlendirildiğini söyleyebilmemiz için ise elbette Tasarı, 1. maddede belirlenen “kişisel verilerin işlenmesinde kişinin temel hak ve özgürlüklerini korumak”, amacını gerçekleştirebilecek nitelikte olmalıdır. Anayasa nın da bir gereğidir.

Avrupa İnsan Hakları Mahkemesi de kişisel verilerin korunmasını 8. madde kapsamında gören çok sayıda karar vermiştir. Ayrıca genel gerekçede de işaret edildiği üzere, bu alandaki eksikliğin giderilmesi AB tam üyelik sürecinin bir gereğidir. Diğer yandan, AB’nin yeterli düzeyde koruma sağlamayan ülkelere kural olarak veri aktarımını yasaklaması Avrupa devletleri ve kurumları ile adli ve cezai iş birliği gerçekleştirilememesine ve ekonomik kayıplara neden olmaktadır.

Kişisel Verilerin Korunması Kanun Tasarısı 9 bölümden oluşmaktadır. Birinci bölümde Kanunun amaç ve kapsamı belirlenmiş; ayrıca kişisel veri, verilerin işlenmesi gibi konuya ilişkin son derece önemli tanımlara yer verilmiştir. Bu noktada tanımların büyük oranda AB sistemi ile uyumlu olduğu söylenebilir. Tasarının “kişisel verilerin işlenmesi” kenar başlıklı ikinci bölümünde ise veri işlemede hakim olan temel ilkelere, kişisel verilerin işlenme şartlarına, özel nitelikli(hassas) kişisel verilere, verilerin silinmesi yok edilmesi ve anonim hâle getirilmesi düzenlenmiştir. Tasarı kapsamında kişilerin “ırkı, kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatıyla ilgili veriler” özel nitelikli (hassas) kişisel veri olarak kabul edilmiş ve işlenmesi yasaklanmıştır (m.6/1). Ancak ikinci fıkrada altı bent altında belirlenen istisnalardan biri “yeterli önlemlerin alınması şartıyla (...) kanunlarda açıkça öngörülmesi” hâlidir. Bu hüküm istisnayı kural, kuralı istisna hâline getirebilecek bir genişliktedir. Tasarının ikinci bölümünde ayrıca kişisel verilerin üçüncü kişilere ve yurt dışında aktarımına ilişkin hükümler yer almaktadır. Bu hükümleri de bir örnek üzerinden değerlendirilebilir. Tasarıda yer alan bir diğer istisna hükmü “ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerinin işlenmesi ”ne ilişkindir. Bu durum kişisel verilerin işlenmesinin(m.5/2,d), özel nitelikli kişisel verilerin işlenmesinin(m.6/2,ç) ve “kanunun amacına ve temel ilkelerine uygun ve orantılı olmak” kaydı düşülerek veri sorumlusunun aydınlatma yükümlülüğünün ve sicile kayıt yükümlülüğü nün istisnası(m.24/2,d) olarak belirlenmiştir. Gerekçede yer alan açıklama ise şöyledir: “ilgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir”. Öncelikle “alenileştirme” ile neyin kastedildiği belirlenmelidir. Örneğin bir kişinin İnternet sitesinde e-posta adresini yazması, kartvizitinde telefon numarasının bulunması, İnternet’te yayımlanan bir bildiriye imza atması, kamusal alanda gerçekleştirilen bir gösteri yürüyüşüne katılması, bir sokak röportajında siyasal görüşünü söylemesi kendisi tarafından ilgili bilgilerin alenileştirildiği anlamına mı gelir? Bu noktada herkes tarafından bilinen bilgiler açısından korunması gereken hukuki yararın ortadan kalkmadığı belirtilmelidir. Nitekim kişisel verilerin korunmasının bir temel hak alanı olarak kabul edilmesi; veri tabanlarındaki ve kayıt etme, ilişkilendirme, arama yapma, aktarma gibi veri işleme teknolojilerindeki gelişmeler ile yakından ilişkilidir. Tasarının üçüncü bölümünde veri sorumlusunun aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülükler ile birlikte ilgili kişinin hakları düzenlenmiştir. Bu düzenlemelerdeki temel hedef kişinin kendisi ile dijital ortamlarda her gün artan oranda işlenen verileri arasındaki bağın korunmasıdır. Bu açıdan önemli başka bazı hükümler de dördüncü bölümde yer alır. Nitekim burada özellikle altıncı bölümde oluşum ve işleyiş prensipleri benimsenen Kişisel Verilerin Korunması Kuruluna şikâyet, bu şikâyetlerin inceleme esasları, yine Kurul Genel Sekreterliği tarafından tutulacak “Veri Sorumluları Sicilli” hüküm altına alınmıştır. Tasarının 18. maddesi ile “görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak” yerine getireceği belirtilen bir Kişisel Verileri Koruma Kurulu oluşturulması öngörülmektedir. Tasarının 20/1 hükmü uyarınca:

*“Kurul, yedi üyeden oluşur. Kurul üyelerinin; ikisi mesleğinde en az on yıl çalışmış avukatlar ve hakimler, biri yükseköğretim kurumlarında en az on yıl çalışmış olan öğretim üyeleri, dördü ise kamuda veya özel sektörde en az on yıl çalışmış olanlar arasından Bakalar Kurulunca seçilir. Kurul, kendi üyeleri arasından bir başkan seçer. Başkan, Kurulun en üst yönetici olup, kurulun genel yönetim ve temsilinden sorumludur”.*

Belirtmek gerekir ki Kurulun Adalet Bakanlığı ile ilişkili olması(m.18/3), üyelerinin Bakanlar Kurulu tarafından belirlenmesi (m.20/1), kurul üyelerinin görevleri sebebiyle işledikleri iddia edilen suçlara ilişkin soruşturma iznini Adalet Bakanının vermesi (m.20/11) gibi hususlar bağımsızlığın sağlanması noktasında kuşku yaratmaktadır. Kurulun kompozisyonu ve idare teşkilatındaki yeri, ilişkili olduğu Adalet Bakanlığının (UYAP gibi) veri işleyen sistemlerini ya da Sağlık Bakanlığı gibi hassas nitelikteki verileri işleyen diğer Bakanlıkları denetimi açısından sorun yaratabilir. Belirtmek gerekir ki Avrupa mevzuatı uyarınca denetim organı “tam bağımsız” olmalıdır. Avrupa Adalet Divanı da sırasıyla Almanya, Avusturya ve Macaristan uygulamalarının bazı yönleriyle tam bağımsızlık koşulunu karşılamadığına ilişkin kararlarında konunun kritik önemine işaret etmiştir. Öte yandan tasarının sekizinci bölümünde yer alan istisnalar, yani Kanun yürürlüğe girdikten sonra bütüncül olarak kapsam dışında kalacak alanlar en çok tartışılan hükümleri arasındadır. Bu noktada ilk dikkat çeken istisna istihbarat gibi bazı etkinliklerin kapsam dışında tutul masıdır. İstihbaratın niteliği gereği gizli yürütülen bir etkinlik olduğu kabul edilse bile, hukuka ve dürüstlük kurallarına uygun olmak, belirli açık ve meşru amaçlar için işlenmek ya da işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek gibi ilkeler (m.4/2) bu alanda da öncelikle ve mutlaka geçerli olmalıdır. Konuyu bütüncül olarak düzenleyen tasarının, başta beşinci bölümde yer alan yaptırım sistemi olmak üzere değerlendirilmesi ve düzenlenmesi gereken başka hükümleri de bulunmaktadır. Bu değerlendirmeler yapılarken kişisel verilerin korunmasının bir insan hakkı olduğu ve yarışan çıkarlar arasında dengenin sağlanması gerekliliği her zaman göz önünde tutulmalıdır. Veri işleme teknolojilerinin yaygın bir biçimde kullanıldığı Türkiye’de bu temel ilkeden hareket eden ve etkin koruma sağlayabilecek güçte bir yasal düzenlemenin bulunmaması dengenin insan hakları aleyhine bozulmasına neden olmaktadır ve her geçen dakika bu alandaki kayıplar artmaktadır. Kişisel verilerin korunması hakkı, özellikle teknolojide yaşanan hızlı gelişmeler dolayısıyla temel hak ve özgürlükler içerisinde her geçen gün biraz daha önemli bir hale gelmektedir. Türkiye’de ise konuya ilişkin basın yayın kuruluşlarına yansıyan haberler ve gündelik yaşamda karşılaşılan çeşitli uygulamalar veri korumaya duyulan ihtiyacın açık göstergeleridir. Öte yandan şu hususa da işaret etmek gerekir: Hukuksal güvenceler, bilişim teknolojileri ile temel hak ve özgürlükler arasındaki dengenin kurulabilmesi için en önemli araçtır. Ancak bunun yanında konuya ilişkin farkındalığın arttırılması ve kişisel önlemlerin alınması gerekir. Pek çok devlette benimsenen bağımsız veri koruma otoritelerinin görevlerinden birinin yurttaşların tehlikeler ve alınabilecek önlemler konusunda bilgilendirilmesi olmasının nedeni de budur. Bunun yanında sivil toplum örgütleri de konuya ilişkin çalışmalar yürütmektedir. Etkin veri koruması sağlanması yönündeki çalışmalar içerisinde teknolojideki gelişmelerden yardım almak ise son yıllarda dikkat çeken bir önem kazanmıştır. “Dizayn aracılılığıyla gizlilik” (privacy by design, PbD) ya da “varsayılanlar aracılılığıyla gizlilik” (privacy by default) bu kapsamda verilebilecek bir kaç örnektir. PbD ile hedeflenen veri korumasının sağlanması, kişinin kendi verileri üzerinde denetime sahip olması ve kuruluşların sürdürülebilir rekabet avantajı elde etmesidir. Bu doğrultuda teknoloji geliştirilirken özel yaşamın gizliliği hakkı merkezli bir yaklaşım benimsenmelidir. “Varsayılanlar aracılılığıyla gizlilik” ise bir kullanıcıya İnternet üzerinden bir hizmet ya da ürün edinirken en güçlü gizlilik ayarlarının uygulanmasıdır. Özellikle son yıllarda bu ve benzeri yaklaşımların benimsenmesinin hukuksal düzenlemeler ile de desteklenmesi yönünde bir eğilim gelişmektedir.

**UNITE 4**

**GİRİŞ**

Bilişim alanında çalışan bir hukukçunun, sadece iyi bir hukukçu kimliğine sahip olması, bu alanda uzmanlaşabilmesi bakımından yeterli olmamakta; bunun yanında bilişim sistemlerine, bu sistemlere bağlı olarak kullanılan teknolojik ürünlere ve internete ilişkin oldukça kapsamlı bilgilere de sahip olması gerekmektedir. Bu bölümde dar anlamda bilişim suçlarının CMK m.135’teki koruma tedbirinin incelenmesi uygun görülmüştür. Bu bağlamda öncelikle TCK’nın 2. kitabının topluma karşı suçların düzenlendiği 3. kısmının 10. bölümünde düzenlenen bilişim alanındaki suçlar inceleme konusu yapılacaktır. Temelde suçun unsurları ve kusurluluk üzerinden yapılacak incelemede, yeri geldiğince şahsi cezasızlık sebebi ve etkin pişmanlık gibi cezaya etkili diğer kurumlar da ele alınacaktır. Bununla birlikte hırsızlık, dolandırıcılık gibi bazı suçların bilişim sistemlerinin kullanılması suretiyle işlenmesi bakımından öngörülen nitelikli haller bölüm kapsamında değerlendirilmeyecektir. Aynı şekilde Fikir ve Sanat Eserleri Kanunu ile Elektronik İmza Kanunu’nda yer alan bilişim suçları da bölüm içerisinde ele alınmayacaktır. Buna karşın CMK m.135’de düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma koruma tedbiri bölüm içerisinde incelenecek konulardandır.

**BİLİŞİM ALANINDAKİ SUÇLARA İLİŞKİN TÜRKİYE’DE YAŞANAN SÜREÇ**

Bilişim suçlarına ilişkin ilk düzenleme TCK’ya 1991 yılında girmiş ve 3756 sayılı kanunla 765 sayılı TCK’nın ikinci kitabına bazı bilişim suçlarını öngören “Bilişim Alanında Suçlar” başlıklı 11. Bap ilave edilmiştir. 3756 sayılı kanundan önce bilişim alanın daki suçlara ilişkin fiillerin büyük çoğunluğunu yaptırım altına alabilme imkânı bulunmamaktaydı. Belki bilgisayar ve bilgisayar sistemlerinin maddi varlığına yönelik mala zarar verme ve hırsızlık gibi fiilleri, eski TCK’nın hükümleriyle cezalandırmak mümkündü; fakat bunlarda yer alan veri, program veya diğer unsurların tahribine, silinmesine, kopyalanmasına veya içeriğinin alınmasına yönelik eylemlerin, suçun konusunu teşkil eden hususlar klasik ceza hukukunun anladığı anlamda mal teşkil etmediğinden, cezalandırılmalarına imkan yoktu. Aynı şekilde dolandırıcılık fiilinin mağdurunun gerçek kişi olması gerektiğinden, makineye karşı gerçekleştirilen hileleri cezalandırmak da mümkün değildi. 1995 yılında 4110 sayılı kanunla Fikir ve Sanat Eserleri Kanununda bilgisayar programlarının da eser sayılacağına ilişkin bir değişiklik yapılmış; bilgisayar programlarına karşı gerçekleştirilen birtakım eylemler yaptırım altına alınmıştır. E-ticaret kavramının ortaya çıkmasına bağlı olarak sözleşme onaylamalarında işlemleri çabuklaştırmak için Elektronik İmza Kanunu adı altında 2004 yılında kanunlaşmıştır. 2005 yılında yürürlüğe giren 5237 sayılı yeni TCK’da ise bilişim alanında işlenen suçlara, önceki 765 sayılı kanundan daha ayrıntılı düzenlemeler yapılarak yer verilmiştir. 5237 sayılı TCK’da hırsızlık, dolandırıcılık gibi bazı suçların bilişim sistemleri vasıtasıyla işlenmesi hali de söz konusu suçların nitelikli hali olarak ayrıca hükme bağlanmıştır. Ayrıca Fikir ve Sanat Eserleri Kanunu ile Elektronik İmza Kanunu’nda düzenlenen bilişim suçları da bulunmaktadır. Son olarak ise internet vasıtasıyla işlenen suçlarla mücadelenin etkinliğini arttırmak için 2007 yılında İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun TBMM tarafından kabul edilip yürürlüğe konulmuştur. Bu kanun kapsamında genel olarak internet yayınları üzerinden işlenen suçlarla mücadele amaçlanarak, söz konusu suçların önlenmesi, soruşturulması ve kovuşturması sırasında uygulanabilecek tedbirler kanuni düzenleme altına alınmıştır. Ayrıca bu tedbirlere ilişkin kararları yerine getirmeyenler bakımından da bir takım cezai fiiller söz konusu kanunda kabul edilmiştir.

**Bilişim Suçlarına İlişkin Temel Kavramlar**

**Bilişim Sistemi:** 765 sayılı eski TCK’da yer alan Bilişim AlanındaSuçlara ilişkin düzenlemenin gerekçesinde, “*bilişim**alanından kastın*“ bilgilerin otomatik olarakişleme tabi tutuldukları sisteme ilişkin alan” olduğuortaya konulmuştur. 5237 sayılı yeni TCK’daise bilişim sisteminden bahsedilmiş ve 243. Maddeningerekçesinde “Bilişim sisteminden maksat, verileritoplayıp yerleştirdikten sonra bunları otomatikişlemlere tâbi tutma olanağını veren manyetiksistemlerdir.” denilerek konuya açıklık getirilmeyeçalışılmıştır.765 sayılı TCK’nın *“bilgileri otomatik olarak işleme tabi tutmuş sistem*” ibaresi yerine 5237 sayılı TCK’da aynı anlamı taşımak üzere tercih edilen “*bilişim sistemi*” tabirinden bir veya birden fazla bölümlerden oluşan ve belirli bir sonuca ulaşmak için iş birliği sistemiyle çalışan ve güvenlik araçlarıyla da korunan bir bütün anlaşılmalıdır. Bu tanımlamadan anlaşılacağı üzere bilişim sistemi teriminin en temel yansıması bilgisayarlardır. Bilgisayarı diğer otomatik işlem yapan araçlardan ayırt eden özellik, bilgileri otomatik olarak işleme tabi tutmasının yanında, genel kapsamlı olarak verileri işleyebilme ve kullanabilmesidir. Zira otomatik çamaşır makinesi, hesap makinesi ve uzaktan kumandalı televizyonlarda da bilgileri otomatik işleme tabi tutma özelliği bulunmaktadır. Ancak bunlar genel kapsamlı olarak verileri işleyebilme özelliğine sahip olmadıklarından ve sadece tek bir amaca yönelik işlem yapabildiklerinden bilgisayar ya da bilişim sistemi sayılmazlar.

**Şifreli Yayınların Konumu:** Şifreli yayınların izlenmesindekullanılan dekoder (şifre çözücü) isimli cihazların,bilgileri otomatik işleme tabi tutmuş sistem kavramıiçinde değerlendirilip değerlen dirilemeyeceğiönceki TCK döneminde ülkemizdeki yoğuntartışma konularından birini oluşturmuştur.Bu konuda doktrinde ve uygulamada baskınolan görüş, dekoderin bilgisayar kapsamında olmadığıve bu sebeple de, bu cihaz aracılığı ile gerçekleştirilen eylemlerin eski TCK’nın 11. bab hükümlerinegöre değerlendirilemeyeceği yönündeydi.Nitekim bu cihazlar, bilgisayarın temel özelliği olan enformatik (genel amaçlı kullanılabilme) özelliğine sahip olmayıp tek amaçlı çalışma özelliğine sahiptirler. Eski kanun döneminde uygulamada şifre çözücü cihazlar, bunları kiralayan şirketle yapılan anlaşmalara aykırı olarak başkalarının da istifadelerine sunulmakta ve sonuçta bu fiiller ceza davalarına konu olmaktaydı. Yeni TCK ile söz konusu fiilleri işleyen kimselerin, artık karşılıksız faydalanma suçu kapsamında cezai sorumlulukları doğacaktır.

**Program ve Veriler:** Program ve veriler, bilgisayarın ya da diğer ifadeylebilişim sisteminin soyut yanını oluşturan, sisteministenilen şekilde çalışmasına yardımcı olan veyerine göre kullanıcı ile sistem arasındaki bağlantıyısağlayan unsurlardır. Program, bir seri bilginin,sistemin belli bir yönde çalışmasını sağlamak içinbir araya gelmiş şeklidir. Veri5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Md. 2 fıkra1. (k) bendi: “bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer” olarak tanımlanmıştır.

**İnternet:**  “International” ve “Network” kelimelerininbaşlangıç kısımlarının birleştirilmesi suretiyle oluşturulan“İnternet” terimi, dünya üzerine yayılmış milyonlarca bilgisayarın birbirine bağlanması ile oluşan ağların yine birbirine bağlanması ile oluşan çok geniş yapıdaki bir ağı ifade etmektedir. İnternete “ağlar arası ağ” da denilmektedir. Sanal alan ise bilişim sistemleri ile bunları birbirine bağlayan her türlü veri işletim ağından oluşan, fiziksel yapısı sayısal verilerden ibaret bir alandır.

**BİLİŞİM SİSTEMİNE GİRME**

765 sayılı TCK’da bilişim sisteminden birtakım verilerin ele geçirilmesi cezai müeyyideye bağlanmakla birlikte; verilerin ele geçirilmesi amacına yönelik olmaksızın, sadece sisteme girip orada kalmayı cezalandıran bir hüküm bulunmamaktaydı. Bu bağlamda 5237 sayılı TCK, 243. maddede düzenlenen bilişim sistemine girme suçuyla, bu tür fiilleri ilk defa cezai müeyyideye bağlamış ve hukuk sistemimiz açısından önemli bir eksikliği de ortadan kaldırmıştır. Bunun yanında 243. maddeye 2016 yılında 6698 s. Kanunla eklenen dördüncü fıkrayla, sisteme girmeksizin bilişim sistemi içerisinde veya bilişim sistemleri arasındaki veri nakillerinin izlenmesi de cezai yaptırıma bağlanmıştır. 5237 sayılı TCK’da izinsiz bilişim sistemine girme düzenlemesiyle birlikte, hukuk sistemimizde, Avrupa Siber Suç Sözleşmesi’nin 2. maddesinde öngörülen hukuka aykırı erişim düzenlemesiyle de paralellik sağlanmıştır. Bilişim sistemine girmenin düzenlendiği 5237 sayılı TCK’nın 243. maddesinin metni şu şekildedir:

*Madde 243 –*

 *(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye 1 yıla kadar hapis veya adlî para cezası verilir.*

*(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.*

*(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, 6 aydan 2 yıla kadar hapis cezasına hükmolunur.*

*(4) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, 1 yıldan 3 yıla kadar hapis cezası ile cezalandırılır.*

Bilindiği üzere bir suçun temel şekline kanun koyucutarafından eklenen bazı hususların varlığıhalinde suçun daha az veya daha fazla ceza ile müeyyidelendirilmesinihükme bağlamış olabilir. Butür hallere nitelikli haller denir. Bununla birliktekanuni düzenleme aynı madde altında yer alsa bilesuçun temel şekline ait unsurları bünyesinde aynışekilde barındırmıyorsa, bu durumda söz konusudüzenleme nitelikli hal olarak değil; bilakis ayrı birsuç olarak kabul edilmelidir. TCK m.243’e bakıldığında madde dört fıkradan oluşmaktadır. Birincive dördüncü fıkralarda iki farklı suç tipine yerverilirken, ikinci ve üçüncü fıkralarda ise birincifıkradaki suçun daha az ve daha fazla cezayı gerektirennitelikli hallerine yer verilmiştir. Bu hallerdenilkinin gerçekleşmesi halinde faile suçun temel şeklinenazaran daha az, ikincisinin gerçekleşmesi halindeise daha fazla ceza verilmesi öngörülmüştür.Burada inceleme yapılırken gerek 1. fıkrada gerekse4. fıkrada düzenlenen suçlara ilişkin ortak açıklamalar yapılacak, suç tiplerinin farklılıkları ise bu anlatım sırasında ayrıca vurgulanacaktır. Hukuka aykırı olarak bilişim sistemine girme ve orada kalma fiili, diğer birçok hukuk sisteminde de cezai yaptırıma bağlanarak suç sayılmıştır.

**Suçla Korunan Hukuki Değer:** Suçla ihlal edilen hukuki varlık veya menfaattir. Suçun ihlal ediciliği kaynağını hukuki konudan alır. Her suçta nasıl bir fail varsa, bir de hukuki konu vardır. Bilişim alanındaki suçlara ilişkin düzenlemelerde ise, bilgisayar ortak özelliği teşkil etmek üzere, birden fazla hukuki yarar korunmaya çalışılmaktadır. Bu bağlamda bilişim suçları ile hem kişinin malvarlığına ilişkin hem de kamunun itimadına ve özel hayatın korunmasına ilişkin yararlar koruma altına alınmaktadır. Bilişim sistemine izinsiz girme suçu kapsamında gerek 1. fıkrada gerekse 4. fıkrada düzenlenen suçlarla, bireyin sanal ya da bir başka deyişle dijital ortamdaki özel alanı koruma altına alınmaktadır. Bireye ait bu alanı korumanın farklı gerekçeleri olabilir. Ancak neticede hangi gerekçeyle olursa olsun, üst başlık olarak bu suçlar ile korunan hukuki menfaatin dijital ortamdaki özel alan olarak ifade edilebileceği kanaatindeyiz. Buna karşın doktrinde bu suç ile korunan hukuki menfaate ilişkin farklı tespitlerin de yapıldığı görülmektedir. Bir görüş, bu suç tipiyle özel hayatın gizliliği ve sırları masuniyetini suçun hukuki konusu olarak kabul ederken; bir başka görüş, bu menfaatin bilişim sisteminin güvenliği olarak kabul etmektedir.

**Tipik Maddi Unsur**

**Suçun Konusu:** Suçun konusu, suçun üzerinde gerçekleştirildiği eşya veya kişi olarak ifade edilebilir. Ancak bu, failin fiziki faaliyetinin somut olarak üzerinde gerçekleştiği her kişi ya da eşya değil; sadece suçu düzenleyen normdaki tanımda söz konusu olan kişi veya eşyadır. Bu bağlamda izinsiz bilişim sistemine girme suçunun konusu, bilişim sistemi veya ona ait parçalardan herhangi birisidir. Nitekim suç tipiyle yasaklanan davranışlar bir bilişim sistemi veya onun parçaları üzerinde gerçekleştirilmelidir ki, bilişim sistemine girme suçu oluşabilsin. Bununla birlikte 4. fıkradaki veri nakillerini izleme suçu bakımından suçun konusu ise sistem içinde veya bir bilişim sisteminden diğerine aktarılan “veri”lerdir.

**Fail:** Suçun faili tipik eylemleri gerçekleştiren kişidir. Söz konusu suçlar bakımından fail olmanın gerektirdiği herhangi bir özellik söz konusu değildir. Herkes 243/1 ve 243/4’deki suçların faili olabilir. Suçun özgü suç olma niteliği vs. bulunmamaktadır.

**Mağdur:** Suçla korunan hukuki değerin ait olduğu kimse mağdur olarak nitelendirilir. Girilen bilişim sistemini kullanan kimse m.243/1’deki sisteme izinsiz girme veya orada kalma suçunun mağdurudur. Nakli izlenen verilerin sahibi ise m.243/4’teki veri nakillerini izleme suçunun mağduru konumundadır. Belirtilen suçların mağduru olabilmek bakımından aranan herhangi bir özellik bulunmamaktadır.

**Fiil:** Bilişim Sistemine Girme Suçu ve Veri Nakillerini İzleme Suçu Bakımından iki kısımda ele alabiliriz. Bilişim Sistemine Girme Suçu Bakımından (TCK m.243/1): Kanunda tanımlanan maddi fiil, bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmektir. Sisteme hukuka aykırı olarak girmekle veya izinli girdikten sonra çıkmayarak izinsiz kalmaya devam etmekle suç oluşur. Bilişim sistemine girme suçu, davranışın şekli bakımından yapılacak bir sınıflamada şekli suçlar arasında yer alır. Bir başka deyişle bu suçun oluşumu suç tipinde öngörülen davranışların gerçekleştirilmesi ile tamamlanmış olur. Bunun dışında ayrıca bir zarar veya başkaca bir takım sonuçların gerçekleşmesi gerekmez. Bununla birlikte, davranışın devamlılığı bakımından da suç kesintisiz (mütemadi) bir suçtur. Yani davranış gerçekleştirildiğinde suç oluşur; ancak hemen sona ermez. Örneğin fail bilişim sistemine girip orada kalmakla suçu işlemiş olur. Ama sisteme girip orada kalmasıyla suç sona ermez. Fail sistemde kalmaya devam ettiği müddetçe suç da devam eder. Suçun maddi unsurunun oluşabilmesi bakımından kanun koyucu sadece sisteme girmeyi değil; izinli girse bile izin ortadan kalktıktan sonra izinsiz olarak orada kalmaya devam etmesini de cezai yaptırıma tabi tutmuştur. Bu bağlamda, aynı ortamda çalıştığı iş arkadaşının rızası hilafına bilgisayarına girip, belgelerine bakan kimsenin davranışları bu suçu oluşturacağı gibi, internet vasıtasıyla başka birinin bilgisayarına erişim sağlayıp, onun verilerini inceleyen kimsenin davranışları da bilişim sistemine girme suçunu oluşturur. Kanun koyucu, suç tipinin yer aldığı 243. Maddenin ilk fıkrasında bir bilişim sisteminin bütününe veya bir kısmına ifadesini kullandığı için, bilişim sistemine ait parçalardan herhangi birisine de hukuka aykırı olarak girmek kanaatimizce bilişim sistemine girme suçu kapsamında değerlen dirilmelidir. Bu bağlamda bilişim sistemine bağlı olarak kullanılabilen ve bu bağlamda onun bir parçası olarak nitelendirilen sanal bellek (USB bellek), disket, CD gibi araçların hukuka aykırı olarak incelenmesi ve içerisindeki verilerle temas edilmesi yine inceleme konumuz olan suçu oluşturacaktır. Bu suçun oluşabilmesi için hukuka aykırı girişin bir bilişim sistemi veya onun parçası üzerinde gerçekleştirilmesi gerekir. Bu nedenle uydu üzerinden yayın yapan şifreli bir kanalı şifresini çözmek suretiyle izlemek, bir bilişim sistemine giriş söz konusu olmadığından, bu suçu oluşturmayacaktır. Bilişim sistemine girme suçunun, bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir (TCK m.243/2). Görüldüğü üzere kanun koyucu belirli bir ücret karşılığı yararlanılabilen bir hizmet veren bilişim sistemlerine girme halinde failin temel tip için kabul edilen ceza ile cezalandırılmasını uygun görmemiştir. Örn; internet vasıtasıyla, belirli bir ücret karşılığında bireylere kişilik testi yapıp onların karakterlerine ilişkin tahminler sunan ya da belirli bilgisayar oyunları oynamaları konusunda imkân veren bir sisteme, söz konusu ücreti ödemeksizin şifre kırmak suretiyle erişim sağlayan kimseler bakımından, suçun daha az cezayı gerektiren halinden sorumluluk söz konusu olacaktır. Bununla birlikte bilişim sistemine girme suçunun gerçekleştirilmesi nedeniyle, sistemin içerdiği veriler yok olur veya değişirse, failin 6 aydan 2 yıla kadar hapis cezasıyla cezalandırılması öngörülmüştür (TCK m.243/3). Veri Nakillerini İzleme Suçu Bakımından (TCK m.243/4): Veri nakillerini izleme suçunun maddi unsurunu, veri nakillerini sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek oluşturmaktadır. Eğer fail sisteme girerse bu suç değil; fakat 1. Fıkrada düzenlenen ve yukarıda incelediğimiz suç oluşacaktır. Ayrıca kanunilik ilkesinin bir gereği olarak veri naklinin teknik araçlarla izlenmesi halinde söz konusu suç oluşacaktır. Nitekim kanun koyucu tipik düzenlemede suçun oluşabilmesi bakımından veri naklinin teknik araçlarla izlenmesini açıkça vurgulamıştır. Bu bağlamda teknik araç; aktarılan veriyi izleme olanağı veren her türlü teknik donanımdır.

**Tipik Manevi Unsur** Suçun manevi unsuru gerek 1. fıkradaki gerekse de 4. fıkradaki suç bakımından kasttır. Suçu oluşturan fiillerin hangi amaçla gerçekleştirildiğinin bir önemi yoktur. Bu bağlamda suçların gerçekleşmesi bakımından özel kast aranmaz.Fiillerin taksirle gerçekleştirilmesine ilişkin bir düzenlemeye kanunda yer verilmemiştir. Bu itibarla internette gezinirken dikkatsiz davranıp, kastı olmaksızın gerçekleştirdiği bazı davranışlarla bir bilişim sistemine giren kimseler bakımından cezai sorumluluk doğmayacaktır.

**Hukuka Aykırılık:** Ceza normu ile yasaklanmış tipik davranışların gerçekleştirilmesi hukuka aykırılığın karinesini oluşturur. Ancak bazı hallerde hukuk düzeni, tipiklikte formüle edilmiş olan yasağı hukuka uygunluk nedenleri denilen müsaade edici durumların mevcudiyeti halinde kaldırır. Böylece herhangi bir fiilin hukuka aykırı olduğu konusundaki kesin hüküm, ancak herhangi bir hukuka uygunluk nedeninin somut olayda bulunmaması halinde verilebilir. Sistem sahibinin rızasını almak suretiyle veya hukuken geçerli bir sözleşmeye dayanarak sisteme giren kimse bakımından cezai sorumluluk söz konusu olmaz. Nitekim failin gerçekleştirdiği davranış, her ne kadar tipe uygun ve kasıtlı olsa da, birinci durumbakımından ilgilinin rızası, ikincisi bakımından da hakkın icrası hukuka uygunluk sebepleri bulunduğundan, hukuka aykırılık ortadan kalkacak ve suç oluşmayacaktır. Hukuka aykırılık bakımından, bu suça ilişkin özellikle üzerinde durulması gereken bir başka konu ise bir bilişim sistemine bağlı olarak internet üzerinden erişilebilen internet sayfalarına ilişkindir. Nitekim bazı internet sayfalarında kişilere ait bir takım bilgiler bulunmakta ya da bireylere bir takım hizmetler sunulmaktadır. Herhangi bir şifreli koruma olmaksızın bu tür sayfalara erişim sağlanması halinde de, bu fiillerin suç teşkil edip etmeyeceği düşünülebilir. Eğer sadece belirli kimselerin sayfaya giriş yapabilmesine yönelik belirli bir şifreleme yöntemi kullanılmamışsa, bu durumda söz konusu sayfalara giriş yapılması ve içeriğinin öğrenilmesi bu suçu oluşturmaz.

**Kusurluluk:** Kusurluluk ve kusurluluğu ortadan kaldıranhallere ilişkin söz konusu suçlar bakımından özellikarz eden bir durum söz konusu değildir. Bu bağlamda zorunluluk hali veya karşı konulamayacak bir cebirveya ağır bir tehdit altında buradaki fiilleri gerçekleştirenlerbakımından kınana bilirlik söz konusuolmayacağından cezai sorumluluk doğmayacaktır.Suçun Özel Görünüş BiçimleriSuçun görünüş biçimlerinden, yukarıda verilensuçun başka hangi hallerde işlendiği anlaşılmaktadır.Teşebbüs seviyesinde kalıp kalmadığı, bir içtimahalinin olup olmadığı hep bu konuyla ilgilidir.

**Teşebbüs:** Kişinin işlemeye kastettiği bir suçuelverişli hareketlerle doğrudan doğruya icraya başlayıpda elinde olmayan nedenlerle tamamlayamamasıdır.Bu bağlamda bilişim sistemine girme veveri nakillerini izleme suçları teşebbüse müsaittirler.Sisteme girmeye çalışmak bir teşebbüs halidir.Aynı şekilde veri aktarımını izlemeye yönelik icrahareketlerini gerçekleştirip bunun başarılamamasıyine teşebbüs sorumluluğunu doğurur. İnternet vasıtasıyla girilmesi yasak bir sisteme cebir veya tehdit altında giriş yapan kimseyi bu davranışı gerçekleştirmeye zorlayan kişi veya kişiler dolaylı fail olarak bilişim sistemine girme suçundan sorumlu olacaklardır. Ayrıca cebir veya tehdit kullanmaya ilişkin diğer cezai sorumlulukları ise saklı kalacaktır. İçtima Bilişim sistemine girme suçunun zincirleme suç şeklinde işlenmesi mümkündür. Bir arkadaşının gizlicekişisel bilgisayarına girip onun bilgisayarda tuttuğu günlüğünü okuyan veya özel resimlerine bakan kimse bakımından tek bir davranışla, birden fazla hükmün ihlal edilmesi söz konusu olacaktır. Bu bağlamda faile sadece daha ağır cezayı gerektiren hüküm olan TCK m.134’de öngörülen cezanın verilmesi gerekecektir. Ancak sisteme girildiğinde sistem içerisinde ayrıca şifrelenmiş dosyalara ulaşılması ve bu surette özel hayatın gizliğinin ihlali söz konusu olursa, artık fiilin tekliğinden söz edilemeyecek ve faile her iki suçtan da ayrı ayrı ceza verilecektir. Bunun dışında başkaca suçların işlenmesi amacıyla bilişim sistemine girilmesi ya da veri nakillerinin izlenmesi halinde ne şekilde hareket edileceği konusunda tereddüt doğabilir

**Ceza**: Bilişim sistemine girme suçunun temel şeklinin gerçekleştirilmesi halinde faile seçenekli bir yaptırım ön görülmüştür. Bu bağlamda fail 1 yıla kadar hapis cezasıyla veya adli para cezası ile cezalandırılabilecektir. Kanunun açık hükmü gereği hakimin her iki cezaya da aynı anda hükmetmesi mümkün değildir. Suçun ikinci fıkrada düzenlenen daha az cezayı gerektiren nitelikli halinin vücut bulması durumunda ise, suçun temel şekli için öngörülen cezanın yarı oranına kadar indirilmesi kabul edilmiştir. Bu yarı oranına kadar indirme seçenek yaptırımları her ikisi bakımından da geçerlidir. Yani faile ister hapis cezası isterse adli para cezası verilmiş olsun, her ikisi de ikinci fıkrada belirtilen halin söz konusu olması durumunda yarı oranına kadar indirilecektir. Suçun üçüncü fıkrasında daha fazla cezayı gerektiren nitelikli hal olarak kabul edilen durumun gerçekleşmesine bağlı olarak ise, faile verilecek ceza 6 aydan 2 yıla kadar olarak kabul edilmiştir. Üçüncü fıkrada düzenlenen bu ihtimalin söz konusu olması durumunda failin hapis cezası ile cezalandırılması öngörülmüştür. Bir başka deyişle suçun temel şekli bakımından söz konusu seçenek yaptırımlardan adli para cezası, üçüncü fıkrada öngörülen unsurların gerçekleşmesi halinde uygulama alanı bulmayacaktır. Dördüncü fıkrada düzenlenen veri nakillerini izleme suçu bakımından ise 1 yıldan 2 yıla kadar hapis cezası öngörülmüştür.

**SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME**

TCK’nın 244. maddesinde sistemi engelleme, bozma, verileri yok etme veya değiştirmeye ilişkin düzenlemeye yer verilmiştir. Söz konusu maddede üç ayrı suç tipi bulunmaktadır. Bu bağlamda

m.244/1’de bilişim sisteminin işleyişini engelleme ve bozma;

m.244/2’de bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi veya mevcut verilerin başka yere gönderilmesi;

m.244/4’de ise haksız çıkar sağlama suçu hükme bağlanmıştır.

m.244/3’de ise 1. ve 2. fıkradaki suçlar bakımından ortak bir nitelikli hal düzenlemesine yer verilmiştir.

TCK m.244’deki suçlar ile genel olarak bilişim sistemine yöneltilen zarar verme fiilleri cezai yaptırıma bağlanmıştır. Suça ilişkin düzenleme şu şekildedir:

 *(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

*(2) 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.*

*(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.*

*(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur.*

**Suçla Korunan Hukuki Değer** TCK m.244/1 ve 2’de hükme bağlanan suçlarile bilişim sisteminin soyut unsurları koruma altınaalınmıştır. Dolayısıyla bu suçlar ile korunan hukukimenfaat bilişim sisteminin işlerliğini sağlayan yazılımlardır.Bununla birlikte ilk iki fıkradaki fiillerinişlenmesi suretiyle haksız yarar sağlanmasını yaptırıma tabi kılan m.244/4’deki suç ise gerek 1. ve 2.fıkrada hükme bağlanan suçlarla korunan hukukimenfaati gerekse de bireylerin malvarlığını korumaaltına almaktadır. 4. fıkradaki suç ilekorunan hukuki menfaat bilişim sisteminin işleyişinisağlayan soyut varlıklar ve bireylerin malvarlığıdeğerleridir. Doktrinde söz konusu suçların, bilişimsistemlerine özgü, özel mala zarar verme suçları olduğuifade edilmektedir.

**Tipik Maddi Unsur**

**Fail:** Suçların faili bakımından kanunda herhangi bir özellik aranmamıştır. Bu bağlamda TCK m.244’de hükme bağlanan suçlar özgü suçlardan değildir. Bununla birlikte suç tüzel kişinin yararına işlenmiş ve tüzel kişiye haksız menfaat sağlanmışsa, TCK m.246 uyarınca tüzel kişi hakkında bunlara özgü güvenlik tedbiri uygulanacaktır.

**Mağdur:** Mağdur bakımından da belirli bir özellik aranmamıştır. Bu nedenle tıpkı failde olduğu gibi, herkes kural olarak bu suçların mağduru olabilir. İşleyişi bozulan, engellenen ya da verileri değiştirilen, yok edilen bilişim sisteminin sahibi suçu mağduru olacaktır. Bununla birlikte bilişim sistemi ortak kullanımdaysa, duruma göre her bir hak sahibinin ayrı ayrı mağdur olması da söz konusu olabilecektir. Örneğin iki kardeşin ortak kullanımındaki bir bilgisayara girilerek veriler silindiğinde, kardeşlerin her ikisi de mağdur olacaktır. 4. fıkradaki suç bakımından ise işleyişi bozulan, verileri yok edilen vs. bilişim sisteminin sahibinin yanında aleyhine haksız çıkar elde edilen kimse de mağdur olacaktır. Birçok olay bakımından bunların her ikisinin de aynı kişi olması muhtemeldir. Ancak ikisinin farklı kimseler olduğu durumlarda mağdur sayısının da birden fazla olacağını ifade etmek gerekir.

**Suçun Konusu**: TCK m.244/1’deki suç bakımından suçun konusu bilişim sistemi iken; m.244/2’deki suç bakımından sistemdeki verilerdir. Nitekim kanuni düzenlemede, suç teşkil eden eylemlerin bunlar üzerinde işlenmesi hükme bağlanmıştır. m.244/4’deki suç bakımından ise haksız çıkarın olaya göre somutlaştığı varlıklar suçun konusunu oluşturur.

**Fiil:** Bilişim Sisteminin İşleyişini Engelleme veyaBozma Suçu Bakımından (TCK m.244/1)TCK m.244’ün birinci fıkrasında sistemin işleyişini engelleme ve bozma suçu düzenleme altına alınmıştır.Buradaki eylemlerin bilişim sistemi üzerinde gerçekleştirilmesi öngörülmüştür. Suç kapsamındasistemi engelleme ve bozma seçimlik hareketlerdendir.Bunlardan sadece birisinin gerçekleştirilmesisuçun tekemmülü bakımından yeterlidir. Sistemüzerinde hem engelleme hem de bozma hareketlerigerçekleştirilirse, bu durumda bunların seçimlikhareketler olmaları dolayısıyla failin tek bir suçtansorumluluğu doğacaktır. Engellemek, bir şeyin yapılmasınıya da gerçekleşmesini önlemek; bozmakise bir şeyi kendisinden beklenen işi yapamayacakduruma getirmektir. Sistemin veri işlemesininönüne geçilmesi ya da sistemin işleyişininbir süre de olsa kesintiye uğratılması söz konususuçu oluşturacaktır. Sistem üzerindekioynamalar sonucu sistemin çalışması yavaşlamışsa,sistem hızını kaybetmişse de bu suçun oluştuğunukabul etmek gerekir. Bahsedilen fiillerin, bir banka veya kredikurumuna ya da bir kamu kurum veya kuruluşunaait bilişim sistemi üzerinde işlenmesi cezayı arttıranbir neden olarak kabul edilmiştir. Böyle bir arttırmayer veril mesinin temel nedeni, gerçekleştirilecekeylemler nedeniyle bu kurum ve kuruluşların hizmetlerinin aksamasının, toplum daki diğer bireylerbakımından da zararlı sonuçlar ortaya çıkartabilecekolmasıdır. Örn: UYAP ya da MERNİS gibikamu kurumlarının kullanımında olan sistemlerüzerinde söz konusu fiillerin gerçekleştirilmesibu ağırlaştırıcı sebebin varlığına vücut verecektir.

Bilişim Sistemindeki Verilerin Bozulması, Yok Edilmesi, Değiştirilmesi, Erişilmez Kılınması, Sisteme Veri Yerleştirilmesi veya Mevcut Verilerin Başka Yere Gönderilmesi Suçu Bakımından (TCK m.244/2) TCK m.244/2’de bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi veya mevcut verilerin başka yere gönderilmesi cezai yaptırıma tabi kılınmıştır. İkinci fıkradaki düzenlemeyi birinci fıkradan ayıran en önemli farklılıklardan bir tanesi, ikinci fıkradaki eylemlerin sistem üzerine değil; bilakis sistemdeki veriler üzerinde gerçekleştirilmesi zorunluluğudur. Bu bağlamda sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, bilişim sistemine veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi ikinci fıkra kapsamında suç oluşturacaktır. Bununla birlikte verinin tümden silinmesi ve böylelikle verinin ortadan kaldırılması şeklinde de ikinci fıkra kapsamındaki fiillerin gerçekleştirilmesi mümkündür. Bilişim Sistemi Aracılığıyla Haksız Çıkar Sağlama Suçu Bakımından (TCK m.244/4) TCK m.244/4’de bilişim sistemi aracılığıyla haksız yarar sağlama suçu düzenleme altına alınmıştır. Bu bağlamda yukarıda açıkladığımız m.244/ 1 ve 2’de düzenlenen fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, cezalandırılması hükme bağlanmıştır. Söz konusu düzenleme bakımından ilk dikkati çeken husus, failin dördüncü fıkra kapsamında sorumlulu ğunun doğabilmesi için öncelikle birinci veya ikinci fıkra kapsamındaki eylemlerden birisini işlemiş olması zorunluluğudur. Bununla birlikte fail, gerçekleştirdiği bu eylemlere bağlı olarak kendisi veya başkası yararına haksız bir çıkar sağlamış olmalıdır.

**Tipik Manevi Unsur:** TCK m.244’de düzenlenen söz konusu suçlarkasten işlenebilen suçlardır. Kanunda taksirli şekillerineaçıkça yer verilmediği için, bu suçların taksirleişlenmesi mümkün değildir. Kast bakımındanise genel kast yeterlidir.

**Hukuka Aykırılık:** TCK m.244’te tanımlanan suçlar bakımındanhakkın icrası, ilgilinin rızası ve görevin ifası hukukauygunluk sebeplerin ortaya çıkması söz konusuolabilecektir. Bu bağlamda başkasına ait bilişimsistemine, bu kimsenin rızasıyla girip verileri nakleden,silen veya bozan kişi bu eylemlerini ilgilininrızası üzerine gerçekleştirdiğinden hukuka aykırılıkortadan kalkacaktır. Yine CMK m.134’e göre yetkilimerciin kararı ile sisteme girip arama, kopyalamave el koyma işlemlerini gerçekleştiren kollukgörevlisi bakımından görevin ifasına dayalı hukukauygunluk nedeni oluşacaktır.

**Kusurluluk:** Kusurluluk ve kusurluluğu ortadan kaldıranhallere ilişkin söz konusu suçlar bakımından özellikarz eden bir durum söz konusu değildir. Bu bağlamdazorunluluk hali veya karşı konulamayacak bir cebirveya ağır bir tehdit altında buradaki fiilleri gerçekleştirenlerbakımından kınana bilirlik söz konusuolmayacağından cezai sorumluluk doğmayacaktır.

**Suçun Özel Beliriş Biçimleri:** Suçun özel beliriş biçimlerinden, yukarıda verilensuçun başka hangi hallerde işlendiği anlaşılmaktadır.Teşebbüs seviyesinde kalıp kalmadığı, bir içtimahalinin olup olmadığı hep bu konuyla ilgilidir.

**Teşebbüs:** TCK m.244’te düzenlenen suçlara teşebbüsmümkündür. Bu bağlamda örneğin bilişim sisteminegirip verileri bozmaya yönelik icra hareketlerinebaşladıktan sonra, verileri bozmayı başaramadanyakalan kimse, ikinci fıkra kapsamındasuça teşebbüsten sorumlu olacaktır. Yine sisteminişleyişini engellemeye çalışırken ama engelleyemedenyakalanan kimse bakımından da birinci fıkrakapsamında teşebbüsten cezai sorumluluk ortayaçıkacaktır.TCK m.244/1 ve2’deki suçlar, TCK m.244/4’deki suçun unsurunuoluşturmaktadır. Dolayısıyla m.244/4’deki suç birbileşik suç düzenlemesidir. Bu bağlamda Haksız birçıkar sağlamak amacıyla bilişim sisteminin işleyişibozulur ama haksız çıkar elde edilemezse, TCKm.244/1’deki suçu işlemekten değil; bilakis TCKm.244/4’deki haksız çıkar sağlama suçuna teşebbüstencezai sorumluluk doğacaktır.

**İştirak:** İştirake ilişkin olarak bu suçlar bakımından özellik arz eden bir durum söz konusu değildir. Herkes tarafından işlenebilen söz konusu suçlarda, özel bir faillik niteliği de aranmamaktadır. Bu bağlamda bir bilişim sisteminin işleyişini bozmak konusunda fiil üzerinde ortak hakimiyet kurmak suretiyle suçu birlikte işleyenler m.244/1’deki suçu müşterek fail olarak gerçekleştirmekten sorumlu olacaklardır. Bunun yanında yardım etme ve azmettirme şeklinde suçların işlenişine şerik olarak katılmak da mümkündür.

**İçtima:** TCK m.244/4’deki suçun bir bileşik suç düzenlemesiolması dolayısıyla, haksız bir çıkar sağlamakamacıyla bilişim sisteminin işleyişi bozulurve çıkar sağlanırsa; fail TCK m.244/1’deki suçuişlemekten dolayı cezalandırılmaz. Suç4. fıkradaki suçun unsuru olduğu için sadece TCKm.244/4’deki haksız çıkar sağlama suçundan cezaisorumluluk doğacaktır.Yine TCK m.244/4’deki suç, açık düzenleme gereği,ancak çıkar sağlamanın başka bir suçu oluşturmaması halinde uygulama alanı bulabilecektir. Bubağlamda bilişim sistemindeki verileri değiştirmeksuretiyle dolandırıcılık yapan kimse, bu eylemi niteliklidolandırıcılık suçunu oluşturacağından TCKm.158 hükmü gereğince cezalandırılır. Bu durumdaTCK m.244/4’deki suç uygulama alanı bulmaz. Nitekimbelirtilen şekilde haksız çıkar sağlama başkabir suçu (nitelikli dolandırıcılığı) oluşturmaktadır.

**Ceza:** Birinci fıkra kapsamında suç işleyen fail için 1 yıldan 5 yıla kadar hapis cezası öngörülmüştür.Eğer failin fiili ikinci fıkra kapsamındaysa bu durumdafaile 6 aydan 3 yıla kadar hapis cezası verilmesihükme bağlanmıştır. Bu fiillerin bir bankaveya kredi kurumuna ya da bir kamu kurum veyakuruluşuna ait bilişim sistemi üzerinde işlenmesihalinde ise verilecek cezanın yarı oranında arttırılmasısöz konusu olacaktır. Son olarak suçun dördüncüfıkra kapsamında gerçekleştirilmesi halinde,2 yıldan 6 yıla kadar hapis ve 5000 güne kadaradli para cezasına hükmolunacağı düzenlenmiştir.Bu son fıkraya giren halde kanun koyucu fail bakımındanhem hapis hem de adli para cezası uygulanmasınıtercih etmiştir. Bununla birlikte sözkonusu suçların işlenmesi suretiyle yararına haksızmenfaat sağlanan tüzel kişiler varsa, bunlar hakkındada tüzel kişilere özgü güvenlik tedbirlerine hükmolunur(TCK m.246; m.60).

**BANKA VE KREDİ KARTLARININ KÖTÜYE KULLANILMASI**

TCK m.245’te banka ve kredi kartlarının kötüye kullanılmasını hüküm altına almıştır. Söz konusu düzenleme şu şekildedir; *Madde 245 –*

*(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kul-lanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve 5000 güne kadar adlî para cezası ile cezalandırılır.*

*(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.*

*(3) Sahte oluşturulan veya 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, dört yıldan sekiz yıla kadar hapis ve 5000 güne kadar adlî para cezası ile cezalandırılır.*

*(4) 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,*

*c) Aynı konutta beraber yaşayan kardeşlerden birinin zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.*

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

**Suçla Korunan Hukuki Değer**

Söz konusu suçlar ile korunması amaçlanan hukuksal değere ilişkin ipuçları madde gerekçesinde verilmiştir. Buna göre suç tipi, *banka veya* *kredi kartlarının hukuka aykırı olarak kullanılması* *suretiyle bankaların veya kredi sahiplerinin zarara* *sokulmasını,* *bu yolla çıkar sağlanmasını önlemek ve* *failleri cezalandırmak amacıyla kaleme alınmıştır.* Dolayısıyla suçlarla korunan hukuki değer karma bir niteliktedir. Birinci fıkradaki suç ile bireylerin malvarlığı koruma altına alınırken, ikinci ve üçüncü fıkradaki suçlarla ise malvarlığının yanında, banka ve kredi kartlarının sahihliğine ilişkin kamu güveninin devamlılığı koruma altına alınmıştır.

**Tipik Maddi Unsur**

**Fail:**Suçların faili herkes olabilir. Bu bakımdan suçun özgü suç niteliği söz konusu değildir. Bununla birlikte suç tüzel kişinin yararına işlenir ve tüzel kişiye haksız menfaat sağlanırsa, TCK m.246 uyarınca tüzel kişi hakkında bunlara özgü güvenlik tedbiri uygulanacaktır (Bkz. TCK m.60).

**Mağdur:**Söz konusu suçların mağduru kural olarak herkes olabilir. Bu bağlamda mağdur bakımından özellik arzeden bir durum bulunmamaktadır. Birinci fıkradaki suç bakımından banka veya kredi kartının hamili mağdurdur. Bununla birlikte ikinci fıkradaki suç bakımından Yargıtay, suçun mağdurunun, “kartın henüz kullanılmamış olması nedeniyle,” hesap sahibi değil, bilakis banka olduğu görüşündedir. Üçüncü fıkradaki suç bakımından ise aleyhine haksız yarar sağlanan kimse suçun mağduru sayılacaktır.

**Suçun Konusu:**TCK m.245/1 ve 3’de düzenlenen suçlar bakımından suçun konusunu elde edilen yararın somutlaşmış hali oluşturmaktadır. Bu bağlamda elde edilen yarar para şeklinde ise somut olay bakımından bu para, hisse senedi şeklinde ise söz konusu hisse senedi suçun konusunu oluşturacaktır. TCK m.245/2’deki suç bakımından ise üzerinde eylemlerin gerçekleştirildiği banka veya kredi kartı oluşturmaktadır. Banka ve kredi kartlarının hukuki tanımına ilişkin olarak 5464 sayılı Banka ve Kredi Kartları Kanunundaki düzenlemelere bakmak gereklidir.

**Fiil:**Fiili, başkasına ait banka veya kredi kartını kullanarak yarar sağlama suçu bakımından, sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçu bakımından ve sahte banka veya kredi kartı kullanarak yarar sağlama suçu bakımından ele alınır. Başkasına Ait Banka veya Kredi Kartını Kullanarak Yarar Sağlama Suçu bakımından (TCK m.245/1) Birinci fıkra kapsamında suçun oluşması için öncelikle sahte olmayan, gerçek bir banka veya kredi kartının bulunması gereklidir. Eğer kart sahte ise bu durumda ancak ikinci veya üçüncü fıkra kapsamında suç oluşabilecektir. Başkasına ait banka veya kredi kartının fail tarafından ele geçirilmiş olması da gereklidir. Ancak ele geçirmenin ne şekilde olduğunun bir önemi yoktur. Kartın ele geçmesi asıl sahibinin rızasıyla olabileceği gibi, rızası dışında da olabilir. Buradaki ele geçirme başka bir suçu oluşturuyorsa, bu durumda fail söz konusu suçtan ayrıca cezalandırılacaktır. Örneğin kredi kartını çalan kişi daha sonra bunu kötüye kullanmışsa hem m.245/1 kapsamında yarar sağlamadan hem de hırsızlıktan ayrı ayrı cezai sorumluluğa sahip olacaktır. Bununla birlikte failin kartı sadece ele geçirmiş olması, TCK m.245/1’deki suçu veya bu suça teşebbüsü oluşturmaz. Eğer ele geçirmenin kendisi hırsızlık veya dolandırıcılık gibi başka bir suçu oluşturuyorsa, sadece bu suçtan sorumluluk doğar. Suçun oluşumu bakımından kredi kartının fiziken ele geçirilmesi gerekli değildir. Nitekim kredi kartları, 5464 s. Banka ve Kredi Kartları Kanununda fiziki varlığı bulunmayan kart numarasını da içine alacak şekilde tanımlanmıştır. Ancak bu durum sadece kredi kartları bakımından geçerlidir. Banka kartları bakımından benzer bir ifadeye kanunda yer verilmediğinden, sadece banka kartı numarasının ele geçirilmesi suretiyle yarar sağlanması halinde bu suç oluşmayacaktır.

**Bilişim Alanında Suçlar ve Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri**

**Tipik Manevi Unsur** TCK m.245’te düzenlenen suçlar kasten işlenebilenbir suçlardır. Kanunda suçların taksirli halineyer verilmediğinden bahsi geçen eylemlerin taksirleyapılması suça vücut vermeyecektir.

**Hukuka Aykırılık** Söz konusu suçlar bakımından hukuka uygunluknedenleri koşulları oluştuğu ölçüde uygulamaalanı bulacaktır. Bu bağlamda önem arz eden ayrıksıbir durum bulunmamaktadır. Bununla birlikteayrıca vurgulamak gerekir ki; TCK m.245/1’deilgilinin rızası tipik düzenlemede açıkça zikredildiğinden,ilgilinin rızasının varlığı durumunda artıkhukuka uygunluk sebebi; bilakis tipikliği kaldıranbir rıza söz konusu olacaktır.

**Kusurluluk** Kusurluğu kaldıran sebepler bu suçlar bakımından da geçerlidir. Bu bağlamda örneğin, karşı konulamayacak bir cebir veya ağır bir tehdit altında sahte kredi kartı üreten kimsenin kınana bilirliği ortadan kalkacağından, cezai sorumluluğu doğmayacaktır.

**Şahsi Cezasızlık Sebepleri** Kanun koyucu TCK m.245/1’deki suç bakımındanbazı şahsi cezasızlık sebeplerine yer vermiştir.Bu bağlamda söz konusu cezasızlık sebepleri sadecefiilin birinci fıkra kapsamında kalması halindegeçerlidir. Eğer gerçekleştirilen fiil diğer fıkralarkapsamındaysa, cezasızlık söz konusu olmayacaktır.Buna göre; birinci fıkra kapsamında suçun,

a)Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz. Eğer eşler hakkında boşanmasalar bile ayrılık kararı verilmiş ise şahsi cezasızlık sebebi geçerli değildir.

Bunun yanında anne babanın kredi kartını izinsiz kullanan çocuk bakımından cezasızlık sebebi söz konusu olacağı gibi, kayın validesinin kartını rızası dışında kullanan damat bakımından da aynı cezasızlık sebebi geçerlidir. Son olarak belirtmek gerekir ki, kardeşler bakımından şahsi cezasızlık sebebinin geçerli olması için kardeşlerin aynı evde yaşıyor olması zorunludur. Ayrı evlerde yaşayan kardeşlerden birisi diğerinin kredi kartını rızası olmaksızın kullandığında, şahsi cezasızlık sebebi geçerli olmaz.

**Etkin Pişmanlık** Kanun koyucu, yine birinci fıkra kapsamına girenfiillerle ilgili olarak etkin pişmanlık halini de kabuletmiştir. Söz konusu fiiller bakımından malvarlığına karşı suçlara ilişkin etkin pişmanlıkhükümleri uygulanacaktır. Birinci fıkra kapsamı dışındakalan fiillerle ilgili olarak etkin pişmanlık hükümlerininuygulanması ise mümkün değildir.Bu bağlamda, birinci fıkra kapsamındaki suç*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.* Bu *etkin pişmanlığın**kovuşturma başladıktan sonra ve fakat hüküm**verilmezden önce gösterilmesi halinde, verilecek cezanın**yarısına kadarı indirilir. Kısmen geri verme**veya tazmin halinde etkin pişmanlık hükümlerinin**uygulanabilmesi için, ayrıca mağdurun rızası aranır**(TCK m.168).*

**Suçun Özel Beliriş Biçimleri** Suçun özel beliriş biçimlerinden, yukarıda verilensuçun başka hangi hallerde işlendiği anlaşılmaktadır.Teşebbüs seviyesinde kalıp kalmadığı, bir içtimahalinin olup olmadığı hep bu konuyla ilgilidir.

**Teşebbüs** Söz konusu suçlara teşebbüs mümkündür.Örneğin başkasına ait kredi kartını kullanırkenyakalanan kimse, doğrudan icra hareketlerine başlamış,ancak fiili tamamlayamamış olduğundan birinci fıkra kapsamında suça teşebbüsten sorumluolacaktır. Yine sahte kredi kartı yapmak için icrahareketlerine başladıktan sonra sahte kart yapmayıtamamlamadan yakalanan kimse de ikinci fıkrakapsamında suça teşebbüsten sorumlu olur.

**İştirak** TCK m.245 kapsamında düzenlenen suçlaraiştirakin her türlüsü mümkündür. Özellik arz edenherhangi bir durum bulunmamaktadır. Bu bağlamdaiki kişi fiil üzerinde hâkimiyet kurmak suretiylesahte bir kredi kartı üretirlerse, müşterek fail olarakikinci fıkra kapsamında suçtan sorumlu olacaklardır.Aklında böyle bir fiil gerçekleştirme düşüncesiolmayan birisine, sahte kart üretme fikrini aşılayankişi ise, bu düşünceyi oluşturduğu kişinin fiili gerçekleştirmesihalinde azmettiren olarak sorumluolacaktır. Fiili gerçekleştiren kişi ise müstakil failolarak cezai sorumluluğa sahip olur.

**İçtima** TCK m.245/1 kapsamında; fail başkasına aitkredi kartını alır ve birden fazla kez kullanırsa, TCKm.43/1 kapsamında zincirleme suç hükümleri uygulama alanı bulacaktır. Bununla birlikte başkasına ait banka kartından çok kısa aralıklarla birden fazla defa para çekme eylemi gerçekleştirilmesini Yargıtay tek suç saymıştır.Fail kullandığı başkasına ait kredi kartını başka bir suçla, örn yağma suçu, işlemek suretiyle ele geçirmişse, gerçek içtima hükümleri uygulanacak ve hem yağmadan hem de TCK m.245/1 kapsamında cezai sorumluluğa sahip olacaktır.

**Ceza** Birinci fıkra kapsamındaki fiiller bakımındanhem adli para cezası hem de hapis cezası öngörülmüştür.Bu kapsamdaki fiillerin faili 3 yıldan 6 yıla kadar hapis ve 5000 güne kadar adli para cezasıile cezalandırılacaktır. İkinci fıkra kapsamındakifiiller için de hapis ve adli para cezasının birlikteuygulanmasını kabul eden kanun koyucu cezalarınmiktarında da belirli oranda arttırıma gitmiştir.Buna göre ikinci, fıkra kapsamındaki fiillerin faili,3 yıldan 7 yıla kadar hapis ve 10000 güne kadar adli para cezası ile cezalandırılacaktır. Üçüncüfıkra kapsamındaki fiiller için ise hapis cezasının miktarı önceki fıkralarda öngörülenden daha fazlabelirlenirken, para cezasının miktarı birinci fıkraylaaynı sınırlar içinde kabul edilmiştir. Bu bağlamdaüçüncü fıkra kapsamında fiili gerçekleştiren kişi4 yıldan 8 yıla kadar hapis ve 5000 günekadar adli para cezası ile cezalandırılır.

**YASAK CİHAZ VE PROGRAMLAR SUÇU**

TCK’da, 24.03.2016 tarihinde yapılan değişiklikle, “Yasak Cihaz ve Programlar” başlıklı 245/A maddesi eklendi. Söz konusu madde ile bilişim alanında bireylere, özellikle zararlı yazılım ve cihazlara karşı ek bir koruma kalkanı sağlanmıştır. Doktrinde uzun zamandır dillendirilen bu ihtiyaç söz konusu düzenleme ile karşılanmaya çalışılmıştır. Nitekim bilişim araçlarından kişilerin özel bilgilerini çalmak amacıyla virüs programı üretilmesi ve bunların kullanımının büyük zararlara yol açması, benzer şekilde sadece bilişim sistemlerine zarar verme amaçlı zararlı yazılımlar üretilmesi son dönemde sıklıkla rastlanan eylemlerdi. Bunlarla mücadelede hukuki zemini güçlendirmek adına özel bir suç tipiyle düzenleme yapılması yerinde olmuştur. TCK’nın söz konusu 245/A maddesinde yer alan düzenleme şu şekildedir; *Yasak cihaz veya programlar*

***Madde 245/A-*** *(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi 1 yıldan 3 yıla kadar hapis ve 5000 güne kadar adli para cezasıyla cezalandırılır*

**Suçla Korunan Hukuki Değer**

Suçla korunan hukuki değer bireyin bilişim alanındaki menfaatleridir. Bilişim alanındaki menfaat kavramı, özel hayat ya da malvarlığı gibi kavramlardan çok daha geniş bir içeriğe sahiptir. Yasak cihaz ve programlara ilişkin suç tipiyle, cihaz ve programların geniş anlamda bilişim suçlarının işlenmesi amacıyla yapılması ve oluşturulması halinde, bunların imali, ithali, sevki, vs. yasaklanmıştır. Yasak cihaz ve programlar suçunun tüm bilişim suçlarının koruma altına aldığı menfaatler toplamını korumaya çalıştığını, bu bağlamda da suçla korunan hukuki değerin bilişim alanındaki menfaatler toplamı olduğunu söylemek yanlış olmayacaktır.

**Tipik Maddi Unsur**

**Fail:**Suçun faili herkes olabilir. Bu bakımdan suçun özgü suç niteliği söz konusu değildir. Ayrıca bu suç, herhangi bir tüzel kişinin yararına işlenir ve tüzel kişiye haksız menfaat sağlanırsa, TCK m.246 uyarınca tüzel kişi hakkında bunlara özgü güvenlik tedbiri uygulanacaktır (Bkz. TCK m.60).

**Mağdur**:Bu suçun mağduru genel olarak toplumu oluşturan bireylerdir. Bu bağlamda mağduru belirli bir kimse olmayan suç kategorisinde değerlendirilmelidir.

**Suçun Konusu:**Suçun konusunu geniş anlamda bilişim suçlarını işlemek amacıyla yapılmış cihaz ve programlar oluşturmaktadır. Nitekim bilişim suçlarının işlenmesi amacıyla oluşturulmaları veya yapılmaları halinde, bunların üretimi, nakli, ithali, vs. suç tipinde yasaklanmaktadır. Suçun üzerinde işlendiği varlıklar olmaları dolayısıyla, suçun konusunu da belirtilen amaçla yapılmış cihaz ve programlar oluşturmaktadır.

**Fiil:**Suç tipiyle geniş anlamda bilişim suçlarının işlenmesine yönelik olarak yapılmış veya oluşturulmuş *bir cihazın, bilgisayar programının, şifrenin* *veya sair güvenlik kodunun* imali, ithali*,* sevki, nakli, depolanması, kabulü, satılması, satışa arzı, satın alınması, başkalarına verilmesi veya bulundurulması cezai yaptırıma tabi kılınmıştır. Bu bağlamda suç seçimlik hareketli bir suçtur. Kanunilik ilkesi bakımından sorun oluşturmaması amacıyla, kanun koyucunun suç kapsamına girecek eylemleri ayrıntılı şekilde oluşturduğu görülmektedir. İmal, ithal, satmak, satışa arzetmek, ivazsız vermek, almak, vs. gibi sayılan eylemlerden bir tanesinin gerçekleştirilmesi söz konusu suçun oluşması bakımından yeterlidir. Bununla birlikte belirtilen seçimlik hareketlerden birkaçının aynı kimse tarafından işlenmesi durumu da ortaya çıkabilir. Bu durumda fail yine tek suçtan sorumlu olacaktır. C*ihazın, bilgisayar* *programının, şifrenin veya sair güvenlik kodunun* suçun konusunu teşkil edebilmesi için TCK’nın bilişim alanında suçlara ilişkin bölümünde yer alan suçlardan birinin ya da *bilişim sistemlerinin araç* *olarak kullanılması suretiyle işlenebilen diğer suçların* *işlenmesi için yapılması veya oluşturulması* aranmıştır. Yazılımlar bakımından herhangi bir ayrım yapılmadığı, belirtilen suçların işlenmesi amacıyla oluşturulan her türlü yazılımın suç kapsamında olacağı görülmektedir. Bu bağlamda özellikle yazılımların geniş anlamda bilişim suçlarının işlenmesine yönelik üretildiğini bilerek bunları depolayan yer sağlayıcılar bakımından da ciddi bir cezai sorumluluk alanı söz konusu olmaktadır Suçun oluşabilmesi bakımından *cihazın, bilgisayar* *programının, şifrenin veya sair güvenlik kodu*nun geniş anlamda bilişim suçlarının işlenmesine yönelik oluşturulduğunun veya yapıldığının bilinmesi gerekir. Eğer fail, böyle bir bilgisi olmadan bu tür bir cihaz veya programı alırsa veyahut satarsa cezai sorumluluğa sahip olmaz. Nitekim bu halde TCK m.30/1 kapsamında fiilin maddi unsurlarının gerçekleştiği konusunda fail hataya düşmüş olacak ve kasten işlenen TCK m.245/A kapsamındaki suçtan sorumlu tutulamayacaktır. Bununla birlikte bilişim güvenliğini test etmek için sisteme giriş veya verileri sistemden almaya yönelik test programları (zafiyet testleri yazılımı) yapan kimselerin programı yaparken ki amacı suç işlemek olmadığı için cezai sorumlulukları doğmayacaktır. Nitekim bu kişilerin söz konusu programları yapma sebebi geniş anlamda bir bilişim suçu işlemek değildir. Oysa tipik düzenleme, geniş anlamda bilişim suçlarını işlemeye yönelik olarak *cihaz, bilgisayar programı, şifre veya sair güvenlik kodu*nun yapılması veya oluşturulmasını aramaktadır.

**Tipik Manevi Unsur** Suç kasten işlenebilen bir suçtur. Kanunda taksirli haline yer verilmediğinden bahsi geçen eylemlerin taksirle yapılması suça vücut vermeyecektir.

**Hukuka Aykırılık** Suç bakımından koşulları gerçekleştiği sürecehukuka uygunluk nedenlerinin hukuka aykırılığıkaldıran bir sebep olarak ortaya çıkması söz konusu olabilir. Bu bağlamda kendi bilişim sistemine süreklisaldırıda bulunan bir başka sisteme, saldırıyıgerçekleştirdiği anda müdahalede bulunarak zararvermesi için bir yazılım yapan kimsenin, böyle biryazılım imal etmekten dolayı sorumluluğu oluşmaz.Çünkü yazılım saldırı anında saldırıyı yapansisteme zarar vermek amacıyla oluşturulmuştur.Meşru savunmada kullanılmaya yönelik böyle birprogram yapılması, TCK m.245/A kapsamındakisuçun hukuka aykırılık unsurunu ortadan kaldıraraksuçun oluşmasını engeller.

**Kusurluluk** Kusurluğu kaldıran sebepler bu suç bakımındanda geçerlidir. Bu bağlamda örneğin, TCK m.28 kapsamındakarşı konulamayacak bir cebir veya ağır birtehdit altında bilişim suçlarını işlemeye yönelik cihazimal eden kimse cezai sorumluluğa sahip olmaz.Ancak bu durumda cebir ve tehditle ona söz konusucihazı imal ettiren kimsenin TCK m.37 kapsamındadolaylı fail olarak cezai sorumluluğu doğar.

**Suçun Özel Beliriş Biçimleri** Suçun özel beliriş biçimlerinden, yukarıda verilensuçun başka hangi hallerde işlendiği anlaşılmaktadır.Teşebbüs seviyesinde kalıp kalmadığı, bir içtimahalinin olup olmadığı hep bu konuyla ilgilidir.

**Teşebbüs** Söz konusu suça teşebbüs mümkündür. Ancaksırf hareket suçu olması dolayısıyla, teşebbüs ancakicra hareketleri tamamlanmadan söz konusu olabilir.Nitekim icra hareketleri tamamlandıktan sonrasuçun oluşmaması diye bir durum söz konusudeğildir.

**İştirak** Bu suça iştirakin her türlüsü mümkündür. Özellikarzeden herhangi bir durum bulunmamaktadır.Bu bağlamda iki kişi fiil üzerinde hakimiyet kurmaksuretiyle bilişim sistemlerine zarar verecek bir yazılımyaparlarsa, müşterek fail olarak bu suçtan sorumluolacaklardır (TCK m.37). Aklında böyle bir programyazma düşüncesi olan arkadaşının, bu düşüncesinidestekleyen ve suç işleme kararını kuvvetlendirenkimse bakımından ise TCK m.39 kapsamında yardımetmeden dolayı cezai sorumluluk ortaya çıkacaktır.

**İçtima** Söz konusu suç, mağduru belirli bir kimseolmayan suç kategorisinde yer aldığı için TCKm.43/1 kapsamında zincirleme suç şeklinde işlenebilir.Örneğin tek suç işleme kararının icrası kapsamındabir bilişim sistemine gizlice sızmaya imkân tanıyan programlar yazan kimse TCK m.43/1’egöre cezalandırılacaktır.Bu noktada ayrıca belirtmek gerekir ki; suç tipinde,*bir cihazın, bilgisayar programının, şifrenin**veya sair güvenlik kodunun;* geniş anlamda bilişimsuçlarını işlemek *için yapılması veya oluşturulması**durumunda, bunları imal eden, ithal eden, sevk**eden, nakleden, depolayan, kabul eden, satan, satışa* **arz** *eden, satın alan, başkalarına veren veya bulunduran**kişi*nin cezalandırılacağı hükme bağlanmıştır.Suçun oluşabilmesi için cihaz,program*, şifre veya kodun* kullanılarak bir bilişimsuçunun işlenmesine gerek yoktur. Eğer bilişim sistemi kullanmak suretiyle hırsızlık yapmak için birprogram yazan kimse, yazdığı programı kullanarak ayrıca planladığı hırsızlığı da gerçekleştirirse gerekm.245/A’daki inceleme konumuz olan suçtan gerekse TCK m.142 kapsamında bilişim sistemlerinikullanmak suretiyle hırsızlıktan dolayı ayrı ayrı cezaisorumluluğa sahip olacaktır.

**Ceza** Suç karşılığında uygulanacak yaptırım olarakgerek hapis gerekse de adli para cezası öngörülmüştür.Bu bağlamda söz konusu eylemleri gerçekleştirenkimsenin *1 yıldan 3 yıla kadar hapis ve 5000**güne kadar adli para cezası* ile cezalandırılması hükmebağlanmıştır. Ayrıca söz konusu suçun işlenmesisuretiyle yararına haksız menfaat sağlanan tüzelkişiler hakkında bunlara özgü güvenlik tedbirlerinede hükmolunacaktır (TCK m.246; m.60).

**BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA**

Ceza muhakemesi sırasında bireysel menfaatle kamusal menfaat arasındaki dengeyi sağlamanın en zorlu olduğu kurumlardan birisi de koruma tedbirleridir. Nitekim bu tedbirler aracılığıyla, hala suçsuzluk karinesinden faydalan makta olan şüpheli veya sanık ile bazı üçüncü kişilerin temel haklarına önemli müdahaleler gerçekleştirilmektedir. Koruma tedbirleri vasıtasıyla soruşturma organlarına etkin takibat gerçekleştirebilme imkânı tanınırken; bu tedbirlerin uygulanmasını belirli koşulların varlığına bağlamak suretiyle de temel haklara müdahalenin orantılı şekilde gerçekleşmesi teminat altına alınmaya çalışılmaktadır. Bu bağlamda koruma tedbiri terimi; *şüpheli veya sanığı ya da bir delili elde* *etmek, duruşmanın yapılmasını yahut hükmün infazın teminat altına almak amacıyla başvurulan, her* *birisi bir veya birden fazla temel hakka müdahale teşkil* *eden muhakeme işlemleri*ni ifade etmektedir. Bilişim sistemlerinin ve dolayısıyla bilgisayarların sosyal ve ticari alanda giderek yaygınlaşması ve bireysel yaşamda da giderek daha fazla önem arz etmesine bağlı olarak kanun koyucu bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve el koyma faaliyetlerini ayrıca düzenleme ihtiyacı hissetmiştir. Bu bağlamda söz konusu tedbir, CMK’nın birinci kitap, dördüncü kısım, dördüncü bölümünde, “arama ve elkoyma” başlığı altında, m.134’te hükme bağlanmıştır. Tedbir sadece soruşturma sırasında başvurulabilen bir tedbirdir. Kanun koyucunun bu tedbirin uygulanmasına kovuşturma bakımından da cevaz verdiğine ilişkin bir düzenleme kanunda bulunmamaktadır. Temel haklara sınırlama getiren bir muhakeme işlemini düzenliyor olması nedeniyle, CMK m.134’teki hükmü kıyasen kovuşturmaya da uygulamak mümkün değildir

**Tedbire Başvurmanın Koşulları** İki koşulu vardır ilk olarak *somut delillere dayanan**kuvvetli şüphe sebeplerinin varlığı* aranmıştır**.** Kuvvetli şüphe soruşturma konusu suçun muhtemelen şüpheli tarafından işlendiğini gösterir delillerin bulunması halinde söz konusu olabilir. Bu bağlamda ceza muhakemesinde şüphenin derecesini elde olan deliller belirler. Elde basit delil varsa basit şüphe, yeterli delil varsa yeterli şüphe, kuvvetli delil varsa da kuvvetli şüphe söz konusudur. Söz konusu tedbire başvurulabilmesi bakımından CMK’da öngörülen en yüksek şüphe derecesinin varlığı aranmıştır. Tedbire başvurulabilmesini için kuvvetli şüphenin yanında, ikinci olarak, *başka surette delil elde* *etme imkânının bulunmaması* koşulu aranmıştır (CMK m.134/1). Eğer hukuka uygun başka bir yöntemle delil elde edilebilecekse, kanun koyucu bu tedbirin uygulanmasını yerinde görmemiştir.

**Tedbire Karar Vermeye Yetkili Merciler** Tedbire Cumhuriyet savcısının istemi üzerinesulh ceza hakimi tarafından karar verilir. Kovuşturmasırasında tedbire başvurma imkânı bulunmadığıiçin mahkemenin bu yönde bir karar alma yetkisibulunmamaktadır. Ayrıca soruşturma sırasında görevliyargılama makamı olan sulh ceza hakimindenbaşka bir adli merciin de herhangi bir koşula bağlıolarak bu tedbire karar vermesi söz konusu değildir.Temel hakları kısıtlayıcı nitelikte bir işlem olması sebebiyle, tedbirin uygulanma alanının kovuşturmayı da kapsar şekilde kıyasen genişletilmesi de mümkün değildir (Bkz. Any. m.13). Kovuşturma sırasında söz konusu tedbire başvurulması ihtiyacı hasıl olduğundaaramaya ilişkin genel kurallara göre bilgisayarlarda,programlarında ve kütüklerinde arama yapılabileceğişeklindeki bir yorum tarzı ise yerinde değildir.Nitekim kanun koyucu bilgisayarlarda, program vekütüklerinde genel kurallara göre arama yapılmasınıyerinde görseydi, ayrıca böyle bir tedbire de ihtiyaçduymazdı. Soruşturma bakımından da ayrı düzenlemeyapmaksızın, genel kurallara göre arama yapılmasınaimkân tanırdı. Eğer tedbirin uygulama alanınınkovuşturmayı da kapsar şekilde genişletilmesiisteniyorsa, bunun ayrıca düzenleme altına alınmasızorunluluktur kanaatindeyiz.

**Tedbirin Uygulanma Usulü** *Cumhuriyet savcısının istemi üzerine şüphelinin**kullandığı bilgisayar ve bilgisayar programları ile bilgisayar**kütüklerinde arama yapılmasına, bilgisayar**kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek**metin haline getirilmesine hakim tarafından**karar verilir (CMK m.134/1)*. Ancak bazen şifrelemenedeniyle söz konusu işlemlerin gerçekleştirilmesimümkün olmayabilir. Kanun koyucu bu ihtimale binaen ilgili araç ve gereçler üzerinde elkoymaişleminin yapılmasına cevaz vermiştir. Buna göre;*“bilgisayar, bilgisayar programları ve bilgisayar kütüklerine**şifrenin çözülememesinden dolayı girilememesi**veya gizlenmiş bilgilere ulaşılamaması halinde**çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi**için, bu araç ve gereçlere el konulabilir. Şifrenin**çözümünün yapılması ve gerekli kopyaların alınması**halinde, el konulan cihazlar gecikme olmaksızın**iade edilir (CMK m.134/2).”* Bilgisayarların ticarive gündelik yaşamda giderek daha fazla yer almalarıve önem arz etmeleri dolayısıyla, kanun koyucuöncelikle bunlar üzerinde el koyma işlemi yapılmaksızın,gerekli arama, kopya çıkarma ve metinhaline getirme işlemlerinin yapılmasını öngörmüştür.  *“Bilgisayar veya bilgisayar kütüklerine elkoyma* *işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır (CMK m.134/3). Alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. (CMK m.134/4).”* Nitekim kendisinden alınıp el konulan donanımdaki veriler üzerinde sonradan değişiklik yapılması ihtimaline binaen, bir kopyanın şüpheliye verilmesi onun bakımından önemli bir güvence oluşturmaktadır. “*Bilgisayar veya bilgisayar kütüklerine el koymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır (CMK m.134/5).*”