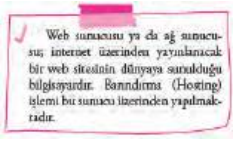
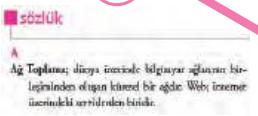
Öğrenme çıktıları
Bölüm içinde hangi bilgi,beceri ve yeterlikleri kazanacağınızı ifade eder.

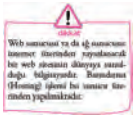
Bölüm Özeti
Bölümün kısa özetini gösterir.



Tanım
Bölüm içinde geçen önemlikavramların tanımları verilir.

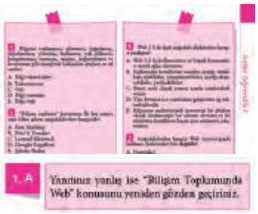


Sözlük
Bölüm içinde geçen önemli kavramlardan oluşan sözlük ünite sonunda paylaşılır.



Dikkat
Konuya ilişkin önemli uyarıları gösterir.

Karekod
Bölüm içinde verilen karekodlar, mobil cihazlarınız aracılığıyla sizi ek kaynaklara, videolara veya web adreslerine ulaştırır.



Neler Öğrendik ve Yanıt Anahtarı
Bölüm içeriğine ilişkin 10 adet çoktan seçmeli soru ve cevapları paylaşılır.

Öğrenme Çıktısı Tablosu

Araştır/İlişkilendir/Anlat-Paylaş
İlgili konuların altında cevaplayacağınız soruları, okuyabileceğiniz ek kaynakları ve konuyla ilgili yapabileceğiniz ekstra etkinlikleri gösterir.

Yaşamla İlişkilendir
Bölümün içeriğine uygun paylaşılan yaşama dair gerçek kesitler veya örnekleri gösterir.

Araştırmalarla İlişkilendir
Bölüm içeriği ile ilişkili araştırmaların ve bilimsel çalışmaları gösterir.

ANADOLU ÜNİVERSİTESİ

Bilişim Hukuku

Editör

Doç.Dr. Gökhan GÜNEYSU

Yazarlar

BÖLÜM 1, 8 Dr.Öğr.Üyesi Reşit KARAASLAN

BÖLÜM 2, 3 Dr.Öğr.Üyesi Elif KÜZECİ

BÖLÜM 4, 5 Doç.Dr. Hakan KARAKEHYA

BÖLÜM 6, 7 Prof.Dr. Tekin MEMİŞ

T.C. ANADOLU ÜNİVERSİTESİ YAYINI NO: 3655
AÇIKÖĞRETİM FAKÜLTESİ YAYINI NO: 2483

Öğretim Tasarımcısı
Dr.Öğr.Üyesi Halil Cem Sayın

Grafik Tasarım ve Kapak Düzeni
Prof.Dr. Halit Turgay Ünalan

Ölçme Değerlendirme Sorumlusu
Ümit Baş

Grafiker
Ayşegül Dibek

Dizgi ve Yayıma Hazırlama
Kader Abpak Arul
Kağan Küçük
Saner Coşkun
Gizem Dalmış
Dilek Özbek
Dilek Kaleci
Diğdem Aydın
Nihal Sürücü

BİLİŞİM HUKUKU

E-ISBN
978-975-06-3384-3

ESKİŞEHİR, Şubat 2019
3109-0-0-0-2002-V01

İçindekiler

BÖLÜM 1 Bilişim, İnternet ve Hukuk

BÖLÜM 2 Bilişim, İnsan Hakları ve Kişisel Verilerin Korunması

BÖLÜM 3 Türkiye'de Kişisel Verilerin Korunması

BÖLÜM 4

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

BÖLÜM 5

5651 Sayılı Kanun Bağlamında İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi

BÖLÜM 6 E-Ticaret

BÖLÜM 7 Bilişim Ortamında Fikrî ve Sınai Haklar

BÖLÜM 8 Bilişim Hukuku Alanındaki Son Gelişmeler

Önsöz

Sevgili öğrenciler,

Elinizdeki kitap güncel bir konuda, alanının uzmanı hukuk akademisyen ve uygulayıcıları tarafından büyük bir özveri ile kısa zamanda hazırlanmış çok değerli bir çalışmadır. Bilişim Hukuku, değişen toplumsal ihtiyaçlara hukukun verdiği tepkinin en iyi şekilde ölçülebildiği, yeni hukuk dallarından bir tanesidir. Bundan kısa bir zaman öncesine kadar internet, unutulma hakkı gibi kavramlar hayatımızda mevcut bile değilken, günümüzde artan ihtiyaç nedeniyle bu konularda ulusal ve uluslararası düzenlemeler yoluna gidilmektedir. Bundan kısa bir zaman öncesine kadar mevcut olmayan bu kavramların hukuki düzenlemeye kavuşturulmaları bu anlamda önemli birer gelişme ve hatta ihtiyaçtır. Bu eserde Bilişim Hukuku ile ilişkili farklı konular ele alınmıştır. Konunun Ticaret Hukuku, İnsan Hakları ve Ceza Hukuku ile çok yakından ilgisi vardır ve zikredilen alanları kapsayıcı bir çalışma hazırlanmaya çalışılmıştır.

Bu kadar güncel, bu kadar yeni bir alanda mevcut olan uzmanlıklarını öğrencilerimiz ile paylaşan kıymetli yazarlara teşekkürlerimizi sunarız. Ciddi bir akademik kalite ile hazırlanmış eserin, alanında öncü eserlerden biri haline geleceği kanaatimizce gerçekçi bir beklentidir. Eserin öğrencilerimiz kadar, alanda çalışan akademisyen ve uygulayıcılar için faydalı olmasını dileriz.

Editör

Doç.Dr. Gökhan GÜNEYSU

Bölüm 1

Bilişim, İnternet ve Hukuk

Öğrenme çıktıları

Bilişim Hukuku

1 Bilişim hukukunu tanımlayabilme
2 Bilişim hukuk dalının yapısını ve ortaya çıkış nedenlerini açıklayabilme

Bilişim Hukuku Mevzuatına Genel Bakış

3 Bilişim hukuku mevzuatında yer alan temel kavramları açıklayabilme

Bilişim, Bilişim Sistemleri ve İnternet

4 Bilişim, bilgisayar ve internete dair bazı önemli teknik kavramları tanımlayabilme

Türkiye'de İnternetin Yönetiminde Yer Alan Yetkili ve Sorumlu Kurumlar

5 İnternetin yönetiminde yer alan yetkili ve sorumlu kurumların yetki ve görevlerini açıklayabilme

İnternet Süjelerinin Sorumluluğu

6 İnternet süjelerini tanımlayabilme
7 İnternet süjelerinin sorumluluklarını açıklayabilme

Anahtar Sözcükler: • Bilişim Hukuku • İnternet • Ulaştırma ve Altyapı Bakanlığı • İnternet Geliştirme Kurulu • Bilgi Teknolojileri ve İletişim Kurumu • İçerik Sağlayıcı (Content Provider) • Yer Sağlayıcı (Host Provider) • Erişim Sağlayıcı (Access Provider)

GİRİŞ

Bilişim hukuku, elektronik ortamlarda, iletişim, bilgi ve belge paylaşımının sağlanmasının hukuki çerçevesi ve sonuçları ile bu ortamlarda vukuu bulan hukuka aykırı fiillere ilişin yaptırımların öngörüldüğü mevzuatın (uluslararası antlaşmalar, kanun, yönetmelik vs.) oluşturduğu hukuk normlarının tamamına verilen bir isimdir. Bu anlamda, internet ve elektronik ortam ile bilgi ve iletişim teknolojilerine ilişkin mevzuat, bu hukuk alanının ana eksenini oluşturmaktadır (Turan, 2016: 35).

BİLİŞİM HUKUKU

Özellikle son çeyrek asırda tüm dünyayı etkileyen ve baş döndürücü bir hızla ilerleyen teknolojik gelişmeler, bilişim hukukunun ortaya çıkış sürecinin nedeni olarak kabul edilmektedir; zira teknoloji alanındaki gelişmeler tarafların yüz yüze yaptıkları hukuksal işlemleri konu alan klasik yasal düzenlemelerin gözden geçirilmesini gerekli kılmıştır. Bu nedenle bilişim hukukunu, bilişim teknolojilerindeki gelişmeler ve yenilikler sebebiyle mevcut yasal düzenlemelerin yetersiz kalması ile ortaya çıkmış bir hukuk dalı olarak tanımlamak yanlış olmayacaktır. Gerçekten de eskiden yalnızca insanlara özgü olarak kabul edilen birçok eylem ve işlem, bugün bilişim sistemleri tarafından yapılmakta veyahut bu sistemler aracılığıyla insanlar tarafından çok hızlı bir şekilde tamamlanmaktadır. İnsanların günlük hayatında önemli bir yer tutan bilişim sistemleri aracılığıyla gerçekleştirilen işlemler neticesinde ise, zamanla hukuksal sorunlar baş göstermiştir. Özelikle e-ticaretin gelişmesi, devletin vatandaşlarıyla olan ilişkilerinde e-devlet gibi bilişim sistemlerini kullanması ve bu sayede her kurum ve bireyin bilgi teknolojilerini kullanan sistemler ile kamu hizmetlerine ulaşabilmesi ya da bilişim sistemleri aracığıyla işlenen suçlardaki artışlar klasik hukuk normlarının gözden geçirilmesini zorunlu kılmıştır. Bunun sonucunda da devletler, bireylerle bireyler ve bireylerle devlet arasındaki hukuk kurallarını bilişim sistemleri çerçevesinde yeniden ele almış ve bu sürecin sonunda da bilişim hukuku denilen yeni bir hukuk dalı ortaya çıkmıştır (Dülger, 2015: 53).

Bilişim hukukunun yeni bir hukuk dalı olması, bilişim hukukunu esas olarak ulusal alanda yapılan düzenlemelerin konusu olmaktan çıkarmamaktadır. Zira bilişim hukukunu oluşturan normlar da tıpkı diğer hukuk dallarının konusu oluşturan normlar gibi, devletlerin egemenlik yetkileri ile yakından ilintilidir. Bu nedenle bilişim hukukunun ilk ortaya çıkış sürecinde savunulan ve bu hukuk dalının devletler tarafından değil de kullanıcılar ve sistem operatörleri tarafından kendiliğinden ortaya konan ve "netiket" olarak isimlendirilen bir kısım kuralların toplanarak, merkezileştirilmeden; "öz düzenleme" (self regulation) ve "iş birliğine dayalı düzenleme" (co-regulation) yöntemleriyle düzenlenmesine ilişkin düşünceler, bugün için kabul edilmemektedir (Dülger, 2015: 914). Diğer taraftan ise, 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. Zira bilişim sistemlerine hukuk düzenlemelerinde yer verilmesi ülkelerin gelişmişlik düzeyleri, ulusal ekonomileri, bilim ve teknolojiyi hayata geçirme istemleri ile yakından ilgilidir (Dülger, 2015: 55). İşte bu nedenle aralarında Türkiye'nin de bulunduğu birçok gelişmiş ülke bilişim sistemlerinin yaygınlaştırılmasını ve vatandaş ve işletmeler tarafından kullanılmasını ulusal düzeyde stratejik bir hedef olarak görmüş ve bu hedefin gerçekleştirilmesi için de farklı teknolojiler, lisanslama yöntemleri ve kamu-özel kesim ortaklıklarının kullanılmasına yönelik teşvikler öngörmüş, değişik stratejiler geliştirmiştir. Bütün bunların altında yatan neden, 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 gelişmiş toplumu, yani "bilgi toplumunun" oluşturulması ve geliştirilmesi yönünde devletlere yüklenen pozitif ödevdir (Avşar ve Öngören, 2010: 44).

Bilgi Teknolojileri ve İletişim Kurumu tarafından 2016-2018 yıllarına dair hazırlanan stratejik Plan'a https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fStratejik_Plan%2fStr_Pln_2016-2018.pdf adresinden ulaşılabilmektedir.

Bilişim Hukukunun Yapısı

Bilişim hukuku bünyesinde birçok farklı hukuk dalını barındırması ve/veya birçok hukuk dalıyla iç içe geçmesi nedeniyle, multi-disipliner bir hukuk dalı olarak tanımlanmaktadır. Bu hususu bir örnekle açıklamak gerekirse; bir internet alışveriş sitesinde satıcı, korsan bir yazılım CD'sini gerçeğe aykırı beyanlarla, tüketiciye orijinal ürün olarak pazarlamış, tüketici de parayı satıcının belirttiği banka hesabına havale etmiştir. Satıcı ise parayı aldıktan sonra tüketiciye hiçbir ürün göndermemiştir. İşte günlük hayatta çok sık karşılan bu örnekte, internet üzerinde yapılan bu sözleşmenin hangi şartlar altında hukuken taraflar açısından bağlayıcı olduğu, diğer bir ifadeyle internet ortamında hangi şartlar altında sözleşmenin kurulduğu borçlar hukuku ve tüketici hukukunun konusuyken, yazılımların korunması, kullanılması fikri mülkiyet hukukunun konusunu teşkil etmektedir. Tarafların mahkemede birbirleri aleyhine sundukları delillerin değerlendirilmesi ise medeni usul hukukunu ilgilendirmektedir. Yine satıcının internet aracılığıyla hileli davranışlar sonucu tüketiciyi dolandırması ceza hukukunun ilgi alanında bulunurken, satıcı hakkındaki soruşturma ve kovuşturma işlemleri ceza usul hukuku normlarıyla ile düzenlenmektedir.

Bilişim hukukunun çok yönlü ilgi alanı sadece bunlarla da sınırlı değildir. 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 (Dülger, 2015: 183). Bu tip örnekler kişilik hakları, özel hayatın gizliliği, kişisel verilerin korunması, rekabet hukuku, adli yardımlaşma hukuku gibi alanlarından verilebilecek başka örneklerle de istenildiği gibi çoğaltılabilir.

Öğrenme Çıktısı

1 Bilişim hukukunu tanımlayabilme
2 Bilişim hukuk dalının yapısını ve ortaya çıkış nedenlerini açıklayabilme

Araştır 1	İlişkilendir	Anlat/Paylaş
Bilişim hukukunu tanımlayanız ve ortaya çıkış nedenini açıklayınız.	Bilişim sistemlerinin bilgi toplumundaki rolünü değerlendiriniz.	E-ticaretin hayatınızı nasıl etkilediğini açıklayınız.

BİLİŞİM HUKUKU MEVZUATINA GENEL BAKIŞ

Bilişim hukukunun irtibatlı olduğu hukuk dallarının çok olması nedeniyle, bilişim hukukunu düzenleyen tek bir kanun ve buna bağlı tali mevzuat bulunmamaktadır. Bilişim hukukunu oluşturan mevzuat, birçok kanunun içine serpiştirilmiş ve bu nedenle 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.

dikkat

Ülkemizde birçok kanun bilişim hukukuna ilişkin normlar içermektedir.

Bünyesinde bilişim hukukunu ilgilendiren normlar bulunduran mevzuatın genel özelliği, bunların esas olarak başka hukuk dallarını düzenlemeleri, ancak yine de bünyelerinde bilişim hukukunun ilgi alanına giren normlara yer vermeleridir. İlerleyen bölümlerde gerekli oldukça söz konusu mevzuatla ilgili olarak daha detaylı bilgiler verileceğinden, bu noktada bunlardan bazılarının isimlerini zikretmek yeterli olacaktır: 6533 sayılı Avrupa Siber Suç Sözleşmesini iç hukukumuza aktaran Sanal Ortamda İşlenen Suçlar Sözleşmesinin Uygun Bulunduğuna Dair Kanun; 5237 sayılı Türk Ceza Kanunu; 5271 sayılı Ceza Muhakemesi Kanunu; 2803 sayılı Jandarma Teşkilat ve Yetkileri Kanunu; 2559 sayılı Polis Vazife ve Salahiyet Kanunu; 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu; 4721 sayılı Türk Medeni Kanunu; 6098 sayılı Türk Borçlar Kanunu; 6502 sayılı Tüketicinin Korunması Hakkında Kanun; 6698 sayılı Kişisel Verilerin Korunması Kanunu; 4982 sayılı Bilgi Edinme Hakkı Kanunu; 6102 sayılı Türk Ticaret Kanunu; 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun; 5070 sayılı Elektronik İmza Kanunu; 5846 sayılı Fikir ve Sanat Eserleri Kanunu; 6279 sayılı Çoğaltılmış Fikir ve Sanat Eserlerini Derleme Kanunu; 5411 sayılı Bankacılık Kanunu; 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu; 6362 sayılı Sermaye Piyasası Kanunu; 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun; 213 sayılı Vergi Usul Kanunu; 488 sayılı Damga Vergisi Kanunu; 5147 sayılı Entegre Devre Topoğraflarının Korunması Hakkında Kanun; 4734 sayılı Kamu İhale Kanunu; 5018 sayılı Kamu Mali Yönetimi Kontrol Kanunu; 5300 sayılı Tarım Ürünleri Lisanslı Depoculuk Kanunu; 6100 sayılı Hukuk Muhakemeleri Kanunu; 2004 sayılı İcra ve İflas Kanunu; 6112 sayılı Radyo ve Televizyon Kuruluş ve Yayın Hizmetleri Hakkında Kanun; 7201 sayılı Tebligat Kanunu; 406 sayılı Telgraf ve Telefon Kanunu; 4691 sayılı Teknoloji Geliştirme Bölgeleri Kanunu.

Bünyesinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulunduran mevzuatın genel özelliği ise, bunların bünyelerinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulundurmalarıdır. İlerleyen bölümlerde belirtilecek hususların daha iyi anlaşılması için bu başlık altında yer alan mevzuata yakından bakmak gerekmektedir.

5651 sayılı 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 yükümlülük ve 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. Buna göre;

a. Bakanlık: Ulaştırma ve Altyapı Bakanlığını,
b. Başkan: Bilgi Teknolojileri ve İletişim Kurumu Başkanını,
c. Bilgi: Verilerin anlam kazanmış biçimini,
ç. Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,
d. Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

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

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

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

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

h. Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

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

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

j. Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

k. Yayın: İnternet ortamında yapılan yayını,

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

m. Birlik: Erişim Sağlayıcıları Birliğini,

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

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

ö. URL adresi: İlgili içeriğin internette bulunduğu tam internet adresini,

p. 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. Bu bilgilerin neler olduğu İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in 5. maddesinde ifade edilmiştir. Buna göre 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, tüzel kişi 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 (md. 4).

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.

dikkat

İnternet kafeleri gibi ticari amaçla toplu kullanım sağlayıcıları internet süjesi sayılmamaktadır.

Kanun 8 ve devamı maddelerinde ise erişimin engellenmesini düzenlemektedir. Kanun 4 farklı kapsamda erişimin engellenmesini düzenlemektedir. Birincisi koruma tedbiri olarak öngörülen erişimin engellenmesi, ikincisi önleme amaçlı olarak erişimin engellenmesi; üçüncüsü kişilik haklarının internet yoluyla ihlaline bağlı olarak ilgililerin başvurusu üzerine erişimin engellenmesi ve dördüncüsü de 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 [bunlar 5237 sayılı Türk Ceza Kanununda düzenlenmiş olan intihara yönlendirme (madde 84), çocukların cinsel istismarı (madde 103/1), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190), sağlık için tehlikeli madde temini (madde 194), müstehcenlik (madde 226), fuhuş (madde 227), kumar oynanması için yer ve imkân sağlama (madde 228) suçları ve 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlardır] oluşturduğu yönünde yeterli şüphe bulunan bir internet sitesine erişim, hakim veya mahkeme tarafından engellenebilir. 5651 sayılı Kanunun 8. maddesinin 4. fıkrasında erişimin engellenmesi kararı için aranan şartların var olduğu takdirde, idari bir makam tarafından da yerine getirilebileceği hüküm altına alınmıştır. Şöyle ki; internet 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, Cumhurbaşkanlığı 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. Cumhurbaşkanlığı 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 kişiler ile 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 engellenmesini 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 hakim 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. Alınacak ücretler, 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. Erişimin engellenmesi 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. Bunların neler olduğu ilerleyen bölümlerde belirtilecektir. Bu noktada belirtilmelidir ki, 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.

dikkat

Telekomünikasyon İletişim Başkanlığı (TİB) 2016 yılında kapatılmıştır.

5369 Sayılı Evrensel Hizmet Kanunu

Kanun'un 1. maddesine göre, bu yasanın amacı; 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.

Kanun'un 2. maddesinde tanımlar başlığı altında yasada yer alan bazı kavramların tanımlarına yer verilmiştir. Buna göre;

a. Bakanlık: Ulaştırma ve Altyapı Bakanlığını,

b. Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

c. 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,

ç. 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,

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

e. 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,

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

g. Alt yapı: Evrensel hizmetin sağlanmasını teminen 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. Buna göre;

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 yatırımların teşvik 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. Buna göre;

a. 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,

b. Elektronik haberleşme alt yapısı: Elektronik haberleşmenin, üzerinden veya aracılığıyla

gerçekleştirildiği anahtarlama ekipmanları, donanım ve yazılımlar, terminaller ve hatlar da dahil olmak üzere her türlü şebeke birimlerini, ilgili tesisleri ve bunların bütünleyici parçalarını,

c. 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,

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

d. 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,

e. 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,

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

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

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

ı. Erişim yükümlüsü: Erişim sağlama yükümlülüğü getirilen işletmeciyi,

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

k. İnternet alan adı sistemi: Okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simgesel 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 gereklerine ve 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 ve Altyapı Bakanlığı'na ve Bilgi Teknolojileri ve İletişim Kurumu'na çeşitli görevler ve yetkiler vermekte; sonraki maddelerde ise bu görev ve yetkileri somutlaştırmaktadır. Bunların ne olduğu ilerleyen bölümlerde belirtilecektir.

Öğrenme Çıktısı

3 Bilişim hukuku mevzuatında yer alan temel kavramları açıklayabilme

Araştır 2

Bünyesinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulunduran mevzuatın genel özelliğini açıklayınız ve bu mevzuat kapsamında değerlendirilen kanunları belirtiniz.

İlişkilendir

Bilişim hukukuna ilişkin normların tek bir kanunda düzenlenmemiş olmasının olumlu ve olumsuz yönlerini belirtiniz.

Anlat/Paylaş

Elektronik haberleşme kavramı ile evrensel hizmet kavramı arasındaki benzerlikleri ve farklılıkları değerlendiriniz.

BİLİŞİM, BİLİŞİM SİSTEMLERİ VE İNTERNET

Bilişim hukukuna ve buna ilişkin mevzuata dair açıklamalar yapıldıktan sonra kavram olarak bilişimin ve internetin ne olduğu ortaya konulmalıdır. Konu böylelikle daha kapsamlı bir şekilde incelemeye tabi tutulmuş olacak, düzenlemenin konusu olan ve bu nedenle hukuki çerçeveden etkilenecek gerçek ilişkiler daha iyi betimlenecektir.

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 (Avşar ve Öngören, 2010: 41).

Bilgisayar ve bilişim sözcükleri zaman zaman birbirleri yerine kullanılagelmişlerdir. 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 (Dülger, 2015: 62). 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 (CD, USB, taşınabilir bellek) 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 (Dülger, 2015: 84). İşte 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 (Avşar ve Öngören, 2010: 42). Bu noktadan hareketle bilgisayar sistemlerinden değil bilişim alanı ve/veya bilişim sisteminden söz edilmektedir (Avşar ve Öngören, 2010: 45). Dolayısıyla her bilgisayarın bir bilişim sistemi olduğu ancak herhangi bir bilişim sisteminin zorunlu olarak bir bilgisayar olmadığı kabul edilmelidir. Buna örnek olarak, bilgisayarın bazı işlevlerini yerine getiren ancak yukarıda açıklaması yapılan bilgisayar tanımına uymayan cep telefonları, kişi ya da araçları otomatik olarak tanıyan güvenlik araçları, ev aletlerinin işlemcileri ya da araç bilgisayarları veyahut POS cihazları, ATM'ler verilebilir (Dülger, 2015: 75).

dikkat

Teknik olarak her bilgisayar bir bilişim sistemi olmakla birlikte, her bilişim sistemi bilgisayar olarak kabul edilmemektedir.

İnternet

Hiç şüphesiz son on yıllardaki teknolojik gelişmeleri tetikleyen en önemli olay, dünya çapındaki küçüklü büyüklü bilişim sistemlerinin kurulması ve varlığı değil, bütün bilişim ağlarını kapsayan genel bir ağ olan internetin tesis edilmesi olmuştur (Avşar ve Öngören, 2010: 29). Zira internet veri iletim ağlarının yalnızca bir türü, dolayısıyla da bilişim sistemleri ve bunları birbirine bağlayan her türlü veri iletim ağının genel adı olan sanal dünyanın yalnızca bir parçasıdır; ancak bugün için en yaygın ve en geniş parçasıdır (Dülger, 2015: 86). Bu nedenle internetin ne olduğu, bunun teknik alt yapısının nelerden oluştuğu, tarihçesi ve interneti organize eden kurumların neler olduğu hususundaki açıklamalara burada yer vermek gerekmektedir.

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 vb. 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. Bu ağların her geçen gün büyümesi ve yeni ağların bu sistemin içine katılması nedeniyle internete merkezi olmayan, küresel seviyede planlanmış, hiyerarşik bir yapısı bulunmayan "ağlar arası ağ" da denilmektedir (Avşar ve Öngören, 2010: 29 vd.; Dülger, 2015: 86).

İnternetin Teknik Alt Yapısı

İnternetin yapısının anlaşılması için bazı teknik terimlere kısaca değinmek gerekmektedir:

Backbone: İnternet üzerindeki veri iletişimi omurga (backbone) 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 AR-

PANET tarafından kurulmuştur. İnternetin ortaya çıkışının ilk yıllarında bu omurgalar kamusal kuruluşlar tarafından yapılmaktaysa da, bu yapıların kurulması bugün için özel sektör tarafından sağlanmaktadır. Bugün dünyada birkaç büyük omurga mevcuttur ve bunlar da birbirleriyle bağlantılıdır (Dülger, 2015: 88).

TCP/IP Protokolü: İnternet içindeki bilişim sistemlerinin birbirleriyle iletişim kurabilmeleri ve veri aktarımında bulunabilmeleri için birtakım kurallara uygun hareket etmeleri gerekmektedir. Bu kurallar, iletişimdeki eşler arasında veri trafiğinin kurallarını oluşturup daha etkin bir iletişim sağlanmasını gerçekleştirirler. Bu kurallara, internet protokolleri ya da TCP/IP (Transmission Control Protocol/Internet Protocol) protokoller ailesi denir. Bu protokoller adeta birbirleriyle iletişim kuran milyonlarca bilgisayardan oluşan bir ağda yer alan farklı yapıdaki bilgisayarların birbirleriyle iletişim kurabilmeleri için oluşturulan bir anlaşma dilidir. TCP/IP protokolünü oluşturan TCP verilerin doğru yere ulaştırılmasından; IP ise adresleme sisteminden sorumludur (Avşar ve Öngören, 2010: 32; Dülger, 2015: 88). Bu noktada IP adresinin ne olduğu biraz daha açıklanmalıdır. IP adresi, internetin teknik alt yapısını kuran internet servis sağlayıcıları tarafından internet kullanıcılarına verilen kimlik numarasıdır. Bunlar 0 ile 255 sayıları arasında değişen, genellikle noktalı onluk (desimal) 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 (Dülger, 2015: 802). Bu nedenle genellikle bir web sayfasının statik IP'si bulunurken, bu sayfayı ziyaret eden son kullanıcının internete bağlanırken kullandığı IP dinamiktir. Bu noktada yeri gelmişken belirtilmesi gereken bir husus da şudur: İnternette vukuu bulan hukuka aykırılıkların sorumlularının bulunmasında kullanılan en sık yöntem IP numarasının tespitidir. Burada kast edilen IP numarası dinamik IP numarasıdır.

TCP/IP protokolünün dışında bazı anlaşma dilleri oluşturulmuşsa da genel olarak kabul görmediğinden şu an için internet ağında en çok kullanılan anlaşma dili TCP/IP protokolüdür. İnternet hizmetlerini kullanabilmek için gerekli olan tüm yazılımlar ve bağlantı yazılımları, TCP/IP protokolüne uygun olarak iletişim kurarlar ve işlev görürler. Bu protokollere örnek olarak, internet üzerindeki bilgisayarlar arasında dosya alma/gönderme protokolü (FTP/File Transfer Protocol), elektronik posta iletişim protokolü (SMTP/Simple Mail Transfer Protocol), TELNET protokolü (internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen login protokolü) veyahut internette birbirine bağlanmış farklı türden objelerin karşı tarafa iletilmesini sağlayan Hyper Text Transfer Protocol (HTTP) verilebilir (Avşar ve Öngören, 2010: 32).

DNS (Domain Name System/alan adı sistemi) de bir TCP/IP servis protokolüdür. Bütün web siteleri bir IP adresi üzerinden yayın yapar. DNS bu alan adı adreslerini kişilerin anlayabileceği hale getirir. Örneğin 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. Böylesine uzun ve karmaşık sayıları kullanıcıların her internete girişlerinde aradıkları sayfaları bulmak için akılda tutmaları mümkün olmadığından, DNS'in ana amacı şu şekilde açıklanabilir: Bir siteye erişmek istendiğinde, hangi site nerede ve hangi IP adresli bilgisayarda olduğu belirlenir ve kullanıcının istediği yere erişmesi sağlanır. DNS sistemi isim sunucuları ve çözümleyicilerinden oluşur. İsim sunucuları olarak düzenlenen bilgisayarlar host isimlerine karşılık gelen IP adresi bilgilerini tutarlar. Çözümleyiciler ise DNS istemcileridir. DNS istemcileri de DNS sunucu ya da sunucuların adresleri bulunur. Bir DNS istemci bir bilgisayarın ismine karşılık IP adresini bulmak istediği zaman isim sunucuya başvurur. İsim sunucu yani DNS sunucuda eğer kendi veri tabanında öyle bir isim varsa bu isme karşılık gelen IP adresini istemciye gönderir. Bu sayede internet kullanıcılarının örneğin 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 yazar ve DNS sunucusu, onu bu IP adresine yönlendirir.

İnternetin teknik alt yapısını oluşturmamakla birlikte, DNS kavramı ile yakından ilintili olan "alan adı" (domain name) kavramını da kısaca açıklamak gerekir. 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 domain). 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 (Avşar ve Öngören, 2010: 34 vd., 267).

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" ya da 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. Web kullanılan platformdan bağımsızdır. Bir Macintosh (Mac), PC ya da Unix Web web sayfalarını aynı şekilde alırlar. Sayfaların alındığı web servisleri de farklı bilgisayar platformlarında olabilir. 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 (Hypertext Markup Language) adı verilen işaretleme dili kullanılarak oluşturulan uygulama yazılımlarının bir araya gelmesinden oluşmaktadır (Avşar ve Öngören, 2010: 33).

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. Zaman içerisinde sistem içinde bulunan farklı özellikteki bilgisayarların birbirini tanımasına yarayan ve aralarındaki uyuşmazlıkları çözmeye yarayan, günümüzde de yerel ağların birbiriyle iletişim

kurmasına yarayan kurallar bütünü olan TCP/IP protokolleri gibi kurallar geliştirilmiştir. 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 (Dülger, 2015: 109).

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 bulunmamaktadır. 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, internet protokolü adresi alanı (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 çözülebilirlikten emin olunması için DNS'in teknik unsurlarının yönetiminin koordinasyonundan da sorumludur. Bunu internetteki işlemlerde kullanılan 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 yetkilendirilmiştir. 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 kuruluşların hiçbirisi ticari amaç gütmez ve hükümetlerin organı değildir. Bugün dünya üzerinde beş adet RIR bölgesi bulunmaktadır. Bunlar Afrika bölgesi için AfriNIC (African Region Internet Registry), Asya ve Pasifik bölgesi için APNIC (Asia Pacific Network Information Centre), Kuzey Amerika için ARIN (American Registry for Internet Numbers), Latin Amerika ve Karayipler bölgesi için LACNIC (Latin America and Caraibbean Adresses Registry) ve Avrupa Bölgesi için RIPE NCC (Réseaux IP Europens Network Coordination 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 toplantılarına katılabilir, politikaları için önerilerde bulunabilir. Genel olarak internetin teknik alt yapısını ve internet servis sağlayıcısı olarak adlandırılan her gerçek veya tüzel kişi LIR'dir. Türkiye'de de örneğin 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 (Dülger, 2015: 909).

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 vazgeçmek 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 iki milyon, günde ise üç milyar telefon görüşmesini denetleyebildiği belirtilmektedir. Veriler, düzenli olarak toplanmakta ve "dictionary" (sözlük) adı verilen şifreleme sisteminden geçirilerek; uzmanlar tarafından anahtar sözcükler yardımıyla izlenmektedir (Dülger, 2015: 837). 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 (Dülger, 2015: 911). 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.

Öğrenme Çıktısı

4 Bilişim, bilgisayar ve internete dair bazı önemli teknik kavramları tanımlayabilme

Araştır 3	İlişkilendir	Anlat/Paylaş
İnterneti tanımlayınız ve internetin teknik alt yapısını oluşturan sistemleri ismen belirtiniz.	Bilişim ve bilgisayar kavramları arasındaki farklılıklara bilişim sistemlerinin kullanımında ne ölçüde dikkat edildiğini değerlendiriniz.	İnternetin ilk ortaya çıktığı zamandaki kullanımı ile bugün evrensel hizmet kabul edilen internetin (5369 s. Kanun) günlük yaşamdaki kullanımı arasındaki farklılıkları ve/veya benzerlikleri belirtiniz.

TÜRKİYE'DE İNTERNETİN YÖNETİMİNDE YER ALAN YETKİLİ VE SORUMLU KURUMLAR

Ülkemizde de internetin teknik alt yapısı konusunda yetkili ve sorumlu olan kurumlar bulunmaktadır. Burada bu kurumlar sayılacak, yetki ve sorumlulukları hakkında güncel bilgi verilecektir. Konu özellikle kurumların yetkisini detaylıca incelemek isteyenler için dikkat çekici ve aynı zamanda çok önemli bir konudur. Yakın zamanda bu yetki ve sorumluluklar hakkındaki mevzuatta önemli değişikler başarıyla gerçekleştirilmiştir.

Ulaştırma ve Altyapı Bakanlığı

Ülkemizde, bilişim ve bilgisayar denilince ilk akla gelen kurum Ulaştırma ve Altyapı Bakanlığı'dır. 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 koordinasyonu 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).

dikkat

Bilişim teknolojileri konusunda ülkemizdeki en yetkili kurum Ulaştırma ve Altyapı Bakanlığı'dır.

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

teminen 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.

Böylece, bilgisayar ağları ve hizmetlerinin düzenlemesi konusunun Ulaştırma ve Altyapı Bakanlığı'nın görevi kapsamında bulunması nedeniyle, bu alandaki ilk ve en yetkili kuruluşun Bakanlık olduğu, diğer yetkili organların ise, Bakanlığa doğrudan bağlı ya da gözetiminde olan kurum ve kuruluşlardan oluştuğu, bünyesinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulunduran mevzuat incelendiğinde rahatlıkla görülmektedir.

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 ve Altyapı 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 ilişkin önerilerde bulunmak.

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

Görüldüğü üzere internet ağı alanında ulusal politikanın belirlenmesi görevini üstlenen İnternet Geliştirme Kurulu, ülkemizde internet ağı ile ilgili planlama, koordinasyon, izleme, öneri oluşturma, eğitim vb. alanlarda projeler yürütmektedir. Kurul kararlarının icrası ise, Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilecektir. 5651 sayılı Kanun md. 10 Bilgi Teknolojileri ve İletişim Kurumu'na İnternet Geliştirme Kurulu'nca internetin yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli kullanılması gibi konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları

almayı bir görev olarak yüklemiştir. Bu yasal düzenleme göz önünde bulundurulduğunda, İnternet Geliştirme Kurulu kararlarının istişari nitelikle kalmayıp, icrai yönünün de bulunduğunu söylemek mümkündür.

dikkat

İnternet Geliştirme Kurulu kararlarının icrası Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilmektedir.

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.

dikkat

Telekomünikasyon İletişim Başkanlığı (TİB) 2016 yılında kapatılmıştır.

Kurum ülkemizde elektronik haberleşme alanında en önemli kurumdur. Zira her ne kadar Ulaştırma ve Altyapı Bakanlığı haberleşme, internet ve alt yapı işlerinde faaliyet gösteren şirketlerin almaları gereken izin ve ruhsat konusunda son işlemi yapsa da, bilişim şirketlerinin kuruluş aşamasında yapmaları gerekenleri belirten, kurulduktan sonra da onların denetimini yapan ve faaliyetleri sırasında da bunların uymaları gereken kuralları koyan Bilgi Teknolojileri ve İletişim Kurumu'dur. 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.

Kurum, Ulaştırma ve Altyapı Bakanlığı ile ilişkilidir. Kurum, idari ve mali özerkliğe sahip bir kamu tüzel kişiliğidir. Kurum görevlerini yerine getirirken bağımsızdır. Hiçbir organ, makam, merci veya kişi Kuruma emir ve talimat veremez.

Kurumun hizmet birimleri; hukuk müşavirliği, daire başkanlıkları ve müdürlükler şeklinde teşkilatlanan ana hizmet, danışma ve yardımcı hizmet birimleriyle bölge müdürlükleri şeklinde teşkilatlanan taşra teşkilatı birimlerinden oluşur.

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 ancak görevini yapmaya engel bir hastalık veya rahatsızlık nedeni ile iş görememe ya da 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 on yıl 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 üçünün 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 üç üyenin kabul etmesi gerekir.

Kurul en az beş üyenin hazır bulunması ile toplanır ve en az dört üyenin aynı yöndeki oyuyla karar alır. Üyeler çekimser oy kullanamaz. Toplantıda bir konuda karar yeter sayısı sağlanamadığı durumlarda, 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 görüşlerinden yararlanmak üzere uzman kişiler Kurul toplantılarına davet edilebilir. Kurul uygun gördüğü kararlarını internet ortamı başta olmak üzere uygun vasıtalarla kamuoyuna duyurur. Kurulun düzenleyici kararları ilişkili Bakanlığa yayımlanmak üzere gönderilir.

dikkat

Ülkemizde elektronik haberleşme alanına ilişkin olarak "regülasyon" yani düzenleme yapma yetkisi Bilgi Teknolojileri ve İletişim Kurumu'na aittir. Bu bağlamda ülkemizde internet alanına özgülenmiş tek birimin Bilgi Teknolojileri ve İletişim Kurumu olduğunu söylemek abartılı olmayacaktır.

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 öngördüğü 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 da Bilgi Teknolojileri ve İletişim Kurumu'na birçok görev ve yetki vermiştir. Gerçekten de söz konusu Kanun'un 10. maddesinin 4 ve devamı fıkralarına göre Kurum'un görev ve yetkileri şunlardır:

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 oluşturan 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 teminen 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.

Öğrenme Çıktısı

5 İnternetin yönetiminde yer alan yetkili ve sorumlu kurumların yetki ve görevlerini açıklayabilme

Araştır 4	İlişkilendir	Anlat/Paylaş
Türkiye'de internetin yönetiminde yer alan yetkili ve sorumlu kurumları sayınız.	Yapay zekâ, nesnelerin interneti gibi bilişim teknolojilerindeki çok hızlı gelişimler karşısında, Türkiye'de internetin yönetiminde yer alan kurumlara verilen yetki ve sorumlulukları bilişim hukuku çerçevesinde değerlendiriniz.	Türkiye'de internetin yönetiminde yer alan yetkili ve sorumlu kurumların birbirleriyle olan hukuki ilişkilerini anlatınız.

İNTERNET SÜJELERİNİN SORUMLULUĞU

Son olarak internet süjeleri olarak isimlendirilen içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcının sorumluluğuna değinilmelidir. Zira bir forumda, bir kullanıcı başka bir kullanıcıya hakaret ettiğinde, forumun bulunduğu internet sayfasının işletmecisinin de sorumlu tutulup tutulamayacağı örneğinde olduğu gibi internette vuku bulan bir hukuka aykırılıktan sonra, kimin hangi şartlar altında sorumlu olduğu sorunsalıyla karşılaşılır. Hemen belirtilmelidir ki, internet süjelerinin sorumluluğu oldukça geniş bir konudur ve her hukuk alanında (örneğin ceza hukuku, tazminat hukuku, kişilik haklarının korunması hukuku, rekabet hukuku, fikri mülkiyet hukuku) kendine özgü birtakım özelliklere haizdir. Bu nedenle aşağıdaki açıklamalar, internet süjelerinin tabi olduğu sorumluluk hukukunun bir özeti olarak anlaşılmalıdır.

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 (örneğin yukardaki örnekte hakaret eden forum kullanıcısı) kadar çok geniş bir kategoriyi oluşturmaktadır.

İçerik sağlayıcısı, 5651 sayılı Kanun'un 2. maddesinde, internet kullanıcılarına her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımlanmıştır. İçerik sağlayıcısının sorumluluğu aynı Kanun'un 4. maddesinde düzenlenmiştir.

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. Bundan dolayı yukarıdaki örnekte bir başka forum kullanıcısına hakaret eden forum kullanıcısı, bu kişiye karşı hem özel hukuk çerçevesinde tazminat ödemekle yükümlü tutulabilecek hem de ceza kanunu çerçevesinde hakaret suçunu işlediği iddiasıyla hakkında soruşturma başlatılabilecektir. Bu husus tartışmasız olmakla birlikte, içerik sağlayıcının link şeklinde bağlantı vermesi halinde sorumluluğunun belirlenmesi uygulamada bazen tereddütler yaratmak-

tadır. 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. Örneğin bir web sitesi sahibi, sitesi üzerinden içeriği başkaları tarafından hazırlanmış başka web sitelerine link yoluyla bağlantı verse ve söz konusu bağlantıların içeriğinde hukuka aykırı içerikler bulunsa dahi bundan sorumlu olmayacaktır. Ancak bu kuralın bir istisnası bulunmaktadır. Zira 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. Tabi bu noktada kuralın istisnai nitelikte olmasından bahisle içerik 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. İlerleyen bölümlerde bilişim suçlarının hukuki yönüyle ilgili olarak detaylı bilgiler verileceğinden, burada şu hususlara değinmek yeterli olacaktır:

Bilişim ortam ve sistemleri gelişmeye elverişli, yaygın kullanıma sahip, her yerden erişilebilen açık bir yapıya sahiptir. Yenilikçi yapısıyla bilişim sistemlerinde kullanılan teknikler her geçen daha da artmaktadır ve suçlular için yeni oyun alanları yaratmaktadır. Bu sebeple bilişim suçlarının ilk ortaya çıktığı zamanlarda, bu suçlarda kullanılan araçlar yazılım, donanım ve bilgisayar ağları iken, bugün bunlara özellikle sosyal medya ve bulut bilişim de eklenmiştir (Turan, 2016: 43).

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. Bu tek taraflılık web 2.0 teknolojisi ile değişmiştir. 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 en yaygın sosyal medya türleridir (Dülger, 2015: 92).

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. Zira bulut bilişim, geleneksel veri işleme yöntemleri ile değerlendirilemeyecek kadar çok büyük hacimli, oldukça kompleks, hızlı değişebilen verinin (büyük veri), birden çok bilişim ağında depolanması ve kullanıcıların da bu büyük veriye her yerden güvenli bir şekilde ulaşabilmesi düşüncesine dayanmaktadır (Turan, 2016: 224).

Buradan hareketle bilişim suçları bilişim sistemlerinin suçta araç olarak kullanıldıkları ya da bu sistemlerin hedef alındıkları hukuka aykırı filler olarak tanımlanmaktadır. 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 (Avşar ve Öngören, 2010: 46 vd.; Dülger, 2015: 80 vd.; Turan, 2016: 43).

Bilişim suçları, özellikle dar anlamda bilişim suçları, "yıkıcı yazılım" olarak adlandırılan tekniklerle işlenmektedir. Bu yazılım ya da tekniklere her gün yenileri eklenmekle birlikte, şu ana kadar sık rastlananlardan hareketle, örnek olarak 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 (örneğin çok sayıda banka hesabından) 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 (Avşar ve Öngören, 2010: 49 vd.; Dülger, 2015: 119). Bugün bilişim suçlarının çok büyük bölümü internet aracılığıyla, geriye kalan küçük bir kısmı ise kapalı ağ ortamı (intranet) ve diğer ağlar aracılığıyla işlenmektedir (Dülger, 2015: 115).

dikkat

Bilinen ilk bilişim suçu 18.10.1966 tarihinde Minneapolis Tribune gazetesinde yayınlanan "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı haber ile kamuoyuna yansımıştır. Bu olayda programlama şirketinde çalışan fail, banka programının mevcuttan fazla para çekilmesini düzenleyen yazılımını bozarak, kendi hesabına para göndermiştir. Bugün için çok basit olarak görülen bu olayın çözümü banka görevlileri ve yerel polis için o denli karmaşık olmuştur ki, olayın çözümü için FBI görevlendirilmiştir (Dülger, 2015: 114).

Bilişim suçlarında şüpheliye ulaşmak için en yaygın kullanılan yöntem, suç işlenirken kullanılan IP numarasının tespit edilerek, IP numarasının tahsis edildiği internet abonesini belirlemektir. Ancak sadece IP numarasının tespiti ile şüpheli hakkında mahkûmiyet kararı verilememektedir. Zira 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 (Dülger, 2015: 209, 802). Tüm bu süreç, bilişim sistemlerinden elde edilen verinin incelenmesini ve analizini yapan "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 (Dülger, 2015: 804).

Son olarak sosyal medyada işlenen suçlarda failin IP numarasının tespitindeki bazı özel durumlara dikkat çekilmelidir. Sosyal medya kullanıcılarının karşılaştıkları hakaret, siber mobbing, şantaj gibi hukuka aykırılıklarda failin bulunması için, ulusal soruşturma ve kovuşturma makamları (savcılık ve mahkemeler), merkezleri yurtdışında bulunan Facebook, Twitter gibi şirketlerden IP bilgisi, trafik verisi ve içeriğe ilişkin bazı bilgilere ihtiyaç duymaktadır. 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. Bu nedenle ulusal soruşturma ve kovuşturma makamları sosyal medyada işlenen bir suça ilişkin IP bilgisi, trafik verisi ve içeriğe ilişkin bilgileri elde etmek için, Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nü harekete geçirmeli ve Genel Müdürlük de istenilen bilgileri ABD'nin adli yardımlaşma hususunda yetkili makamı aracılığıyla şirketlerden talep etmelidir; zira sosyal medya şirketlerinin çoğu ABD merkezlidir (Dülger, 2015: 204 vd., 209). 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.

Oluşabilecek tereddütleri gidermek adına belirtmek gerekir ki, adli soruşturmada veya ceza yargılamasında, soruşturma ve kovuşturma makamlarının sosyal medya aracılığıyla delil etmesi ise, örneğin polisin sanığa karşı kullanacağı delilleri onunla Facebook listesinden arkadaş olma yoluna giderek elde etmesi veya bir hırsızlık şüphelisinin herkese açık bir Facebook paylaşımında çalınan arabayı kullanırken çektirdiği fotoğrafı savcılığın delil sayması, bilişim hukukuyla ilgili anlatılanlardan ziyade, genel olarak ceza muhakemesinin konusudur. 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 imkanına sahip olmayabilir (Avşar ve Öngören, 2010: 121).

> 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. Örneğin 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. Zira 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 doğacaktır. 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 imkana sahip olduğu kabul edilmelidir. Bu şartlar gerçekleştiği halde içerik kaldırılmıyorsa, yer sağlayıcısının da sorumluluğunun bulunduğu kabul edilebilecektir. Bu durum uygulamada genellikle internette vuku bulan kişilik haklarının ihlallerinde yaşanmaktadır. İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişiler, yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebilmektedirler (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. Yukarıdaki örnekte de kendisine hakaret edilen kullanıcı, kendisine hakaret eden forum kullanıcısına karşı yöneltebileceği tazminat talebini, forum sayfasının bulunduğu web sitesinin sahibine de yöneltebilecektir. Ceza hukuku bakımından ise farklı düşünmek gerekebilir. Yer sağlayıcısına karşı da ceza kanunu çerçevesinde hakaret suçunu işlediği iddiasıyla soruşturma açılabilmesi için, forum sayfasının bulunduğu web sitesinin sahibinin, hakaret eden kullanıcıyla ortak iştirak iradesiyle hareket ettiğinin ispatlanması gerekir ki, bu oldukça güçtür. Zira 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 barındırmazlar.

> 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. Zira internet 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 (Avşar ve Öngören, 2010: 118).

İşte internet servis sağlayıcısı sadece erişim hizmeti veriyor ise yani başkalarına ait bilgileri sunucularında barındırmıyorsa internet erişim sağlayıcısı adını alır. Aksi takdirde internet servis sağlayıcısı yer sağlayıcısı kabul edilir ve sorumluluğu yukarıda anlatılanlar ışığında belirlenir.

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, zira bunlar sadece internetin teknik altyapısını oluşturan, internete bağlantıyı sağlayan süjelerdir (Superonline, TTnet gibi). Bu bağlamda yukarıdaki örnekte kendisine hakaret edilen kullanıcı tazminat davasını erişim sağlayıcısına karşı açamaz. Yine erişim sağlayıcısının ceza sorumluluğunun doğmadığı başka açıklamaya gerek kalmadan anlaşılmaktadır. 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. Zira bu yöntemde kullanılan filtre doğru programlanmazsa, örneğin Essex Üniversitesinin sayfası da içerdiği sözcükler nedeniyle erişime engellenebilmektedir. 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 (Dülger, 2015: 875).

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 (örneğin kişilik haklarının ihlali) halinde hukuka aykırılık bulunduran web sitelerine erişimin engellenmesidir (Dülger, 2015: 876). 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 (5651 sayılı Kanun m. 8). 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 (Dülger, 2015: 873). Ancak bu noktada unutulmamalıdır ki, 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.

Yaşamla İlişkilendir

Türkiye'de yaklaşık 45 milyon, dünya genelinde ise 2 milyar civarında kullanıcısı olan sosyal paylaşım sitesi Facebook'ta asılsız haberlerin paylaşılması milyonları yanıltabiliyor. Facebook yönetimi, yalan haberlerin tespitine yönelik kullanıcıları bilgilendiren bir makale yayınladı.

'Asılsız Haberleri Tespit Etme' kılavuzunda asılsız haberleri tespit etmek için ipuçları da yer veriliyor. Facebook asılsız haberlerle mücadele amacıyla kendi web sitesinin Yardım Merkezi sekmesi altında "Asılsız Haberleri Tespit Etmek İçin İpuçları" başlıklı bir makale yayınladı. Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK), kamuoyuna duyurduğu makalede Facebook'ta yayınlanan haberlerin sahte olup olmadığını anlamak için kullanıcılara bazı ipuçları veriliyor. Makalede, paylaşımın esas olduğu sosyal medya mecralarında, asılsız haberlerin paylaşımı daha kolay ve yaygın olduğundan, kullanıcılar özellikle haber ve benzeri linkleri paylaşmadan önce bazı kriterleri göz önünde bulundurmaları gerektiği hatırlatılıyor. Asılsız ve yalan haberlerin yayılmasını önlemek için şüpheli ve güvenli bulunmayan linkler paylaşılmaması gerekiyor.

Paylaşım yapılmadan önce haber kaynağının ve internet adresinin (URL) güvenilir olup olmadığı kontrol edilmesi gerektiğinin vurgulandığı yazıda, 'Şüpheli ve güvenli olmayan bağlantılar dolaşıma girdiğinde ve tıklandığında, virüs ve zararlı yazılımlar bilgisayarlara otomatik olarak yerleşir. Bu zararlı yazılımlar ve virüsler de dolandırıcılık amacıyla kullanılmaktadır. Asılsız haberleri önceden fark etmek ve internette doğru bilginin dolaşımına katkı sağlamak için; bilgi kaynağının güvenilir olması, bilgiye - habere birden fazla kaynaktan ulaşmak, eleştirel bir bakış açısı edinmek ve bilgileri farklı kaynaktan teyit etmek gerekir . Unutulmamalıdır ki; internette ve sosyal medya ortamlarında karşılaşılan her bilgi doğru ve güvenilir değildir' ifadeleri kullanıldı.

Başlıklara aldanmayın

Asılsız haberlere karşı kullanıcıların dikkat etmesi gereken hususlar ise şu şekilde açıklandı: 'Başlıklara şüpheyle yaklaşın: Çoğu zaman asılsız haberlerin, tamamı büyük harflerle yazılmış ve ünlem işareti eklenmiş dikkat çekici başlıkları vardır. Başlıktaki sarsıcı iddialar size inanılmaz geliyorsa, muhtemelen inanmamanız gerekir.

İnternet adresine (URL) yakından bakın

Sahte veya taklit bir internet adresi (URL), asılsız bir haberi işaret ediyor olabilir. Pek çok asılsız haber sitesi, internet adresinde (URL) küçük değişiklikler yaparak gerçek haber kaynaklarını taklit etmektedir. Siteye giderek internet adresini (URL) gerçek kaynaklarla karşılaştırabilirsiniz.

Kaynağı araştırın

Haberin, doğruluk konusunda itibarlı, güvendiğiniz bir kaynak tarafından yazıldığından emin olun. Haber tanımadığınız bir kuruluştan geliyorsa, daha fazla bilgi almak için 'Hakkında' kısmına bakın.

Yazı biçiminin olağandışı olup olmadığına dikkat edin

Pek çok asılsız haber sitesinde yazım hataları veya tuhaf sayfa düzenleri olur. Bunları görürseniz habere dikkat edin.

Fotoğraflara dikkat edin

Asılsız haberler çoğu zaman üzerinde oynanmış görüntüler veya videolar içerir. Bazen fotoğraf gerçek olduğu halde bağlam dışında kullanılmış olabilir. Nereden geldiğini doğrulamak için fotoğrafı veya görüntüyü internette aratabilirsiniz.

Tarihleri inceleyin

Asılsız haberlerdeki tarih ve saat çizgisi mantıksız olabilir veya olayların tarihleri değiştirilmiş olabilir.

Kanıtları kontrol edin

Yazarın kaynaklarını kontrol ederek doğru olduklarından emin olun. Kanıt olmaması veya adı belirtilmeyen uzmanlara güvenilmesi haberin yalan olduğuna işaret edebilir.

Başka haber kaynaklarına bakın

Aynı haberi bildiren başka haber kaynağının olmaması, haberin asılsız olduğunu gösterebilir. Haber, güvendiğiniz birden fazla kaynak tarafından bildiriliyorsa, haberin doğru olma ihtimali daha yüksektir.

Haber bir şaka mı?

Bazen asılsız haberler ile mizahı veya hicvi ayırt etmek zor olabilir. Haber kaynağının parodi konusunda tanınmış olup olmadığını kontrol edin ve haberin detaylarından ve tonundan sadece eğlence amaçlı olup olmadığını anlamaya çalışın.

Bazı haberler kasten yanlış bilgi içerir

Okuduğunuz haberler hakkında eleştirel bir yaklaşımla düşünün ve sadece güvenilir olduğunu bildiğiniz haberleri paylaşın.

Kaynak: http://www.on5yirmi5.com/haber/bilim-teknoloji/internet/221863/facebooktan-kullanicilarina-onemli-uyari.html

Öğrenme Çıktısı

6 İnternet süjelerini tanımlayabilme
7 İnternet süjelerinin sorumluluklarını açıklayabilme

Araştır 5	İlişkilendir	Anlat/Paylaş
İnternet süjelerini belirtiniz ve internet servis sağlayıcısını açıklayınız.	İnternet süjelerinin sorumluluğunun belirlenmesinde yapılan üçlü ayrımın yeterli olup olmadığını değerlendiriniz.	Bilişim suçlarının faillerinin neden genellikle içerik sağlayıcı olduğunu anlatınız.

öğrenme çıktıları ve bölüm özeti

1 Bilişim hukukunu tanımlayabilme

2 Bilişim hukuk dalının yapısını ve ortaya çıkış nedenlerini açıklayabilme

Bilişim Hukuku

Bilişim hukuku, elektronik ortamlarda, iletişim, bilgi ve belge paylaşımının sağlanmasının hukuki çerçevesi ve sonuçları ile bu ortamlarda vukuu bulan hukuka aykırı fiillere ilişin yaptırımların öngörüldüğü mevzuatın oluşturduğu hukuk normlarının tamamına verilen bir isimdir. Bilişim hukuku, bilişim teknolojilerindeki gelişmeler ve yenilikler sebebiyle mevcut yasal düzenlemelerin yetersiz kalması ile ortaya çıkmış bir hukuk dalıdır. Bilişim hukukunun hedefi bilgi toplumunun oluşturulması ve geliştirilmesidir.

3 Bilişim hukuku mevzuatında yer alan temel kavramları açıklayabilme

Bilişim Hukuku Mevzuatına Genel Bakış

Bilişim hukuku multi-disipliner bir hukuk dalı olarak tanımlanmaktadır. Bundan dolayı bilişim hukukunu düzenleyen tek bir kanun ve buna bağlı tali mevzuat bulunmamaktadır. Bilişim hukukunu oluşturan mevzuat, birçok kanunun içine serpiştirilmiştir ve bu nedenle de 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 doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulunduran mevzuatın genel özelliği, bunların bünyelerinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulundurmalarıdır. Bunlar 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5369 sayılı Evrensel Hizmet Kanunu ve 5809 sayılı Elektronik Haberleşme Kanunu'dur.

4 Bilişim, bilgisayar ve internete dair bazı önemli teknik kavramları tanımlayabilme

Bilişim, Bilişim Sistemleri ve İnternet

Bilişim hem verilerin işlenmesini, yani bilgi işlemi, hem de bilgi işlemin sonucunun aktarılmasını, yani veri iletişimini ifade eden bir kavramdır. Bundan dolayı bilgisayar ve bilişim sözcükleri farklı anlamlara sahiptirler. Bilişim bir bilim dalını, bilgisayar ise bir makineyi ifade eder. Dolayısıyla her bilgisayarın bir bilişim sistemi olduğu ancak herhangi bir bilişim sisteminin zorunlu olarak bir bilgisayar olmadığı kabul edilmelidir.

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. İnternete ağlar arası ağ da denilmektedir. İnternetin teknik alt yapısını veri iletişimini sağlayan omurgalar (backbone), internet içindeki bilişim sistemlerinin birbirleriyle iletişim kurabilmeleri ve veri aktarımında bulunabilmeleri sağlayan TCP/IP (Transmission Control Protocol/Internet Protocol) protokolleri ve web browser ve web sayfasının bir araya gelmesinden oluşan World Wide Web (www) oluşmaktadır.

İnternetin ortaya çıkışı soğuk savaş döneminde ABD ve Sovyetler Birliği arasında yaşanan rekabete dayanmaktadır. ABD'de Savunma Bakanlığı'na bağlı olan ve birbirinden uzakta olan bazı askeri birliklerin geliştirdiği projelerin ortak bir ağ üzerinden birleştirilmesi temeline dayanan ARPA adlı bir birim oluşturmuştur. Buradaki çalışmalar sonucunda da farklı sistemleri birbirine bağlamak için ARPANET adlı bir askeri bilgisayar ağı kurulmuştur.

İnternetin yönetiminde çeşitli kurumlar bulunmaktadır. Bunlardan ilki internetin yönetim ve gelişme politikalarını belirleyen ICANN kurumudur. ICANN, alan adları sisteminin teknik yönetimi, protokol parametrelerinin belirlenmesi ve kök sunucu sistemi yönetimi işlevlerini koordine etmekle görevlidir. Diğer bir kurum IANA kurumudur. Her iki kurumun altında dünyanın beş bölgesi için internet kaynaklarını ICANN'in belirlediği politikalara göre yöneten kuruluşlar vardır. Bunlara RIR denir. Türkiye RIPE NCC bölgesindedir. RIPE NCC'nin merkezi Hollanda'dadır. RIR merkezleri altında son kullanıcıya IP adresi veren internet servis sağlayıcıları vardır. Bunlara da LIR denilir.

öğrenme çıktıları ve bölüm özeti

5 İnternetin yönetiminde yer alan yetkili ve sorumlu kurumların yetki ve görevlerini açıklayabilme

Türkiye'de İnternetin Yönetiminde Yer Alan Yetkili ve Sorumlu Kurumlar

Ülkemizde bilgisayar ağları ve hizmetlerinin düzenlemesi konusunda en yetkili kurum Ulaştırma ve Altyapı Bakanlığı'dır. Bünyesinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulunduran mevzuat incelendiğinde bu alandaki diğer yetkili organların Bakanlığa doğrudan bağlı ya da gözetiminde olan kurum ve kuruluşlardan oluştuğu görülmektedir.

İnternet Geliştirme Kurulu'nun ana işlevi, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na danışmanlık yapmaktır. 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.

Bilgi Teknolojileri ve İletişim Kurumu ülkemizde elektronik haberleşme alanında en önemli kurumdur. Zira bilişim şirketlerinin kuruluş aşamasında yapmaları gerekenleri belirten, kurulduktan sonra da onların denetimini yapan ve faaliyetleri sırasında da bunların uymaları gereken kuralları koyan Bilgi Teknolojileri ve İletişim Kurumu'dur. 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. 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.

6 İnternet süjelerini tanımlayabilme

7 İnternet süjelerinin sorumluluklarını açıklayabilme

İnternet Süjelerinin Sorumluluğu

İçerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcısına internet süjeleri denir. İnternet kullanıcılarınca herhangi bir internet içeriğini hazırlayan veya bilgiyi, veriyi bizzat üreten internet süjesine içerik sağlayıcı denir. İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur (5651 sayılı Kanun m. 4). Bu sorumluluğun gerek özel hukuk ve gerekse de ceza hukuku sorumluğu olduğuna şüphe yoktur. Bundan dolayı bilişim suçlarının faili de genelde içerik sağlayıcıdır. Bilişim suçları bilişim sistemlerinin suçta araç olarak kullanıldıkları ya da bu sistemlerin hedef alındıkları hukuka aykırı filler olarak tanımlanmaktadır. 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. Buna karşın geniş anlamda bilişim suçları ise bilişim sistemleri kullanılarak veya bilişim sistemlerinden yararlanılarak işlenen klasik suçlardır.

Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilere yer sağlayıcı denir. Yer sağlayıcılarının kural olarak sorumluluğu bulunmamaktadır. Zira 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 doğacaktır.

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, çoğu kez internet servis sağlayıcıları ile aynı anlamda kullanılmaktaysa da, bu her zaman doğru değildir. İnternet servis sağlayıcısı sadece erişim hizmeti veriyor ise yani başkalarına ait bilgileri sunucularında barındırmıyorsa internet erişim sağlayıcısı adını alır. Aksi takdirde internet servis sağlayıcısı yer sağlayıcısı kabul edilir. İnternet erişim sağlayıcısı, kullanıcılarının internete koymuş oldukları içerikten sorumlu değildir, zira bunlar sadece internetin teknik altyapısını oluşturan, internete bağlantıyı sağlayan süjelerdir.

Erişimin engellenmesi hususunda erişimin genel engellenmesi ve erişimin özel engellenmesi ayrımı yapılır. Genel engelleme, devletlerin interneti bir filtreye tabi tutularak bazı web sitelerine erişimi henüz bir suç unsuru oluşmadan engellemesidir. 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 (örneğin kişilik haklarının ihlali) halinde hukuka aykırılık bulunduran web sitelerine erişimin engellenmesidir. Erişimin özel engellenmesinde birçok teknik kullanılmaktadır. Bunlardan en yaygın olanları IP engellemesi, DNS engellemesi ve URL engellemesidir. IP ve DNS engellemesinin en büyük dezavantajı web sayfasında yer alan içeriğin tümünün engellenmesidir. URL engellemesi yönteminin en önemli avantajı hukuka aykırı bir içerik için tüm web sitesinin erişime engellenmemesidir.

1 İnternet süjelerinin yükümlülük ve sorumluluklarını düzenleyen temel Kanun aşağıdakilerden hangisidir?

A. 5070 sayılı Elektronik İmza Kanunu
B. 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
C. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
D. 5369 sayılı Evrensel Hizmet Kanunu
E. 5809 sayılı Elektronik Haberleşme Kanunu

2 Hem verilerin işlenmesini hem de bu işlemin sonucunun aktarılmasını ifade eden akademik ve mesleki disipline ne ad verilir?

A. Netiket
B. Bilişim
C. Bilgisayar
D. ARPANET
E. World Wide Web

3 Aşağıdakilerden hangisi TCP/IP (Transmission Control Protocol/Internet Protocol) yazışma diline örnek olarak **gösterilemez?**

A. Carnivore
B. FTP/File Transfer Protocol
C. SMTP/Simple Mail Transfer Protocol
D. DNS/Domain Name System
E. HTTP/Hyper Text Transfer Protocol

4 İnternetin ortaya çıkışında önemli rol oynayan ABD'de hazırlanan askeri projeye ne ad verilir?

A. Sputnik
B. Backbone
C. Carnivore
D. Arpanet
E. Echelon

5 Alan adları sisteminin teknik yönetimi, protokol parametrelerinin belirlenmesi ve kök sunucu sistemi yönetimi işlevlerini koordine etmekle görevli olan uluslararası kurum aşağıdakilerden hangisidir?

A. Internet Assigned Numbers Authority/IANA
B. Regional Internet Registry/RIR
C. Local Internet Registry/LIR
D. Advanced Research Project Agency/ARPA
E. Internet Corporation for Assigned Names and Numbers/ICANN

6 Aşağıdakilerden hangisi internet ortamıyla ilgili olarak Ulaştırma ve Altyapı Bakanlığı'na danışmanlık yapmakla görevlidir?

A. Haberleşme Genel Müdürlüğü
B. Bilgi Teknolojileri ve İletişim Kurumu
C. Bilgi Teknolojileri ve İletişim Kurulu
D. Erişim Sağlayıcıları Birliği
E. İnternet Geliştirme Kurulu

7 5651 sayılı Kanun'a 671 sayılı Kanun Hükmünde Kararname (KHK) ile eklenen ek madde 3 ile 2016 yılında kapatılan organ aşağıdakilerden hangisidir?

A. Telekomünikasyon İletişim Başkanlığı
B. Haberleşme Genel Müdürlüğü
C. İnternet Geliştirme Kurulu
D. Bilgi Teknolojileri ve İletişim Kurumu
E. Bilgi Teknolojileri ve İletişim Kurumu

8 İnternet ortamında yapılan yayınların içeriklerini izleyerek, 5651 sayılı Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak öngörülen gerekli tedbirleri almakla yetkili kılınan organ aşağıdakilerden hangisidir?

A. İnternet Geliştirme Kurulu
B. Bilgi Teknolojileri ve İletişim Kurumu
C. Haberleşme Genel Müdürlüğü
D. Erişim Sağlayıcıları Birliği
E. İnternet Geliştirme Kurulu

9 İnternet ortamında kullanıma sunduğu her türlü içerikten sorumlu olan internet süjesi aşağıdakilerden hangisidir?

A. Yer sağlayıcı
B. Erişim sağlayıcı
C. Servis sağlayıcı
D. İçerik sağlayıcı
E. Toplu kullanım sağlayıcı

10 Aşağıdakilerden hangisi yalnızca hukuka aykırı içeriğe erişimin engellenmesi amacıyla kullanılan tekniklerden biridir?

A. URL engellemesi
B. IP engellemesi
C. DNS engellemesi
D. Genel engelleme
E. Özel engelleme

1. C	Yanıtınız yanlış ise "Bilişim Hukuku Mevzuatına Genel Bakış" konusunu yeniden gözden geçiriniz.
2. B	Yanıtınız yanlış ise "Bilişim" konusunu yeniden gözden geçiriniz.
3. A	Yanıtınız yanlış ise "İnternetin Teknik Alt Yapısı" konusunu yeniden gözden geçiriniz.
4. D	Yanıtınız yanlış ise "İnternetin Tarihçesi" konusunu yeniden gözden geçiriniz.
5. E	Yanıtınız yanlış ise "İnternetin Yönetimi" konusunu yeniden gözden geçiriniz.
6. E	Yanıtınız yanlış ise "Türkiye'de İnternetin Yönetiminde Yer Alan Yetkili ve Sorumlu Kurumlar" konusunu yeniden gözden geçiriniz.
7. A	Yanıtınız yanlış ise "Bilişim Hukuku Mevzuatına Genel Bakış" konusunu yeniden gözden geçiriniz.
8. B	Yanıtınız yanlış ise "Türkiye'de İnternetin Yönetiminde Yer Alan Yetkili ve Sorumlu Kurumlar" konusunu yeniden gözden geçiriniz.
9. D	Yanıtınız yanlış ise "İnternet Süjelerinin Sorumluluğu" konusunu yeniden gözden geçiriniz.
10. A	Yanıtınız yanlış ise "İnternet Süjelerinin Sorumluluğu" konusunu yeniden gözden geçiriniz.

1 Araştır Yanıt Anahtarı

Araştır 1

Bilişim hukuku, elektronik ortamlarda, iletişim, bilgi ve belge paylaşımının sağlanmasının hukuki çerçevesi ve sonuçları ile bu ortamlarda vukuu bulan hukuka aykırı fiillere ilişin yaptırımların öngörüldüğü mevzuatın oluşturduğu hukuk normlarının tamamına verilen bir isimdir. Bilişim hukuku, bilişim teknolojilerindeki gelişmeler ve yenilikler sebebiyle mevcut yasal düzenlemelerin yetersiz kalması ile ortaya çıkmış bir hukuk dalıdır.

Araştır 2

Bünyesinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulunduran mevzuatın genel özelliği, bunların bünyelerinde doğrudan internet ortamını veya bilişim alanını düzenlemeye yönelik normlar bulundurmalarıdır. Bunlar 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5369 sayılı Evrensel Hizmet Kanunu ve 5809 sayılı Elektronik Haberleşme Kanunu'dur.

Araştır 3

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. İnternete ağlar arası ağ da denilmektedir. İnternetin teknik alt yapısını veri iletişimini sağlayan omurgalar (backbone), internet içindeki bilişim sistemlerinin birbirleriyle iletişim kurabilmeleri ve veri aktarımında bulunabilmeleri sağlayan TCP/IP (Transmission Control Protocol/Internet Protocol) protokolleri ve web browser ve web sayfasının bir araya gelmesinden oluşan World Wide Web (www) oluşmaktadır.

1 Araştır Yanıt Anahtarı

Araştır 4

Ulaştırma ve Altyapı Bakanlığı; İnternet Geliştirme Kurulu, Bilgi Teknolojileri ve İletişim Kurumu.

Araştır 5

İçerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcısına internet süjeleri denir. İnternet erişim sağlayıcıları, çoğu kez internet servis sağlayıcıları ile aynı anlamda kullanılmaktadır. İnternet servis sağlayıcısı sadece erişim hizmeti veriyor ise yani başkalarına ait bilgileri sunucularında barındırmıyorsa internet erişim sağlayıcısı adını alır. Aksi takdirde internet servis sağlayıcısı yer sağlayıcısı kabul edilir.

Kaynakça

Avşar, B.Z. ve Öngören, G. (2010). *Bilişim Hukuku*. Türkiye Bankalar Birliği Yayınları, İstanbul.

Dülger, M. V. (2015). *Bilişim Suçları ve İnternet İletişim Hukuku*. 6. Baskı, Seçkin Yayıncılık, Ankara.

Turan, M. (2016). *Bilişim Hukuku*. Seçkin Yayıncılık, Ankara.

Bölüm 2

Bilişim, İnsan Hakları ve Kişisel Verilerin Korunması

Öğrenme çıktıları

Bilişim Teknolojileri ve İnsan Hakları

1 İnsan hakları ile bilişim teknolojileri arasındaki ilişkiyi açıklayabilme

Kişisel Veri ve Kişisel Verilerin İşlenmesi

2 Kişisel veri ve kişisel verilerin işlenmesini tanımlayabilme

Kişisel Verilerin Korunmasının Önemi

3 Kişisel verilerin korunmasının önemini açıklayabilme

Kişisel Verilerin Korunması Hakkı

4 Kişisel verilerin korunması hakkının diğer temel hak ve özgürlüklerle ilişkisini açıklayabilme

Kişisel Verilerin Korunmasında Hakim Olan Temel İlkeler

5 Kişisel verileri korunmasında hakim olan temel ilkelerin neler olduğunu açıklayabilme

Anahtar Sözcükler: • İnsan Hakları • Kişisel Veri • Kişisel Verilerin Korunması • Özel Yaşamın Gizliliği • Düşünceyi Açıklama Özgürlüğü • Özel Haberleşmenin Gizliliği

GİRİŞ

20. Yüzyıl pek çok açıdan insanlık tarihine damgasını vurmuştur. İki dünya savaşının yaşandığı bu dönemde bir yanda acısı unutulmayacak bir yıkım yer alır. Bu acıların bir daha yaşanmaması dileği ise yine aynı dönemde insan haklarının güçlü bir şekilde seslendirilmesine neden olmuştur. Özellikle II. Dünya savaşı sonrasında pek çok devletin anayasasında ve uluslararası metinlerde temel hak ve özgürlükleri sağlamaya yönelik güçlü koruma rejimleri oluşturulmuştur. Bu durum başta Batı Avrupa olmak üzere dünyanın pek çok yerinde devlet ve yurttaş ilişkilerinin insan hakları ekseninde değerlendirilmesini gerekli kılmıştır. Öte yandan özellikle yirminci yüzyılın ikinci yarısı farklı bir gelişim dolayısıyla daha insanlık tarihi açısından önemlidir. 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. Başta İnternet'in ortaya çıkması ve yaygınlaşması olmak üzere bilişim alanında hızı her geçen gün artan gelişmeler henüz başında olduğumuz 21. Yüzyılda bilişim teknolojileri ve insan hakları kesişiminde pek çok tartışmayı beraberinde getirmektedir. Gelişen teknolojinin insan hakları üzerindeki olumlu ya da olumsuz etkileri, içinde bulunduğumuz zaman parçasının en çok tartışılan konularından biridir.

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 yüzde 753 oranında artmıştır. Bugün dünyada üç milyarın üzerinde İnternet kullanıcısı olduğu tahmin edilmektedir (Internet World Stats, 2015). 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 alışverişini İnternet üzerinden sipariş etmekte, sohbet odalarında yeni bir sosyal çevre yaratmaktadır. Bunlar saymakla bitmeyecek pek çok örneğin yalnızca bir kaçıdır. İşte 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. Bilişim teknolojilerindeki gelişim İnternet'e erişim hakkı ve kişisel verilerin korunması hakkı başta olmak üzere yeni hak kategorilerinin filizlenmesini ve hızla gelişmesini de sağlamıştır.

İnsan hakları odaklı bir İnternet ortamının yaratılması yönünde talepler artmakta bu konuda çeşitli girişimlerde bulunulmaktadır. İnsan haklarının eksen kavramlarından eşitlik, sanal ortamda gerçekleştirilmesi gereken yeni bir boyut kazanmıştır. Bu anlamda halen İnternet'e dünyanın nüfusunun belirli bir bölümünün erişebilmesi sosyal adalet konusunda da yeni tartışma alanları yaratmaktadır. Bu açıdan İnternet'e erişim hakkı bir yandan herkesin ağa ulaşacak araçlara sahip olmasını gerektirirken, diğer yandan bu erişimin güvenli ve özgür olması gereksinimini ortaya koymaktadır. İnternet'e erişim hakkına ilişkin yakın zamanda gerçekleşen iki gelişme bu konudaki çalışmaların artarak devam edeceği yönünde dikkat çekici sinyaller vermektedir. Nitekim 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 önümüzdeki dönemde 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. Bu yaklaşım birey, devlet ve teknoloji ilişkisinde dengeyi sağlayan hukuksal düzenlemelerin geliştirilmesini gerektirir. Bu açıdan İnternet ve diğer bilişim teknolojileri yardımıyla işlenen suçlar ya da diğer hukuka aykırılıklarla mücadele ederken, bu araçların kendine özgü nitelikleri ve özgür toplumsal yapı açısından ifade ettikleri değer dikkate alınmalıdır. Gelişimin nasıl seyredeceği konusunda kesin bir öngörüde bulunmak olanaklı değildir. Ancak bugünün sorunlarını ve ulaşılan çözüm yollarını değerlendirmek insan hakları ve bilişim arasındaki ilişkiyi ortaya koyabilmek açısından gereklidir. Bu noktada kişisel verilerin korunması özel bir öneme sahiptir.

Bilişim ile doğrudan ilgili ilk hukuksal düzenleme 1970 yılında Almanya'nın Hessen eyaletinde kişisel verilerin korunmasına ilişkin olarak gerçekleştirilmiştir. Kişisel verilerin korunması hakkı, teknolojinin sağladığı olanakları güçlendirmek ile değil, yarattığı yan etkiler ile ilişkilidir. Bilişim ile insan hakları arasında dengenin kurulması açısından da kırk yıldan uzun bir süre içerisinde gelişen, çeşitlenen, yaygınlaşan hukuksal düzenlemelerden ulusal ve uluslararası düzeyde çok çeşitli örnekler sunmaktadır. Bu hukuksal düzenlemeleri değerlendirmeye geçmeden önce kişisel verinin ne olduğunu, neden önemli olduğunu ve öneminin neden her geçen gün arttığını ilişkili olduğu diğer hak ve özgürlükleri de dikkate alarak incelemek ve kişisel verilerin korunmasında hâkim olan temel ilkeleri belirlemek gerekir.

Öğrenme Çıktısı

1 İnsan hakları ile bilişim teknolojileri arasındaki ilişkiyi açıklayabilme

Araştır 1	İlişkilendir	Anlat/Paylaş
Bilişim ile ilgili düzenlemeler kapsamında kişisel verilerin korunmasına yönelik düzenlemelerin tarihsel gelişim sürecini araştırınız.	Bilişim teknolojilerindeki gelişim ile insan hakları ihlalleri arasındaki bağlantıyı tartışınız.	nternet üzerinden gerçekleştirilmiş insan hakları ihlallerine ilişkin örnekleri çevrenizle paylaşınız.

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, başkalarına aktarılmasını olanaklı kılmaktadır. Bu durum, kişisel verilerin korunmasının çağımızın en dikkat çekici hak alanlarından biri olmasının nedenidir. 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. İşte bu hukuksal güvenceler, özel yaşamın gizliliği hakkı ile yakından ilişkili olan "kişisel verilerin korunması" çatısı altında toplanmaktadır.

Hemen bu noktada kişisel verilerin korunması ile özgür bilgi akışı önünde bariyerler kurmanın amaçlanmadığını belirtmek gerekir. Kişisel verilerin korunması, veri işleme teknolojileri ile temel hak ve özgürlükler arasında denge kurmayı hedefler. Bu denge veri işlemenin meşru temellerinin ve uyulması ge-

reken 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 ve önemi her geçen gün artan hak alanının tanımlanmasında "veri" (data) kavramının kullanılmasının nedeni de budur. Ancak "kişisel veri" kavramının doğrudan kişi ile ilgili olduğu unutulmamalıdır. Aşağıda kişisel verilerin korunması hakkının önemi, gelişimi ve hukuksal kaynakları üzerinde durulacaktır. Ancak bundan önce bazı deyimsel açıklamaların yapılması gerekir. Nitekim kişisel veri ve kişisel verilerin işlenmesi deyimlerinin kapsamını belirlemek konuya ilişkin tartışmaların anlaşılmasında yararlı olacaktır.

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. Şu hususun altını çizmek gerekir ki bu ilkelerin benimsenmesindeki temel gaye, "veri"lerin, yani herhangi bir rakamın, herhangi bir bilginin, herhangi bir görüntünün, korunması değildir. Burada hedeflenen kişilerin korunmasıdır.

Dikkat çeken hususlardan biri, "kişisel veri" deyiminin, konuyla doğrudan ilişkili olmayan kişilerce, çoğu kez, biraz soğuk ve fazla teknik bir kavram olarak algılanmasıdır. Konunun teknik bir boyutu olduğu doğrudur. Nitekim aşağıda açıklanacağı üzere kişisel verilerin korunmasına yönelik ilk hukuksal düzenlemeler kabul edilirken, bilgisayar veri tabanlarının gelişmesi sonucunda kişisel bilgilerin otomatik yollarla işlenmesinden kaynaklı kaygılar etkili olmuştur.

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. Bu tanımda "her türlü" bilgi ifadesinin kullanılması oldukça geniş bir alanın hedeflendiğinin işaretidir. Burada bilginin türüne ilişkin herhangi bir ayrım yapılmamaktadır. Sayı, yazı, ses ya da görüntüden oluşan bir bilgi bu kapsamda yer alabilir. Ancak bu noktada her türlü bilginin önünde yer alan tanımlamayı unutmamak gerekir. Buna göre 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.

Bu kapsamda hangi bilgilerin kişisel veri olarak kabul edileceği, hangilerinin bu kapsamın dışında kalacağını birkaç örnek üzerinden açıklamaya çalışalım. Bir kişinin adı ve soyadı onu belirli kılan, bir başka anlatımla onu diğer herkesten ayıran bilgiler arasında ilk akla gelendir. Bu anlamda ad ve soyadı bilgisi, kişisel veri niteliğindedir. Ancak bazı durumlarda tek başına yeterli olmayabilir. Örneğin, yaygın bir adı ve soyadı olan bir kişiye ilişkin yalnızca bu bilgiye sahip olmak o kişiyi belirlenebilir kılmaz. Aynı şekilde bazen bir kişinin, adı ve soyadı belirtilmese de belirlenebilir olduğu görülür. *"…"* adresinde ikamet eden kişi ya da *"Anadolu Üniversitesi Hukuk Fakültesi Dekanı"* bilgisi, bu kişileri belirlenebilir kılmak için yeterlidir.

Bir başka örnek, kişinin görüntüsüne ilişkin olarak verilebilir. Örneğin kapalı devre televizyon sistemlerine ya da genel olarak kameralara yansıyan görüntüler kişisel veri olarak kabul edilecek midir? Bu görüntünün bir kişiyi belirlenebilir kılması olasılığı söz konusu olduğu durumlarda kişisel veri olarak kabul edileceği hususunda şüphe yoktur. 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. Nite-

kim 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.

Bu noktada kısaca **kişisel verilerin işlenmesi** kavramını da açıklamak gerekir. Yukarıdaki tanıma uygun olan bir bilgi ya da bilgi kümesi, yani kişisel verilerin, üzerinde gerçekleştirilen her türlü işlem bu kapsamdadır. Konuya ilişkin ulusal ve uluslararası metinlerde bu işlemler sınırlı sayım ile belirlenmemiş, aksine örnekleme yoluna gidilmiştir. Örneğin konuya ilişkin AB Yönergesinde (95/46/AT) "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" işleme olarak tanımlanmıştır. Türkiye'de konuya ilişkin hukuksal düzenlemeler kapsamında incelenecek olan Veri Koruma Kanun Tasarısı'nda da benzer bir tanımın benimsendiğini belirtmek gerekir. Dikkat çekmek gerekir ki verilerin işlenmesi ile kastedilen yalnızca bu bilgilerin kayıt edilmesi ya da kullanılması değildir. Kişisel verileri değiştirme, silme, yok etme gibi işlemlerin de veri koruma hukuku açısından "işleme" olarak nitelendirilen etkinliğin kapsamında olduğuna şüphe yoktur.

Öğrenme Çıktısı

2 Kişisel veri ve kişisel verilerin işlenmesini tanımlayabilme

Araştır 2	İlişkilendir	Anlat/Paylaş
Kişisel verilerin işlenmesi kavramından ne anlaşılmaktadır?	Kişisel verilerin işlenmesi ne gibi riskler doğurabilir?	Kişisel verilerin işlenmesi hakkında çevreniz bilinçli mi? Gözleyiniz.

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. Öte yandan modernleşme sonrasında hız kazanmakla birlikte önceki dönemler de dahil olmak üzere yöneticilerin, sosyal ya da siyasal toplulukların da ilişkide oldukları kişilere ilişkin çeşitli araçlar geliştirdikleri görülmektedir. 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.

Gerçekten, verilerimize yönelen bilme isteği yeni olmasa da kişisel verilerin korunması 1960'larda tartışılmaya, 1970'lerde ise hukuksal düzenlemelerin konusu olmaya başlar. Bunda teknolojideki, özellikle de bilişim teknolojilerindeki gelişmenin etkisi yadsınamaz. Bu dönemde bir yanda kökeni çok daha eskilere dayanan devletin gözetim isteği, diğer yanda yeni gelişmeler ile bu isteğin eski dönemlerde görülmeyen ölçüde kapsayıcı bir şekilde gerçekleşme olasılığı, bireysel özerkliğe ilişkin kaygıların gelişmesine neden olmuştur. O halde, kişisel verilerin korunması hukukunun ortaya çıkışında temelde üç etkenin bulunduğu söylenebilir: çeşitli örgütlerce kişisel verilere duyulan gereksinim, teknolojideki gelişmeler, gözetim teknolojilerindeki gelişmeler nedeniyle duyulan kaygı.

Kişisel verilerin korunması, bireyleri, kendilerine ilişkin bilgilerin bilişim teknolojileri ya da dosyalama gibi geleneksel yöntemlerle işlenmesinden doğacak zararlardan koruma amacına yönelmiş ve bazı temel ilkelerde somutlaşmış bir dizi önlemi ifade eder. Kişisel verilerin korunması hukuku ilk aşamada devlete karşı bireyin korunmasına yönelmiştir. Bu koruma alanı halen önemini ve güncelliğini korumaktadır. Ancak şirketlerin de veri işleme yöntemlerini artan oranda ve yaygın bir biçimde kullanmaları özel teşebbüslere karşı da koruma sağlanmasını gerekli kılmaktadır. Özellikle sosyal paylaşım sitelerinde kimisi oldukça hassas da olan bilgilerin paylaşılması özel teşebbüsler tarafından işletilse de bu alanlarda da korumaya ihtiyaç duyulduğunu açıkça ortaya koymaktadır.

Özellikle son on yılda iş yaşamımızın, alışveriş yapma şeklimizin, bankacılık faaliyetlerimizin ve sosyal ilişkilerimizin teknolojinin sunduğu yeni olanaklarla dönüşüme uğradığına tanık olmaktayız. Bunu görebilmek için cüzdanlarımızdaki onlarca indirim ve kredi kartına, e-postalarımızı ve cep telefonlarımızın mesaj kutularını dolduran reklamlara, her gün biraz daha sıklıkla karşılaştığımız el izi, parmak izi, retina tarayan sistemlere ya da yalnızca en yakın mesai arkadaşımıza, yani bilgisayar(lar)ımıza bakmamız yeterlidir. Bu araçların tamamı kişisel verileri içermekte ve yeni veri işleme alanları yaratmaktadır. Bunun yanında ilk aşamada dikkatimizi çekmeyen başka bazı araçların da izlenmemize hizmet edebileceğini unutmamalıyız. Bunun en açık örneğini son dönemlerde hızla yaygınlaşan RFID oluşturur. İngilizce bir deyim olan "Radio Frequency Identification"ın kısaltması olarak kullanılan RFID'nin tam Türkçe karşılığı: Radyo Frekanslı Tanımlamadır. Bu aracın kullanımı her geçen gün yaygınlaşmaktadır. Giysilerin etiketlerinin içine ya da kartlara yerleştirilmiş olan bu yongalar şu an belki bizlerin sürekli izlenmesine hizmet etmiyor, ancak bu teknolojinin hızla yaygınlaştığı, geliştiği ve ucuzladığını düşünüldüğünde yakın zamanda bu ve benzeri teknolojiler ile ilgili daha fazla sorunla karşılaşabileceğimiz ortadadır. Bu örnek, izlemenin görünür araçlar yanında, saptamamızın daha zor olduğu araçlarla da yapılabileceğini ortaya koymaktadır.

Bütün bu teknolojilerin bize daha iyi hizmet sunulmasını sağlayan oldukça önemli yararlar sağladığı açıktır. Ancak öte yandan bu teknolojilerin ilk aşamada fark edilemeyen "yan etkileri", başta özel yaşamın gizliliği hakkı olmak üzere temel hak ve özgürlüklerimize ciddi müdahaleler oluşturabilecek niteliktedir. İşte bu noktada, kişisel verilerin korunması, teknolojinin kamu kurum ve kuruluşlarına, özel teşebbüslere ve bizlere sunduğu olanaklarla, temel hak ve özgürlüklerimiz arasında bir denge kurmayı hedeflemektedir.

Kişisel bilgilerin toplanması, kayıt edilmesi, kullanılması, aktarılması ya da en genel ifadesiyle işlenmesi kaçınılmazdır ve pek çok noktada gereklidir. Ancak bu uygulamaların keyfi olması, kişinin sürekli olarak izlenme tehlikesini hissetmesi benzersiz kişiliğini özgürce geliştirmesinde engel oluşturacak ve bireysel özerkliğin yitimi gibi temelde insan onuruna yönelik ciddi bir saldırının oluşmasına neden olacaktır. Özel alana böylesine bir müdahale, kişinin kendisine ilişkin bilgiler ya da bir başka anlatımla kendi özeli ile arasındaki bağı kaybetmesi tehlikesini de beraberinde getirir. Temeldeki önemli sorun da budur.

Sürekli izlenen, yaşamına ilişkin bilgiler kayıt altına alınan, bütün bunların sonucunda adeta şeffaflaşan bireyin kişiliğini serbestçe geliştirebilmesi olanaklı değildir. Bu kişinin toplumsal yaşamda kişiliğini özgürce belirleyememesi, kendinden beklenen davranış tarzına göre hareket etmesi de olasıdır. Bu noktada kişisel verilerin korunması hakkı, bireye kişisel verilerinin hukuka aykırı olarak sınırsız bir şekilde kaydedilmesi, işlenmesi, paylaşılması karşısında temel bir hak vermektedir. Böylelikle bireye verilerinin kullanılması üzerinde karar verme hakkını tanır. Bu tehlikeleri bertaraf etmek ve sözünü ettiğimiz dengeyi sağlayabilmek için kişisel verilerin korumasına ilişkin hukuksal düzenleme-

lerde, bazı temel ilkelerin kabul edildiğini görüyoruz. Kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi, verilerin toplanma amacının meşru, açık ve belirli olması, amacın gerektirdiğinden daha uzun süre tutulmaması, ilgilinin rızasının bulunması, veri güvenliği gibi ilkeler bu kapsamda sayılabilir.

Öğrenme Çıktısı

3 Kişisel verilerin korunmasının önemini açıklayabilme

Araştır 3	İlişkilendir	Anlat/Paylaş
Kişisel verilerin korunmasını hangi değişimler daha önemli hale getirmiştir?	Kişisel verilerin korunması ve haber alma hürriyeti arasında nasıl bir denge gözetilmeli?	Kişisel veriler hakkında aileniz ve arkadaşlarınız bilinçli mi? Bu konuda tecrübe ve bilgilerinizi paylaşarak, meseleyi tartışınız?

KİŞİSEL VERİLERİN KORUNMASI HAKKI

Kişisel verilerin korunması, kendisinden daha köklü bir tarihe sahip başka hak alanları ile yakından ilişkilidir. Bunların başında özel yaşamın gizliliği hakkı gelir. 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. Öte yandan kişisel verilerin ekonomik bir değerinin bulunduğu da tartışmasızdır. Özellikle ticarî işlemler söz konusu olduğunda bu değer daha açık bir şekilde hissedilebilir. Bu anlamda bireylerin, başka çıkarlarının yanında, ekonomik çıkarlarının korunması gerekir. Ancak bu kişisel verilerin üzerindeki hakkın mülkiyet hakkı üzerinden kurulabileceği anlamına gelmez. Gerçekten taşınır ya da taşınmaz mallara uygulanan kuralları elle ya da otomatik olarak işlenen kişisel verilere uygulamak, örneğin seçme hakkını ya da düşünceyi açıklama özgürlüğünü mal haline getirmekten farksızdır. Bir başka anlatımla mülkiyet hakkı ve benzeri yaklaşımlar yalnızca korumada yetersiz kalmaları, bu sistemlerin işlemesinin zor olması ya da iki hak alanı arasında ortak paydaların bulunmaması gibi nedenlerle değil, etik açıdan da yanlıştır. 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 (Miller, 1971:212).

Nitekim günümüzde kişisel verilerin korunmasının temel bir insan hakkı olduğu yönünde şüphe bulunmamaktadır. Mülkiyet hakkı üzerinden temellendirme yönünde tartışmaların olduğu ABD'de bile insan hakları yaklaşımının etkisi hissedilmektedir. Bu kapsamda kişisel verilerin korunması hakkının çoğu zaman özel yaşamın gizliliği hakkına ilişkin hükümler ile hukuksal olarak temellendirildiği görülmektedir. Hatırlatmak gerekir ki 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. Bu genel açıklamalar çerçevesinde şuna da işaret etmek gerekir: 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 (BVerfGE, 65, 1-Volkszählung) kararında bu duruma işaret etmiştir. Bu kararın yarattığı etkinin en önemli nedeni 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.

Belirtmek gerekir ki karara konu olan yasa uyarınca 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 (Şimşek, 2008). 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.

Mahkemenin bu kararındaki gerekçesi veri korumanın önemini ve veri işleme teknolojilerinin temel insan hakları ile ilişkisini anlayabilmemiz için son derece önemlidir. Bu kapsamda işaret edilen ilk husus, anayasal düzenin merkezinde insan onurunun bulunmasıdır. Bilişim teknolojilerinin ortaya çıkardığı tehlikeler karşısında kişiliğin korunması ise özel bir önem kazanmaktadır. Mahkemeye göre kendisine ilişkin bilgilere hangi kapsamda ve kimler tarafından erişildiğini öğrenebilme olanağına sahip olmayan bir kişi, bireysel özerkliğin gereklerini yerine getiremeyebilir. Örneğin, yaşamına ilişkin bir konuda kendi özgür iradesi ile değil, yönetimin beklentilerine göre karar vermek zorunda kalabilir. Bu durum bilişim teknolojisinin ve veri bankalarının geliştiği bir dönemde daha da ciddi bir tehlike olarak karşımıza çıkar.

Nitekim otomatik sistemler ile kişisel verilerin neredeyse sınırsız bir şekilde kaydedilebilmesi, bunlara farklı yerlerden ulaşabilme imkanı, bilgilerin ilişkilendirilerek ayrıntılı kişilik profilinin oluşturulabilme olasılığı bulunmaktadır. Bunun yalnızca olasılık olarak kalması durumunda bile, birey psikolojik baskı hissedebilir ve temel haklarını kullanmaktan kaçınabilir. Bir örnek vermek gerekirse bir gösteri yürüyüşüne katıldığının resmi makamlarca kayıt altına alındığını ve bunun ileriki yaşamında bazı olanaklardan yoksun kalmasına neden olacağını düşünen birey, bu tehlikeyi bertaraf etmek için anayasal hakkını kullanmaktan vazgeçebilir. Mahkemeye göre böylesine bir durum yalnızca bireyin kendi kişiliğini geliştirme hakkını zedelemez. Bunun yanında kamu çıkarlarına da zarar verir. Çünkü özgürlükçü bir demokrasinin işlemesi topluma katılma ve toplum içerisinde işlev görme becerisine bağlıdır. Bu nedenle, kişiliğin serbestçe gelişebilmesi ve demokratik toplum yapısının sürekliliği için devlet tarafından kişisel verilerinin toplanılması, kaydedilmesi, kullanılması ve devredilmesi karşısında bireyin korunması bir gerekliliktir. Sürekli izlenen yaşamına ilişkin bilgiler kayıt altına alınan, bütün bunların sonucunda adeta şeffaflaşan bireyin kişiliğini serbestçe geliştirebilmesi olanaklı değildir. Kısacası verilerin geleceğini belirleme hakkı, birey ile kendisine ilişkin bilgiler arasında-teknolojideki gelişmeler neticesinde-silikleşen bağın yeniden kurulmasını sağlamaktadır.

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. Bu anlamda kişisel verilerin korunmasının özel yaşamın gizliliği hakkının özellik taşıyan bir türü olduğu ve kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olarak algılanmaya başlandığını söyleyebiliriz. Nitekim 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. Nitekim 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".*

Benzer bir durum anayasal düzenlemeler açısından da kendini göstermektedir. Özel yaşamın gizliliği hakkı, hemen hemen bütün devletlerin anayasalarında temel bir hak olarak belirlenmiştir. Ancak kişisel verilerin korunması hakkının bağımsız olarak anayasal temelde korunduğu örnekler de artmaktadır.

Özel yaşamın kapsamı ve bu hak alanının kişisel verilerin korunması ile ilişkisini belirlemek gerekir. Öncelikle 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 (Cavoukian, Tapscott, 1997). Bu güçlüğü aşabilmek için, bireyin çevresi ile ilişkileri iç içe geçmiş alanlara, çemberlere benzetilmiş ve bu şekilde özel yaşamın sınırlarını belirlemeye çalışılmıştır. Bu çemberler ortak özellikleri bakımından 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 (Araslı, 1979).

Kişinin özel yaşamının çevreye açıklık derecesinin yararlanacağı korumanın oranı ve şekliyle ilgili olduğu söylenebilir. 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 (Şimşek, 2008). 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.

Prosser'a göre özel yaşamın gizliliği hakkı dört tür haksız fiile karşı, dört tür çıkarı korumaktadır. Bunlar şu şekilde belirlenebilir (Prosser, 1960):

Tablo 2.1

Haksız Fiiller	Çıkarlar
Kişinin özel yaşamına ilişkin utanç verici durumların kamuya açıklanması	Kişinin şeref ve onuru
Kişinin topluma yanlış tanıtılması	Kişinin şöhreti ve adı
Kişinin adının veya resminin çıkar sağlamak amacıyla kullanılması	Kişinin adından ve resminden doğan maddi çıkarları
Kişinin sükunetinin, yalnızlığının, gizlerinin ve özel yaşamının ihlali	Kişinin manevi bütünlüğü

dikkat

Kişisel verilerin korunmasının özel yaşamın gizliliği hakkının özellik taşıyan bir türü olduğu ve kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olarak algılanmaya başlanmıştır.

Bu noktada özel yaşamın gizliliği hakkının ve kişisel verilerin korunmasının insanın insan olmasından doğan yüksek değeri için neden gerekli olduğu sorusu akla gelir. Belirtilen çeşitli çıkarlar yanında, bu gerekliliğin antropolojik ve psikolojik temelleri olduğu ileri sürülmüştür. Buna göre, antropoloji, biyoloji gibi sosyal bilim alanlarında yapılan çalışmalar, bütün canlılarda özel yaşamın gizliliği gereksinimi bulunduğunu ortaya koymaktadır. Bunun karşılanmadığı durumlarda ise bazı fiziksel ve psikolojik bozuklukların oluşabileceği belirtilmektedir (Westin, 1970). O zaman özel yaşamın gizliliğinin insanın sağlıklı bir fiziksel ve ruhsal yapıya sahip olması için gerekli olduğunu söyleyebiliriz. Ancak bununla da sınırlı kalmamaktadır: birey, sosyal yaşam içerisinde ilişkilerini sürdürebilmek ve demokratik bir düzende siyasal haklarını tam anlamıyla kullanabilmek için de bu hakka gereksinim duyar.

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 (Rachels, 1975). 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 (hatta bazı durumlarda bunların açıklanmasından dolayı iş yaşamında çeşitli çıkarlar da sağlayabileceği düşünülebilir) 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. Bize ve bize ilişkin bilgilere kimlerin ulaşabileceğini denetleyebildiğimiz ölçüde farklı kişilerle çeşitli ilişkiler kurabiliriz. İşte bu, özel yaşamın gizliliğine verdiğimiz önemin temel nedenidir (Rachels, 1975).

Bu tanımlamalar kişisel verilerin korunması hakkına neden gereksinim duyduğumuzu açıklamada da yardımcıdır. Ayrıca özellikle son dönemde güvenlik gerekçesi ile veri işleme teknolojilerinin neredeyse sınırsız bir şekilde kullanılmasını savunanların dile getirdiği *"Saklayacak bir şeyin yoksa korkacak bir şeyin de yoktur."* sloganına da yanıt oluşturur. Unutulmamalıdır ki özel yaşamın gizliliği hakkı ve kişisel verilerin korunması hakkı suçluların bilgilerini gizleyerek onların korunmasına hizmet etmemektedir. Bu iki önemli hak alanı *"insan"*ın yalnızca insan olması dolayısıyla sahip olduğu değerleri korumaya yönelmiştir ve bu şekliyle insanların kendileri hakkındaki bilgilere ilişkin bir denetim sağlar.

Güvenlik elbette insanın çok temel bir gereksinimidir. Ancak burada karar verilmesi gereken asıl soru, bu vazgeçişin ne kadar gerekli olduğudur: Güvenliğin sağlanabilmesi için olağan dışı tedbirlerin alınması bir zorunluluk mudur, yoksa normal koşullarda bireylerin kabul etmeyeceği, ancak yö-

netimdekilerin istediği koşulların yaratılması için bir bahane midir? Bu, yanıtlanması çok da kolay olmayan önemli bir sorudur. Elbette terörle mücadele ve güvenliğin sağlanması devletin başlıca görevleri arasındadır. Ancak bu, belirtilen amaçlarla ölçüsüz önlemlerin alınabileceği anlamına gelmez. Dengeyi sağlamak kolay değildir. Güvenlik gereksinimi karşısında özgürlüklerin korunması hem sanal hem gerçek dünyada çağımızın en önemli sorunlarından biridir.

Bilgi toplumunda koşulsuz özel yaşamın korunması hakkının giderek daha az önem verilen bir değer haline geldiği görülmektedir. Ancak bu özel yaşamın gizliliği hakkının artık önemsiz olduğu anlamına gelmez. Değerler arasında uygun bir denge bulunmalıdır. Bilgi teknolojileri kötüye kullanılabilir ve bu noktada unutulmaması gereken, insanlar hakkında bazı olguların bilinmesinin bunların her türlü amaç için kullanılabileceği anlamına gelmediğidir. Örneğin bir kişinin ciddi bir hastalığı olduğunu bilmek, sigorta şirketlerine risk ve maliyet hesaplamalarını daha doğru bir şekilde yapabilme olanağı verir. Ancak belirtilen bilgiler, bu kişilerin sigorta sözleşmesi yapma haklarının ellerinden alınması gibi bir sonuç doğurmamalıdır. Bunun yanında, yalnızca kötüye kullanılması yönündeki korkudan dolayı, kişisel verilerin işlenmesinden vazgeçmek de akla uygun görünmemektedir.

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

Bu noktada özellikle üzerinde durulması gereken ilk temel hak, düşünceyi açıklama özgürlüğüdür. Düşünceyi açıklama özgürlüğü, *"insanın serbestçe düşünce ve bilgilere ulaşabilmesi, edindiği düşünce ve kanaatlerden dolayı kınanması ve bunları tek başına ya da başkalarıyla birlikte (dernek, toplantı, sendika vb.) çeşitli yollarla (söz, basın, sinema, tiyatro vb.) serbestçe açıklayabilmesi, savunabilmesi, başkalarına aktarabilmesi ve yayabilmesi anlamına gelir"*(Tanör, 1994). Düşünceyi açıklama özgürlüğü, bu kapsamda özgürce yayın yapan kitle iletişim araçları olmadan açık ve aydınlanmış bir toplumdan söz edilemez. Ancak Immanuel Kant'ın da belirttiği gibi, sorumlulukla özgürlüğü birbirine bağlamak gerekir. Bu nedenle düşünceyi açıklama özgürlüğünün belirli sınırları olduğu kabul edilmektedir. Bu sınırlardan biri de kişisel verilerin korunması hakkının da temel dayanaklarından olan kişiliğin geliştirilmesine ilişkin ilkelerdir. Nitekim düşünceyi açıklama özgürlüğü, demokratik bir toplumun eksen özelliklerinden biri olsa da, bu özgürlük, *"Bireylerin öğrenmek istedikleri her şeyi bilme hakkı olduğu anlamında yorumlanamaz."* (Uluşahin, 2007).

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. Ancak bu yayınlarının önemli hukuksal sonuçları da olmaktadır ve özel yaşamın gizliliği hakkının ilk kez ortaya çıktığı zamandan beri tartışılmaktadır. Nitekim Warren ve Brandeis'in, *"yalnız bırakılma hakkı"*nı geliştirdikleri ünlü makalelerini bireyin özel yaşamından beslenen azgın basının insan onuru, bireysel özerklik gibi önemli değerleri yok etmesi korkusundan hareketle kaleme alındığı bilinmektedir (Bloustein, 1964). O halde en azından Amerikan hukuku açısından özel yaşamın gizliliği hakkının koruma altına alınmasında magazin basınının tacizkar hareketlerinin etkisi bulunduğu söylenebilir.

Bir tarafta halkın ilgisini çeken konuları araştıran, değerlendiren, yayınlayan basın kuruluşları, diğer yanda, kişisel bilgilerinin paylaşılmamasını isteyen bireyler arasında adeta gerilim hattını andıran bir çekişme söz konusu olmaktadır. 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 özgürlüğünü 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 gerilim 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 (Cavoukian, Tapscott, 1997).

Ayrıca, kimsenin düşüncelerini açıklamaya zorlanamayacağı kuralı düşünceyi açıklama özgürlüğü kapsamında değerlendirilirken, diğer yandan da kişisel verilerin korunması açısından kısmi bir güvence sağlamaktadır. Bu kural, bireyin gizli kalmasını istediği verileri açıklamaya zorlanamamasına ve özellikle hassas verilerinin kendisinde saklı tutması isteğine destek verir. Her sözü, her türlü üyeliği, her protestosu bir şekilde kayıt altına alındığını düşünen kişi, muhalif görüşlerini açıklamaktan kaçınabilir. Bu noktada belirtilen sorunla da yakından ilgili son derece önemli bir konuya *"anonimlik hakkı"*na kısaca değinmekte yarar vardır.

Hem düşünceyi açıklama özgürlüğü, hem de özel yaşamın gizliliği hakkı ekseninde tartışılan anonimlik genel olarak, bir kişi ya da grubun görüş ve düşüncelerini kimliğini ortaya çıkarmadan açıklaması ve yayması olarak tanımlanabilir. İhbarcılar, muhalifler, utangaç kişiler, görüşlerini açıklamalarının kendilerini olumsuz bir şekilde etkileyeceğini düşünenler, kişisel verilerinin toplanmamasını ve hareketlerinin izlenmesini istemeyenler için anonimlik oldukça yararlıdır (Lee, 2000). Anonimlik hakkı, özellikle İnternet kullanımının yaygınlaşmasıyla güncellik kazanmış ve tartışılmaya başlanmıştır. Özellikle yeni yeni yaygınlaşmaya başladığı dönemde İnternet ortamında kişilerin kimliklerini gizleyebilmelerinin kolaylığı dolayısıyla görüşlerini ortaya koymada daha özgürce hareket edebilecekleri dile getirilmiştir. Binlerce insan, İnternet'te kendi özel yaşamlarına ilişkin yalnızca kim oldukları bilinmediği takdirde söyleyebilecekleri şeyleri açıklamaktadır.

Bu yargı yalnızca kısmen doğrudur. Nitekim anonimliğin temelde iki çeşidi bulunur. Birincisi ilgilinin kimliğinin ortaya çıkarılma olanağının bulunmadığı tam anlamıyla anonimliktir (comple te anonymity). İkincisi ise daha çok takma isimlilik (pseudonymity) olarak adlandırılır. Takma isim kullanıldığında, yine kimse gerçek kimliği bilmez ancak farklı iletişimlerin aynı kişi tarafından yapıldığını bilebilir. Her iki çeşidi de siber uzayda sağlayabilmek zordur çünkü pek çok yapı bizi tanımlamaya olanak sunmaktadır. Bu nedenle siber uzayda yüzeysel bir anonimlik kolaydır, ancak gerçek anlamda bunu gerçekleştirebilmek belki de olanaksızdır (Schneier, 1998).

Oysa anonimlik pek çok temel hak açısından elverişli bir araçtır. Örneğin Dünyanın pek çok yerinde siyasal yakınmalar, yaşamsal bir tehdit altına girmeden, ancak bu şekilde yapılabilmektedir. Öte yandan kişilere ilişkin verilerin anonim olarak tutulmasının kişisel verilerin korunması açısından çok çeşitli yararları bulunduğu söylenebilir. Kayıt tutmak pek çok alanda bir zorunluluk olsa da bu bilgilerin her zaman kişisel veri niteliğinde olmasına gerek yoktur. Özellikle istatistiksel verilerin yeterli olduğu, planlama gibi amaçlarla yapılan işlemlerde bu açıkça görülebilir. Bu durumda anonimlik bir yandan bu işlerin en iyi şekilde yerine getirilmesini sağlamaya yardımcı olurken diğer yandan da bireylerin kişisel verilerinin korunması hakkının zarar görmemesini sağlayacaktır. Ayrıca anonimlik

hakkı, bir yandan kişisel verilerin korunmasına, bir yandan düşünceyi açıklama özgürlüğünün sağlanmasına destek verir yapısı ile iki hak alanı arasında ortak bir payda da oluşturmaktadır.

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 gereklilikler 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. Nitekim 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. Nitekim, verilerin toplanmasında ve işlenmesinde hukuka uygunluk ve dürüstlük kişisel verilerin korunmasına hakim olan temel ilkelerdendir. Ancak gelişen bilişim teknolojileri ile verilerin izlenmesi, toplanması, saklanması maliyetlerinin düşmesi ve kolaylaşması iletişimin içeriğinin dinlenmesi yanında yeni tartışma noktalarının da alevlenmesine neden olmuştur. Gerçekten özel haberleşmenin içeriği yanında, özel iletişime ilişkin çeşitli verilerin tutulması da önemli bir sorun olarak karşımıza çıkmaktadır. 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

Yukarıda kimi zaman çatışan, kimi zaman kesişen yönleriyle bazı temel hak ve özgürlüklerin kişisel verilerin korunması hakkı ile ilişkisini değerlendirdik. Bunların yanında kişisel verilerin korunmasının kısmi güvenceler sağladığı ya da kişisel verilerin korunmasına kısmi güvenceler sağlayan başka temel hak ve özgürlük kategorileri de bulunmaktadır.

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.

Öğrenme Çıktısı

4 Kişisel verilerin korunması hakkının diğer temel hak ve özgürlüklerle ilişkisini açıklayabilme

Araştır 4	İlişkilendir	Anlat/Paylaş
Kişisel verilerin korunması hakkı ile ilişkili olan diğer hakları sayınız.	Kişisel verilerin korunması ile benzer özellikte olan, yani bu hakkı güçlendiren haklar vardır. Bu hakkı kısıtlamayı gerektiren başka bazı toplumsal menfaatler mevcut olabilir mi?	Kişisel verilerin korunması hakkına ilişkin bilgilerinizi çevrenizle paylaşınız.

KİŞİSEL VERİLERİN KORUNMASINDA HÂKİM OLAN TEMEL İLKELER

Ulusal ve uluslararası düzeyde güvenceye tabi olan pek çok temel insan hakkı ile kişisel verilerin korunması arasındaki ilişkiyi böylelikle ortaya koymuş olduk. Şimdi yanıtlanması gereken önemli bir soru bu hakkın etkin bir şekilde tanınmasının nasıl sağlanacağıdır. Bir sonraki ünitede Türkiye' de kişisel verilerin korunması üzerinde durulacaktır. Ancak ondan önce kişisel verilerin korunması için yasal düzeyde benimsenmesi gereken ilkelerin neler olduğunu açıklamak gerekir. Bu Türkiye'deki durumu incelerken bizlere bir ölçüt sunacaktır. Bu ilkeler saptanırken konuya ilişkin uluslararası metinler yanında kişisel verilerin korunması hakkının anavatanı olan Avrupa devletlerinde benimsenen sistem dikkate alınmıştır. Bu nedenle öncelikle kısaca bu kaynakların neler olduğunu açıklamak gerekir.

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 sınırötesi 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 (Bygrave, 2002).

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.

Şimdi bütün bu metinlerde ortak olduğu kabul edilebilecek temel ilkeler üzerinde duralım. Belirtmek gerekir ki bu ilkelerin birbirlerinden kesin çizgilerle ayrılması oldukça zordur. Aşağıda görüleceği gibi, kimi ilkeler diğerlerine kaynaklık eden genel bir nitelik sergilerken, pek çoğu da birbirini tamamlamaktadır. Bu nedenle yapılan açıklamalar değerlendirilirken bu ilkelerin birbirleri ile olan yakın ilişkisi unutulmamalıdır. Konunun anlaşılmasını kolaylaştırmak amacıyla bazı ilkeler belirli başlıklar altında toplanmış ve ayrıca bu ilkelerin uygulamaya geçirilmesinde son derece önemli olan başka bazı hususlara da bu bahis altında değinilmiştir.

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 kendi kendini açıklar niteliktedir. Kolaylıkla anlaşılabileceği gibi bu gereklilik, kişisel verilerin işlenmesinde yasalarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu ifade eder. Dürüstlük kuralına uygun olma ilkesi ile veri işleyenlerin 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. Bu ünite içerisinde daha önce de açıklandığı üzere kişisel verilerin korunması ile amaçlanan veri işlemenin yasaklanması değildir. Aksine veri işlemenin hukuka uygun bir biçimde gerçekleştirilmesi sağlanarak bilişim alanındaki gelişmeler sonucunda birey aleyhine bozulan dengenin yeniden kurulması hedeflenmektedir. Verilerin kaliteli olması bu hedefe hizmet eder. Bir örnek üzerinden açıklamaya çalışalım. İş başvurusu sırasında işverenin başvuruda bulunan kişiye bazı sorular yöneltmesi doğaldır. Bu konuda bir anket doldurmasını ya da kendisine işle ilgili bazı belgeleri teslim etmesini de isteyebilir. Buradaki amaç, kişinin işe uygunluğunun saptanmasıdır. Ancak bu amacı aşarak, işle ilgili olmayan bilgileri işlemesi hukuka aykırılık yaratır.

İlgili 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. Bu ünitenin önceki bölümlerinde açıklandığı gibi bireyin kendisine ilişkin bilgiler ile arasındaki bağın korunması son derece önemlidir. 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 bulara 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 olacağı da açıktır. Bu durum, veri güvenliğinin ekonomik olarak ölçülebilir çıkarları da güvence altına aldığını ortaya koymaktadır.

Bağımsız Organlarca Denetim

Kişisel verilerin korunabilmesi için kabul edilen temel ilkelerden söz etik. 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. Örneğin belirsiz ya da henüz belirlenmemiş bir amaç için kişisel verilerin bir yerde depo edilmesi bu ilkelere aykırılık oluşturacaktır.

Yaşamla İlişkilendir

"BM İnternet Erişimini Temel İnsan Hakkı olarak tanımladı!

Yazar: Ergun Dinçer

Birleşmiş Milletler, 3 Haziran'da yayınladığı bir raporda, internet erişimini "bir insan hakkı" olarak tanımladı ve politikacıların bunu sağlamakla yükümlü olduklarını belirtti. Son dönemde, önce Wikileaks belgeleri, sonra Arap dünyasındaki politik hareketlenmeye Facebook neden oldu söylentileri, pek çok hükümetin internete bakışını olumsuz yönde etkiledi. Bu nedenle olsa gerek, Birleşmiş Milletler bu konuda bir rapor yayınladı. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" başlığını taşıyan rapor, İnternet erişim hakkının bir "insan hakkı" olduğunu tanımlıyor. Raporun yazarı Frank La Rue, web'in diğer insan haklarını da destekleyen bir araç haline geldiğini not ediyor. Raporda ilgili bölüm şu şekilde: *İnternetin benzersiz ve dönüştürücü doğası, sadece bireylere fikri ve ifade özgürlüğünü sağlamakla kalmıyor, yanı sıra toplumun bir bütün olarak gelişmesini sağlayacak, diğer insan haklarını da destekliyor.* İnternet bir dizi insan haklarını destekleyen, gelişmeleri hızlandıran önemli bir araç haline geldi. Bu nedenle internete global erişimi sağlamak bütün devletlerin en önemli önceliği olmalıdır.

Bu nedenle her devlet, internetin, uygun fiyatlarla, geniş bir şekilde var olmasını, kullanımını temin edecek anlamlı ve güçlü bir yasal ortamı geliştirmelidir.

Amerikan Telekom ve Bilgi Teknolojileri Derneği (US National Telecommunications and Information Association – NCIA)'nin FCC ile birlikte, ülkedeki geniş bant durumunu analiz ettiği bildiriliyor. Buna göre, Amerika'da % 5-10 arası Amerikalı internete ulaşamıyor. Yani bu madde sadece 3.dünya ülkelerini değil, gelişmiş ülkeleri de (digital divide) ilgilendiriyor.

Son dönemde Ortadoğu'da meydana gelen politik gelişmeler, İnternetin adalet, eşitlik, insan hakları arayan insanlara, seslerini duyurmak yolunda yardımcı olabildiğini gösteriyor.

Bu arada bazı Kuzey Avrupa Ülkelerinin geçen yıl İnternet erişim hakkını Anayasalarına ilave ettiğini de hatırlatalım. Özellikle yeni Anayasa'dan bahsedildiği bugünlerde, internetin Anayasa'ya bir vatandaşlık hakkı olarak konulmasına dikkat etmemiz lazım".

Rapor için bakınız:

http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Kaynak: *http://www.turk-internet.com/portal/yazigoster.php?yaziid=32795*

Araştırmalarla İlişkilendir

İnternet'in Evrenselliğini, Bütünlüğünü ve Açıklığını Korumak ve Geliştirmek…

İnternet Özgürlüğü İlkelerden Küresel Hukukta Anlaşmaya

Avrupa Konseyi Konferansı, Strazburg, 18-19 Nisan 2011

İnternet'in Evrenselliğini, Bütünlüğünü ve Açıklığını Korumak ve Geliştirmek

1. Avrupa Konseyi üye ülkeleri, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşmeye Taraf devletler (Avrupa İnsan Hakları Sözleşmesi – ETS No.5) herkesin insan hakları ve temel özgürlüklerini sözleşmede tanımlanan çerçevede güven altına almayı üstlenir. Bu hakları ve özgürlükleri koruma ve geliştirmeyi sağlamada sorumlukları ve özel görevleri vardır ve Avrupa İnsan Hakları Mahkemesinden önceki hakları için de sorumluluğu alabilirler.
2. Demokratik sürece katılacak vatandaşlar için ifade özgürlüğü hakkı gereklidir. Bu hak hem çevrimiçi hem de çevrimdışı faaliyetlerde uygulanır ve sınırlara bakılmaz. Bu hakların korunması Avrupa İnsan Hakları Sözleşmesi'nin 10'uncu maddesi uyarınca sağlanmalıdır.
3. İnternet insanların bilgiye ve hizmetlere erişimini, bağlantı ve iletişim kurmasını, bilgiyi ve fikirleri küresel olarak paylaşmasını sağlar. Siyasal katılım ve müzakere ve diğer kamu yararı faaliyetlerine katılması için gerekli temel araçları sağlar.
4. Bireylerin özgürlüğü, İnternet'te bilgiye erişim, bilgiyi oluşturma ve görüşlerini söyleme ve grupların iletişimine izin verme ve fikirlerini paylaşma ehliyeti, İnternet altyapısı ve krtitik kaynaklarla ilgili eylemlere ve enformasyon teknolojisi tasarımına hem de hükümet eylemlerine dayanır.
5. Özellikle, erişim ve İnternet kullanımı, teknik nedenlerden dolayı ağın istikrarlı ve sürekli biçimde işlemesinin bozulması riskleriyle karşı karşıya kalabilir ve İnternet altyapısına müdahale gibi diğer eylemlere karşı savunmasızdır. İnternet'in istikrarı ve esnekliği sorusu aslen sınır ötesi birbirine bağlantılılık ve altyapısına bağlılığıyla ilişkilidir. Bir hükümetin nüfuzundaki bölgede gerçekleşen eylemler kullanıcıların İnternet'teki bilgiye erişim olanağını etkiler.
6. Hatta, İnternet'in çalışması için kritik olan kaynakların yönetimi ve teknik koordinasyonu bağlamında kararlar alınır ve İnternet protokol adresleri kullanıcıların bilgiye erişimi ve kişisel verinin korunmasında doğrudan etkiye sahip olabilir. Bu kaynaklar farklı yetki alanlarına dağılır ve farklı uluslararası özel girişimler tarafından yönetilir.
7. Bu artalanına karşı, hem ifade özgürlüğünün ve İnternet'te bilgiye erişimin korunmasında hem de İnternet'in kamu hizmeti değerinin geliştirilmesi İnternet'in evrenselliğini, açıklığını ve bütünlüğünü nasıl sağlayacağımız hakkındaki büyük endişelerin bir parçasıdır.
8. İnsanlar artan bir şekilde gündelik hayatlarında İnternet'e bel bağlamakta ve vatandaş olarak haklarını temin etmektedirler. İnternet hizmetlerinin erişilebilir, güvenli, güvenilir ve sürekli olması konusunda meşru beklentileri vardır. İnternet, benzer biçimde, ekonominin birçok sektörü ve kamu yönetimi için kritik bir kaynaktır.
9. Toplumun bu beklentilerinin, devletlerin, İnternet'le ilgili politika üretme süreçlerinde genel kamu yararını koruma konusunda dikkatli olmasını gerektirmektedir. Aslında, birçok ülkede, o ülkelerin ulusal politikalarında ya da yasalarında ya da uluslararası platformlardaki forumları da içeren siyasi beyanlarında olsun ya da olmasın kamu hizmeti olarak İnternet'in değeri bilinmektedir.
10. Bir görevin taşıyıcıları olarak temel hakların ve vatandaşlarının özgürlüklerinin korunması ve birincil katılımcıların İnternet'in kritikliğine ilişkin meşru beklentilerine ilişkin, devletlerin ulusal ve uluslararası alanda İnternet'le ilgili kamu politikasında kamu yararını koruma sorumluluğu vardır.

11. Ayrıca, devletlerin birbirlerine karşı, İnternet'in kamu hizmeti değerini koruma ve geliştirmede ellerinden geleni yapacaklarına dair karşılıklı beklentileri vardır. Bu bağlamda, devletlerin İnternet'in evrenselliğini, bütünlüğünü ve ülke sınırlarındaki bilgi ve ifade özgürlüğünün korunması için İnternet'in açıklığını koruma konusunda gerekli tedbirlerin alınması konusunda ortak ve karşılıklı sorumluluklarını kabul etmeleri gerekir.
12. Bu nedenle, Bakanlar Komitesinin üye ülkelere tavsiyeleri:
    - hem ulusal İnternet'le ilgili politikaların geliştirilmesi bağlamında hem de uluslararası toplum içinde bu tür faaliyetlere katıldığı zaman. İnternet yönetişimi ilkelerine ilişkin Bakanlar Kurulu Komitesi Bildirgesinde yer alan ilkeler tarafından yönlendirilmesi,
    - İnternet'in evrenselliğini, bütünlüğünü ve açıklığını, ilkeleri göz önünde tutarak ve bu tavsiyede belirtilen taahhüt uyarınca ve pratikte ve hukukta yansıması olduğundan emin olarak, korumak ve geliştirmek,
    - Ek'teki taahhüdün tüm kamu yetkililerine ve özel girişimlere yayılmasını sağlamak, özellikle İnternet için kritik olan kaynakların yanı sıra sivil toplum örgütlerinin yönetimini sağlamak,
    - Buradaki ilkelerin uygulanmasını desteklemek ve geliştirmekte aktörleri cesaretlendirmek.

(Bölüm'ün yer sınırları nedeniyle Avrupa Konseyi Tavsiye Kararı kapsamında yer alan taahhüt metnine burada yer verilmemiştir.)

Çeviren: Sevda Ünal

Kaynak:https://yenimedya.wordpress.com/2011/06/09/internet%E2%80%99in-evrenselligini-butunlugunu-ve-acikligini-korumak-ve-gelistirmek/

Öğrenme Çıktısı

5 Kişisel verileri korunmasında hakim olan temel ilkelerin neler olduğunu açıklayabilme

Araştır 5

Hassas sayılan veriler hangileridir?

İlişkilendir

Özel hayatın gizliliği ile hassas sayılan veriler arasında nasıl bir ilişki mevcuttur, tartışınız.

Anlat/Paylaş

Şahsımıza ait verilerin başkalarının eline geçmesi hakkında çevrenizde nasıl bir algı yaygın. Hassas verileri de dâhil ederek arkadaşlarınızla tartışınız.

öğrenme çıktıları ve bölüm özeti

1 İnsan hakları ile bilişim teknolojileri arasındaki ilişkiyi açıklayabilme

Bilişim Teknolojileri ve İnsan Hakları

Özellikle yirminci yüzyılın ikinci yarısı farklı bir gelişim dolayısıyla daha insanlık tarihi açısından önemlidir. 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.

Bilişim teknolojilerindeki gelişim İnternet'e erişim hakkı ve kişisel verilerin korunması hakkı başta olmak üzere yeni hak kategorilerinin filizlenmesini ve hızla gelişmesini de sağlamıştır.

2 Kişisel veri ve kişisel verilerin işlenmesini tanımlayabilme

Kişisel Veri ve Kişisel Verilerin İşlenmesi

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. Bu tanımda "her türlü" bilgi ifadesinin kullanılması oldukça geniş bir alanın hedeflendiğinin işaretidir. Burada bilginin türüne ilişkin herhangi bir ayrım yapılmamaktadır. Sayı, yazı, ses ya da görüntüden oluşan bir bilgi bu kapsamda yer alabilir. Ancak bu noktada her türlü bilginin önünde yer alan tanımlamayı unutmamak gerekir. Buna göre 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.

Kişisel verilerin işlenmesi kavramını da açıklamak gerekir. Bir bilgi ya da bilgi kümesi, yani kişisel verilerin, üzerinde gerçekleştirilen her türlü işlem bu kapsamdadır. Konuya ilişkin ulusal ve uluslararası metinlerde bu işlemler sınırlı sayım ile belirlenmemiş, aksine örnekleme yoluna gidilmiştir. Örneğin konuya ilişkin AB Yönergesinde (95/46/AT) "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" işleme olarak tanımlanmıştır.

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.

3 Kişisel verilerin korunmasının önemini açıklayabilme

Kişisel Verilerin Korunmasının Önemi

Kişisel verilerin korunması, bireyleri, kendilerine ilişkin bilgilerin bilişim teknolojileri ya da dosyalama gibi geleneksel yöntemlerle işlenmesinden doğacak zararlardan koruma amacına yönelmiş ve bazı temel ilkelerde somutlaşmış bir dizi önlemi ifade eder. Kişisel verilerin korumasına ilişkin hukuksal düzenlemelerde, bazı temel ilkelerin kabul edildiğini görüyoruz. Kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi, verilerin toplanma amacının meşru, açık ve belirli olması, amacın gerektirdiğinden daha uzun süre tutulmaması, ilgilinin rızasının bulunması, veri güvenliği gibi ilkeler bu kapsamda sayılabilir.

4 Kişisel verilerin korunması hakkının diğer temel hak ve özgürlüklerle ilişkisini açıklayabilme

Kişisel Verilerin Korunması Hakkı

Kişisel verilerin korunması hakkı, çoğunlukla özel yaşamın gizliliği hakkı kapsamına 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. Bu anlamda kişisel verilerin korunmasının özel yaşamın gizliliği hakkının özellik taşıyan bir türü olduğu ve kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olarak algılanmaya başlandığını söyleyebiliriz.

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. Ancak bu yayınlarının önemli hukuksal sonuçları da olmaktadır ve özel yaşamın gizliliği hakkının ilk kez ortaya çıktığı zamandan beri tartışılmaktadır.

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 gereklilikler 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.

öğrenme çıktıları ve bölüm özeti

5 Kişisel verileri korunmasında hakim olan temel ilkelerin neler olduğunu açıklayabilme

Kişisel Verilerin Korunmasında Hakim Olan Temel 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
- İlgilinin otomatik kararların konusu olmama hakkı

1 Aşağıdakilerden hangisi bilişim teknolojilerinin gelişmesinden etkilenen temel insan haklarından biri **değildir?**

A. Düşünceyi açıklama özgürlüğü
B. İnternet'e erişim hakkı
C. Kişisel verilerin korunması
D. Örgütlenme hakkı
E. Yaşam hakkı

2 Aşağıdakilerden hangisi kişisel verinin tanımıdır?

A. Bir kişi için özel olarak hazırlanmış veri demetidir.
B. Bir kişin kendi başına hazırladığı veri demetidir.
C. Belirli ya da belirlenebilir bir kişiye ilişkin her türlü bilgidir.
D. İstatistik amacıyla toplanan anonim bilgidir.
E. Bir tür bilgisayar yazılımıdır.

3 Aşağıdakilerden hangisi kişisel veri **değildir?**

A. T.C. kimlik numarası
B. Bir kişinin sabıka kaydı
C. Bir kişinin akciğer filmi
D. Bir limited şirketin ticaret ünvanı
E. Bir kişinin pasaport numarası

4 Kişisel verilerin işlenmesi kısaca nasıl tanımlanabilir?

A. Kişisel verilerden anlamlı sonuçlar çıkarılmasıdır.
B. Kişisel verilere ilişkin konuların değerlendirilmesidir.
C. Kişisel veriler üzerinde gerçekleştirilen her türlü işlemdir.
D. Kişisel verilerin bilişim sistemlerinden basılı dosyalara aktarılmasıdır.
E. Kişisel verilerin başka bilgiler katılarak zenginleştirilmesidir.

5 Alman Anayasa Mahkemesi, "bilgilerin geleceğini belirleme hakkını" hangi temel ilkelere dayandırarak geliştirmiştir?

A. İnsan onuru ve kişiliğin korunması
B. Düşünceyi açıklama özgürlüğü
C. Özel yaşamın gizliliği hakkı
D. Bilgi edinme hakkı
E. Din ve vicdan özgürlüğü

6 Avrupa İnsan Hakları Mahkemesi kişisel verilerin korunmasına ilişkin kararlarını Avrupa İnsan Hakları Sözleşmesinin aşağıdaki hükümlerinden hangisi çerçevesinde değerlendirir?

A. Yaşam hakkı (Madde 2)
B. Özel yaşamın gizliliği hakkı (Madde 8)
C. İşkence yasağı (Madde 3)
D. Düşünceyi açıklama özgürlüğü (Madde 10)
E. Adil yargılanma hakkı (Madde 6)

7 Aşağıdaki metinlerden hangisinde kişisel verilerin korunması açıkça tanımlanmış ve ayrı bir hak alanı olarak düzenlenmiştir?

A. Avrupa İnsan Hakları Sözleşmesi
B. Alman Temel Yasası
C. Birleşmiş Milletler Evrensel İnsan Hakları Beyannamesi
D. Avrupa Birliği Temel Haklar Şartı
E. Amerika Birleşik Devletleri Anayasası

8 Aşağıdakilerden hangisi düşünceyi açıklama özgürlüğü kapsamında **korunmaz?**

A. Özel yaşamın gizliliği hakkı
B. Serbestçe düşünce ve bilgilere ulaşabilme
C. Düşünce ve kanaatlerden dolayı kınanmama
D. Çeşitli yollarla düşüncelerini savunabilme
E. Düşüncelerini yayabilme

neler öğrendik?

9 Aşağıdakilerden hangisi kişisel verilerin kaliteli olması ilkesinin gereklerinden biri **değildir?**

A. Hukuka ve dürüstlük kurallarına uygun işleme
B. Belirli, açık ve meşru amaçlar için toplanma
C. Doğru ve eğer gerekli ise güncel olarak tutulma
D. Amacın gerektirdiğinden uzun sure tutulmama
E. Yüksek ekonomik değeri olma

10 Kişisel verilerin korunmasıyla ilgili aşağıdaki ifadelerden hangisi **yanlıştır?**

A. Özel nitelikli kişisel veriler (hassas veriler) veri koruma ilkelerinin uygulanmadığı veri kategorilerini nitelemek için kullanılan bir deyimdir.
B. Veri güvenliği kişisel verilerin korunmasından hakim olan temel ilkelerden biridir.
C. Kişisel verilerin korunmasında hakim olan temel ilkeler uyarınca ilgili kişinin otomatik kararların konusu olmama hakkı bulunur.
D. Kişisel verilerin toplanma amaçlarına uygun bir şekilde işlenmesi gerekir.
E. Kişisel verilerin korunması hakkı Avrupa Birliği Temel Haklar Şartı'nda açıkça düzenlenmiştir.

1. E	Yanıtınız yanlış ise "Bilişim Teknolojileri ve İnsan Hakları" konusunu yeniden gözden geçiriniz.
2. C	Yanıtınız yanlış ise "Kişisel Veri ve Kişisel Verilerin İşlenmesi" konusunu yeniden gözden geçiriniz.
3. D	Yanıtınız yanlış ise "Kişisel Veri ve Kişisel Verilerin İşlenmesi" konusunu yeniden gözden geçiriniz.
4. C	Yanıtınız yanlış ise "Kişisel Veri ve Kişisel Verilerin İşlenmesi" konusunu yeniden gözden geçiriniz.
5. A	Yanıtınız yanlış ise "Kişisel Verilerin Korunması Hakkı" konusunu yeniden gözden geçiriniz.
6. B	Yanıtınız yanlış ise "Kişisel Verilerin Korunması Hakkı" konusunu yeniden gözden geçiriniz.
7. D	Yanıtınız yanlış ise "Kişisel Verilerin Korunması Hakkı" konusunu yeniden gözden geçiriniz.
8. A	Yanıtınız yanlış ise "Düşünceyi Açıklama Özgürlüğü" konusunu yeniden gözden geçiriniz.
9. E	Yanıtınız yanlış ise "Kişisel Verilerin Korunmasında Hâkim Olan Temel İlkeler" konusunu yeniden gözden geçiriniz.
10. A	Yanıtınız yanlış ise "Kişisel Verilerin Korunmasında Hâkim Olan Temel İlkeler" konusunu yeniden gözden geçiriniz.

2 Araştır Yanıt Anahtarı

Araştır 1

Kişisel verilerin korunmasına yönelik ilk düzenlemeler Avrupa'da yürürlüğe girmiştir. Burada öncülüğü Almanya almış ve 1970'de Hessen Eyaleti'nin çıkarmış olduğu veri koruma yasasını, 1979 yılında federal düzeydeki Veri Koruma Yasası takip etmiştir. Bunun ardından Avrupa Birliği'ne üye diğer ülkeler de kendi ulusal veri koruma kanunlarını hazırlamışlardır. Ulusal düzeyde her ülkenin verilerin korunması konusunda düzenleme getirmesi, veri güvenliğinin sağlanması açısından faydalı olmuş; ama Avrupa Birliği içerisinde verinin serbest dolaşımı hususunda engelleyici bir durum yaratmaya başlamıştır. Bu durumun önüne geçilebilmesi için 95/46 sayılı AB Direktifi kabul edilmiştir. Bu direktif ile bir yandan verinin Avrupa Birliği içerisinde serbest dolaşımının sağlanması, öte yandan verinin Avrupa Birliği ile eşdeğer koruma sağlamayan ülkelere gönderilmesinin engellenmesi amaçlanmıştır. Zamanla Avrupa Birliği'ne üye 28 ülkenin kendi özel veri koruma kanunlarındaki farklılıkları ortadan kaldırmak ve Direktif'in kabulünden sonra internet kullanım oranlarındaki artışın yarattığı yeni ihtiyaçlara yanıt verebilmek için hem üye devletleri bağlayıcı hem de güncel bir düzenleme yapma gereği doğmuştur (European Commission, 2012). Bu amaçla, "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunmasına, Verilerin Serbest Dolaşımına ve 95/46 sayılı AB Direktifinin Kaldırılmasına İlişkin 2016/679 sayılı Tüzük" kabul edilmiştir.

2 Araştır Yanıt Anahtarı

Araştır 2

İşleme, AB Yönergesinde (95/46/AT) "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" olarak tanımlanmıştır. Türkiye'de konuya ilişkin hukuksal düzenlemeler kapsamında incelenecek olan Veri Koruma Kanun Tasarısı'nda da benzer bir tanımın benimsendiğini belirtmek gerekir. Dikkat çekmek gerekir ki verilerin işlenmesi ile kastedilen yalnızca bu bilgilerin kayıt edilmesi ya da kullanılması değildir. Kişisel verileri değiştirme, silme, yok etme gibi işlemlerin de veri koruma hukuku açısından "işleme" olarak nitelendirilir.

Araştır 3

Bilişim teknolojilerindeki gelişmenin etkisi yadsınamaz. Bu dönemde bir yanda kökeni çok daha eskilere dayanan devletin gözetim isteği, diğer yanda yeni gelişmeler ile bu isteğin eski dönemlerde görülmeyen ölçüde kapsayıcı bir şekilde gerçekleşme olasılığı, bireysel özerkliğe ilişkin kaygıların gelişmesine neden olmuştur. O halde, kişisel verilerin korunması hukukunun ortaya çıkışında temelde üç etkenin bulunduğu söylenebilir: çeşitli örgütlerce kişisel verilere duyulan gereksinim, teknolojideki gelişmeler, gözetim teknolojilerindeki gelişmeler nedeniyle duyulan kaygı.

Araştır 4

Bu hak ile ilgili olan haklar arasında şunları sayabiliriz: Düşünceyi Açıklama Özgürlüğü, Özel Yaşamın Gizliliği, İnsan Onur, Bireysel Özerklik ve Bilgilerin Geleceğini Belirleme Hakkı

Araştır 5

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.

Kaynakça

Araslı, O. (1979). Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi, Ankara: Yayınlanmamış Doçentlik Tezi.

Bygrave, L. (2002). Data Protection Law, Hollanda: Kluwer Law International.

Bloustein, E. (1964). "Privacy as an Aspect of Human Dignity", ABD: New York University Law Review, C.39, S.5, s. 962-1007.

Cavoukian, A., Tapscott, D. (1997). Who Konows, Safeguarding Privacy in a Networked World, ABD.

Kaboğlu, İ. (2002). Özgürlükler Hukuku, Ankara: İmge.

Küzeci, E. (2010), Kişisel Verilerin Korunması, Turhan Yayınevi, Ankara.

Lee, T. (2000). "Privacy, Security and Intellectual Property", (s. 135-164) Understanding the Web, ABD: Iowa State University.

Miller, A. (1971). The Assault on Privacy, ABD: The University of Michigan Press.

Prosser, W.(1960). Privacy, ABD: California Law Review, C. 48,S.3, s.383-423.

Rachels. (1975). Why Privacy Is Important, Philosophy and Public Affairs, C.4, S.4, s.323-333.

Schneier, B. (1998). Secrets and Lies, ABD: Wiley.

Şimşek, O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul:Beta.

Tanör, B. (1994). Türkiye'nin İnsan Hakları Sorunu, İstanbul: BDS Yayınları.

Uluşahin, N. (2007). İnsan Onuru Kavramı Temelinde Mahremiyet, İfade Özgürlüğü ve Medya, Ankara: II.Ulusal Uygulamalı Etik Kongresi Bildiriler Kitabı.

Westin, A. (1970). Privacy and Freedom, ABD.

Bölüm 3

Türkiye'de Kişisel Verilerin Korunması

Öğrenme çıktıları

Türkiye Cumhuriyeti Anayasası

1 Türkiye Cumhuriyeti Anayasası'nda kişisel verilerin korunmasına ilişkin sağlanan güvenceleri açıklayabilme

Avrupa İnsan Hakları Sözleşmesi

2 Avrupa İnsan Hakları Sözleşmesinde kişisel verilerin korunmasına yönelik düzenlemeleri ifade edebilme

Türk Ceza Kanunu

3 Kişisel verilerin hukuka aykırı işlenmesi ile ilişkili suçları tanımlayabilme

Türk Medeni Kanunu

4 Türk Medeni Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeleri açıklayabilme

Türk Borçlar Kanunu

5 Türk Borçlar Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeleri açıklayabilme

Elektronik Haberleşme ve Elektronik Ticaret Kanunları

6 Elektronik ticaret ve elektronik haberleşme sektörlerinde kişisel veriler işlenirken uyulacak temel kuralları açıklayabilme

Anahtar Sözcükler: • Kişisel Verilerin Korunması • Avrupa İnsan Hakları Sözleşmesi • Elektronik Haberleşme • Elektronik Ticaret • Hassas Kişisel Veri

GİRİŞ

Bir önceki bölümde bilişim teknolojileri ile kişisel verilerin korunması hakkı arasındaki ilişki açıklanmıştı. Hatırlatmak gerekirse: konuya ilişkin ilk hukuksal düzenlemeler bilgisayar ve veri tabanlarının devletler tarafından kullanımının yaygınlaşması ile oldu. İlk düzenlemelerden yaklaşık yarım asır sonra ise artık veri işleme teknolojilerinin yaşamın her alanına yayıldığı bir zaman diliminde yaşıyoruz. Bu durum, teknolojinin yarattığı yan etkilerin günümüzde daha ciddi bir tehlike oluşturmasına neden olmaktadır. Nitekim 21. yüzyılda bireylerin bu konudaki kaygılarının arttığı da görülmektedir.

Örneğin 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 (Eurobarometer, 2011). Bu durum mevcut hukuksal düzenlemelerin daha da geliştirilmesi gerekliliğini ortaya koymaktadır. Nitekim bu gereksinimden hareketle hazırlanan Avrupa Birliği Veri Koruma Reform Paketi'nin önümüzdeki yıl yürürlüğe girmesi beklenmektedir.

Dünyada kişisel verilerin korunması alanında belirtilen gelişmeler yaşanırken Türkiye'de ne yazık ki tartışmaların nispeten sınırlı kaldığı söylenebilir. Oysaki Türkiye gerek bireysel, gerek kurumsal, gerekse yönetimsel düzeyde veri işleyen teknolojilerin oldukça yaygın kullanıldığı bir ülkedir. Nitekim Türkiye'de yalnızca cep telefonu abonesi, İnternet ve Facebook kullanıcısı sayılarının incelenmesi bile bireysel düzeyde kullanım yaygınlığına kavrayabilmek için yeterlidir. Bunun yanında bankacılık sektörü, perakende satış, müşteri ilişkileri gibi alanlar başta olmak üzere özel teşebbüslerin tüketici bilgilerini kayıt altına alan sistemleri Batılı devletlerle kıyaslanır bir şekilde kullandıkları görülmektedir. Ayrıca kamu kurumları da yurttaşların bilgilerini toplayan ve kayıt eden sistemleri oldukça gelişkin bir şekilde kullanmaktadır. Bunun en açık örneği T.C. Kimlik Numarasıdır. 2006 yılından itibaren her Türkiye Cumhuriyeti yurttaşının 11 haneli bir kimlik numarasına sahip olması ve bu numaranın her türlü kamu hizmetinde kullanım zorunluluğu bulunmaktadır. Bunun yanında MERNİS, MOBESE, UYAP, POLNET gibi gelişkin veri tabanlarının yaygın kullanımı da dikkat çekicidir.

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. Raporda verilen örneklerden biri seçmen bilgilerine ilişkindir. DDK raporunda ifade edildiği şekliyle "seçmen niteliğine sahip 50 milyonun üzerindeki vatandaşın, adı, soyadı, ana ve baba adı, doğum yılı, doğum yeri, adres bilgisi seçimlere girme yeterliliğini taşıyan onlarca partiyle paylaşılmaktadır. Paylaşılan elektronik ortamdaki verilerin çoğaltılmasını ve başkalarıyla paylaşılmasını engelleyecek hiçbir mekanizma öngörülmemiştir. Bu verileri alan partilerin bu verileri koruma yeterlilikleri ve almaları gereken önlemler konusunda da herhangi bir belirleme yapılmamıştır."(DDK, 2013).

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 (DDK, 2013).

Türkiye'de kişisel veriler "yeterli" düzeyde korunmamaktadır. Bu nedenle kural olarak AB ülkelerinden Türkiye'ye veri gönderilmesi yasaktır. Bu durum Türkiye'nin hem ekonomik alanda hem de adli ve cezai iş birliği alanlarında çeşitli kayıplar yaşamasına neden olmaktadır. Ancak bu, konuya ilişkin Türkiye'de hiçbir bir düzenleme olmadığı anlamına gelmez. Aşağıda açıklanacağı üzere başta Türkiye Cumhuriyeti Anayasası olmak üzere iç hukukumuzda kişisel verilerin korunmasını açıkça

tanıyan bazı düzenlemeler bulunmaktadır. Şimdi bunların değerlendirilmesine geçelim.

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.

Unutulmamalıdır ki maddi ve manevi varlığını geliştirme hakkı kaynağını insan onurunda bulmaktadır (Kaboğlu, 2002). Türk Anayasa Mahkemesi bir kararında göre insan onuru kavramını şu şekilde tanımlamıştır: *"İnsanın ne durumda, hangi şartlar altında bulunursa bulunsun sırf insan oluşunun kazandırdığı değerin tanınmasını ve sayılmasını anlatır. Bu öyle bir davranış çizgisidir ki ondan aşağı düşünce, muamele ona muhatap olan insanı insan olmaktan çıkarır."* (E. 1963/132, K. 1966/29, 28/6/1966). Görüldüğü gibi Anayasa Mahkemesi "insan onuru"nu insan olmanın anlamı ile bütünleşik olarak değerlendirmiştir. Bir önceki bölümde açıklandığı üzere sınırsız veri işleme süreçleri karşısında bireyin korunmasının bu yaklaşımla ilişkisi kolaylıkla saptanabilir. Nitekim insanı insan yapan önemli özelliklerden biri bireysel özerkliğidir.

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. Bu kapsamda ilgili kişinin kişisel verileri üzerinde denetimini sağlayacak temel ilkelerden örnekler verildiği de görülmektedir. Dikkat çekmek gerekir ki hukuksal güvenceye kavuşması gereken ilkeler hükümde sayılanlar ile sınırlı değildir. Hüküm metninden bu kolaylıkla anlaşılabilir.

Kişisel verilerin korunması hakkının anayasada açıkça yer alması olumlu bir gelişme olsa da hükümde bazı eksiklikler bulunduğu dikkatten kaçmamalıdır. Öncelikle 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. Dikkat çeken bir diğer husus, Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinin aksine hükümde kişisel verilerin korunmasında hakim olan ilkelerin uygulamasını denetleyecek bağımsız bir organın kurulmasına yer verilmemiştir. Elbette bu durum bağımsız bir denetim organının kurulması önünde engel değildir. Kanun koyucunun denetim mekanizmasının önemini dikkate alarak bu konuya ilişkin düzenleme yapması gerekir. Nitekim aşağıda incelenecek olan Kişisel Verilerin Korunması Kanun Tasarısı'nda Veri Koruma Kurulu adıyla böylesine bir organa yer verilmiştir. Ancak Anayasada bağımsız bir denetim organının kurulmasının hüküm altına alınmış olması, Tasarının en tartışmalı yönlerinden olan denetleyici organın bağımsızlık vasfını güvence altına alabilirdi.

Bunun yanında Anayasa Mahkemesinin kişisel verilerin korunmasına ilişkin oldukça tartışmalı kararlarının bulunduğunu da belirtmek gerekir. 2000'li yıllara gelinceye kadar Anayasa Mahkemesi konuya ilişkin üç önemli karar vermiştir. Bunlardan ilk ikisi nüfus cüzdanlarında din hanesinin bulunmasına ilişkindir. Anayasa Mahkemesi yaptığı her iki incelemede de aile kütüklerinde ve nüfus cüzdanlarında din hanesinin bulunma zorunluluğunun Anayasaya aykırı olmadığına karar vermiştir. Her ne kadar bu kararlarda ve kararlara ilişkin tartışmalarda din ve vicdan özgürlüğü ekseninde bir değerlendirme yapılsa da aslında bu kararların dolaylı olarak kişisel verilerin korunması hakkı ile ilişkili olduğu da belirtilmelidir. Nitekim kişinin dini inancına ilişkin bilgiler "hassas" veri kategorisinde yer almakta ve işlenmesi kural olarak

yasaklanmaktadır. Nüfus cüzdanında yer alan din hanesine ilişkin olarak bu noktada bir tartışma yürütülebilir. Ayrıca nüfus hizmetlerinin dijital veri bankalarına aktarıldığı günümüzde bu türdeki verilerin istatistiki amaçlarla anonim tutulması yerine, belirli bir kişiyle ilişkili olarak tutulmasının yaratabileceği tehlikelerin daha ciddi olduğuna işaret etmek gerekir.

Anayasa Mahkemesi'nin bir diğer önemli kararı ise Kimlik Bildirme Kanunu'na eklenen bir hükme ilişkindir. İlgili hüküm uyarınca genel kolluk kuvvetlerinin bilgisayarlarında otel motel, yurt, misafirhane gibi konaklama yerlerinde kalan kişilerin kişisel verilerinin toplanması zorunluluğu getirilmektedir. Ancak bu zorunluluk getirirken kolluk kuvvetlerinin uyacakları esaslar yasada belirlenmemiştir. Anayasa Mahkemesinin karardaki değerlendirmesinden kişisel verilerin korunmasını özel yaşamın gizliliği hakkının bir parçası olarak kabul ettiği anlaşılsa da Anayasaya aykırılık iddiasının reddine karar vermesi düşündürücüdür.

Bunun yanında Mahkemenin 2008 yılında verdiği bir karar, kişisel verilerin korunmasının özel yaşamın gizliliği ve düşünce özgürlüğü çerçevesinde gördüğünü açıkça ortaya koymaktadır. Bu karara konu olan Türkiye İstatistik Kanunu'nun ilgili hükümleri uyarınca istatistik amacıyla gerçek kişilerin de dâhil olduğu "istatistikî birimler"den her türlü bilgi istenebilir. Bu isteğin istenilen şekil, süre ve standartlarda ücretsiz olarak karşılanması zorunludur. Bu zorunluluğu yerine getirmeyenler ise idari para cezası yaptırımı ile karşılaşacaklardır. Anayasa Mahkemesi ilgili hükümleri, "kişilerin bilgi toplama, saklama, işleme tekeline sahip idareye ve diğer kişilere karşı korumasız bırakılması ve veri toplamanın sınırlarına yasal düzenlemelerde yer verilmemesi" nedeniyle Anayasaya aykırı bulmuştur (E. 2006/17, K. 2008/86, 20/3/2008). Dikkat çekmek gerekir ki bu kararın konusu Alman Anayasa Mahkemesinin 1983 yılında verdiği ünlü Nüfus Sayımı Kararı ile benzerlik göstermektedir. Mahkemenin 2008 yılında verdiği bu kararın gerekçesinden bir bölüm bu Ünite sonunda okuma metni olarak yer almaktadır.

İptal edilen hükümden kaynaklı boşluğu doldurmak amacıyla kabul edilen yeni düzenlemede ise bazı ufak değişiklikler yapılmış, bu yükümlülüğün "Anayasa'da belirlenen temel haklar ve ödevler çerçevesinde" gerçekleştirileceği belirtilmiştir. Tekrar Anayasa Mahkemesinin önüne giden hüküm, bu kez oy çokluğu ile Anayasa'ya aykırı bulunmamıştır (E.2010/12, K.2011/135,12/10/2011). Anayasa Mahkemesi, konuya ilişkin ikinci kararında idari makamların bireyin temel haklarını ihlal edecek şekilde bilgi talep etmeme yükümlülüğü bulunduğuna, bu yükümlülüğün yerine getirilmemesi durumunda ise "istatistikî birimler"in haklarını yargı makamları önünde arayabileceklerine işaret etmiş ve "bireyin haklarına ölçüsüz bir müdahaleye izin verilmediği" sonucuna ulaşmıştır. Oysa ilk kararda işaret edilen "korumasızlık" ve veri işleme süreçlerine ilişkin belirsizlik hâlen sürmektedir.

Devletin sosyal ve ekonomik hedefler belirleme ve planlama gibi konularda istatistiklere gereksinim duyduğu açıktır. Bu aynı zamanda etkin yönetim için bir zorunluluktur. Ancak Türkiye'de kişisel verilerin korunmasına ilişkin çerçeve bir düzenlemenin bulunmadığı ve Devlet Denetleme Kurulunun konuya ilişkin raporunda da işaret ettiği üzere, bilgi güvenliğine ilişkin yeterli önlemlerin alınmadığı da dikkatten kaçmamalıdır. Öte yandan istatistik çalışmalarına katılmanın bir zorunluluk olarak belirlenmesi temel hak ve özgürlükler açısından tartışmalı bir durum yaratmakta, Alman Anayasa Mahkemesinin de daha önce işaret ettiği üzere, bireyin devlet karşısında nesneleşmesi tehlikesini taşımaktadır.

Anayasa Mahkemesi'nin başta sağlık verilerinin korunması ile ilişkili olmak üzere yakın zamanda verdiği başka bazı kararlar da bulunmaktadır. Örneğin, her türlü sağlık verisinin Sağlık Bakanlığına gönderilmesine ilişkin 663 sayılı Kanun Hükmünde Kararnamenin 47. maddesi-temel hak ve özgürlüklere ilişkin düzenlemelerin yasa ile yapılması zorunluluğu nedeniyle-Anayasa Mahkemesi tarafından iptal edilmiştir (E.: 2011/150, K.: 2013/30, 14/2/2013). Bunun üzerine kanun koyucu bir torba kanun ile aynı hükmü yeniden 663 sayılı Kanun Hükmünde Kararnameye eklemiştir. Bu hüküm ise yeninden Anayasa Mahkemesi önüne götürülmüş ve Anayasa Mahkemesi yürütmenin durdurulmasına karar vermiştir (E.: 2013/114, K.: 2014/22, 6/12/2014). Bu bölüm yayıma hazırlandığı sırada henüz bu kararın gerekçesi Resmî Gazete'de yayımlanmamıştır. Bunun yanında Anayasa Mahkemesi, hastane ve polikliniklerde kimlik doğrulaması amacıyla biyometrik yöntemlerin kullanılmasına ilişkin hükmü değerlendirmiş ancak Anayasa'ya aykırı bulmamıştır (AYMK E.2014/180, K.2015/30, k.t. 19/03/2015).

Öte yandan Anayasa Mahkemesi, 2012 Eylül ayından itibaren bireysel başvuruları da kabul etmeye başlamıştır. Konuya ilişkin uygulamada karşılaşılan sorunlar dolayısıyla yakın zamanda kişisel verilerin korunması hakkına ilişkin bireysel başvuruların artacağı öngörülebilir. Bu noktada ümit edilen, Anayasa Mahkemesinin kişisel verilerin korunması yönünde güçlü bir tutum takınmasıdır.

Kişisel verilerin korumasının anayasal temellerini incelerken dikkate alınması gereken bir diğer hüküm, Anayasa'nın 90. maddesinde yer alır. Anayasa'nın 90. maddesi uyarınca *"Usulüne göre yürürlüğe konulmuş Milletlerarası antlaşmalar kanun hükmündedir"*. Dolayısıyla 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.

Öğrenme Çıktısı

1 Türkiye Cumhuriyeti Anayasası'nda kişisel verilerin korunmasına ilişkin sağlanan güvenceleri açıklayabilme

Araştır 1	İlişkilendir	Anlat/Paylaş
Türkiye Cumhuriyeti Anayasası'nda kişisel verilerin korunmasına ilişkin sağlanan güvenceleri açıklayınız.	Anayasa'da kişisel veriler ile ilgili direkt koruma bir hüküm olmasa da kişisel veriler için koruma mümkün olur mu? Kıyaslayınız.	Kişisel verilerin Anayasa ile korumaya kavuşturulması şart mıdır? Tartışınız.

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 düşünüldüğünde 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".*

Hemen belirtelim: AİHM, özellikle 1980'li yılların ortalarından beri ve gittikçe artan bir yoğunlukta, kişisel verilerin korunmasını, Sözleşme'nin sağladığı güvenceler kapsamında değerlendirmiştir. Nitekim 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 (Tyrer, Birleşik Krallık, 5856/72,28/4/1978). 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 değerlendirilmektedir.

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 değerlendirilmiştir. Bunun yanında Mahkemenin içtihadı uyarınca *"özel yaşam"*, kimlik hakkını ve 8. maddedeki güvencelerin yorumlanmasında oldukça önemli olan, kişilik ve bireysel özerklik ilkeleri dolayısıyla, kişisel gelişim hakkını da kapsamaktadır.

Ancak belirtmek gerekir: AİHM, konuya ilişkin pek çok kararında, m.8/1'in ihlalini 2. fıkra hükümleri uyarınca meşru görmüştür. Buna karşın hangi konuları *"özel yaşama saygı hakkı"* kapsamında değerlendirdiğini saptamak, en az Mahkemenin somut olaylarda ihlale ilişkin verdiği karar kadar önemlidir. Nitekim Mahkemenin Sözleşme'nin 8/1 hükmü kapsamında özel yaşama müdahale olarak değerlendirdiği bir durumun, 8/2 hükmünde yer alan koşullara uygun olarak meşruluk kazanmadığı durumlarda ihlal kararının doğacağı açıktır.

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. Görüldüğü gibi meşru amaçlar oldukça geniş bir şekilde belirlenmiştir. O kadar ki herhangi bir müdahalenin burada belirlenen meşru amaçları karşılayamaması oldukça zordur. Ancak bir müdahalenin Sözleşme'de belirlenen ilkelere uygun olması için meşru bir amaca yönelik olması ve yasa ile öngörülmesi yeterli değildir. Bunların yanında ayrıca ve mutlaka demokratik bir toplum için gerekli ve orantılı olması da gerekir. Bu, kişisel verilerin korunması ile hedeflenen denge yaklaşımı ile de uyumludur.

Öğrenme Çıktısı

2 Avrupa İnsan Hakları Sözleşmesinde kişisel verilerin korunmasına yönelik düzenlemeleri ifade edebilme

Araştır 2	İlişkilendir	Anlat/Paylaş
Anayasa'nın 90. maddesi milletlerarası antlaşmaları nasıl düzenlemektedir?	Anayasa'nın 90. Maddesine göre, uluslararası antlaşmalar ile "temel hak ve hürriyetlere" ilişkin antlaşmaları karşılaştırınız. Bir farklılık varsa, farklılığının nedenini araştırınız.	Temel hak ve hürriyetlere Avrupa İnsan Hakları Sözleşmesi'nde verilen önemi arkadaşlarınızla paylaşınız.

TÜRK CEZA KANUNU

Özellikle son yıllarda kabul edilen yasal düzenlemelerde kişisel verilerin korunmasına yönelik hükümlere yer verildiği görülmektedir. Bunlar içerisinde şüphesiz en dikkat çekici olan, 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 bir yıldan üç 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.

Şuna işaret etmek gerekir: TCK'nin 135. maddesinde yalnızca verilerin işlenmesinin bir türü olan kayıt etmenin 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, iki yıldan dört 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 bir yıldan iki 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.

Belirtmek gerekir ki bu suçların hiç birinin takibi şikayete 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.

Öğrenme Çıktısı

3 Kişisel verilerin hukuka aykırı işlenmesi ile ilişkili suçları tanımlayabilme

Araştır 3	İlişkilendir	Anlat/Paylaş
Kişisel verilerin hukuka aykırı işlenmesi ile ilişkili suçları sayınız?	Kişisel verilerin hukuka aykırı işlenmesi ile ilişkili suçları sayınız?	Ceza Kanununda bu konuya ilişkin düzenlemelerin varlığı sizce ne anlama gelmektedir?

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 değerlendirileceğine 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 değerlendirilmektedir. 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 korumasını 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 düzenlemenin 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.

Öğrenme Çıktısı

4 Türk Medeni Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeleri açıklayabilme

Araştır 4	İlişkilendir	Anlat/Paylaş
Medeni Hukukta, kişisel verilerin korunması ile yakından ilişkili kavram veya haklar mevcut mudur?	Medeni Hukuk neden önemlidir? Medeni Kanun'da kişisel verilerin direkt veya dolaylı korunması sizce farklı bir durum yaratır mı?	Türk Medeni Kanunu'nun sağladığı korumayı çevrenizle paylaşınız.

TÜRK BORÇLAR KANUNU

Yakın tarihte yürürlüğe giren Türk Borçlar Kanunu'nda işçinin kişisel verilerinin korunmasına yönelik bir hüküm yer almaktadır. Yeni 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 kurmada 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 görülmektedir.

Yeni Borçlar Kanunu'nda benimsenen hükmün bu anlamda son derece yerinde olduğu söylenebilir. 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.

Öğrenme Çıktısı

5 Türk Borçlar Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeleri açıklayabilme

Araştır 5	İlişkilendir	Anlat/Paylaş
Türk Borçlar Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeler daha ziyade hangi hukuk dalı ve insan grubu ile ilgilidir?	Belli bir çalışan grubu için tedbir alınmış olmasını nasıl değerlendiriyorsunuz? Bunu kanun koyucu neden yapmış olmalı?	rçlar Kanunu ile tanınan hakkı ve sosyal unsuru çevrenizle paylaşınız.

ELEKTRONİK HABERLEŞME VE ELEKTRONİK TİCARET KANUNLARI

Bu kısımda, elektronik ticaret ve elektronik haberleşme sektörlerinde kişisel veriler işlenirken uyulacak temel kuralların düzenlendiği Elektronik Haberleşme Kanunu ile Elektronik Ticaret Kanunu ele alınacaktır.

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 kısacık 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 (E.2013/22, K.2014/74,9/4/2014).

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 Kanunu'ndaki 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 abonelerin/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.

Nitekim bu 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

Türk hukuk mevzuatında kişisel verilerin korunmasına ilişkin oldukça yeni bir düzenleme de 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu'nda yer almaktadır. Nitekim bu kanun 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)Bu 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 Kanunu'nda bu yükümlülüğe aykırı hareket edenler için bir yaptırım öngörülmemiş olması bir eksiklik olarak değerlendirilebilir. Öte yandan Türk Ceza Kanunu'nun yukarıda açıklanan hükümlerinin bu alan için de geçerli olacağını dikkatten kaçırmamak gerekir.

Kişisel Verilerin Korunması Kanunu

Yukarıda kısaca açıklanan hükümler yanında 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.

Günümüzde teknolojideki hızlı gelişme ve yaygınlaşma dolayısıyla kişisel verilerin korunması, 1981 yılındakinden çok daha önemli bir gereksinimdir. Yüze yakın devlette veri koruma yasası bulunmasının ve mevcut hükümlerin daha da kapsayıcı düzenlemeler ile yenilenmesi çalışmalarının nedeni de budur.

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 ilegeç kalınmış da olsa-ihlallerin asgari ve denetlenebilir bir düzeye indirilmesi için yeni bir fırsat doğmuştur. Kişisel Verilerin Korunması Kanunu 2016 yılında yasalaşmıştır. Bu kanunun 1. maddesine göre Kanunun amacı "Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir". Bu, Anayasa'nın da bir gereğidir.

Kanunun hükümlerini değerlendirirken Avrupa uygulamasını dikkate almak yararlı olacaktır. Bunun bir nedeni, Avrupa'da konuya ilişkin ilk yasanın kabul edildiği 1970 yılından bugüne yasal düzenlemelerin ve içtihatların oldukça gelişmesidir. 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 Kanunu Yedi bölümden oluşmaktadır. Buna göre 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. Kanunun "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 ile kişisel verilerin aktarılması düzenlenmiştir. Bu noktada belirtmek gerekir ki metin olarak düşünülmüştür, ancak pek çok maddesi ile diğer kanunlarda yer alan hükümlerin saklı tutulduğu görülmektedir. Örneğin, Kanun kapsamında kişilerin "ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" özel nitelikli (hassas) kişisel veri olarak kabul edilmiş ve işlenmesi yasaklanmıştır (m.6/1). Maddenin ikinci fıkrasına göre "Özel ni-

telikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır." Maddeye göre; "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."

Hassas kişisel verilerin işlenmesini sağlayan bir başka istisna ise farklı bir açıdan tartışılabilir. Bu istisna uyarınca sivil toplum kuruluşları amaçlarına uygun olarak, faaliyet alanlarıyla sınırlı olmak kaydıyla kendi üyelerine ilişkin verileri işleyebilir. Dernek, vakıf ya da sendika üyeliği hassas veri kategorisinde sayıldığı için bu makul bir istisnadır. Dikkat çekici olan ise bu türdeki verilerin ancak kanunda açıkça öngörülmesi, ilgili kişinin açık rızası ile Kurulun izninin birlikte bulunması hallerinde üçüncü kişilere ve yeterli koruma bulunması koşuluyla yurtdışına aktarılabilmesidir(m. 9/2, b). Diğer hiçbir özel nitelikli veri için böylesine bir koşul belirlenmemiştir. Nitekim kişinin açık rızasının bulunduğu hâllerde, bunun yeterli görülmeyerek bir de Kurulun onayının gerekmesinin nedeni açık değildir. Bu hüküm dolayısıyla bir dernek-ilgililerin açık rızası ile-yönetim kurulunu İnternet sitesinde yayınlayamayacak ya da-yine üyelerinin açık rızası da olsa-Kurulun onayı olmadan benzer faaliyetler gösteren uluslararası bir örgüte üyelerinin adlarını bildiremeyecek midir? Bu güçte bir sınırlamaya neden ihtiyaç duyulduğu madde gerekçesinde de açıklanmamıştır.

Kanunun ikinci bölümünde ayrıca kişisel verilerin üçüncü kişilere ve yurt dışında aktarımına ilişkin hükümler yer almaktadır. Bu hükümleri de bir örnek üzerinden değerlendirilebilir. Nitekim Kanunda 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 yükümlülüğünün 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.

Kanunun 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 şikayet, bu şikayetlerin inceleme esasları, yine Kurul Genel Sekreterliği tarafından tutulacak "Veri Sorumluları Sicilli" hüküm altına alınmıştır. Bu noktada Kişisel Verilerin Korunması Kurulu üzerinde biraz daha ayrıntılı durmak gerekir.

Kanunun 18. maddesi ile "görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak" yerine getireceği belirtilen bir Kişisel Verileri Koruma Kurulu oluşturulması öngörülmektedir. Kanunun 21. maddesine göre:

Kurul, bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz. (2) Kurul, dokuz üyeden oluşur. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanı tarafından seçilir. (3) Kurula üye olabilmek için aşağıdaki şartlar aranır:

a) Kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak.

b) 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 48 inci maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşımak.

c) Herhangi bir siyasi parti üyesi olmamak.

ç) En az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak.

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.

Kurulun görev ve yetkileri şunlardır:

a) Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak.

b) Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak.

c) Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak.

ç) Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek.

d) Veri Sorumluları Sicilinin tutulmasını sağlamak.

e) Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak.

f) Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak.

g) Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.

ğ) Bu Kanunda öngörülen idari yaptırımlara karar vermek.

Öte yandan tasarının yedinci bölümünde yer alan istisnalar, yani bütüncül olarak Kanunun kapsamı dışında kalacak alanlar en çok tartışılan hükümleri arasındadır. Bu noktada ilk dikkat çeken istisna istihbarat gibi bazı etkinliklerin kapsam dışında tutulmasıdır. 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 bu alanda da öncelikle ve mutlaka geçerli olmalıdır.

Konuyu bütüncül olarak düzenleyen Kanunda 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 aracılığıyla gizlilik" (privacy by design, PbD) ya da "varsayılanlar aracılığıyla 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 aracılığıyla 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.

Yaşamla İlişkilendir

AB'den Google'a: İnternette 'unutulma hakkı'na uy

Avrupa Birliği Adalet Divanı, Google İnternet sitesinin kullanıcıların 'unutulma hakkı'nı korumak amacıyla arama sonuçlarında değişikliğe gitmesine hükmetti. Kararda, "ilgisiz" ve "geçersiz" verilere erişim sağlayan İnternet sitesi bağlantılarının talep doğrultusunda silinmesi gerektiği belirtildi. Dava, evinin açık artırmaya çıkarıldığına dair bir ilanın Google arama sonuçlarında çıkmasıyla gizliliğin ihlal edildiğini savunan bir İspanyol kullanıcı tarafından açıldı.

Google ise, verilerin kaldırılmasına zorlanmanın sansür anlamına geldiğini ifade ediyor.

Google sözcüsü yazılı açıklamasında karar için "Arama motorları ve genel olarak tüm İnternet yayımcıları için hayal kırıklığı yaratıyor. Şimdi olası sonuçlarını irdelemeye zaman ayırmalıyız" dedi. Google, verileri kontrol etmediklerini yalnızca İnternette özgürce ulaşılabilen bilgiye bağlantı sunduklarını söylüyor.

"Unutulma hakkı" arama motorlarının, bazı sonuçları düzenleyip kişisel verilerin korunması için Avrupa yönergelerine uyumlu olmasını zorunlu kılıyor. Lüksemburg'daki Adalet Divanı kararında, kullanıcıların "eksik, geçersiz veya geçerliliğini yitiren" bilgilerin kaldırılması yönünde talepte bulunma hakkı olduğunu ifade etti.

Çok sayıda dava var

İspanyol kullanıcı Mario Costeja Gonzalez, Google arama sonuçlarında 16 yıl önce borcunu ödemek için bir gayrimenkulü satışa çıkardığına dair gazete haberlerinin çıkması üzerine mahkemeye başvurmuştu. Gonzalez meselenin çözüldüğünü ve arama sonuçlarında çıkan haberlerin artık kendisiyle ilgili olmadığını söyledi.

İspanya'da benzeri gerekçelerle Google'dan arama sonuçlarından kişisel bilgileri silmesi talebiyle açılan çok sayıda dava bulunuyor. Avrupa Komisyonu 2012 yılında, İnternet kullanıcılarının özel hayatlarıyla ilgili kişisel bilgileri korumak amacıyla "unutulma hakkı" yasası olarak bilinen bir dizi köklü reform talebini onaylamıştı. Yasaya, "aksi yönde meşru bir gerekçeleri olmadığı" sürece tüm İnternet sitelerinin uyması zorunluluğu var.

"Unutulma hakkı", Avrupa Komisyonu'nun 1995 tarihli Veri Koruma Yönergesi dâhilinde değerlendiriliyor.

Kaynak: http://www.bbc.com/turkce/haberler/2014/05/140513_unutulma_hakki_ab 13 Mayıs 2014

Araştırmalarla İlişkilendir

Türkiye Cumhuriyeti Anayasa Mahkemesinin 5429 sayılı Türkiye İstatistik Kanununun istatistiksel birimlerin (haklarından veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların yetkililerinin) kendilerinden istenen veri veya bilgileri vermekle yükümlü olduklarına ilişkin hükümlerin iptaline ilişkin ve E.2006/167, K. 2008/86 künyeli, 20 Mart 2008 tarihli kararından alıntıdır.

"Maddede açıklayıcı bir düzenleme bulunmadığı için, "kişisel veri" veya "isteme bağlı veri" olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin istenebileceği kuşkusuzdur. İstatistiki birimlerin kendilerinden istenen bilgileri belirlenen şekil ve sürede eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmış olmasına karşın, istenilecek veri ve bilgilerin kapsamı ya da sınırlarının ne/neler olacağına, başka bir anlatımla, temel hak ve özgürlüklere müdahale niteliğinde olan veri ve bilgilerin bu zorunluluk kapsamında bulunup bulunmadığına ilişkin herhangi bir düzenlemeye rastlanmamaktadır. Dolayısıyla, istatistiki birimler kendilerinden istenildiği takdirde her türlü bilgiyi temel hak ve özgürlüklerine müdahale niteliğinde olsa bile vermek zorundadırlar. Anayasa'nın 20. maddesinde herkesin özel hayatına ve aile yaşayışına saygı gösterilmesini isteme hakkına sahip olduğu; 25. maddesinde de herkesin düşünce ve kanaat özgürlüğüne sahip olduğu, her ne sebep ve amaçla olursa olsun kimsenin düşünce ve kanaatlerini açıklamaya zorlanamayacağı hüküm altına alınmıştır. 20. madde gerekçesinde, özel hayatın korunmasının her şeyden önce bu hayatın gizliliğinin korunması, resmi makamların özel hayata müdahale edememesi anlamına geldiği belirtilmiştir. AİHM kararlarında da belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi toplamasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur. Anket formlarında yer alan bazı sorular özel yaşamın gizliliği ile düşünce ve kanaatin açıklanması sonucunu doğurabilir. Bir ülkede en güçlü veri tekeli idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir. Anayasa'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmüyle kişiler, bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın sınırlarına yasal düzenlemede yer verilmemiştir. Açıklanan nedenlerle itiraz konusu kuralların Anayasa'nın 20. ve 25. maddelerine aykırı olduğundan iptali gerekir".

Öğrenme Çıktısı

6 Elektronik ticaret ve elektronik haberleşme sektörlerinde kişisel veriler işlenirken uyulacak temel kuralları açıklayabilme

Araştır 6

Ticari elektronik iletiler, hangi şartlar altında gönderilebilir?

İlişkilendir

Ticari elektronik iletiler ile ilgili olarak, tacirler ve tacir olmayanlar arasında farklılık var mıdır?

Anlat/Paylaş

Çevreniz ve siz, ticari elektronik iletiler ile ne sıklıkta muhatap olmaktasınız? Tartışınız.

öğrenme çıktıları ve bölüm özeti

1 Türkiye Cumhuriyeti Anayasası'nda kişisel verilerin korunmasına ilişkin sağlanan güvenceleri açıklayabilme

Türkiye Cumhuriyeti Anayasası

Türkiye gerek bireysel gerek kurumsal gerekse yönetimsel düzeyde veri işleyen teknolojilerin oldukça yaygın kullanıldığı bir ülkedir. Başta Türkiye Cumhuriyeti Anayasası olmak üzere iç hukukumuzda kişisel verilerin korunmasını açıkça tanıyan bazı düzenlemeler bulunmaktadır. 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".

Bu hüküm ile Türkiye'de kişisel verilerin korunması açıkça anayasal bir hak olarak düzenlenmiştir. Hukuksal güvenceye kavuşması gereken ilkeler hükümde sayılanlar ile sınırlı değildir.

2 Avrupa İnsan Hakları Sözleşmesinde kişisel verilerin korunmasına yönelik düzenlemeleri ifade edebilme

Avrupa İnsan Hakları Sözleşmesi

Kişisel verilerin korumasında dikkate alınması gereken bir diğer hüküm, Anayasa'nın 90. maddesinde yer alır. Anayasa'nın 90. maddesi uyarınca "Usulüne göre yürürlüğe konulmuş Milletlerarası antlaşmalar kanun hükmündedir". Dolayısıyla 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, 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 Anayasanın 90. maddesinde de bulmaktadır. Türkiye'de mahkemelerde konuya ilişkin somut olaylarla karşılaşıldığında AİHS'e ve Sözleşme'nin denetim organı olan AİHM'in içtihatlarına da bakmanın önemli bir gereklilik olduğu dikkatten kaçmamalıdır.

3 Kişisel verilerin hukuka aykırı işlenmesi ile ilişkili suçları tanımlayabilme

Türk Ceza Kanunu

ürk Ceza Kanunu'nun (TCK) 135. maddesi uyarınca kişisel verilerin hukuka aykırı olarak kaydedilmesi suçtur. Buna göre kişisel verileri hukuka aykırı olarak kayıt eden kimseye bir yıldan üç 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 136. maddesinde ise kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu düzenlenmiştir.

Konuya ilişkin bir diğer önemli düzenlemenin TCK'nin 138. Maddesinde yer aldığı görülür. 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.

4 Türk Medeni Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeleri açıklayabilme

Türk Medeni Kanunu

ürk Ceza Kanunu'nun (TCK) 135. maddesi uyarınca kişisel verilerin hukuka aykırı olarak kaydedilmesi suçtur. Buna göre kişisel verileri hukuka aykırı olarak kayıt eden kimseye bir yıldan üç 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 136. maddesinde ise kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu düzenlenmiştir.

Konuya ilişkin bir diğer önemli düzenlemenin TCK'nin 138. Maddesinde yer aldığı görülür. 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.

öğrenme çıktıları ve bölüm özeti

5 Türk Borçlar Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeleri açıklayabilme

Elektronik Haberleşme ve Elektronik Ticaret Kanunları

Türk Borçlar Kanunu'nda işçinin kişisel verilerinin korunmasına yönelik bir hüküm yer almaktadır. Yeni 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". 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 görülmektedir. Yeni Borçlar Kanunu'nda benimsenen hükmün bu anlamda son derece yerinde olduğu söylenebilir. 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.

6 Elektronik ticaret ve elektronik haberleşme sektörlerinde kişisel veriler işlenirken uyulacak temel kuralları açıklayabilme

Türk Borçlar Kanunu

Türk hukuk mevzuatında kişisel verilerin korunmasına ilişkin oldukça yeni bir düzenleme de 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu'nda yer almaktadır. Nitekim bu kanun 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." 26 Aralık 2014 tarihinde hâlen gündemde bulunan Kişisel Verilerin Korunması Kanun Tasarısı Meclise sevk edilmiştir. Kişisel Verilerin Korunması Kanun Tasarısı ile ihlallerin asgari ve denetlenebilir bir düzeye indirilmesi için yeni bir fırsat doğmuştur.

1 Aşağıdakilerden hangisi kişisel verilerin işlenmesinin Anayasa ile belirlenmiş meşru temelidir?

A. İlgili kişinin açık rızası
B. Yönetmelikle öngörülmüş olma
C. İlgili kişinin eşinin onay vermesi
D. Veri işleme gereksiniminin ortaya çıkması
E. İdarenin veri işlemenin gerekliliğine karar vermesi

2 Aşağıdakilerden hangisi Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi uyarınca özel yaşama müdahalenin hukuka uygun kabul edilebilmesi için gerçekleşmesi gerekli olan koşullardan biri **değildir?**

A. Veri işleme koşullarının yasa ile belirlenmiş olması
B. Veri işlemenin 8. maddenin 2. fıkrasında belirlenen nedenlerden birine yönelik olması
C. Müdahalenin demokratik bir toplumda gerekli olması
D. Müdahalenin orantılı olması
E. Müdahalenin idarenin bir kararına dayanması

3 Türk Ceza Kanunu'nda göre aşağıdaki eylemlerden hangisi suç olarak **düzenlenmemiştir?**

A. Kişisel verilerin hukuka aykırı olarak kayıt edilmesi
B. Kişisel verilerin hukuka aykırı olarak yok edilmesi
C. Kişisel verilerin hukuka aykırı olarak yayılması
D. Kişisel verilerin hukuka aykırı olarak ele geçirilmesi
E. Kişisel verilerin kanunda belirlenen süre geçmiş olmasına karşın sistem içerisinde yok edilmemesi

4 İşçinin kişisel verilerinin korunması ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. İşveren işçinin kişisel verilerini dilediği gibi işleyebilir.
B. İşveren işçiye ilişkin olarak iş yerinde topladığı verileri dilediği gibi aktarabilir.
C. İşveren işçinin kişisel verilerini hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.
D. İşveren işçinin kişisel verilerini hiç bir durumda işleyemez.
E İşveren işçinin verilerini gerekçe göstermek kaydıyla her durumda işleyebilir.

5 Aşağıdaki yasa metinlerden hangilerinde kişisel verilerin korunmasına yönelik düzenlemelere yer **verilmemiştir?**

A. Türk Ceza Kanunu
B. Türk Borçlar Kanunu
C. Elektronik Ticaret Kanunu
D. Elektronik Haberleşme Kanunu
E. Karayolları Trafik Kanunu

6 Türk Ceza Kanunu'nda kişisel verilerin korunmasına yönelik hükümlerde aşağıdaki yaptırımlardan hangisi öngörülmüştür?

A. Uyarma B. İdari para cezası
C. Para cezası D. Hapis cezası
E. Meslekten men etme

7 Kişisel verilerle ilgili aşağıdaki ifadelerden hangisi **yanlıştır?**

A. Türkiye'de çerçeve nitelikte kapsayıcı bir Kişisel Verilerin Korunması Kanunu yürürlüktedir.
B. Türkiye, kişisel verilerin korunmasına ilişkin 108 sayılı Avrupa Konseyi Sözleşmesini imzalamış ancak onaylanmamıştır.
C. Türkiye Cumhuriyeti Anayasası uyarınca Avrupa İnsan Hakları Sözleşmesi yasa hükmündedir.
D. Türk Medeni Kanunu'nun kişilik haklarının korunmasına ilişkin 24 ve 25. madde hükümleri bazı konularda kişisel verilerin korunmasını destekleyici niteliktedir.
E. Elektronik Ticaret Kanunu uyarınca hizmet sağlayıcı elektronik ticaret işlemleri dolayısıyla elde ettiği kişisel verilerin güvenliğinden sorumludur.

8 Aşağıdakilerden hangisi kişisel verilerin etkin korunmasını destekleyici unsurlardan biri **değildir?**

A. Çerçeve nitelikte bir yasal düzenleme
B. Veri korumayı destekleyici teknik önlemlerin alınması
C. Veri korumaya yönelik bireysel önlemlerin alınması
D. Veri koruma alanında farkındalık arttırıcı çalışmaların yapılması
E. Kişisel verilerin sınırsız şekilde işlenmesini sağlayıcı hukuksal düzenlemelerin yapılması

neler öğrendik?

9 Kişisel Verilerin Korunması Kanunu uyarınca Kişisel Verileri Koruma Kurulu üyeleri nasıl belirlenir?

A. Bakanlar Kurulu, TBMM ve Cumhurbaşkanı tarafından seçilir.
B. Bakanlar Kurulu ve Cumhurbaşkanı tarafından seçilir.
C. Yüksek Öğretim Kurulu (YÖK) seçer.
D. Türkiye Barolar Birliği tarafından seçilir.
E. Halk seçer.

10 Aşağıdakilerden hangisi Türkiye'de kişisel verilerin korunması alanında yaşanan sorunlardan biri **değildir?**

A. Kişisel verilerin güvenliğine ilişkin eksiklikler
B. Çerçeve niteliğinde bir yasal düzenlemenin bulunmaması
C. Konuya ilişkin bazı düzenlemelerde yaptırım sistemindeki eksiklikler
D. Kolay ulaşılabilir bazı anahtar bilgiler aracılığıyla başka bilgilere erişilebilmesi
E. Kişisel verilerin hukuka aykırı ele geçirilmesine karşı herhangi bir yaptırımın öngörülmemesi

1. A	Yanıtınız yanlış ise "Türkiye Cumhuriyeti Anayasası" konusunu yeniden gözden geçiriniz.
2. E	Yanıtınız yanlış ise "Avrupa İnsan Hakları Sözleşmesi" konusunu yeniden gözden geçiriniz.
3. B	Yanıtınız yanlış ise "Türk Ceza Kanunu" konusunu yeniden gözden geçiriniz.
4. C	Yanıtınız yanlış ise "Türk Borçlar Kanunu" konusunu yeniden gözden geçiriniz.
5. E	Yanıtınız yanlış ise "Genel Olarak" konusunu yeniden gözden geçiriniz.
6. D	Yanıtınız yanlış ise "Türk Ceza Kanunu" konusunu yeniden gözden geçiriniz.
7. A	Yanıtınız yanlış ise "Kişisel Verilerin Korunması Kanunu" konusunu yeniden gözden geçiriniz.
8. E	Yanıtınız yanlış ise "Kişisel Verilerin Korunması Kanunu" konusunu yeniden gözden geçiriniz.
9. A	Yanıtınız yanlış ise "Kişisel Verilerin Korunması Kanunu" konusunu yeniden gözden geçiriniz.
10. E	Yanıtınız yanlış ise "Kişisel Verilerin Korunması Kanunu" konusunu yeniden gözden geçiriniz.

3 Araştır Yanıt Anahtarı

Araştır 1

Bu kapsamda ilk olarak kişinin maddi ve manevi varlığını geliştirme hakkı dikkate alınmalıdır. Anayasanın 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 "İnsanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" (m.5) yer alır. Anayasa'nın 20. maddesine 2010 Anayasa değişiklikleri ile eklenmiş olan son fıkra ise 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".

Araştır 2

Anayasa'nın 90. maddesi uyarınca "Usulüne göre yürürlüğe konulmuş Milletlerarası antlaşmalar kanun hükmündedir". Dolayısıyla 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.

Araştır 3

TCK'nin 135. maddesi uyarınca kişisel verilerin hukuka aykırı olarak kaydedilmesi suçtur. 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, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır".

Konuya ilişkin bir diğer önemli düzenlemenin TCK'nin 138. maddesinde yer aldığı görülür.

Araştır 4

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 değerlendirilmektedir. Bu doğrultuda konuya ilişkin hukuksal korumanın ise Türk Medeni Kanunu'nun (MK) 24. ve 25. maddelerinde getirildiği görülmektedir.

3 Araştır Yanıt Anahtarı

Araştır 5

Türk Borçlar Kanunu'nda işçinin kişisel verilerinin korunmasına yönelik bir hüküm yer almaktadır. Bu madde uyarınca "İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir".

Araştır 6

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. Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir.

Kaynakça

Bygrave, L. (2002). Data Protection Law, Hollanda: Kluwer Law International.

Küzeci, E. (2010). Kişisel Verilerin Korunması, Ankara: Turhan.

Küzeci, E. (2015). "1981'den 2015'e Türkiye'de Kişisel Verilerin Korunması Kanun Tasarısının Serüveni", İstanbul: Güncel Hukuk.

Miller, A. (1971). The Assault on Privacy, ABD: The University of Michigan Press.

Şimşek, O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul: Beta.

Bölüm 4

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

Öğrenme çıktıları

Bilişim Alanındaki Suçlara İlişkin Türkiye'de Yaşanan Süreç

1 Bilişim suçlarına ilişkin Türkiye'de yaşanan süreci ifade edebilme

2 Bilişim suçlarına ilişkin temel kavramları açıklayabilme

Bilişim Sistemine Girme

3 Bilişim sistemine girme başlığı altındaki suçları analiz edebilme

Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

4 Sistemi engelleme, bozma, verileri yok etme veya değiştirme başlığı altındaki suçların unsurlarını açıklayabilme

Banka ve Kredi Kartlarının Kötüye Kullanılması

5 Kredi kartlarının kötüye kullanılması başlığı altındaki suçları saptayabilme

Yasak Cihaz ve Programlar Suçu

6 Yasak cihaz ve programlar suçunun unsurlarını tespit edebilme

Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma

7 Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanma koşullarını açıklayabilme

Anahtar Sözcükler: • Bilişim Sistemi • Bilişim Suçları • Bilişim Sistemine Girme • Bilişim Sistemini Engelleme ve Bozma • Verileri Yok Etme veya Değiştirme • Bilişim Sisteminde Arama • Bilişim Sisteminde Kopyalama • Bilişim Sistemine Elkoyma

GİRİŞ

Bilişim alanında son çeyrek asırda yaşanan devrim niteliğindeki gelişmelerle birlikte, insanlık bundan yüzyıl önce yaşayan insanların hayal bile edemeyeceği bir yaşam standartına ve tarzına ulaşmıştır. Öyle ki, çok değil, birkaç yıl önce son teknoloji diye sunulan ve yere göğe sığdırılamayan bilişim alanındaki teknolojik bir ürün, birkaç yıl sonra kimsenin ilgi duymadığı ve ikinci el piyasasında yeri bile olmayan bir ürüne dönüşebilmektedir. Bilgisayarlar artık o kadar ufalmış ve kullanışlı hale getirilmiştir ki, onların girmediği, götürülemediği veya kullanılamadığı yaşam alanı yok denecek kadar azalmıştır.

Bilişim alanındaki gelişmelerin hukuk alanında da önemli birtakım sorunlara neden olduğu aşikardır. Nitekim bu alanda yaşanan gelişmelerle birlikte mülkiyet, fikri hak, haksız fiil, özel hayat gibi çok önemli hukuksal kavramların tanımları ya da anlayış biçimleri değişmiştir. Örneğin bu alanda ortaya konulan özellikle yazılıma ilişkin ürünler üzerindeki haklar bakımından bunların korunması sorunu ortaya çıkmış, bunlara verilen zararlara bağlı olarak haksız fiil algısı yeni bir boyut kazanmış, bilişim sistemlerine kaydedilen bilgilere izinsiz ulaşılması ve bunların kullanılmasına bağlı olarak özel hayat kavramının yeniden ele alınması gerekmiştir.

Konuyu ceza hukuku bakımından ele alırsak, bilişim alanındaki suçlar bu hukuk dalının en güncel ve en hızlı değişim gösteren konularından birini oluşturmaktadır. Nitekim bilişim alanında yaşanan gelişmelere bağlı olarak daha önceden hiç öngörülemeyen ve dolayısıyla suç tipleri arasında düzenlenmeyen bir takım yeni fiiller ortaya çıkabildiği gibi, mevcut suç tipleriyle öngörülen fiillerin yeni yöntemlerle işlenmesi de söz konusu olabilmektedir. Bu bağlamda yasa koyucunun da bu alanda görülen gelişmelere paralel olarak, mevcut düzenlemelerini değiştirmesi ya da yeni düzenlemeler yapması gerekmektedir. Aksi takdirde ortaya çıkabilecek hukuki boşluklar, sosyal hayatta önemli sorunların yaşanmasına neden olabilecektir.

Kıyasın mümkün olduğu hukuk alanlarında, mevcut kuralların kıyasen uygulanması suretiyle, hukuki boşluk nedeniyle ortaya çıkan sorunların çözüme kavuşturulması belli oranda mümkün olabileceğinden, bilişim alanında ortaya çıkan yeni gelişmeler en çok ceza hukuku alanında uygulamacıyı çaresiz bırakmaktadır. Nitekim ülkemizin de içinde yer aldığı Kıta Avrupa'sı ceza hukuku sistemlerinde biçimsel kanunilik ilkesi kabul edilmiştir. Dolayısıyla ceza hukukunda kıyasa başvurulması suretiyle suç sayılmayan bir takım anti-sosyal fiillerin cezalandırılması mümkün değildir. Bu nedenle bilişim alanındaki değişimlerin yakından takip edilerek bunlara yönelik düzenlemelerin bir an önce yapılması zorunluluğu, tüm hukuk alanlarının içerisinde en çok ceza hukuku bakımından ortaya çıkmaktadır.

Bu alanda gelişmeleri takip etme ve buna uygun düzenleme yapmak kanunkoyucu bakımından ne kadar zorsa; aynı zorluk ceza hukuku alanında çalışan hukukçular bakımından da söz konusudur. Nitekim bu alanda 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 elkoyma koruma tedbiri bölüm içerisinde incelenecek konulardandır.

Aşağıda suçlara ilişkin inceleme gerçekleştirilirken suçun unsurları tipik maddi unsur, tipik manevi unsur ve hukuka aykırılık unsuru olmak üzere üç alt başlıkta incelenmiştir. Bu inceleme şekli, suç teorisi anlayışımıza ve konunun daha rahat anlaşılabilmesi amacına yönelik pragmatik gerekçelere dayanmaktadır.

BİLİŞİM ALANINDAKİ SUÇLARA İLİŞKİN TÜRKİYE'DE YAŞANAN SÜREÇ

Bilişim alanında yaşanan gelişmeler karşısında kanunkoyucu, 90'lı yılların başında, bir yandan uygulamada kendini hissettiren ihtiyaçları karşılayabilmek diğer yandan da Türkiye'nin üyesi bulunduğu çeşitli uluslararası kuruluşların tavsiye kararlarına uyum sağlayabilmek amacıyla birtakım düzenlemeler yapmıştır. Bu bağlamda 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 alanındaki 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 (765 sayılı TCK. m.516 ve 491) 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 imkân yoktu. Aynı şekilde dolandırıcılık fiilinin mağdurunun gerçek kişi olması gerektiğinden, makineye karşı gerçekleştirilen hileleri cezalandırmak da mümkün değildi.

Büyük bir eksikliği tamamlamanın yanında bu düzenlemeler, yetersiz olmaları ve birtakım ihtiyaçları karşılamaktan uzak kalmaları sebebiyle, bazı yazarlarca haklı olarak eleştirilmekteydiler. Kanaatimizce, bilişim suçlarına yönelik olarak TCK'da yapılan bu değişiklikler, eksik ve dolayısıyla eleştirilebilir olmalarına rağmen, uygulamadaki büyük bir ihtiyacı karşılamış olmaları nedeniyle, o dönem açısından gayet faydalı düzenlemelerdi.

TCK'da 1991 yılında yapılan söz konusu düzenlemeyi takiben 1995 yılında ise, 4110 sayılı kanunla Fikir ve Sanat Eserleri Kanununda bilgisayar programlarının da eser sayılacağına ilişkin bir değişiklik yapılmış; bilgisayar programlarına karşı gerçekleştirilen birtakım eylemler de yaptırım altına alınmıştır.

Daha sonra ise iletim ağlarının ticarette kullanılmaya başlaması ve e-ticaret kavramının ortaya çıkmasına bağlı olarak sözleşme onaylamalarında işlemleri çabuklaştırmak için dünyada hızla kullanılmaya başlayan elektronik imzaya ilişkin düzenleme de Elektronik İmza Kanunu adı altında 2004 yılında kanunlaşmıştır. Bu kanunda da bilişim alanında bazı suçlar öngörülmüştür.

2004 yılında kanunlaşan ve 2005 yılında yürürlüğe giren 5237 sayılı yeni TCK'da ise bilişim alanında işlenen suçlara, önceki 765 sayılı kanundan daha ayrıntılı düzenlemeler yapılarak yer verilmiştir. Kanunda söz konusu suçlara, özel hükümlerin yer aldığı TCK'nın 2. kitabının topluma karşı suçların düzenlendiği 3. kısmının 10. bölümünde "Bilişim Alanında Suçlar" başlığı altında yer verilmiştir. Görüldüğü üzere 765 sayılı TCK'nın söz konusu suçlara ilişkin olarak 11. babında kullanılan başlık ile 5237 sayılı yeni TCK'nın söz konusu 10. bölümünde kullanılan başlık aynıdır. Kanunkoyucu her iki kanunda da bu suçları, *bilişim alanında suçlar* başlığı altında toplamayı uygun bulmuştur. Bununla birlikte 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

Gerek 765 sayılı önceki TCK'da gerekse 5237 sayılı yeni TCK'da bilişim suçlarına ilişkin düzenleme yapılırken bu suçlara ilişkin temel bazı terimlerin tanımlanmadığı görülmektedir. Bir başka deyişle bilişim sistemi, bilgisayar, veri gibi kavramlar yasal olarak tanımlanmamışlardır. Ancak özellikle suç tiplerine ilişkin düzenlemeler bakımından bu tür teknik terimlerin tanımlanması, tipik düzen-

lemenin anlamını orta koyma bakımından zorunluluk teşkil etmektedir. Bu nedenle aşağıda gerek inceleyeceğimiz suç tipine ilişkin kanuni düzenlemede geçen gerekse anlatımlarımız sırasında bizim sıklıkla kullanacağımız birtakım terimlerin içeriklerini belirlemeyi uygun buluyoruz.

Bilişim Sistemi

765 sayılı eski TCK'da yer alan Bilişim Alanında Suçlara ilişkin düzenlemenin gerekçesinde, "bilişim alanı"ndan kastın "bilgilerin otomatik olarak işleme tabi tutuldukları sisteme ilişkin alan" olduğu ortaya konulmuştur. 5237 sayılı yeni TCK'da ise bilişim sisteminden bahsedilmiş ve 243. maddenin gerekçesinde "Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir." denilerek konuya açıklık getirilmeye çalışılmıştır.

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.

> Bilişim sistemleri, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.

Şifreli Yayınların Konumu

Yayıncılık alanındaki gelişmelerin ülkemizdeki son örneği, şifreli kanal olarak ifade edilen ve yayınları şifrelerle bozarak yayınlayıp, abonelere dağıtılan şifre çözücülerle bu şifreleri kaldırıp yayınların sadece abonelerce izlenmesine olanak tanıyan yayın sistemleri olmuştur. Şifreli yayınların izlenmesinde kullanılan dekoder (şifre çözücü) isimli cihazların, bilgileri otomatik işleme tabi tutmuş sistem kavramı içinde değerlendirilip değerlendirilemeyeceği ise, önceki TCK döneminde ülkemizdeki yoğun tartışma konularından birini oluşturmuştur.

Bu konuda doktrinde ve uygulamada baskın olan görüş, dekoderin bilgisayar kapsamında olmadığı ve bu sebeple de, bu cihaz aracılığı ile gerçekleştirilen eylemlerin eski TCK'nın 11. bab hükümlerine göre değerlendirilemeyeceği yönündeydi. Bizim kanaatimiz de bu yöndedir. 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. Bu tür eylemlere ilişkin bazı ceza davaları 5846 sayılı FSEK.'nin ilgili maddelerinden, bazıları da eski TCK'nın 525/a/2 ve 525/b/2 maddelerinden dolayı takibata uğramaktaydılar. Mahkemeler ise, konunun cezai olmayıp hukuki nitelikte olduğu veya belirtilen suçların unsurlarının oluşmadığı gerekçesiyle açılan ceza davalarını reddetmekteydiler. Buna karşın ceza hukukumuzda bu konuda bir ihtiyaç olduğu açıktı. Bu sebeple kanunkoyucu yeni TCK'da bu konuda açık bir düzenleme öngörmüştür. Ancak düzenleme yukarıda belirttiğimiz nedenlere bağlı olarak bilişim alanında suçlar başlığı altında değil; karşılıksız faydalanma suçuna ilişkin olarak getirilmiştir. Dolayısıyla söz konusu fiilleri işleyen kimselerin, artık karşılıksız faydalanma suçu kapsamında cezai sorumlulukları doğacaktır.

Program ve Veriler

Program ve veriler, bilgisayarın ya da diğer ifadeyle bilişim sisteminin soyut yanını oluşturan, sistemin istenilen şekilde çalışmasına yardımcı olan ve yerine göre kullanıcı ile sistem arasındaki bağlantıyı sağlayan unsurlardır. Program, bir seri bilginin,

sistemin belli bir yönde çalışmasını sağlamak için bir araya gelmiş şeklidir. Veri ise, bilgilerin soyut halde belirli bir formata dönüştürülmüş halidir.

Verinin ne olduğuna ilişkin kanuni bir düzenlemeye, 5651 sayılı *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*'da da rastlanmaktadır. Söz konusu kanunun 2. maddesinin 1. fıkrasının (k) bendinde veri, *bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer* olarak tanımlanmıştır.

dikkat

Program, bir seri bilginin, sistemin belli bir yönde çalışmasını sağlamak için bir araya gelmiş şeklidir. Veri ise, bilgilerin soyut halde belirli bir formata dönüştürülmüş halidir.

İnternet

Her ne kadar kanunda yer alan suça ilişkin düzenlemede geçen kavramlardan birisi olmasa da bilişim sistemleri arasında bağlantı sağlanmasında ve bu tür sistemlere erişimde önemli bir araç olan internet kavramını da birkaç kelimeyle kısaca açıklamayı uygun buluyoruz.

"International" ve "Network" kelimelerinin başlangıç 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. Bu nedenle internete "ağlar arası ağ" da denilmektedir. İnternet sanıldığının aksine veri iletim ağlarının yalnızca bir türü, dolayısıyla sanal alanın yalnızca bir parçasıdır. Ancak dünya üzerinde bugün kullanılan en yaygın ve en geniş ağdır. Sanal alan ise bilişim sistemleri ile bunları birbirine bağlayan her türlü veri işletim ağından oluşan, fiziksel yapısı sayısal verilerden ibaret bir alandır.

Öğrenme Çıktısı

1 Bilişim suçlarına ilişkin Türkiye'de yaşanan süreci ifade edebilme
2 Bilişim suçlarına ilişkin temel kavramları açıklayabilme

Araştır 1	İlişkilendir	Anlat/Paylaş
İnternet nedir?	İnternet ve hukuk konusunda farklı çalışmaların toplandığı bir derleme için bkz. İnternet Hukuku, (Editör: Yener Ünver), Seçkin yayıncılık, Ankara 2013.	Bilişim sistemi terimi neyi ifade etmektedir?

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 bir yıla kadar hapis veya adlî para cezası verilir.* [(1)]
>
> *(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, altı aydan iki 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, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*

Bilindiği üzere bir suçun temel şekline kanunkoyucu tarafından eklenen bazı hususların varlığı halinde suçun daha az veya daha fazla ceza ile müeyyidelendirilmesini hükme bağlamış olabilir. Bu tür hallere nitelikli haller denir. Bununla birlikte kanuni düzenleme aynı madde altında yer alsa bile suçun temel şekline ait unsurları bünyesinde aynı şekilde barındırmıyorsa, bu durumda söz konusu düzenleme nitelikli hal olarak değil; bilakis ayrı bir suç olarak kabul edilmelidir. Bu bağlamda gerek burada incelemekte olduğumuz bilişim sistemine girme suçu başlığı altında gerekse de bu bölümde inceleyeceğimiz diğer suç başlıkları altında kanunkoyucunun aynı maddede birbirinden farklı unsurları bünyesinde barındıran farklı suç tiplerine yer verdiği görülmektedir.

Bu bağlamda TCK m.243'e bakıldığında görüldüğü üzere, madde dört fıkradan oluşmaktadır. Birinci ve dördüncü fıkralarda iki farklı suç tipine yer verilirken, ikinci ve üçüncü fıkralarda ise birinci fıkradaki suçun daha az ve daha fazla cezayı gerektiren nitelikli hallerine yer verilmiştir. Bu hallerden ilkinin gerçekleşmesi halinde faile suçun temel şekline nazaran daha az, ikincisinin gerçekleşmesi halinde ise daha fazla ceza verilmesi öngörülmüştür. Burada inceleme yapılırken gerek 1. fıkrada gerekse 4. fıkrada düzenlenen suçlara ilişkin ortak açıklamalar yapılacak, suç tiplerinin farklılıkları ise bu anlatım sırasında ayrıca vurgulanacaktır. Bununla birlikte tipik maddi unsur incelenirken, fiile ilişkin kısımda her iki suç bakımından ayrı ayrı başlık açılması uygun görülmüştür.

Hukuka aykırı olarak bilişim sistemine girme ve orada kalma fiili, diğer birçok hukuk sisteminde de cezai yaptırıma bağlanarak suç sayılmıştır. Bunlara örnek olarak; Alman Ceza Kanunu m.202a, Fransız Ceza Kanunu m.323 ve Norveç Ceza Kanunu m.145/2 verilebilir. Karşılaştırmalı hukukta söz konusu suçun daha çok verilerin ele geçirilmesi suçuyla birlikte düzenlendiği görülmektedir.

Suçla Korunan Hukuki Değer

Suçun hukuki konusu olarak da ifade edilen 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 menfaati bilişim sisteminin güvenliği olarak kabul etmektedir.

✓ Suçun hukuki konusu olarak da ifade edilen suçla korunan hukuki değer; suçla ihlal edilen hukuki varlık veya menfaattir.

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. Bu bağlamda 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 kanunkoyucu sadece sisteme girmeyi değil; izinli girse bile izin ortadan kalktıktan sonra izinsiz olarak orada kalmaya devam etmesini de cezai yaptırıma tabi tutmuştur.

Suçun maddi unsurunun gerçekleşmesi bakımından sisteme doğrudan doğruya girilebileceği gibi, örneğin internet gibi bir vasıtayı kullanmak suretiyle de girilebilir. 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.

Kanunkoyucu, 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 değerlendirilmelidir. 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.

Kanunkoyucu söz konusu suça ilişkin daha az veya daha fazla cezayı gerektiren nitelikli hallere de yer vermiştir. Bu bağlamda bilişim sistemine girme suçunun, bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir (TCK m.243/2). Görüldüğü üzere kanunkoyucu belirli bir ücret karşılığı yararlanılabilen bir hizmet veren bilişim sistemlerine girme halinde failin temel tip için kabul edilen ceza

ile cezalandırılmasını uygun görmemiştir. Örnek vermek gerekirse; 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 altı aydan iki yıla kadar hapis cezasıyla cezalandırılması öngörülmüştür (TCK m.243/3). Daha fazla cezayı gerektiren nitelikli halin varlığı için, verilerin yok olması veya değişmesi failin kastı kapsamında olmamalıdır. Aksi takdirde, yani bu hallerin kasten gerçekleştirilmesi halinde, ayrıca TCK m.244/2'de düzenlenen suç vücut bulacaktır. Burada düzenlenen nitelikli hal, netice sebebiyle ağırlaşmış bir suç tipi olarak karşımıza çıkmaktadır. Dolayısıyla netice sebebiyle ağırlaşmış suçlara ilişkin kurallar, bu suç tipi açısından da geçerlidir. Bu bağlamda örneğin bir başkasının şifreleme yöntemiyle korunan bilgisayarına izinsiz olarak giren kimsenin, şifrenin çözülmesi için gerçekleştirdiği işlemlere bağlı olarak, kastı dışında, bilgisayardaki verilerden bir kısmının bozulması ya da kaybolması söz konusu olursa, fail, bilişim sistemine girme suçunun daha fazla cezayı gerektiren nitelikli halinden sorumlu olacaktır.

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 kanunkoyucu 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.

Bununla birlikte belirtmek gerekir ki, suç sırf hareket suçudur (şekli suçtur). Veri naklinin izlenmesi yeterlidir. Suçun oluşması için izlemeye bağlı olarak dış dünyada ayrıca bir neticenin, değişikliğin meydana gelmesi gerekmez.

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.

Bilişim sistemine girme başlığı altında düzenlenen suçlar bakımından hukuka uygunluk nedenlerine ilişkin özellik arzeden bir durum söz konusu değildir. Bu bağlamda genel ilkeler bu suç tipleri bakımından da geçerlidir. Örneğin, 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 durum bakımından 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. Nitekim sanal ortamda bir sayfa oluşturup hiçbir şifreleme yapmaksızın bunun içeriğine hiç kimse tarafından erişilmemesini istemek, sokağa bir ilan asıp bunu kimsenin okumamasını talep etmek gibidir. Söz konusu kimse zaten bu verileri şifrelemeksizin internet ortamına koymakla, aleniyetini sağlamış ve kamunun bilgisine/hizmetine sunmuş olmaktadır. Bu nedenle bu tür erişimler söz konusu suçu oluşturmaz.

Buna kaşın sadece belirli kimselerin içeriğini görmesini sağlamaya yönelik olarak bir internet sayfası oluşturulur ve bu sayfaya fail tarafından şifre kırılmak suretiyle erişim sağlanırsa; bu suçun oluştuğunun kabulü gerekir. Nitekim söz konusu internet sayfası, bir bilişim sistemine bağlı olarak sanal ortamda bulunmakta ve şifreleme yöntemiyle buna sadece belirli kimselerin ulaşması temin edilmeye çalışılmaktadır.

Kusurluluk

Kusurluluk ve kusurluluğu ortadan kaldıran hallere ilişkin söz konusu suçlar bakımından özellik arzeden bir durum söz konusu değildir. Bu bağlamda zorunluluk hali veya karşı konulamayacak bir cebir veya ağır bir tehdit altında buradaki fiilleri gerçekleştirenler bakımından kınanabilirlik söz konusu olmayacağından cezai sorumluluk doğmayacaktır.

Suçun Özel Görünüş Biçimleri

Suçun görünüş biçimlerinden, yukarıda verilen suçun başka hangi hallerde işlendiği anlaşılmaktadır. Teşebbüs seviyesinde kalıp kalmadığı, bir içtima halinin olup olmadığı hep bu konuyla ilgilidir.

Teşebbüs

Teşebbüs kişinin işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamamasıdır. Bu bağlamda bilişim sistemine girme ve veri nakillerini izleme suçları teşebbüse müsaittirler. Sisteme girmeye çalışmak bir teşebbüs halidir. Aynı şekilde veri aktarımını izlemeye yönelik icra hareketlerini gerçekleştirip bunun başarılamaması yine teşebbüs sorumluluğunu doğurur. Ancak bu hallerde teşebbüsten cezai sorumluluğun söz konusu olabilmesi bakımından da genel ilkeler geçerlidir. Dolayısıyla mutlak elverişsiz davranışlarla veya mutlak elverişsiz vasıtalarla sisteme girilmeye ya da veri naklinin izlenmeye çalışılması işlenemez suça vücut verecek; bu da cezai sorumluluk doğurmayacaktır.

Bir örnekle konuyu somutlaştırmak gerekirse; internet kullanıcısı bir kimse, ücret karşılığı verilecek şifre ile girilen ve son derece güvenli kodlanmış bir sisteme hukuka aykırı olarak girmek ister. Bunun için ücret ödemediği ve dolayısıyla şifresi olmadığı halde, internet adresinin giriş sayfasında yer alan şifre kutusuna rasgele birtakım rakamlar yazar, ancak sisteme giriş konusunda başarılı olamaz. Bu durumda failin sisteme girme suçuna teşebbüsten sorumluluğu söz konusu olmaz kanaatindeyiz. Çünkü rasgele rakamlarla son derece güvenli kodlanmış bir sisteme girmek son derece düşük bir olasılıktır. Her ne kadar sisteme girişin olasılık dahilinde olduğu düşünülebilirse de bu olasılığın gerçekleşme ihtimali göz ardı edilebilecek kadar çok küçüktür. Bu bağlamda burada sisteme girmeye çalışan kimsenin davranışları mutlak elverişsizlik kapsamında değerlendirilecek ve suça teşebbüs söz konusu olmayacaktır.

Bununla birlikte şifre kırma konusunda uzman bir kimse, aynı sisteme girme konusunda gayret gösterse ve kıl payı sisteme girmeyi başaramasa, bu durumda failin davranışları fiili gerçekleştirmek bakımından elverişli olduğundan, suça teşebbüsün varlığı kabul edilecektir.

İştirak

Tek kişi tarafından işlenebilen bir suçun, birden fazla kimse tarafından bir iş birliği içerisinde işlenmesine iştirak denir. İştirake ilişkin genel kurallar söz konusu suçlar bakımından özel bir önem arzetmeksizin geçerlidir. Fiilleri doğrudan doğruya birlikte gerçekleştirenler, daha doğru bir ifade ile fiil üzerinde birlikte hakimiyet kuranlar fail olarak, fiil üzerinde doğrudan hakimiyet kurmaksızın faile yardımda bulunanla ise yardım eden olarak sorumlu tutulacaklardır. Bu bağlamda bir bilişim sistemine girmek ya da sisteme girmeksizin sistem içindeki veri akışını takip etmek isteyen kimse, kendisinin bilişim sistemleri hakkında yeterli bilgisi olmadığından, bu konuda uzman bir arkadaşını, bu eylemleri gerçekleştirmesi konusunda ikna ederse azmettiren olarak cezai sorumluluğa sahip olacaktır. Buna karşın sisteme giren ya da veri naklini doğrudan izleyen uzman kimse ise fail olarak suçu gerçekleştirmiş sayılacaktır.

Bununla birlikte internet 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. Örneğin tek suç işleme kararının icrası kapsamında aynı kimseye ait değişik bilişim sistemlerine veya aynı kimseye ait tek bir bilişim sisteminin değişik parçalarına giren veya orada kalan kimse bakımından zincirleme suça ilişkin düzenlemeler uygulama alanı bulacaktır.

Ayrıca tek davranışla hem bilişim sistemine girme suçu hem de başka bir suçun vücut bulması halinde fikri içtimaya ilişkin hükümlerin uygulanması söz konusu olacaktır. Örneğin bir arkadaşının gizlice kişisel bilgisayarına girip onun bilgisayarda tuttuğu günlüğünü okuyan veya özel resimlerine bakan kimse bakımından tek bir davranışla, birden fazla hükmün ihlal edilmesi söz konusu olacaktır. Çünkü sisteme girilmesi ve içeriğin incelenmesi davranışın tekliği kapsamında değerlendirilmelidir kanaatindeyiz. Fail sisteme girmekle söz konusu verilerin içeriğine neredeyse eş zamanlı olarak ulaşmaktadır. 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. Örneğin bilişim sistemini kullanmak vasıtasıyla gerçekleştirilecek dolandırıcılığın söz konusu olduğu hallerde, fail tek suçtan mı yoksa iki suçtan ayrı ayrı mı ceza alacaktır. Bu konuda TCK'nın 42. maddesindeki düzenlemeyi göz önünde bulundurmak gerekir kanaatindeyiz. TCK m.42'ye göre; "*biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz.*" Bu düzenlemenin mefhumu muhalifinden çıkan sonuç ise, bir suç diğer bir suçun unsuru veya ağırlaştırıcı nedeni olmadıkça her birinden ayrı ayrı ceza verileceği şeklindedir. Yani sisteme girme suçun unsuru veya zorunlu davranışı değilse, fail hem bilişim sistemine girmeden hem de amaç suçtan ayrıca cezalandırılacaktır.

Ceza

Bilişim sistemine girme suçunun temel şeklinin gerçekleştirilmesi halinde faile seçenekli bir yaptırım öngörülmüştür. Bu bağlamda fail bir 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 altı aydan iki 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 *bir yıldan üç yıla kadar hapis cezası* öngörülmüştür. Bu suç bakımından daha fazla ya da daha az cezayı gerektiren nitelikli hallere kanunda yer verilmemiştir. Bu bağlamda ikinci ve üçüncü fıkrada yer alan nitelikli hallere ilişkin düzenlemeler sadece birinci fıkradaki bilişim sistemine izinsiz girme suçu bakımından geçerlidir.

TCK'ya göre, tüzel kişiler hakkında ceza yaptırımı uygulanamaz (TCK m.20/2). Bununla birlikte, TCK m.60/4'ün göndermesi ve m.246'daki "bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur." düzenlemesi birlikte ele alındığında, burada anlatılan suçlar bağlamında tüzel kişiler hakkında güvenlik tedbirinin uygulanabileceği sonucuna ulaşılmaktadır.

Öğrenme Çıktısı

3 Bilişim sistemine girme başlığı altındaki suçları analiz edebilme

Araştır 2	İlişkilendir	Anlat/Paylaş
Bilişim sistemine girme başlıklı TCK m.243'de kaç suç tipi düzenleme altına alınmıştır?	TCK m.243/1 kapsamında bilişim sistemine girme suçu hakkında daha ayrıntılı açıklmalar için bkz. Hakan Karakehya, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", Türkiye Barolar Birliği Dergisi, S.81, Mart-Nisan 2009	Bilişim sistemine girme suçu ile korunan hukuki menfaat nedir?

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME

TCK'nın 244. maddesinde *sistemi engelleme, bozma, verileri yok etme veya değiştirme*ye 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:

> ***Madde 244-*** *(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 beşbin güne kadar adlî para cezasına hükmolunur.*

Suçla Korunan Hukuki Değer

TCK m.244/1 ve 2'de hükme bağlanan suçlar ile bilişim sisteminin soyut unsurları koruma altına alınmıştır. Dolayısıyla bu suçlar ile korunan hukuki menfaat bilişim sisteminin işlerliğini sağlayan yazılımlardır. Bununla birlikte ilk iki fıkradaki fiillerin işlenmesi suretiyle haksız yarar sağlanmasını yaptırıma tabi kılan m.244/4'deki suç ise gerek 1. ve 2. fıkrada hükme bağlanan suçlarla korunan hukuki menfaati gerekse de bireylerin malvarlığını koruma altına almaktadır. Dolayısıyla 4. fıkradaki suç ile korunan hukuki menfaat bilişim sisteminin işleyişini sağlayan soyut varlıklar ve bireylerin malvarlığı değerleridir. Doktrinde söz konusu suçların, bilişim sistemlerine özgü, özel mala zarar verme suçları olduğu ifade edilmektedir. Ancak kanaatimizce burada sadece malvarlığı değerleri değil; onunla birlikte aynı zamanda sistemin güvenliği de koruma altına alınmıştır. Bu nedenle suçun özel bir mala zarar verme türü olduğunu söylemek eksik olacaktır.

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 (Bkz. TCK m.60).

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 suçun 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. Bu bağlamda örneğin somut olayda haksız kazancın konusunu oluşturan varlık para ise suçun konusunu bu para oluşturacaktır.

Fiil:

Bilişim Sisteminin İşleyişini Engelleme veya Bozma 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 kapsamında sistemi engelleme ve bozma seçimlik hareketlerdendir. Bunlardan sadece birisinin gerçekleştirilmesi suçun tekemmülü bakımından yeterlidir. Sistem üzerinde hem engelleme hem de bozma hareketleri gerçekleştirilirse, bu durumda bunların seçimlik hareketler olmaları dolayısıyla failin tek bir suçtan sorumluluğu doğacaktır. Engellemek, bir şeyin yapılmasını ya da gerçekleşmesini önlemek; bozmak ise bir şeyi kendisinden beklenen işi yapamayacak duruma getirmektir. Bu bağlamda sistemin veri işlemesinin önüne geçilmesi ya da sistemin işleyişinin bir süre de olsa kesintiye uğratılması söz konusu suçu oluşturacaktır. Bu bağlamda sistem üzerindeki oynamalar sonucu sistemin çalışması yavaşlamışsa, sistem hızını kaybetmişse de bu suçun oluştuğunu kabul etmek gerekir. Nitekim sistem çalışsa bile artık kendisinden beklenen performansı söz konusu müdahale nedeniyle gerçekleştiremiyordur.

Ayrıca belirtmek gerekir ki, buradaki suçun bilişim sisteminin soyut yapısına, yazılımına müdahale ile gerçekleştirilmesi gerekir. Aksi takdirde sisteminin somut yapısına, donanımına zarar verilerek işleyişi engellenirse bu madde kapsamında değil; mala zarar vermeye ilişkin hükümler kapsamında cezai sorumluluk doğacaktır.

Düzenlemenin üçüncü fıkrasında gerek birinci gerekse de ikinci fıkrada düzenlenen suçlar bakımında ortak bir nitelikli hale yer verilmiştir. Bu bağlamda bahsedilen fiillerin, *bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi* cezayı arttıran bir neden olarak kabul edilmiştir. Böyle bir arttırıma yer verilmesinin temel nedeni, gerçekleştirilecek eylemler nedeniyle bu kurum ve kuruluşların hizmetlerinin aksamasının, toplumdaki diğer bireyler bakımından da zararlı sonuçlar ortaya çıkartabilecek olmasıdır. Örneğin UYAP ya da MERNİS gibi kamu kurumlarının kullanımında olan sistemler üzerinde söz konusu fiillerin gerçekleştirilmesi bu ağırlaştırıcı sebebin varlığına vücut verecektir. Kamu kurum ve kuruluşu ifadesinden, devletin yasama yürütme ve yargı faaliyetlerinin yapıldığı, mahalli idareleri ve KİT'leri kapsayacak şekilde geniş bir devlet aygıtının içerisindeki kurum ve kuruluşlar anlaşılmalıdır. Düzenlemede geçen "banka" ifadesi, 5411 s. Bankalar Kanunu'nun 3. maddesi kapsamında değerlendirilmelidir. Kredi kurumları ise, TCK'nın 158/1/j maddesinin gerekçesinde, banka olmamasına karşın kanunen borç vermeye yetkili kurumlar olarak ifade edilmiştir. Bağlayıcı olmamakla birlikte söz konusu kavramın içeriğini tespitte gerekçe metninin de yol gösterici olduğu kanaatini taşımaktayız.

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. Örneğin bilişim sistemindeki bir veriye müdahale edilerek onun kullanılmaz hale getirilmesi ikinci fıkra kapsamında sorumluluk doğuracaktır. Bozma sisteme sokulan virüs vb. programlarla söz konusu olabileceği gibi, veriyi bozmaya yönelik fiziksel müdahale ile de olabilir. Verinin kısmen tahrip edilmesi de bozma kapsamında değerlendirilmelidir. Bununla birlikte verinin tümden silinmesi ve böylelikle verinin ortadan kaldırılması şeklinde de ikinci fıkra kapsamındaki fiillerin gerçekleştirilmesi mümkündür. Bir verinin yerine başka veri konulması ise verinin değiştirilmesi kapsamında yine bu suça vücut verecektir. Veriyi bozmadan, değiştirmeden veya silmeden, sadece ona erişilmesi imkânını ortadan kaldırmak da bu suçu oluşturacaktır. Sistemde olmayan verinin dışarıdan sisteme yerleştirilmesi ya da sistemde var olan verilerin dışarıya aktarılması da bahis konusu suçun işlenmiş olması sonucunu doğuran eylemlerdendir (Yaşar, Gökcan ve Artuç, 2014:7311).

Suç seçimlik hareketli bir suçtur. Bu bağlamda kanunda 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. Nitekim seçimlik hareketli suçlarda, cezai sorumluluğun ortaya çıkması için hareketlerden birisinin yapılması yeterlidir; ancak bunlardan birden fazlası yapılırsa işlenen suç yine tek suç olmaya devam eder.

TCK m.244/3'de gerek 1. fıkradaki gerekse de 2. fıkradaki incelediğimiz suç bakımından ortak nitelikli hale yer verilmiştir. Yukarıda birinci fıkradaki suça ilişkin açıklamaları yaparken bu nitelikli hale ilişkin tespitlerde de bulunulduğumuz için burada tekrardan kaçınmak adına aynı hususlardan bahsetmemeyi uygun buluyoruz. Bu bağlamda bu suç bakımından söz konusu olan nitelikli hale ilişkin açıklamalar için yukarıdaki metne gönderme yapmakla yetinmekteyiz.

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 sorumluluğunun 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. Dolayısıyla m.244/4'deki suçun bir bileşik suç düzenlemesi olduğunu söylemek yanlış olmayacaktır. Nitekim birinci ve ikinci fıkradaki suçlar bu suçun unsurunu oluşturmaktadırlar (Bkz. TCK m.42).

TCK m.244/4 kapsamında sağlanması gereken çıkarın mutlaka maddi olmasına gerek yoktur. Örneğin kişi sisteme girip bazı verileri değiştirerek ücretli izlenen bazı tv kanallarını ücretsiz izleme imkânı elde etmişse, söz konusu fıkra kapsamında sorumlu olacaktır. Ayrıca belirtmek gerekir ki, haksız çıkarın failin kendisine veya başkasına sağlamış olmasının önemi yoktur. Önemli olan, kimin için olduğundan bağımsız olarak çıkarın sağlanmasıdır. Bunun dışında söz konusu çıkar sağlamanın başka bir suçu oluşturmuyor olması da gerekir. Eğer öyleyse, eylem hırsızlık, dolandırıcılık, zimmet gibi başkaca suçları oluşturuyorsa, fail örneklendirdiğimiz diğer suça ilişkin düzenlemeye göre sorumlu olacaktır. Eylemin oluşturduğu diğer suçun dördüncü fıkra kapsamında öngörülen cezadan daha ağır cezayı içermesi gerekliliğine madde metninde yer verilmemiş olsa da madde gerekçesinde bu husus ifade edilmiştir. Yargıtay Ceza Genel Kurulu, yerinde olarak, kişinin internet bankacılığı şifresini kırarak hesaptaki parayı başka hesaba aktarma eyleminin m.244/4'teki suçu değil; bilakis 142/2/e kap-

samında bilişim yoluyla hırsızlık oluşturduğunu kabul etmiştir (Yaşar, Gökcan ve Artuç, 2014:7315).

Tipik Manevi Unsur

TCK m.244'de düzenlenen söz konusu suçlar kasten işlenebilen suçlardır. Kanunda taksirli şekillerine açıkça yer verilmediği için, bu suçların taksirle işlenmesi mümkün değildir. Kast bakımından ise genel kast yeterlidir. Nitekim suçun oluşumu bakımından özel kast, bir başka deyişle failin belirli bir saikle (motivasyonla) hareket etmesi zorunluluğu aranmamıştır. Bununla birlikte suçların olası kastla da işlenmesi söz konusu olabilir. Örneğin sisteme girip belirli eylemler gerçekleştirince, her ne kadar bunu amaçlamasa da muhtemelen bazı verilerin bozulacağını öngören fail, bu riski kabullenerek sadece kendini arkadaşlarına ispatlamak amacıyla bu tür davranışları gerçekleştirir ve bazı verilerin bozulmasına neden olursa, bu suça ilişkin olası kast sorumluluğu doğacaktır. _

Hukuka Aykırılık

TCK m.244'te tanımlanan suçlar bakımından hakkın icrası, ilgilinin rızası ve görevin ifası hukuka uygunluk sebeplerin ortaya çıkması söz konusu olabilecektir. Bu bağlamda başkasına ait bilişim sistemine, bu kimsenin rızasıyla girip verileri nakleden, silen veya bozan kişi bu eylemlerini ilgilinin rızası üzerine gerçekleştirdiğinden hukuka aykırılık ortadan kalkacaktır. Yine CMK m.134'e göre yetkili merciin kararı ile sisteme girip arama, kopyalama ve elkoyma işlemlerini gerçekleştiren kolluk görevlisi bakımından görevin ifasına dayalı hukuka uygunluk nedeni oluşacaktır.

Kusurluluk

Kusurluluk ve kusurluluğu ortadan kaldıran hallere ilişkin söz konusu suçlar bakımından özellik arzeden bir durum söz konusu değildir. Bu bağlamda zorunluluk hali veya karşı konulamayacak bir cebir veya ağır bir tehdit altında buradaki fiilleri gerçekleştirenler bakımından kınanabilirlik söz konusu olmayacağından cezai sorumluluk doğmayacaktır.

Suçun Özel Beliriş Biçimleri

Suçun özel beliriş biçimlerinden, yukarıda verilen suçun başka hangi hallerde işlendiği anlaşılmaktadır. Teşebbüs seviyesinde kalıp kalmadığı, bir içtima halinin olup olmadığı hep bu konuyla ilgilidir.

Teşebbüs

TCK m.244'te düzenlenen suçlara teşebbüs mümkündür. Bu bağlamda örneğin bilişim sistemine girip verileri bozmaya yönelik icra hareketlerine başladıktan sonra, verileri bozmayı başaramadan yakalan kimse, ikinci fıkra kapsamında suça teşebbüsten sorumlu olacaktır. Yine sistemin işleyişini engellemeye çalışırken ama engelleyemeden yakalanan kimse bakımından da birinci fıkra kapsamında teşebbüsten cezai sorumluluk ortaya çıkacaktır.

Yukarıda da açıklandığı üzere; TCK m.244/1 ve 2'deki suçlar, TCK m.244/4'deki suçun unsurunu oluşturmaktadır. Dolayısıyla m.244/4'deki suç bir bileşik suç düzenlemesidir. Bu bağlamda Haksız bir çıkar sağlamak amacıyla bilişim sisteminin işleyişi bozulur ama haksız çıkar elde edilemezse, TCK m.244/1'deki suçu işlemekten değil; bilakis TCK m.244/4'deki haksız çıkar sağlama suçuna teşebbüsten cezai sorumluluk doğacaktır.

İştirak

İştirake ilişkin olarak bu suçlar bakımından özellik arzeden 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 düzenlemesi olması dolayısıyla, haksız bir çıkar sağlamak amacıyla bilişim sisteminin işleyişi bozulur ve çıkar sağlanırsa; fail TCK m.244/1'deki suçu işlemekten dolayı cezalandırılmaz. Nitekim bu suç 4. fıkradaki suçun unsuru olduğu için sadece TCK m.244/4'deki haksız çıkar sağlama suçundan cezai sorumluluk doğacaktır.

Yine TCK m.244/4'deki suç, açık düzenleme gereği, ancak çıkar sağlamanın başka bir suçu oluştur-

maması halinde uygulama alanı bulabilecektir. Bu bağlamda bilişim sistemindeki verileri değiştirmek suretiyle dolandırıcılık yapan kimse, bu eylemi nitelikli dolandırıcılık suçunu oluşturacağından TCK m.158 hükmü gereğince cezalandırılır. Bu durumda TCK m.244/4'deki suç uygulama alanı bulmaz. Nitekim belirtilen şekilde haksız çıkar sağlama başka bir suçu (nitelikli dolandırıcılığı) oluşturmaktadır.

Ceza

Birinci fıkra kapsamında suç işleyen fail için bir yıldan beş yıla kadar hapis cezası öngörülmüştür. Eğer failin fiili ikinci fıkra kapsamındaysa bu durumda faile altı aydan üç yıla kadar hapis cezası verilmesi hükme bağlanmıştır. Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde ise verilecek cezanın yarı oranında arttırılması söz konusu olacaktır. Son olarak suçun dördüncü fıkra kapsamında gerçekleştirilmesi halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacağı düzenlenmiştir. Bu son fıkraya giren halde kanunkoyucu fail bakımından hem hapis hem de adli para cezası uygulanmasını tercih etmiştir. Bununla birlikte söz konusu suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler varsa, bunlar hakkında da tüzel kişilere özgü güvenlik tedbirlerine hükmolunur (TCK m.246; m.60).

Öğrenme Çıktısı

4 Sistemi engelleme, bozma, verileri yok etme veya değiştirme başlığı altındaki suçların unsurlarını açıklayabilme

Araştır 3	İlişkilendir	Anlat/Paylaş
TCK m.244'de düzenlenen suçların tipik manevi unsuru nedir?	TCK m.244 kapsamında düzenlenen fiillerle ilgili olarak bkz. Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara 2014	TCK m.244/4'deki hükme bağlanan suçun bir bileşik suç düzenlemesi olduğu söylenebilir mi?

BANKA VE KREDİ KARTLARININ KÖTÜYE KULLANILMASI

Gerek banka kartları gerekse kredi kartları son dönemde gündelik hayatta giderek daha fazla yer tutmaya başlamıştır. Birçok insan artık yanında para taşımamakta, doğrudan veya internet üzerinden yaptığı alış-verişlerde çoğunluk banka kartı veya kredi kartı kullanmayı tercih etmektedir. Banka kartları sayesinde banka şubesine gitmeden insanlar kolaylıkla para çekebilmekte, bu durum da gündelik hayatı son derece kolaylaştırmaktadır. Banka ve kredi kartlarının alış-verişlerde kullanımı, harcama ve satışların kayıt altında tutulmasını kolaylaştırmaktadır. Böylelikle söz konusu kartlarının kullanımı vergilendirmeyi etkili kıldığı için, bu şekilde alış-veriş yapılması iktidarlar tarafından da desteklenmektedir. Ancak bu kartların kullanımının yaygınlaşması kartlara duyulan güvenin oluşturulması ve devamlılığının sağlanmasıyla mümkün olabilmektedir. Toplum içerisinde yaygınlaşmasına bağlı olarak bu kartların kötüye kullanılmasını özel düzenlemeye tabi tutarak bu tür suçlulukla etkin şekilde mücadele etmeyi ve böylelikle kartlara olan güvenin devamlılığını teminat altına almayı amaçlayan kanunkoyucu da 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 beşbin 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 beşbin 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.

TCK m.244/4'deki hükme bağlanan suçun bir bileşik suç düzenlemesi olduğu söylenebilir mi?

Gerekçede ifade edildiği üzere, *banka kartı, bankanın kurduğu sisteme hukuka uygun olarak girmeyi sağlamaktadır. Bu kart, saptanan ve kart sahibince bilinen bir numara marifetiyle, banka görevlisinin yardımı olmadan, kart sahibinin kendi hesabından para çekmesini sağlamaktadır. Kredi kartları ise, banka ile kendisine kart verilen kişi arasında yapılmış bir sözleşme gereğince, kişinin bankanın belirli koşullarla sağladığı kredi olanağını kullanmasını sağlayan araçtır. İşte bu kartların kötüye kullanılmaları, söz konusu maddede suç olarak tanımlanmıştır.*

Görüldüğü üzere TCK m.245'te banka ve kredi kartlarının kötüye kullanılması başlığı altında üç farklı suç tipine yer verilmiştir. TCK m.245/1'de başkasına ait banka veya kredi kartını kullanmak suretiyle yarar sağlama; TCK m.245/2'de sahte banka veya kredi kartı üretme, satma, satın alma ve kabul etme; TCK m.245/3'te ise sahte banka veya kredi kartı kullanarak yarar sağlama suçları hükme bağlanmıştır. Doktrindeki yaygın görüş ve uygulamadaki durum bu şekilde olmakla birlikte; bazı yazarlar söz konusu fıkraların suçun temel şekli ve nitelikli hallerini düzenleme altına aldığı düşüncesindedirler. (Baş, 2015 :140).

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. Yargıtay da banka kart numarası ele geçirilerek internet ortamında işlem yapılması ve yarar elde edilmesi halinde, bu suçun değil, bilişim yoluyla hırsızlık suçunun oluşacağına hükmetmiştir.

Bununla birlikte ele geçirilen kredi veya banka kartının sahibinin rızası dışında kullanılması gerekir ki, suç oluşsun. Sahibin rızasıyla kartın kullanılması halinde söz konusu suçun varlığından bahsedilemeyecektir.

Ayrıca kartın kullanılması suretiyle yarar sağlanması da birinci fıkra kapsamında suçun oluşması için zorunlu hususlardandır. Yarar failin kendisine sağlanabileceği gibi, üçüncü bir kişiye de sağlanabilir. Kanaatimizce burada sağlanan yararın ekonomik bir yarar olması gerekir. Nitekim suç tipiyle, güvenilirliği teminat altına alınmaya çalışılan banka ve kredi kartları ekonomik araçlardır. Bu nedenle bunların kötüye kullanılmasıyla elde edilecek yararın ekonomik olması gerektiği kanaatindeyiz.

Sahte Banka veya Kredi kartı Üretmek, Satmak, Devretmek, Satın Almak veya Kabul Etmek Suçu Bakımından (TCK m.245/2)

TCK m.245/2'de sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suç olarak düzenlenmiştir. Söz konusu düzenleme ile banka ve kredi kartlarında sahtecilik cezai yaptırıma bağlanmıştır. Bu kapsamda suçun, banka veya kredi kartını sahte olarak üretmek, sahte üretilmiş kartı satmak, devretmek, satın almak veya kabul etmek şeklinde gerçekleştirilmesi mümkündür. Bu seçimlik hareketlerden sadece birinin yapılması ikinci fıkra kapsamında cezai sorumluluğun doğması için yeterlidir. Ancak sayılanlardan birden fazlası gerçekleştirilirse de fiil tek suç olmaya devam eder. Örneğin kartı sahte olarak üreten aynı zamanda satarsa fiil yine tek suç oluşturur.

İkinci fıkra kapsamında cezai sorumluluğun doğması bakımından sahte kartın kullanılması suretiyle bir yarar elde edilmesine gerek yoktur. Bu bağlamda sadece sahte kartı bu özelliğini bilerek kabul eden kimse bile ikinci fıkra kapsamında cezai sorumluluğa sahip olacaktır.

Yine bu kapsamda cezai sorumluluğun oluşması için, banka veya kredi kartının başkasına ait bir hesapla ilişkilendirilmesi gereklidir. Böyle bir ilişkilendirilme olmadan söz konusu kartın kullanılması imkânı olmayacak ve dolayısıyla suç oluşmayacaktır.

Sahte Banka veya Kredi kartı Kullanarak Yarar Sağlama Suçu Bakımından (TCK m245/3)

TCK m.245/3'te sahte banka veya kredi kartı kullanarak yarar sağlama suçu hükme bağlanmıştır. Bu bağlamda sahte oluşturulan bir banka ve kredi kartının kullanılması suretiyle failin kendisine veya üçüncü bir kimseye yarar sağlaması cezai yaptırıma tabi tutulmuştur. Üçüncü fıkraya göre cezai sorumluluk doğması bakımından ilk şart, sahte bir kart oluşturulmuş veya gerçek bir kart üzerinde sahtecilik yapılmış olmasıdır. Başkasına ait sahte olmayan bir kart kullanılarak yarar sağlanırsa birinci fıkra kapsamındaki suç oluşacakken, sahte bir kartı kullanarak yararın sağlanması üçüncü fıkra kapsamında suça vücut verecektir.

Üçüncü fıkra kapsamında sahte bir kartın ele geçmesi yetmez. Bu durumda ikinci fıkra kapsamında sorumluluk doğar. Ancak ele geçirilen sahte kartın kullanılması halinde üçüncü fıkraya göre sorumluluk

oluşacaktır. Bu kapsamda sağlanacak yararın ekonomik bir yarar olması gerekir. Nitekim bahsi geçen kartlar ekonomik kullanıma hizmet eden araçlardır. Dolayısıyla sahte kartı kullanılarak otomattan para çekilmesi bu yararın ve suçun oluşmasına yetecektir. Ancak kişi kimliğini ispatlamada bu sahte kartı kullanırsa, üçüncü fıkra kapsamında sorumluluk doğmaz.

Ayrıca belirtmek gerekir ki, üçüncü fıkra kapsamında sorumluluğun doğabilmesi için eylemin daha ağır bir suçu oluşturmaması gerekir. Eğer böyle bir durum varsa, üçüncü fıkra kapsamında değil, daha ağır ceza gerektiren suçtan sorumluluk oluşacaktır. Bu husus ilgili düzenlemede açıkça ifade edilmiştir.

Yaşamla İlişkilendir

Bu kez de temassız kredi kartları dolandırıcıların hedefinde

11.09.2017 Pazartesi

Toplu taşıma araçları gibi kalabalık yerlerde yanınıza yaklaşan bu kişiler, rakamı önceden girdiği 50 TL'den küçük tutarları, pos cihazını size yaklaştırarak temassız özellik sayesinde çekebiliyor.

Teknoloji tüm insanlığın olduğu gibi hırsızların da işini kolaylaştırıyor. Dolandırıcıların son yöntemi cebimizdeki temassız kredi kartlarını hedef alıyor. Bankalararası Kart Merkezi (BKM) verilerine göre, adedi 13,6 milyonu aşan temassız kartlarımızdan çok basit bir yöntemle ancak bilgimiz dışında para çekiliyor.

Kalabalıkta sizi buluyor

Yeni Şafak'ın haberine göre; gelişen teknoloji sayesinde okuyucusu olan tüm noktalarda 50 TL'ye kadar olan işlemler, şifreye gerek kalmadan temassız kartlar ile gerçekleştiriliyor. Bu özellik sayesinde bozuk para aramadan ve para üstü beklemeden kartımızı cihaza gösterip kolayca ödeme yapabiliyoruz.

İşte bunu fırsat bilen sahtekârlar, gün içinde kalabalık yerlerde şansını deniyor. Usulca yaklaşan dolandırıcılar, cihazı size doğru tutarak önceden makineye yazdığı 28 lira gibi rakamı temassız özellik sayesinde kartınızdan çekiyor. Mesela Metrobüs'te ayakta gidiyorsunuz, bu kişilerin yanınızda durması ve elindeki cihazı yaklaştırması yeterli. İlgili teknolojinin en önemli özelliği, işlemin saniyeler içinde gerçekleşmesi yani cihaz kredi kartınızı okuduğu an ödeme tamamlanıyor. Otobüste, alışveriş merkezinde, parkta kısacası her yerde hedeftesiniz. Rakam küçük olduğu için bankalardan uyarı mesajı gelmiyor.

Yaklaşıp ücreti anında çekiyor

Rakamlar ufak olduğu için kart ekstremiz geldiğinde çoğumuz fark etmiyor veya umursamıyoruz. Bu şekilde günde yüzlerce hatta binlerce kişinin kartından işlem yapıldığı tahmin ediliyor. BKM'ye göre 2016'da kartlarla yapılan 4,2 milyar adet ödemenin yüzde 63'ü, 50 TL ve altındaki tutarlardan oluştu.

Sorunun şu andaki tek çözümü ise vatandaşın dikkati. Ay sonundaki ekstreleri kontrol etmek ve harcamaları not etmek de önemli. Şüpheli işlemin bankaya bildirilmesi yanında savcılık ve Emniyet Genel Müdürlüğü bünyesindeki Bilişim Suçları Daire Başkanlığı'na başvuru yapılabilir.

"Uyanık olunması gerekir"

Tüketici Hakları Derneği Başkanı Turhan Çakar, teknoloji sayesinde dolandırıcılığın bu gibi sahalara uzandığını belirterek şunları söyledi:

"Tüketiciler, çok dikkatli olmalı. Vatandaşın bir anlık dikkatsizliğinden yararlanan bu kişilere karşı uyanık olunması, firma bilgilerinin ve harcamalarımızın iyi takip edilmesi gerekir. Gerekirse bu tip kartları kullanmayın, hatta ciddi şüpheleriniz varsa doğrudan banka şubesinden işlem yapın."

İsme özel çıkarılan pos cihazları

Akıllara bu cihazları nasıl buldukları sorusu da gelebilir. Uzmanlar, adeta peynir ekmek gibi pos cihazı dağıtılmasına ve denetimlerin yetersizliğine dikkat çekiyor. Örneğin, ülkemizde bir kişinin ismine pos cihazı çıkarılabiliyor. Kredi kartı ekstremizde bazen firma adı değil ad soyad ve alışveriş tutarını görüyoruz. Yani kişi belli bir şirket adına değil, kendi ismiyle pos cihazını kullanıyor. Haliyle buradaki alışverişi hatırlamıyor dikkat dahi etmiyoruz.

Kuryeler zan altında

Ayrıca, eve teslimat yapan restoran zincirlerinin elemanları da zan altında diyebiliriz. Pos cihazı bulunan, kötü niyetli her türlü esnaf veya çalışanı bu yola başvurabilir. Mahallenizdeki pideci de olabilir köşedeki bakkalın çırağı da. Bazı sahtekarların pos cihazını kullanmak için kurye olarak çalışmaya başladığı iddia ediliyor. Öte yandan, hemen herkesin eline bu tür bir makine alıp sokağa çıkabileceğini hatırlatalım.

Kaynak: https://www.cnnturk.com/ekonomi/bu-kez-de-temassiz-kredi-kartlari-dolandiricilarin-hedefinde?page=1

Tipik Manevi Unsur

TCK m.245'te düzenlenen suçlar kasten işlenebilen bir suçlardır. Kanunda suçların taksirli haline yer verilmediğinden bahsi geçen eylemlerin taksirle yapılması suça vücut vermeyecektir.

Hukuka Aykırılık

Söz konusu suçlar bakımından hukuka uygunluk nedenleri koşulları oluştuğu ölçüde uygulama alanı bulacaktır. Bu bağlamda önem arzeden ayrıksı bir durum bulunmamaktadır. Bununla birlikte ayrıca vurgulamak gerekir ki; TCK m.245/1'de ilgilinin rızası tipik düzenlemede açıkça zikredildiğinden, ilgilinin rızasının varlığı durumunda artık hukuka uygunluk sebebi; bilakis tipikliği kaldıran bir 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 kınanabilirliği ortadan kalkacağından, cezai sorumluluğu doğmayacaktır.

Şahsi Cezasızlık Sebepleri

Kanunkoyucu TCK m.245/1'deki suç bakımından bazı şahsi cezasızlık sebeplerine yer vermiştir. Bu bağlamda söz konusu cezasızlık sebepleri sadece fiilin birinci fıkra kapsamında kalması halinde geçerlidir. Eğer gerçekleştirilen fiil diğer fıkralar kapsamındaysa, 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

Kanunkoyucu, yine birinci fıkra kapsamına giren fiillerle ilgili olarak etkin pişmanlık halini de kabul etmiştir. Buna göre; söz konusu fiiller bakımından malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanacaktır. Birinci fıkra kapsamı dışında kalan fiillerle ilgili olarak etkin pişmanlık hükümlerinin uygulanması 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 verilen suçun başka hangi hallerde işlendiği anlaşılmaktadır. Teşebbüs seviyesinde kalıp kalmadığı, bir içtima halinin olup olmadığı hep bu konuyla ilgilidir.

Teşebbüs

Söz konusu suçlara teşebbüs mümkündür. Örneğin başkasına ait kredi kartını kullanırken yakalanan kimse, doğrudan icra hareketlerine başlamış, ancak fiili tamamlayamamış olduğundan birinci fıkra kapsamında suça teşebbüsten sorumlu olacaktır. Yine sahte kredi kartı yapmak için icra hareketlerine başladıktan sonra sahte kart yapmayı tamamlamadan yakalanan kimse de ikinci fıkra kapsamında suça teşebbüsten sorumlu olur.

İştirak

TCK m.245 kapsamında düzenlenen suçlara iştirakin her türlüsü mümkündür. Özellik arzeden herhangi bir durum bulunmamaktadır. Bu bağlamda iki kişi fiil üzerinde hakimiyet kurmak suretiyle sahte bir kredi kartı üretirlerse, müşterek fail olarak ikinci fıkra kapsamında suçtan sorumlu olacaklardır. Aklında böyle bir fiil gerçekleştirme düşüncesi olmayan birisine, sahte kart üretme fikrini aşılayan kişi ise, bu düşünceyi oluşturduğu kişinin fiili gerçekleştirmesi halinde azmettiren olarak sorumlu olacaktır. Fiili gerçekleştiren kişi ise müstakil fail olarak cezai sorumluluğa sahip olur.

İçtima

TCK m.245/1 kapsamında; fail başkasına ait kredi kartını alır ve birden fazla kez kullanırsa, TCK m.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 suç, örneğin yağma suçu, işlemek suretiyle ele geçirmişse, gerçek içtima hükümleri uygulanacak ve hem yağmadan hem de TCK m.245/1 kapsamında cezai sorumluluğa sahip olacaktır.

TCK m.245/3'de fiilin daha ağır cezayı gerektiren başka bir suçu oluşturmadığı durumda failin bu fıkra hükmüne göre cezalandırılacağı hükme bağlanmıştır. Dolayısıyla işlenen eylem için kanunda daha ağır cezayı içeren bir ceza normu mevcutsa, faili TCK m.245/3 hükmüne göre cezalandırmak mümkün olmayacaktır.

Son olarak belirtmek gerekir ki; fail hem sahte kredi kartı hem de bunu kullanırsa, gerek TCK m.245/2'ye gerekse de TCK m.245/3'e göre ayrı ayrı cezalandırılacaktır. Nitekim bu suçlardan birisi diğerinin unsurunu veya ağırlaştırıcı sebebini oluşturmamaktadır.

Ceza

Birinci fıkra kapsamındaki fiiller bakımından hem adli para cezası hem de hapis cezası öngörülmüştür. Bu kapsamdaki fiillerin faili üç yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılacaktır. İkinci fıkra kapsamındaki fiiller için de hapis ve adli para cezasının birlikte uygulanmasını kabul eden kanunkoyucu cezaların miktarında da belirli oranda arttırıma gitmiştir. Buna göre ikinci, fıkra kapsamındaki fiillerin faili, üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası ile cezalandırılacaktır. Üçüncü fıkra kapsamındaki fiiller için ise hapis cezasının miktarı önceki fıkralarda öngörülenden daha fazla belirlenirken, para cezasının miktarı birinci fıkrayla aynı sınırlar içinde kabul edilmiştir. Bu bağlamda üçüncü fıkra kapsamında fiili gerçekleştiren kişi dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır. Bununla birlikte üçüncü fıkra kapsamındaki fiil daha ağır cezayı gerektiren başka bir suçu oluşturuyorsa, fail bu daha ağır ceza gerektiren fiilden dolayı cezalandırılacaktır. Ayrıca söz konusu suçun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine de hükmolunacaktır (TCK m.246; m.60).

Öğrenme Çıktısı

5 Kredi kartlarının kötüye kullanılması başlığı altındaki suçları analiz edebilme

Araştır 4	İlişkilendir	Anlat/Paylaş
TCK m.245/1'deki suça ilişkin fiilin sahte bir kredi kartı üzerinde işlenebilmesi mümkün müdür?	Banka ve Kredi Kartlarını kötüye kullanılması suçuna ilişkin ayrıntılı bir inceleme için bkz. Eylem Baş, Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, Ankara 2015	TCK m.245/1 kapsamındaki suçun zincirleme suç şeklinde işlenmesi söz konusu olabilir mi?

YASAK CİHAZ VE PROGRAMLAR SUÇU

Bölümün başında belirttiğimiz üzere bilişim alanı en hızlı gelişen teknolojik alanlardan birisidir. Buna bağlı olarak bilişim alanında ihtiyaç duyulan hukuki düzenlemeler de hızlı şekilde gelişmektedir. Nitekim birkaç yıl önce ihtiyacı karşılayan hukuki mevzuat, bilişim alanındaki gelişmeler ve yeni suç işleme yöntemleri dolayısıyla birkaç yıl sonra ihtiyaca cevap veremez duruma gelebilmektedir. Bu bağlamda yakın zaman içerisinde ortaya çıkan ihtiyaca bağlı olarak, TCK'ya, 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, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile 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. Dolayısıyla bilişim alanındaki tüm suçlarla koruma altına alınan hukuki menfaatler toplamı aynı zamanda bu suç tipiyle de koruma altına alınmaya çalışılmaktadır. Bu nedenle 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, kanunkoyucucunun 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. Nitekim seçimlik hareketli suçlarda, cezai sorumluluğun ortaya çıkması için hareketlerden birisinin yapılması yeterlidir; ancak bunlardan birden fazlası yapılırsa işlenen suç yine tek suç olmaya devam eder. Örneğin bir kimse belirtilen amaçlarla üretilmiş bir cihazı hem depolayıp hem satışa arzedip hem de satmış olabilir. Bu durumda failin suçu bir kez işlemekten dolayı cezai sorumluluğu doğacaktır. Ancak seçimlik hareketlerden birden fazlasını gerçekleştirmiş olması hakim tarafından ceza belirlenirken, TCK m.61 kapsamında alt sınırdan ayrılmaya gerekçe olabilecektir.

Bununla birlikte suç şekli bir suçtur (sırf hareket suçudur). Kanunda belirtilen imal, ithal, satış, vs. gibi davranışlar gerçekleştirildiği anda suç tamamlanmış olacaktır. Bunun dışında ayrıca dış dün-

yada gözlenebilen bir neticenin meydana gelmesi aranmamaktadır. Örneğin bir virüs programını, başkalarının verilerine zarar vermek için yapıldığını bilerek, birisinden alan kimse, bu programı hiç kullanmasa ve kullanmayı düşünmese bile "kabul etmiş olmaktan" dolayı TCK m.245/A hükmüne göre cezai sorumluluğa sahip olacaktır.

Ayrıca belirtmek gerekir ki; *cihazın, 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. TCK'nın özel hükümlerinde, topluma karşı suçlar arasında yer alan onuncu bölümde m.243-245 arasında bilişim alanında suçlara yer verilmiştir. Bununla birlikte TCK m.142 nitelikli hırsızlık, TCK m.158 nitelikli dolandırıcılık örneklerinde olduğu gibi, bazı suçların bilişim sistemlerinin kullanılması suretiyle işlenmesi de mümkündür. Gerek onuncu bölümde düzenlenen gerekse de işlenmesinde bilişim sisteminin araç olarak kullanılabileceği suçları "geniş anlamda bilişim suçları" başlığı altında toplamak mümkündür. Bu bağlamda *cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodu*nun geniş anlamda bilişim suçlarını işlemeye yönelik yapılması, m.245/A'da hükme bağlanan ve bunlar üzerinde gerçekleştirilmesi aranan davranışların cezai sorumluluk doğurabilmesi bakımından zorunludur.

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 sürece hukuka uygunluk nedenlerinin hukuka aykırılığı kaldıran bir sebep olarak ortaya çıkması söz konusu olabilir. Bu bağlamda kendi bilişim sistemine sürekli saldırıda bulunan bir başka sisteme, saldırıyı gerçekleştirdiği anda müdahalede bulunarak zarar vermesi için bir yazılım yapan kimsenin, böyle bir yazılım imal etmekten dolayı sorumluluğu oluşmaz. Çünkü yazılım saldırı anında saldırıyı yapan sisteme zarar vermek amacıyla oluşturulmuştur. Meşru savunmada kullanılmaya yönelik böyle bir program yapılması, TCK m.245/A kapsamındaki suçun hukuka aykırılık unsurunu ortadan kaldırarak suçun oluşmasını engeller.

Kusurluluk

Kusurluğu kaldıran sebepler bu suç bakımından da geçerlidir. Bu bağlamda örneğin, TCK m.28 kapsamında karşı konulamayacak bir cebir veya ağır bir tehdit altında bilişim suçlarını işlemeye yönelik cihaz imal eden kimse cezai sorumluluğa sahip olmaz. Ancak bu durumda cebir ve tehditle ona söz konusu cihazı imal ettiren kimsenin TCK m.37 kapsamında dolaylı fail olarak cezai sorumluluğu doğar.

Suçun Özel Beliriş Biçimleri

Suçun özel beliriş biçimlerinden, yukarıda verilen suçun başka hangi hallerde işlendiği anlaşılmaktadır. Teşebbüs seviyesinde kalıp kalmadığı, bir içtima halinin olup olmadığı hep bu konuyla ilgilidir.

Teşebbüs

Söz konusu suça teşebbüs mümkündür. Ancak sırf hareket suçu olması dolayısıyla, teşebbüs ancak icra hareketleri tamamlanmadan söz konusu olabilir. Nitekim icra hareketleri tamamlandıktan sonra suçun oluşmaması diye bir durum söz konusu değildir. Bu bağlamda örneğin, bilişim sistemlerine gizlice girmeyi sağlayacak bir yazılım oluşturmaya çalışan kimse, bu yazılımı tamamlamadan yakalanırsa TCK m.245/A'daki suça teşebbüsten sorumlu olacaktır. Benzer şekilde bilişim sistemlerine zarar verecek bir programı bir başkasından almak üzereyken yakalanan kimse bakımından da teşebbüs hükümleri uygulama alanı bulacaktır.

İştirak

Bu suça iştirakin her türlüsü mümkündür. Özellik arzeden herhangi bir durum bulunmamaktadır. Bu bağlamda iki kişi fiil üzerinde hakimiyet kurmak suretiyle bilişim sistemlerine zarar verecek bir yazılım yaparlarsa, müşterek fail olarak bu suçtan sorumlu olacaklardır (TCK m.37). Aklında böyle bir program yazma düşüncesi olan arkadaşının, bu düşüncesini destekleyen ve suç işleme kararını kuvvetlendiren kimse bakımından ise TCK m.39 kapsamında yardım etmeden dolayı cezai sorumluluk ortaya çıkacaktır.

İçtima

Söz konusu suç, mağduru belirli bir kimse olmayan suç kategorisinde yer aldığı için TCK m.43/1 kapsamında zincirleme suç şeklinde işlenebilir. Örneğin tek suç işleme kararının icrası kapsamında bir bilişim sistemine gizlice sızmaya imkân tanıyan programlar yazan kimse TCK m.43/1'e göre cezalandırılacaktır.

Bu noktada ayrıca belirtmek gerekir ki; suç tipinde, *bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun;* geniş anlamda bilişim suçlarını 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. Dolayısıyla bu suçun oluşabilmesi için cihaz, program, *şifre veya kodun* kullanılarak bir bilişim suçunun işlenmesine gerek yoktur. Eğer bilişim sistemi kullanmak suretiyle hırsızlık yapmak için bir program yazan kimse, yazdığı programı kullanarak ayrıca planladığı hırsızlığı da gerçekleştirirse gerek m.245/A'daki inceleme konumuz olan suçtan gerekse TCK m.142 kapsamında bilişim sistemlerini kullanmak suretiyle hırsızlıktan dolayı ayrı ayrı cezai sorumluluğa sahip olacaktır.

Ceza

Suç karşılığında uygulanacak yaptırım olarak gerek hapis gerekse de adli para cezası öngörülmüştür. Bu bağlamda söz konusu eylemleri gerçekleştiren kimsenin *bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası* ile cezalandırılması hükme bağlanmıştır. Ayrıca söz konusu suçun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine de hükmolunacaktır (TCK m.246; m.60).

Öğrenme Çıktısı

6 Yasak cihaz ve programlar suçunun unsurlarını tespit edebilme

Araştır 5

TCK m.245/A'daki suça ilişkin seçimlik hareketlerden birden fazlası birlikte gerçekleştirilirse, failin cezai sorumluluğu ne şekilde ortaya çıkar?

İlişkilendir

Yasak programlar ve cihazlar suçu hakkında daha ayrıntılı bilgi için bkz. Mahmut Koca-İlhan Üzülmez, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayınevi, Ankara 2017.

Anlat/Paylaş

TCK m.245/A'da hükme bağlanan yasak cihaz ve programlar suçu serbest mi, bağlı mı yoksa seçimlik hareketli mi bir suçtur?

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 faydalanmakta 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 infazını 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 arzetmesine bağlı olarak kanunkoyucu bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve elkoyma 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. Kanunkoyucunun 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.

Aşağıda özel olarak ayrı bir maddede hükme bağlanmış olan söz konusu tedbir alt başlıklar halinde incelenecektir.

Tedbire Başvurmanın Koşulları

Tedbire başvurulabilmesi bakımından kanunkoyucu iki koşul öngörmüştür. Buna göre tedbire başvurulabilmesi için ilk olarak *somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı* aranmıştır (Dülger, 2014: 685). 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, kanunkoyucu bu tedbirin uygulanmasını yerinde görmemiştir.

Tedbire Karar Vermeye Yetkili Merciler

Tedbire Cumhuriyet savcısının istemi üzerine sulh ceza hakimi tarafından karar verilir. Kovuşturma sırasında tedbire başvurma imkânı bulunmadığı için mahkemenin bu yönde bir karar alma yetkisi bulunmamaktadır. Ayrıca soruşturma sırasında görevli yargılama makamı olan sulh ceza hakiminden başka bir adli merciin de herhangi bir koşula bağlı olarak 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 olduğunda aramaya ilişkin genel kurallara göre bilgisayarlarda, programlarında ve kütüklerinde arama yapılabileceği şeklindeki bir yorum tarzı ise yerinde değildir. Nitekim kanunkoyucu bilgisayarlarda, program ve kütüklerinde genel kurallara göre arama yapılmasını yerinde görseydi, ayrıca böyle bir tedbire de ihtiyaç duymazdı. Soruşturma bakımından da ayrı düzenleme yapmaksızın, genel kurallara göre arama yapılmasına imkân tanırdı. Eğer tedbirin uygulama alanının kovuşturmayı da kapsar şekilde genişletilmesi isteniyorsa, bunun ayrıca düzenleme altına alınması zorunluluktur 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 şifreleme nedeniyle söz konusu işlemlerin gerçekleştirilmesi mümkün olmayabilir. Kanunkoyucu bu ihti-

male binaen ilgili araç ve gereçler üzerinde elkoyma işleminin 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 elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir (CMK m.134/2)."* Bilgisayarların ticari ve gündelik yaşamda giderek daha fazla yer almaları ve önem arzetmeleri dolayısıyla, kanunkoyucu öncelikle bunlar üzerinde elkoyma işlemi yapılmaksızın, gerekli arama, kopya çıkarma ve metin haline getirme işlemlerinin yapılmasını öngörmüştür. Bu şekilde söz konusu bilgisayarın şüphelinin kullanımından alınması söz konusu olmayacaktır. Ancak şifreleme nedeniyle bu işlemler yapılamazsa, mecburen elkoymaya cevaz verilmiştir.

Tedbir kapsamında belirlenen işlemler şüphelinin kullandığı bilgisayarlar üzerinde yapılabilecektir. Bu bağlamda üçüncü kişilere ait bilgisayarlar üzerinde söz konusu tedbirin öngördüğü işlemlerin yapılabilmesi, şüphelinin bu üçüncü kişiye ait bilgisayarı kullanıyor olması koşuluna bağlıdır. Aksi takdirde bu tedbirin başkalarına ait bilgisayarlar üzerinde icra edilmesi söz konusu değildir.

"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 elkonulan donanımdaki veriler üzerinde sonradan değişiklik yapılması ihtimaline binaen, bir kopyanın şüpheliye verilmesi onun bakımından önemli bir güvence oluşturmaktadır.

"*Bilgisayar veya bilgisayar kütüklerine elkoymaksızın 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).*"

Öğrenme Çıktısı

7 Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanma koşullarını belirleyebilme

Araştır 6	İlişkilendir	Anlat/Paylaş
Hangi merci, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirine karar vermeye yetkilidir?	CMK m.134 kapsamında düzenlenen koruma tedbiri hakkında daha ayrıntılı bilgi için bkz. Nur Centel-Hamide Zafer, Ceza Muhakemesi Hukuku, Beta Yayınevi, İstanbul 2017	Muhakeme hukuku bakımından koruma tedbiri kavramı neyi ifade eder?

1 Bilişim suçlarına ilişkin Türkiye'de yaşanan süreci ifade edebilme

2 Bilişim suçlarına ilişkin temel kavramları açıklayabilme

Bilişim Alanındaki Suçlara İlişkin Türkiye'de Yaşanan Süreç

Bilişim alanındaki gelişmelerin hukuk alanında da önemli birtakım sorunlara neden olduğu aşikardır. Nitekim bu alanda yaşanan gelişmelerle birlikte mülkiyet, fikri hak, haksız fiil, özel hayat gibi çok önemli hukuksal kavramların tanımları ya da anlayış biçimleri değişmiştir. Konu ceza hukuku bakımından ele alınırsa, bilişim alanındaki suçlar bu hukuk dalının en güncel ve en hızlı değişim gösteren konularından birini oluşturmaktadır. Nitekim bilişim alanında yaşanan gelişmelere bağlı olarak daha önceden hiç öngörülemeyen ve dolayısıyla suç tipleri arasında düzenlenmeyen bir takım yeni fiiller ortaya çıkabildiği gibi, mevcut suç tipleriyle öngörülen fiillerin yeni yöntemlerle işlenmesi de söz konusu olabilmektedir. Bu bağlamda yasa koyucunun da bu alanda görülen gelişmelere paralel olarak, mevcut düzenlemelerini değiştirmesi ya da yeni düzenlemeler yapması gerekmektedir. Aksi takdirde ortaya çıkabilecek hukuki boşluklar, sosyal hayatta önemli sorunların yaşanmasına neden olabilecektir.

TCK'da ise bilişim alanında işlenen suçlara, önceki 765 sayılı kanundan daha ayrıntılı düzenlemeler yapılarak yer verilmiştir. Kanunda söz konusu suçlara, özel hükümlerin yer aldığı TCK'nın 2. kitabının topluma karşı suçların düzenlendiği 3. kısmının 10. bölümünde "Bilişim Alanında Suçlar" başlığı altında yer verilmiştir. Bununla birlikte 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.

3 Bilişim sistemine girme başlığı altındaki suçları analiz edebilme

Bilişim Sistemine Girme

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 bir 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, altı aydan iki 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, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*

TCK m.243'e bakıldığında görüldüğü üzere, madde dört fıkradan oluşmaktadır. Birinci ve dördüncü fıkralarda iki farklı suç tipine yer verilirken, ikinci ve üçüncü fıkralarda ise birinci fıkradaki suçun daha az ve daha fazla cezayı gerektiren nitelikli hallerine yer verilmiştir. Bu hallerden ilkinin gerçekleşmesi halinde faile suçun temel şekline nazaran daha az, ikincisinin gerçekleşmesi halinde ise daha fazla ceza verilmesi öngörülmüştür.

4 Sistemi engelleme, bozma, verileri yok etme veya değiştirme başlığı altındaki suçların unsurlarını açıklayabilme

Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

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: ***Madde 244-*** *(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 beşbin güne kadar adlî para cezasına hükmolunur.*

5 Kredi kartlarının kötüye kullanılması başlığı altındaki suçları analiz edebilme

Banka ve Kredi Kartlarının Kötüye Kullanılması

Gerek banka kartları gerekse kredi kartları son dönemde gündelik hayatta giderek daha fazla yer tutmaya başlamıştır. Birçok insan artık yanında para taşımamakta, doğrudan veya internet üzerinden yaptığı alış-verişlerde çoğunluk banka kartı veya kredi kartı kullanmayı tercih etmektedir. Banka kartları sayesinde banka şubesine gitmeden insanlar kolaylıkla para çekebilmekte, bu durum da gündelik hayatı son derece kolaylaştırmaktadır. Banka ve kredi kartlarının alış-verişlerde kullanımı, harcama ve satışların kayıt altında tutulmasını kolaylaştırmaktadır. Böylelikle söz konusu kartlarının kullanımı vergilendirmeyi etkili kıldığı için, bu şekilde alış-veriş yapılması iktidarlar tarafından da desteklenmektedir. Ancak bu kartların kullanımının yaygınlaşması kartlara duyulan güvenin oluşturulması ve devamlılığının sağlanmasıyla mümkün olabilmektedir. Toplum içerisinde yaygınlaşmasına bağlı olarak bu kartların kötüye kullanılmasını özel düzenlemeye tabi tutarak bu tür suçlulukla etkin şekilde mücadele etmeyi ve böylelikle kartlara olan güvenin devamlılığını teminat altına almayı amaçlayan kanunkoyucu da 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 kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin 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 beşbin 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.*

Görüldüğü üzere TCK m.245'te banka ve kredi kartlarının kötüye kullanılması başlığı altında üç farklı suç tipine yer verilmiştir. TCK m.245/1'de başkasına ait banka veya kredi kartını kullanmak suretiyle yarar sağlama; TCK m.245/2'de sahte banka veya kredi kartı üretme, satma, satın alma ve kabul etme; TCK m.245/3'te ise sahte banka veya kredi kartı kullanarak yarar sağlama suçları hükme bağlanmıştır.

6 Yasak cihaz ve programlar suçunun unsurlarını tespit edebilme

Yasak Cihaz ve Programlar Suçu

Başlangıçta da ifade ettiğimiz üzere bilişim alanındaki gelişmelere bağlı olarak ihtiyaç duyulan hukuki düzenlemeler de hızlı şekilde gelişmektedir. Nitekim birkaç yıl önce ihtiyacı karşılayan hukuki mevzuat, bilişim alanındaki gelişmeler ve yeni suç işleme yöntemleri dolayısıyla birkaç yıl sonra ihtiyaca cevap veremez duruma gelebilmektedir. Bu bağlamda yakın zaman içerisinde ortaya çıkan ihtiyaca bağlı olarak, TCK'ya, 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. TCK'nın söz konusu 245/A maddesinde yer alan düzenleme şu şekildedir; ***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, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.*

7 Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanma koşullarını belirleyebilme

Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma

Son olarak bilişim sistemlerinin ve dolayısıyla bilgisayarların sosyal ve ticari alanda giderek yaygınlaşması ve bireysel yaşamda da giderek daha fazla önem arzetmesine bağlı olarak kanunkoyucu bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve elkoyma 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 ve hakim kararıyla başvurulabilen bir tedbirdir. Kanunkoyucunun 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.

neler öğrendik?

1 Bilişim sistemine girme suçunun faili ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Herkes suçun faili olabilir.
B. Yalnız kamu görevlileri suçun faili olabilir.
C. Yalnız erkekler suçun faili olabilir.
D. Yalnız kadınlar suçun faili olabilir.
E. Yalnız onsekiz yaşından büyükler suçun faili olabilir.

2 Şifreli televizyon yayınlarını, şifreyi kırmak suretiyle ödeme yapmaksızın izleyen kimse aşağıdaki hangi suçtan sorumlu olacaktır?

A. Hırsızlık
B. Karşılıksız yararlanma
C. Bilişim sistemine girme
D. Dolandırıcılık
E. Güveni kötüye kullanma

3 Bilişim sistemine girme (TCK m.243/1) suçunun daha fazla cezayı gerektiren nitelikli hali aşağıdakilerden hangisidir?

A. Kamu görevlisine karşı işlenmesi
B. Ticari işletmelere karşı işlenmesi
C. Mağdurun on sekiz yaşından büyük olması
D. Fiil nedeniyle verilerin yok olması veya değişmesi
E. Fiilin bir örgütün faaliyeti kapsamında gerçekleştirilmiş olması

4 Bilişim sisteminin işleyişini engelleme veya bozma (TCK m.244/1) suçunun daha fazla cezayı gerektiren nitelikli hali aşağıdakilerden hangisidir?

A. Suçun örgütün faaliyeti kapsamında işlenmesi
B. Suç sonucunda herhangi bir tüzel kişiliğe menfaat sağlanması
C. Suçun bir bankaya karşı işlenmesi
D. Suçun mağdurunun otuz yaşından büyük olması
E. Suçun failinin otuz yaşından büyük olması

5 Bilişim sistemi aracılığıyla haksız çıkar sağlama (TCK m.244/4) suçunun manevi unsuru bakımından aşağıdakilerden hangisi doğrudur?

A. Genel kast gerekli ve yeterlidir.
B. Failin özel bir kastla hareket etmesi aranır.
C. Suç kasten veya taksirle işlenebilir.
D. Basit taksir gerekli ve yeterlidir.
E. Suç ancak bilinçli taksirle işlenebilir.

6 Başkasına ait kredi kartını çalan ve alışverişte kullanan kimsenin cezai sorumluluğu ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Sadece başkasına ait banka veya kredi kartını kullanarak yarar sağlama suçundan sorumludur.
B. Sadece hırsızlıktan sorumludur.
C. Sadece bilişim sistemine girmekten sorumludur.
D. Hırsızlıktan ve başkasına ait banka veya kredi kartını kullanarak yarar sağlamaktan ayrı ayrı sorumludur.
E. Bilişim sistemine girme, Hırsızlık ve başkasına ait banka veya kredi kartını kullanarak yarar sağlamaktan ayrı ayrı sorumludur.

7 Başkasına ait banka veya kredi kartını kullanarak yarar sağlama (TCK m.245/1) suçunun faili bakımından hangi halde şahsi cezasızlık sebebi söz konusudur?

A. Suçu babasına karşı işlemişse
B. Suç nedeniyle ortaya çıkan zararı gidermişse
C. Yargılama sırasında pişmanlığını açıkça ifade etmişse
D. Kamu kurumu yararına suçu işlemişse
E. Hukuki alacağının tahsili amacıyla suçu işlemişse

8 Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirine karar vermek için, somut delillere bağlı olarak en az hangi şüphe derecesinin bulunması gerekir?

A. Basit Şüphe
B. Makul şüphe
C. Yeterli şüphe
D. Kuvvetli şüphe
E. Kesin şüphe

9 Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirine karar vermeye yetkili merci ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Tedbire sadece hakim karar verebilir.
B. Tedbire kural olarak hakim, gecikmesinde sakınca bulunan hallerde ise Cumhuriyet Savcısı karar verebilir.
C. Tedbire kural olarak hakim, gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı, Cumhuriyet Savcısına ulaşılamıyorsa da kolluk amiri karar verebilir.
D. Tedbire kural olarak hakim, gecikmesinde sakınca bulunan hallerde ise mülki amir karar verebilir.
E. Tedbire yalnızca Cumhuriyet Savcısı karar verebilir.

10 Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanabileceği muhakeme safhası ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Yalnızca soruşturma sırasında başvurulabilen bir tedbirdir.
B. Yalnızca duruşma sırasında başvurulabilen bir tedbirdir.
C. Yalnızca iddianamenin değerlendirilmesi aşamasında başvurulabilir.
D. Yalnızca kanunyolu aşamasında başvurulabilir.
E. Hem soruşturma hem de kovuşturma da başvurulabilir.

neler öğrendik yanıt anahtarı

1. A	Yanıtınız yanlış ise "Bilişim Sistemine Girme Suçu" konusunu yeniden gözden geçiriniz.
2. B	Yanıtınız yanlış ise "Şifreli Yayınların Konumu" konusunu yeniden gözden geçiriniz.
3. D	Yanıtınız yanlış ise "Bilişim Sistemine Girme Suçu" konusunu yeniden gözden geçiriniz.
4. C	Yanıtınız yanlış ise "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu" konusunu yeniden gözden geçiriniz.
5. A	Yanıtınız yanlış ise "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu" konusunu yeniden gözden geçiriniz.
6. D	Yanıtınız yanlış ise "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu" konusunu yeniden gözden geçiriniz.
7. A	Yanıtınız yanlış ise "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu" konusunu yeniden gözden geçiriniz.
8. D	Yanıtınız yanlış ise "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" konusunu yeniden gözden geçiriniz.
9. A	Yanıtınız yanlış ise "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" konusunu yeniden gözden geçiriniz.
10. A	Yanıtınız yanlış ise "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" konusunu yeniden gözden geçiriniz.

4 Araştır Yanıt Anahtarı

Araştır 1

"International" ve "Network" kelimelerinin başlangıç 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. Bu nedenle internete "ağlar arası ağ" da denilmektedir. İnternet sanıldığının aksine veri iletim ağlarının yalnızca bir türü, dolayısıyla sanal alanın yalnızca bir parçasıdır. Ancak dünya üzerinde bugün kullanılan en yaygın ve en geniş ağdır. Sanal alan ise bilişim sistemleri ile bunları birbirine bağlayan her türlü veri işletim ağından oluşan, fiziksel yapısı sayısal verilerden iberet bir alandır.

Araştır 2

TCK m.243'e bakıldığında görüldüğü üzere, madde dört fıkradan oluşmaktadır. Birinci ve dördüncü fıkralarda iki farklı suç tipine yer verilirken, ikinci ve üçüncü fıkralarda ise birinci fıkradaki suçun daha az ve daha fazla cezayı gerektiren nitelikli hallerine yer verilmiştir.

Araştır 3

TCK m.244'de düzenlenen söz konusu suçlar kasten işlenebilen suçlardır. Kanunda taksirli şekillerine açıkça yer verilmediği için, bu suçların taksirle işlenmesi mümkün değildir. Kast bakımından ise genel kast yeterlidir. Nitekim suçun oluşumu bakımından özel kast, bir başka deyişle failin belirli bir saikle (motivasyonla) hareket etmesi zorunluluğu aranmamıştır. Bununla birlikte suçların olası kastla da işlenmesi söz konusu olabilir.

4 Araştır Yanıt Anahtarı

Araştır 4

TCK m.245/1'deki 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. Bu bağlamda söz konusu suça ilişkin fiilin sahte kart üzerinde işlenmesi mümkün değildir.

Araştır 5

Söz konusu suç seçimlik hareketli bir suçtur. Kanunilik ilkesi bakımından sorun oluşturmaması amacıyla, kanunkoyucucunun 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. Nitekim seçimlik hareketli suçlarda, cezai sorumluluğun ortaya çıkması için hareketlerden birisinin yapılması yeterlidir; ancak bunlardan birden fazlası yapılırsa işlenen suç yine tek suç olmaya devam eder. Bununla birlikte, seçimlik hareketlerden birden fazlasını gerçekleştirmiş olması hakim tarafından ceza belirlenirken, TCK m.61 kapsamında alt sınırdan ayrılmaya gerekçe olabilecektir.

Araştır 6

Tedbire Cumhuriyet savcısının istemi üzerine sulh ceza hakimi tarafından karar verilir. Kovuşturma sırasında tedbire başvurma imkânı bulunmadığı için mahkemenin bu yönde bir karar alma yetkisi bulunmamaktadır. Ayrıca soruşturma sırasında görevli yargılama makamı olan sulh ceza hakiminden başka bir adli merciin de herhangi bir koşula bağlı olarak bu tedbire karar vermesi söz konusu değildir.

Kaynakça

Baş, E. (2015). *Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu.* Ankara.

Dülger, M. V. (2014). *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara.

Özen, M. ve Baştürk, İ. (2011). B*ilişim-İnternet ve Ceza Hukuku.* Ankara.

Yaşar, O., Gökcan, H. T. ve Artuç, M. (2014). *Yorumlu-Uygulamalı Türk Ceza Kanunu (5. Cilt).* Ankara.

Bölüm 5

5651 Sayılı Kanun Bağlamında İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi

Öğrenme çıktıları

1 Temel Kavramlar, Kurumun Görevleri ve Erişim Sağlayıcılar Birliği

1 5651 sayılı kanun kapsamındaki temel kavram ve kurumları açıklayabilme

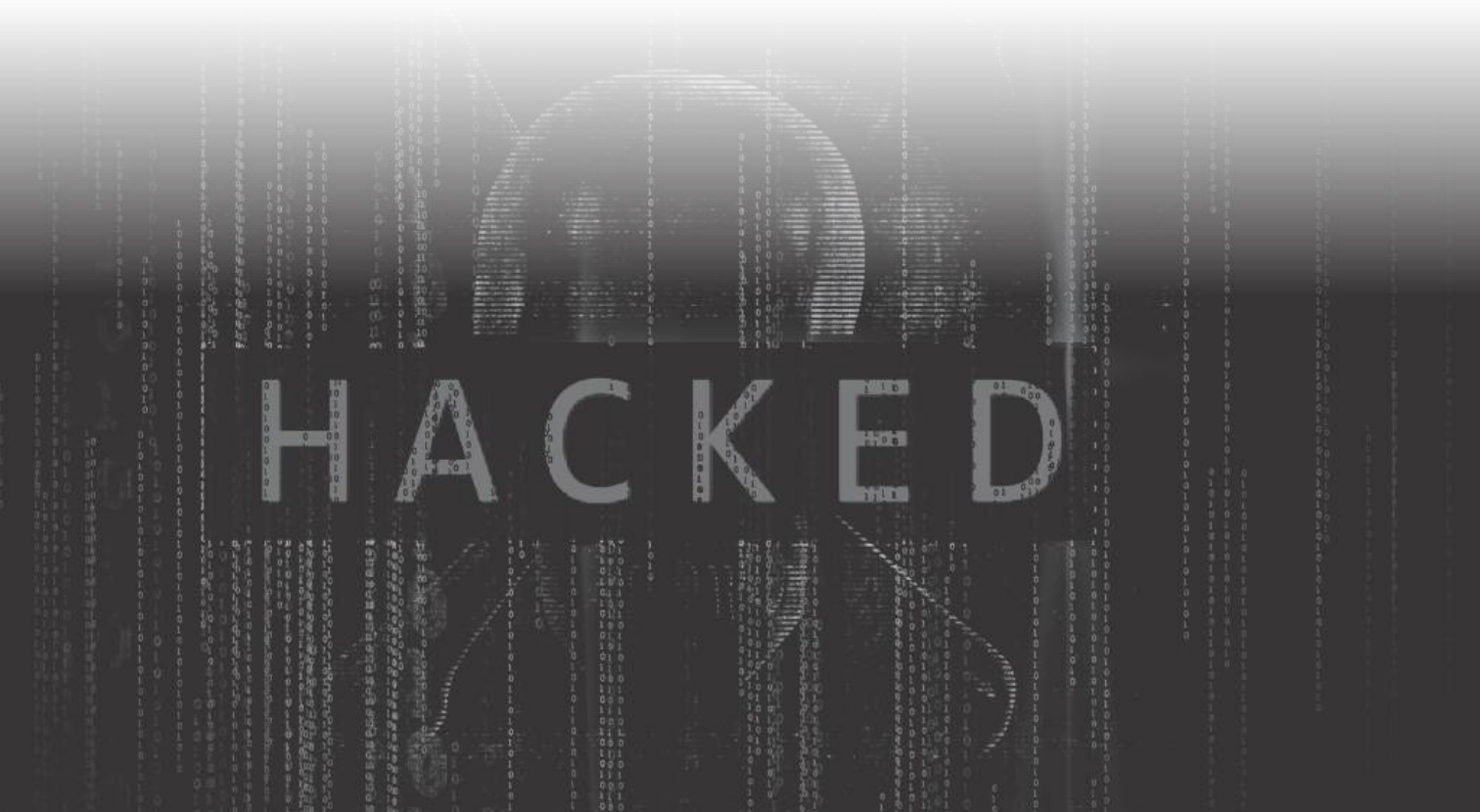
2 İçerik, Yer ve Erişim Sağlayıcılar Bakımından Öngörülen Bilgilendirme Yükümlülüğü

2 İçerik, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerini ifade edebilme

3 İçeriğin Çıkartılması ve/veya Erişimin Engellenmesi Tedbirlerine İlişkin Genel Açıklamalar

3 Farklı kapsamdaki içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirlerinin uygulanma koşullarını belirleyebilme

Anahtar Sözcükler: • 5651 Sayılı Kanun • İçerik Sağlayıcı • Yer Sağlayıcı • Erişim Sağlayıcı • Toplu Kullanım Sağlayıcı • İçeriğin Çıkartılması • İçeriğe Erişimin Engellenmesi • Siteye Erişimin Engellenmesi



GİRİŞ

İçinde bulunduğumuz zaman diliminde, internet gündelik ve ticari hayatta giderek önemini arttırmakta ve her geçen gün daha fazla yer işgal etmektedir. Eğlenceden haberleşmeye, eğitimden alışverişe kadar hemen her sosyal alanda internet kullanımına giderek daha fazla rastlanmaktadır. Bu bağlamda internet sayesinde insanoğlunun hayatının çok kolaylaştığını ve daha konforlu hale geldiğini söylemek yanlış olmayacaktır.

Bununla birlikte internet insanoğlunun hayatını sadece kolaylaştırmakla kalmamış aynı zamanda asosyalleşme, internet bağımlılığı gibi bazı dezavantajları da beraberinde getirmiştir. Ancak her halükârda modern dönemin bu göreli yeniliğinin, insanlık için dezavantajlarına nazaran çok daha büyük avantajlar sağladığı kanaatindeyiz. Bu nedenle interneti sosyal hayattan çıkarmak artık mümkün olmadığına göre, onun toplumsal menfaat bakımından getirdiği zararları mümkün olduğunca aza indirmeye gayret etmelidir.

İnternetin en önemli toplumsal dezavantajlarından birisi, yeni suç işleme yöntemlerine imkân tanıması ve ortaya çıkardığı yeni bireysel menfaatlere bağlı olarak, yeni suç tiplerine ilişkin düzenlemeler yapılmasını zorunlu kılmasıdır. Gerçekten de internet sayesinde insanlık artık sadece daha rahat iletişim sağlamamakta, bilgiye daha kolay ulaşmamakta; bunlarla birlikte aynı zamanda daha kolay çalmakta, daha rahat zarar vermekte ve tahrip edebilmektedir. Bundan birkaç yüzyıl önceki insanların hayal bile edemediği yeni imkânlar ve haklar ortaya çıkartan internet, bu haklara karşı işlenecek suçlarda da önemli bir araç haline gelebilmektedir. Buna rağmen interneti suçla özdeşleşmiş bir araç olarak görmekten de kaçınmak gerekir (Gedik, 2008:180).

Bu bağlamda internet yoluyla işlenen suçlarla mücadele adına kanun koyucunun da birtakım özel düzenlemeler yapması kaçınılmazdır. Çünkü modern dönemin getirdiği bu yeni araç, klasik suç, ceza ve muhakeme anlayışının öngöremediği toplumsal zararlar ve suç işleme yöntemleri ortaya çıkarmıştır. Bunlarla mücadele edebilmek ise ancak internetin özellikleri ve yapısı göz önünde bulundurularak yapılacak özel hukuki düzenlemelerle mümkün olabilecektir.

İnternet yoluyla işlenen suçlardan önemli bir kısmı ise internet yayınları vasıtasıyla gerçekleştirilmektedir. Dolayısıyla bu tür suçlarla mücadele adına özel birtakım düzenlemelerin yapılması kaçınılmazdır. Bu gereklilikler karşısında kanun koyucumuz da internet yayınları yoluyla işlenen suçlarla mücadele adına özel bir kanun düzenlemesi yapmıştır. 23.05.2007 tarihli ve 5651 sayılı bu kanunun ismi; İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dur (5651 s.K.). Söz konusu kanunun amacı 1. maddede; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemek olarak belirlenmiştir.

Bu ünitede söz konusu kanunun öngördüğü düzenlemeler ve bunların içeriği inceleme konusu yapılacaktır. Nitekim bilişim hukukuna ilişkin yazılmış bir kitapta, söz konusu düzenlemenin ele alınması sistematik açıdan bir zorunluluk olarak karşımıza çıkmaktadır.

TEMEL KAVRAMLAR, KURUMUN GÖREVLERİ VE ERİŞİM SAĞLAYICILAR BİRLİĞİ

Ünitenin başında, ünitede kullanılacak ve ilgili kanunda geçen temel kavramların açıklanmasının, 5651 s. K.'nın uygulanmasında çok önemli bir rolü bulunan Bilgi Teknolojileri ve İletişim Kurumunun görevlerinin belirlenmesinin ve 5651 s. Kanunun 8. maddesi kapsamı dışında kalan hallerde erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere kurulan erişim sağlayıcılar birliğinin yapısının analiz edilmesinin sistematik açıdan uygun olacağı kanaatindeyiz. Nitekim söz konusu hususları diğer anlatımlara geçmeden açıklamak, ileride anlatılacakların da daha iyi anlaşılmasına imkân tanıyacaktır.

Temel Kavramlar

5651 s. Kanunun ikinci maddesinde kanunda geçen bazı kavramların tanımlanması yoluna gidilmiştir. Böylelikle kanun koyucu içeriği konusunda tereddüte düşülebilecek bazı kavram ve terimlerden ne anlaşılması gerektiğini açıklığa kavuşturmak istemiştir. Anlatımlarımız sırasında biz de yeri geldikçe aynı kavramları kullanacağımız için ünitenin hemen başında bu düzenlemeye yer vermeyi uygun buluyoruz.

Bu bağlamda 5651 s. kanun uygulamasında (5651 s. K. m.2);

Bakanlık: Ulaştırma 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 çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını,

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 alınamaması hâlinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini ifade etmektedir.

İçerik Sağlayıcı
İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir.

Yer Sağlayıcı
Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.

Bilgi Teknolojileri ve İletişim Kurumunun Görevleri

5651 sayılı kanunla verilen görevler, Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilir (5651 s.K. m.10/1). Kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Kurumun bu Kanun kapsamındaki görev ve yetkileri şunlardır (5651 s.K. m.10/4):

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 oluşturan 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 dahilinde 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.

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

e. İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8 inci 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 işbirliği ve koordinasyonu sağlamak.

g. Bu Kanunun 8 inci 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 teminen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkânları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

Ayrıca Kurum; Bakanlık bünyesinde 26/9/2011 tarihli ve 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 alır (5651 s.K. m.10/5). Bunun dışında ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar (5651 s.K. m.10/6). Bu noktada belirtmek gerekir ki; Kurumun kanunlarla kendisine verilen görevlerin ifası amacıyla araştırma ve geliştirme merkezleri kurmasına da imkân tanınmıştır (5651 s.K. m.10/7).

Erişim Sağlayıcılar Birliği

Temel kavramlar ve kurumun görevleri açıklandıktan sonra kanun koyucunun 5651 s.K.'nın 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamaya yönelik kurulmasını hüküm altına aldığı Erişim Sağlayıcıları Birliği adındaki tüzel kişiliğe ilişkin açıklamaları da ünitenin başında yapmayı uygun buluyoruz. Bu bağlamda belirtmek gerekir ki; birliğin kuruluş amacının 8. madde kapsamına girmeyen erişimin engellenmesi kararlarının uygulanması olduğu kanun koyucu düzenlemede açıkça ifade etmiştir. Nitekim 5651 s.K.'nın 6/A/1. maddesi şu şekildedir: Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur.

Söz konusu birlik, özel hukuk tüzel kişiliğini haizdir ve birliğin merkezi Ankara'dır (5651 s.K. m.6/A/2). Birlik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılmasıyla oluşan ve koordinasyonu sağlayan bir kuruluştur (5651 s.K. m.6/A/5). 5651 s. K.'nın 8. maddesi kapsamı dışındaki erişimin engellenmesi kararları erişim sağlayıcılar tarafından yerine getirilir. Kararların uygulanması amacıyla gerekli her türlü donanım ve yazılım erişim sağlayıcıların kendileri tarafından sağlanır (5651 s.K. m.6/A/6). Söz konusu erişimin engellenmesi kararları, gereği için Birliğe gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır. Birlik, kendisine gönderilen mevzuata uygun olmadığını düşündüğü kararlara itiraz edebilir (5651 s.K. m.6/A/7, 8). Birliğin gelirleri, üyeleri tarafından ödenecek ücretlerden oluşur. Alınacak ücretler, Birliğin giderlerini karşılayacak miktarda belirlenir. Bir üyenin ödeyeceği ücret, üyelerin tamamının net satış tutarı toplamı içindeki o üyenin net satışı oranında belirlenir. Üyelerin ödeme dönemleri, yeni katılan üyelerin ne zamandan itibaren ödemeye başlayacağı ve ödemelere ilişkin diğer hususlar Birlik Tüzüğünde belirlenir. Süresinde ödenmeyen ücretler Birlikçe kanuni faizi ile birlikte tahsil edilir. Bu birliğe üye olmayan internet servis sağlayıcıları faaliyette bulunamaz (5651 s.K. m.6/A/9, 10).

Öğrenme Çıktısı

1 5651 sayılı kanun kapsamındaki temel kavram ve kurumları açıklayabilme

Araştır 1	İlişkilendir	Anlat/Paylaş
İnternet sosyal hayat bakımından zararlı bir araç mıdır?	Erişim Sağlayıcılar Birliği hakkında daha fazla bilgi için internet sayfasını ziyaret edebilirsiniz. Bkz. https://www.esb.org.tr/	Erişim sağlayıcılar birliğinin temel yapısı ve hukuki kişiliği ne şekildedir?

İÇERİK, YER VE ERİŞİM SAĞLAYICILAR BAKIMINDAN ÖNGÖRÜLEN BİLGİLENDİRME YÜKÜMLÜLÜĞÜ

İnternet ortamındaki yayınlarda düzenin sağlanması bakımından kanun koyucu içerik, yer ve erişim sağlayıcılarına bilgilendirme yükümlülüğü getirmiştir. Söz konusu sağlayıcılar, yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür. Bu bağlamda bahsi geçenler bakımından hem söz konusu bilgileri kullanıcıların ulaşabileceği şekilde bulundurma hem de bunlarda bir değişiklik olursa güncelleme yükümlülüğü getirilmiştir (5651 s. K. m.3/1). Bununla birlikte belirtilen yükümlülüğü yerine getirmeyen sağlayıcılar bakımından iki bin TL'den elli bin TL'ye kadar idari para cezası verilmesi öngörülmüştür. Bu yaptırımı uygulamakla yetkili merci ise başkandır (5651 s.K. m.3/2). Başkanın idari para cezasına karşı 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine kanun yoluna başvurulması da mümkündür (5651 s.K. m.8/12).

Kanun koyucu 5651 s. Kanun kapsamındaki faaliyetleri yurt içi veya yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabileceğini de hükme bağlamıştır (5651 s.K. m.3/3). Dolayısıyla içerik, yer ve erişim sağlayıcılara tanıtıcı bilgileri ulaşılabilir şekilde paylaşma yükümlülüğü getiren kanun koyucu, bu kanun kapsamında faaliyet yürütenlere de internet sayfalarında paylaşılan bilgiler ve sayılan diğer araçlarla bildirim yapılmasına da cevaz vermiştir.

İçerik Sağlayıcının Kullanıma Sunduğu İçerikten Sorumluluğu ve Yükümlülükleri

Kanun koyucu içerik sağlayıcının internet ortamında kullanıma sunduğu her türlü içerikten sorumlu olacağını hükme bağlamıştır (5651 s.K. m.4/1). Burada sadece sorumluluktan bahsettiği için ve cezai sorumluluğu ayrıca vurgulamadığından, cezai alan dışındaki hukuki sorumluluk anlaşılmalıdır. Nitekim suç ve cezada kanunilik ilkesinin (Anayasa m.38/1; TCK m.2) doğal sonucu olarak, bir kimseye cezai sorumluluk yüklenebilmesi fiilin ve cezanın kanunla açıkça düzenlenmesi gereklidir. Bu bağlamda içerik sağlayıcı internet ortamına koyduğu içeriğin hukuki sorumluluğunu taşır. Ancak içeriğin yayınının aynı zamanda suç teşkil etmesi halinde, suçun kast veya taksirle işlenmesine göre, içerik sağlayıcın bu fiili gerçekleştirmekte kast ve taksirinin olup olmadığına bakılmalıdır. Bunun dışında suç teorisinin hata, iştirak gibi kurumlarının uygulanması bakımından da genel kurallara göre hareket edilmelidir.

Bununla birlikte kanun koyucu içerik sağlayıcının, bağlantı sağladığı başkasına ait içerikten sorumlu olmayacağını da hüküm altına almıştır. Bununla birlikte, içerik sağlayıcının bağlantı sağladığı içeriği benimsediği ve kullanıcıların söz konusu içeriğe ulaşmasını amaçladığı, bağlantıyı sunuş biçiminden

açıkça belli ise bu durumda genel hükümlere göre bağlantı sağladığı içerikten de sorumlu olacaktır (5651 s.K. m.4/2) (Özen ve Baştürk, 2011:269).

Ayrıca içerik sağlayıcı, kurumun 5651 sayılı kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında talep ettiği bilgileri, talep edilen şekilde kuruma teslim etmekle ve kurumca bildirilen tedbirleri almakla da yükümlüdür (5651 s.K. m.4/3).

Yer Sağlayıcının Yükümlülükleri

Kanun koyucu yer sağlayıcının, kural olarak yer sağladığı içerik bakımından denetim sorumluluğunun olmadığını kabul etmiştir. Bu bağlamda yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir (5651 s.K. m.5/1). Bununla birlikte 5651 s.K'nın 8. ve 9. maddelerine uygun olarak, yer sağladığı içeriğin hukuka aykırı olduğundan haberdar edilmesi üzerine, söz konusu içeriği yayından çıkarma yükümlülüğü vardır (5651 s.K. m.5/2).

Ayrıca yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla da yükümlü kılınmıştır (5651 s.K. m.5/3). Dolayısıyla içeriğe hangi IP numarasından ulaşıldığı, ne kadar süreyle içeriğe erişimin devam ettiği gibi hususları içeren trafik bilgileri belirtilen süre kadar saklanmalıdır. Nitekim ileride bir suç soruşturması nedeniyle söz konusu içeriklere kimlerin eriştiğinin tespiti CMK m.135/6'ya göre iletişimin tespiti kapsamında istenebilecektir. Bununla birlikte yer sağlayıcı, kurumun talep ettiği bilgileri talep edilen şekilde kuruma teslim etmekle ve kurumca bildirilen tedbirleri almakla yükümlüdür (5651 s.K. m.5/5).

Son olarak belirtmek gerekir ki; yer sağlayıcılık bildiriminde bulunmayan veya 5651 s.K.'da öngörülen diğer yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında, Başkan tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verilmesi de hükme bağlanmıştır. Başkanın bu idari para cezasına karşı, 6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu (İYUK) hükümlerine göre kanun yoluna başvurulması da mümkündür (5651 s.K. m.8/12).

Erişim Sağlayıcının Yükümlülükleri

Yer sağlayıcı da olduğu gibi, erişim sağlayıcının da erişimine aracılık ettiği içeriklerin hukuka uygun olup olmadığını denetleme yükümlülüğünün bulunmadığı 5651 s.K.'da açıkça hükme bağlamıştır. Bu bağlamda, erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir (5651 s.K. m.6/2).

İçeriği denetim yükümlülüğü olmamakla birlikte kullanıcıların internet ortamına girebilmelerine imkân sağlayan erişim sağlayıcılar bakımından da kanun koyucu birtakım yükümlülükler getirmiştir. Bu doğrultuda erişim sağlayıcı (5651 s.K. m.6/1);

a. Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde erişimi engellemekle,

b. Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

c. Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usullere uygun olarak Kuruma teslim etmekle,

ç. Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d. Kurumun talep ettiği bilgileri talep edilen şekilde kuruma teslim etmekle ve kurumca bildirilen tedbirleri almakla yükümlüdür.

Bu sayılanlardan (b), (c) ve (ç) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkan tarafından on bin Türk Lirasından elli bin Türk Lirasına kadar idarî para cezası verileceği hususu da kanunda açıkça düzenleme altına alınmıştır (5651 s.K. m.6/3).

Toplu Kullanım Sağlayıcının Yükümlülükleri

5651 s. K.'da özellikle internet cafeler gibi ticari amaçlı olanlarının giderek yaygınlaştıkları görülen toplu kullanım sağlayıcılara da birtakım yükümlülükler getirilmiştir. Bu doğrultuda ticari amaçlı toplu kullanım sağlayıcıların mahalli mülki amirden izin belgesi almaları zorunlu tutulmuştur. Dolayısıyla il merkezlerinde validen ilçelerde ise kaymakamdan izin alınmadan bu tür faaliyetlerin yürütülmesi hukuka aykırı olacaktır. Bununla birlikte izne ilişkin bilgiler otuz gün içinde mahalli mülki amir tarafından Kuruma bildirilir. Bunların denetimi mahalli mülki amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usuller, yönetmelikle düzenlenir (5651 s.K. m.7/1). Ayrıca ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür (5651 s.K. m.7/2). Görüldüğü üzere bu yükümlülük ticari amaçlı olup olmadığına bakılmaksızın tüm toplu kullanım sağlayıcılar bakımından öngörülmüştür. Bununla birlikte sadece ticari amaçlı toplu kullanım sağlayıcılara yönelik bir yükümlülük daha öngörülmüştür. Buna göre ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür (5651 s.K. m.7/3).

Son olarak belirtmek gerekir ki; yukarıda bahsettiğimiz yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir (5651 s.K. m.7/4).

Öğrenme Çıktısı

2 İçerik, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerini ifade edebilme

Araştır 2	İlişkilendir	Anlat/Paylaş
5651 s. kanunla, içerik, yer ve erişim sağlayıcılar bakımından öngörülen bilgilendirme yükümlülüğünün içeriği nedir?	İçerik, yer, erişim ve toplu kullanım sağlayıcıların yükümlülükleri konusunda ayrıntılı bilgi için bkz. Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara 2014	5651 sayılı kanun kapsamında toplu kullanım sağlayıcıların ne tür yükümlülükleri bulunmaktadır?

İÇERİĞİN ÇIKARTILMASI VE/VEYA ERİŞİMİN ENGELLENMESİ TEDBİRLERİNE İLİŞKİN GENEL AÇIKLAMALAR

5651 s.K.'da dört farklı kapsamda erişimin engellenmesi ve/veya içeriğin çıkartılmasıyla ilgili tedbirlere yer verilmiştir. Bunlardan ilki koruma tedbiri olarak öngörülen erişimin engellenmesi koruma tedbiridir. Bunun dışında önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi tedbiri farklı koşullara bağlı olarak düzenleme altına alınmıştır. Ayrıca kişilik haklarının internet yayınları yoluyla ihlaline bağlı olarak ilgililerin başvurusu üzerine içeriğin çıkartılması ve/veya erişimin engellenmesi hüküm altına alınmıştır. Son olarak aslında kişilik hakları kapsamında yer alan özel hayatın gizliliğinin ihlaline yönelik internet yayınlarına erişimin engellenmesi de ayrıca düzenlemeye tabi tutulmuştur. Kanaatimizce içeriğin çıkartılması ve/veya

erişimin engellenmesi tedbirlerinin bir veya en fazla iki madde kapsamında birleştirilerek düzenlenmesi, kanunun sistematiği açısından daha uygun olacaktır. Mevcut durumda kanun koyucu kendince ortaya çıkan ihtiyaca göre kanunda sürekli değişiklik yaparak yeni maddeler eklemekte ve söz konusu tedbirleri sistematikten yoksun, anlaşılması zor bir biçimde hükme bağlamaktadır. Son yapılan değişikliklerle birlikte, tedbirlerin uygulanması bakımından idari makamların yetkisinin arttırılması, kamuoyunda tepkiyle karşılanmakta, doktrinde de yer yer sert biçimde eleştirilmektedir (Dülger, 2014:757). Bu eleştirilerden bazılarına bizim de katıldığımızı ifade etmek isteriz. Ancak uzaktan öğretime ilişkin hazırlanan bu kitapta, söz konusu tartışmalara girmenin kitabın amacının aşılması sonucunu doğuracağı kanaatiyle, sadece mevcut düzenlemeleri incelemekle yetinmeyi uygun buluyoruz.

İnternet yayınları yoluyla işlenen hukuka aykırılıklarla mücadele gerçekten zordur. Nitekim başlangıç kısmında da belirttiğimiz üzere, internet yayınları vasıtasıyla klasik adalet ve muhakeme anlayışının öngöremediği şekillerde suç işlenmesi veya kamusal düzenin tehlikeye düşürülmesi söz konusu olabilmektedir. Kanun koyucu da çoğu kez bu tehlikeleri karşılaştıkça deneyimlemekte ve buna ilişkin acele düzenlemelere gitmektedir. Ancak ilk fırsatta karşılaştırmalı hukuktaki durum da göz önünde bulundurularak, özellikle bu tedbirlere ilişkin düzenlemelerin daha sistematik bir şekilde ele alınması zorunluluk arz etmektedir.

Erişimin Engellenmesi Koruma Tedbiri

Ceza muhakemesi faaliyeti sırasında, birbiriyle uyuşması zor, iki karşıt menfaatin çatışması söz konusu olur. Bunlardan bir tanesi bireysel özgürlüğe ilişkin menfaat; diğeri ise kamunun genel güvenliğine ilişkin menfaattir. Modern ceza muhakemesi kuralları, muhakeme taraflarının menfaatleri arasında bir değerlendirme yapar ve anayasal ilkeler doğrultusunda, bir taraftan iddia makamına etkin bir takibat gerçekleştirmek suretiyle maddi gerçeği bulmak için gerekli imkânları tanırken, diğer taraftan da sanığın minimum haklarını garanti altına alır. 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 faydalanmakta 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 ön açıklamalar ışığında koruma tedbirlerine ilişkin doktrinde birçok yazarca büyük ölçüde paylaşılan bir tanım yapmak gerekirse; şüpheli veya sanığı ya da bir delili elde etmek, duruşmanın yapılmasını yahut hükmün infazını teminat altına almak amacıyla başvurulan, her birisi bir veya birden fazla temel hakka müdahale teşkil eden muhakeme işlemlerine koruma tedbirleri denilmektedir. Koruma tedbirlerinin ilk göze çarpan özelliği bunların temel haklara müdahale oluşturmalarıdır. Ancak bir muhakeme işleminde sadece bu özelliğin varlığı, o işlemi koruma tedbiri saymaya yetmemektedir. Bunun dışında söz konusu tedbirin yukarıdaki tanımda belirttiğimiz amaçlardan bir veya birkaçını gerçekleştirmeye yönelik olması gerekir. Örneğin arama hem şüpheli veya sanığı hem de bir delili elde etmek amacıyla gerçekleştirilebilen bir koruma tedbiridir. Aynı zamanda arama ile bazı temel haklara da müdahale edilmektedir. Bu bağlamda kişi üzerinde arama yapıldığında Anayasanın 20. maddesinde hüküm altına alınan vücut dokunulmazlığı ve özel hayatın gizliliğine; konutta arama yapıldığında da Anayasanın 22. maddesinde güvence altına alınmış olan konut dokunulmazlığına müdahale edilmiş olur. Tutuklama tedbiri ile sanığın duruşmada hazır bulundurulması veya hükmün teminat altına alınması amaçlanmış olabilir. Nitekim sanığın kaçma tehlikesi varsa onun duruşmada hazır bulundurulması tutuklama vasıtasıyla güvence altına alınabilir. Aynı şekilde mahkûmiyet hükmü kurulduktan sonra sanığın kaçma tehlikesi varsa, hükmen tutukluluğuna karar verilmesi suretiyle, hüküm kesinleşinceye kadar el altında tutulması sağlanabilir. Böylelikle sanığın kaçmasına engel olunarak mahkûmiyet hükmünün infazı teminat altına alınır.

Bu bağlamda belirtmek gerekir ki; kanun koyucu 5651 s.K.'da da internet yayınları yoluyla işlenen suçlarla mücadele adına erişimin engellenmesi koruma tedbirine yer vermiştir. Kanun koyucunun bu uygulamayı koruma tedbiri olarak gördüğü ko-

nusunda tereddüt yoktur. Nitekim 5651 s.K.'nın 8. maddesinin 2. ve 10. fıkrasında bu kurumu açıkça koruma tedbiri olarak nitelendirmiştir. Ancak söz konusu tedbirin klasik bir koruma tedbiri olmadığı da aşikardır. Nitekim söz konusu tedbir diğer koruma tedbirlerinin aksine, sanığı veya bir delili elde etme, sanığı duruşmada hazır bulundurma ya da hükmün infazını teminat altına alma amaçlarına hizmet etmemektedir. Bilakis tedbir internet yoluyla işlendiği düşünülen bazı suçların devamlılığına engel olmaktadır. Örneğin bir internet yayınında intihara yönlendirme söz konusuysa, bu yayına erişimin engellenmesi sayesinde, söz konusu suçun devamlılığına engel olunmuş olmaktadır. Dolayısıyla tedbir, koruma tedbirleri kavramının da yeniden tanımlanması ihtiyacını beraberinde getirmiştir.

Tedbirin Uygulanabilmesi İçin Gerekli Olan Şüphe Derecesi

Kanun koyucu erişimin engellenmesi tedbirine karar verilebilmesi bakımından yeterli şüphe derecesini gerekli görmüştür. Yeterli şüphe, internet ortamında yapılan yayınlarla, kanunda sayılan katalog suçların işlendiği hususunda olmalıdır (5651 s.K. m.8/1). Söz konusu suçların işlenme ihtimali, işlenmemiş olma ihtimalinden fazlaysa, bu durumda söz konusu tedbire başvurulabilmesi bakımından gerekli olan yeterli şüphe derecesine ulaşılmış demektir.

Erişimin Engellenmesi Kararı Verilebilmesi Bakımından Katalog Suçlar

Erişimin engellenmesi tedbirinin uygulanabilmesi, tüm suçlarla ilgili muhakemeler bakımından kabul edilmemiştir. Bu bağlamda internet ortamındaki yayınların içeriğinin kanunda belirtilen suçları oluşturduğuna ilişkin bir muhakeme yürütülüyorsa, erişimin engellenmesi kararı verilebilecektir. Erişimin engellenmesi, temel haklara müdahale teşkil eden bir tedbir olduğundan ve ilgili suçlar kanunda tek tek sayıldığından, bunların kıyas yoluyla genişletilebilmesi mümkün değildir (Any. m.13).

Bu bağlamda, internet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir (5651 s.K. m.8/1):

a. 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;
   1. İntihara yönlendirme (madde 84),
   2. Çocukların cinsel istismarı (madde 103, birinci fıkra),
   3. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
   4. Sağlık için tehlikeli madde temini (madde 194),
   5. Müstehcenlik (madde 226),
   6. Fuhuş (madde 227),
   7. Kumar oynanması için yer ve imkân sağlama (madde 228) suçları.

b. 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

Tedbire Karar Verebilecek Merciler

Erişimin engellenmesi kararı, soruşturma evresinde hakim, kovuşturma evresinde ise mahkeme tarafından verilir. Dolayısıyla tedbire hem soruşturma hem de kovuşturma sırasında başvurulması mümkündür. Bununla birlikte soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. İşlem derhal yapılmadığında sonradan yapılması imkânsız hale gelecekse veya muhakeme bakımından zararlı sonuçlar doğuracaksa, ilgili işlemin yapılmasında gecikmesinde sakınca bulunan hal var demektir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hakimin onayına sunar ve hakim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır (5651 s.K. m.8/2). Bu noktada belirtmek gerekir ki; aşağıda ayrı bir başlık halinde incelemeyi uygun bulduğumuz düzenlemeyle, bu tedbire belirli koşullar altında başkan tarafından da karar verilmesine imkân tanınmıştır. Bu husus ayrıca inceleneceği için burada daha fazla ayrıntıya girmemeyi uygun buluyoruz.

Tedbirin Süresi ve Tedbire Karşı Kanun Yolu

Erişimin engellenmesi kararının uygulanması bakımından kanunda belirli bir süre öngörülmemiştir. Dolayısıyla muhakeme devam ettiği bu tedbirin uygulanması mümkün görünmektedir. Bununla birlikte amacı gerçekleştirebilecek nitelik-

te görülürse, erişimin engellenmesi kararının belirli bir süreyle sınırlı olarak verilmesine de imkân tanınmıştır (5651 s.K. m.8/2).

Hakim veya mahkeme tarafından verilen veya onaylanan tedbire karşı, 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu (CMK) hükümlerine göre itiraz edilebilir (5651 s.K. m.8/2). İtiraz usulü ve itiraz üzerine hangi mercin inceleme yapacağı CMK m.267 vd. maddelerde hükme bağlanmıştır.

Bununla birlikte kanunda kurumun tedbire karşı itiraz yoluna başvurabilmesi imkânı da özel olarak düzenlenmiştir. Buna göre; işlemlerin yürütülmesi için kuruma gönderilen hakim ve mahkeme kararlarına CMK hükümlerine göre kurum tarafından da itiraz edilebilecektir (5651 s.K. m.8/13).

Tedbirin Uygulanması

Hakim, mahkeme veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere kuruma gönderilir. Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir. Başkan tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkan tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur (5651 s.K. m.8/3,5,6).

Soruşturma sonucunda kovuşturmaya yer olmadığı veya kovuşturma sonucunda beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda soruşturma sonunda Cumhuriyet savcısı kovuşturmaya yer olmadığı kararının bir örneğini, kovuşturma sonunda ise mahkeme beraat kararının bir örneğini kuruma gönderir (5651 s.K. m.8/7,8).

Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır (5651 s.K. m.8/10). Görüldüğü üzere kanun koyucu koruma tedbirinin gereğinin yer ve erişim sağlayıcıların sorumluları bakımından, bu davranışı adli, para cezasına tabi bir suç olarak düzenlemiştir. TCK m.52/2 gereğince, en az yirmi ve en fazla yüz Türk Lirası olan bir gün karşılığı adli para cezasının miktarı, kişinin ekonomik ve diğer şahsi halleri göz önünde bulundurularak takdir edilir.

İçeriğin Yayından Çıkartılmasının Tedbire Etkisi

Konusu yukarıda saydığımız katalog suçlardan biri veya birkaçını oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır (5651 s.K. m.8/9). Nitekim artık erişimin engellenmesi tedbirinin uygulanmasına gerek kalmamıştır.

Erişimin Başkan Kararıyla Engellenmesi

Kanunda belirli hallerde erişimin engellenmesi tedbirinin idari bir merci olan Başkanın kararıyla uygulanmasına da imkân tanınmıştır. Buna göre, içeriği katalog suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği çocuğun cinsel istismarı (TCK m.103/1), müstehcenlik (TCK m.226) ve fuhuş (TCK m.227) suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkan tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir (5651 s.K. m.8/4).

Doğrudan Başkan tarafından verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, yine Başkan tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idari para cezası verilir. İdari para cezasının verildiği andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde Kurum tarafından yetkilendirmenin iptaline karar verilebilir (5651 s.K. m.8/11). Başkanın vereceği bu idari para cezasına karşı İYUK hükümlerine göre kanun yoluna başvurulması da mümkündür (5651 s.K. m.8/12).

Bununla birlikte 14/3/2007 tarihli ve 5602 sayılı Şans Oyunları Hasılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3'üncü maddesinin birinci fıkrasının (ç) bendinde tanımlanan kurum ve kuruluşlar (örneğin Milli Piyango İdaresi gibi), kendi görev alanına giren suçların internet ortamında işlendiğini tespit etmeleri halinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilirler. Erişimin engellenmesi kararları uygulanmak üzere kuruma gönderilir (5651 s.K. m.8/14).

Önleme Amaçlı Olarak İçeriğin Çıkartılması ve/veya Erişimin Engellenmesi Tedbiri

Kanun koyucu belirli durumlarda önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi kararı verilebilmesine de imkân tanımıştır. Bu uygulama kapsamında sadece içeriğin çıkartılmasına veya sadece erişimin engellenmesine karar verilebileceği gibi, aynı anda hem içeriğin çıkartılması hem de erişimin engellenmesi kararı verilebilmesi mümkündür. Bunun dışında tedbirin önleme amaçlı uygulanabiliyor olması, yukarıda incelediğimiz erişimin adli amaçlı engellenmesi tedbirinden bu kurumu ayırmaktadır. Bu bağlamda önleme amaçlı uygulanan bu tedbir henüz suç işlenmeden önce uygulanabileceği gibi, suçun işlenmesinden sonra başkaca suçların işlenmesi ihtimali varsa, onları engelleme amaçlı olarak da uygulanabilir. Örneğin suç işlemek amacıyla kurulmuş bir örgüt adına kişilerin bir internet sitesi üzerinden suç işlemeye yönelik haberleştiklerine dair makul sebepler varsa, henüz ortada işlenmiş bir suç olmamasına rağmen internet sitesine erişimin engellenmesine ve/veya bazı içeriklerin çıkartılmasına karar verilebilecektir. Bununla birlikte internet sitesi üzerinden halkı kin ve düşmanlığa tahrik ederek, suç teşkil edecek eylemlerde bulunma çağrısı yapılıyorsa; hem halkı kin ve düşmanlığa tahrik suçu işlenmiş hem de ileride başka suçların işlenecek olması tehlikesi ortaya çıkmış olacaktır. Dolayısıyla bu tür hallerde de tedbirin uygulanması söz konusu olabilecektir.

Tedbire Başvurulmasının Koşulları

Kanun koyucu söz konusu önleme amaçlı tedbire sadece belirli hallerde başvurulmasına imkân tanımıştır. Bu bağlamda tedbir, yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya birkaçına bağlı olarak verilebilecektir (5651 s.K. m.8/A/1). Dikkat edilecek olursa burada gösterilen sebeplerin her birisi koruma ve önlemeye yönelik hususlardır. Bu nedenle tedbirin önleme amaçlı bir tedbir olarak nitelendirilmesi yerinde olacaktır.

Tedbire Karar Verebilecek Merciler ve Tedbirin Uygulanması

Tedbire karar vermeye yetkili merci olarak hakim gösterilmiştir. Dolayısıyla kural olarak önleme amaçlı içeriğin çıkartılmasına ve/veya erişimin engellenmesine hakim karar verebilecektir. Bununla birlikte gecikmesinde sakınca bulunan hallerde başkan da bu tedbire karar vermeye yetkilidir. Ancak başkanın re'sen bu kararı verebilmesi mümkün değildir. Bunun için belirli nedenlere bağlı olarak Cumhurbaşkanlığı veya ilgili bakanlığın talebinin bulunması aranmıştır.

Bu bağlamda, yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hakim veya gecikmesinde sakınca bulunan hâllerde, Cumhurbaşkanlığı veya milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından tedbire karar verilebilecektir (5651 s.K. m.8/A/1). Gecikmesinde sakınca bulunan hallerde yukarıda belirtilen tüm sebeplere bağlı olarak Cumhurbaşkanlığı talepte bulunabilirken; ilgili bakanlıklar sadece milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerine bağlı olarak tedbirin uygulanması talebinde bulunabileceklerdir.

Belirtilen usulle tedbire ilişkin verilen karar, Başkan tarafından derhal erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.

Başbakanlık veya ilgili Bakanlıkların talebi üzerine Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, yine Başkan tarafından, yirmi dört saat içinde sulh ceza hakiminin onayına sunulur. Hakim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar (5651 s.K. m.8/A/2).

Bu kapsamda verilen erişimin engellenmesi kararları, ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir. Ancak, teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi ya-

pılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir (5651 s.K. m.8/A/3). Dolayısıyla kanun koyucu içeriğin sadece ihlalle ilgili kısmına erişimin engellenememesi durumunda, ilgili internet sitesini erişimin tümüyle engellenmesine de imkân tanımıştır.

Bu tedbirin uygulanmasına neden olan suça konu internet içeriklerini oluşturan ve yayanlar hakkında Başkan tarafından, Cumhuriyet Başsavcılığına suç duyurusunda bulunulur. Bu suçların faillerine ulaşmak için gerekli olan bilgiler içerik, yer ve erişim sağlayıcılar tarafından hakim kararı üzerine adli mercilere verilir. Bu bilgileri vermeyen içerik, yer ve erişim sağlayıcıların sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, üç bin günden on bin güne kadar adli para cezası ile cezalandırılır (5651 s.K. m.8/A/4). Bu bağlamda içeriği yayanların fiile iştirak iradeleri söz konusuysa ve iştirak ettikleri suçun cezası belirtilen adli para cezasından daha ağırsa, bu durumda yayan kişinin sadece daha ağır olan suça iştirakten cezai sorumluluğu doğacaktır.

Kanun koyucu ayrıca yukarıda belirtilen usule uygun olarak verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcılar ile ilgili içerik ve yer sağlayıcılara başkan tarafından elli bin Türk lirasından beş yüz bin Türk lirasına kadar idari para cezası verilmesini de hükme bağlamıştır (5651 s.K. m.8/A/5).

Kişilik Haklarının İhlaline Bağlı Olarak İçeriğin Yayından Çıkartılması ve Erişimin Engellenmesi

5651 s.K.'da internet aracılığıyla yapılan yayınlar dolayısıyla kişilik hakları ihlal edilen kişilerin, kanunda gösterilen mercilere başvurarak söz konusu içeriklerin yayından çıkartılmasını veya içeriğe erişimin engellenmesini sağlama imkânı tanınmıştır. Yukarıda açıklanan içeriği çıkarma ve erişimi engelleme tedbirlerinden farklı olarak, bu tedbir kişilik haklarının ihlali iddiasına özel öngörülmüş bir kurumdur.

Bu bağlamda internet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hakimine başvurarak içeriğe erişimin engellenmesini de isteyebilir (5651 s.K. m.9/1). Görüldüğü üzere söz konusu başvurular hem gerçek hem de tüzel kişiler bakımından öngörülmüştür.

İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır. Ayrıca internet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hakim kanunda belirtilen kapsamda erişimin engellenmesine karar verebilir. Hakim, bu bağlamda vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hakim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi halinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir (5651 s.K. m.9/2,3,4). Kanun koyucu öncelikle kişilik haklarını ihlal eden yayına erişimin engellenmesini öngörmüş; ancak bunun mümkün görülmemesi halinde, ilgili internet sitesine erişimin tümüyle engellenmesine karar verilmesine cevaz vermiştir.

Hakim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı CMK m.267 vd. hükümlerine göre itiraz yoluna gidilebilir. Hakimin bu kapsamda verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir. Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hakim kararı kendiliğinden hükümsüz kalır. Görüldüğü üzere kanun koyucu, kişilik haklarını ihlal eden içeriğin yayından çıkartılması halinde, erişimin engellenmesi tedbirinin kaldırılmasına dair yeni bir karar verilmesini aramamış; hakim kararının otomatikman hükümsüz kalacağına hükmetmiştir. Eğer böyle bir çıkarma söz konusu değilse, kendisine gelen hakim tarafından verilmiş erişimin engellenmesi kararı, Birlik tarafından erişim sağlayıcıya gönderilir. Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği ise derhal veya en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir (5651 s.K. m.9/5,6,7,8).

Bu tedbir kapsamında hakimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi halinde mevcut karar bu adresler için de uygulanır (5651 s.K. m.9/9). Dolayısıyla aynı yayını paylaşan diğer internet içeriklerine erişimin engellenmesi için tekrar hakim kararı alınmasına gerek yoktur. Nitekim içeriğin kişilik haklarını ihlal ettiği ve bu içeriğe erişimin engellenmesi gerektiğine hakim tarafından karar verilmiştir. Bu kararı her bir internet sitesindeki içerik için tekrar tekrar aramak yersiz olacaktır. Bu bağlamda kanun koyucunun düzenlemesi yerinde olmuştur.

Son olarak belirtmek gerekir ki; sulh ceza hakiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır (5651 s.K. m.9/10). Görüldüğü üzere kanun koyucu kararın yerine getirilmemesini adli para cezasına tabi kasıtlı bir suç olarak düzenleme altına almıştır.

Özel Hayatın Gizliliğinin İhlali Nedeniyle İçeriğe Erişimin Engellenmesi

Kanun koyucu 5651 s.K.'da internet yayınları yoluyla özel hayatın gizliliğinin ihlal edildiği hallerde erişimin engellenmesine yönelik özel bir tedbire daha yer vermiştir. Aslında özel hayatın gizliliğinin ihlali de, yukarıda incelediğimiz kişilik hakları ihlalini oluşturur. Bir başka deyişle özel hayatın gizliliği de kişilik hakları kapsamında yer alır. Ancak kanun koyucu özel hayatın gizliliğine ilişkin hakkın ihlalini diğer kişilik haklarından ayırarak, ihlaline özel bir tedbir getirmeyi tercih etmiştir. Bu bağlamda internet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir (5651 s.K. m.9/A/1).

Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz. Başkan, kendisine gelen bu talebi uygulanmak üzere derhal Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır (5651 s.K. m.9/A/2,3,4).

Bununla birlikte söz konusu talepte bulunanlar bakımından hakime başvurma zorunluluğu da öngörülmüştür. Aksi takdirde tedbir kendiliğinden kalkacaktır. Bu bağlamda erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hakim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan kuruma gönderir; aksi halde, erişimin engellenmesi tedbiri kendiliğinden kalkar (5651 s.K. m.9/A/5). Hakim tarafından verilen bu karara karşı Başkan tarafından CMK m.267 vd. hükümlerine göre itiraz yoluna gidilebilir (5651 s.K. m.9/A/6).

Ayrıca belirtmek gerekir ki, erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hakim kararı kendiliğinden hükümsüz kalır. Bir başka deyişle, erişimin engellenmesinin kaldırılması için ayrıca karar alınmasına gerek yoktur (5651 s.K. m.9/A/7).

Bununla birlikte özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hallerde doğrudan Başkanın emri üzerine erişimin engellenmesinin kurum tarafından yapılacağı da hükme bağlanmıştır. Bu kapsamda Başkan tarafından verilen erişimin engellenmesi kararı, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hakim, kararını kırk sekiz saat içinde açıklar (5651 s.K. m.9/A/8,9).

dikkat

Aslında özel hayatın gizliliğinin ihlali de, yukarıda incelediğimiz kişilik hakları ihlalini oluşturur. Bir başka deyişle özel hayatın gizliliği de kişilik hakları kapsamında yer alır. Ancak kanun koyucu özel hayatın gizliliğine ilişkin hakkın ihlalini diğer kişilik haklarından ayırarak, ihlaline özel bir tedbir getirmeyi tercih etmiştir.

Yaşamla İlişkilendir

İnternette özel hayatın ifşasına 4 saatte tedbir alınıyor

19.06.2017

Bilgi Teknolojileri ve İletişim Kurumu (BTK), internette özel hayatının ifşa olduğunu öne süren vatandaşın müracaatı üzerine 4 saatte ilgili yayına erişim engeli tedbiri uygulandığına dikkat çekiyor.

İnternet kullanımının yaygınlaşmasıyla siber zorbalar, Twitter ya da Facebook'ta açtıkları sahte hesaplarla başkasına ait kişisel verileri paylaşıyor. Çeşitli yöntemlerle sanal alemde özel hayatının gizliliği ihlal edilen vatandaşlar büyük sıkıntılar yaşayabiliyor. Bilgi Teknolojileri ve İletişim Kurumu (BTK), internette özel hayatının ifşa olduğunu öne süren vatandaşın müracaatı üzerine 4 saatte ilgili yayına erişim engeli tedbiri uygulandığına dikkat çekiyor.

BTK, internet ortamında özel hayatın gizliliğinin ihlali durumunda yapılması gerekenleri kamuoyu ile paylaştı. İnternet ortamında yapılan yayılan içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğini iddia eden kişiler, 5651 sayılı Kanunun 9/A maddesi kapsamında BTK'ya doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebiliyor.

Dilekçede; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilme şartı getirildi. Bu bilgilerin eksik olması halinde talep işleme konulmuyor. Kurum, bu talebi uygulanmak üzere derhal Erişim Sağlayıcıları Birliği'ne bildiriyor. Birlik bu tedbir talebini derhal, en geç dört saat içinde yerine getiriyor. Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bolüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanıyor.

BTK'dan yapılan açıklamada şunlar kaydedildi: "Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan kuruma gönderir. Aksi halde, erişimin engellenmesi tedbiri kendiliğinden kalkar."

Kaynak: http://www.milliyet.com.tr/internette-ozel-hayatin-ifsasina-4-internet-haber-2471074/

Öğrenme Çıktısı

3 Farklı kapsamdaki içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirlerinin uygulanma koşullarını belirleyebilme

Araştır 3

Erişimin engellenmesi koruma tedbirinin uygulanması bakımından kanun koyucu hangi şüphe derecesinin varlığını aramıştır?

İlişkilendir

5651 sayılı kanunda yer alan tedbirlerin anayasal ilkeler çerçevesinde değerlendirildiği özlü bir makale için bkz. Ömer Gedik, "Türkiye'de İnternet Özgürlüğü ve 5651 Sayılı Kanun," Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C.14, S.1-2, 2008

Anlat/Paylaş

5651 sayılı kanunda hangi tür içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirlerine yer verilmiştir?

1 5651 sayılı kanun kapsamındaki temel kavram ve kurumları açıklayabilme

Temel Kavramlar, Kurumun Görevleri ve Erişim Sağlayıcılar Birliği

Modern zamanların en önemli keşiflerinden birisi olan internet insanlığa sağladığı faydalar yanında birçok olumsuzluğu da beraberinde getirmiştir. Dolayısıyla internet insanoğlunun hayatını sadece kolaylaştırmakla kalmamış aynı zamanda asosyalleşme, internet bağımlılığı gibi bazı toplumsal sorunları da beraberinde getirmiştir. Ancak her halükârda modern dönemin bu önemli yeniliğinin insanlık bakımından dezavantajlarına nazaran çok daha büyük avantajlar sağladığı açıktır. Bu nedenle interneti sosyal hayattan çıkarmak mümkün olmadığına göre, onun toplumsal menfaat bakımından getirdiği zararları mümkün olduğunca aza indirmeye gayret etmelidir. İnternetin toplumsal menfaat bakımından ortaya çıkardığı en önemli dezavantajlardan birisi yeni suç işleme yöntemlerine imkân tanıması ve ortaya çıkardığı yeni bireysel menfaatlere bağlı olarak yeni suç biçimlerinin ortaya çıkması olarak sayılabilir. Bundan birkaç yüzyıl önceki insanların hayal bile edemediği yeni imkânlar ve haklar ortaya çıkartan internet, bireysel haklara karşı işlenecek suçlarda önemli bir araç haline de gelebilmektedir.

Bu bağlamda internet yoluyla işlenen suçlarla mücadele adına kanun koyucunun da birtakım özel düzenlemeler yapması kaçınılmazdır. Bu gereklilikler karşısında kanun koyucumuz da internet yayınları yoluyla işlenen suçlarla mücadele adına özel bir kanun düzenlemesi yapmıştır. 23.05.2007 tarihli ve 5651 sayılı bu kanunun ismi; İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanundur.

5651 s. Kanunun 2. maddesinde kanunda geçen bazı kavramların tanımlanması yoluna gidilmiştir. Böylelikle kanun koyucu içeriği konusunda tereddüte düşülebilecek bazı kavram ve terimlerden ne anlaşılması gerektiğini açıklığa kavuşturmak istemiştir. Bu bağlamda Bakanlık, Başkanlık, Erişim, Veri gibi birtakım terimlerin tanımlarına söz konusu kanunun 2. maddesinde yer verildiği görülmektedir.

5651 s.K.'nın 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur. Söz konusu birlik, özel hukuk tüzel kişiliğini haizdir ve birliğin merkezi Ankara'dır (5651 s.K. m.6/A/2). Birlik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılmasıyla oluşan ve koordinasyonu sağlayan bir kuruluştur (5651 s.K. m.6/A/5). 5651 s. K.'nın 8. maddesi kapsamı dışındaki erişimin engellenmesi kararları erişim sağlayıcılar tarafından yerine getirilir.

2 İçerik, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerini ifade edebilme

İçerik, Yer ve Erişim Sağlayıcılar Bakımından Öngörülen Bilgilendirme Yükümlülüğü

Kanun koyucu internet ortamındaki yayınlarda düzenin sağlanması bakımından öncelikle içerik, yer ve erişim sağlayıcılara bilgilendirme yükümlülüğü getirmiştir. Bu bağlamda söz konusu sağlayıcılar, yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür. Bu bağlamda söz konusu sağlayıcılar bakımından hem bahsi geçen bilgileri kullanıcıların ulaşabileceği şekilde bulundurma hem de bunlarda bir değişiklik olursa güncelleme yükümlülüğü getirilmiştir (5651 s. K. m.3/1).

Kanun koyucu içerik sağlayıcının internet ortamında kullanıma sunduğu her türlü içerikten sorumlu olacağını hükme bağlamıştır (5651 s.K. m.4/1). Burada sadece sorumluluktan bahsettiği için ve cezai sorumluluğu ayrıca vurgulamadığından, cezai alan dışındaki hukuki sorumluluk anlaşılmalıdır. Nitekim suç ve cezada kanunilik ilkesinin (Anayasa m.38/1; TCK m.2) doğal sonucu olarak, bir kimseye cezai sorumluluk yüklenebilmesi fiilin ve cezanın kanunla açıkça düzenlenmesi gereklidir. Bu bağlamda içerik sağlayıcı internet ortamına koyduğu içeriğin hukuki sorumluluğunu taşır. Ancak içeriğin yayınının aynı zamanda suç teşkil etmesi halinde, suçun kast veya taksirle işlenmesine göre, içerik sağlayıcın bu fiili gerçekleştirmekte kast ve taksirinin olup olmadığına bakılmalıdır. Bunun dışında suç teorisinin hata, iştirak gibi kurumlarının uygulanması bakımından da genel kurallara göre hareket edilmelidir.

Kanun koyucu yer sağlayıcının, kural olarak yer sağladığı içerik bakımından denetim sorumluluğu olmadığını kabul etmiştir. Bu bağlamda yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir (5651 s.K. m.5/1). Bununla birlikte 5651 s.K'nın 8. ve 9. maddelerine uygun olarak, yer sağladığı içeriğin hukuka aykırı olduğundan haberdar edilmesi üzerine, söz konusu içeriği yayından çıkarma yükümlülüğü vardır (5651 s.K. m.5/2).

Yer sağlayıcı da olduğu gibi, erişim sağlayıcının da, erişimine aracılık ettiği içeriklerin hukuka uygun olup olmadığını denetleme yükümlülüğünün bulunmadığı 5651 s.K.'da açıkça hükme bağlamıştır. Bu bağlamda, erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir (5651 s.K. m.6/2).

5651 s. K.'da özellikle internet cafeler gibi ticari amaçlı olanlarının giderek yaygınlaştıkları görülen toplu kullanım sağlayıcılara da birtakım yükümlülükler getirilmiştir. Bu doğrultuda ticari amaçlı toplu kullanım sağlayıcıların mahalli mülki amirden izin belgesi almaları zorunlu tutulmuştur. Dolayısıyla il merkezlerinde validen ilçelerde ise kaymakamdan izin alınmadan bu tür faaliyetlerin yürütülmesi hukuka aykırı olacaktır. Bununla birlikte izne ilişkin bilgiler otuz gün içinde mahalli mülki amir tarafından Kuruma bildirilir. Bunların denetimi mahalli mülki amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usuller, yönetmelikle düzenlenir (5651 s.K. m.7/1). Ayrıca ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür (5651 s.K. m.7/2).

3 Farklı kapsamdaki içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirlerinin uygulanma koşullarını belirleyebilme

İçeriğin Çıkartılması ve/veya Erişimin Engellenmesi Tedbirlerine İlişkin Genel Açıklamalar

Bu noktada belirtmek gerekir ki; 5651 s.K.'da dört farklı kapsamda erişimin engellenmesi ve/veya içeriğin çıkartılmasıyla ilgili tedbirlere yer verilmiştir. Bunlardan ilki koruma tedbiri olarak öngörülen erişimin engellenmesi koruma tedbiridir. Bunun dışında önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi tedbiri farklı koşullara bağlı olarak düzenleme altına alınmıştır. Ayrıca kişilik haklarının internet yayınları yoluyla ihlaline bağlı olarak ilgililerin başvurusu üzerine içeriğin çıkartılması ve/veya erişimin engellenmesi hüküm altına alınmıştır. Son olarak aslında kişilik hakları kapsamında yer alan özel hayatın gizliliğinin ihlaline yönelik internet yayınlarına erişimin engellenmesi de ayrıca düzenlemeye tabi tutulmuştur.

neler öğrendik?

1 İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilere ne ad verilir?

A. Yer sağlayıcı
B. Toplu kullanım sağlayıcı
C. Erişim sağlayıcı
D. Fiziksel sağlayıcı
E. İçerik sağlayıcı

2 İnternet ortamında yapılan yayınların içeriklerini izleyerek, 5651 s. Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak yine 5651 s. Kanunda öngörülen gerekli tedbirleri almak aşağıdakilerden hangisinin görevidir?

A. Kurum
B. Bakanlık
C. Yer sağlayıcı
D. Erişim sağlayıcılar birliği
E. Cumhurbaşkanlığı

3 Aşağıdakilerden hangisi 5651 s. Kanunun 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere kurulmuştur?

A. Erişim Sağlayıcıları Birliği
B. Bilgi Teknolojileri ve İletişim Kurumu
C. Yer Sağlayıcılar Birliği
D. İçerik sağlayıcılar Birliği
E. Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı

4 Yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait inter-net ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurma yükümlülüğünü ihlal eden yer sağlayıcılar bakımından hangi tür bir hukuki yaptırım öngörülmüştür?

A. İdari para cezası
B. Adli para cezası
C. Hapis cezası
D. Müsadere
E. Sürgün

5 Ticari amaçlı toplu kullanım sağlayıcıların faaliyette bulunabilmeleri için aşağıdaki mercilerin hangisinden izin almaları gerekir?

A. Ulaştırma ve Altyapı Bakanlığı
B. Belediye başkanından
C. Emniyet Müdürlüğünden
D. Bilgi Teknolojileri ve İletişim Kurumundan
E. Mülki amirden

6 Erişimin engellenmesi koruma tedbirine başvurulabilmesi bakımından kanun koyucu katalog suçların işlendiği hususunda en az aşağıdaki şüphe derecesinden hangisine ulaşmış olmalıdır?

A. Basit şüphe
B. Makul şüphe
C. Yeterli şüphe
D. Kuvvetli şüphe
E. Kesin şüphe

7 Aşağıdakilerden hangisi erişimin engellenmesi koruma tedbirine karar verilebilmesi bakımından internet yayını içeriğinin oluşturması gereken katalog suçlardan biridir?

A. Soykırım
B. İntihara yönlendirme
C. Görevi kötüye kullanma
D. Rüşvet
E. Sahtecilik

8 Aşağıdakilerden hangisi önleme amaçlı olarak içeriğin çıkartılması veya erişimin engellenmesi tedbirine başvurma nedenlerinden biri **değildir?**

A. Milli güvenlik ve kamu düzeninin korunması
B. Suç işlenmesinin önlenmesi
C. Yaşam hakkının korunması
D. Genel Sağlığın korunması
E. Suç faillerinin yakalanması

9 Aşağıdakilerden hangisi normal şartlarda önleme amaçlı olarak içeriğin çıkartılması veya erişimin engellenmesi tedbirine karar verecek mercilerden biridir?

A. Hakim
B. C. Savcısı
C. Ulaştırma Bakanlığı
D. Bilgi Teknolojileri ve İletişim Kurumu
E. Başbakanlık

10 Gecikmesinde sakınca bulunan hallerde, özel hayatın gizliliğinin ihlali nedeniyle, içeriğe erişimin engellenmesi tedbirinin uygulanması bakımından doğrudan emir verme yetkisine sahip olan merci aşağıdakilerden hangisidir?

A. Başkan
B. Ulaştırma Bakanı
C. Başbakan
D. Erişim Sağlayıcılar Birliği
E. Cumhurbaşkanı

neler öğrendik yanıt anahtarı

1. E	Yanıtınız yanlış ise "Temel Kavramlar" konusunu yeniden gözden geçiriniz.
2. A	Yanıtınız yanlış ise "Bilgi Teknolojileri ve İletişim Kurumunun Görevleri" konusunu yeniden gözden geçiriniz.
3. A	Yanıtınız yanlış ise "Erişim Sağlayıcıları Birliği" konusunu yeniden gözden geçiriniz.
4. A	Yanıtınız yanlış ise "İçerik, Yer ve Erişim Sağlayıcılar Bakımından Öngörülen Bilgilendirme Yükümlülüğü" konusunu yeniden gözden geçiriniz.
5. E	Yanıtınız yanlış ise "Toplu Kullanım Sağlayıcının Yükümlülükleri" konusunu yeniden gözden geçiriniz.
6. C	Yanıtınız yanlış ise "Erişimin Engellenmesi Koruma Tedbiri" konusunu yeniden gözden geçiriniz.
7. B	Yanıtınız yanlış ise "Erişimin Engellenmesi Koruma Tedbiri" konusunu yeniden gözden geçiriniz.
8. E	Yanıtınız yanlış ise "Önleme Amaçlı Olarak İçeriğin Çıkartılması ve/veya Erişimin Engellenmesi Tedbiri" konusunu yeniden gözden geçiriniz.
9. A	Yanıtınız yanlış ise "Önleme Amaçlı Olarak İçeriğin Çıkartılması ve/veya Erişimin Engellenmesi Tedbiri" konusunu yeniden gözden geçiriniz.
10. A	Yanıtınız yanlış ise "Özel Hayatın Gizliliğinin İhlali Nedeniyle İçeriğe Erişimin Engellenmesi" konusunu yeniden gözden geçiriniz.

5 Araştır Yanıt Anahtarı

Araştır 1

İnternet, insanoğlunun hayatını birkaç yüzyıl önce hayal dahi edilemeyecek kadar kolaylaştıran ve rahatlatan yeniliklerdendir. Bununla birlikte kolaylığı ve rahatlığı sadece insanlığın menfaatine olan hususlarda değil, suçluluğun ve yeni suç işleme yöntemlerinin yaygınlaşması gibi aleyhine olan hususlarda da sağlamaktadır. Bu bağlamda internet salt iyi ya da salt kötü değildir. Ancak her halükârda sağladığı avantajlar, dezavantajlarına nazaran çok daha fazladır.

Araştır 2

İnternet ortamındaki yayınlarda düzenin sağlanması bakımından kanun koyucu içerik, yer ve erişim sağlayıcılarına bilgilendirme yükümlülüğü getirmiştir. Söz konusu sağlayıcılar, yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür. Bu bağlamda bahsi geçenler bakımından hem söz konusu bilgileri kullanıcıların ulaşabileceği şekilde bulundurma hem de bunlarda bir değişiklik olursa güncelleme yükümlülüğü getirilmiştir (5651 s. K. m.3/1).

Araştır 3

Kanun koyucu CMK'da hükme bağlanan diğer birçok koruma tedbiri gibi, 5651 s. Kanunla düzenlenen erişimin engellenmesi koruma tedbirine başvurulabilmesi bakımından da belirli bir şüphe derecesinin varlığını zorunlu kabul etmiştir. Bu bağlamda erişimin engellenmesi tedbirine karar verilebilmesi bakımından yeterli şüphe derecesine ulaşılmış olması gerekir. Yeterli şüphe, internet ortamında yapılan yayınlarla kanunda sayılan katalog suçların işlendiği hususunda olmalıdır (5651 s.K. m.8/1). Söz konusu suçların işlenme ihtimali, işlenmemiş olma ihtimalinden fazlaysa, bu durumda söz konusu tedbire başvurulabilmesi bakımından gerekli olan yeterli şüphe derecesine ulaşılmış demektir. Bu şüphenin oluşup oluşmadığını belirlemede kullanılacak yegâne gösterge ise eldeki delil miktarı olacaktır.

Kaynakça

Dülger, M. V. (2014). Bilişim Suçları ve İnternet İletişim Hukuku. Ankara.

Gedik, Ö. (2008). Türkiye'de İnternet Özgürlüğü ve 5651 Sayılı Kanun. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 14, ss.1-2.

Özen, M. ve Baştürk, İ. (2011). Bilişim-İnternet ve Ceza Hukuku. Ankara.

Bölüm 6

E-Ticaret

Öğrenme çıktıları

Elektronik Ortamda Sözleşmeler

1 Sözleşme kavramının elektronik ortamda ne anlama geldiğini açıklayabilme

2 Sözleşmelerde dikkat edilmesi gereken noktaların ne olduğunu sıralayabilme

3 Sözleşmelerin nasıl yapılması gerektiğini ifade edebilme

Elektronik Ortamda Reklamlar

4 Elektronik reklamları betimleyebilme

Elektronik Ortamda Haksız Rekabet

5 Haksız rekabetin yeni formlarını sıralayabilme

Anahtar Sözcükler: • İrade Açıklamaları • Sözleşmeden Dönme • Tüketici • Mesafeli Satım • Cayma • Elektronik İmza • Spam

GİRİŞ

İnsanoğlunun var olduğu günden bu yana hayatını devam ettirmek için yaptığı ilk işlemlerin **sözleşme** olduğu kabul edilir. Sözleşme kavramı öylesine derin ve güçlü bir anlama sahiptir ki bazı düşünürler, devletin kuruluşunu ve meşruiyetini dahi sözleşmelere dayandırır. Sözleşme, yüzyıllar öncesinde var olduğu gibi yüzyıllar sonrasında dahi var olacak en tipik bir hukuki işlemdir. Sözleşme, hayatın vazgeçilmez unsuru olduğu gibi hukukun da vazgeçilmez kavramıdır. En genel tanımı ile sözleşme, belirli bir hukuki sonuç doğurmaya yönelmiş olan iki veya daha fazla tarafın birbirine uygun karşılıklı irade beyanlarından oluşan hukuki bir işlemdir. Her gün belki de hiç konuşmadan gazete almamız sözleşme olduğu gibi bir ev kiralamamız ya da bir konser bileti satın almamız da bir sözleşmedir.

Bu bölümde, elektronik ortamda sözleşmeler, reklamlar ve haksız rekabet konuları ele alınacaktır.

ELEKTRONİK ORTAMDA SÖZLEŞMELER

Elektronik ortam, insan hayatının vazgeçilmezi olan sözleşmeler alanını da etkilemiştir. Daha önce yüzyüze kurulan sözleşmeler, kitle iletişim araçları ile de kurulabilmeye başlanmıştır. İnsana, zaman kazandıran daha karşılaştırılabilir sözleşme seçenekleri sunan bu ortam çoktan gündelik hayatın bir parçası olmuştur. İnternetten yemek veya çiçek sipariş etmek, seyahat ya da konser bileti almak sıklıkla yapılan bir hukuki işlemdir, yani sözleşmedir. Elektronik ortamda kurulan bu sözleşmelerin sayısının giderek artacağını söylemek hiç yanlış olmaz.

dikkat

Elektronik ortamda sözleşmelerin avantajları şunlardır:
1. Zamandan tasarruf
2. Kolay karşılaştırma
3. Mal ve hizmetlere kolay ulaşım
4. Mesafelerin engel olmaktan çıkması

Gündelik hayatta 'bir tık ötede sloganı' ile elektronik ortamda sözleşme kurulması için teşvik edilmekteyiz. Ürün ya da hizmete ilişkin bütün özellikleri web sayfasında görmek, hatta yorumları okumak, elektronik ortamdaki sözleşmelerin kurulmasını kolaylaştırmaktadır. Hatta sözleşme kurmak isteyenlere yardımcı olmak ve mal ve hizmet sunanları derecelemek ve puanlamak için yeni sivil kurumlar ortaya çıkmaktadır. Yine sözleşmelerin kurulmasında ya da ifa aşamasında şikayetlerimizi iletebileceğimiz birçok yeni kurumla karşılaşmaktayız. Bütün bu açıklamalarımız, esasen yeni dönemin, yani diğer deyişle sanal alemin yeni kavram ve kurumlarını daha görünür kılmak içindir.

dikkat

Türkiye'de e-ticaret hacminin yıllara göre büyüme oranları şu şekildedir:
2009-2010: %40,61,
2010-2011: %46,32,
2011-2012: %34,35,
2012-2013: %37,44,
2013-2014: %35

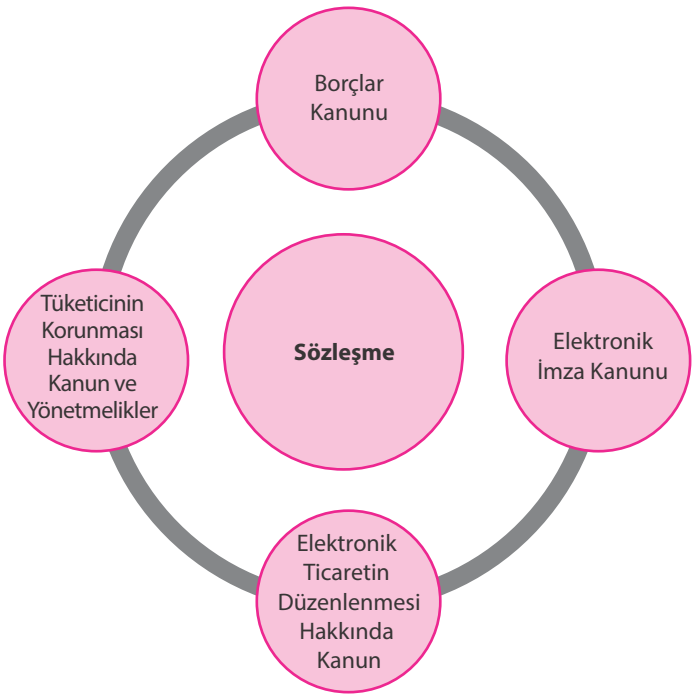
Elektronik ortamda bir sözleşmenin kurulması sırasında şu şemadaki aşamalar yaşanır. Elbette bu türden sözleşmelerde –aşağıda açıklanacağı üzere– bu şemada bulunan bütün aşamalar yer almayabilir. Bu örnek bir e-sözleşme sürecidir.

E-Sözleşme
Taraf iradelerinin elektronik ortamda yani yüz yüze gelmeksizin karşılaştığı ve uyuştuğu elektronik ortamda kurulmuş sözleşmelerdir.

Şekil 6.1

Bizler, bir ürünü ya da hizmeti bir web sayfasında ya da bir online markette beğeniriz. Ancak hâlen bizler bu sayfanın ve bu sayfada yapılan ticaretin güvenilirliği konusunda tereddütler yaşarız. Bu durumda irademizin oluşumunda bize yardımcı olacak iki farklı açıklama bulunur. Bunlardan ilki, ürünün reklamının ya da sunumunun yapıldığı sayfanın açıklamaları, diğeri ise bunlardan bağımsız kullanıcı yorumları, şikâyet sitesinde yazılanlar yahut bazı sivil derecelendirme ya da puanlama kuruluşlarıdır. İrademiz bu şekilde ürün ve hizmetin niteliği ve fiyatı hakkında oluştuktan sonra irademizi beyan da etmemiz gerekir ki bunun akabinde sözleşme kurulmuş olur. Sözleşme kurulduktan sonra, mal ya da hizmetin ifa edilmemesi, vaat edildiği gibi çıkmaması ya da gecikme hâlinde devreye yasalardaki koruyucu düzenlemeler ya da şikâyet siteleri girer. Esasen bu sistemlerde eksik olan, online uyuşmazlık çözüm merkezleridir. Bu merkezler mahkemeye gitmeksizin taraflar arasında meydana gelen uyuşmazlıkların daha dostane çözümlenmesi uğraşısıdır. Sözleşme kurmaya yönelmiş irade beyanlarının birbiri ile uyuşması gerekir. Sözleşme hukukunda öneri ve kabul şeklinde tanımlanan iki irade beyanı, birbirine yönelmiş irade beyanlarının genel tanımıdır.

Elektronik Ortamda Yapılan Sözleşmelerin Yasal Çerçevesi



Şekil 6.2 Elektronik ortamda yapılan sözleşmelerin yasal çerçevesi

Elektronik ortamda kurulan bir sözleşmeye uygulanacak olan çok sayıda yasal düzenleme bulunmaktadır. Sözleşmenin kurulmasına ilişkin temel düzenlemeler Borçlar Kanunu'nda yer almakla birlikte, başkaca düzenlemeler de sözleşmenin kuruluşunda göz önünde bulundurulmalıdır. Bunlar aşağıda bir şekil hâlinde verilmiştir.

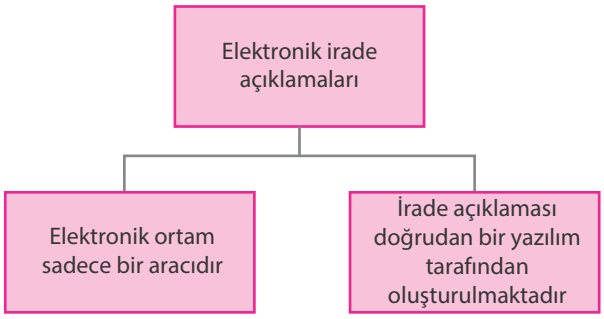
Sözleşmenin kurulması için gerekli irade açıklamaları, irade açıklamalarının sonuçları, irade açıklamalarından dönebilme imkânları, irade açıklamalarındaki sakatlıklar Borçlar Kanunu'nda düzenlenmiştir. Kanunlarda sözleşmelerin şekil şartına tabi tutulabilmesi mümkündür. Adi yazılı şekil şartı varsa elektronik ortamda kurulan sözleşmelerde şekil şartının tamamlanabilmesi için güvenli elektronik imzaya ihtiyaç duyulacaktır. Güvenli elektronik imzaya ilişkin düzenlemeler ise Elektronik İmza Kanunu'nda düzenlenmiştir.

Sözleşmenin taraflarından birinin tüketici olması durumunda, sözleşmenin kurulması ve sözleşmeden caymaya ilişkin özel düzenlemeler ise Tüketicinin Korunması Hakkında Kanun ve ilgili Yönetmeliklerde yer almaktadır. Elektronik ortamda sözleşmeleri etkileyen bir diğer düzenleme ise Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'dur. Bu düzenlemeler yanında sözleşmelerin türüne göre farklı yasal düzenlemelerin uygulama alanı bulabilmesi de mümkündür.

Sözleşmelerin Kurulmasında İrade Açıklamaları

Bilindiği üzere BK m. 1'e göre sözleşme, tarafların birbirine uygun ve karşılıklı irade açıklamaları ile kurulur. İrade açıklamalarının elektronik ortamda yapılması mümkündür. İrade beyanının elektronik ortamda yapılmış olması, sözleşmelerin Borçlar Kanunu'nda düzenlenen prensiplerden daha farklı prensiplere tabi kılınmasını gerektirmez. İrade açıklamalarının elektronik ortamda yapılması, seçilen iletişim yolunun farklılaşmasının getirdiği birtakım farklı hukuki sonuçların olması tabiidir. Elektronik ortamda yapılan irade açıklamalarına hukukun ne tür sonuçlar bağladığı önem kazanmaktadır. Bu nedenle bu tür işlemlerin yakından ele alınıp değerlendirilmesi gerekmektedir.

Elektronik ortamda gerçekleşen irade açıklamaları kendi içinde ikiye ayrılarak incelenmiştir. Bunlardan ilkinde elektronik ortam sadece bir aracıdır. Diğerinde ise iradenin oluşumunda bir insan iradesi olmaksızın bir bilgisayar yazılımı tarafından irade açıklaması yapılmaktadır.



Şekil 6.3 Elektronik irade açıklamaları türleri

Bir kimsenin sözleşme kurmaya yönelmiş olan irade açıklaması, chat, skype, facebook sohbeti veya elektronik posta ile yapılabilir. Ya da bir web sayfasında 'fare' yardımı ile bir sözleşmenin kabul edilmesi gibi. Bu tür irade beyanlarında elektronik ortam, sadece bir aracıdır. Esasen bu türden yapılan irade açıklamalarının benzerleri, önceki teknolojide telefon ya da telsiz aracılığı ile yapılan irade açıklamasından pek de farklı değildir.

İkinci tür elektronik irade açıklamasını diğer irade açıklamalarından ayıran husus, öncelikle irade açıklamasının yapılması ile onun karşı tarafa ulaşması sırasında aktif bir insani eylemin bulunmayışıdır. Bir web sayfasında sözleşmenin kurulması için adım adım yapılan işlemlerden sonra, örneğin bir uçak biletinin satın alınmasında, hava yolu şirketinin sistemi, bir insan yardımı olmaksızın bileti oluşturmakta ve kredi kartımızdan da parayı tahsil etmektedir. İşte hava yolu şirketinin açıklamaları, bir insan iradesi mi yoksa bir makine iradesi midir? Ancak belirtelim ki bilgisayar açıklaması ya da otomatik irade açıklaması olarak da isimlendirilebilecek elektronik irade açıklaması, aslında irade açıklamasının usulü ile ilgilidir. Bilgisayar yazılımını oraya koyan ve yerleştiren irade, genel olarak irade beyanı bulunmak arzu ve niyetindedir. Yani diğer bir ifade ile bilgisayar yazılımını hazırlayan sunucu, genel nitelikteki bir fiili iradesini ortaya koymuştur. Burada sadece bilgisayarın kullanıcısı, makinesini irade açıklamalarının aracı olarak kullanmaktadır. Aslında klasik anlamda elektronik irade açıklaması, sadece bir bilgisayar programı veya bir diğer iletişim aracı vasıtası ile yapılmış bir irade açıklamasından başka bir şey değildir.

Doğrudan makineler ve yazılımlar tarafından oluşturulan elektronik irade açıklamasının nasıl nitelendirileceği hukukçular arasında tartışılmıştır. Burada Amerikan hukukundaki 'elektronic agent' kavramına da temsil kavramına da gitmeye gerek yoktur. Bir irade açıklaması bir insan tarafından yapılmalıdır ve hukuki bir etki ortaya çıkarmaya yönelik bir beyan olmalıdır. Elektronik irade beyanı, ister elektronik ortam kullanılarak yapılsın isterse bilgisayar üzerinde yazılmış bir program aracılığıyla karşı tarafa açıklansın, kanaatimizce sonuç değişmemektedir ve irade beyanları gerçekte bir insan iradesine dayanmaktadır. Bu nedenle elektronik irade açıklamaları geçerli bir irade beyanı olarak kabul edilir.

Elektronik irade beyanının etkili olabilmesi için irade açıklamasını yapan kimsenin irade beyanını karşı tarafa göndermesi, bunu yaparken de genel ilkelere göre gönderenin yapması gereken her şeyi yerine getirmesi gerekir.

İrade Açıklamalarının Tasnifi: Öneri ve Kabul

İrade açıklamalarından sözleşmenin kurulması için esaslı unsurları içeren ve muvafakat edildiği takdirde sözleşmenin meydana gelmesini sağlayan nitelikteki irade açıklaması öneri olarak adlandırılır. Öneri bir kişiye yapılabileceği gibi birden fazla kişiye de yapılabilir. Bu çerçevede web sayfalarında bulunan ilanların nasıl niteleneceği tartışılmalıdır.

İrade açıklamaları bakımından İnternet ortamındaki sunumlar nasıl değerlendirilecektir? Yani bir web sayfasında bulunan mal ya da hizmetin teşhiri, açık artırmaya çıkarılan bir ürün sunumu, nasıl bir irade açıklamasıdır? Bunları hukuken nasıl nitelemeliyiz?

Web sayfaları, İnternet'te önemli bir sunum imkânlarıdır. World Wide Web olarak tanınan "(www)"de e-posta, haber ve Ftp gibi İnternet ortamının parçasıdır. Bu web sayfasının teknik olarak hazır tutulması, Hyper Text Markup Languge Standart (HTML) ve Hyper Text Transfer Protocol (HTTP) yoluyla tanımlanır. Bunlar, mal ve hizmetlerin yazı veya grafik form içinde sunulmasını mümkün kılmaktadır. Bunlardan başka HTML/HTTP diğer İnternet hizmetlerinin sağlanmasını da mümkün kılmakta ve kullanıcıya sistemde bir adresin verilmesi suretiyle herhangi bir sayfayı görme imkânı da verilmektedir.

Bu tür web sayfaları zamanla mal ve hizmetlerin sunulduğu bir pazar hâline gelmiştir. Çoğunlukla bunlara online sipariş verme fonksiyonları da ilave edilmiştir. Burada bu tür sayfaların bağlayıcı olmayan bir öneri mi yoksa herkese açık öneri mi (BK.m.8) olduğu sorusu karşımıza çıkmaktadır. Bu sorunun cevabı her şeyden önce sunumların objektif açıklama değerine bağlıdır. Bir mahkeme kararında kataloglar, fiyat listeleri, özel kartlar ve benzerleri "herkese açık öneri" olarak nitelendirilmişlerdir. Bilgisayar ekranında görüntü olarak malların sunumlarında da aynı durum geçerli olmalıdır. Çünkü herkese açık öneri kurumu özellikle mal ve hizmetlerin sunucusunu korumaktadır. Zira sunmuş olduğu mal ve hizmetler için ne kadar kimsenin kendisiyle sözleşme yapacağı belli değildir. Belirsiz bir sayıda sözleşme yapmak isteyen kimselerin taleplerini de öneri sahibinin karşılaması mümkün olmayabilir.

Hukuk camiasında metro istasyonlarında ya da okul kantinlerinde bulunan mal otomatlarındaki satımlarda mevcut olan tartışmanın bir benzerine internet yoluyla kurulan sözleşmelerde de rastlamak mümkündür. Acaba mal otomatında öneri ve kabul nasıl belirlenecektir? Burada büyük çoğunluğun fikrine göre, otomatın kurulması, otomatın çalışabilirliği ve içinde mal bulunması belirli şartlar altında otomatın kurucusu için belirli olmayan bir kişiye yöneltilen "ad incertas personas" öneri olarak kabul edilir. Makineyi kuran bir kabul beyanında bulunmamıştır. Fakat karşı ve kanaatimizce daha haklı bir görüşe göre makinenin kurulması sadece herkese açık bir öneridir. Bu tür irade faaliyeti ile öneri gerçekleşmekte, paranın atılması ile de kabul gerçekleşmektedir. İnternet üzerinden yapılan sözleşmelerde icap ve kabulün belirlenebilmesinde de aynı yol izlenebilir.

Web sayfaları, birbirinden farklı niteliktedirler. Bazı web sayfalarında sadece mal ve hizmetler sunulmakta fakat bunların sipariş edilmesi fonksiyonu bu sayfalarda bulunmamaktadır. Bu mal ve hizmetlerin siparişi ise İnternet üzerinden yapılamamaktadır. Bu sayfalar tam bir öneriye davet olarak görülmelidir. Çünkü burada sadece reklamların bir türü söz konusudur.

Web sayfalarında şayet mal ve hizmetler hakkında ayrıntılı bilgi mevcut değilse ve İnternet kullanıcısı bunlar hakkında somut bir veriye ulaşamıyorsa bunların hukuki olarak bir icap olarak kabul edilmesi mümkün olmaz. Evlere gönderilen katalog ve televizyon satış reklam yayınlarında da alıcı, sunulan mal ve hizmetler hakkında somut bilgilere ulaşamamakta fakat telefon aracılığı ile siparişlerde bulunabilmektedir. Dolayısıyla sadece sipariş fonksiyonunun web sayfasında bulunması onun "öneriye davet" özelliğini değiştirmez.

İnternet üzerinden pazarlaması yapılan malların çeşidine göre bir ayrım yapmak da gerekecektir. "Herkese yapılan öneri" kurumu, sunucuyu, kendisine yönelen çok sayıda talep karşısında korumaktadır. Burada öneri sahibi, sadece mevcutları kadar sözleşme yapmak isteyenlerin talepleri ile bağlı bulunmaktadır. Fakat bu koruma sadece maddi bir cisme sahip mallar için geçerli olabilir. Yoksa maddi bir cisme sahip olmayan mal ve hizmetlerde böyle bir sonuca ulaşmak doğru olmaz. Örneğin dijital ortamda kaydedilmiş metinler, resimler, yazılım programları İnternet üzerinden kural olarak istenildiği kadar alıcıya teslim edilebilir. Burada teorik olarak bu tür mallar, sınırsız bir müşteri kitlesine sunulma kabiliyetine sahiptir. İnter-

net üzerinden mal sunumunda bulunan kimsenin "herkese yapılan öneri" kurumu ile korunmasına ihtiyaç yoktur. Bu tür sayfalar da otomatların bir türü olarak düşünülebilir. Bu tür otomatlarda hazır tutulan liste, bir öneridir.

Elektronik Ortamda Açık ve Örtülü İrade Açıklaması

Borçlar Kanunu, irade açıklamasının açık ya da örtülü olabileceğini söylemektedir (m. 1/2). Ancak bilişim sistemlerinde bir irade açıklamasından bahsedebilmek için kural olarak açık bir irade açıklamasına ihtiyaç olduğu söylenebilir. Borçlar Kanunu, örtülü kabulü, belirli bir süre susmaya veya başka bir deyişle reddetmeme hâlinde kabul etmiş ve sözleşmenin kurulacağını hükme bağlamıştır (BK m. 6). Oysa, bilişim ortamlarında istisnai durumlar haricinde örtülü kabule yer vermemek gerekir. Yani bir bilişim sisteminde sadece ekrandaki teklifin belli bir zaman içinde reddedilmemesi irade açıklaması olarak kabul edilemez.

Hazır Olanlar ve Olmayanlar Arasında İrade Açıklamaları

Kanun koyucu, etkili bir irade beyanını, hazır olanlar ve hazır olmayanlar arasında yapılmasına göre farklı hükümlere tabi tutmuştur. BK m.4/2, telefon, bilgisayar gibi iletişim sağlayabilen araçlarla doğrudan iletişim sırasında yapılan öneriyi, hazır olanlar arasında yapılmış bir öneri olarak saymaktadır. Ancak bu hükümde dikkat edilmesi gereken husus, doğrudan iletişimdir. Yoksa bilgisayar marifetiyle yapılmakla birlikte e-posta yazışmaları hazır olanlar arasında bir irade açıklaması olarak kabul edilemez.

Bir görüşe göre burada hazır olanlar ve olmayanlar arasındaki irade beyanı ayrımı, yapılan irade beyanının canlandırılıp canlandırılmamasına bağlıdır. Bir irade beyanının canlanması, irade beyanının tespit edilmesini ifade eder. İnternet üzerinden gönderilen irade açıklamaları tespit edilmiyorsa yani sonradan herhangi bir usulle tekrar okunabilecek hâle veya yazılı forma getirilmiyorsa bu takdirde İnternet üzerinden hazır olanlar arasında irade açıklamaları söz konusudur. Sözlü beyanlar, özel aletler vasıtasıyla yazıya dökülebiliyorsa canlanır. İnternette gönderilen irade beyanları "kaydedici/ram-harddisk" denilen aletlerle teorik olarak saklanabilir. Yazarlar, günümüz teknolojisinin elektronik araçlar vasıtasıyla irade açıklamalarının belirli formlar içinde tekrar yazı olarak saklanabileceğine ve canlandırılabileceğine işaret etmektedir. Bir görüşe göre de telesekretere yapılmış olan sözlü beyanların herhangi bir canlanma olmaksızın saklanabildiğini belirtmektedirler. Kanaatimce bu açıklamalar, bizlere önerinin/irade beyanının hazır olanlar ya da olmayanlar arasında bir ayrım yapmada sadece kolaylık sağlar yoksa kesin bir ölçü getirmez. BK m. 4/2'nin ölçüsü son derece açıktır, eğer iletişim doğrudan sağlanıyor ise bu hâlde hazır olanlar arasında irade beyanı vardır.

dikkat

BK. m. 4/2 gereğince, telefon, bilgisayar gibi iletişim sağlayabilen araçlarla doğrudan iletişim sırasında yapılan öneri, hazır olanlar arasında yapılmış sayılır.

MSN, IRC (Internet Relay Chat), Gmail ya da Facebook sohbet odalarında arada herhangi bir kaydedici sistem olmaksızın irade beyanları internet altyapısı ya da telefon hattı sayesinde ekranda zaman farkı olmadan görülebilmektedir. Bu arada belirtelim ki ses ya da görüntünün birkaç saniyelik gecikmesi, kanun koyucu bakımından dikkate alınmamıştır. Bu hâlde hazır olanlar arasında bir irade açıklaması vardır. Buna karşılık gönderici, alıcının e-posta kutusuna bir haber bıraktığında bu telesekretere benzer bir durum arz eder. Burada alıcı, gönderenin irade beyanını e-posta kutusunu açtığında görecek ve öğrenecektir. Doğrudan bağlantının olduğu hâller hazır olanlar, diğer durumlar ise hazır olmayanlar arasındaki hukuki ilişkiye benzerlik göstermektedir.

Hazır olmayanlar arasında irade beyanı, BK.m.5'e göre ulaşma anında tesirli olur. Şimdiye kadarki hâkim görüşe göre, irade beyanı, alıcının hâkimiyet alanına ulaşması ile ve normal hâllerde bu beyanın içeriğini alıcının öğrenmesiyle tesir kazanır. Burada hâkim görüş, irade beyanının alıcının bunu öğrenme imkânına sahip olması şartıyla alıcının e-posta kutusuna girmesiyle tesirli olduğunu savunmaktadır. Burada tartışılması gereken, bu e-postanın ne zaman ulaştığının beklendiğidir. Gerçekten e-posta, mektup ya da fakstan farklıdır ve insanların evinin

önündeki posta kutusunu kontrolü ile e-postalarını kontrol aynı şeyler değildir. Klasik öğretide savunulan, hazır olmayanlar arasında gönderilen irade açıklamalarının etki anının o beyanın alıcı tarafından öğrenildiği veya normal hayatın akışı içinde öğrenildiğinin kabul edildiği andır. Oysa e-postanın kullanımı ve kontrolü için alışılmış bir zamanın tespiti bugün oldukça zordur. Her ne kadar günümüzde artık kartvizitlerin üzerinde bulunan e-posta adreslerinin, özel hayatta ve iş hayatında artan yaygın kullanımına rağmen e-postanın günümüz için henüz hayatın bir parçası olmadığı kanaatindeyiz. Ancak şunu da belirtmemiz gerekir ki, akıllı telefonların artması, İnternet kullanımının yaygınlaşması ile bu görüşümüzün yıllar içinde e-posta kullanımının yaygınlaşması yönünde değişmesi de mümkündür. Burada e-posta üzerinden yapılan irade açıklamaları için bir çözüm arayışı da gerekir: E-postaya gönderilen irade açıklamasının öğrenildiği anın tespiti, gönderilen kimsenin (ticaret erbabı) olup olmamasına göre bir ayrım yapılarak incelenmelidir. Bir iş adamı, üzerinden ticari bağlantılar yaptığı e-postasını sürekli ve düzenli olarak kontrol etmekte ve hatta kendisine yapılan yazışmaları beklemektedir. Oysa e-postasını tamamen şahsi amaç için kullanan bir kimse e-posta kutusunu düzenli olarak kontrol etmeyebilir. Bir iş adamına e-posta yoluyla mesai saatleri dışında gönderilen irade açıklamaları, göndermeyi takip eden ilk mesai gününde ulaşmış kabul edilmelidir.

E-posta yoluyla gönderilen haberin (mailin/postanın) kodlanmamış veya kodlansa bile bunu çözecek bir şifrenin alıcıda bulunması gerekir. Buna karşılık ulaşmanın, alıcının posta kutusunun sahibi tarafından boşaltılması ile meydana geleceği görüşü kabul edilemez. Öneriyi yapanın postasını özen içinde göndermesi de gerekir. Örneğin e-posta sunucuları tarafından spam mail olarak kabul edilebilecek ve bu çerçevede filtrelenecek olan mailler, alıcıya ulaşamaz. Bu türden bir e-postanın alındığının ispatını gönderenin üzerinde bırakmak daha uygundur.

Hazır olanlar arasında irade beyanı bu beyanın alıcı tarafından öğrenildiği andır. Fakat elektronik irade açıklamalarında tartışmalı olan husus, alıcının irade beyanını akustik veya optik olarak doğru öğrenip öğrenmediğidir. Burada göz önünde bulundurulması gereken, online eş zamanlı bağlantıların dahi fiziki olarak karşılıklı hazır bulunmadan daha farklı olduğu ve iletişim emniyetinin artırılmasına ihtiyaç duyulduğudur. Burada hukuki problemlerden başka bir de teknik problemler de karşımıza çıkmaktadır. Online bağlantılarda dahi irade beyanını kendi bilgisayarına yazan kimse, bunu onaylayan tuşa (Enter veya Return tuşu) yanlış veya geç basması hâlinde irade beyanının karşı tarafa ulaşmasında zaman bakımından bir farklılık ortaya çıkabilecektir. Ancak bu durumda dahi enter tuşu, irade açıklamasının yapıldığı andır. Buna karşın nette meydana gelen bir sorun nedeni ile irade beyanının gecikme ile karşı tarafa geç ulaşmasında teknik bir sorun vardır. Kanaatimizce bu gibi teknik problemlerin ispat edilemediği durumlarda taraflar arasında hazır olanlar arasında irade açıklamalarının varlığını kabul etmek doğru olacaktır. Yine belirtelim ki benzeri iletişim aksaklıkları normal yüzyüze bir iletişimde de ortaya çıkabilir. İki kişinin konuşması esnasında büyük bir gürültünün yaşanması ya da birinin bir anlık bile olsa sesinin kısılması gibi.

Teknolojinin gelişimine bağlı olarak esasen öneren yani irade beyanında bulunana BK m. 5/2'de bir kolaylık sağlanmıştır. Buna göre öneren, önerisini zamanında ulaşmış sayabilecektir. İrade açıklaması, öneri şeklinde gerçekleşebileceği gibi kabul şeklinde de gerçekleşebilir. Bu hâlde kabul için de aynı esaslar söz konusudur. Yani diğer bir deyişle kabulün de makul bir süre içinde önerene ulaşması gerekir. Ancak kabul konusunda BK m. 5/3'de daha farklı bir düzenlemenin getirildiği söylenebilir. Zira öneriye olumlu bir cevap verilmediği sürece kabul anlamına gelmez. Bu nedenle öneren bakımından öneri reddedilmiş sayılır. Buna karşın kabul beyanının ulaşması için bir zaman sınırlamasına ihtiyaç bulunur. İşte BK m. 5/3, kabul beyanının geç ulaşması hâlinde önerene bir imkân vermiş ve kabul beyanı ile bağlı olmak istemediği takdirde durumun kabul edene derhal bildirilmesi gerektiğini hükme bağlamıştır.

Elektronik ortamda yapılmış bir öneri ya da kabul geri alınabilir. Geri alma açıklaması, diğer tarafa öneri ya da kabulden önce veya aynı anda ulaşmış ya da daha sonra ulaşmakla birlikte diğer tarafça öneriden ya da kabulden önce öğrenilmiş olursa geri alma gerçekleşmiş sayılır (BK m. 10).

Öneri ya da kabul anlık iletişim araçlarında (chat, msn gibi) yapıldığında bile hemen geri alma beyanı yapılırsa ya da ilk elektronik posta okunmadan önce geri almaya ilişkin irade beyanı da ulaşırsa geri alma gerçekleşmiş sayılmalıdır.

İrade Açıklamasında Bozukluklar ve İptal Edilebilirlik

Elektronik irade açıklamalarında birçok eksiklik ve hata ortaya çıkabilir. Aslında elektronik irade açıklamasında ilk bakışta hata olması mümkün görünmeyebilir. Çünkü burada irade sadece bilgisayar yardımıyla iletilmektedir. Ancak irade beyanında, sistemden kaynaklanan bilgi aktarımı hataları ortaya çıkabilir. Burada her şeyden önce elektronik irade açıklamasında bulunan kimsenin, karşı tarafın yapılan beyanın doğruluğuna güvenmesi dolayısıyla ortaya çıkan zararlardan sorumlu olup olmayacağı sorunu ortaya çıkar (BK m. 35).

Bilgisayar kullanıcısının irade açıklamasında tıpkı bir daktilo kullanımında olduğu gibi bir hata söz konusu olabilir, bu takdirde BK m. 31/1-1 uygulama alanı bulur ve ortada bir beyan hatasının olduğuna hükmedilir. Bilgisayar kullanıcısı beyanını iptal edebilir.

Beyanda ortaya çıkan birtakım hatalar da gönderilme aşamasında olabilir. Doktrinde elektronik irade açıklamalarındaki eksikliklere BK m. 33'ün uygulanıp uygulanmayacağı tartışmalıdır. BK m. 33, irade açıklamasının haberci dolayısıyla yanlış yöneltilmesini BK m. 31'deki vakıalarla bir tutmuştur. Bazı yazarlar BK m. 33'ün ilke olarak bütün elektronik irade açıklamalarının nakillerinde kullanılabileceği düşüncesindedir. Kanaatimizce de burada BK m. 33'ün kullanımı mümkün olmalıdır. Zaten BK m. 33 metninde açıkça 'bir araç tarafından' yanlış iletilmeden de bahsedilmektedir. Çünkü yanlış gönderilen bir irade beyanı söz konusudur. Habercinin beyanı yanlış göndermesi durumunun elektronik bir versiyonu burada mevcuttur. Burada beyanı göndermeyi üstlenen İnternet servis sağlayıcısını ya da e-posta sağlayıcısını haberci olarak yorumlamak mümkündür. Şayet bir online hizmet sunucusunda yanlışlık ve hatalar söz konusu ise bu takdirde irade beyanı iptal edilebilir. Fakat burada şu hususun da belirtilmesi gerekir ki şayet gönderme hatası bilgisayar kullanıcısının kendi kullandığı araçlardan kaynaklanıyorsa irade beyanı iptal edilemez. Çünkü BK m. 33, irade beyanının gönderiminde hata hâlini sadece bu hataya üçüncü bir kişinin sebep olması durumunda kabul etmiştir.

İrade beyanında ortaya çıkan hatalar bakımından aslında elektronik irade açıklamalarında hata riski daha yüksektir. Çünkü çoğu zaman İnternet üzerinden yapılan sözleşmelerin kurulması daha basit bir eylemle mümkün olmaktadır. Bir fare (mouse) kliklemesi ile sözleşmenin kurulması onaylanmış olmaktadır. Oysa o anda yapılan bir gayri iradi el hareketi yahut kasılma da bir sözleşmenin oluşumuna sebebiyet verebilir.

Burada iradenin oluşumunda da birtakım hataların ortaya çıkabileceğine dikkat çekmek gerekir. Özellikle İnternet ortamında eski bir fiyat listesine itibar ederek bir sözleşme ilişkisine giren kimsenin irade beyanında hatadan bahsedilemez. Çünkü aslında irade beyanında hata mevcut değildir ancak iradenin oluşumunda bir saik hatasından bahsedilebilir.

İrade Açıklamasının Yorumu

İrade beyanı, açık değilse yoruma ihtiyaç vardır. Bu yorum yapılırken gönderilen irade beyanı objektif ölçülere riayet edilmekle birlikte, olayın münferit özelliklerine de dikkat edilir. Bilgisayar aracılığıyla yapılan irade açıklamalarında anlaşılabilirliğin objektif ölçülere göre tayin edilmesi gerekir. Burada İnternet üzerinde yapılan irade açıklamalarına büyük ölçüde bir kitlenin ulaşacağı gözden kaçırılmamalıdır.

Sözleşmelerin Kurulmasında

İrade açıklamaları ve sözleşmelerin kurulması kural olarak şekil serbestisi ilkesine tabidir (BK m. 12). Yani sözleşmenin tarafları sözleşme yaparken diledikleri şekli seçmekte serbest oldukları gibi kural olarak sözleşmenin kurulması da kanunen herhangi bir şekle tabi tutulmamıştır. Şekle bağlı sözleşmeler kanunda sayılmıştır. Bunlara örnek olarak evlenme akdi, gayrimenkul devir sözleşmeleri örnek olarak verilebilir.

AB Direktifleri'nde ise kural, yine şekil serbestisidir. Ancak bununla birlikte resmî bir makamın katılması gereken sözleşmeler (taşınmaz satımları) istisna tutulmuştur. Ayrıca aile ve miras hukuku ile ilgili sözleşmeler de şekil serbestisi ilkesine tabi değildir ve İnternet üzerinden yapılmaları mümkün değildir. Avrupa direktiflerinde sayılan şekil serbestisi ilkesinin bu istisnaları kesin ve son bir sıralama değildir. Bilgi toplumunun ilerlemesi ve teknolojinin gelişmesi ile yeniden bir uyarlamanın yapılması mümkündür. Uyarlamanın yapılabileceği Avrupa Birliği Direktifleri'nde de açıkça belirtilmiştir.

Sözleşmenin tarafları şekil serbestisi ilkesi sayesinde yapacakları sözleşmeyi isterlerse kanunun tipik sözleşme formlarından birinde isterlerse atipik bir formda isterlerse de kanunun öngördüğü birkaç sözleşme türünün özelliklerini taşıyan bir sözleşme şeklinde kurabilirler.

Atipik sözleşmelere Web-Hosting sözleşmeleri örnek olarak verilebilir. Webhost sunucusu bu sözleşme ile müşterisine her kullanıcının bir adres altında ulaşabileceği web sayfasını sunma imkânı sağlamaktadır. Webhost sunucusunun müşterisi, kendisinin hazırladığı veya derlediği bilgileri sunan özel bir şahıs da olabilir, kendi ürünlerini İnternet ortamında pazarlamak isteyen bir işletmeci de olabilir. Webhost sunucusunun ortağı ise kural olarak bir içerik, konu sunucusudur ve içerik sunucu (content-provider) olarak adlandırılır. Bu sözleşmede hem kira sözleşmesine ait nitelikler hem de hizmet sözleşmesine ait nitelikler bulunmaktadır.

Web host
Bizler tarafından hazırlanan web sayfalarının kesintisiz olarak sunulması ve ulaşılabilirliğinin sağlanmasını sağlayan misafir eden bilgisayarlar.

Birleşmiş Milletler'in elektronik ticaret için hazırlamış olduğu örnek yasada da irade açıklamaları ve sözleşmenin kurulması için şekil serbestisi ilkesi kabul edilmiştir. Fakat örnek yasada şekil serbestisi ilkesinin istisnaların olabileceği de kabul edilmiştir (m. 11).

Türk hukukunda da BK m. 12 ile birlikte sözleşmelerin geçerliliğinin kanunda aksi öngörülmedikçe şekle bağlı olmadığı kurala bağlanmıştır. Ancak eğer kanunda bir şekil öngörülmüş ise kural olarak bu şekil geçerlilik şartıdır ve şekle uyulmaksızın kurulan sözleşmeler geçersiz olacaktır.

İstisna: Şekil Şartı

Türk hukukunda kural, sözleşmelerin akdinde şekil serbestisi olsa da bazı sözleşmeler için kanun koyucu özel şekil şartları öngörmüştür. Bu şekil şartları, kendi içinde merasimli şekil şartı (evlilik gibi), resmi şekil şartı (tapu ve noterde yapılan sözleşmeler gibi) ve yazılı şekil şartı şeklinde üç ana başlıkta toplanabilir.

BK m. 12/2'ye göre eğer kanunda bir sözleşme için şekil şartı öngörülmüş ise bu şekil kural olarak sözleşmenin geçerlilik şartıdır. Bu şekle uyulmaksızın akdedilen sözleşmeler hüküm doğurmaz. Bu nedenle bazı sözleşmelerin elektronik ortamda yapılması mümkün olmaz. Evlilik sözleşmesi, gayrımenkul alım satım sözleşmeleri gibi sözleşmelerin mutlaka kanunda öngörülen şekil şartına tabi olarak akdi gereklidir.

Kanunun adi yazılı şekli aradığı hâllerde ise esasen yine elektronik ortamda sözleşme akdedilemez, akdedilirse de hüküm doğurmaz. Bu hâllerde esasen bir kilitlenme söz konusudur. Bilişim toplumunun önünde bu türden şekil şartları bir engel olarak durmaktadır.

Adi yazılı şekil şartını da sağlayarak sözleşmeleri acaba, elektronik ortamda akdetmek mümkün olabilir mi? Bilindiği üzere yazılı şekil şartının en önemli unsuru, iradesini yazılı olarak açıklayan kimsenin irade açıklamasının altına ıslak imzasını koymasıdır (BK m. 14). Metnin daktilo ya da bilgisayar ile yazılmasının yahut üçüncü bir kişi tarafından kaleme alınmasının bir önemi yoktur.

Esasen burada bir tartışmaya kısaca değinmek gerekir. Yazılı şekil şartından bahsederken üzerinde durulması gereken bir diğer unsur, metnin kendisidir. Metin sürekli, kalıcı ve dayanıklı bir madde üzerine yazılmış olmalıdır. Bu yönü ile kâğıt, odun ya da bir taş parçasına yazım arasında fark bulunmaz. Ancak hemen vurgulayalım ki kanun koyucu bu anlamda bir metni, sözleşmelerde şart kılmamıştır. Aksine okunabilir belge de bir metin olarak kabul edilmektedir (BK m. 14/2).

Elektronik İmza Kanunu'nun kabulü ile birlikte, BK m. 14/1'de yer alan imza şartı da yerine getirilebildiği için artık yazılı şekil şartına tabi sözleşmelerin de elektronik ortamda yapılabilmesi mümkün hâle gelmiştir. Zira Kanun'un 15. maddesine göre, güvenli elektronik imza da ıslak imzanın bütün sonuçlarını doğurur. BK m. 14/2'ye göre ise güvenli elektronik imza ile imzalanmış bir belge, yazılı şekil şartının yerine geçer.

Bu açıklamalarımızdan anlaşılacağı üzere, güvenli elektronik imza ile imzalanan belgenin yazılı şekil şartını yerine getirebildiği şekil, adi yazılı şekildir. Buna karşın resmî yazılı şeklin öngörüldüğü sözleşmeler ve tabii olarak irade beyanları ile merasimli şekil şartına tabi sözleşmeler, elektronik imza yolu ile de olsa yapılamazlar. Yine bono, poliçe ya da çekin de elektronik imza ile şekil şartının tamamlanması mümkün olmaz.

Sözleşmelerin ya da Elektronik İrade Açıklamalarının İspatı

Günümüzde elektronik ortamda yapılan işlemler hızla gelişmektedir. İrade açıklamaları, elektronik olarak iletilmekte, sözleşmeler elektronik ortamda kurulmaktadır. Bilişim dünyasındaki bu ilerlemelere karşın hukuk sistemi ve kuralları aynı hızda değişmemekte, ortaya çıkan yeni sorunlara çözümler üretilememektedir. Yeni teknoloji, sözleşmelerin yeni şekiller içinde yapılması karşısında mevcut bütün kanunlar yorumlanarak çözüm bulunmaya çalışılmaktadır. Son zamanlarda hukuk aleminde elektronik dokümanların nasıl kullanılacağı, ispat değerinin ne olduğuna ilişkin tartışmalar yaşanmaktadır. Aslında problem, teknolojik gelişmeler karşısında yürürlükte bulunan hükümlerin yetersiz kalmasından ibaret değildir. Son yıllara kadar hem teknolojiyi hem de hukuku takip eden ve bunu kamuoyuna taşıyan hukukçuların yokluğu da bir başka problemdir. Fakat hemen burada belirtmek gerekir ki ispat hukuku bakımından ortaya çıkan sorunlara mevcut kanunların yorumu ile çözüm bulmak imkânsız gibidir. Senedin altında bulunması gereken imza nasıl atılacak, noterde yapılması gereken sözleşmeler nasıl akdedilecektir? Yazılı şeklin arandığı sözleşmelerin yerini, bilgisayar ekranındaki bir görüntü doldurabilecek midir? Uluslararası sözleşmelerde şekil şartının katı kurallara bağlı olması ticari hayatın önünde ciddi bir engel teşkil etmektedir. Bu sebeple elektronik işlemlerin ispat hukuku bakımından yeni ve uluslararası normlara uygun hükümlerle düzenlenmesi gerekir.

Elektronik ticaretin yaygınlaşması elektronik dokümanların ispat değerinin artmasına bağlıdır. Elektronik dokümanlar yeterli bir ispat değerine sahip kılınmazsa elektronik ticaret de hukuki güvenceye bağlanamaz.

Bu bölümde elektronik dokümanların ispat değerine değinilecektir. Mukayeseli hukukta konunun düzenlenişi ortaya konulacak, çözümler üretilmeye çalışılacaktır. Özellikle elektronik dokümanların ispat değerinin sağlanması ile ilgili örnek çalışmalar burada sunulacaktır.

Belge - Senet Kavramları

İsviçre ve Alman hukukunda senet kavramının karşılığında kullanılan belge ("Urkunde") kavramı, geniş bir anlama sahiptir. Bu hukuk sistemlerinde bu kavramla içerisinde bir fikir veya bilginin mevcut olduğu yazılı bir cisim ifade edilir. Bu kavram Türk dilinde belge ile karşılanabilir ki belge, senet kavramından daha geniş bir anlamda kullanılır. Belge ile sadece belirli bir yazılı şekil anlatılmaz. Örneğin ceza hukuku anlamında belge, içinde sadece yazı değil herhangi bir işaretin de bulunabildiği bir cisim olarak anlaşılır. Yine ceza hukukunda bir video filmi veya fotoğraf da belge olarak kabul edilir. Burada elbette bilgisayar ortamında kaydedilmiş elektronik dokümanlar da diğer yazılı cisimlerle eş değerde bir ispat değeri taşımaktadır.

HMK m. 199'a göre, uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanun'a göre belgedir.

Elektronik dokümanların ispat değerinin asıl tartışıldığı alan ise özel hukuk alanıdır. Usul hukuku bakımından bir belgenin veya usul hukuku deyimi ile senedin ispat değeri taşıması onun yazılı bir cisim olmasını gerektirir. Türk usul hukuk sisteminde senet kesin deliller arasında sayılmıştır. HMK m. 200'e göre bir hakkın değeri, ikibinbeşyüz Türk lirasını geçtiği takdirde senetsiz ispat artık mümkün değildir.

Özel hukukta senetlerin ispat gücüne sahip olması da zamanla olmuştur. Günümüz ispat hukukunda senetlerin yazılı formda olması ve altında imzanın bulunması şartı bundan birkaç yüzyıl önce kâfi gelmiyordu. Yine geçen yüzyılda telgrafın belge değerinde sayılıp sayılmayacağı tartışılıyordu. Nihayet gönderilen telgraf, bazı ülkelerde bir belge değerinde kabul edilmeye başlanmıştır. Günümüzde de elektronik iletişimin gelişmesi, ticaretin web sayfaları üzerine kayması, ispat değerinin hukuk düzenince tanındığı yeni dokümanların ihdasını gerekli kılmıştır.

Bu problemin önemini burada özellikle vurgulamak gerekmektedir. Zira esasen sözleşme bir şekle bağlı olmayabilir, ancak eğer sözleşme içinde bulunan konu, ikibinbeşyüz TL'yi geçiyor ise artık burada senetsiz ispat mümkün olmayacaktır. Bir taraftan sözleşmelerdeki şekil serbestisi ilkesi diğer taraftan da ispata ilişkin kural düşünüldüğünde mutlaka bir senede ihtiyaç duyacağımız açıktır. Elektronik sözleşmelerde ise her zaman güvenli elektronik imza kullanılamayacağı için çoğu kez ispat zorlukları yaşanacaktır.

Mevcut Hukuk Sisteminde Elektronik Dokümanların İspat Gücü

Elektronik dokümanlar, maddi bir cisim taşımamaktadır. Ayrıca elektronik dokümanlarda yazılı formun altında bulunması gerekli olan imza da bulunmamaktadır. Bu eksiklikler sebebiyle elektronik dokümanlar -kural olarak- usul hukukunda senet niteliği taşımazlar. Fakat elektronik dokümanların maddi cisim taşımamaları onları tamamen de ispat değerinden yoksun bırakmamaktadır. İlke olarak elektronik dokümanlar takdiri delil olarak kabul edilir. Fakat mevcut hukuk düzeninde elektronik dokümanların takdiri delil olarak kullanılabilmesi için de tabii olarak onların sonradan okunabilir olması şartı aranmaktadır. HMK m. 195, elektronik ortamdaki verilerin belge sayılacağını hükme bağlamıştır. Yine burada belirtmek gerekir ki bazı hâllerde kanun koyucu, bazı işlemlerin –güvenli elektronik imza olmaksızın- elektronik olarak imzalanmasına imkân vermiştir. Konişmento, taşıma senedi ve sigorta poliçesi bunlara örnek olarak verilebilir (TTK m. 1526/2).

Belge sayılmasının önemi ise şuradadır. Eğer yukarıda bahsettiğimiz HMK m.200 anlamında senetle ispatı zorunlu bir husus bile olsa elektronik ortamda bir belge varsa bu hâlde bu durumlarda tanık dinlenebilir (HMK m.202). Böylece elektronik ortamdaki belge, senetle ispata yarayacak hâllerde bile işe yarayacak ve delil başlangıcı teşkil edecektir.

Elektronik dokümanların taraflar arasında yapılacak bir anlaşma ile ispat değerinin artırılması düşünülebilir. Yani taraflar aralarında anlaşarak elektronik dokümanların senet olarak kabul edileceğine dair aralarında bir sözleşme yapabilir veya yaptıkları sözleşmeye böyle bir hüküm koyabilirler (HMK m.193). Fakat bu delil sözleşmesi hâkim için bağlayıcı değildir. Hâkim elektronik dokümanların delil niteliğini reddedebilir. Ayrıca müşteri açısından böyle bir delil sözleşmesinin varlığı da her zaman için iptal edilebilir. Çünkü çoğunlukla bu tür sözleşmeler genel işlem şartlarının bir maddesi olarak müşteriye imzalatılacaktır. Bu takdirde Türk hukukunda da BK m.20 ve devamı hükümleri devreye girmekte, genel işlem şartları denetime tabi tutulmakta ve sözleşmenin zayıf tarafı korunmaktadır.

Elektronik Dokümanların İspat Değerine Sahip Olma Gereksinimi

Elektronik dokümanlar, klasik senetlerden orijinali, kopyası (sureti) veya onaylı onaysız suretlerinin olmaması ile de ayrılır. Bu farklılık, elektronik dokümanlarda, klasik senetlerde olduğu gibi gerçek ve sahte karşılaştırmasını da anlamsız kılar. Senetlerde bulunan imzaların karşılaştırılması da senetlerin güvenliğini artıran bir yoldur. Elektronik dokümanlarda imzanın tatbiki imkânı bulunmamaktadır. Ticari hayatın hukuki güvenliğinin sağlanması için elektronik dokümanlarda bulunmayan imza ve asıl-kopya unsurlarının yeni ihdas edilecek ve senet değeri taşıyacak belgelerde de sağlanması gerekmektedir. Elektronik dokümanlarda, özellikle ticari amaçlı web sayfalarında güvenlik sistemleri bulunmakta ve işlemler özel şifrelerle gerçekleştirilmektedir. Burada kullanılan şifre bir yönü ile klasik senetlerde imzanın yerini tutmaktadır. Senetlerde asıl ve suretin sağladığı güvenlik de bugün bilgilerin kaydedilmesi ile sağlanmaya çalışılmaktadır.

Bundan birkaç yüzyıl önce senetlere, geçen yüzyılın başında telgrafa duyulan güvensizliğin benzeri günümüzde de elektronik dokümanlar için geçerlidir. Fakat ticari hayatın hızlılığı, elektronik dokümanlarla ilgili gerekli düzenlemelerin yapılmasını bugün zaruri kılmıştır. Bu nedenle birçok ülke elektronik ortamdaki içeriğe ilişkin düzenlemelerini yapmıştır. Bu çerçevede gerek HMK gerekse Elektronik İmza Kanunu ile Türk hukukundaki eksiklikler de giderilmiştir.

Güvenli Elektronik İmza ve İspat Gücü

Elektronik içeriğin elektronik imza ile imzalanması, belgeye senet gücü vermez. Zira elektronik imzaların güvenilirlikleri aynı değildir. Elektronik belgenin senet mahiyetini kazanabilmesi için güvenli elektronik imza ile imzalanması gerekir.

Elektronik imza, 'başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi' ifade etmektedir (Elektronik İmza Kanunu-EİK, m. 3). Yani diğer bir deyişle burada kalemle atılan bir imza bulunmamakta aksine kimlik doğrulayan başka bir elektronik veri bulunmaktadır.

EİK'de sadece elektronik imza tanımlanmamış aynı zamanda güvenli elektronik imza da bir tanıma kavuşturulmuştur. Buna göre bir elektronik imzanın güvenli elektronik imza sayılabilmesi için münhasıran imza sahibine bağlı olması, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma amacı ile oluşturulması, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlaması ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitinin sağlanması şarttır (EİK.m. 4).

Senet, kendisini borçlandıran bir işlemin altında borçlanan kimsenin imzasını taşıdığı belgedir. Elektronik ortamda ise veri altına imza koymak mümkün değildir. Eğer bu verinin altında güvenli elektronik imza varsa bu takdirde bu veriler de bir bütün olarak senettir ve senetle ispat edilebilen her husus güvenli elektronik imza ile imzalanmışsa bu elektronik veri ile de ispat edilebilir. HMK m. 205/2'de de bu husus, usulüne göre güvenli elektronik imza ile oluşturulan verilerin senet hükmünde olduğu hükme bağlanmıştır. Böyle bir belge mahkemeye delil olarak sunulmuş ise bu hâlde hâkim, bu belgenin güvenli elektronik imza ile imzalanıp imzalanmadığını re'sen incelemek zorundadır (HMK m. 205/3). Mahkemede bir uyuşmazlık görülür iken delil olarak güvenli elektronik imza ile imzalanmış bir belge sunulur ve karşı taraf da buna itiraz ederse hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılmaya çalışılır. Ancak belirtelim ki söz konusu bu hüküm fuzulidir. Zira güvenli elektronik imza hakkında inkâr eden tarafın beyanı ile bu sorun çözümlenemez. Çünkü son derece teknik bir işlem olan güvenli elektronik imza, bu hâlde sanki hâkimin itiraz edeni dinleyerek doğruluğunu anlayabileceği ve karar verebileceği bir belge konumuna düşürülmektedir ki bu doğru değildir. Hâkimin yapması gereken şey, bilirkişi incelemesine başvurmaktır (HMK m. 210).

Güvenli elektronik imza ile imzalanmış bir veri, HMK anlamında senet olsa da yazılı şekil şartına tabi sözleşmelerde şekil şartını gerçekleştirip gerçekleştirmeyeceği de ayrı bir sorundu. Zira Kanun, yazılı bir şekil şartı öngörmüş ise bu hâlde bu şekil geçerlilik şartıdır (BK m.12) ve güvenli elektronik imza ile imzalansa bile yazılılık şartı yerine gelmez. İşte bu boşluğun doldurulması amacıyla Kanun koyucu, BK m.14/2'de güvenli elektronik imza ile gönderilip saklanabilen metinlerin de yazılı şekil yerine geçtiğini hükme bağlamıştır. Yine sözleşme altında bağlayıcılık kazanabilmesi için gerekli imzaların da güvenli elektronik imza ile atılabileceği BK m. 15'te teyit edilmiş ve böyle bir imzanın elle atılmış imzanın bütün hukuki sonuçlarını doğuracağı kuralı getirilmiştir.

Elektronik Ortamda Kurulan Sözleşmelerde Akdin Zayıf Tarafının Korunması

Esasen elektronik ortamda kurulan sözleşmelerin diğer sözleşmelerden bir farkı yoktur. Zira, sözleşme sözleşmedir ve deyim yerinde ise tarafların anayasasıdır. Bu nedenle sözleşmenin bağlayıcılığı ve diğer hükümleri bakımından Borçlar Kanunu'nda elektronik ortamda yapılmış sözleşmeler için özel düzenlemeler getirilmemiştir.

Buna karşın tüketicinin ve sözleşme yapanların korunması için tüketici ve elektronik ortamdaki ticareti düzenleyen mevzuatımızda sözleşmelere özgü birtakım düzenlemeler bulunmaktadır. Elektronik sözleşmelerin yapılmasında bu hususlara da dikkat edilmelidir.

Tüketicinin Korunması Hakkında Kanun'da Mesafeli Sözleşmeler

İnternetle birlikte tüketicilerin korunması özel bir önem kazanmıştır. Mal ve hizmet sürümünün İnternetten yapılması ile birlikte sınırlar da önemini kaybetmiştir. Çünkü tüketicinin alışveriş ilişkisine girdiği satıcının dünyanın öbür ucunda bulunması mümkündür. İnternetle birlikte bütün dünya bir pazar hâline gelmiştir. İnternet üzerinden sınır ötesi sürümlerin fayda ve zararları da bulunmaktadır. Zaman ve masraflardan tasarrufun yanında sözleşmenin yapılması ve icrası aşamasında İnternete has birtakım riskler de vardır. Bunlardan ilki, vaat edilen mal ya da hizmetin hiç

ya da gereği gibi ifa edilmemesidir. Uzakta olan satıcı ile doğrudan temasın olmaması nedeniyle, alınanın iadesi ya da değiştirilmesi talepleri de bir başka problemli alandır. Başka bir ülkeden mal ya da hizmet alan tüketicinin maruz kalacağı bir diğer güçlük de ortaya çıkacak uyuşmazlıklarda kendi ülke hukukunun uygulanmamasıdır. Elektronik ortamda tüketici bakımından sayılabilecek çok sayıda tehlike vardır. Ancak önemle vurgulayalım ki bu tehlikeler, elektronik ticaretin hukuk sistemlerince yasaklanmasını gerektirmez, tam aksine hukuk sistemleri elektronik ticareti teşvik etmekte ancak bazı hususlarda da tüketiciyi koruyucu düzenlemeler getirmektedir.

6502 sayılı Tüketicinin Korunması Hakkında Kanun'a göre "tüketici", 'ticari veya mesleki olmayan amaçlarla hareket eden gerçek veya tüzel kişiyi' ifade etmek için kullanılmıştır. Ancak tüketiciyi, bir mal veya hizmeti özel amaçlarla satın alarak nihai olarak kullanan veya tüketen gerçek veya tüzel kişiyi ifade etmek daha tanımlayıcıdır. E-ticaret için de aynı tanım geçerlidir ve uluslararası düzenlemelerde de aynı görüş kabul edilir.

İnternet ortamında tüketicinin almış olduğu mal ve hizmetler bakımından bir ayrıma gitmek gerekmektedir. İnternet ortamında hem fiziki varlığı bulunan hem de müzik, veri ya da yazılım gibi fiziki varlığı bulunmayan ürünler satışa sunulmaktadır.

Burada tüketicinin korunması konusunda bir başka konunun da göz önünde bulundurulması gerekmektedir. Bu da tüketicinin sözleşme yaptığı kimsenin karşı tarafının nerede ikâmet ettiğidir. Şayet tüketici Türkiye içinde ikâmet etmekte ise sorun tüketici açısından daha kolay çözülebilmektedir. Fakat Türkiye dışında bir satıcı ile işlem yapan tüketicinin haklarının koruması daha zor ve ayrıca tüketici açısından oldukça masraflıdır.

Türkiye Düzenlemeleri

Konunun tüketicilerin korunmasında özel bir önem taşıması ve özel bir düzenleme gereği dolayısıyla Sanayi ve Ticaret Bakanlığı da 4077 sayılı eski Kanun'u güncel gelişmeleri özellikle de elektronik ortamda kurulan sözleşmeleri de göz önünde bulundurarak değiştirmiş ve 6502 sayılı yeni Tüketicinin Korunması Yasası'nı kabul etmiştir.

Mesafeli sözleşme (TKHK m.28/1), satıcı veya sağlayıcı ile tüketicinin eş zamanlı fiziksel varlığı olmaksızın, mal veya hizmetlerin uzaktan pazarlanmasına yönelik olarak oluşturulmuş bir sistem çerçevesinde, taraflar arasında sözleşmenin kurulduğu ana kadar ve kurulduğu an da dâhil olmak üzere uzaktan iletişim araçlarının kullanılması suretiyle kurulan sözleşmelerdir.

Elektronik ortamda akdedilecek sözleşmelere ilişkin olarak Tüketicinin Korunması Hakkında Kanun'un tercih ettiği kavram 'mesafeli sözleşmedir'.

Mesafeli sözleşmelerde Avrupa Birliğinde olduğu gibi, ayrıntıları yönetmeliklerle belirlenecek konularda teklifin kabulünden önce tüketici bilgilendirilmek zorundadır. Aynı zamanda siparişinin onaylanması hâlinde de ödeme yükümlülüğünün bulunduğu konusunda uyarılmalıdır (m. 48/2). Bu durum, mesafeli sözleşmelerde sıklıkla karşımıza çıkan bilgilendirme yükümlülüğüdür ve tüketicinin bilgilendirildiğinin ispatı da satıcı ya da sağlayıcıya aittir.

dikkat

Sağlayıcı (TKHK m.3): Kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla tüketiciye hizmet sunan ya da hizmet sunanın adına ya da hesabına hareket eden gerçek veya tüzel kişiyi, ifade eder.

Satıcı ya da sağlayıcı, siparişten sonra taahhüt edilen süre içinde edimini yerine getirmelidir. Mal ya da hizmetin sağlanması için de mesafeli satışlarda azami bir süre öngörülmüştür. Bu süre 30 günü geçemez. Eğer bu süre aşılır ise bu hâlde tüketici sözleşmeyi fesih hakkına sahiptir (m. 48/3).

Mesafeli satışlarda tüketici, satın aldığı mal ya da hizmeti kontrol etme imkânına sahip değildir. Bu nedenle görmediği ya da sadece görsellerini gördüğü bir mal ya da hizmeti şartsız bir şekilde almaktan vazgeçebilir, yani cayabilir. Kanun, tüketiciye hiçbir gerekçe göstermeksizin 14 günlük bir cayma hakkı tanımıştır (m.48/4). Ayrıca tüketici cayma hakkının varlığı konusunda bilgilendirilmelidir. Eğer bu bilgilendirme yapılmamışsa bu hâlde

bu 14 günlük süre ile de bağlı değildir. Ancak tüketiciye verilen bu cayma hakkı sonsuza kadar da devam etmez, her hâlükârda cayma hakkının bittiği ilk 14 günlük süreden bir yıl sonra sona erer.

Tüketicinin cayma hakkını kullanacağı sürede malın mutat kullanımı ya da değişimlerinden sorumlu tutulması da mümkün değildir (m. 48/4). Böylece tüketici, cayma hakkının bertaraf edilmesine yarayacak satıcı itirazlarından kurtarılmıştır.

Elektronik ortamdaki sözleşmelerde tüketiciye sınırsız bir cayma hakkının verilmesi, bazı hâllerde adil olmayabilir. Bazı ürünler bakımından cayma hakkının bu şekilde sınırsız kullanımı, satıcıyı ciddi zarara uğratabilir. Mesafeli Sözleşmeler Yönetmeliği'nde tüketiciye tanınan cayma hakkı sınırlanmıştır (m. 15). Bu sınırlamalar, fiyatı finansal piyasalardaki dalgalanmalara bağlı olarak değişen satıcı ve sağlayıcının kontrolünde olmayan mal ve hizmetlere, tüketici istek ve ihtiyaçlarına ilişkin olarak hazırlanan ürünlere, çabuk bozulabilecek, ambalajı açıldığında hijyen bakımından tehlikeli olabilecek ürünlere, teslimden sonra başka ürünlerle karışabilen ürünlere, dijital ürünlere, gazete dergi gibi süreli yayınların teslimine, elektronik ortamda teslim edilen ürünlere ve cayma hakkı süresi sona ermeden tüketicinin talebi ile ifa edilmeye başlanmış ürünlere ilişkin sözleşmelerde aksi kararlaştırılmadığı sürece cayma hakkı kullanılamaz.

Esas itibarıyla tüketici karşısında satıcı sorumlu tutulmakta iken satıma aracılık edenler varsa bunlar da satıcı veya sağlayıcı ile yaptıkları sözleşmeye aykırı fiillerinden dolayı sorumludur (m. 48/5).

Mesafeli Sözleşmeler Yönetmeliği de elektronik ortamdaki sözleşmelere ilişkin düzenlemeler getirmiştir. Yönetmelik hükümlerine göre, tüketici, sözleşmenin kurulmasından önce, sözleşmenin konusu, mal ya da hizmetin temel nitelikleri, satıcı ya da sağlayıcının adı, unvanı, irtibat bilgileri, temsilcileri, şikâyetin iletileceği iletişim bilgileri, mal ya da hizmetin vergiler de dâhil toplam fiyatı ya da son fiyat hesaplanamıyor ise buna ilişkin ek ödeme çıkabileceği uyarı, ilave maliyetler, şikâyetlerin çözüm yöntemleri, cayma hakkının varlığında bunun kullanım usulü, cayma hakkının kullanılmadığı durumlarda kaybedileceği, tüketici tarafından ödenmesi gereken depozito ve teminatlar, dijital içeriklerin korunmasına yönelik teknik koruma önlemleri, dijital içeriğin hangi donanımla çalışması gerekeceğine ilişkin bilgi, uyuşmazlıklarda Tüketici Mahkemesi ve Tüketici Hakem Heyetlerine başvurulabileceği konusunda bilgilendirilmelidir (Yönetmelik, m. 5). Bu bilgilendirmenin kapsamı bazı durumlarda daha da kapsamlı hâle gelebilmekte ve bilgilendirmeye ilave konular olabilmektedir (Yönetmelik m. 6 ve 7).

Sözleşme öncesi tüketicinin bilgilendirildiğinin ispatı, satıcı ya da sağlayıcıya aittir. Ayrıca sözleşme kurulmadan önce tüketici, bu hususlarda Yönetmeliğin 6. maddesine göre bilgilendirildiğini teyit etmek zorundadır. Aksi hâlde sözleşme kurulmamış sayılmaktadır (Yönetmelik m. 7).

Belirtelim ki Yönetmelik'te ayrıntılı bir bilgilendirme yükümlülüğü arkasında, tüketiciye verilen 14 günlük cayma hakkına ilaveten sözleşmenin kurulmamış sayılması son derece ağır bir yaptırımdır. Bu hükmün katı bir şekilde uygulanması hâlinde uygulamada elektronik ticaretin çok büyük bir kısmının kurulmamış sayılacağı söylenebilir. Bu nedenle esasen Kanun'da olmayan bir geçersiz yaptırımın Yönetmelik düzenlemeleri ile getirilmesi de isabetli olmamıştır.

Mal ya da hizmetlere ilişkin düzenlemelere paralel olarak benzeri bir düzenleme de Kanun'un 49. maddesinde finansal hizmetlere ilişkin getirilmiştir. Burada da tüketicinin bilgilendirilmesi, cayma hakkı konusunda bilgi verilmesi, edimlerin yerine getirilmesi, sözleşme süresi içinde yazılı örneğinin teslimini isteyebilmesi ve 14 gün içinde cayma hakkı düzenlenmiştir (m.49).

Elektronik Ticaret Kanunu'nda Sözleşmelere İlişkin Düzenlemeler

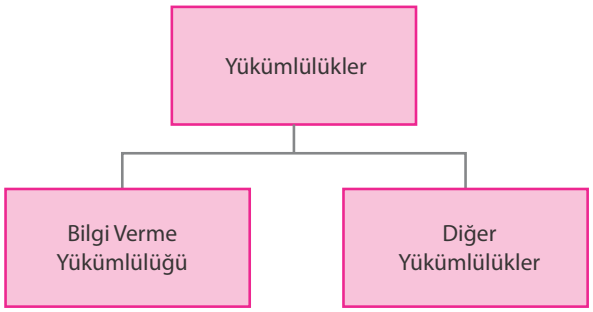
Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (ETK), genel itibarıyla bugüne kadar Türk hukukunda düzenlenmemiş alanları ele alıp düzenlemiştir. Kanun'un asıl amacı, elektronik ortamda icra edilen ticarete ve sözleşmelere güvenin sağlanmasıdır. Kanun koyucunun temel düşüncesi, güvenin sağlandığı hâllerde elektronik ticaret büyüme kaydedecektir. Burada önemle vurgulayalım ki bu Kanun, doğrudan tüketicileri korumayı amaçlayan bir Kanun değildir. İlk amaç, elektronik ticarete olan güvenin sağlanmasıdır. Elektronik ticarete güven sağlandığı takdirde esasen tüketici de dolaylı olarak bundan yarar sağlayacaktır.

Bu Kanun, Tüketicinin Korunması Hakkındaki Kanun'dan farklı olarak uygulanması için taraflar-

dan birinin tüketici olması şart değildir. Zaten taraflardan birinin tüketici olduğu hâllerde özel Kanun olduğu için Tüketicinin Korunması Hakkında Kanun hükümleri uygulanacaktır.

Sözleşmelere İlişkin Düzenlemeler

Elektronik ticaretin yaygınlaştırılması, tüketicilerin ya da elektronik ortamda işlem yapan kimselerin güveninin sağlanmasına bağlıdır. Bu güvenin sağlanması için, elektronik ortamda şeffaflık ve erişilebilirlik şarttır. Bu nedenle elektronik ticaretle uğraşanlar için getirilen Kanun'daki yükümlülükler, bu güvenin ve şeffaflığın sağlanması için getirilmiştir.



Şekil 6.4

Hizmet sağlayıcı, elektronik iletişim araçlarıyla bir sözleşmenin yapılmasından önce; alıcıların kolayca ulaşabileceği şekilde ve güncel olarak tanıtıcı bilgilerini, sözleşmenin kurulabilmesi için izlenecek teknik adımlara ilişkin bilgileri, sözleşme metninin sözleşmenin kurulmasından sonra, hizmet sağlayıcı tarafından saklanıp saklanmayacağı ile bu sözleşmeye alıcının daha sonra erişiminin mümkün olup olmayacağı ve bu erişimin ne kadar süreyle sağlanacağına ilişkin bilgileri, veri girişindeki hataların açık ve anlaşılır bir şekilde belirlenmesine ve düzeltilmesine ilişkin teknik araçlara ilişkin bilgileri ve uygulanan gizlilik kuralları ve varsa alternatif uyuşmazlık çözüm mekanizmalarına ilişkin bilgileri sunar. Yine hizmet sağlayıcı, varsa mensubu olduğu meslek odası ile meslekle ilgili davranış kurallarını ve bunlara elektronik olarak ne şekilde ulaşılabileceğini belirtir (m.3).

ETK m.2/ç: Hizmet Sağlayıcı: Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişileri ifade eder.

Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da siparişe ilişkin düzenlemeler de yer almaktadır. Hizmet sağlayıcı, alıcıya, siparişin onaylanması aşamasında ve ödeme bilgilerinin girilmesinden önce ödeyeceği toplam bedeli ve sözleşme şartlarını görebilme imkânı sağlamalı, siparişi teyit etmeli, sipariş verilmeden önce veri hatalarını belirleyebilme ve düzeltebilme imkânları verilmelidir (m. 4).

Ticari iletişim söz konusu ise bu iletişimin kimin adına yapıldığı da başta belirtilmelidir. Ayrıca indirim, hediye ya da promosyon amaçlı yarışma ya da oyun varsa bunlara ilişkin açıklamalar da yer almalı ve bu açıklamalar anlaşılabilir olmalıdır (m.5).

Bu düzenlemeler dikkate alındığında, esasen elektronik ticaret yapanlar için çok büyük külfetlerin getirilmediği görülmektedir. Bunlara uymamanın yaptırımı ise idaridir ve idari para cezaları getirilmiştir (m. 12).

Öğrenme Çıktısı

1 Sözleşme kavramının elektronik ortamda ne anlama geldiğini açıklayabilme
2 Sözleşmelerde dikkat edilmesi gereken noktaların ne olduğunu sıralayabilme
3 Sözleşmelerin nasıl yapılması gerektiğini ifade edebilme

Araştır 1

Sözleşme kavramı elektronik ortamda ne anlama gelmektedir?

İlişkilendir

Gerçek hayatta sözleşme yaparken elektronik ortamda yapılanlar ile diğer sözleşmeler arasında ne gibi farklılıklar görmektesiniz?

Anlat/Paylaş

Elektronik ortamda gerçekleştirilen Sözleşmelere dair bilgilerinizi çevrenizle paylaşınız.

ELEKTRONİK ORTAMDA REKLAMLAR

İnternet, ticaret yapanlar için yeni bir reklam imkânı olarak algılanmıştır. Büyük şirketlerin her birisinin bir web sayfası kurması, ticari faaliyetlerinin sanal ortamda reklamı olarak görülmekte idi. Elektronik ortam, zamanla reklam fonksiyonunun ötesine geçmiş, bir pazar yeri olarak işlev görmeye başlamıştır. Ancak İnternet ve bilişim ortamı, geniş anlamı ile elektronik ortam, farklı bir reklam mecrası olmuştur. Bugün itibarıyla birçok ülkede reklam alanında İnternet hâkim mecra hâline gelmiştir. İnternet'in halen reklam pazarından en yüksek payı alan televizyonu da birkaç yıl içinde geçeceği tahmin edilmektedir.

dikkat

Araştırmalara göre televizyonun 13 yılda, radyonun 38 yılda geçirdiği aşamayı İnternet sadece 5 yılda geçirmiş ve bir reklam mecrası olmayı başarabilmiştir.

Reklam, bir ürün ya da görüşün iletişim araçları ile kişisel olmayan bir biçimde kitlelere aktarılmasıdır. Bir başka tanımı ile duyuruculuk ve ikna etme özellikleri ile malın veya hizmetin içeriğini ve özelliklerini, üretim biçimini, kullanıldığı yer ve fiyatı konularında bilgi vererek insan davranışlarını belli bir yönde etkilemek amacıyla kullanılan kitle iletişim tekniklerdir.

Pazarlama, mal, hizmet ya da ürün ve fikirlerin üreticilerden tüketicilere ulaştırılması ve tüketici ihtiyaç ve isteklerinin karşılanmasına yönelik faaliyetler ile gelecekte olabilecek ihtiyaçlarını tahmin etmek ve yaratmak üzere araştırma, geliştirme, fiyatlandırma ve tutundurma faaliyetlerinin bütünü olarak tanımlanmaktadır. Bu noktada pazarlama teknikleri, reklam faaliyetlerini de içine alan daha geniş bir kavram olarak karşımıza çıkmaktadır.

İnternet mecrasında yapılan reklamlar, diğer mecralarda yapılan reklamlardan birçok bakımdan ayrılır. Bir kere başka hiçbir mecrada olmayan iki taraflılık, İnternet mecrasında vardır. Maliyetler diğer mecralara göre son derece ucuzdur ve reklamın etkisi bu mecrada daha kolay ölçülebilmektedir. Reklamın muhatapları, İnternet mecrasında aktiftir. Genellikle, reklamı bulan muhataplardır. Ya bir arama motorundan ya da bir reklam banner'ini tıklayarak reklama ulaşırlar. Yahut da ilgilendiği konuların takibi sebebiyle bu muhataplara ilgilendiği mal ya da ürünlerin reklamları gelmektedir.

Banner

Reklam ve tanıtım amaçlı hazırlanan, web siteleri ile gazetelerde başlık ya da alt kısmında yer alabilecek ölçülerde ya da afiş olarak, tasarlanmış kurumsal iletişim öğesidir.

dikkat

Bannerlar genelde logo ile bütünleşik olarak kullanılır. Siteyi görsel açıdan zenginleştirdiği gibi ziyaretçileri de olumlu yönde yönlendirmek için kullanılır. Hareketli bannerlar genelde .gif veya .swf (flash) uzantılarına sahip olurlar. Bannerların kullanımını düzenlemek için dünya genelinde bazı standartlar belirlenmiştir.

Başlıca İnternet Reklam Türleri

İnternet teknolojilerinin gelişmesi ile birlikte ortaya yeni sektörler çıkmakta, yeni iş kolları doğmakta veya mesleklerin icra şekli değişmektedir. Reklam, bir ürün veya hizmetin tanıtımı için öteden beri kullanılan bir yoldur. Reklamın niteliğinde bir değişiklik olmamakla birlikte İnternet teknolojisinin gelişmesi ile birlikte icrasında birtakım değişiklikler meydana gelmiştir. Bilişim teknolojilerinin hızlı gelişimi, her geçen gün yeni bir reklam türünü karşımıza çıkarmaktadır. Seyredilen bir film ya da dizide aktörlerin giydikleri elbiselerin mausu üzerine getirdiğimizde marka ve fiyatının öğrenilebilmesinden, çerez tabir edilen bilgilerin izinde doğrudan hedefe yapılan reklamlar ve Google'ın adwords reklam sistemi. Bunlar şimdilik bizlerin tanıdığı reklam türleri. Ancak bu hızlı gelişen teknolojide ve teknolojinin yakınsaması nedeniyle karşımıza yeni dönemlerde çıkacak yeni reklam türlerine hazırlıklı olmalıyız.

Yakınsama, tek bir cihazda birden fazla teknolojik cihazın işlevlerinin birleştirilmesidir. Örneğin cep telefonunda televizyon, radyo ve bilgisayarın birleştirilmesi gibi.

Elektronik Ortamdaki Reklamlara İlişkin Hukuki Hukuki Çerçeve

Elektronik ortamda reklamlara ilişkin özel bir düzenleme bulunmamaktadır. Bazı alanlarda reklamlara ilişkin özel düzenlemeler vardır. Örneğin radyo ve televizyonlarda yayınlanan reklamlara ilişkin genel bir kanuni çerçeve vardır (6112 sayılı Radyo ve Televizyon Kuruluş ve Yayın Hizmetleri Hakkında Kanun, m. 10 vd). Buna karşın elektronik ortamda reklamlara ilişkin özel bir düzenleme bulunmaz. Bu nedenle elektronik ortamda yapılan reklamların hukuki çerçevesi ilgili yasal düzenlemeler çerçevesinde belirlenir.

Elektronik ortamda yapılan reklamlar, tüketicilere yönelik olacağı için tüketici mevzuatında bulunan düzenlemeler de reklamların hukuki çerçevesini çizecektir. Bu düzenlemeler, İnternet ortamındaki reklamların genel çerçevesini de belirler. Bazı ürünlerin reklamlarının yapılması da yasaktır. Bu çerçevede bu tür ürünlerin reklamlarının İnternet ortamında yapılması da sınırlandırılmıştır. Yine İnternetteki reklamlara ilişkin diğer bir sınırlama da bazı mesleklere ilişkindir. Aşağıda bu çerçeveyi bir şema hâlinde görebilirsiniz. Reklamlar konusundaki bir diğer genel düzenleme ise Türk Ticaret Kanunu ile Borçlar Kanunu'nda bulunan haksız rekabete ilişkin düzenlemelerdir.

Şekil 6.5 Elektronik ortamdaki reklamların hukuki çerçevesi

Kural: Reklam Serbestisi

Elektronik ortamda reklam yapmak için özel bir izne ihtiyaç bulunmaz. Radyo ya da televizyon mecrasında olduğu gibi elektronik mecraya özgü belirli kısıtlamalar da bulunmamaktadır. Bu nedenle İnternet ortamında reklam yapmak serbesttir. Ancak bu durum, İnternet ortamındaki reklamlar için hiçbir kuralın ya da sınırlamanın bulunmadığı anlamına da gelmemelidir. İnternet ortamında reklam faaliyetleri için serbesti esası yanında riayet edilmesi gereken genel ilkeler ve reklam yasakları da vardır.

Elektronik Ortamda Yapılacak Reklamlara İlişkin Genel İlkeler

Yukarıda bir şema hâlinde verdiğimiz düzenlemelerden yola çıkarak elektronik ortamda yapılacak reklamlara ilişkin genel ilkeleri sıralamak mümkündür. Bu ilkeler reklam mecralarına göre değişiklik gösterebilecek olmakla birlikte ortak ilkeler olduğu söylenebilir. Bu ilkeler, Türk Ticaret Kanunu ve Borçlar Kanunu'nda bulunan haksız rekabet kurallarından ve tüketicilere ilişkin mevzuat esas alınarak belirlenmiştir:

a. Reklamların aldatıcı, yanıltıcı ve haksız rekabete yol açar nitelikte olmaması,
b. Karşılaştırmalı reklam yapılıyor ise karşılaştırılan ürünlerin aynı nitelikte olması ve müşteriye yarar karşılaştırmaların yapılması, karşılaştırılan hususların ölçülebilir olması,
c. Reklamı yapılan mal ve hizmetlerin toplam bedeli hakkında yanıltıcı bilgilerin verilmemesi,
d. Sayısal verilere dayanan reklam unsurlarının bilimsel test ve raporlara dayanması,
e. Rakiplerin kötülenmemesi, karalanmaması,

f. Rakiplerin itibarından haksız yararlanmaya yol açılmaması,
g. Örtülü reklamlarla bilinçaltı reklamların yapılmaması,
h. Çocuklara yönelik reklamlarda onların zihni durumlarını sömürecek, onları gerçek dışı beklentilere ya da şiddete itecek reklamlara yer verilmemesi,
i. Kişisel hesaplarına istenmeyen reklam içeriklerinin gönderilmemesi,
j. Kişisel verileri esas alan reklamlarda ilgilisinden izin alınması,
k. Bir başkasına ait fikri ya da sınai hakkın kullanımına riayet etmek,
l. Ayrımcı, aşağılayıcı ya da saldırgan ifadelere reklamlarda yer verilmemesi.

Temel olarak hangi türden olursa olsun reklamlara ilişkin bu temel ilkeler, elektronik ortamda yapılan reklamlarda da geçerlidir. Vurgulamak gerekir ki yukarıdaki ilkeler, elektronik ortamın çoklu ve etkileşimli ortamı dikkate alınarak uygulanmalıdır.

Reklam Yasakları

Bazı meslekler için reklam yasakları vardır. Bu mesleklerde reklam yasaklarının getirilmesinin nedeni, bu mesleklerin hayati öneme sahip olması ve reklam yolu ile bu hizmete ihtiyaç duyanların yanıltılması endişesidir.

Normal mesleki hayatlarında reklam yasağına tabi olan meslek grupları, avukatlar, doktorlar, eczacılar ve mali müşavirlerdir. Bu meslek grupları kendi mevzuatları gereğince reklam yapamazlar. Ancak yine belirtmek gerekir ki bu tür meslekleri icra edenlerin hangi tür olursa olsun reklam yasağına tabi oldukları için web sayfaları da problem olarak görülebilmektedir. Web sayfaları, sadece bir reklam aracı olarak algılanmamalıdır. Bu meslek gruplarının kendilerini ve mesleklerini tanıttıkları web sayfaları aynı zamanda bilgiye erişimin de temel bir unsuru olarak değerlendirilmelidir. Bu çerçevede web sayfalarının içeriklerine odaklanılmalı, gerçekten reklam olarak değerlendirilecek olanlar yasaklanmalıdır.

Elektronik ortamda bazı ürünlerin reklamlarının yapılması da o ürünlere ilişkin yasal düzenlemeler gereği yasaktır. Bunlardan biri ilaçtır. İlaçların reklamının yapılıp yapılmaması konusunda değişik anlayışlar bulunmaktadır. Reklama karşı olanların argümanlarının en başında uygun olmayan ilaç kullanımı ve paralelinde ilaç satışlarına artış, reklamlarda ilacın yararları ile yan etkileri konusunda bilgi vermede dengelerin bozulma olasılığı, reklamlara ağırlık veren ilaç firmalarının araştırma geliştirme çabalarını ihmal etme olasılığı, bu tür reklamların tüketicinin kafasını karıştıracağı endişesi gelmektedir. Buna karşın, tüketiciler ise kendilerine yönelik reklamlarla aydınlatıldıkları ve bilgilendirildikleri için konuya daha olumlu yaklaşmaktadır. Reçeteli ilaçlar için genel bir reklam yasağı getirilmiştir. Bu yasağın amacı, tüketicinin zarar görmesinin engellenmesidir. İspençiyari ve Tıbbi Müstahzarlar Kanunu'nun 13. maddesine göre ilaçların övülmesi veya aslında sahip olunmayan özellikleri ile reklamının yapılması yasaklanmıştır. Sadece tıpla ilgili dergilerde reklama izin verilmiştir.

dikkat

Elektronik ortamda bazı ürünlerin reklamlarının yapılması da o ürünlere ilişkin yasal düzenlemeler gereği yasaktır. Bunlardan biri ilaçtır.

Reçetesiz satılan ilaçlara ilişkin olarak ise her ne kadar sadece gazete ve tarifnamelerde bir serbesti var gibi görünse de daha sonra çıkarılmış bulunan Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında 6112 sayılı Kanun'un 11. maddesinde izin verilmiştir. Böylece Türk hukukunda reçetesiz satılan ilaçların radyo ve televizyon yoluyla reklamının yapılmasına imkân verilmiştir. Bu düzenleme, birçok sağlık kuruluşu tarafından eleştirilmiştir. Bu düzenlemeler ışığında da bilişim ortamlarında reçetesiz ilaçların reklamlarının yapılabileceği sonucuna ulaşılmalıdır.

Alkol ve alkollü içeceklerin reklamı yapılamaz. Kanun'la sadece reklam yasaklanmamış aynı zamanda bu ürünlerin kullanılmasını ve satışını özendiren veya teşvik eden kampanya, promosyon ve etkinlik de yasak kapsamına alınmıştır (**İspirto ve İspirtolu İçkiler İnhisari Kanunu, m. 6).** Yine tütün ürünlerinin ve üretici firmaların isim,

marka veya alametleri kullanılarak her ne suretle olursa olsun reklam ve tanıtımının yapılması, bu ürünlerin kullanılmasını özendiren veya teşvik eden kampanyaların düzenlenmesi yasaklanmıştır. Yine tütün ürünü üreten ve pazarlamasını yapan firmaların, her ne surette olursa olsun etkinliklere isimlerini, amblemlerini veya ürünlerinin marka ya da işaretlerini kullanarak destek olamayacakları da hükme bağlanmıştır (Tütün Ürünlerinin Zararlarının Önlenmesi ve Kontrolü Hakkında Kanun, m. 3). Alkollü içeceklerle tütün ve tütün mamullerinin elektronik ortamda reklamının yapılması da yasaklanmıştır.

İnternette Reklamlara İlişkin Özel Sorunlar

İnternet yoluyla reklamın kullanıcılara ulaşması son derece kolaylaşmış, ayrıca elektronik posta adreslerine gönderilen reklamlar ile aracısız reklam imkânına kavuşulmuştur. E-posta ile yapılan reklamlar, klasik usulde yapılan reklamlara göre daha avantajlıdır. Bu tür reklamlar öncelikle tüketiciye doğrudan ulaşmaktadır. Posta kutusunu açan kişi, içeriğini okumasa bile en azından firmanın adı ile karşılaşmaktadır. Ayrıca bu tür reklamlar, diğer reklam usullerine göre son derece masrafsızdır. E-posta yolu ile yapılan reklamların bir başka avantajı ise müşteri kitlesine hızlı ulaşmasıdır. Bir tuş yardımı ile aynı anda binlerce adrese reklam gönderme imkânı mevcuttur. E-posta yolu ile reklam yapmak telefon ile reklamdan daha güvenlidir ve belirli bir zamanda yapılmasına da gerek yoktur. İş saatleri dışında da gönderilen e-postalar, ertesi iş günü reklam yapılan kimsenin bilgisayarında okunabilecektir. E-postayla muhtemel müşteri kitlesinin seçimini yapmak daha kolaydır. Kitap alıcılarının e-posta adreslerinin toplanması ve sadece onlara yönelik kitap reklamı yapılması gibi. Nihayet bu reklamlar daha ucuza mal edilebilmektedir. Bütün bu avantajlı tarafları ile elektronik posta yoluyla reklam günümüzde bir sektör hâline gelmiştir.

İzinsiz Elektronik Postalar

Doğrudan müşteriye yapılan bu reklam türü, reklamı yapan ve reklamı yapılan açısından faydalı olmakla birlikte; elektronik postasına reklam gönderilen kimseler açısından faydalı görülmeyebilir. Posta kutusu dolan ve bu sebeple kendisine gönderilen diğer e-postaları alamayan İnternet kullanıcıları bu durumdan yakınmaktadır. Yine bu tür reklamların zaman israfı olduğu, İnternet kullanma kapasitelerini boşa harcadığı gerekçeleriyle eleştirilmektedir. Hepsinden önemlisi, kişinin rızası dışında onunla iletişime geçilmektedir. Bu tür reklamların hiçbir kurala bağlı olmaması nedeniyle de kişilere ait veriler (telefon numaraları, e-posta adresleri vb.) kişilerden izinsiz toplanmakta ve satılmaktadır.

Hiçbir temas olmaksızın tartışma forumlarından, dağıtılan listelerden, piyasadaki izinsiz veri tabanlarından ve web sayfalarından elde edilen elektronik adreslere alıcının talebi olmaksızın ara sıra büyük hacimlerde gönderilen ve ticari amaç taşıyan e-postalar, izinsiz e-postadır.

İzinsiz e-posta ya da geniş anlamı ile ticari iletiler konusunda dünyada iki sistem bulunmaktadır. Bunlardan ilki, ilk ticari iletinin izinsiz de olsa gönderilebilmesi ancak ticari iletiyi alan kimsenin bir daha ileti almayacağını bildirerek sistemden çıkabilmesi (opt-out); ikincisi ise ilk ticari iletinin dahi önceden izin almak suretiyle gönderilebilmesidir (opt-in).

Elektronik Ticaret Kanunu'nda karma bir sistem benimsenmiştir. Buna göre esnaf ve tacirlere gönderilecek ilk ticari ileti için izin alınmasına gerek yoktur. Buna karşın esnaf ya da tacirler, sonraki iletileri almak istemeyebilirler (m. 6/2). Buna karşın diğer kimselere önceden onay alınmaksızın ticari ileti gönderilemez. Bu hususa aykırılık hâlinde Kanun'un 11. maddesine göre idari para cezası yaptırımları uygulanır.

İzinsiz ticari iletilere ilişkin şikâyetlerin yapılabilmesi için Ticaret Bakanlığı'nın devreye sokmuş olduğu özel sisteme http://tiss.gtb.gov.tr/gtb/giris.xhtml adresinden erişebilirsiniz.

Esnaf ve tacirlere gönderilecek ilk ticari ileti için izin alınmasına gerek yoktur.

Arama Motorlarında Kelime Tabanlı Reklamlar (Adwords Reklamlar)

Dünyanın tanınmış arama motoru Google, "Sponsore Edilmiş Bağlantılar" şeklinde hazırlanmış "AdWords" adını verdiği ve reklam verenlerin reklamlarını, aramada kullanılan kavramlarla bağlantılı olarak kullanıcılara gösteren bir sistem kullanmaktadır. Adwords, İngilizce *"advertising words"*un kısaltılmışıdır ve işletmelerin, anahtar kelimelere bağlı olarak İnternet arama motorlarında yaptıkları reklamları ifade eder. Keyword advertising, İnternet arama motorlarının temel gelir kaynağını oluşturmaktadır. Pazarın lideri konumundaki Google kendi reklam programını "*Google Adwords*" olarak adlandırmaktadır. Diğer İnternet arama motorları da benzer sistemler kullanmaktadır.

Başlangıç itibarıyla arama motorlarında reklamlar; cins, meslek ya da bir ürün veya ürünün özelliğine göre kullanıcının karşısına çıkarılmakta iken zaman içinde rakip firma isimleri, tanınmış kişiler ya da rakip markalara göre çıkarılmaktadır. Sağ tarafta çıkarılan ve rakip firmanın unvanı ya da markasına ayarlı reklamların her "tık"lanmasında Google'a kararlaştırılmış bir ücret ödenmektedir.

Web sitesi birden çok reklama imkân verdiğinden, reklamların kaçıncı sırada yer alacağını, işletmelerin kendileri belirlemektedir; zira sıralama, işletmenin reklama her tıklama için ödemeye hazır olduğu fiyata göre belirlenmektedir. Google Adwords reklamlarında, bir anahtar sözcük için en yüksek ücreti ödeyen kimse reklam sıralamasında yukarılarda, hatta ilk sırada yer almaktadır. Reklam veren işletmeci, İnternet kullanıcısının reklamı dikkate alıp reklamdaki linke tıklayarak işletmenin İnternet sitesine girdiği tıklamalar için reklam ücreti ödemek durumundadır.

Bu türden reklamlarda temel mantık, İnternette çok aranan bir kavramın tespiti ve reklamın bu kavramı arayanların karşısına çıkarılmasıdır. Bu ünlü bir sanatçı, sporcu olabileceği gibi çok tanınmış bir marka da olabilir.

Esasen bu türden bir reklam prensip olarak yasak değildir. Ancak reklamın bağlandığı kavram, bir marka ya da ticaret unvanı ise ya da kişi ismi ise bazı ihlallerin ortaya çıkacağı söylenebilir.

Google adwords reklamların bir marka ihlali olup olmadığına ilişkin mukayeseli hukukta farklı yaklaşımların olduğu görülmektedir. Bu yaklaşımların temeli ise adwords reklamda markanın fonksiyonlarının kullanılmasının ihlal teşkil edip etmediğidir.

Adwords reklamların nasıl işlediği dikkate alındığında, bilhassa rakip şirketin markasının çekiciliğinden faydalanıldığı, teknolojinin yardımı ile reklamı yapılan markanın öne çıkarıldığı görülmektedir. Bu hâlde aslında adwords reklam, mahiyet itibarıyla "metatag-yönlendirici kod" olarak kullanımın farklı bir uygulamasıdır.

556 sayılı Markaların Korunması Hakkında Kanun Hükmünde Kararname'de 21.1.2009 tarihinde yapılan değişiklikle marka sahibine işaretin markasal kullanımını yasaklama hakkı verildiği gibi ilave olarak bazı kullanımları da yasaklayabilme imkânı getirilmiştir (m. 9). Bu kullanımlardan biri de elektronik ortamdaki kullanımdır. Bu hükme göre, "işareti kullanan kişinin, işaretin kullanımına ilişkin hakkı veya meşru bir bağlantısı olmaması koşuluyla, işaretin aynı veya benzerinin İnternet ortamında ticari etki yaratacak biçimde, alan adı, yönlendirici kod, anahtar sözcük veya benzeri biçimlerde kullanılması" yasaktır.

Rakip markanın adwords reklamda anahtar ve yönlendirici sözcük olarak kullanıldığı aşikârdır. Hâl böyle olunca 556 sayılı KHK'de yapılan son düzenlemeden sonra "adwords" reklamın bir marka ihlali olarak kabul edilmesi zorunlu olacaktır.

Adwords reklamlarda bir kişi isminin kullanılabilmesi de mümkündür. Örneğin İbrahim Tatlıses, Funda Arar gibi sanatçıların ismi hâlihazırda adwords reklamlarda kullanılmaktadır. Herhangi bir kimseden izin alınmaksızın kişinin adının kullanılamayacağı MK m. 26 ile açıkça hükme bağlanmıştır. Bu hükme göre "Adı haksız olarak kullanılan kişi buna son verilmesini; haksız kullanan kusurlu ise ayrıca maddi zararının giderilmesini ve uğradığı haksızlığın niteliği gerektiriyorsa manevi tazminat ödenmesini isteyebilir.". Bazı hâllerde özellikle de kişinin isminin şahsiyetini rencide edebileceği reklamlarda kullanılabilmektedir.

Kişi isminin şahsiyetini rencide edecek linklerde ve web sayfalarında adwords kelime olarak seçilmesi hâlinde MK m.26'ya göre adının kullanımının engellenmesinden başka maddi ve manevi tazminat davalarının açılabilmesi de mümkündür.

Öğrenme Çıktısı

4 Elektronik reklamları betimleyebilme

Araştır 2

Elektronik ortamda yapılan reklamlar ile ilgili çocukları koruyucu özel ilke veya ilkeler mevcut mudur?

Reklamının yapılması yasak olan mal ve hizmetler hangisidir?

İlişkilendir

Çocukları koruyucu ayrı ilkeler olmalı mı? Benzeri, korumaya ihtiyaç duyan şahıs grupları var mı?

Anlat/Paylaş

Elektronik ortamda yapılan reklamlara ilişkin ilkeler hakkında arkadaşlarınıza bir kısa e-mail hazırlayarak gönderiniz.

ELEKTRONİK ORTAMDA HAKSIZ REKABET

Rekabet toplum hâlinde yaşayan insanlar arasında her zaman ortaya çıkabilecek bir psikolojik vakıadır. İnsanların daha iyi şartlar altında hayatlarını sürdürebilmek için birbirleriyle ve tabiatla yapmakta oldukları mücadele bir tür rekabettir. Hangi amaçla yapılırsa yapılsın rekabet, kötüye kullanılmadığı müddetçe toplumun ilerlemesi için gereklidir ve topluluk hayatına büyük katkı sağlar.

Rekabetin yapılmasında uygun araçların kullanılması, ahlak ve dürüstlük kurallarına uygun davranmak gerekmektedir. Bu yönüyle rekabetin kanuna uygun olması ve de öyle kalması da şarttır. Aksi hâlde bu durum, haksız rekabet olarak adlandırılır ve hukukun öngördüğü yaptırımlarla karşılaşır.

Rekabet, dünyanın var oluşundan bu yana yaşanan ve ölçülü olduğu müddetçe arzulanan bir olaydır. Rekabet, mal hizmetlere kalite kazandırmakta, tüketicinin mal hizmetleri daha düşük bedellerle alabilmesini sağlamaktadır. Rekabetin korunması için bütün ülkelerde ilave önlemler alınmaktadır. Örneğin bu durum Amerika'da Anti-tröst yasaları ile sağlanırken Avrupa Birliğinde mal ve hizmetlerin serbest dolaşımı ve monopol yasakları ile sağlanmıştır. Rekabet olgusu bir yandan rekabetin yapılması yönünde kanuni düzenlemeler ile diğer taraftan rekabetin kötüye kullanılmaması için yapılan düzenlemelerle korunmaktadır. Haksız rekabet, ekonomik rekabetin her türlü kötüye kullanımı olarak tanımlanmaktadır. Haksız rekabet yasalarının iki temel fonksiyonu bulunmaktadır. Bir taraftan piyasaya katılanların alıcılar etrafındaki mücadeleleri düzenlenirken diğer taraftan serbest rekabetin işlevi korunmaktadır.

Bir ara sonuç olarak rekabetin korunması için kullanılan iki enstrüman bulunmaktadır. Bunlardan ilki, "rekabetin (anti-tröst) korunması" yasaları, ikincisi ise haksız rekabet yasalarıdır. Bu çalışmada, İnternet ortamında yapılan faaliyetlerin ikinci ve daha sık rastlanan türü ile yani haksız rekabet hükümleri açısından bir değerlendirilmesi yapılacaktır.

İnternet ortamında meydana gelen faaliyetlerin hukuka uygunluğunda ilk amaç elde bulunan teknolojinin kötüye kullanımının önlenmesidir. Fakat İnternet ortamında kötüye kullanımın çok değişik türlerinin ortaya çıktığı görülmektedir. Her bir kötüye kullanım görünümü için özel hükümler çıkarılması ise mümkün değildir. Özel hukuk alanında soyut norm koyabilme imkânından yararlanan hukuk bilimi, soyut norm vaz'ı ile hayatın değişik görünümlerini düzenleme altına almaya çalışmıştır.

Gelişmiş ülkelerde haksız rekabet hükümlerinin son derece geliştirildiği, özel hukukun tüm alanlarında uygulanabildiği görülmektedir. Bunların ötesinde kötüye kullanımın yaptırıma tabi tutulabilmesi gerekmektedir. Özel hukukun diğer hükümleri ile kıyaslandığında bu faaliyetlerden zarar gören kimselerin haklarının haksız rekabet hükümleri ile daha iyi korunduğu görülmektedir.

Haksız rekabete ilişkin düzenlemeler Türk hukukunda iki Kanun'da düzenlenmiştir. Bunlardan ilki Türk Ticaret Kanunu diğeri ise Borçlar Kanunu'dur. Ancak temel ve ayrıntılı düzenlemelerin Türk Ticaret Kanunu düzenlemeleri olduğu söylenebilir. Türk Ticaret Kanunu'nun 54. maddesinde haksız rekabete ilişkin çok sayıda örnek verilmiştir. Ancak bu sayımlar, sadece örnek kabilinden sayımlar olup sınırlayıcı bir sayım değildir ve bilişim ortamında çok sayıda haksız rekabetin görünümleri karşımıza çıkabilecektir. Aşağıda bunlar ele alınacak olmakla birlikte bunların bugün karşımıza çıkan örnekler olduğu daha farklı haksız rekabet hâlleri ile her zaman karşılaşılabileceği unutulmamalıdır.

İnternette Haksız Rekabet Örnekleri

İnternette haksız rekabetin farklı görünümleri söz konusudur. Aşağıda farklı örneklerle mesele derinlemesine incelenmiştir.

Alan Adı Kullanımı Yolu ile

Alan adı haksız rekabetin tipik hâlleri söz konusu olmaktadır. Haksız rekabet hükümlerinin uygulanması, özellikle tescil edilmemiş ancak fiili olarak kullanılan ticari isimlerin hak sahibinden başkası tarafından kullanılmasında söz konusu olur. Bir başka haksız rekabet hâli ise cins ve meslek isimlerinin veya tanınmış diğer isimlerin alan adı olarak kullanılması hâlidir. Bu tür haksız rekabet hâlleri uygulamada en yaygın görülenidir.

Alan Adı
İnternet Alan Adları Yönetmeliği m. 3'e göre, İnternet üzerinde bulunan bilgisayar veya İnternet sitelerinin adresini belirlemek için kullanılan İnternet protokol adresini tanımlayan adları ifade eder.

Tescil edilmemiş olan bir markanın MarKHK'nin hükümleri ile korunması mümkün değildir. Tescil edilmeyen bir markanın ve yine diğer ticari isimlerin alan adı olarak seçilmesi hâlinde haksız rekabet hükümlerine göre korunması mümkündür. Alan adı kullanımı yolu ile haksız rekabetten bahsedebilmek için; a. Bir fiil ile ekonomik serbest rekabet hakkı kötüye kullanılmış olmalıdır, b. Bu kötüye kullanma, iyi niyet kurallarına aykırı bir kötü kullanma niteliği taşımalıdır, c. Haksız rekabet teşkil eden fiil dolayısıyla bir başkasının ekonomik yararları zarar görmüş veya zarar görme tehdidine maruz kalmış olmalıdır. Tescilli olmayan bir markanın alan adı olarak seçilmesi hâlinde şartları oluşmuşsa haksız rekabet davası açılabilme imkânı mevcuttur. Alan adı olarak kullanılan ve başkasına ait tescil edilmemiş marka ve diğer ticari isimlerin kullanılması, bir yanılmaya yol açmalıdır veya yanılma tehlikesi bulunmalıdır. Burada yanılma veya yanılma tehlikesinin varlığına, kullanılan alan isminin bütünü göz önünde tutularak karar verilmesi gerekmektedir.

Alan adı olarak kullanılan isimlerin işyeri hakkında yanlış ve yanıltıcı olması durumu da haksız rekabet hâlini teşkil edebilir. Alan adlarının iş yeri, mallar ve hizmetler hakkında yanlış yönlendirmesine şu örnekler verilebilir: Devlete ait ya da bir kurumsal organizasyonuna ait üst düzey alan adlarının kullanılması da haksız rekabet sayılabilir. Örneğin "org" üst düzey alan adını bir ticaret şirketinin alan isminde kullanması, eğitim kurumlarına ayrılmış olan "edu" alan isminin ticarethane tarafından kullanılması, gibi.

Yine bir diğer tanınmış şirketi veya ürünü karalayıcı alan isminin alınması hâlinde haksız rekabet hâli söz konusu olmaktadır. Örneğin "karaca" markasına ilave yaparak "çürük karaca" alan isminin kullanılması gibi.

Ticari hayatta kullanılan meslek isimleri ve cins isimlerinin alan adı olarak alınması hâlinde ortaya birtakım problemler çıkmaktadır. Alan adlarının temel özelliği, kullanılan bir alan adının dünyada teknik olarak sadece bir kez kullanılabilmesidir. Yani herhangi bir alan adından dünyada sadece bir tane bulunmaktadır.

Cins ve meslek isimlerinin alan adı olarak kullanılması hâlinde bu meslek ismini ve cins ismini kullanan kimse büyük bir avantaj elde etmiştir. Çünkü bu tür alan isimleri İnternette konuyu araştıran kimseler için çok çekicidir. Arama motorlarında meslek ve cins isimlerini yazan kimselerin karşısına ilk gelecek site adresi bu adresler olacaktır. Arama motorlarının kanalize etme fonksiyonu sayesinde kullanıcılar bu sitelere yönlendirilmektedir. Bu tür alan isimlerini alan kimselerin aslında temel hedefi de budur. Bu nedenle www.avukat.com.tr ya da

www.muhasebe.com.tr gibi alan adlarının alınması haksız rekabet sayılmalıdır.

Genel isimler veya meslek isimlerinin bir kamu hizmeti yapan kurumun kullanacağı isimler de olabilir. Bu hâlde genel olarak bu tür alan isimlerinin mahkeme tarafından silinmesine karar verilmektedir. Bir Alman mahkeme kararında "bahnhof.de" (istasyon.de) alan adı üzerinde Alman Demiryollarının öncelikli bir hakkı bulunduğu, bir diğer kararda ise "amtsgericht.de" (sulh mahkemesi.de) alan ismi altında İnternet kullanıcılarının ve halkın mahkemeye ait kararları görmeyi bekledikleri için bu ismin alan adının olarak kullanımının haksız rekabet sayılacağı kabul edilmiştir.

Frankfurt Temyiz Mahkemesinin bu kararının sorunun tartışılmasında merkezî bir yere sahiptir. Öncelikle alan ismi olarak seçilen bir isim teknik olarak sadece bir kez kullanılabilmektedir. Dolayısıyla bu özellik sadece genel kavramlar ve meslek isimlerinin alan ismi olarak kullanılmasına özgü olmayıp diğer bütün seçilen alan isimleri için geçerli olmaktadır. Bu sebeple doktrinde özellikle de genel kavramların alan ismi olarak seçilebileceği veya bir alan ismi içinde kullanılabileceği belirtilmektedir. Kullanılan bu tür alan isimlerinin haksız rekabet teşkil ettiğini ileri sürebilmek için mutlaka bir yönüyle rekabeti haksız olarak ihlal ettiğini ispatlamak gerekmektedir. Örneğin açıkça bir rakibi engellemek için alınan bir alan isminde olduğu gibi.

Almanya'da bir avukatlık (hukuk) bürosunun "rechtsanwaelte-koeln.de" (avukatlık bürosu-köln.de) alan ismini alması mahkeme tarafından Alman Haksız Rekabet Yasası'nın 1 ve 3'üncü maddelerine aykırı bulunmuştur. Çünkü bu alan ismi altında Köln şehrinde faaliyet gösteren sadece bir avukatlık bürosu değil, bilakis bütün Kölnlü avukatlar veya Köln Barosunun faaliyet göstereceği beklenmektedir.

İsviçre mahkemesi, davalının sadece "berneroberland.ch" alan adının değişik varyasyonlarını da kendi adına kaydettirmesini, coğrafi bir işaret üzerinde tekel oluşturmanın bir değişik görünümü olarak değerlendirmiş ve iktisadi rekabetin her türlü kötüye kullanımı olarak tanımlamıştır.

Alan adı kullanımı yolu ile bir diğer haksız rekabet hâline örnek de alan adı stoklamalarıdır (Domain-Gabbing). Bilgisayar ve rekabet alanında uzmanlık bilgisine sahip kimseler, tescilli olmayan ama tanınmış markaları ve büyük şirketlerin veya tanınmış insanların isimlerini kendi adlarına almakta ve daha sonra bunları satışa sunmaktadır. Yine meşhur olabilecek ve coğrafi veya teknik alanlarla ilgili birden fazla ismi kendi adlarına alan adı olarak tescil ettirmektedirler. Örneğin bir broker tarafından Bill Gates'in ismi "billgates.com" alan adı olarak kaydedilmiş ve bir milyon dolardan satışa sunulmuştur. Çoğunlukla bu tür alan adları kullanılmamakta veya kullanılsa bile bu web sayfalarında herhangi bir veri bulunmamaktadır. Alan adı stoklaması, özellikle birkaç şekilde söz konusu olabilmektedir. Bir şirket kendi isminin veya markasının belirli bir parçasını, parçalarını veya kısaltmasını alan adı olarak kaydettirmektedir. Bu alan adı, bir diğer firmanın alan ismi ile aynı veya benzer olabilmektedir. İkinci olarak ilgili şirkete satmak, kiralamak veya başka bir bedel almak için uygun kısaltmaları alan adı olarak adına kaydettirme şeklidir. Burada alan adlarının alınıp satıldığı bir borsa türü de ortaya çıkmaktadır. Üçüncü olarak bir şirket, rakiplerinin İnternet ortamında faaliyetini engellemek için kendi adına birçok alan adı almaktadır. Dördüncü olarak ise tanınmış marka veya isimlerin, özel ve gayri ticari amaçlar için alan adı olarak seçilmesi hâlidir.

Alan adları bu şekilde alınmış bulunan şirketler bu durumda söz konusu alan adını satın almakta veya kiralamaktadır. Alan adı borsasının varlığı bile konunun hangi boyutlara ulaştığını göstermektedir.

dikkat

İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) uluslararası düzeyde organize olmuş, İnternet Protokolü (IP) adresi alanı tahsisi, protokol tanıtıcı ataması, genel (gTLD) ve ülke kodu (ccTLD) Üst Düzey Alan ismi sistemi yönetimi ve kök sunucu sistemi yönetimi işlevlerinden sorumlu kâr amacı gütmeyen bir kurumdur.

Alan isminin stoklandığı nasıl ispat edilecektir? ICANN'ın iyi niyete aykırı bir şekilde tescil edilen bir alan isminin varlığını tespitte koymuş olduğu kriterlerden faydalanılabilir:

dikkat

www.icann.org/udrp/udrp-polcy.24oct99.htm.

Alan isimlerini alan kimse, bu isimler üzerinde hak sahibi olan kimseye veya onun rakibine satmak, kiralamak veya bir bedel karşılığı devretmek ve bu alan ismini gerçek maliyeti üzerinde bir fiyatla satmak isterse veya (4/B-I),

Belirli alan isimleri, bu isimler üzerinde gerçek hak sahibinin bu isimleri alan ismi olarak kullanmasını engellemek için alınırsa veya (4/B-II),

Alan isimleri, rakip firmaların işlerini bozmak için kayıt yapılır veya (4/B-III),

Tanınmış isimlerini alan ismi olarak seçerek ve bu isimler üzerinde hak sahibi olduğu (sponsor, vekil vs.) izlenimini yaratarak kendi web sayfasına İnternet kullanıcılarını çekerek ticari kazanç hedeflerse (4/B-IV) bu iyi niyetin kötüye kullanıldığını gösterir. Bu türden bir alan adı stoklaması, haksız rekabet ve marka hukukunun kuralları ile engellenebilir.

dikkat

Alan adı kullanımı yolundan bahsedebilmek için, bir fiil ile ekonomik serbest rekabet hakkı kötüye kullanılmış olmalıdır. Buna ilaveten, bu kötüye kullanma, iyi niyet kurallarına aykırı bir kötü kullanma niteliği taşımalıdır. Son olarak, haksız rekabet teşkil eden fiil dolayısıyla bir başkasının ekonomik yararları zarar görmüş veya zarar görme tehdidine maruz kalmış olmalıdır.

Yanlış ve Yanıltıcı Beyanlar

Sanal ortamda gerçek ortama göre daha fazla yanıltıcı ve yanlış beyanların kullanılabilmesi mümkündür. Zira burada İnternet kullanıcıları sadece web sayfasını görebilmektedir. Çoğu kullanıcı ise bu sayfaların nasıl bir teknikle oluşturulduğunu, sahibinin kim olduğunu bilmemektedir. Bu nedenle web sayfasında kullanılan beyanların ve yapılan aktivitelerin doğru ve gerçeğe uygun olması gerekmektedir. Kullanıcıları yanıltan, işletme ve işletmenin ticari hacmi hakkında yanlış intibalar bırakan beyan ve eylemler haksız rekabet olarak değerlendirilmelidir.

Almanya'da web sayfasında satış işlemlerini gerçekleştiren bir bilgisayar işletmesinin kendisinin 120 şubesi olduğunu, yapılan taleplerin bu şubelerden karşılandığını belirten ilanı haksız rekabet sayılmıştır.

Bir başka örnek de bir web sayfasına konulan ve ziyaretçi giriş sayısını tespit eden sayaçların (counter) maniple edilmesidir. Ücrete tabi servislerde kullanıcıya geçerli olan fiyatlar belirtilmelidir. Böyle bir olayı inceleyen mahkeme "01805" ile başlayan numaranın özel ücrete tabi olduğunun belirtilmemesi hâlini haksız rekabet olarak nitelemiştir. Benzeri bir fiyat aldatmacası ise "dialer" programlarında söz konusudur.

Dialer Program

Bilgisayara yüklenen programlar yolu ile normal İnternet bağlantısını koparark daha pahalı programlara aktaran yazılımlara verilen isimdir.

Belirli hizmetlerin paralı, bazılarının ise ücrete tabi tutulduğu bir İnternet hizmetinin kullanıcısına söz konusu durumun bildirilmemesini mahkeme haksız rekabet saymıştır. Mahkemeye göre bu durum müşteri tarafından öngörülememekte ve anlaşılamamaktadır.

Bir mahkeme kararında ise "parasız İnternet", "Nette parasız/özgür" gibi reklamlar haksız rekabet olarak nitelendirilmiştir. Mahkemeye göre bu tür ilan ve reklamlardan müşterilerin anladığı telefon bağlantı ücretinin de olmamasıdır. Oysa gerçek durum, İnternet kullanıcısının beklediğinden farklıdır.

Başlık Tekniği (Meta-Tag)

Browserlerin hazırlanan sayfaya yöneltilebilmesi için arama mekanizmalarınınn meta-taging denilen bir yöntemle maniple edilmesi gerekmektedir. Danimarka mahkemesi, bir kararında Melitta Grubu'nu arayan İnternet kullanıcılarının, meta-taging usulüyle bir kahve filtre torbaları imal eden firma tarafından kendi sitelerine çekilmesini dürüstlük kuralına aykırı bulmuş ve haksız rekabet olarak nitelendirmiştir. Bu yönteme verilen güzel bir örnek de şudur: Bir işyeri sahibi "Biz XXX ürünlerini satıyoruz. YYY ürünleri de iyi olmasına karşın bunları satmıyoruz", şeklinde bir ibareyi web sayfasında kullanmıştır. Arama motorlarına "YYY" kelimesi verildiğinde otomatik olarak söz konusu işyeri sahibinin web sayfası da sonuç listesi içinde yer almaktadır. Diğer yayın araçlarında bu şekilde bir ibarenin kullanılması rekabete aykırı değildir.

Ancak İnternette bu şekildeki bir ibare YYY müşterilerini yanlış yönlendirebilmekte ve uyuşmazlıklara sebep olabilmektedir.

Haksız Rekabette Sorumluluk

Haksız rekabet fiilini işleyen kimsenin sorumlu olacağı açıktır. Ancak İnternet ortamında haksız rekabet fiilini işleyenler yanında haksız rekabete neden olan eylemin ve sonuçlarının ortadan kaldırılabilmesi için sorumlunun yanında İnternet ortamındaki diğer aktörler için başkaca yasal tedbirler de öngörülmüştür. Bu yasal tedbirleri şu şekilde izah etmemiz mümkündür.

Kural olarak haksız rekabete ilişkin olarak TTK m.56'da yer alan tespit men ve ref davaları esasen ancak haksız rekabet eylemini gerçekleştirenlere karşı açılabilir (TTK m.58/1). Ancak bazı hâllerde haksız rekabet fiilini işlememiş olmakla birlikte haksız rekabet eyleminin ortaya çıkmasına katkıda bulunan kimselere, yazı işleri müdürü, genel yayın yönetmeni, program yapımcısı, görüntüyü, sesi, iletiyi, yayın, iletişim ve bilişim aracına koyan veya koyduran kişi ve ilan servisi şefi; bunlar gösterilemiyorsa işletme veya kuruluş sahibi aleyhine de bazı şartlar altında bu davaların açılabilmesi mümkündür.

İnternet ortamında yapılan faaliyete göre birden fazla sıfat/aktör vardır;

İçerik sağlayıcı (content provider): Bilişim ortamında içeriği hazırlayan kimsedir. Haksız rekabet eylemini yapan, örneğin rakibi karalayan yazıyı kaleme alan kişidir.

Misafir eden sağlayıcı (content provider): Bilişim ortamında başkasının hazırladığı içeriği tutan kimsedir.

Aracı hizmet sağlayıcı: Başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişilerdir.

İnternet servis sağlayıcısı (internet provider): Bilişim sisteminin altyapısını hazırlayan kişi ya da kurumdur.

Burada özellikle vurgulamam gerekirse söz konusu sıfat, değişmez bir sıfat olmayıp her eylem ve işlemde değişebilmektedir. Yani bir İnternet servis sağlayıcı, aynı zamanda kendi sayfasında bir içeriği hazırlıyor ise bu fonksiyonu bakımından içerik sağlayıcı sayılır.

Haksız rekabet eylemini gerçekleştiren yanında İnternet'in diğer aktörlerine karşı bir dava açılamaz. Bu husus, özellikle TTK m.58/4'de vurgulanmıştır. Haksız rekabet fiilinin iletimini başlatmamış, iletimin alıcısını veya fiili oluşturan içeriği seçmemiş veya fiili gerçekleştirecek şekilde değiştirmemişse bu maddenin birinci fıkrasındaki davalar hizmet sağlayıcısı aleyhine açılamaz; tedbir kararı verilemez. Böylece, içerik sağlayıcıdan başkası için haksız rekabete dayalı tedbir kararı verilmesinin önüne geçilmiştir. Buna karşın haksız rekabetin olumsuz sonuçlarının kapsamlı veya vereceği zararın büyük olacağı durumlarda ilgili hizmet sağlayıcı da dinlenilerek haksız rekabet fiilinin sona erdirilmesine veya önlenmesine ilişkin tedbir kararı hizmet sağlayıcı aleyhine de verilebilir veya içeriğin geçici olarak kaldırılması dâhil somut olaya uyan uygulanabilir başka tedbirler de alınabilir. Bu hükümlerin bilişim sistemi için uygun bir düzenleme olduğu belirtilmelidir. Zira yersiz verilen tedbir kararları ile bütün bir bilişim sisteminin, e-ticaret sitesinin ya da sisteminin engellenmesi ölçüsüz bir tedbir olurdu.

Öğrenme Çıktısı

5 Haksız rekabetin yeni formlarını sıralayabilme

Araştır 3	İlişkilendir	Anlat/Paylaş
İnternette haksız rekabetin farklı görünümlerini kısaca sayınız.	İnternet üzerinde haksız rekabet uygulamasına hiç rastladınız mı? Öğrendiğiniz türlerden hangisine giriyordu?	İnternet üzerinde haksız rekabet uygulamalarına hakkında çevrenizdekilerle fikir alışverişi sağlayınız.

1 Sözleşme kavramının elektronik ortamda ne anlama geldiğini açıklayabilme

2 Sözleşmelerde dikkat edilmesi gereken noktaların ne olduğunu sıralayabilme

3 Sözleşmelerin nasıl yapılması gerektiğini ifade edebilme

Elektronik Ortamda Sözleşmeler

Sözleşmenin kurulması için gerekli irade açıklamaları, irade açıklamalarının sonuçları, irade açıklamalarından dönebilme imkânları, irade açıklamalarındaki sakatlıklar Borçlar Kanunu'nda düzenlenmiştir. Kanunlarda sözleşmelerin şekil şartına tabi tutulabilmesi mümkündür. Adi yazılı şekil şartı varsa elektronik ortamda kurulan sözleşmelerde şekil şartının tamamlanabilmesi için güvenli elektronik imzaya ihtiyaç duyulacaktır. Güvenli elektronik imzaya ilişkin düzenlemeler ise Elektronik İmza Kanunu'nda düzenlenmiştir. Sözleşmenin taraflarından birinin tüketici olması durumunda, sözleşmenin kurulması ve sözleşmeden caymaya ilişkin özel düzenlemeler ise Tüketicinin Korunması Hakkında Kanun ve ilgili Yönetmeliklerde yer almaktadır. Elektronik ortamda sözleşmeleri etkileyen bir diğer düzenleme ise Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'dur. Bu düzenlemeler yanında sözleşmelerin türüne göre farklı yasal düzenlemelerin uygulama alanı bulabilmesi de mümkündür.

BK m. 1'e göre sözleşme, tarafların birbirine uygun ve karşılıklı irade açıklamaları ile kurulur. İrade açıklamalarının elektronik ortamda yapılması mümkündür. İrade beyanının elektronik ortamda yapılmış olması, sözleşmelerin Borçlar Kanunu'nda düzenlenen prensiplerden daha farklı prensiplere tabi kılınmasını gerektirmez.

Elektronik ortamda yapılan irade açıklamalarına hukukun ne tür sonuçlar bağladığı önem kazanmaktadır. Bu nedenle bu tür işlemlerin yakından ele alınıp değerlendirilmesi gerekmektedir. Elektronik ortamda gerçekleşen irade açıklamaları kendi içinde ikiye ayrılarak incelenmiştir. Bunlardan ilkinde elektronik ortam sadece bir aracıdır. Diğerinde ise iradenin oluşumunda bir insan iradesi olmaksızın bir bilgisayar yazılımı tarafından irade açıklaması yapılmaktadır.

Borçlar Kanunu, irade açıklamasının açık ya da örtülü olabileceğini söylemektedir (m .1/2). Ancak bilişim sistemlerinde bir irade açıklamasından bahsedebilmek için kural olarak açık bir irade açıklamasına ihtiyaç olduğu söylenebilir. Borçlar Kanunu, örtülü kabulü, belirli bir süre susmaya veya başka bir deyişle reddetmeme hâlinde kabul etmiş ve sözleşmenin kurulacağını hükme bağlamıştır (BK m. 6). Oysa, bilişim ortamlarında istisnai durumlar haricinde örtülü kabule yer vermemek gerekir. Yani bir bilişim sisteminde sadece ekrandaki teklifin belli bir zaman içinde reddedilmemesi irade açıklaması olarak kabul edilemez.

Elektronik ortamda akdedilecek sözleşmelere ilişkin olarak Tüketicinin Korunması Hakkında Kanun'un tercih ettiği kavram 'mesafeli sözleşmedir'. Mesafeli sözleşmelerde ayrıntıları yönetmeliklerle belirlenecek konularda teklifin kabulünden önce tüketici bilgilendirilmek zorundadır. Aynı zamanda siparişinin onaylanması hâlinde de ödeme yükümlülüğünün bulunduğu konusunda uyarılmalıdır (m. 48/2). Bu durum, mesafeli sözleşmelerde sıklıkla karşımıza çıkan bilgilendirme yükümlülüğüdür ve tüketicinin bilgilendirildiğinin ispatı da satıcı ya da sağlayıcıya aittir. Satıcı ya da sağlayıcı, siparişten sonra taahhüt edilen süre içinde edimini yerine getirmelidir. Mal ya da hizmetin sağlanması için de mesafeli satışlarda azami bir süre öngörülmüştür. Bu süre 30 günü geçemez. Eğer bu süre aşılır ise bu hâlde tüketici sözleşmeyi fesih hakkına sahiptir (m. 48/3).

öğrenme çıktıları ve bölüm özeti

4 Elektronik reklamları betimleyebilme

Elektronik Ortamda Reklamlar

Mesafeli satışlarda tüketici, satın aldığı mal ya da hizmeti kontrol etme imkânına sahip değildir. Bu nedenle görmediği ya da sadece görsellerini gördüğü bir mal ya da hizmeti şartsız bir şekilde almaktan vazgeçebilir, yani cayabilir. Kanun, tüketiciye hiçbir gerekçe göstermeksizin 14 günlük bir cayma hakkı tanımıştır (m. 48/4). Ayrıca tüketici cayma hakkının varlığı konusunda bilgilendirilmelidir. Eğer bu bilgilendirme yapılmamışsa bu hâlde bu 14 günlük süre ile de sınırlı değildir. Ancak tüketiciye verilen bu cayma hakkı sonsuza kadar da devam etmez, her hâlükârda cayma hakkının bittiği ilk 14 günlük süreden bir yıl sonra sona erer.

Hizmet sağlayıcı, elektronik iletişim araçlarıyla bir sözleşmenin yapılmasından önce; alıcıların kolayca ulaşabileceği şekilde ve güncel olarak tanıtıcı bilgilerini, sözleşmenin kurulabilmesi için izlenecek teknik adımlara ilişkin bilgileri, sözleşme metninin sözleşmenin kurulmasından sonra, hizmet sağlayıcı tarafından saklanıp saklanmayacağı ile bu sözleşmeye alıcının daha sonra erişiminin mümkün olup olmayacağı ve bu erişimin ne kadar süreyle sağlanacağına ilişkin bilgileri, veri girişindeki hataların açık ve anlaşılır bir şekilde belirlenmesine ve düzeltilmesine ilişkin teknik araçlara ilişkin bilgileri ve uygulanan gizlilik kuralları ve varsa alternatif uyuşmazlık çözüm mekanizmalarına ilişkin bilgileri sunar.

5 Haksız rekabetin yeni formlarını sıralayabilme

Elektronik Ortamda Haksız Rekabet

Alan adı haksız rekabetin tipik hâlleri söz konusu olmaktadır. Haksız rekabet hükümlerinin uygulanması, özellikle tescil edilmemiş ancak fiili olarak kullanılan ticari isimlerin hak sahibinden başkası tarafından kullanılmasında söz konusu olur. Bir başka haksız rekabet hâli ise cins ve meslek isimlerinin veya tanınmış diğer isimlerin alan adı olarak kullanılması hâlidir. Bu tür haksız rekabet hâlleri uygulamada en yaygın görülenidir. Tescil edilmemiş olan bir markanın MarKHK'nin hükümleri ile korunması mümkün değildir. Tescil edilmeyen bir markanın ve yine diğer ticari isimlerin alan adı olarak seçilmesi hâlinde haksız rekabet hükümlerine göre korunması mümkündür. Alan adı kullanımı yolu ile haksız rekabetten bahsedebilmek için; a. Bir fiil ile ekonomik serbest rekabet hakkı kötüye kullanılmış olmalıdır, b. Bu kötüye kullanma, iyi niyet kurallarına aykırı bir kötü kullanma niteliği taşımalıdır, c. Haksız rekabet teşkil eden fiil dolayısıyla bir başkasının ekonomik yararları zarar görmüş veya zarar görme tehdidine maruz kalmış olmalıdır. Tescilli olmayan bir markanın alan adı olarak seçilmesi hâlinde şartları oluşmuşsa haksız rekabet davası açılabilme imkânı mevcuttur. Alan adı olarak kullanılan ve başkasına ait tescil edilmemiş marka ve diğer ticari isimlerin kullanılması, bir yanılmaya yol açmalıdır veya yanılma tehlikesi bulunmalıdır. Burada yanılma veya yanılma tehlikesinin varlığına, kullanılan alan isminin bütünü göz önünde tutularak karar verilmesi gerekmektedir.

Alan adı olarak kullanılan isimlerin işyeri hakkında yanlış ve yanıltıcı olması durumu da haksız rekabet hâlini teşkil edebilir. Yine bir diğer tanınmış şirketi veya ürünü karalayıcı alan isminin alınması hâlinde haksız rekabet hâli söz konusu olmaktadır. Örneğin "karaca" markasına ilave yaparak "çürük karaca" alan isminin kullanılması gibi.

1 Elektronik irade açıklaması ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. İnternette yapılan açıklamayı ifade eder.
B. Bir icaba davet şeklindedir.
C. Bir bilgisayar yazılımı yolu ile yapılan icap ve kabulleri ifade eder.
D. Karşı tarafa varması gerekli bir icaptır.
E. Bu tür öneri ve kabullerle bağlı olunmaz.

2 Ürün ve fiyatların da belirtildiği web sayfaları ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Öneridir.
B. Herkese açık bir öneridir.
C. Kabuldür.
D. Bir irade açıklaması olarak değerlendirilemez.
E. Sadece bir reklamdır.

3 Aşağıda sayılan sözleşmelerden hangisi elektronik ortamda yapılabilir?

A. Gayrimenkulün devrine ilişkin sözleşme
B. Evlilik sözleşmesi
C. Resmî şekil şartına tabi sözleşmeler
D. Bütün sözleşmeler
E. Şekle bağlı olmayan sözleşmeler

4 Elektronik ortamda yazılı şekil şartına tabi tutulan bir sözleşmenin yapılabilmesi için aşağıdakilerden hangisi gerekir?

A. Tarafların ayrıca kâğıt ortamında da sözleşmeyi yapması
B. Tarafların tanık göstermesi
C. Tarafların yemin beyanında bulunması
D. Elektronik imza ile sözleşmeyi imzalamaları
E. Güvenli elektronik imza ile sözleşmeyi imzalamaları

5 I. Bu sözleşme geçerli olur.
II. Taraflarca inkâr edilemez.
III. İspat problemi yaşanmaz.
IV. Geçerliliği için elektronik imza ile imzalanması da gerekir.
V. Bu sözleşmeye dair elektronik ortamdaki veriler belge sayılır.

Elektronik ortamda yapılan şekil şartına tabi olmayan bir sözleşme ile ilgili yukarıdaki ifadelerden hangisi doğrudur?

A. I ve II
B. I ve IV
C. I ve V
D. II ve III
E. IV ve II

6 Yazılı şekil şartına tabi olmayan ve 5.000 TL'lik ödemeyi içeren bir sözleşmede güvenli elektronik imza kullanılmışsa bunun sonucu aşağıdakilerden hangisidir?

A. Sözleşmenin geçerliliğini sağlar.
B. Sözleşmenin damga vergisine tabi olmasını gerektirir.
C. Sözleşmenin yazılı şekil şartına tabi olduğunu gösterir.
D. Borcun ispatını sağlar.
E. Borca ilişkin tanık dinleme imkânını verir.

7 Elektronik ortamda kurulan sözleşmelerle ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. E-posta yolu ile sözleşme kurulamaz.
B. E-posta karşı tarafa ulaşsa bile öneriden dönülebilir.
C. Elektronik ortamda irade açıklamasında bulunanların irade açıklamasında hata kabul edilemez.
D. Sözleşmelerin kurulmasında teknik hatalara kullanıcı katlanır.
E. Bilişim sisteminde sadece ekrandaki teklifin belli bir zaman içinde reddedilmemesi irade açıklaması olarak kabul edilemez.

8 Mesafeli sözleşmelerin kurulmasında cayma hakkı kaç gündür?

A. 1 hafta
B. 8 gün
C. 14 gün
D. 1 ay
E. 1 yıl

9 Tüketici mesafeli sözleşmelerde cayma hakkı konusunda bilgilendirilmezse bunun sonucu aşağıdakilerden hangisidir?

A. Satıcı idari para cezası ile cezalandırılır.
B. Cayma hakkını 1 yıl içinde kullanabilir.
C. Cayma hakkı verilmemiş olur.
D. Satım sözleşmesi geçersiz olur.
E. Satım sözleşmesindeki aleyhe şartlar geçersiz olur.

10 Elektronik ortamdaki reklamlar ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır?**

A. Reklamların aldatıcı, yanıltıcı ve haksız rekabete yol açar nitelikte olmamalıdır.
B. Reklamı yapılan mal ve hizmetlerin toplam bedeli hakkında yanıltıcı bilgilerin verilmemelidir.
C. Bir web sayfasında kesintisiz reklam yapılmamalıdır.
D. Rakiplerin kötülenmemeli, karalanmamalıdır.
E. Rakiplerin itibarından haksız yararlanmaya yol açılmamalıdır.

1. A	Yanıtınız yanlış ise "Sözleşmelerin Kurulmasında İrade Açıklamaları" konusunu yeniden gözden geçiriniz.
2. B	Yanıtınız yanlış ise "İrade Açıklamalarının Tasnifi" konusunu yeniden gözden geçiriniz.
3. E	Yanıtınız yanlış ise "Sözleşmelerin Kurulmasında Şekil" konusunu yeniden gözden geçiriniz.
4. E	Yanıtınız yanlış ise "Sözleşmelerin Kurulmasında Şekil" konusunu yeniden gözden geçiriniz.
5. C	Yanıtınız yanlış ise "Sözleşmelerin ya da Elektronik İrade Açıklamalarının İspatı" konusunu yeniden gözden geçiriniz.
6. D	Yanıtınız yanlış ise "Mevcut Hukuk Sisteminde Elektronik Dokümanların İspat Gücü" konusunu yeniden gözden geçiriniz.
7. E	Yanıtınız yanlış ise "Sözleşmelerin Kurulmasında İrade Açıklamaları" konusunu yeniden gözden geçiriniz.
8. C	Yanıtınız yanlış ise "Tüketicinin Korunması Hakkında Kanun'da Mesafeli Sözleşmeler" konusunu yeniden gözden geçiriniz.
9. B	Yanıtınız yanlış ise "Tüketicinin Korunması Hakkında Kanun'da Mesafeli Sözleşmeler" konusunu yeniden gözden geçiriniz.
10. C	Yanıtınız yanlış ise "Elektronik Ortamdaki Reklamlara İlişkin Hukuki Düzenlemeler" konusunu yeniden gözden geçiriniz.

6 Araştır Yanıt Anahtarı

Araştır 1

Taraf iradelerinin elektronik ortamda yani yüz yüze gelmeksizin karşılaştığı ve uyuştuğu elektronik ortamda kurulmuş sözleşmelerdir.

Araştır 2

Çocuklara yönelik reklamlarda onların zihni durumlarını sömürecek, onları gerçek dışı beklentilere ya da şiddete itecek reklamlara yer verilmemesi.

Normal mesleki hayatlarında reklam yasağına tabi olan meslek grupları, avukatlar, doktorlar, eczacılar ve mali müşavirlerdir. Bu meslek grupları kendi mevzuatları gereğince reklam yapamazlar. Ayrıca, Elektronik ortamda bazı ürünlerin reklamlarının yapılması da o ürünlere ilişkin yasal düzenlemeler gereği yasaktır. Bunlardan biri ilaçtır. Sadece tıpla ilgili dergilerde reklama izin verilmiştir. Alkollü içeceklerle tütün ve tütün mamullerinin elektronik ortamda reklamının yapılması da yasaklanmıştır.

Araştır 3

Başlık Tekniği, Yanlış ve Yanıltıcı Beyanlar, Alan adı kullanımı yolu.

Kaynakça

Acar, F. (2000). Uzağa Satış Sözleşmesi Yapımında Tüketicinin Korunması Hakkındaki Avrupa Topluluğu Direktifi (Die neue Richtlinie 97/7/EG). İstanbul Barosu Dergisi, 74, s. 1.

Afra, S. (2004). Dijital Pazar'ın Ortak Noktası E-Ticaret: Dünyada Türkiye'nin Yeri, Mevcut Durum ve Geleceğe Yönelik Adımlar. TÜSİAD, İstanbul (http://www.tusiad.org/__rsc/shared/file/eTicaretRaporu-062014.pdf).

Arkan, S. (1998). Marka Hukuku. Cilt II, Ankara.

Arslanlı, H. (1960). Kara Ticareti Hukuku Dersleri, Umumi Hükümler. İstanbul.

Ayhan, R. (1990). Haksız Rekabet Münasebetiyle Elde Edilen Menfaatlerin İadesi. Konya.

Bettinger, T. (1997). Kennzeichenrecht im Cyberspace: Der kampf um die Domain-Namen. GRUR-Int, H.5.

Bielfeldt, M., Slink, T., Pernice, M., Rappelmund, H. & Scheinpflug, J. (2000). Electronic Commerce. 2. Aufl. Berlin.

Bugiel, A. (2000). Rechtliche Rahmen des E-Commerce in Deutschland und Europa. TOBB, 11, 12 Mayıs.

Demir, M. (2004). Mesafeli Sözleşmelerin İnternet Üzerinden Kurulması. Ankara.

Eichhorn, B. (2000). İnternet-Recht, Ein Lehrbuch für das Recht im World Wide Web. Köln.

Fikentscher, W. & Möllers, M. J. T. (1998). Die (negative) Informationsfreiheit als Grenze von Werbung und Kunstdarbietung. NJW, 18.

Fröhlich, M. (2001). Zentrale Institutionen des deutschenrheberrechts und französischen Droit d'auteur auf dem Prüfstand der elektronischen Netzwerke. Frankfurt am Main.

Funk, A. (1998). Wettbewerbliche Grenzen von Werbung per E-Mail. CR, 7.

Göle, C. (1983). Ticaret Hukuku Açısından Aldatıcı Reklamlara Karşı Tüketicinin Korunması. Ankara.

Halbscheid, W.J. (1988). Schweizerisches Zivilprozes –und Gerichtsorganisationsrecht. 2. Auf. Basel/Frankfurt. A Main.

Hanika, H. (2000). Internetrecht versus Schutz der öffentlichen Gesundheit und Standesrecht. MedR, Heft 5.

Heun, S. E. (1994). Die Elektronische Willenserklaerung, CR.

Hoeren, T. (1997). Cybermannes und Wettbewerbsrecht-Einige Überlegungen zum Lauterkeitsrecht im Internet. WRP, 11.

Hoeren, T. (1997). Werberecht im Internet am Beispiel der ICC Guedilines on Interactive Marketing Communications", Internet und Multimediarecht (Cyberlaw) (Hrsg. Lehmann, M.) Stuttgart.

İmre, Z. (1974). Şahsiyet Hakkının Korunmasına İlişkin Genel Esaslar, Özellikle İsim Hakkı ve İsim Hakkının Korunması. A. Recai Seçkin'e Armağan, Ankara.

İnal, E. (2005). E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması. İstanbul.

Jaeger-Lenz, A. (1999). Werberecht-Recht der Werbung in Internet, Film, Funk und Printmedien. Weinheim.

Karayalçın, Y. (1968). Ticaret Hukuku. Cilt 1, Giriş-Ticari İşletme. Ankara.

Kolb, A. (2001). Cyberethik: Verantwortung in einer digital vernetzten Welt. World Congress Safety of Modern Technikal Systems, Saarbrücken.

Körner, R. & Lehment, C. (1999). Allgemeine Wettbewerbsrecht. Ed. Hoeren, T. & Sieber, U. Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschaeftsverkehrs. München.

Ladeur, K. (1999). Neue Werbeformen und der Grundsatz der Trennung von Werbungund Programm, Virtuelle Werbung, Split Screen und Vernetzung von Medien als Herausforderung der Rundfunkregulierung. ZUM, 10.

Laga, G. (1998). Internet im rechtsfreien Raum? Dissertation, Wien, Geschichte.

Lettl, T. (2000). Rechtsfragen des Direktmarketings per Telefon und E-Mail. GRUR.

Leupold, A. (1998). Die massenweise Versendung von Werbe-e-Mails: Innovatives Direktmarketing oder unzumutbare Belaestigung des Empfaengers. WRP, 3.

Maibach, M.C. (1999). The Internet: The Great Equalizer", Economic Reform Today. Number 2.

Mankowski, P. (1999). Besondere Formen von Wettbewerbsverstössen im Internet und Internationales Wettbewerbsrecht. GRUR Int.

Mayer, F.C. (1996). Recht und Cyberspace. NJW, Heft 28, s. 1782.

Mehner, A. (1999). Wettbewerbliche Bewertung geschaeftlicher Aktivitaeten im Internet und in sonstigen Online Plattform. Cyberlaw (Hrg. Schwerdtfeger/Everyz/Kruezer/Peschel-Mehner/Poeck) Weisbaden.

Müko & Kramer (1993). Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1(3). Auf.

Naumann, T. (2001). Praesentationen im Internet als Verstoss gegen §§ 1, 3 UWG, Unter besonderer Berücksichtigung der Online-Angebote von Rechtsanwaelten. Frankfurt am Main.

Özdemir, H. (2009). Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara.

Öztek, S. (1991). Haksız Rekabete İlişkin Yeni İsviçre Düzenlemesinin Öngördüğü Bazı Haksız Rekabet Halleri. Prof. Dr. Jale G. Akipek'e Armağan, Konya.

Palant & Heinrichs (1996). Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Kommentar, 55. Auf.

Peschel-Mehner, A. (1999). Wettbewerbsrechtlicher Bewertung geschaeftlicher Aktivitaeten im Internet und in sonstigen Online-Plattform. Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck: Cyberlaw, Wiesbaden.

Reich, N. (1997). Die Neue Richtlinie 97/7/EG über den Verbraucherschutz bei Vertragbschlüssen im Fernabsatz. EuZW, Heft 19(97).

Reichelsdorfer, J. (1997). eMails zu Werbezwecken-ein Wettbewerbsstoss? GRUR.

Rosenthal, D. (1999). Unverlangte Werbe E-Mail ohne Rechtsfolgen. Media Lex, 4(99).

Rüßmann, H. (1998). Internationale Zuständigkeit für die Durchsetzung von Ansprüchen aus Geschäfts- und Wettbewerbshandlungen im Internet. JurPC Web-Dok. 108/1998, Abs. 1-56 (www.jurpc.de/aufsatz/19980108.htm).

Sarıakçalı, T. (2008). İnternet Üzerinden Akdedilen Sözleşmeler, Ankara.

Schneider, J. (1997). Handbuch des EDV-Rechts. 2. Aufl. München.

Schwarz, M. Merkmale, Entwicklungstendenzen und Problemstellungen des Internet. http://www.jura.uni-münchen.de/Institute/Internet_I.html,

Taşkın, A. (1992). Tüzel Kişilerin Kişilik Haklarının Korunması. AÜHFD, 42.

Vehslage, T. (1999). Auswirkungen der Fernabsatzrichtlinie auf die Telefon- und E-Mail-Werbung. GRUR, H. 8/9.

Von Herget, H. & Reimer,M. (1996). Rechtsformen und Inhalte von Vertraegen im Online-Bereich. DStR.

Watel, J. (2001). Le probléme du Spamming ou comment guérir le cancer de l'internet. Jurpc Web-Dok. 163, (www.jurpc.de).

Weber, R. H. (1997). Internet als Subventionsnetz? Wettbewerbsrechtliche Rahmenbedingungen von Internet-Dienstleistungsangeboten durch öffentlich kontrollierte: Einheiten. CR1997.

Yasaman, H. (1978). Tanınmış Markalar. Halil Arslanlı'nın Anısına Armağan, İstanbul.

Ziem, C. (2000). Spamming, Zulaessigkeit nach § 1 UWG, Fernabsatzrichtlinie und E-Commerce Richtlinienentwurf. MMR 2000/3; Schrick, A. "Direktmarketing mittels E-Mail und seine Entwicklung", MMR 2000/7.

Bölüm 7

Bilişim Ortamında Fikrî ve Sınai Haklar

Öğrenme çıktıları

1 İnternet Ortamında Fikrî Haklar ve Korunması

1 Eser sahibinin haklarını detaylı bir şekilde açıklayabilme

2 İnternet Ortamında Sınai Hakların Korunması

2 Fikrî ve sınai hakların korunması konusunda internette ne tür özelliklerin olduğunu açıklayabilme

3 İhlallerin nasıl niteleneceğini ifade edebilme

Anahtar Sözcükler: • Dijitalleşme • Eser Sahibinin Hakları • Multimedya • Meta-Tag • Adwords • Alan Adı • P2p-Filesharing • Senkron-Asenkron

GİRİŞ

Bilişim ve iletişim teknolojilerinin gelişmesi ile birlikte fikri haklar, eser, eserden yararlanma ve eser sahibinin korunması önem kazanmaktadır. İnternet'in artan hızı ve yaygınlığı, ayrı bir İnternet kültürünü beraberinde getirmiştir. Yeni nesil, bilişim neslidir ve İnternet ve ağa bağlanma, bu yeni nesil için hayatın vazgeçilmezleri arasındadır. Akıllı cep telefonlarının yaygınlaşması, onların her an ağa bağlılığını sağlamaktadır. Bu durum eser sahipleri için bir taraftan avantaj sağlarken diğer taraftan da şimdiye kadar mevcut olmayan bir başka tehlikeyi de beraberinde getirmektedir.

Eser sahibine İnternet yeni imkanlar sunmaktadır. Eser sahibi eserini daha geniş kitlelere kolayca ulaştırabilmektedir. Eserler için iyi bir reklam yoludur. Eser hakkı sahibi, eserini üçüncü ve ilgili kimselere daha çabuk ve daha ucuz bir reklamla tanıtabilme imkânına kavuştuğu gibi, eserini dijital ortamda yayınlayabilme imkânına da kavuşmuştur. Ayrıca eserler dijital ortamda satışa da sunulabilmektedir.

İNTERNET ORTAMINDA FİKRÎ HAKLAR VE KORUNMASI

İnternet yoluyla dünyanın her tarafından esere ulaşanların çokluğu ve kullanıcıların çeşitliliği, eserin haksız ve izinsiz kullanılması ihtimalini de artırmıştır. Herhangi bir kişisel bilgisayara ve internet bağlantısına sahip olan kimse, internet üzerinde bulunan bir eseri kalite kaybı olmaksızın kopyalayabilmekte ve çoğaltabilmektedir.

Bilişim sisteminde eser sahipleri ile ilgili temel düzenleme, 5846 sayılı Fikir ve Sanat Eserleri Kanununda (FSEK) yer almaktadır. Bunun yanında çok sayıda uluslararası anlaşma da fikri hukukun kaynağını teşkil eder.

İnternet Ortamında Eser ve İnternet'te Eserlerin Yer Alma Türleri

İnternette telif haklarının koruması söz konusu edildiğinde iki türlü ihtimal ele alınmalıdır. Bu ihtimallerden ilki zaten mevcut eserlerin internette sunulması ikincisi söz konusu eserlerin ilk defa internette meydana getirilmesi, orda görülmesidir. İnternet ortamından önce zaten mevcut olan FSEK.m.1 anlamında sahibinin hususiyetini taşıyan ve internet ortamında da sunulabilen müzik, edebiyat ve sinema gibi her türlü fikir ve sanat ürünleridir. Bu ürünler, dijital teknik sayesinde internet ortamında elektronik kitap veya beste olarak sunulmakta ya da hazırlanmış olan web sayfasında seslendirme veya görüntü olarak bir bütün içinde sunulmaktadır.

Eserlerin koruma kapsamı, eserlerin hem münferit olarak hem de bütün içinde korunmasına yönelmiştir. Eserlerin online ortamda sunulması, onların koruma kapsamında herhangi bir değişikliğe uğramasına sebep olmaz. FSEK. m.13/2' de aynı husus vurgulanmaktadır. Bu sebeple eserin umuma arz edilip edilmemesini, yayımlanma zamanını ve tarzını eser sahibinin belirleme hakkı bulunmaktadır (FSEK.m. 14).

Fikir ve sanat ürünleri Kanunda, "sahibinin hususiyetini taşıyan ve ilim, edebiyat, güzel sanatlar veya sinema eserleri sayılan her nevi fikir ve sanat mahsulü" olarak tanımlanmaktadır (FSEK.m.1/A). Ayrıca Kanunda bu tanım altında değerlendirilmesi gereken fikir ve sanat eserlerinin çeşitleri ayrıntılı olarak düzenlenmiştir (FSEK.m.2-7). Bu ayrıntılı sayım şu başlıklar altında toplanmaktadır:

- İlim ve edebiyat eserleri
- Musiki eserleri
- Güzel sanat eserleri
- Sinema eserleri

Bu sayılan fikir ve sanat eserlerinin her birinin internet ortamında sunulması mümkündür. Örnek olarak klasik ressamların eserlerinin sunulduğu web sitesi, müzik eserlerinin elde edilebileceği siteler ve resim eserlerinin bulunabileceği siteler sayılabilir.

İnternete özgü fikri ürünler de olabilir. İnternet ortamındaki hususiyet taşıyan web sayfaları buna örnek olarak verilebilir.

Eserin Niteliği Olarak Dijitalleşme

Elektronik ortamda eserlerin görünüm biçimlerinden bahsederken dijitalleştirme kavramından da mutlaka bahsetmek gerekir. Eser ortaya çıktıktan sonra elektronik ortamda sunulabilmesi için veri mesajları, sayısal bilgiler hâline dönüştürülmektedir.

Fikri haklar için dijitalleşme, bir eserin ortaya çıkarılmasından sonra sayısal hâle getirilmesinden başka bir şey değildir. Teknik bir yenilenmenin mevcut olmasına rağmen telif hakları bakımından olaya bakıldığında yeni bir nitelik değişmesi söz konusu değildir. Dijitalleşmede eser sahibi ile kullanıcı arasındaki menfaat çekişmesi ve hukuki araçlar aynı kalmaktadır. Fikri hakların temel

problemleri, dijital hâle getirilmiş olan eserler için de mevcuttur. Bu temel problem, ortaya çıkarılan eser, mülkiyet hakkı dolayısıyla iktisadi faydanın sağlanabilmesi için uygun bir koruma ile teminat altına alınmasıdır.

Dijitalleşmenin Tehlikeleri

Eserlerin dijitalleşmesinde gözden kaçırılmaması gereken husus, bir eserin dijitalleşmesi ile telif hakkının ihlalinin kolaylaşmasıdır. Birkaç tuş yardımı ile internette dolaşan eserler izinsiz olarak sınır ötesine taşınabilmekte, kopyalanabilmekte ve çoğaltılabilmektedir. Kolayca taklit edilebilme ve yanıltılabilme, kopyalanabilmeye karşı yeni hukuki enstrümanlar aranmakta ve yeni teknolojiler geliştirilmeye çalışılmaktadır. Bu çok kolay kopyalanma tehlikesine karşı teknik önlemler alınmaya çalışılmakta, dijital eserlerde "su üzerine yazı" gibi kopyalanamaz bir hâle getirilmesine çalışılmakta ve Serial Copy Manegement System (SCMS) "Seri Kopya Yönetim Sistemi" ile dijital hâldeki eserlerin sadece bir defa kopyalanmasını sağlayan teknoloji ile korunmaya çalışılmaktadır.

İnternete Mahsus Eser Görünümleri: Çoklu Ortam (Multimedya) Eserleri

Çoklu ortam eseri (multimedya eser), sinema filmi, müzik ve resmi içeren değişik medya ürünlerinin bir arada sunulmasıdır. Ancak bu tanımlamanın son bir tanımlama olmadığını da burada belirtmek gerekmektedir. Çünkü enformasyon teknolojisinin hızlı gelişimi sayesinde multimedya kavramı sürekli bir değişim içindedir.

İnternet üzerinden fikri haklara konu olan eserlerin önemli özelliği, bu eserlerin çoğunlukla çoklu ortam/multimedya özelliği taşımasıdır. Yani eserler, internet üzerinde yazı, görüntü, ses, film ve müzik eserleri ile karışık olarak sunulmaktadır. Dijitalleşme dolayısıyla hem zamana bağlı video ve ses kaydı gibi medya hem de zamana bağlı olmayan kalıcı resim ve metinler gibi medyanın karışımı ile eserler internet ortamına verilmektedir. Kullanıcının isteğine göre bir ortam hazırlanmaktadır. Burada multimedyanın bir diğer özelliği de karşımıza çıkmaktadır ki bu da etkileşimdir. Multimedya ürünleri, tamamen kullanıcı ile iletişime dayanan bir dijital ortamda gerçekleşmektedir. Artık kullanıcılar daha önceki ürünlerdeki gibi sadece programı açmak veya kapamak gibi iki seçenek arasında sıkışmamışlardır. Burada artık kendileri de programa katkıda bulunabilmektedir.

Multimedya ürünleri çevrimdışı (offline) kullanım ve çevrimiçi (online) kullanım olarak öncelikle ikiye ayrılabilir. Çevrimdışı-kullanım, CD gibi veri taşıyıcılarla kullanımı anlatırken, çevrimiçi-kullanım radyo, kablolu yayın ve internet ortamındaki kullanımı anlatmaktadır. Çevrimiçi ve çevrimdışı kullanım yanında sunulan hizmetin interaktif olup olmamasına göre bir ayrım da yapılabilir. Çevrimiçi kullanım, kendi içinde eşzamanlı/senkron ve eşzamansız/asenkron kullanım olarak kendi arasında ikiye ayrılmaktadır. Senkron kullanımda, radyo ve televizyon yayınlarında olduğu gibi eş zamanlı bir tüketim söz konusu iken asenkron kullanımda internet ortamında olduğu gibi eş zamanlı bir tüketim şart değildir. İnternet kullanıcıları, birbirinden farlı zamanlarda sunulanlara erişme ve onları tüketme imkânına sahiptir.

Tablo 7.1 Multimedya Kullanımın Tasnifi

Çevrimiçi		Çevrimdışı
Senkron	Radyo, televizyon	-------
Asenkron	İnternetten web sayfasının çağrılması	Veri taşıyıcılarla kullanım (CD, DVD)

Senkron ve asenkron kullanımlarda fikri haklar bakımından ilginç farklılıklar oluşmaktadır. Örneğin yeniden yayınlama kavramı (FSEK. m. 25) asenkron kullanımlara her zaman uygun düşmemektedir. Ancak internet ortamında yapılan multimedya sunumlar çok çeşitlidir ve hem senkron hem de asenkron sunumlar yapılabilmektedir. Örneğin internet radyo ve televizyonlarında yapılan yayınlar, aynı zamanda senkron yayınların bütün özelliklerine sahiptir.

İnternette Fikri Hukuk Bakımından Özellik Arz eden Uygulamalar

Eser sahibinin hakları ve haklarının korunması bakımından eserin bilişim ortamına taşınması, uygulanacak olan kuralları değiştirmez. Eser sahibi, eseri üzerinde eserinin umuma arz edilmesi, eserinde değişiklik yapılması, eserinin işlenmesi, çoğaltılması ve yayınlanması konusunda münhasıran hak sahibidir. Eser sahibine Kanun ile tanınan bu haklar, eserin elektronik ortamda kullanılması hâlinde de aynen geçerlidir.

Esasen eser sahibinin bu hakları değişmemekle birlikte internet ortamında özellik gösteren ve hakların korunması bakımından tartışılması gereken birtakım uygulamalar karşımıza çıkmaktadır. Bunların özel olarak ele alınıp değerlendirilmesi gerekir. Bu bölümde bunlar inceleme konusu yapılacaktır.

Link ve Frame Kullanılması

Link, Türkçe'de "çengel" veya bağlantı olarak adlandırılmaktadır. Link verme veya çengel atma, özel bir bilgisayar programı ile gerçekleştirilen ve bir web sayfasından diğerine geçişi mümkün kılan tekniğin ismidir. Aslında link verme, normal bir yazı (Word) metni üzerinde de yapılabilmektedir. Zira günümüz word tabanlı yazılımlarda bugün akıllı sayfa dediğimiz tanıma olayı gerçekleştirilmektedir. Yani word metninde yazılan bir web adresi, otomatik olarak geçişe uygun hâle getirilmektedir. İnternet bağlantısının mevcut olması ve adrese tıklanması hâlinde web sayfalarına geçiş mümkün olmaktadır. Link veya hyperlink, web sayfasından internet kullanıcısını, yabancı web sayfasına aktaran bir program kodudur.

Bir linkte (çengel) iki esas unsur bulunmaktadır. Bunlardan ilki, ağda herhangi bir yerde bulunan bir içeriğe işaret, diğeri ise bu içeriğe ulaşabilme imkânıdır. Link verilme hâlinde işaret edilen web sayfaları veya bilgiler, link veren veya ziyaret edilen sayfanın sunucusunda tutulmamakta, link verilen sayfanın veya atıf yapılan web sayfasının kendi sunucusunda bulunmaktadır.

Linkler, uygulanan tekniklere göre farklı isimler alabilmektedir. Öncelikle linkler, deeplinks, surface links ve inline link olarak adlandırılmaktadır. 'Surface link'in verilmesi hâlinde web sayfası ziyaretçisi, bu linki seçmesi ile birlikte bir başka sayfayı açmaya başlayacaktır. Bu tür linklerde link verilen sayfa bağımsız bir sayfa olarak kullanıcının karşısına gelecektir. Buna karşılık 'Deeplinks'te kullanıcı, doğrudan ziyaret ettiği sayfa üzerinden bir diğer kimsenin sayfasındaki bilgilere giriş sayfasını kullanmaksızın ulaşabilme imkanına kavuşmuştur. Nihayetinde aslında 'deeplinks' bir dahili link olarak kabul edilmektedir.

Konunun fikri hukuk bakımından ele alınacağı bu çalışmada temelde linkler, intern (dâhili) ve ekstern (harici) link olarak ikiye ayrılmaktadır. Harici (ekstern) linklerde internet kullanıcısı, link verilen sayfada bulunan linklerin tıklanması ile diğer sayfaya ulaşmaktadır. Bu, doğrudan diğer web sitesinin ana sayfası olabileceği gibi, o site içinde bulunan bir diğer sayfa da olabilir. Dâhili (intern) linklerde ise internet kullanıcısı, bir başka sayfaya aktarılmamaktadır. Kullanıcı link veren sayfada kalmakta, ancak linkin verildiği sayfa, bu sayfa içinde görülebilmektedir. Dâhili (intern) linkler sayesinde, yüzlerce grafik ve büyük hacimli veriler, link veren kimsenin serverı meşgul edilmeksizin kullanılmaktadır. Bu tür linkler, bir eserin sahibinin link veren kimse olduğu görünümü verilerek kötüye kullanılabilmektedir.

Frame verme hâlinde ise bir web sayfasında birbirinden bağımsız bölümlerde birden çok doküman görülmektedir. Burada frame veren ile frame verilen yabancı web sayfası, internet kullanıcısının ekranında birleşik olarak görülmektedir. Modern internet browserları, kullanıcının ekranının bölünebilmesini sağlamaya elverişlidir. Frame tekniği ile web sayfası yapımcısı, bir başkasına ait web sayfasını kendi sayfası içine monte etme imkânını elde etmektedir. Her frame verilmesinde, internet kullanıcısının ekranında yabancı web sayfaları görüntülenebilmektedir. Frame, intern link vermeden farklıdır. İntern linklerde bir web sayfasının sadece belirli bir metni veya grafiği görüntülenmekte iken frame vermede link verilen tüm sayfa görüntülenmektedir.

Tablo 7.2 Bir Frame Görüntüsü

B'nin Framesi	
B'nin Framei	A'nın Sayfası

Link ve Frame Vermeye Eser Sahibinin Rızası Sorunu

Link verme, ilk anlamda çoğaltma olarak düşünülebilir. Zira bir web sayfasının çağrılması, tipik bir çoğaltma olarak kabul edilmektedir. Fakat sadece bir link atmanın eser sahibinin çoğaltma hakkının ihlali olduğu söylenemez. Çünkü link atma, sadece sayfanın adresinin verilmesi, o sayfaya işaret edilmesi veya o sayfaya internet kullanıcılarının ulaşmasının kolaylaştırılmasıdır. Ayrıca link aktif hale getirildiğinde işlemler link verilen sayfanın üzerinde gerçekleşmektedir. Bu, özellikle ekstern link atma hâllerinde söz konusudur.

Bir web sayfasının işleticisinin yani bir anlamda eser sahibinin bir web sayfasında sunum yapması hâlinde onun en azından kendi web sayfasına başkalarının link vermesini zımni olarak kabul ettiği varsayılmalıdır. Çünkü link, web sayfasında sunulan imkânlardan biridir ve link atılan sayfaya da ulaşılabilme imkânı eser sahibi tarafından sağlanmaktadır. İnternetin temel felsefesini oluşturan bir tür bilgi bankası olması da bu görüşü haklı kılmaktadır. Eser sahibi tarafından başkaca bir hakkın ihlali söz konusu değilse link verme yasaklanamaz.

Doktrinde ekstern link verme, kural olarak atıf hakkı ve kaynak gösterme hakkı ile karşılaştırılmaktadır. Bu nedenle doktrine hâkim olan görüşe göre de link verme yasaklanmamalıdır. Amerikan içtihatlarında da internette bir web sayfası kuran kimsenin kendisine bu şekilde linkler verilmesine baştan rıza gösterdiği sonucuna ulaşılmıştır.

Hemen burada söylenmesi gereken bir husus da link veren kimseler arasındaki özel ilişkilerdir. İki rakip arasında verilen linkler ayrıca değerlendirilmeye tabi tutulmalıdır. Buna İskoç adalarında yaşanan bir çekişmezlik örnek olarak verilebilir: Ekstern linklerin kullanılmasında ilk hukuki problem, İskoç adalarında 1996 yılında yaşanmıştır. 'Shetland Times' günlük haberlerinin bir kısmını web sayfasında da yayınlayan günlük bir gazetedir. 'Shetland News'de web sayfasında haber yayınlanan bir gazetedir. Bu gazete, kendi web sayfasında 'Shetland Times'den bir habere kendi sayfasından link vermiştir. Bu link nitelik itibariyle bir harici linktir. İnternet kullanıcısı, söz konusu linki tıklayarak 'Shetland Times' gazetesinin haberine ulaşabilmektedir. Bunun üzerine 'Shetland Times' yöneticileri, İskoç mahkemelerinde bir dava açmıştır. Dava bir ara karardan sonra 1997 yılında mahkeme dışı bir anlaşma ile sonuçlandırılmıştır. Buna göre verilen linklerin her biri için logo ile birlikte 'A Shetland Times Story' ve ayrıca 'Shetland Times'in ana sayfası için ayrı bir link ilavesi yapılacaktır.

Dâhili (intern) linklerin ve framelerin konulması halinde eser sahibinin bu duruma ekstern linklerde olduğu gibi zımnen izin vermesinden söz edilemez. Çünkü burada eser sahibinin web sayfasından ummakta olduğu haklı menfaatler ihlal edilebilmektedir. İnternet kullanıcısı, eser sahibinin sayfasına ulaşmamakta, geçiş yapmamakta, dâhili link veya frame veren kimsenin sayfasında kalmakta ve eserin link veren kimseye ait olduğunu düşünebilmektedir. Zira frame veren web sayfası ile frame verilen web sayfası arasında bağlantı kurulmakta; frame veren kişinin web sayfasına monte edilerek kullanıcının karşısına çıkmaktadır. Amerika' da TotalNews firması, frame verme yolu ile 1100 adet radyo, televizyon ve gazeteyi sayfalarına monte etmiştir.

Dâhili link (deeplink ya da intern link) verilmesi halinde de eser sahibinin rızasının alınması gerekmektedir. Kanaatimce eser sahibinin adının belirtilmesi hakkı, manevi haklardan olduğu ve bunlardan vazgeçmenin bile mümkün olmadığı düşünüldüğünde, sadece zımni bir rızanın varlığından bahsedilmemeli, eser sahibinin açık bir rızası aranmalıdır. Dâhili link ve frame verilmesi hâlinde bugüne kadar verilen mahkeme içtihatları, eser sahibinin zımni bir rızasından bahsedilemeyeceğini kabul etmiştir.

Link ve Frame Verilmesi ve Eser Sahibinin Hakları

Link ve frame verilmesinde ortaya çıkacak sorunlara genel bir bakıştan önce link türleri arasında başlangıçta bir ayrım yapmak gerekmektedir. Fikri hukuk açısından problem olabilecek link türleri dahili linklerdir. Zira harici linkler, internetin kalbi olarak nitelendirilmekte ve atıf hakkına benzetilmektedir. Burada sadece eser sahibinin sayfasına bir geçiş sağlanmaktadır. Zaten eser sahibinin söz konusu sayfasına internet ağında ulaşmak mümkündür. Dahili link ve framelerde ise eser sahibinin ihlal edilebilen haklarının tek tek ele alınması ve incelenmesi gerekmektedir.

Eser Sahibinin Hakları

Eser sahibinin hakları manevi ve mali haklar olarak ikiye ayrılabilir. Birbirinden farklı olan bu haklar demetinin kendine ait özellikleri ile konu alt başlıklar halinde incelenecektir.

Eser Sahibinin Manevi Hakları

Eser sahibinin eserinden kaynaklanan mali ve manevi hakları mevcuttur. Manevi haklarını aşağıda inceleyeceğiz.

Eser Sahibinin Adının Belirtilmesi

Bern Sözleşmesi 6(bis) 1'e uygun olarak, eser sahibinin bu sıfatının, yani eserin sahibi olduğunun belirtilmesi, Fikir ve Sanat Eserleri Kanununun 15. maddesinde belirtilmiştir. Eser sahibinin adının belirtilmesi hakkı, eser sahibinin adının eserde yer almasını kapsadığı gibi eserin kullanıldığı her yer ve durumda açıkça belirtilmesini de kapsamaktadır. Bu hak, bir taraftan eseri sahibine bağlar, diğer taraftan da eser sahibini eser hırsızlarına karşı (intihal) korur. Bu hak, eserin kullanıldığı her tür ve bütün boyutlarda her halde mevcuttur, kullanmanın nitelik ve çapı önemli değildir.

"Eser sahibinin adının eser yayımlanırken yazılması gerekir. Aksi halde maddi ve manevi tazminat istenebilir." Eser sahibinin isminin yazılmaması hali bir kusur olarak kabul edilmektedir ve manevi tazminatı gerektirmektedir.

Dahili (inline-intern) link verme halinde ise eser sahibinin ihlal edilen birtakım haklarından bahsetmek mümkündür. Zira bu link türünde link verilen sayfa (eser) bağımsız bir sayfa olarak açılmamakta, link veren sayfanın içinde görüntülenmekte; link veren sayfanın adeta bir parçası görünümü verilmektedir. Bu durumda eser sahibinin korunmaya değer menfaatlerinden bahsetmek gerekmektedir. Öncelikle eser sahibinin manevi haklarından adının belirtilmesi hakkının çiğnenmesi söz konusu olabilir (FSEK m. 15).

Deeplink verilmesi halinde genellikle eser sahibi tanınabilmektedir. Burada kullanıcı, içeriğin gerçek eser sahibini tanımlayabilmektedir. Deeplinkte, link verilen sayfa, bazen web sitesinin ilk sayfası olabilmektedir. Bu durumda eser sahibinin tanınabilmesi daha kolaydır. Ancak deeplinkle hedefteki web sayfasının giriş sayfasından başka bir sayfaya bağlanılıyor ise bu durumda eser sahipliğinin karıştırılma ihtimali ortaya çıkmaktadır. Zira internet kullanıcısının linkle bağlandığı sayfadan web sayfasının diğer içeriğine geçmesi beklenemez. Bu durumda deeplink verilen sayfanın sahibinin rızası alınmalıdır.

Frame vermede birbirinden farklı iki teknik kullanılabilmektedir. Bunlardan ilkinde internet kullanıcısı, hangi sayfanın verilerini ekranda gördüğünü bilmemektedir. Diğerinde ise bu sayfanın URL adresi belirtilmektedir. Kullanıcının hangi sayfanın görüntülendiğini bilmediği hallerde eser sahibinin adının belirtilmesi hakkı ihlal edilmektedir.

Eserde Değişiklik Yapılmasını Yasaklama Hakkı

Fikir ve sanat eserleri, eser sahibinin adı, eserin adı ve muhteva ile şekil olarak bir bütün teşkil eder. Bu bütünlüğün korunmasında eser sahibinin manevi bir menfaati bulunmaktadır. Eser sahibinin eserinde zorunlu hallerde değişiklik yapılabilmektedir. Bu zorunluluk halleri, onarım, ihtiyaca uygun hale getirmek, halkın ve çevrenin güvenliği zorunlu hallere örnek olarak verilebilir. Eser sahibinin zorunlu haller dışında eserinde değişikliklere izin verme yetkisi sadece onun tarafından kullanılabilmektedir ve miras yolu ile intikale yahut üçüncü şahıslara devredilmeye elverişli bulunmamaktadır.

Normal olarak hangi tür olursa olsun linklerde ve framelerde eserin değiştirilmesi söz konusu değildir. Ancak bazı hallerde eserin belirli bir parçasının frame ve dahili linklerle bir başka sayfaya bitiştirilmesi halinde eser sahibinin eserinin bütünü veya parçasında belirli bir değişiklik yapıldığının kabul edilmesi gerekmektedir.

Mali Haklar

Eser sahibinin manevi hakları olduğu gibi, mali hakları mevcuttur.

İşleme Hakkı

Fikir ve Sanat Eserleri Kanunu anlamında bir işlemeden bahsedilebilmesi için eseri dönüştüren kimsenin de esere katkısının bulunması gerekmektedir. İşleme eserde iki unsurun bulunması gerekir. Birincisi işleme eser, orijinal eserden bağımsız değildir, ikincisi ise onu işleyen kişilerin de esere bir katkısını taşımaktadır.

Eserin kısaltılması veya genişletilmesi işlenme sayılmaz. Bir roman veya hikâyenin kısaltılması, bir tablodan belirli bir kısmın çıkarılması, senaryonun rejisör tarafından kısaltılması birer işlenme değildir. Eserin büyüklüğünde veya buutlarında değişiklik yapılması işleme değil, çoğaltmadır. Hatta mekanik vasıtaların kullanımı ile de bunun yapılması sonucu değiştirmez. Eserde meydana getirilen dış değişiklikler, ona bir yaratıcı emeğin katkısı değil de sadece bir sunumun, nakilin sonucu ise yine ortada bir işlenme eserin varlığından bahsetmek mümkün olmayacaktır. Mesela bir tablonun değişik ışıklandırılmalar altında sergilenmesi gibi. Esere bir başka buut kazandırılması durumlarında da işlenme eser mevcut değildir. Bir müzik parçasına yeni bir güftenin yazılması da işlenme eser olarak kabul edilemez. Böyle bir durumda eserin metni değişmemekte, ilave ve ikame bir metin daha esere bitiştirilmektedir. Burada işlenme eserden değil, bir eser beraberliğinden bahsedilmektedir. Eser beraberliğinde ortada yeni bir eser mevcut olmadığından her eser bağımsız bir eser olarak değerlendirilir. Bir müzik eserinin operada kullanılması, bir şiirin tiyatro temsilinde okunmasında da ortada işlenme eserden bahsedilemez.

Dahili linklerde eser sahibinin yani link verilen sitenin sadece belirli kısımları ile yeni bir görünümün elde edilebilmesi de mümkündür. Bu durumda ise eser sahibinin işleme hakkının ihlali söz konusudur. İşleme hakkı da münhasıran eser sahibine aittir (FSEK. m. 21). Özellikle dahili link ve framelerde link verilen sayfalar, adeta kullanıcının ziyaret ettiği ve aynı zamanda link ve frameyi veren sayfanın bir parçası olarak gösterilebilmektedir. Burada bir başkasının yaptığı web sayfasının değiştirilmesi, bir başka görünüme kavuşturulması söz konusudur. Ancak işlemenin var olup olmadığı her somut olayda ayrıca araştırılmalıdır.

Frame veya link verilmesi halinde aslında sadece link ve frame verilen sayfa ile teknik bir bağlantının yapıldığı, dolayısıyla eserin aslına bir müdahalede bulunulmadığı doktrinde savunulmaktadır. Ancak eserin kullanıcının ekranına yansıyan halinde şayet esere katkıda bulunulmuş ise ortada bir işlemenin varlığından bahsetmek gerekmektedir. Fakat kullanıcının sadece linki seçmesi ile onun ekranına gelen görüntünün frame veya link veren kimsenin işlemesi olarak nasıl kabul edileceği de şüpheli bulunmaktadır. Ancak kanaatimce bu durum, asıl olarak kullanıcının bir eylemi olmayıp, web sayfasını düzenleyen yani linki veya frame'i veren kimsenin eylemi olarak düşünülmelidir.

Amerika'da dava konusu olan bir olayda da mahkeme, fikri hukuk bakımından korunan fotoğrafların ortaya yeni bir eser konulmamasına rağmen işleme hakkı ile ilgili olduğuna karar vermiştir. Fakat benzeri bir olayda bir başka mahkeme haklı olarak, işleme hakkının ihlali için frame verilen sayfanın yeni biçiminin yaratıcı ve özgün bir formda olması şartını aramıştır.

Çoğaltma Hakkı

FSEK 22. maddesinin I. fıkrasına göre, bir eserin aslının veya kopyalarının herhangi bir şekil veya yöntemle, tamamen veya kısmen, doğrudan veya dolaylı, geçici veya sürekli olarak çoğaltılmasıdır. Ayrıca çoğaltma kavramının kapsamı II. fıkrada genişletilmiştir: "Eserlerin aslından ikinci bir kopyasının çıkarılması ya da eserin işaret, ses ve görüntü nakil ve tekrarına yarayan, bilinen ya da ileride geliştirilecek olan her türlü araca kayıt edilmesi, her türlü müzik ve ses kayıtları ile mimarlık eserlerine ait plan, proje krokilerin uygulanması da çoğaltma sayılır."

Çoğaltma kavramının içeriği her gün genişlemektedir. Özellikle bilgisayar teknolojisinin gelişmesi ile birlikte çoğaltma kavramı da oldukça gelişmiştir. Bir bilgisayar disketine kayıt edilmiş bulunan eserin, bilgisayarda görünmesi anında bile 'geçici' de olsa bir çoğaltma bulunmaktadır. Çünkü bilgisayar ekranına getirilen görüntüler, bilgisayar RAM'lerinde geçici olarak kaydedilen bilgilerdir. Bilgisayarın harddiskine kayıt ve gönderme de çoğaltma sayılmaktadır. Kanunun kullanmış olduğu ifadeler de sınırlayıcı olmadığından teknolojinin gelişmesi ile birlikte çoğaltma kavramı da gün geçtikçe genişleyecektir.

Bir eserin aslından veya kopyasından taklidin çıkarılması ise çoğaltma değildir. Çoğaltma, eserin herhangi bir yolla aynen kopyalanmasıdır.

Çoğaltma, günlük dilde geniş halk kitlelerinin yararlanmasını sağlayacak kadar çok nüshanın çıkarılmasını ifade etmektedir. Ancak fikri hukukta aslının yerine ondan yararlanmayı sağlayan tek bir nüshanın çıkarılması da çoğaltma sayılmaktadır. FSEK. m.22/II'de 'ikinci bir kopyasının çıkarılması' ifadesi ile de bu durum açıkça ortaya konmuştur.

Çoğaltma hakkı münhasıran eser sahibine verilen bir haktır. Fakat kanun koyucu, bazı hallerde çoğaltma hakkına bazı sınırlamalar getirilmiştir. Örneğin FSEK. m. 38'de belirtilen şahsen kullanım amacı ile çoğaltma, bu hakkın bir istisnasını oluşturmaktadır.

İnternet ve bilgisayar ortamında eserlerin sunumunda birden fazla çoğaltma süreci bulunmaktadır. Önbelleğe kayıt, eserin görülebilmesi için zorunlu olan teknik bir çoğaltma işlemidir. Yine bir bilginin internetten kullanıcının bilgisayarına gelene kadar değişik duraklarda kaydedilmesi de bir çoğaltma işlemidir (routing). World Wide Web, birbirine bağlı milyonlarca bilgisayardan oluşmaktadır. Bu bilgisayarlar arasında internet erişiminde bir bilgi, diğer bilgisayara giderken birden fazla yol takip etmektedir. Takip edilen bu yolda bilgisayarlardan oluşan birçok durak bulunmaktadır. Bu duraklardaki bilgisayarlar 'router' ismini almaktadır ve kendisine gelen bilgileri gideceği hedef bilgisayara aktarmaktadır.

Bu aşamalardan her birinde ayrıca bilgiler kayıt edilmekte ve gönderilmektedir. İstenilen bilgiler, internet ağında küçük parçalara ayrılmaktadır. Bu bilgiler hedef bilgisayarda birleştirilmektedir. Bu kayıtlar bir başka bilgisayara 'transfer için yapılan kayıtlar'dır. Bu nedenle bu süreçteki kayıtlar da çoğaltma kavramı içinde değerlendirilmelidir. Kanaatimce, bu aşamadaki çoğaltma da fikri hukuk anlamında çoğaltma kavramı içinde değerlendirilmelidir. Ancak bu çoğaltma hali, klasik çoğaltma hallerinden ayrı ve bağımsız olarak müeyyidelendirilemez. Zira bu süreçteki çoğaltmalar, nihai çoğaltmanın zorunlu parçalarıdır. Bir başka çoğaltma süreci de ana bellekte gerçekleşmektedir. Önbellekte yapılan kayıt işlemine göre kalıcı bir kayıt işlemi olarak adlandırılabilir ve fikri hukuk bakımından tartışmasız bir şekilde çoğaltma olarak kabul edilir. Dijital hale getirilmiş olan bir eserin internetten veya bilgisayarın harddiskinden bir CD veya diskete kaydedilmesi de fikri hukuk bakımından bir çoğaltma sayılmaktadır. CD veya diskete kayıt, sürekli bir kayıttır. FSEK m. 22/III, bir bilgisayar programının görüntülenmesini de geçici çoğaltmayı gerektirdiği ölçüde çoğaltma olarak kabul etmiştir. Fakat doktrin sadece ekranda görüntülemeyi, çoğaltma olarak kabul etmemektedir.

Link ve frame verilmesinde eser sahibinin çoğaltma hakkının ihlal edilip edilmediği de burada ayrıca araştırılmaya değer bir konu olarak karşımıza çıkmaktadır. Bir linkin aktif hale getirilmesi halinde, çoğaltma bizzat link veren kimsenin eylemi olarak gerçekleşmemektedir. Çoğaltma üçüncü kişinin, yani web sayfası ziyaretçisinin bilgisayarında meydana gelmektedir. Bu nedenle link ve frame veren kimse, doğrudan eser sahibinin çoğaltma hakkını ihlal etmemektedir.

Frame verme de doğrudan bir çoğaltma değildir. Zira burada ilgili bir program yardımı ile iki web sayfası arasında bir bağlantı kurulmaktadır. Bu durumun aynısı link türleri için de söz konusu olmaktadır. Böyle bir durumda link ve frame veren kimse eser sahibinin çoğaltma hakkını ihlal etmemiş kabul edilmelidir.

Fakat doktrinde savunulan bir görüşe göre dahili linklerde ve framelerde web sayfası ziyaretçisi olan üçüncü kişi, şayet link veya frame ile ulaştığı sayfanın kime ait olduğunu anlayamıyorsa bu durumda eser sahibinin çoğaltma hakkı ihlal edilmektedir.

Dahili linklerin kullanımı ile ilgili olarak 1996 yılının yazında Amerika'da meydana gelen bir çekişmezlik incelemeye değerdir. Burada "Dilbert" adı verilen popüler komik figür, intern link yoluyla özel bir web sayfasında kullanılmıştır. Bu figürü günlük olarak 'United Media' firması, kendi web sayfasında yenilemekte ve sunmaktadır. Fakat aynı figürleri intern linklerle bu özel şahıs kendi sayfasına eklemektedir. Mahkeme, bu durumda, eser sahiplerinin haklarının ihlal edildiğine karar vermiştir.

Almanya'da uyuşmazlık konusu bir olayda çevrimiçi ortamda sunulan bir sözlüğe link verilmekte, bu sözlük kişinin web sayfasında görüntülenmektedir (framing). Bu durum mahkeme tarafından söz konusu bilgi bankasının kısmen çoğaltılması olarak kabul edilmiştir ki bu durum eser sahibinin münhasır haklarının bir ihlalidir. Burada bilgi bankasını sunan kimsenin link verilmesine zımni rızasından da bahsedilemeyecektir. Zira bu rıza sadece link verilmesine gösterilen bir rıza olup bir yabancı web sayfasında görüntülenmesine verilen rıza değildir.

Konunun Türk hukuku bakımından değerlendirmesine gelince; normal linklerde, yani harici linklerde ve hangi sayfanın görüntülendiğinin bilindiği dahili link ve framelerde çoğaltma hakkının ihlal edilmediği sonucuna varılmalıdır. Ancak kullanıcı tarafından hangi sayfanın link ve frame sonucu kullanıldığı bilinemiyorsa bu takdirde çoğaltma hakkının ihlal edildiği sonucuna ulaşılmalıdır. FSEK m. 22 metni son derece geniş ve ayrıntılı düzenlenmiştir. Buna göre her ne kadar çoğaltma, link veya frame veren kimsenin kendi serverında meydana gelmese de burada uygulanan teknik, dolaylı bir çoğaltma olarak kabul edilmelidir. Dolayısıyla bu şekilde bir link veya frame verecek kimsenin mutlaka eser sahibinin iznini alması gerekmektedir. Hakkaniyet ilkesi de burada bir çoğaltmanın varlığının kabulünü ve eser sahibinin izninin alınmasını gerektirmektedir. Herhangi bir çoğaltma işlemini kendi sayfasında yasal olarak yapamayan kimse bunu link ve frameler yolu ile de gerçekleştirememelidir.

Umuma İletim Hakkı

FSEK m. 25'in yeni düzenlemesi ile umuma iletim, bir eserin veya çoğaltılmış nüshalarının radyo, televizyon veya herhangi diğer bir teknik usulle umumun yararlanmasına sunulmasıdır. Umuma arz kavramında önem taşıyan kavram 'umum' kavramına yüklenecek anlamdır. Fikir ve Sanat Eserleri Kanunumuzda umum kavramı tanımlanmamıştır. Buna karşın Alman Telif Hakları Yasasının (UrhG) § 15/III de tanımlanmıştır. Bu tanımlamaya göre belirli bir çevre ile sınırlı olmayan, birbirine karşılıklı ilişkiler içinde bağlı bulunmayan veya bir organizasyonla birbirine bağlanmayan birden fazla kimse, umum kavramını oluşturmaktadır.

Umuma iletim hakkının ihlal edilip edilmediği sorununda da dikkate alınması gereken husus, umuma iletimin nasıl gerçekleştiğidir. Zira burada fikri hakka konu teşkil eden eser, yine sahibinin sunucusunda (serverında) bulunmakta, erişim oradan sağlanmaktadır.

Herhangi bir teknik usulle umumun yararlanmasına sunulma tanımı, dahili link veya frame veren kimsenin dolaylı da olsa yapmış olduğu sunumları da kapsayıp kapsamadığı sorunu gündeme gelmektedir. Fakat kanaatimce dahili link ve frame verilmesi halinde umuma iletim hakkının link veya frame veren tarafından ihlal edilmediği sonucuna ulaşılmalıdır. Zira burada yine umuma iletim, eser sahibinin sayfasından gerçekleştirilmektedir. Umuma iletimi düzenleyen FSEK m. 25'de eser sahibinin çoğaltma hakkını düzenleyen FSEK m. 22 genişliğinde değildir ve 'dolaylı da olsa umuma arz', madde kapsamına alınmamıştır.

Link ve Frame Veren Kimselerin Sorumluluğu

Dahili link ve frame veren kimsenin sorumluluğunu tespit etmek için öncelikle bu kimselerin sorumluluk esaslarının ve link vermenin hukuki niteliğinin belirlenmesi gerekmektedir. Dahili link veren kimsenin sorumluluğunun kendi sayfasını hazırlayan kimse sorumluluğuna mı yoksa bir başkasının sayfasına aracılık yapan kimsenin sorumluluğuna mı tabi olacağı sorusunun da cevaplandırılması gerekmektedir.

Bir görüşe göre web sayfasına link yerleştirilmesi hali, bir hazır bulundurmadır. Link tesis edilmesi, kısmen internet girişine aracılık olarak kabul edilebilir. Fakat bu görüş kabul edilmemektedir. Zira ekstern link atma halinde sadece link verilen siteye işaret edilmektedir. Bir başka görüşe göre ise, link tesis edilmesi, yabancı bir kimsenin içeriğinin bulundurulması olarak düşünülmelidir (host-provider). Ancak bu görüş de isabetli değildir. Çünkü burada link veya frame veren kimse link ve frame verilen sayfanın içeriğini kendi serverinde tutmamaktadır. İçerik yine link veya frame verilen sayfanın hazırlayıcısının serverinde tutulmaktadır.

Amerika'da film endüstrisi temsilcisi olan MPAA, Hacker-dergisi çıkaran Eric Corley'e karşı bir dava açmıştır. Davanın sebebi ise, Corley'in kendi web sayfasında DVD üzerine kaydedilmiş olan sinema eserlerinin çoğaltma ve seyretmeye karşı esere ilave edilmiş bulunan şifreleri etkisiz kılan kodların yayınlaması veya bu şifreleri yayınlayan sitelere link vermesidir. Bu davada mahkeme, Corley'in hem şifrelerin kendi web sayfasında açılmasını hem de şifrelerin kırıldığı başka sitelere link verilmesini yasaklamıştır. Hâkim, söz konusu eylemleri Digital Milineum Copyright Act'a da aykırı bulunmuştur. DMCA bölüm 1201 (a) (2) hükmü, fikrî hakların korunmasını hedefleyen bir teknik sistemin 'ilk planda' aşılmasını hedefleyen teknolojileri yasaklamaktadır. Burada getirilen ölçülere göre link verilen sayfanın içeriğinin suç teşkil etmesi ve link veren kimsenin bu sayfanın içeriğini bilmesi gerekmektedir.

Türk hukukunda link ve frame veren kimsenin sorumluluğu genel hükümlere göre belirlenmelidir. Link verilen sayfada eser sahibinin hakları ihlal ediliyorsa bu durumda link veren kişi, yardım ve teşvik etmekten dolayı sorumlu olacaktır.

Burada müteselsil sorumluluk hali de düşünülebilir. Müteselsil sorumluluk, taraf iradelerinden ya da kanunun öngördüğü durumlarda kanundan doğar. Kanunen öngörülen müteselsil sorumluluk hallerinden birisi haksız fiiller alanındadır. Türk/İsviçre kanun koyucusu birden fazla kimselerin aynı zarardan sorumlu olmalarının iki türünü düzenlemiştir. Birden çok kişi birlikte bir zarara sebebiyet verdikleri veya aynı zarardan çeşitli sebeplerden dolayı sorumlu oldukları takdirde müteselsilen sorumlu olacakları hükme bağlanmıştır (BK. m. 61).

Harici (ekstern) link veren kimsenin yaptığı eylem, aracılık olarak nitelenmelidir. Zira onun diğer sayfanın içeriğine herhangi bir etkisi bulunmamaktadır. Ayrıca link verdiği sayfanın içeriğinin kendi serverı üzerinden sunulması da söz konusu değildir. Bu nedenle link veren web sayfası işleticilerine aracılık yapan kimselere dair bir sorumluluk türünün uygulanması gerekmektedir.

Yasal olmayan bir şekilde eser sahibinin sitesine intern link veren kimsenin durumu ise aracılık yapmaktan daha farklı bir niteliğe kavuşmaktadır. Bir başkasının hazırlamış olduğu içeriği kendi web sayfasından sunmakla içeriği bilmediği savını ortadan kaldırdığı gibi, link veren yasal olmayan içeriğe sahiplenerek bunu kendi içeriği gibi sahiplenmektedir.

İnternet (Web) Sayfalarının Korunması

İnternet web sayfasının fikri hukuk bakımından nasıl korunacağı konusunda bir fikir beyan etmeden önce web sayfasının özelliklerinin ele alınması gerekmektedir. Web sayfası, multimedya ürün niteliği arz eden ve bir eser türü olarak nitelenemeyen çoklu eser türleri arasında yer almaktadır. Bir web sayfasında internet öncesinde kitap, resim, grafik, fotoğraflar gibi dijitalleştirilmiş *analog* eser türleri bulunabileceği gibi, internete özgü tasarımlar da bulunmaktadır. Bu münferit eser türlerinin eser sayılacağı tabiidir. Ancak web sayfası denildiğinde eser türleri ayrı ayrı değil de hepsinin bütünleşmiş olduğu toplu ve ayrı bir birleşik bütün anlaşılmaktadır.

Analog
Sayısal olmayan.

Birden fazla eser türünün birbiri içinde bütünleştirilerek bulunduğu bazı eser bileşimlerinin FSEK'te ayrı bir eser kategorisi olarak korunmasına rastlamak mümkündür. Gerçekten sinema eseri, birden fazla eser türünün birleşimidir ve kanun koyucu tarafından ayrı bir eser türü olarak düzenlenmiştir (FSEK.m.5). Eser türünün belirlenmesi elbette kanun koyucunun bir tercihidir ve bir hukuk politikasıdır. Bu nedenle henüz kanun koyucu, web sayfalarını bağımsız bir eser türü olarak kabul etmediği sonucuna ulaşılmalıdır. Eğer bir gün kanun koyucu web sayfalarını aynen sinema eserlerinde olduğu gibi ayrı ve bağımsız bir eser türü olarak kabul ederse bu durumda web sayfasının bütünü itibarıyla ayrı ve bağımsız bir eser olduğu kabul edilecektir. Bugün itibariyle web sayfaları, ayrı bir eser türü olarak kabul edilmemektedir.

Bilindiği gibi Fikir ve Sanat Eserleri Kanununa göre bir fikri ürünün eser sayılabilmesi için öncelikle Kanun'da sayılan 4 adet eser türü içinde yer almalıdır ve sübjektif şartın yerine gelmesi gerekir. Eserin sahibinin hususiyetini taşıması, sübjektif şartı oluşturur iken; söz konusu fikri ürünün kanunda sayılan eser türlerinden biri olması yanında algılanabilir bir niteliğe sahip olması da objektif şartı oluşturmaktadır. Hal böyle olunca web sayfası, bir multimedya ürün olarak, yani çoklu ortam ürünü olarak karşımıza çıkmaktadır. Ancak bununla birlikte Kanunda sayılan eser tiplerinden herhangi birine girmemektedir. Bu durum, web sayfasının fikri hukuka göre hiç korunmayacağı anlamına da gelmez.

İnternet web sayfaları, içinde bulundurdukları münferit unsurlarına ayrılarak pekâlâ korunabilecektir. Web sayfası, resimlerden, seslerden ve birbirine geçişi sağlayan teknik süreçten ve bazı hallerde bilgisayar yazılımlarından oluşan bir bütün olarak karşımıza çıkar. İşte bu unsurlar, fikri hukuk bakımından zaten web sayfasından bağımsız olarak korunacaktır. Yani web sayfasında kullanılan metinlerin şartları varsa ilmi ya da edebi eser olarak; bir müzik eseri kullanılıyor ise müzik eseri olarak yine resim kullanılıyorsa güzel sanat eseri ya da bir film kullanılıyor ise sinema eseri olarak; arkasında bir veri bankası varsa veri tabanı olarak korunması mümkündür.

Web sayfasında ilmi ve edebi eserler, güzel sanat eserleri, musiki eserler ve sinema eserleri kullanıl-

mışsa bunların FSEK kapsamında korunmasında herhangi bir problem bulunmamaktadır.

İnternet web sayfalarında ayrıca HTML kodları dediğimiz kodlar bulunmaktadır. Bunlar aslında FSEK bakımından yazılım olarak kabul edilebilir. Özellikle son zamanlarda interaktif yazılımların gelişmesi ile birlikte web sayfaları, artık klasik HTML kodlarından daha karmaşık yazılımlara doğru gidiş seyri izlemektedir. İnternet web sayfaları, 'ASP' tekniği kullanılarak da hazırlanabilir. Bu teknikte, web sayfası her seferinde yeniden kullanıcının talebine göre üretilebilmektedir. Yani web sayfasının arkasında artık bir yazılım çalışmaktadır. Bu durumda web sayfası, yazılımı koruma altına alan FSEK hükümlerine göre korunabilir. Yine web sayfaları, Javascript denilen programlarla da yapılabilir. Bu durumda da ortada FSEK bakımından yazılım koruması söz konusu olacaktır.

dikkat

HTML kodları, Hypertext Markup Language, ks. HTML) web sayfalarını oluşturmak için kullanılan standart metin işaretleme dilidir.

Active Server Pages'in kısaltılmışı olan ASP dilimizde 'Aktif Sunucu Sayfaları' anlamına gelmektedir. ASP ile kodlanan sitelere dinamik web siteleri de denmektedir. Java programlama dilinin web sayfaları için özelleştirilmiş biçimidir. Script dilleri ile hazırlanan kodlar programlardan farklı olarak satır satır işletilirler. Bu programlar ise bir bütün olarak ele alınır ve değerlendirilirler. Ancak, klasik anlamda, web sayfası hazırlamak için kullanılan HTML dilinden farklı olarak statik bir sayfa ortaya çıkmaz, kodlara bağlı olarak farklı sayfalar ortaya çıkar.

Web sayfalarının arkasında bazı zamanlar işleyen bir veri bankası da bulunabilir. FSEK'nin 6/11. maddesinde veri tabanı tanımlanmıştır: "belli bir maksada göre ve hususi bir plan dahilinde verilerin ve materyallerin seçilip derlenmesi sonucu ortaya çıkan ve bir araç ile okunabilir veya diğer biçimdeki" veri tabanları (Ancak, burada sağlanan koruma, veri tabanı içinde bulunan veri ve materyalin korunması için genişletilemez)". Burada veri tabanından bahsedebilmek için iki tane unsur sıralanmıştır. Bunlardan ilki belirli bir maksada yönelik materyallerin derlenmesi, ikincisi ise bu materyallerin bir araç ile okunabilmesidir.

Widget Programlarının Kullanımı

İnternet kullanıcılarının, sürekli olarak internette ziyaret ettikleri sayfalar vardır. Bu sayfalar, değişik sayfalar oldukları için bunların tek tek aranması ve ziyaret edilmesi oldukça uzun bir vakit almaktadır. İnternet kullanıcılarını ziyaret ettiği bu sayfaları tek tek arayıp bulmaktan kurtaran yeni programlar geliştirilmiştir. Bu programlar, widget programları olarak adlandırılmaktadır. Bu programlar, internete giren kişinin istediği sayfaları onun sayfasına getiren küçük programcıklardır.

Bu tür programların kullanılması halinde ortaya birçok hukuki sorunun çıkacağı en azından internet sayfasının sahipleri tarafından çıkmasının arzulanacağı aşikardır. Zira bu durumda programa kayıtlı internet sayfaları artık ziyaret edilmeyecek, yani bir diğer deyişle reytingi düşecektir. Haksız rekabet açısından bunların ayrıca ele alınması gerekir.

Bu programlar, internet sayfalarını, kullanıcının sadece kendi özel sayfasında görüntülemesine hizmet etmekte ve sadece kullanıcı tarafından görüntülenmektedir. FSEK bakımından değerlendirildiğinde kullanıcının bu sayfayı şahsi kullanım çerçevesinde bu şekilde arzusuna göre kullanabilmesinin önünde bir engelin bulunmadığı sonucuna ulaşılmalıdır (m.38).

Şekil 7.1

Değişim Programları

Değişim programlarını anlayabilmek için değişim programlarına giden bir takım özel teknolojilerin öncelikle izah edilmesi gerekir. Önceki açıklamalarımızda eserin dijitalleşmesinden bahsetmiştik. Burada ise eserin internet ortamında daha rahat nakledilebilmesi için geliştirilen, sıkıştırma, değişim ve paylaşım gibi diğer teknolojilerin incelenmesi gerekmektedir.

Sıkıştırma Teknikleri-Mp3, DivX vb.

Dijitalleşme sonrasında, özellikle büyük hacimli müzik ve sinema eserlerinin internet ortamında nakledilmesi yine de çok zordu ve nakli ve download edilmesi saatler, hatta günler sürebiliyordu. Fakat geliştirilen sıkıştırma teknolojileriyle büyük hacimli müzik ve sinema eserleri de internette kolaylıkla nakledilebilmeye başlandı. Alman Frauenhofen Enstitüsünde geliştirilen ve Mp3 adı verilen bir teknoloji ile eserler 10-12 kat küçültülmeye başlandı. Böylece bir CD'ye daha önceleri 10-12 müzik parçası kaydedilebilirken, bu teknoloji ile 100-150 müzik parçası kaydedilmeye başlandı. Benzeri teknoloji film eserleri alanında DivX veya DVD teknolojileri ile gerçekleştirildi. Bir müzik eseri artık kalite kaybı olmadan internette yayılabilmekte ve birkaç dakika içinde kopyalanabilmektedir.

Müzik Değişim Programları-Filesharing-P2P

İnternet ortamında eser ve bağlantılı hak sahiplerinin haklarının ihlalinde en fazla kullanılan ve çözümsüzlük arz eden problem 'peer to peer' veya 'filesharing' olarak adlandırılan müzik değişim programlarıdır. Bu programlar, internet ortamında ücretsiz olarak sunulmaktadır. Bu yazılımların esası, arama motoru, elektronik posta ve Windows'un dosya paylaşım fonksiyonlarının birleştirilmesine dayanmaktadır. Bu programlarda sadece müzik ya da yazılım değişilmemekte, her türlü verinin değişimi yapılmaktadır. Merkezi ve merkezi olmayanlar olarak ikiye ayrılmaktadır. Napster, kapatılmadan önce 70 milyon kullanıcıya sahip olmuştu. 2004 yılında dünya internet kullanıcılarının %33'ünün bu tür değişim platformlarının kullanıcısı olacağı tahmin edilmektedir. Böylece dünya adeta her gün genişleyen bir dijital müzik kütüphanesine dönüşmektedir.

dikkat

Müzik alanında ihlalin boyutlarına örnekler vermek gerekirse:

• Arama motorlarında en fazla aranan kavram "Mp3" kavramıdır.

• Bugün net rakamlar bilinmemekle birlikte 1988 yılında 30 ayrı ülkede 2 binin üzerinde sitede 200 bin müzik parçası sunulmuştur. IFPI'nin son rakamlarına göre illegal müzik sunumu yapan 700 bin web sayfası bulunmaktadır.

• IFPI'ye göre bir güne 1 milyon 100 bin müzik verisi serverlerdan alınmaktadır. Sadece 2001 Ağustos ayında 3 milyar müzik verisi transfer edilmiştir.

• 2003'de sadece müzik değişim platformlarından biri olan Kazaa'da 2,6 milyar müzik verisi değiş-tokuş edilmiştir.

• Bir tahmine göre dünya müzik piyasasının internette yasal olmayan müzik sunumları dolayısıyla kayıpları 32,6 milyar dolara ulaşmaktadır.

Fikri Hak İhlalleri

Değişim programları fikri hukuk bakımından çözümü oldukça güç sorunları beraberinde getirmiştir. Bu zorluklar şu şekilde sıralanabilir. Öncelikle sayısı milyonlara varan web sayfalarında bu tür ihlallerin tespiti nasıl yapılacaktır? Örneğin AB ile ilgili bir web sayfasında bile müzik sunumları yapılabilmektedir. İkincisi sınır ötesi sunumlarda kime karşı ve nasıl dava açılacaktır? Bunlar çözümlenmesi güç problemlerdir.

Hukuki Nitelemeler

Bir web sayfasına müzik yükleme (upload), müzik değişim programı için hazır bulundurma bir çoğaltmadır ve bu eser sahibinin münhasır haklarındandır (FSEK m.22). FSEK. m.38 anlamında şahsi kullanım amacıyla bir çoğaltma kabul edilemez. Zira şahsi kullanım amacıyla çoğaltma ilişkinin bulunduğu tabii ve dar bir alanı kapsar. Sınırları belli olmayan ve adeta bütün bir dünyaya kopyalama imkânı veren bir çoğaltma FSEK m.38 anlamında bir çoğaltma sayılamaz.

Bu tür eylemler, FSEK m.25 anlamında bir 'umuma iletim' olarak kabul edilmelidir. Umum, belirli bir çevre ile sınırlı olmayan, birbirine karşılıklı ilişkiler içinde bağlı bulunmayan veya bir organizasyonla birbirine bağlanmayan birden fazla kimse olarak tanımlanmaktadır. Müzik değişim platformlarında oluşan kullanıcı çevresi ise bu anlamda 'umum' kavramını oluşturur ve eser sahibini 'umuma iletim' hakkını ihlal eder.

Bu konuda önemli davalara da işaret etmek gerekir. Bunlardan biri, merkezi bir sisteme dayanan değişim programı Napster ile ilgilidir, diğeri ise merkezi olmayan değişim programı Kazaa'ya ilişkindir.

Napster, merkezi serveri olan ve kullanıcılarına müzik değişim imkânı sağlayan bir yazılımdır. Müzik değişim platformları arasında en fazla meşhur olmuş ve 70 milyona varan kullanıcı sayısına ulaşmıştır.

Napster'in ilk derece ve temyiz merci aşamalarında mahkeme, Napster'in fikri hakların ihlalinde iki aşamalı bir sorumluluğunun bulunduğuna karar vermiştir. Bu sorumlulukların ilk aşamasını fikri hakların müşterek ihlali, ikinci aşamasını ise dolaylı ihlal oluşturmaktadır. Napster, kurmuş olduğu müzik değişim sistemi ile telif hakkı bakımından korunan eserlerin izinsiz olarak kullanılabileceğini, yayılabileceğini biliyordu ve kurduğu sistemle de buna yardımcı olmuştur. İkinci aşamada ise Napster, sistemi üzerinden yapılan değişimlerde fikri hukuk bakımından korunan eserlerin değişimine engel olmayarak, kontrol yapmayarak gözetim görevini yerine getirmemiştir. Dava aşamalarının devamında mahkeme filtre sistemini öngörmüş, ancak bu meslek birlikleri ve hak sahiplerini tatmin etmemiş, nihayet Napster sistemini paralı hale getirerek ve meslek birliklerine değişimler karşılığını ödeyerek mahkeme aşamaları sonuçlandırılmıştır.

Merkezi olmayan müzik değişim platformlarından en ünlüsü olan Kazaa'ya karşı Hollanda'da dava açılmıştır. Hollandalı Hâkim, müzik değişim platformu olan Kazaa'nın iki hafta içinde kapalı kalmasını ve bu süre içinde fikri hukuk bakımından korunan eserlerin değişiminin teknik olarak engellenmesine karar vermiştir. Aksi takdirde P2P servisi, hizmetlerini bitirmek zorunda kalacaktır. İki haftalık süre sonrasında fikri hukuk bakımından korunan eserlerin değişimi halinde Kazaa, günlük 40 bin-80 bin dolar ceza ödemek zorunda kalacaktır.

Kazaa, bu karara karşı temyize gitmiş ve temyiz merciinde verilen kararda hem ihtiyati tedbir kararı kaldırılmış hem de Kazaa'nın kullanıcılarının fikri hak ihlallerinden sistem işleticisinin sorumlu olmayacağına hükmedilmiştir.

Paylaşım Programları

Paylaşım programları, günümüzün en popüler programlarındandır. Kişisel paylaşım programları ve genel paylaşım programları olarak kendi içinde tasnif edilebilir. Paylaşım programlarında kişiler, kendilerine ait bilgileri, yazıları ve fotoğrafları paylaşabildiği gibi fikri hukuk bakımından korunan eserler de paylaşılabilmektedir. Yine değişik internet platformlarında da sadece müzik, video, film ya da fotoğraf paylaşılabilmektedir.

Bu platformlarda eserlerin paylaşımı hali, FSEK bakımından umuma iletim sayılmalıdır (FSEK.m.25). Bu nedenle umuma iletim için mutlaka eser sahibinden izin alınmalıdır. Burada platform kullanıcılarının fikri hak ihlallerinden sorumluluğu konusu ele alınmalıdır.

Bir platforma (Youtube, Instagram) bir başkasının eserini izinsiz bir şekilde koyan kişinin fikri hukuk bakımından eser sahibinin umuma iletim ve çoğaltma haklarını ihlal ettiğinde şüphe yoktur. Bu kimseye karşı eser sahibinin FSEK'te belirtilen davaları açabileceğinde bir tereddüt de yaşanmamaktadır.

Platformu işletenin sorumluluğu ise ayrıca ele alınmalıdır. Platform işleticisinin sayfada paylaşılan milyonlarca veriyi kontrol etmesi ve denetlemesi düşünülemez. Bu nedenle bu tür veriler bakımından platform işleticisinin sorumlu olduğu söylenemez. Platform sorumlusu, burada paylaşılan eserler bakımından kendisine bir uyarı geldiğinde bunların paylaşılmasına engel olmak zorundadır. Aksi takdirde platform işleticileri sorumlu olacaktır.

Platform işleticileri için esasen Türk Hukukunda Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'a kadar bir düzenleme bulunmamakta idi. Ancak Kanun ile, aracı hizmet sağlayıcı tanımı getirilmiş ve aracı hizmet sağlayıcılara ilişkin düzenlemeler yapılmıştır. Kanun'un 9. maddesine göre "aracı hizmet sağlayıcılar, hizmet sundukları elektronik ortamı kullanan gerçek ve tüzel kişiler tarafından sağlanan içerikleri kontrol etmek, bu içerik ve içeriğe konu mal veya hizmetle ilgili hukuka aykırı bir faaliyetin ya da durumun söz konusu olup olmadığını araştırmakla yükümlü değildir". Böylece aracı hizmet sağlayıcı için eserlerin paylaşımı ile ilgili olarak kullanıcıların yaptığı ihlallerden sorumluluk engellenmiştir. Hemen belirtelim ki, bu tür paylaşım siteleri, fikri hak ihlalleri hakkında kendilerine bir ihbar geldiğinde bunları içerikten çıkarmaktadır.

Kanunda Eser Sahipleri İçin Getirilen Özel Koruma Usulü

Kanun, eser sahiplerinin internet ortamında daha etkin korunabilmesi için özel bir usul öngörmüştür. FSEK.m. ek-4'de getirilen sistem, dünyada uygulanan uyar-kaldır sisteminin -eleştirilecek birçok yanı olmakla birlikte- Türk hukukundaki görünümüdür.

Eser sahiplerinin ya da bağlantılı hak sahiplerinin haklarının dijital ortamda ihlal edilmesi halinde, hak sahiplerinin başvuruları halinde söz konusu eserler içerikten çıkarılır. Bunun için hak sahiplerinin içerik sağlayıcıya başvurması gerekir. Başvurudan itibaren üç gün içinde içerikten çıkarma gerçekleştirilmelidir. İhlal devam ederse Cumhuriyet başsavcısına başvuru yapılır. Cumhuriyet başsavcısı, üç gün içinde servis sağlayıcıdan ihlale devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulmasını ister. İhlalin durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır. Böylece internet ortamında gerçekleşen ihlal çok basit bir yöntemle ortadan kaldırılmış olacaktır. Belirtelim ki bu usulün kullanılması, hak sahiplerinin tazminat haklarına ve ihlali yapanlara karşı suç duyurusunda bulunma imkanını ortadan kaldırmayacaktır.

Fikri Hak İhlallerinde Uygulanacak Hukuk

Bilişim sisteminde meydana gelen eser ve bağlantılı hak sahiplerinin haklarının ihlalinde çoğunlukla yabancılık unsuru bulunabilir. Bu durumda hakimin önüne gelen uyuşmazlıkta hangi hukuku uygulayacağı sorunu karşımıza çıkmaktadır. Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun'un (MÖHUK) 23. maddesinde fikrî mülkiyete ilişkin hakların korunmasında, hangi ülkenin hukukuna göre koruma talep ediliyorsa o hukuka tabi olacağı, ancak tarafların ihlalden sonra mahkemenin hukukunun uygulanmasını da kararlaştırabilecekleri düzenlenmiştir.

Belirtmek gerekir ki koruma talep edilen ülke hukuku (lex loci protectionis) bağlama kuralının temelinde ülkesellik prensibi vardır. Bu ilke hem milletlerarası sözleşmelerde hem de milli hukuklarda kabul edilmiştir. Bu durumda fikri hakkın kullanıldığı veya ihlal edildiği iddia edilen eylemin ortaya çıktığı ülkenin hukukuna göre 'korumanın talep edildiği yer' olarak tespiti gerekecektir.

Esasen bu ilkenin MÖHUK'ta kabulü, fikri hak sahiplerini koruyucu bir işlevdedir. Eser ya da bağlantılı haklar üzerinde Türk hukukuna göre hak sahibi olan kimse, bu hakkına diğer bir ülkede koruma talep etmesi halinde, bu ülke hukukuna göre himaye edilip edilmeyeceği konusu önem kazanır. Bu takdirde, MÖHUK m. 23 gereği uygulanacak hukuk değişir. Dolayısıyla başka bir ülkede koruma talep edildiğine göre, uygulanacak hukuk da değişecektir. Türkiye'de eser ya da bağlantılı hak sahibi olan kimse, korumanın talep edildiği ülkede ve bu ülkenin hukukuna göre, aynı haklara sahip değilse, korunmaya değer bir hakkın varlığından söz etmek mümkün olmayabilir. Bütün bunların yanında Türk mahkemelerinden verilmiş bir kararın, koruma talep edilen ülkede icrası ise ayrı bir konudur ve bu konu o ülkedeki tanıma ve tenfiz rejimine tabidir.

Öğrenme Çıktısı

1 Eser sahibinin haklarını detaylı bir şekilde açıklayabilme

Araştır 1	İlişkilendir	Anlat/Paylaş
Eser sahibinin manevi ve mali hakları nelerdir, kısaca sayınız.	Mali ve manevi terimleri nasıl bir farklılığa işaret etmektedir? Eser sahibine manevi haklar neden veriyor olabilir?	Eser sahibinin haklarının önemini, sahibi ve genel olarak toplum bağlamında çevrenizdekilerle paylaşınız. Bu hakların olmaması durumunda nasıl bir hukuki durum söz konusu olabilirdi, düşününüz.

İNTERNET ORTAMINDA SINAİ HAKLARIN KORUNMASI

Bilişim sistemlerinde sınai hak olarak nitelendirilen hakların korunması da özel bir öneme sahiptir. Ticaret unvanının, markanın ve alan adının kullanımı ve korunması gerekir. Bu korumanın nasıl olacağı ve hangi hükümlere göre gerçekleşeceği, ihlalin tespiti ve ihlale karşı müracaat edilecek hukuki yollar önem kazanmaktadır. Bu bölümde alan adının kullanımından başlayarak, ticaret unvanı ve markanın kullanımı ve korunması konularını önem sırasına göre inceleyeceğiz.

Alan Adı ve Markasal Kullanım

İnternete özgü en tipik kullanımlardan biri, markanın alan adı (domain name) olarak kullanılmasıdır. Bu sorunun ele alınıp net bir şekilde değerlendirilebilmesi için alan adının teknik yönünün de bilinmesi ve ortaya konulması gerekmektedir. Aşağıda sorunun hem teknik yönleri hem hukuki yönleri ve ayrıca meydana gelebilecek ihtilaflar ve çözüm yolları bakımından konular tasnif edilerek ele alınmıştır.

Alan Adının Niteliği ve Sorunun Ortaya Konulması

İnternet sistemi, birbirinden bağımsız binlerce ağdan oluşmaktadır. Bu bilgisayarların birbiri ile iletişim kurabilmesi için bunların tanınabilmesi gerekmektedir. Bilgisayarların birbirlerini tanıyabilmeleri için geliştirilmiş adresler bulunmakta ve bunlara IP (İnternet Protocol) adresi denilmektedir. Bu sistemde kullanılan her bir web sayfasının birbirinden farklı isimleri bulunmaktadır. Bu isimler alan isimleri (Domain Name) olarak adlandırılmaktadır. İnternete bağlanan kullanıcı, adres kısmına bu isimleri yazdığında bilgisayar, kullanıcıyı istediği sayfalara ulaştırmaktadır. Aslında alan isimleri gerçekte telefon numaraları gibi birer sayıdan ibaret olup, sadece kullanıcıların kolay hatırlayabilmeleri için harf karakterlerine dönüştürülmüştür. "Alan adı" yazıldığı an, bilgisayar bunları otomatik olarak sayılara çevirmektedir. Her alan adı, üst düzey alan adı (int, com, edu gibi gTLD-generik Top Level Domain) ve ülke isimlerini temsil eden (ccTLD-Country Code Top Level Domain) ile alt düzey

alan adı olarak nitelenen bir ön ekten oluşmaktadır. Örneğin Devlet Planlama Teşkilatının internet adresi olan "dpt.gov.tr" alan adının "gov.tr" kısmı üst düzey alan adını, "dpt" kısmı ise ikinci düzey alan adını oluşturmaktadır.

Alan Adı ve Hukuki Niteliği

Alan adının hukuki niteliği üzerinde tartışmalar bulunmaktadır. Bu tartışmalardan ilki, alan adının teknik özelliğinden kaynaklanmaktadır. Alan isimlerinin gerçekte birer sayı olması dolayısıyla medeni hukuk anlamında birer isim değil de telefon numaraları gibi kabul edilmelerine neden olmuştur. Fakat sadece teknik özelliğine dayanılarak alan isminin nitelemesi yapılamaz. İnternet kullanıcıları, alan adının gerçek sayı değerlerini değil, harf kombinasyonlarından oluşan isimlerini bilmekte ve kullanmaktadırlar. Mahkeme kararlarında da alan adının hukuken isim niteliğinde olduğu kabul edilmektedir.

Alan adı etrafında ortaya çıkan bir diğer tartışma da alan adının bilgisayarların tanınmasında kullanıldığı, bilgisayarların da bir hukuk süjesi olarak kabul edilemeyeceği ve dolayısıyla alan adlarının da hukuki anlamda bir isim olmadığı görüşü savunulmaktadır. İsim, niteliği itibarıyla kişilerin tanınmasını sağlayan bir ifade olmakla birlikte dış dünyada bir bilinci ifade etmekte ve ekonomik alanda da bir varlığı temsil etmektedir. Alan adı da aslında iletişimin ana unsuru olan bilgisayarı ifade etmemekte, bilakis bu bilgisayar yardımıyla başkalarıyla iletişime geçen bir gerçek ya da tüzel kişiyi ifade etmektedir. Dolayısıyla burada hukuki anlamda bir ismin varlığından söz edilmelidir.

Sorunun Ortaya Çıkması

Gerçek dünyada isimler birden fazla gerçek ya da tüzel kişi tarafından kullanılabilmektedir. Kullanılan isimlerin cins, meslek ya da bir meslek ismi olması da kullanımın çokluğu bakımından sonucu etkilemektedir. Mustafa Sarıkaya ismi ile birden fazla kişi bulunabilmekte, 'avukat, doktor, mühendis' gibi meslek isimleri birden fazla kimseyi niteleyebilmekte ve bu kimselerin her biri tarafından kullanılabilmektedir. Oysa alan adı teknik olarak bir kere alınabilmektedir, yani bir alan adından dünyada sadece bir tane bulunabilmektedir. Gerçek dünyada kullanılan isimlerin tekelleştirici ve kısıtlayıcı özelliği bulunmamasına karşın, alan adlarının tekelleştirici ve kısıtlayıcı özelliği bulunmaktadır. Bu sebeple özellikle meslek isimlerini ilk olarak adına kaydettiren kimse diğer meslektaşları karşısında büyük bir avantaj yakalamış olacaktır.

Ortaya Çıkan Sorunlar

Alan adları başlangıçta sadece internet erişimini kolaylaştırmak için düşünülmüşken, sonradan ticari alanda iş yerini belirleyen bir kimlikle eş değer hale gelmiştir. Bununla birlikte tanınmış markalar ve işletme adları alan adı olarak kullanılmaya, kartvizitlerde, reklamlarda yer almaya başlamıştır.

Belirli bir ismin, alan adı olarak kullanılması halinde mevcut marka, işaret ve isim haklarının ihlali söz konusu olabilmektedir. Belirli şartlar altında kullanılan alan adlarının tamamı veya belirli bir bölümü, mevcut marka, ticari isim ve gerçek veya tüzel kişilerin isimleri ile aynı veya benzer ise bir ihlalden bahsedilebilmektedir. Alan adlarının hukuk düzeni tarafından korunmasının arka planında, kullanılan bu isimler üzerinde korunmaya değer öncelikli hakların bulunmasıdır.

Alan adı kullanımı yoluyla ihlallere örnekler:

www.ecevit.com

www.mesutyilmaz.com

www.audi.de

www.bmw.de

www.akbank.com

www.refahpartisi.com

Teknik bakımdan alan adlarının birbiri ile karışması veya birden fazla alan adının kaydedilebilmesi mümkün değildir. Çünkü her bir alan adında mevcut harf karakterleri, bir sayısal karakteri temsil etmektedir. Aslında gerçek internet adresi, telefon numaraları gibi birer sayıdan ibarettir. Numaralandırılmış adresler olan bu sayılar yazıldığı zaman ilgili ana sayfanın bilgisayarına (server) bağlanır. Fakat numaraların kullanımı ve hatırlanmasının zorlukları düşünülerek bu sayısal adresler 'alan' adlarına dönüştürülmektedir. Herhangi bir alan ismi yazıldığı an, bilgisayar bunu otomatik olarak sayılara çevirir ve ilgili sayfaya bağlanır. Alan isminin yazılmasından sonra ekranın alt tarafında görülen rakamlar, gerçek adresi oluşturmaktadır.

Hukuki bakımdan alan adı etrafında ortaya çıkacak sorun bir cümle ile ifade edilebilir: "Alan adının aynen veya benzerinin kullanımın haksız olduğu id-

diası." Sorunun çözümünde uygulanacak hükümler özel hukukun birden fazla dalını ilgilendirmektedir.

Alan adları ile marka ve işletme adları arasında ortaya çıkan bu sorunların temelinde 'marka tescil sistemi' ile 'alan tescil sistemi' arasında bir bağlantının olmamasıdır. Marka tescili, genel olarak coğrafi alan bazında bir kamu kurumu tarafından yürütülmekte iken, alan isimlerinin dağıtımı, herhangi bir fonksiyonel sınırlama olmaksızın kamu kurumu dışında bir kurum tarafından yürütülmektedir. Aynı şekilde ticari (ticaret unvanı, işletme adı vs.) ve gerçek kişilere ait isimlerin hukuki statüsü ile alan adlarının hukuki statüsü birbirinden farklıdır. Tescil sistemindeki uyumsuzluk, ticari ve gerçek kişilere ait isimlerle alan adlarının statülerinin farklılığı, tanınmış marka ve işletme veya gerçek kişilerin isimlerinin hakkı olmayan üçüncü kişiler tarafından haksız olarak kullanılabilmesi imkânını (cybersquatting) ortaya çıkarmıştır. Alan adlarının korunması her ülkenin hukuk sistemlerinde farklı kanun ve hükümlerle sağlanmaktadır.

Alan adı etrafında ortaya çıkan hukuki sorunlar için uluslararası kuruluşlar tarafından değişik çözüm önerileri getirilmeye çalışılmaktadır. Bu kuruluşlardan biri olan WIPO toplantılarında marka ile alan isimleri arasındaki bağlantı üzerinde durulmuş, alan isimleri ile markalar arasındaki ortak sınır veya bağlantı (interface) araştırılmaya değer bulunmuştur ve marka hukukuna ait hükümlerin internette de uygulama alanı bulabileceği belirtilmiştir. Değişik ülkelerde verilen mahkeme kararlarında da olaya markalara ait hükümler uygulanmıştır.

Marka Hakkına Tecavüz

Marka Hakkına tecavüzün en tipik örneklerinden birini tescilli markaların alan adı olarak seçilmesi teşkil eder.

Tescilli Markaların Alan İsmi Olarak Seçilmesi

Burada ikili bir korumadan bahsetmek mümkündür. Aynı iş kolunda çalışanlara karşı ve farklı iş kolunda çalışanlara şeklinde bir ayrım söz konusudur.

Aynı İş Kolunda Çalışan Kimselerin Kullandığı Alan İsimlerine Karşı Tescilli Markaların Korunması

Girişimciler, alan adı alırken kendi alanında belirli bir müşteri kitlesine ulaşmış olan bir markayı alan adı olarak seçebilmektedirler. Böyle bir alan adı seçmiş olan kimseler, bu markanın tanınmışlığından faydalanarak kendi mal ve hizmetlerini daha geniş kitlelere duyurabilmektedirler. Ancak bu durumda markayı kullanma hakkına sahip olan kimsenin ticari itibarı, haksız olarak kullanılmakta, marka sahibinin markası için harcadığı emeğin karşılığını bir başkası devşirmektedir. Ayrıca markanın kalite, garanti ve reklam fonksiyonu da ortadan kalkmaktadır. Bilindiği gibi marka, bir malı diğerlerinden ayırt etmeye yarayan, ferdileştiren ve özelliklerini belirten işaretlerdir. Markaların mahreç gösterme fonksiyonunun yanında, garanti fonksiyonu, malın belirli bir yapımcı tarafından üretildiğini ve belirli bir kaliteye sahip olduğunu gösteren reklam fonksiyonu da bulunmaktadır. Tanınmış markaların alan ismi olarak belirlendiği web sayfalarında tüketici bu markalardan beklediği kaliteyi bulamamakta ve bu sayfanın kim tarafından sunulduğunu da bilememektedir. Bilgisayar kullanıcısı, bu web sayfası içinde reklamı yapılan resimleri görmekte, tanıtıcı yazıları okumakla birlikte, ilgili personelle konuşamamakta ve mal ve hizmetlerin yapımcısı (mahreç gösterme) hakkında bilgi alamamaktadır. WIPO, bu hallerde doğrudan bir marka tecavüzünün olduğunu veya korunan bir isim dolayısıyla bir yanıltma tehlikesinin söz konusu olacağı görüşündedir. Marka haklarından birini teşkil eden iyi bir şöhretin ve tutturulan yüksek kalite dolayısıyla bırakılan iyi izlenimin haksız olarak kullanılan bir alan adı dolayısıyla tecavüze uğraması da mümkündür.

Türk hukukunda markalar, 556 sayılı 'Markaların Korunması Hakkında Kanun Hükmünde Kararname' hükümleri ile korunmaktadır. Tescil edilmiş olan markaların hak sahibinden başka biri tarafından alan ismi olarak kullanılması, KHK.'nin 9'uncu maddesi ile engellenebilir. Bu hükümde, 'işareti kullanan kişinin, işaretin kullanımına ilişkin hakkı veya meşru bir bağlantısı olmaması koşuluyla, işaretin aynı veya benzerinin internet ortamında ticari etki yaratacak biçimde, alan adı, yönlendirici kod, anahtar sözcük veya benzeri biçimlerde kullanılması' yasaklanmıştır.

Bu halde bir markanın alan adı olarak kullanılmasında meşru bir menfaatinin bulunması gerekir. Meşru bir menfaat nedir? Meşru menfaati, söz konusu ibareyi kullanmasını haklı gösteren her türlü kullanımdır. Bu kişinin soyadı olabileceği gibi, işletme adı ya da ticaret unvanı yahut kendi markası da olabilir.

556 sayılı KHK'nın korumasından faydalanabilmek için söz konusu markanın tescil edilmiş olması gerekmektedir. Şayet marka tescil edilmemiş ise, ilgili koruyucu hükümlerden faydalanılamamaktadır. Ayrıca korumanın bir diğer şartı da markayı alan adı olarak seçmiş olan kimsenin bir ticari amaç taşımasıdır. Tescilli bir marka, ticari bir amaç dışında alan ismi olarak alınmış ise, örneğin bir şahsın sanat ürünlerini, bu alan ismi altında oluşturulan web sayfasında sunması gibi durumlarda KHK hükümlerinden faydalanılamamaktadır.

Koruma, markanın aynen kullanımı ile benzer ve çağrıştırıcı işaretlerin kullanılması hallerinde söz konusu olmaktadır. Markanın aynen alan ismi olarak kullanımı ne anlama gelmektedir? Markalar esas ve yardımcı unsurlar olmak üzere iki kısımdan oluşmaktadırlar. Markanın aynen kullanımına karar verilirken, esas unsurların dikkate alınması gerekmektedir. Bir markanın esas unsuru, o markayı benzerlerinden ayırt etmeye yarayan unsurdur. Bir markanın gerek aynının gerekse benzerlerinin kullanıldığının tespitinde esas unsuru teşkil eden şekil veya kelimenin aynının veya benzerinin kullanımı dikkate alınır. Esas unsuru teşkil eden şekil ve kelimelere yapılacak cüz'i değişiklikler iltibas halini ortadan kaldırmaz. Alan adları değişik üst düzey alan adları altında kaydedilmektedir. 'tr' ve 'com, org, net, edu ...' gibi üst düzey alan adları altında değişik ikinci düzey alan adları bulunmaktadır. Burada markanın aynı kullanımının nasıl tespit edileceği sorunu ile karşılaşılmaktadır. Burada iki alan adı arasında ayırıcı unsur olan üst düzey alan isimleri 'com' ve 'org' acaba markanın farklı kullanımı mı yoksa benzeri kullanımı olarak mı kabul edilecektir? Öncelikle bu soru teknik bakımdan ele alındığında; bir alan isminin yeryüzünde sadece bir tane olabileceği görülmektedir. Fakat farklı düzey isimleri altında aynı ismin kullanımı mümkündür. İki alan adının birbirinden teknik olarak ayrılabilmesi mümkündür ve her iki adresi alan kimselerin de bu alan adlarını almaya hakları bulunmaktadır. İnternet üzerindeki web sayfalarında bu üst düzey alan isimleri teknik olarak ayırıcı bir unsur olduğu gibi, markaların korunması söz konusu olduğunda bunların yine ayırıcı unsur olarak kabul edilmeleri gerektiği kanaatindeyim. Her ne kadar bunlar yardımcı unsurlar olarak kabul edilip söz konusu markayı ferdileştirmekten uzak ve başka web adreslerinde sayısız bir şekilde kullanılmakta olmasına rağmen, benzer alan adlarının kullanılmasında iltibasın tespitinde kullanılan ölçünün müşteri kitlesinin yanılma riski olduğundan hareketle internet kullanıcılarının üst düzey alan isimleri arasındaki farkı ayırabilecek kapasitede olduklarını kabul etmek gerekmektedir.

Markanın sahibinden başkasının marka benzeri bir ismi alan adı olarak kullanması da mümkündür. Markanın aynen ve aynı branşta faaliyet gösteren bir girişimci tarafından kullanılması halinde KHK'ye göre korumanın mümkün olduğu şüphesizdir. Tescil edilmiş bir markanın benzerinin alan ismi olarak marka sahibinden bir başkası tarafından kullanılması da KHK'nin 9'uncu maddesine göre mümkün olmamalıdır. Benzer alan isimleri ile ilgili Actmedia.Inc. ile Active Media International arasındaki bir davada bu gerekçe ile olaya bakan mahkeme, Active Media International şirketine 'www.actmedia.com' alan ismini kullanmayı yasaklamıştır. Burada mahkeme ayrıca ortalama bir yanılma riskini de yeterli görmüştür.

KHK'nin tescilli markaların korunması hakkında getirdiği sınırlamalar, alan adları için de geçerlidir. KHK.m. 12'ye göre; 'dürüstçe ve ticari veya sanayi konularıyla ilgili olarak kullanılmaları koşuluyla üçüncü kişilerin, ad ve adresini mal veya hizmetlerle ilgili cins, kalite, miktar, kullanım amacı, değer, coğrafi kaynak, üretim veya sunuluş zamanı veya diğer niteliklere ilişkin açıklamaları kullanmaları marka sahibi tarafından engellenemez'. Örneğin; alan ismi olarak seçilen 'bmw-tamircisi.com' gibi.

Farklı İş Kollarında Faaliyet Gösteren Kimselerin Kullandıkları Alan İsimlerine Karşı Tescilli Markaların Korunması

Tescil edilmiş bir markanın alan adı olarak hak sahibi dışında bir kimse tarafından alınması halinde de birtakım problemler ortaya çıkmaktadır. Alan isimlerinin teknik olarak bir defa kaydedilebilmesi özelliğinden dolayı, markanın bir başka kimse tarafından daha önce alınması halinde, marka sahibi artık markasını alan adı olarak kaydettiremeyecektir. Marka hukukunda, tescil edilmiş olan bir marka farklı iş kolunda faaliyet gösteren bir kimse tarafından alan ismi olarak alınması halinde kural olarak bir koruma mümkün değildir. Çünkü marka hukuku hükümlerine göre benzer emtia sistemi dolayısıyla farklı emtia için tescilli bir markanın aynen veya benzeri kullanılabilmektedir. Fakat farklı

iş kollarında faaliyet gösterseler bile bir markanın tanınmışlığından istifade etmek için o marka alan ismi olarak seçilebilmektedir. Dünyaca meşhur bir bilgisayar şirketi olan IBM, alan adı almak için müracaat ettiğinde bu ismin altında "Integrated Bituminious Mining" şirketine verildiğini tespit etmiştir. Bu şirket kayıt zamanına kadar olan faaliyetlerinde IBM kısaltmasını kullanmamıştır. Fakat alan adı olarak 24 harflik bir sınırlama getirildiği için şirketin baş harflerinden oluşan bir kısaltma kullanmak yolunu seçmiştir.

Benzer bir uyuşmazlık da 14 Nisan 1998 tarihinde Fransız mahkemelerinde görülmüştür. Alan adı olarak 'alice'yi kullanan ve farklı branşlarda faaliyet gösteren iki şirket arasında ortaya çıkan uyuşmazlıkta mahkeme çözüme esas olarak 'first come first served' yani "İlk gelen ilk alır," kuralına dayanmıştır. Mahkeme kararı, burada marka hukukunun uygulanmadığı ve aralarında bir rekabetin de söz konusu olmadığı şirketlerde de haksız bir rekabetin söz konusu olabileceğine işaret etmektedir.

Farklı sektörlerde faaliyet gösteren şirketler arasında Münih Mahkemesi'nde ortaya çıkan bir uyuşmazlıktan bahsetmek gereklidir. 'www.freundin.de' alan ismi altında bir web sayfası açan davalı Çöpçatan Şirketi ile 1948'den beri yayıncılık alanında faaliyet gösteren ve 'freundin' isimli bir gazete yayınlayan yayıncılar arasında uyuşmazlık çıkmıştır. Yayın şirketinin 'freundin'i alan adı olarak kullanmasının önlenmesi talebi reddedilmiştir. Buna gerekçe olarak davacıların yayın alanında faaliyet gösterdiği ve "freundin" isminin çöpçatanlık işleri için tescil edilmediği ve bu yüzden bir yanılma tehlikesinin söz konusu olamayacağı gösterilmiştir. Burada BGB.12'nin de korumasından faydalanılamayacağı; çünkü 'freundin' isminin, davacıların ismi olarak görülemeyeceği kabul edilmiştir.

Farklı branşlarda çalışan kimselerin bir marka adı alan ismi olarak seçmesi halinde dahi, iyi niyet kurallarına aykırılık söz konusu ise, yani sadece ismin marka sahibi tarafından kullanımının engellenmesi niyeti varsa mahkeme genel hükümlere göre (MK.m.2) bir koruma sağlamalıdır, zira ortada kötü niyetli bir tescil söz konusudur.

Farklı emtia sınıfında ya da iş kolunda bile olsa alan adının tanınmış bir marka karşısında korunması mümkün değildir. Bir markanın tanınmış olması, müşteri, akraba ya da düşman olmaları, sınıf, kültür, yaş farkı gözetmeksizin aynı çevredeki insanlar tarafından tanınması olarak tanımlanmıştır. Tanınmış bir markanın farklı sektörlerde çalışan kimseler tarafından alan ismi olarak kullanılmasının, KHK m. 12 kapsamında değerlendirilip değerlendirilmeyeceği konusunda iyi niyet kurallarından faydalanılması en uygun çözüm olarak görülmektedir.

Tescil Edilmemiş Markalarla Diğer Ticari İsimlerin Alan İsmi Olarak Kullanılması

Tescil edilmemiş olan bir markanın KHK'nin hükümleri ile korunması mümkün değildir. Tescil edilmeyen bir markanın ve yine diğer ticari isimlerin alan adı olarak seçilmesi halinde ancak haksız rekabet hükümlerine göre korunması mümkündür.

Bir Alan Adı Üzerinde Yarışan Hak Sahipliği

Yukarıda bahsedildiği üzere, alan adının teknik yapısı nedeniyle bir alan adından dünyada sadece bir tane olabilir. Buna karşın aynı ismi çok sayıda kimse taşıyabilir. Aynı ticaret unvanının çekirdek kısmından çok sayıda olabilir.

Alan adı olarak seçilen isimler üzerinde kullanıcıların her birinin yetkili olması durumunda ortaya incelemeye değer sorunlar çıkabilmektedir. İsim ve soy isimleri aynı olan iki kimsenin kendi adlarına web sayfası açmaları halinde ya da aynı marka ya da ticaret unvanına sahip iki tacir arasında böyle bir sorun söz konusudur.

Bu tip uyuşmazlıklar nasıl çözüme bağlanacaktır? "İlk gelen ilk alır" prensibinin uygulanması burada her zaman haklı ve adil çözümlere ulaşılmasını sağlamamaktadır. Aynı zamanda burada 'üstün veya öncelikli hak'tan bahsedilebilir mi?

Bu tür uyuşmazlıkların çözümünde ilk önce alan adının dayandığı markalar, ticari unvanlar veya isimleri arasında yanıltma tehlikesinin giderilmesi ve öncelik prensiplerinin irdelenmesi gerekmektedir. Öncelik ilkesi, herhangi bir alan adını ilk kaydettiren kimsenin bu ismi kullanmaya hak sahibi olduğunu ifade etmektedir. Kullanılan isimler arasında meydana çıkabilecek uyuşmazlıklarda adın birinin öncelik hakkına sahip olduğu belirlenir veya diğer isim yanıltma tehlikesi dolayısıyla bu yanılmayı giderme ile yükümlü bulunursa bu takdirde alan adları arasındaki uyuşmazlık da buna göre çözümlenebilmektedir. Fakat öncelik prensibinin hakkaniyete uygun bir şekilde uygulanabilmesi, önceliğe sahip olan hakkın aynı zamanda da hukuk tarafından daha korunan bir hak konumunda bu-

lunmasına bağlıdır. Bir kararda bir şirketin ismini, alan ismi olarak kaydettirmiş olan bir üniversite öğrencisine karşı açılan davanın reddine karar verilmiştir. Bu kararda uyuşmazlık konusu olan alan adının, aynı zamanda üniversite öğrencisinin soyadı olduğu ve öncelik ilkesi uyarınca bu ismi, alan adı olarak kullanmaya hak sahibi olduğu belirtilmiştir.

Öncelik ilkesine göre getirilen çözümün hakkaniyete uygunluğunun sağlanabilmesi için ayrıca alan adını alan kimsenin iyi niyet kurallarına aykırı davranmaması da gerekmektedir. Bir hakkın sadece bir başkasını zarara sokmak için kullanılmasını kanun himaye etmemektedir (MK.2/2).

Bazı adların alan ismi olarak kullanılmasında öncelik prensibi terk edilebilir. Özellikle bir üstün veya öncelikli hak söz konusu ise alan ismi öncelik prensibine göre değil, öncelikli hak prensibine göre tahsis edilmelidir. Bir mahkeme kararında bir şirket tarafından bir şehir ismi olan 'ansbach' isminin kullanılması durumu incelenmiş ve şirketin bu ismi kullanamayacağına karar vermiştir. Mahkeme bu kararında özellikle, internet kullanıcılarının böyle bir alan ismi altında sadece bir şehir hakkında bilgi edinmedikleri, aynı zamanda belediyeden bu bilgileri vermesini bekledikleri gerekçesine de dayanmaktadır. İsim ve soy isimleri kısaltmalarının bir kamu kurumun kullandığı kısaltmalarla aynı olması hâlinde de bu kısaltmaları kullanma hususunda kamu kuruluşuna üstün bir hak tanınmalıdır. Çünkü burada da internet kullanıcıları bir yanılgıya düşebilmektedirler ve de bu isim altında bu kurumdan bilgi vermesini beklemektedirler.

Alan Adlarına Karşı Açılacak Davalarda Üst Düzey Alan Adının Önemi

Alan adları yönetimi (ICANN) tarafından her ülke resmi ya da resmi olmayan sözleşmeli kurumlara 'ülke üst düzey' alan adları altında tahsis yapma imkânı açılmıştır. Türkiye'de ilk dönemlerde ODTÜ tarafından yapılan alan adı tahsisi daha sonra kurulan başka 'nic.tr' isimli kuruluşa devredilmiştir. Ancak gerek ODTÜ gerekse "nic.tr" yönetimi, eleştirilen yöntemleriyle 'tr' alan adından kaçışa da neden olmuştur.

Her ülkede ICANN tarafından yetkilendirilmiş bu kuruluş ve kurumlar benimsedikleri politikalar nedeniyle kendi ülkelerine ait uzantılarla alan adı tescili yapmaktadırlar. Örneğin Türkiye 'tr' üst düzey alan adını, Almanya 'de' alan adını, Fransa 'fr' alan adını kullanmaktadır. Ayrıca herhangi bir ülke üst düzey alan adı olmayanlar vardır. Örneğin 'com', 'org', 'biz' gibi.

Ülke üst düzey alan adı ile ilgili ihtilaflarda hangi ülke alan adı kullanılıyorsa o ülke alan adı yönetim sistemi karar vermeye yetkilidir. Örnek olarak 'tr' uzantılı bir alan adı varsa, Türk mahkemelerinin verdiği kararlar da kolaylıkla icra edilebilecektir. Ancak ülke uzantısız ise bu durumda alan adının geri alınması ve ihtilafın çözüme kavuşması oldukça zorlaşmaktadır. Bu durumda ihtimaller:

1. Türk mahkemelerinden alınan kararın tanınması ve tenfizi,
2. Doğrudan Virjinya'da dava açılması,
3. Akredite edilen kurumlar nezdinde alan adı uyuşmazlık giderim usulüne başvurmaktır.

Bunlardan en bilineni WIPO'dur.

Türkiye'deki birçok kişi ve kuruluş haksız yere başkalarınca tescil edilen alan adını tahkim benzeri usulle geri almıştır.

Ticaret Unvanı ve İşletme Adının Korunması

Türk Ticaret Kanunu hükümlerine göre tacirler için ticaret unvanını seçmek ve kullanmak zorunludur. Aynı şekilde bir tacirin kullandığı bir işletme adı varsa bunu da sicile tescil ettirir. Türk Ticaret Kanunu, ticaret unvanı ve işletme adından sadece bir tane bulunabileceğini kabul etmiştir. Bu nedenle daha önce Türkiye'de tescil ve ilan edilmiş bulunan bir unvanın ya da işletme adının bir başkası olarak alınabilmesi mümkün değildir. Bir şekilde alınmış olsa bile TTK.m.52'ye göre terkin ettirilmesi ve şartların varlığı halinde tazminat davalarının açılabilmesi de mümkündür.

Türk Ticaret Kanunu'nda MarKHK.m.9'dan farklı olarak ticaret unvanını alan adına karşı koruyan bir düzenleme bulunmamaktadır. Bu durum, bir tacirin ticaret unvanı ya da işletme adının alan adı karşısında korumasız kaldığı şeklinde de anlaşılmamalıdır.

Bir başkasına ait ticaret unvanının haksız olarak alan adı olarak alınması halinde kanaatimce TTK.m.50'de açıkça bahsedilmese ticaret unvanının inhisar hakkına alan adları da girer. Zira aksinin kabulü, ticaret unvanını seçmiş, ona belli bir yatırım yapmış kimsenin mağdur olmasına sebep olur. Bu nedenle bir taraftan TTK.m.50 diğer taraftan TTK.m.52 gereğince ticaret unvanı haksız alan adı olarak alınmış kimsenin korunması gerekir.

Alan Adının Korunması

Herhangi bir marka, ticaret unvanı ya da işletme adına dayanmaksızın tescil edilmiş, belli bir süre kullanılmış olan alan adlarının da korunması gerekir. Esasen Türk hukukunda birçok hukuk sistemine benzer bir şekilde bu yönde bir düzenleme bulunmamaktadır. Bu halde örneğin marka değeri çok yüksek olan 'Google' veya 'Yahoo' gibi bir ismin marka ya da ticaret unvanı olarak alınabilmesi mümkün müdür?

Kanaatimizce bu soruya olumsuz cevap vermek gerekir. Bunun sebeplerine gelince: Öncelikle gerek marka gerekse ticaret unvanı ile ilgili korumanın temelinde öncelik ilkesi büyük bir önem taşır. Türk hukukunda her ne kadar karma sistem kabul edilmiş ise de gerek ticaret unvanı gerekse marka hukuku, bir işareti önce tanıtan kişinin hakkını daha korunmaya değer bulmaktadır. Yine MarKHK.m. 8'e göre bu durumlarda alan adının varlığı, marka tescili önünde bir engeldir. Gerçekten söz konusu hükme göre "Tescil için başvurusu yapılmış markanın, başkasına ait kişi ismi, fotoğrafı, telif hakkı veya herhangi bir sınai mülkiyet hakkını kapsaması halinde, hak sahibinin itirazı üzerine tescil başvurusu reddedilir". Yine bir alan adı haksız olarak bir başkası tarafından marka olarak tescil edilmiş bile olsa alan adının sahibi, MarKHK.m.42'ye göre hükümsüzlük davası açabilecektir. Dolayısıyla bir başkasının aldığı ve tanıttığı bir alan adının başkaları tarafından ticaret unvanı, işletme adı ya da marka olarak tescil edilmesi de Türk hukukunda önlenmiştir.

Markanın Adwords Reklamlarda ve Başlıklarda (Meta Tag) Kullanılması

Browserların hazırlanan sayfaya yöneltilebilmesi için arama mekanizmalarının meta-taging denilen bir yöntemle maniple edilmesi gerekmektedir. Bu maniple, web sayfasının esas başlığında (header) bulunmayan kelimelerin bir liste halinde arama motorlarına verilmesiyle yapılmaktadır. Adwords reklamlar ise Google arama motorunun reklam yapmak isteyenlere sunduğu kelime bağlantılarıdır. Bu bağlantılar sayesinde arama motorlarında çok taranan marka, kişi arandıkça ilgili reklam kullanıcının karşısına çıkarılmaktadır. Bu reklamın kullanıldığı markanın haksız kullanımdır.

Gerek meta-tag kullanımı, gerekse adwords reklam yolu ile marka sahibi dışında bir kullanım marka ihlalidir (MarKHK.m.9).

Arama Motoru
Webde yayınlanan bilgiyi aramak için kullanılan bir yazılım paketidir.

Keyword advertising, bir üst kavram olarak adwords ve adsense reklamlarını da kapsayan, başta Google olmak üzere, Yahoo ve Microsoft gibi önde gelen arama motorlarınca kullanılan, arama içeriğine bağlı, anahtar sözcüklerle yapılan reklam sistemini ifade etmektedir.

Öğrenme Çıktısı

2 Fikrî ve sınai hakların korunması konusunda internette ne tür özelliklerin olduğunu açıklayabilme
3 İhlallerin nasıl niteleneceğini ifade edebilme

Araştır 2	İlişkilendir	Anlat/Paylaş
Fikrî ve sınai hakların İnternet'te ihlal edilmesi gibi hukuki sorunlara neden olmaktadır?	Fikri ve sınai hakların internet üzerinden ihlal edilmesi ile başka türlü ihlal edilmesi arasında hukuken bir farklılık var mıdır?	İnternet'in varlığının hak ihlalleri üzerindeki etkisini çevrenizle paylaşınız.

1 Eser sahibinin haklarını detaylı bir şekilde açıklayabilme

İnternet Ortamında Fikrî Haklar ve Korunması

Eser sahibinin hakları manevi ve mali haklar olarak ikiye ayrılabilir.

Eser sahibinin adının belirtilmesi hakkı, eser sahibinin adının eserde yer almasını kapsadığı gibi eserin kullanıldığı her yer ve durumda açıkça belirtilmesini de kapsamaktadır. Bu hak, bir taraftan eseri sahibine bağlar, diğer taraftan da eser sahibini eser hırsızlarına karşı (intihal) korur.

Eserde Değişiklik Yapılmasını Yasaklama Hakkı, fikir ve sanat eserleri, eser sahibinin adı, eserin adı ve muhteva ile şekil olarak bir bütün teşkil eder. Bu bütünlüğün korunmasında eser sahibinin manevi bir menfaati bulunmaktadır. Eser sahibinin eserinde zorunlu hâllerde değişiklik yapılabilmektedir. Bu zorunluluk halleri, onarım, ihtiyaca uygun hâle getirmek, halkın ve çevrenin güvenliği zorunlu hâllere örnek olarak verilebilir. Eser sahibinin zorunlu hâller dışında eserinde değişikliklere izin verme yetkisi sadece onun tarafından kullanılabilmektedir ve miras yolu ile intikale yahut üçüncü şahıslara devredilmeye elverişli bulunmamaktadır.

İşleme Hakkı, Fikir ve Sanat Eserleri Kanunu anlamında bir işlemeden bahsedilebilmesi için eseri dönüştüren kimsenin de esere katkısının bulunması gerekmektedir. İşleme eserde iki unsurun bulunması gerekir. Birincisi işleme eser, orijinal eserden bağımsız değildir, ikincisi ise onu işleyen kişilerin de esere bir katkısını taşımaktadır. Eserin kısaltılması veya genişletilmesi işlenme sayılmaz. Bir roman veya hikâyenin kısaltılması, bir tablodan belirli bir kısmın çıkarılması, senaryonun rejisör tarafından kısaltılması birer işlenme değildir. Çoğaltma Hakkı, FSEK 22. maddesinin I. fıkrasına göre, bir eserin aslının veya kopyalarının herhangi bir şekil veya yöntemle, tamamen veya kısmen, doğrudan veya dolaylı, geçici veya sürekli olarak çoğaltılmasıdır.

Umuma İletim Hakkı, FSEK m. 25'in yeni düzenlemesi ile umuma iletim, bir eserin veya çoğaltılmış nüshalarının radyo, televizyon veya herhangi diğer bir teknik usulle umumun yararlanmasına sunulmasıdır.

öğrenme çıktıları ve bölüm özeti

2 Fikrî ve sınai hakların korunması konusunda internette ne tür özelliklerin olduğunu açıklayabilme

3 İhlallerin nasıl niteleneceğini ifade edebilme

İnternet Ortamında Sınai Hakların Korunması

Eser sahibine İnternet yeni imkânlar sunmaktadır. Eserini daha geniş kitlelere kolayca ulaştırabilmektedir. Eserler için iyi bir reklam yoludur. Eser hakkı sahibi, eserini üçüncü ve ilgili kimselere daha çabuk ve daha ucuz bir reklamla tanıtabilme imkânına kavuştuğu gibi eserini dijital ortamda yayınlayabilme imkânına da kavuşmuştur. Ayrıca eserler dijital ortamda satışa da sunulabilmektedir.

İnternet yoluyla dünyanın her tarafından esere ulaşanların çokluğu ve kullanıcıların çeşitliliği, eserin haksız ve izinsiz kullanılması ihtimalini de artırmıştır. Herhangi bir kişisel bilgisayara ve İnternet bağlantısına sahip olan kimse, İnternet üzerinde bulunan bir eseri kalite kaybı olmaksızın kopyalayabilmekte ve çoğaltabilmektedir.

Bilişim sisteminde eser sahipleri ile ilgili temel düzenleme, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda (FSEK) yer almaktadır. Bunun yanında çok sayıda uluslararası anlaşama da fikri hukukun kaynağını teşkil eder.

Fikir ve sanat ürünleri Kanunda, "sahibinin hususiyetini taşıyan ve ilim, edebiyat, musiki, güzel sanatlar veya sinema eserleri sayılan her nevi fikir ve sanat mahsulü" olarak tanımlanmaktadır.

Eser sahibine İnternet yeni imkânlar sunmaktadır. Eserini daha geniş kitlelere kolayca ulaştırabilmektedir. Eserler için iyi bir reklam yoludur. Eser hakkı sahibi, eserini üçüncü ve ilgili kimselere daha çabuk ve daha ucuz bir reklamla tanıtabilme imkânına kavuştuğu gibi eserini dijital ortamda yayınlayabilme imkânına da kavuşmuştur. Ayrıca eserler dijital ortamda satışa da sunulabilmektedir.

İnternet yoluyla dünyanın her tarafından esere ulaşanların çokluğu ve kullanıcıların çeşitliliği, eserin haksız ve izinsiz kullanılması ihtimalini de artırmıştır. Herhangi bir kişisel bilgisayara ve İnternet bağlantısına sahip olan kimse, İnternet üzerinde bulunan bir eseri kalite kaybı olmaksızın kopyalayabilmekte ve çoğaltabilmektedir.

Bilişim sisteminde eser sahipleri ile ilgili temel düzenleme, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda (FSEK) yer almaktadır. Bunun yanında çok sayıda uluslararası anlaşama da fikri hukukun kaynağını teşkil eder.

Fikir ve sanat ürünleri Kanunda, "sahibinin hususiyetini taşıyan ve ilim, edebiyat, musiki, güzel sanatlar veya sinema eserleri sayılan her nevi fikir ve sanat mahsulü" olarak tanımlanmaktadır.

1 Aşağıdakilerden hangisi internet teknolojisinin eser sahibi için getirdiği tehlikelerden biridir?

A. Eserlerin hızlı yayılması
B. Eserlerin kopyalanması
C. Dijitalleşme
D. Multimedya olması
E. Arama motorlarından bulunması

2 Değişim programlarında bir eserin kullanılması halinde eser sahibi ya da hak sahibinin aşağıdaki haklarından hangisi ihlal edilir?

A. Mali haklarının tümü
B. Manevi haklarının tümü
C. Çoğaltma hakkı, umuma iletim hakkı
D. İşleme hakkı, adın belirtilmesi hakkı
E. Eserde değişiklik yapılmasını men hakkı

3 Link tekniği ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır?**

A. Link, internet kullanıcısına bir başka içeriği işaret eder.
B. İnternet kullanıcısının bir diğer sayfaya geçişini mümkün kılar.
C. Harici ve dahili link olarak iki kısma ayrılabilir
D. Bir sayfada diğer sayfanın da görüntülenmesini sağlar.
E. Çoğaltmalar kullanıcının bilgisayarında gerçekleşir.

4 Frame teknolojisi ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Bir sayfadan diğerine geçişi sağlar.
B. İnternet kullanıcısının tek bir sayfasında birçok işlevi yüklemesini mümkün kılar.
C. Verilerin sıkıştırılmasını sağlar.
D. Verilerin hızlı transferini sağlar.
E. Bir internet sayfasında bir başka sayfanın görüntülenebilmesini sağlar.

5 Değişim programları ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır?**

A. Merkezi olan ve olmayan değişim programları vardır.
B. Her türlü verinin değişimi mümkündür.
C. Kullanıcının yaptığı fikri ürüne ilişkin değişimler FSEK.m.38 kapsamında yasaldır.
D. Değişimlerde eserin çoğaltılması söz konusudur.
E. Eserlerin umuma iletimi de vardır.

6 Paylaşım platformlarının sorumluluğu ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Aracı hizmet sağlayıcı olan paylaşım platformu kural olarak sorumlu değildir.
B. Eser sahiplerinin haklarının ihlalinden sorumludur.
C. Eser sahiplerinin hak ihlalleri nedeniyle sitelerinin erişime engellenmesi mümkündür.
D. Eser sahiplerinin platforma koydukları eserleri kontrol yükümlülüğündedir.
E. İhlal teşkil eden eserlere ilişkin tazminat davasının tarafıdırlar.

7 Alan adı ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Alan adı bir markadır.
B. Alan adı bir ticaret unvanıdır.
C. Alan adı bir coğrafi işarettir.
D. Alan adı kendine özgü bir isimdir.
E. Alan adı, sayılardır.

8 İnternet alan adının bir başkası tarafından marka olarak tescili halinde aşağıdakilerden hangisi yapılabilir?

A. Marka tesciline öncelik verilir ve marka tescili korunur.
B. Markanın hükümsüzlüğü talep edilir.
C. Marka sahibine tazminat davası açılır.
D. Hem marka hem de alan adı birlikte var olmaya devam eder.
E. Marka sahibi alan adı sahibine markasının korunması için dava açabilir.

neler öğrendik?

9 Aşağıdakilerden hangisi marka ihlali **sayılmaz?**

A. Siemens markasının Bosch şirketi tarafından meta-tag olarak kullanımı
B. AEG tarafından Grundig markasının adwords reklamlarda kullanımı
C. Arçelik markasının Profilo olarak alan adı olarak kullanımı
D. Regal markasının bir web sayfasında asıl unsur olarak kullanılması
E. Arçelik tamircisinin, arceliktamircisierkan.com şeklinde bir alan adı alması.

10 Bir eserin web sayfasında yayınlanması halinde eser sahibinin yararlanabileceği özel usul aşağıdaki kanunlardan hangisinde bulunur?

A. Türk Ticaret Kanunu
B. Fikir ve Sanat Eserleri Kanunu
C. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
D. Borçlar Kanunu
E. Elektronik İmza Kanunu

1. B	Yanıtınız yanlış ise "İnternet Ortamında Fikri Haklar ve Korunması"? konusunu yeniden gözden geçiriniz.
2. C	Yanıtınız yanlış ise "Değişim Programları" konusunu yeniden gözden geçiriniz.
3. D	Yanıtınız yanlış ise "Link ve Frame Kullanılması" konusunu yeniden gözden geçiriniz.
4. E	Yanıtınız yanlış ise "Link ve Frame Kullanılması" konusunu yeniden gözden geçiriniz.
5. C	Yanıtınız yanlış ise "Değişim Programları" konusunu yeniden gözden geçiriniz.
6. A	Yanıtınız yanlış ise "Paylaşım Programları" konusunu yeniden gözden geçiriniz.
7. D	Yanıtınız yanlış ise "Alan Adının Niteliği ve Sorunun Ortaya Konulması" konusunu yeniden gözden geçiriniz.
8. B	Yanıtınız yanlış ise "Tescilli Markaların Alan İsmi Olarak Seçilmesi" konusunu yeniden gözden geçiriniz.
9. E	Yanıtınız yanlış ise "Tescilli Markaların Alan İsmi Olarak Seçilmesi" konusunu yeniden gözden geçiriniz.
10. B	Yanıtınız yanlış ise "İnternet Ortamında Eser ve İnternet'te Eserlerin Yer Alma Türleri" konusunu yeniden gözden geçiriniz.

7 Araştır Yanıt Anahtarı

Araştır 1

Eser sahibinin hakları manevi ve mali haklar olarak ikiye ayrılabilir: Eser sahibinin adının belirtilmesi hakkı, Eserde Değişiklik Yapılmasını Yasaklama Hakkı, eser sahibinin manevi haklardır. İşleme Hakkı, Çoğaltma Hakkı, Umuma İletim Hakkı ise eser sahibinin mali haklarıdır.

Araştır 2

İnternet yoluyla dünyanın her tarafından esere ulaşanların çokluğu ve kullanıcıların çeşitliliği, eserin haksız ve izinsiz kullanılması ihtimalini de artırmıştır. Herhangi bir kişisel bilgisayara ve internet bağlantısına sahip olan kimse, internet üzerinde bulunan bir eseri kalite kaybı olmaksızın kopyalayabilmekte ve çoğaltabilmektedir. Bir eserin dijitalleşmesi ile telif hakkının ihlalinin kolaylaşmasıdır. Birkaç tuş yardımı ile internette dolaşan eserler izinsiz olarak sınır ötesine taşınabilmekte, kopyalanabilmekte ve çoğaltılabilmektedir. Kolayca taklit edilebilme ve yanıltılabilme, kopyalanabilmeye karşı yeni hukuki enstrümanlar aranmakta ve yeni teknolojiler geliştirilmeye çalışılmaktadır.

Kaynakça

Bechtold, S. Schutz des Anbieter von Information Urheberrecht und Gewerblicher Rechtsschutz im Internet. www.jura.uni-tuebingen.de/ri/96ws/bechtold/seminar.htm

Bosak, V.M. (2001). Urheberrechtliche Zulaessigkeit privaten Downloadings von Musikdateien. CR 3.

Bozbel, S. (2006). Mukayeseli Hukukta ve Türk Hukukunda Karşılaştırmalı Reklam Hukuku. Ankara.

Burmeister, K. (2000). Urheberrechtsschutz gegen Framing im Internet-eine rechtsvergleichende Untersuchung des deutschen und US-amerikanischen Urheberrechts. Köln.

Çabuk, S. & Bağcı, M.İ. (2003). Pazarlamaya Çağdaş Yaklaşım. İstanbul.

Decker, U. (1999). Urheberpersönlichkeitsrecht im Internet. "Hoeren, T. & Sieber, U. (1999) Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschaeftsverkehrs", München.

Eichhorn, B. (2000). Internet-Recht, Ein Lehrbuch für das Recht im World-Wide-Web. Köln.

Erel, Ş. (2009). Türk Fikir ve Sanat Hukuku. Ankara.

Eren, F. (2015). Borçlar Hukuku Genel Hükümleri. Ankara.

Federrath, H. (2000). Multimediale Inhalte und technischer Urheberrechtsschutz im Internet. ZUM.

Fröhlich, M. (2001). Zentrale Institionen des deutschen Urheberrechts und des fransözischen Droit d'autteur auf dem Prüfstand der elektronischen Netzwerke. Frankfurt am Main.

Gabel, D. (1988). Anmerkung zum Urteil des LG Düsseldorf vom 29.4.1998. K&R.

Gahrau, E. (1999). Einleitende Überlegungen. (Hoeren, T./ Sieber, U.: Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschaeftsverkehrs), München.

Haas, E. M. (1998). Die Französische Rechtsprechung zum Konflikt zwischen Domaninnamen und Kennzeichenrechten. GRUR-Int., s. 939.

Hüsch, M. (2006). Der Gebrauch geschützter Kennzeichen als Advertising Keywords (AdWords). K&R, s. 223.

Ihde, R. Hyperlinks. www.graefe-partner.de/ecom/hyperlinks.html; Ernst, NJW-CoR

Junker, M. (2002). Anwendbares Recht und internationale Zustaendigkeit bei Urheberrechtsverletzungen im Internet. Kassel.

Karahan, S., Suluk, C., Saraç, T. & Nal, T. (2013). Fikri Mülkiyet Hukukunun Esasları. Ankara.

Klett, A. (1998). Urheberrecht im Internet aus deutscher und amerikanischer Sicht. Baden-Baden.

Kur, A. (1996). Namens-und Kennzeichenschutz im Cyberspace. CR.

Kur, A. (1999). Neue perspektiven für die Lösung von Domainnamenkonflikten: Der WIPO-Interim Report. GRUR, Int., Heft 3.

Laga, G. (1998). Neue Techniken im World Wide Web - Eine Spielwiese für Juristen? JurPC Web-Dok. 25, Abs. 1 – 50 (www.jurpc.de)

Lehmann, M. (1997). Digitalisierung und UrhR, Internet und Multimdiarecht (Cyberlaw). Stutgart.

Lehmann, M. & Tucher, T. (1999). Urheberrechtlicher Schutz von multimedialen Webseiten. CR.

Leistner, M. & Bettinger, T. (1999). Immaterialgüterrechtlicher und wettbewer bsrechtlicher Schutzdes Web-Designers. CR.

Leupold, A. & Demisch, D. (2000). Bereithalten von Musikwerken yum Abruf in digitalen Netzen. ZUM, s. 385.

Mankowski, P. (1999). Besondere Formen von Wettbewerbsverstössen im Internet und Internationales Wettbewerbsrecht. GRUR Int., Heft 12, s. 998.

Memiş, T. (2001). Alan İsmi Etrafında Ortaya Çıkan Hukuki Sorunlar. Bilişim Toplumuna Giderken Psikoloji, Sosyoloji ve Hukukta Etkiler Sempozyumu, Ankara.

Memiş, T. (2000). İnternette Cins ve Meslek İsimlerinin Alan İsmi Olarak Kullanılması ve Ortaya Çıkan Hukuki Sorunlar. Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, Erzincan, VI, ss. 1-2.

Memiş, T. (2003). Fikri Hukuk Bakımından İnternet ortamında Müzik Sunumları. Ankara.

Memiş, T. (2006). FSEK Değişikliği İle İnternet Ortamında Fikri Hak İhlallerinin Engellenmesi İçin Getirilen Usul. Fikri Mülkiyet Hukuku Dergisi, Sayı 1.

Memiş, T. & Bozbel, S. (2008). Marka Ve Haksız Rekabet Hukuku Bakımından Adwords Reklamlar. E-Akademi Dergisi, Kasım, Sayı 81 (www.e-akademi.org).

Meyer, S. (2007). Google & Co. – Aktuelle Rechtsentwicklungen bei Suchmaschinen. K&R (Kommunikation und Recht).

Nordemann, W. (1998). Urheberrecht, Kommentar zum Urheberrecht und zum Urheberrechtswahrnehmungsgesetz. Stuttgart.

Öztek, S. (1991). Haksız Rekabete İlişkin Yeni İsviçre Düzenlemesinin Öngördüğü Bazı Haksız Rekabet Halleri. Jale G. Akipek'e Armağan, Konya.

Peter M. (1999). Besondere Formen von Wettbewerbsverstössen im Internet und Internationales Wettbewerbsrecht. GRUR Int.

Plass, G. (2000). Hyperlinks im Spannungsfeld von Urheber-, Wettbewerbs- und Haftungsrecht. WRP, 6.

Saacke, A. (1998). Schutzgegenstand und Rechtsinhaberschaft bei Multimediaprodukten-Grundfragen des Rechtsschutzes und der Lizenzierung. in: Götting, Horst-Peter (Editor)- "Multimedia, Internet und Urheberrecht".

Sabih A. (1998). Marka Hukuku. Cilt II, Ankara.

Schack, H. (2001). Urheber- und Urhebervertragsrecht. 2. Aufl. Tübingen.

Schack, H. (2001). Urheberrechtliche Gestaltung von Webseiten unter Einsatz von Links und Frames. MMR.

Schuster, F. & Müller, U. (2000). Entwicklung des Internet- und Multimediarechts von Januar 1999 bis Juni 2000. MMR-Beilage, 10.

Selim K. (1961). İsviçre Federal Mahkemesinin Markalar Arasında İltibasla İlgili Kararları. Batider, 2(2).

Sosnitza, O. (2001). Das Internet im Gravitationsfeld des Rechts: Zur rechtlichen Beurteilung so genannter Deep Links. CR (10).

Strömer, T. H. (1999). Online Recht, Rechtsfragen im Internet. 2. Auflage, Heidelberg.

Tekinalp, Ü. (2012) Fikrî Mülkiyet Hukuku. İstanbul.

Tekinalp, Ü. (1999). Markanın Üçüncü Kişi Tarafından Kullanılması. Prof. Dr. Selahattin Sulhi Tekinay'ın Hatırasına Armağan, İstanbul.

Tekinay, S. S. (1988). Esas Unsurları Dolayısıyla Koruma Dışı Bırakılan Markalar. Prof. Dr. Yaşar Karayalçın'a Armağan, Ankara.

Von Bonin, A. & Köster O. (1997). Internet im Lichte neuer Gesetze. ZUM, s. 823.

Völker, S. & Lührig, N. (2000). Abwehr unerwünschter Inline-Links. K&R (1).

Zscherpe (1998). Urheberrechtsschutz digitalisierter Werke im Internet, MMR.

Bölüm 8

Bilişim Hukuku Alanındaki Son Gelişmeler

Öğrenme çıktıları

İnsan Hakları Teorisine İlişkin Temel Bilgiler

1 İnternete erişim hakkını insan hakları teorisi çerçevesinde açıklayabilme ve dördüncü kuşak insan haklarını tanımlayabilme

Unutulma Hakkı

2 Unutulma hakkını genel olarak tanımlayabilme, bu hakkın normatif dayanağını belirtebilme ve diğer temel hak ve özgürlükler ile ilişkisini açıklayabilme

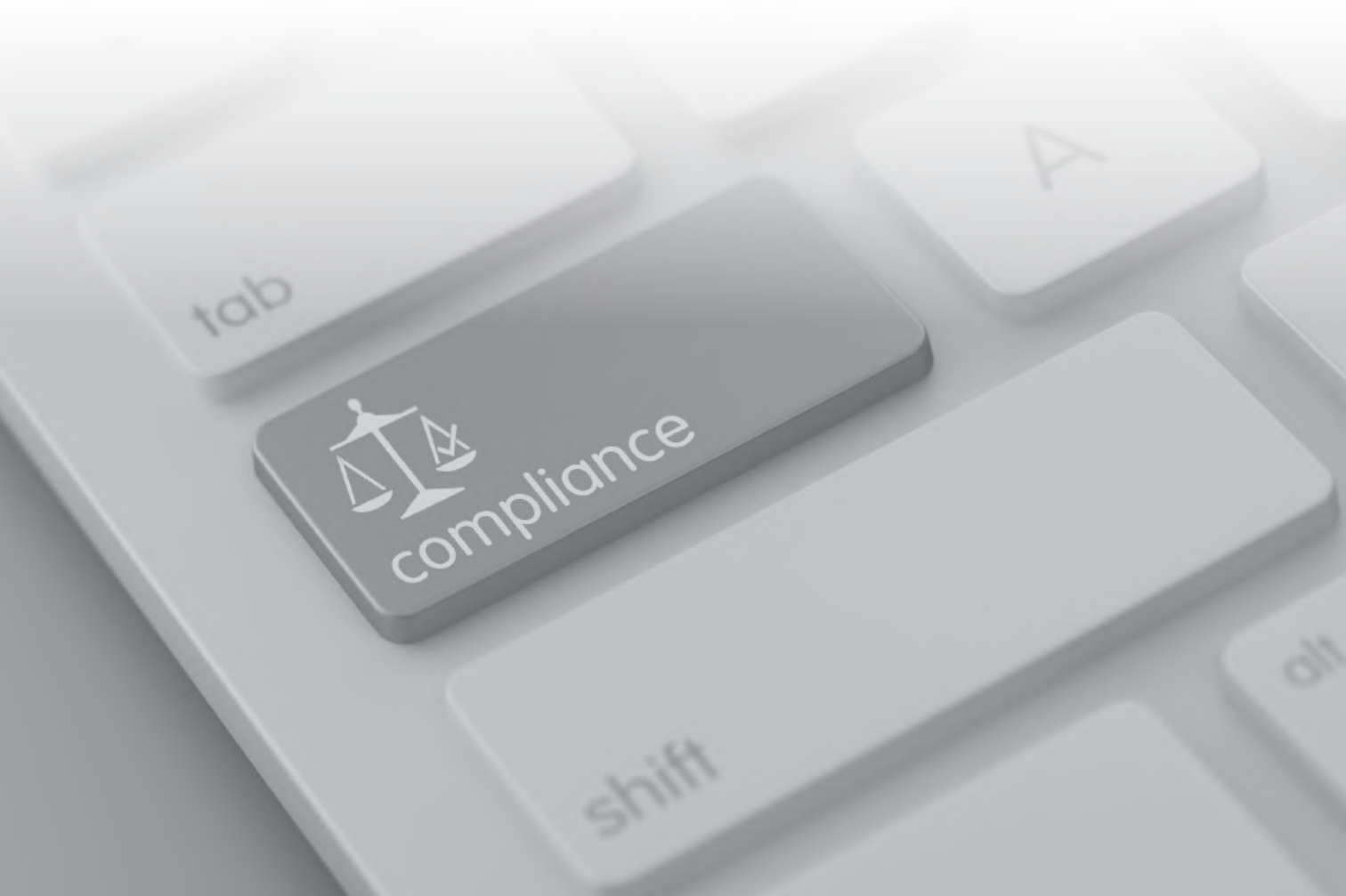
Unutulma Hakkına İlişkin Yargı Kararları

3 Unutulma hakkına ilişkin ABAD, AYM ve HGK tarafından verilmiş kararları tartışabilme

Unutulma Hakkına İlişkin Ulusal Mevzuat

4 Mevzuatımızda yer alan normları unutulma hakkı çerçevesinde değerlendirebilme

Anahtar Sözcükler: • İnsan Hakları • Üç Kuşak Haklar Teorisi • Dördüncü Kuşak Haklar • Unutulma Hakkı



GİRİŞ

Bilişim teknolojilerine her geçen gün yenilerinin eklenmesi ve bu teknolojiler nedeniyle yeni hukuki sorunların baş göstermesi, bilişim hukukunun güncel sorunlarının çok çeşitli olmasına neden olmaktadır. Bu hukuk dalının, örneğin yakın gelecekte birçok işletmenin son kullanıcıya bulut bilişim (cloud computing) hizmetlerini sunacak olması dolayısıyla, bu sistemlerde sözleşmenin kurulması, sözleşmenin sona ermesi, verilerin gizliliği, veri mülkiyeti, bulut bilişim sağlayıcısı ve alt hizmet sağlayıcılar arasında doğrudan doğruya veya dolaylı sorumluluk ilişkisinin belirlenmesi, bulut bilişimde saklanan verilerde adli soruşturma çerçevesinde yapılacak olan arama, kopyalama ve el koyma gibi güvenlik tedbirlerinde mevcut kanuni düzenlemelerin yeterli olup olmayacağı; yine benzersiz bir şekilde adreslenebilir nesnelerin kendi aralarında oluşturduğu, dünya çapında yaygın bir ağ ve bu ağdaki nesnelerin belirli bir protokol ile birbirleriyle iletişim içinde olmaları olarak tanımlanmakta olan nesnelerin interneti (internet of things) gibi konularla ilgilenmek zorunda kalacağı kesindir. Üzerinde tartışma yapmak için insanoğlunun bir nebze daha fazla zamanı olan bir diğer konu da, yapay zekanın (artificial intelligence) bilişim sistemlerinde yapmış olduğu işlemlerden doğan hukuki ve hatta cezai sorumluluğudur.

Bütün bu sayılan veya sayılamayan güncel sorunların tek bir ünitede açıklanması doğal olarak mümkün değildir. Bu ünitede bilişim hukukunun nihayetinde bir hukuk dalı olması ve her hukuk dalının olduğu gibi, bu hukuk dalının da insan hakları ile bağlantılarının bulunması nedeniyle, insan hakları teorisi ve bu teori ile ilgilenen hukukçuların bilişim sistemleri karşısında nasıl hareket ettikleri "unutulma hakkı" örneği üzerinden anlatılacaktır. Ancak bunun için öncelikle insan hakları teorisine ilişkin bazı açıklamaların yapılması gereklidir.

İNSAN HAKLARI TEORİSİNE İLİŞKİN TEMEL BİLGİLER

İnsan Hakları Evrensel Beyannamesi (İHEB), İnsan Hakları Avrupa Sözleşmesi (İHAS), Avrupa Birliği Temel Haklar Bildirgesi (ABTHB) ve Türkiye Cumhuriyeti Anayasası gibi insan haklarına yer veren metinlerde, insan hakları, kişinin sırf insan olduğu için sahip olduğu haklar olarak kabul edilmektedir. Anayasa'nın 12. maddesi "herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez haklara sahiptir" diyerek bu hakların niteliğini açıklamıştır. İnsan hakları teorilerini "Üç Kuşak Haklar Teorisi" ve "Dördüncü Kuşak Haklar" olmak üzere iki kısmıda inceleyebiliriz.

Üç Kuşak Haklar Teorisi

İnsan hakları öğretisinin oluşmaya başladığı tarihten bu yana, insan haklarını sayan ve sınıflandıran çok sayıda liste ortaya çıkmıştır. Bu sınıflandırmalardan en ünlüsü Karel Vasak tarafından ortaya konan "üç kuşak haklar" teorisidir; zira bu sınıflandırma, insan hakları öğretisinin tarihsel gelişimi ile paralellik gösterdiği gibi bilişim çağının gereksinimlere göre dördüncü kuşak haklara ilişkin tartışmalara da olanak tanımaktadır. Karel Vasak'a göre birinci kuşak hakların temel özelliği, kişilere, devletin karışmayacağı özel bir alan yaratmasıdır. Bu haklar, kişileri devlete karşı korur; devlete kişilerin özel alanına girmeme, karışmama yükümlülüğü getirir. Birinci kuşak haklar, kişi haklarını yani medeni hakları ve siyasal hakları içerir. Bunlara örnek olarak, yaşam hakkı ve kişi dokunulmazlığı, kişi özgürlüğü ve kişi güvenliği, düşünce ve düşünceyi açıklama özgürlüğü, inanç ve ibadet özgürlüğü, konut dokunulmazlığı hakkı verilebilir. İkinci kuşak haklar ise, devlete karışmama ödevi değil, aksine eylemde bulunma, harekete geçme yani hizmet sağlama ödevi yüklemektedir. Bunlar genellikle sosyal haklar olarak adlandırılmaktadır. Bunlara örnek olarak toplu sözleşme hakkı, dinlenme hakkı, sosyal güvenlik hakkı, sağlık hakkı, korunmaya muhtaç toplumsal sınıfların (yaşlılar, engelliler, çocuklar vs.) korunmasına yönelik haklar verilebilir. Üçüncü kuşak haklar ise ilk iki kuşak haklardan farklı olarak belirli bir grubun değil, bir toplumdaki tüm sosyal grupların ihtiyaçlarına cevap vermeyi amaçlayan haklardır. Zira örneğin çevre kirliliğinin korkunç boyutlara ulaşması, nükleer silahların tüm insanlığı yok edecek bir savaş tehlikesine yol açması, tüm sosyal grupları ilgilendirir ve çevrenin korunması, barışın sağlanması gibi amaçlar ancak tüm sosyal grupların dayanışması ile olur. Bu nedenle üçüncü kuşak haklara dayanışma hakları da denilmektedir. Bunlara örnek olarak çevre hakkı, gelişme hakkı, insanlığın ortak mal varlığına saygı hakkı, tüketici hakları verilmektedir.

Birinci ve ikinci kuşakta yer alan hakların insan hakkı kabul edilmesi hususunda tartışma yaşanmamaktadır. Buna karşın üçüncü kuşakta yer alan hakların gerçekten insan hakkı olarak kabul edilip edilmeyeceği hususunda farklı görüşler mevcuttur. Bazı hukukçular, üçüncü kuşak hakların henüz anayasalara veya uluslararası sözleşmelere girebilecek derecede iyi formüle edilmediğinden hareketle bunların insan hakkı olarak değerlendirilemeyeceğini belirtmektedirler. Zira klasik anlayışa göre bir hakkın hukuk normu olarak düzenlenebilmesi için hakkın konusunun, hakkın öznesinin ve hakkın yükümlüsünün net olarak ifade edilebilir olması gerekmektedir. Birinci ve ikinci kuşak haklarda hak ve ödevin süjeleri birbirinden ayrılır. Oysa üçüncü kuşak haklarda hak ve ödev birbirinden kolaylıkla ayrılmaz; keza kim hak sahibi, kim ödev sahibi kolayca tespit edilmez. Örneğin bir kişi çevre konusunda hem hak hem de ödev sahibidir. Yani aynı kişi hem sağlıklı çevrede yaşama hakkına sahiptir hem de bu kişi çevreyi kirletmeme ve koruma ödevi altında bulunur. Nihayet üçüncü kuşakta yer aldığı söylenen bazı haklar şu ya da bu şekilde diğer kuşak haklardan türer veya onların mantıki uzantısıdır veya en azından onlarla ilgilidir. Örneğin üçüncü kuşak olduğu söylenen bilgi edinme hakkı, aslında düşünceyi açıklama hürriyetinin bir uzantısıdır (Gözler, 2017: 160).

Bu eleştiriler de kesinlikle haklılık payı mevcuttur. Bununla birlikte, insan haklarının her zaman yürürlükteki hukukun önünde koştuğu ve hukukun da ona ayak uydurduğu gerçeği unutulmamalıdır. Yakın zamanlarda üçüncü kuşak insan hakları bağlamında tartışılan "*internete erişim hakkı*" bu duruma güzel bir örnektir; zira bu hak, hukukun bilişim çağında toplumsal dönüşümlere cevap vermesi zorunluluğu karşısında, uygarlığın gelişmesiyle ortaya çıkan nimetlerden herkesin, her topluluğun eşit ve dengeli biçimde faydalanmasını amaçlayan gelişme hakkının özel bir görünümü ya da Anayasa'nın 5. ve 17. maddelerinde güvence altına alınan insanın maddi ve manevi varlığının gelişiminin bir parçası olarak kabul edilebilecekken, kendi başına ayrı bir hak olarak kabul edilmiştir.

dikkat

İnternete erişim hakkı üçüncü kuşak haklar arasında kabul edilmektedir.

Gerçekten de internete erişim hakkının ülke anayasalarında yer almasını teklif eden birçok önemli metin bulunmaktadır. Ülkemiz açısından bunlardan en önemlisi Birleşmiş Milletlerin 2011 yılında internet erişimini temel insan hakkı olarak tanımladığı raporudur. Bu rapora göre "internet diğer insan haklarını destekleyen bir araç haline gelmiştir. İnternetin benzersiz ve dönüştürücü doğası, sadece bireylere düşünceyi açıklama özgürlüğünü sağlamakla kalmıyor, bunun yanında toplumun bütün olarak gelişmesini sağlayacak diğer insan haklarını da destekliyor. İnternet bir dizi insan hakkını destekleyen, gelişmeleri hızlandıran önemli bir araç haline gelmiştir. Bu nedenle internette global erişimi sağlamak bütün devletlerin en önemli önceliği olmalı ve her devlet internetin uygun fiyatlarla, geniş bir şekilde var olmasını, kullanımını temin edecek anlamlı ve güçlü bir yasal ortamı geliştirmelidir". Türkiye de bu rapor doğrultusunda hazırlıklar yapmaya başlamıştır. Örneğin hazırlanan taslak maddeye göre "herkes, bilgiye, internete ve diğer elektronik iletişim ortamlarına serbest erişim hakkına sahiptir. Devlet bu hakkın etkin ve adil biçimde kullanılabilmesi için gerekli düzenlemeyi yapar. İnternet aracılığı ile yapılan haberleşmenin gizliliği esastır. Herkes internet aracılığıyla paylaştığı kişisel verilerin korunmasını, düşünce ve kanaatlerin gizliliğine saygı gösterilmesini isteme hakkına sahiptir." Bu veya benzeri bir metnin yakın gelecekte Anayasa'da yer alması hiç de şaşırtıcı olmayacaktır (Gören, 2014: 22).

Dördüncü Kuşak Haklar

Bilişim teknolojisindeki gelişmeler sayesinde, kişilerin kişisel bilgilerini, görüntülerini, konuşmalarını, kişiler hakkında çıkan haberleri, söylentileri ve diğer birçok bilgiyi elde etme, saklama ve istenildiğinde bunlara anında ulaşma imkânı ortaya çıkmıştır. Bu veriler sayesinde kişinin faaliyetleri günün her saatinde izlenebilmekte, kişilik analizi yapılabilmekte, her türlü alışkanlığı öğrenilebilmektedir. Bu tür verilerin bir kısmının sağlık ve güvenlik gibi değerli amaçlar için saklanması ve kullanılmasında kuşkusuz kişisel ve toplumsal yarar bulunmaktadır. Ancak bu verilerin kişi özgürlüğünü ve mahremiyetini ihlal edecek biçimde kullanılma olasılığı da çok yüksektir (Gözler, 2017: 161; Uygun, 2014: 570). Bundan dolayı son yıllarda dördüncü kuşak insan haklarından bahsedilmektedir. Bunlar bilişim teknolojisinde yaşanan gelişmelerin insan onurunun korunması bakımından yarattığı riskler nedeniyle ortaya çıkmıştır. Bu bağlamda, dördüncü kuşak hakların bilimin ve teknolojinin olası kötüye kullanımına karşı insan onurunun korunması amacına dayan-

dığı kabul edilmektedir. Diğer bir ifadeyle bilişim teknolojisinin günümüzde eriştiği düzeyin ortaya çıkardığı, insan onurunu tehdit eden yeni tehlikelere karşı yeni hakların güvence altına alınması ve/veya mevcut hakların yeni durumları kapsayacak biçimde ek güvencelerle desteklenmesi dördüncü kuşak hakların tanınmasının temel nedenidir (Uygun, 2014: 568).

Bu noktada Anayasa'nın "Devletin Temel Amaç ve Görevleri" başlıklı 5. maddesi önemlidir. Bu maddeye göre, devletin temel amaç ve görevi insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaktır. Yine Anayasa madde 17'ye göre herkes maddi ve manevi varlığını geliştirme hakkına sahiptir. Dolaysıyla dördüncü kuşak hakların tanınmasının ve korunmasının devlete Anayasa tarafından verilen bir görev olduğunu belirtmek abartılı olmayacaktır. Nitekim yakın tarihimizdeki anayasa değişiklikleri de bunu destekler niteliktedir; zira 2010 Anayasa Referandumu ile kabul edilen 2010 değişikliğiyle, dördüncü kuşak haklardan biri olarak kabul edilen kişisel verilerin korunması hakkı, ülkemizde de anayasal güvenceye bağlanmıştır. Anayasa m. 20/3: "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."

Bölümün bundan sonraki kısımlarında dördüncü kuşak haklardan kabul edilen bir başka hak olan unutulma hakkı (right to be forgotten/Recht auf Vergessenwerden) etraflıca incelenecektir. Hemen belirtilmelidir ki, unutulma hakkı kişisel verilerin korunması hakkı ile yakından bağlantılıdır. Nitekim unutulma hakkının yeni bir şey olmadığı düşüncesinde olanlar, bu hakkı; kişinin kendisine ait veriye erişebilmesi, verinin düzeltilmesini isteyebilme, yasal dayanağı bulunmayan kişisel verilerin işlenmesine itiraz edebilme gibi kişisel verilerin korunması hakkına ilişkin prensiplerin yeniden gruplandırılması, nitelendirilmesi olarak görmektedirler (Akgül, 2015: 14).

dikkat

Unutulma hakkı dördüncü kuşak insan haklarından kabul edilmektedir.

Bu düşünce de haklılık payı vardır. Zira her iki hakkın özünde, bireyin onurlu yaşaması, kişiliğini serbestçe geliştirmesi ve kişisel verileri üzerinde özgürce tasarruf etmesi yatmaktadır. Ancak gerek Avrupa Birliği Adalet Divanı'nın (ABAD, Court of Justice of the European Union/CJEU, Europäischer Gerichtshof/EuGH) gerekse Türk yargı sisteminin en tepesinde yer alan Anayasa Mahkemesi'nin (AYM) gerekse de Yargıtay Hukuk Genel Kurulu'nun (HGK) yeni tarihli kararlarında unutulma hakkını açıkça zikretmesi, söz konusu hakkın kişisel verilerin korunması hakkıyla ilişkili ama son tahlilde ondan ayrı ele alınmasını mümkün kılan hukuki zemini oluşturmuştur.

Öğrenme Çıktısı

1 İnternete erişim hakkını insan hakları teorisi çerçevesinde açıklayabilme ve dördüncü kuşak insan haklarını tanımlayabilme

Araştır 1	İlişkilendir	Anlat/Paylaş
Dördüncü kuşak insan haklarının ortaya çıkış nedenini açıklayınız ve bilişim hukuku çerçevesinde hangi insan haklarının dördüncü kuşak insan haklarından sayılabileceğini belirtiniz.	İnternete erişim hakkını üç kuşak haklar teorisi çerçevesinde açıklayınız.	Bilişim teknolojilerindeki gelişmelerin insan hakları teorisini nasıl etkilediğini anlatınız.

UNUTULMA HAKKI

Unutulma hakkı, bireyin dijital hafızada yer alan kişisel verilerinin kendi talebi üzerine bir daha geri getirilemeyecek şekilde ortadan kaldırılması şeklinde tanımlanmaktadır. Dijital dünyada kişilerin haklarında yer alan rahatsız edici içerikleri veya üzerinde hak sahibi oldukları kişisel verileri silme, daha fazla yayılmasını önleme hakkı veren unutulma hakkı; genel olarak bireyin üçüncü kişilerin elinde bulunan kişisel verilerini kontrol etme ve bunları silme ve/veya sildirme hakkı olarak ifade edilir. Bu hak yoluyla birey kişisel verilerinin üçüncü kişiler tarafından artık izlenmemesini, görüntülenmemesini, indirilmemesini, kayıt edilmemesini ve benzeri diğer şeylerin verileri üzerinde yapılmamasını amaçlamaktadır (Akgül, 2015: 16). Diğer bir ifadeyle unutulma hakkı, gündemde olmayan, yani güncellik taşımayan bir haber veya resimden dolayı kişilik hakları sürekli ihlal edilen ya da kişilik haklarının ihlal edilmesine yönelik somut tehlike ile karşı karşıya kalan bireylerin, gerçeklik taşısa bile güncel olmayan haber, fotoğraf ve görüntülerinin yer aldığı linklere erişimin engellenmesi ve/veya içeriğin kaldırılması yoluyla kişilik haklarının korunmasıdır.

> Unutulma hakkı, üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olayların bir süre sonra unutulmasını, başkaları tarafından bilinmesi istenmeyen bilgilerin silinmesini isteme hakkı olarak ifade edilmektedir.

Unutulma hakkının gerekçesine dair yaklaşımlar farklılık göstermekle birlikte, bu konuda üç temel anlayıştan bahsedilmektedir: (1) Kişisel verilerin belirli bir süre geçtikten sonra silinmesi gerektiği temelinden hareket eden görüş; (2) "Beyaz sayfa" yaklaşımından yola çıkan ve eski tarihli olumsuz bilgilerin kişilere karşı kullanılmaması gerektiğini savunan sosyal perspektifli görüş; (3) Yine beyaz sayfa temelinden hareket eden, fakat bireyin kendini geliştirme hakkını temel alan ve böylece kişilerin geçmişlerinden endişe etmeksizin kendilerini ifade edebilmeleri gerektiğini savunan görüş (Önok, 2017: 7738).

Unutulma hakkına neden ihtiyaç duyulduğu ortadadır: internetin olmadığı zamanlarda bir kişi hakkında çıkan haber günlük gazetede yayınlanır, haberin yayınlandığı gün birçok kişi bu haberi okur; ancak daha sonra haber içeriği gazete kâğıdı ile birlikte bir kenara bırakıldığı an unutulurdu. Bu dönem unutmak/unutulmak esas, hatırlamak/hatırlanmak ise istisnaydı. İnternet istisnayı esas yaptı. Bugün Google aracılığıyla arama motorunda arama yapan herkes, bir başkası hakkında yıllar önce yayınlanan bir habere, yıllar sonra birkaç saniye içinde ulaşmaktadır.

Bu durum dördüncü kuşak hakların tanınmasına dair ortaya konan felsefenin doğruluğunu teyit etmektedir. Bilişim çağında veriler bir kere paylaşılmakla kayıt altına alınmakta, bireyin unutmak istediği anıları, fotoğrafları diğer internet süjeleri tarafından kullanılmakta ve bireylerin kişisel verileri deyim yerindeyse ifşa olmaktadır. İşte her türlü kişisel verinin sınırsız biçimde kayıt altına alındığı ve bu verilerin bir kere kayıt altına alınmasından sonra hızlı ve geniş paylaşım nedeniyle ortadan kaldırılmasının oldukça zor olduğu günümüz teknolojisinde, bireyin üçüncü kişilerin gözetiminden kurtulma ve dolayısıyla yaşamını özgür biçimde sürdürebilme isteği unutulma hakkına olan ihtiyacı ortaya çıkarmaktadır (Akgül, 2015: 15; Elmalıca, 2016: 1611). Böyle bir ihtiyaca hukuk düzeninin cevap vermesi zorunludur; zira kişisel verilerin kişinin rızası dışında yayılması sonucunda kişinin insanca yaşama hakkı, kişinin maddi ve manevi varlığını geliştirme hakkı gibi çok önemli bazı temel hak ve özgürlükleri doğrudan etkilenmektedir. Dolayısıyla unutulma hakkına, insan hakkı kavramının en temel düşüncesi olan insan onuru açısından bakmak gerekmektedir. Bu hakkın tanınmasının altında yatan en önemli faktör, birey hakkında internette veya sosyal medyada yer alan rahatsız edici bir bilginin onun şeref ve onuru ile yaşamını tamamen yok etme potansiyelinin bulunmasıdır.

Öyleyse bireylerin hayatlarında yeni bir sayfa açma hakkı bulunduğunun kabulü, unutulma hakkının çıkış noktasıdır. Sırf haber gerçek diyerek güncelliğini kaybettiği veya haber değerini yitirdiği bir dönemden sonra, habere konu kişinin, ailesinin ve çevresinin sürekli toplumsal dışlamaya tabi tutulması yani geçmişindeki hatadan dolayı sürekli hedef alınması doğru değildir. Böylesi bir durum devletin koruma yükümlülüğü ile de çelişmekte-

dir. Bir kişi hakkında kamu davası açılıp hakkında mahkûmiyet kararı verilse ve bu karar kesinleşse dahi, mevzuat gereği karar sadece belli kişilerin görebileceği adli sicil kaydı arşivine alınmaktadır. Bu arşivdeki bilgiler dahi belli bir süre silinmektedir. Tek başına bu bile unutulma hakkının kabul edilmesi gerekliliğinin altını çizmekle kalmayıp; gazetelerin, haber portallarının, sosyal medya paylaşımlarının adli haberleri, yorumları, fotoğrafları denetimsiz ve süresiz yayınlamasının, bireylerin yeniden topluma kazandırılması düşüncesiyle çeliştiğini ortaya koymaktadır. İnternetin doğası gereği sahip olduğu özgürlüğünün, masumiyet karinesi karşısında sınırsız ve denetimsiz şekilde kullanılamayacağını yukarıdaki açıklamalardan sonra belirtmeye gerek dahi yoktur. Bir soruşturma kapsamında gözaltına alınan, tutuklanan kişi beraat edip masumiyetini kanıtlasa bile, hakkındaki haberler internet ortamında yer almaya devam ettiği sürece toplumun gözünde sürekli olarak suçlu ilan edilebilecektir. İnternet ortamında yayınlanan haberler sadece yargılan kişilerin değil, suçtan zarar görenlerin de mağduriyetlerine neden olabilmektedir. Örneğin aile içi şiddet veya cinsel suç mağduru kişi hakkında yayınlanan haber, olayın üzerinden yıllar geçmesine rağmen yayınlanmaya devam etmekte ve mağdurun psikolojisi üzerinde yıkıcı etki yaratan bu olayın izlerinin silinmesi mümkün olmamaktadır (Şen, 2016). Bu itibarla unutulma hakkına, bireye, hayatının önceki aşamalarında yaşadıkları nedeniyle engellenen sosyal ve ekonomik yaşamını yeniden şekillendirmesini sağlayan yani bireye rızasına aykırı olarak internet ortamında uzunca bir süre ve gereksiz biçimde yer alan verilerin silinmesi yoluyla yaşamına yeni bir başlangıç yapma fırsatı sağlayan bir hak olarak bakmak doğru olacaktır.

Unutulma Hakkının Pozitif ve Negatif Yönü

Unutulma hakkı pozitif ve negatif olmak üzere iki yönlüdür. Unutulma hakkı, kişisel veriler üzerindeki tasarruf hakkının bir uzantısı olması yönüyle pozitif bir hak içermektedir. Bu yönüyle unutulma hakkı ile bir kişinin kendisi hakkındaki bilgilerin kapsamlı ve geniş biçimde silinmesini talep edebileceği kabul edilmektedir. Söz konusu kişisel verilerin içeriği doğru olabileceği gibi yayınlamanın yasal dayanağı bulunabilir veya üçüncü kişi tarafından yayınlanmış olabilir. Bu hakkın; bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlamayı içermesinin yanında geçmişteki cezalarına ilişkin bilgilerin veya haklarında olumsuz yorumlara neden olabilecek bilgi ve fotoğraflarının kaldırılmasını isteme hakkını tanıdığı kabul edilmektedir. Unutulma hakkının negatif yönü ise bireylerin rahatsız edici bulduğu kişisel verilerin geleceklerini olumsuz etkilememesi için, bu verilerin bir daha geri getirilemeyecek biçimde ortandan kaldırılmasını isteyebilmeleri olarak tanımlanmaktadır. Dolayısıyla bu hak bireyin geçmişiyle ilgili belirli verilerin hatırlanmaması için önlemler alınmasını da içermektedir. Bireyin unutulma hakkı yönündeki talebi sonrasında verinin kontrolünden sorumlu kişinin veriyi silme veya yok etme yükümlülüğü bulunmaktadır. Bu verilerin kullanımının ve işleme konulmasının ifade özgürlüğü kapsamında görülmesi, hukuki zorunluluk olması veya kamu yararının bulunması hallerinde veriyi kontrol edenin bu talebi reddetme hakkı vardır (Akgül, 2015: 18).

Unutulma Hakkının Diğer Temel Hak ve Özgürlükler ile Çatışması

Unutulma hakkının pek çok başka hak ile ilişkisi mevcuttur. Bu ilişki kimi zaman kişisel verilerin korunması hakkında olduğu gibi kesişme ve birbirini tamamlama şeklindedir, kimi zaman ise haberleşme ve ifade özgürlüğü, iletişim özgürlüğü, basın hürriyetinde olduğu gibi çatışma şeklinde kendini gösterir. Öyleyse haberleşme ve ifade özgürlüğü, iletişim özgürlüğü, basın hürriyeti ile unutulma hakkı arasında adil bir dengenin kurulması gerektiği kuşkusuzdur. Ancak kamu için hayati önem taşıyan bir bilgi dışında, bireyin rızasına aykırı olarak kişisel verilerinin uzun süre internet ortamında yer alması haberleşme özgürlüğü ve ifade özgürlüğü çerçevesinde kabul edilemez. Aksi durumun bireyin hayatını özgür ve serbest biçimde sürdürememesine neden olacağı açıktır (Akgül, 2015: 23).

Daha basit ifade etmek gerekirse, elbette demokratik hukuk toplumunda bilgiye ulaşabilirlik, kamuoyunun ilgisini çeken bilgilerin üstünün örtülmemesi, ifade özgürlüğü, haber alma ve verme hakkı ve daha birçok başka temel hak ve özgürlükler açısından zorunludur. Ancak bazı durumlarda bu temel hak ve özgürlüklerin, bireyin sahip olduğu haklar karşısında sınırlanması gerekebilir. Gerçekten de her ne kadar bireyin kendisi hakkında ger-

çek, güncel, kamuoyunun ilgisini çeken, sebep ve sonuç ilişkisi bulunan bilgi, yorum ve hatta eleştiri olarak kamuoyuna aktarılan haber ve görüntülere tahammül etme zorunluluğu bulunsa da, böylesi bir zorunluluğun, haberin güncelliğini kaybetmesi sonucu internette yer alan bilgilerin haber değerini yitirmesinden itibaren devam etmesini beklemek mümkün değildir. Elbette ki bu söylenenleri kamuoyunun ilgisini çeken kişi ve olaylar ile önemi açısından toplumsal güncelliğini hiçbir zaman kaybetmeyen olaylar ve onun aktörleri bakımından farklı değerlendirmek mümkündür. Örneğin doping yapan sporcu haberi, haber gerçek olduğu sürece güncelliğini korur; fakat aynı sporcunun bir kavgaya karıştığına yönelik haber, haber gerçek olsa dahi, güncelliğini çabuk yitirir (Şen, 2016).

Unutulma hakkı ile bu hakkın çatıştığı diğer haklar arasındaki ilişki şu şekilde özetlenebilir: Kamu yararı ile birey yararı arasındaki denge, ilk bakışta güncellik, görünür gerçeklik, kamuoyu ilgisi sebebiyle haber, fotoğraf ve görüntülerin üçüncü kişilerin bilgisine sunulması lehine kurulduğu halde; unutulma hakkı sayesinde bu bilgilerin güncelliğini yitirdiği andan itibaren denge bu defa birey lehine değişmektedir. Öyleyse unutulma hakkı, üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olayların bir süre sonra unutulmasını, başkaları tarafından bilinmesi istenmeyen bilgilerin silinmesini isteme hakkı olarak ifade edilebilir. Böylece her bilginin ebediyen hatırlanabileceği sanal dünya bakımından bireyin kendine ait veriler üzerinde kontrol hakkı sağlanmaktadır.

Unutulma Hakkının Normatif Dayanağı

Unutulma hakkı, 14.04.2016 tarihinde Avrupa Parlamentosu tarafından onaylanan ve 04.05.2016 tarihinde Avrupa Birliği Resmi Gazetesi'nde yayınlanan ve 25.05.2018 tarihinde yürürlüğe girecek olan 2016/679/EU sayılı "Gerçek Kişilere Dair Kişisel Verilerin İşlenmesine ve 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktifin Kaldırılmasına Dair Regülasyon"a ya da bilinen adıyla Genel Veri Koruma Regülasyonu'na (Generel Data Protection Regulation/GDPR) kadar, çeşitli uluslararası sözleşmeler ve/veya Avrupa Birliği'nin 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif" kapsamında ve kişisel verilerin korunması hakkı çerçevesinde incelenmekteydi. Diğer bir ifadeyle unutulma hakkı yakın bir zamana kadar normatif dayanağı olmayan; ABAD, AYM ve HGK gibi yüksek yargı organlarının içtihatlarıyla insan hakları teorisine kazandırılmış bir haktır.

2016/679/EU sayılı Regülasyon'a http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679; 95/46/EC sayılı Direktif'e ise http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 adresinden ulaşılabilmektedir.

Unutulma hakkının yazılı metinlerde yer almasına dair çalışmalar Avrupa Birliği (AB) Komisyonu'nun, 95/46/EC sayılı Direktifin yeniden gözden geçirilmesi yönündeki önerisinin ardından başlamıştır. Komisyon, 2010 yılının Kasım ayında unutulma hakkının kabul edilmesini önermiştir.

Hemen belirtilmelidir ki 95/46/EC sayılı Direktifin gözden geçirilmesine neden olan husus tek başına unutulma hakkına dair yapılan tartışmalar değildir. Her ne kadar 95/46/EC sayılı Direktif kişisel verilerin korunması hususunda, sadece AB coğrafyasında sınırlı kalmayarak, genel bir anlayışın oluşmasına katkı sağlamışsa da akıllı telefonlar, sosyal medya, bulut bilişim gibi bilgi ve iletişim teknolojilerinde 1995 yılından bu yana meydana gelen değişikliklerin ve başlı başına küreselleşmenin bazı yenilikleri zorunlu kıldığı AB yetkilileri tarafından kabul edilmekteydi. Yine benzer şekilde üye ülkelerin Direktife istinaden hazırladıkları kişisel verilerin korunmasına dair yasalarda ve bu yasaların uygulanmasında bazı farklılıkların bulunduğu gözlemlenmekteydi. Ayrıca koruma düzeyinin ülkeden ülkeye farklılık oluşturması, veri koruması düzeyi daha düşük AB üyesi ülkeler üzerinden veri transferlerinin gerçekleştirilmesine neden olmakta, bu fiili durum ise ortak pazar bakımından önemli bir sorun oluşturmaktaydı (Başalp, 2015: 82).

Bunlar dışında bazı siyasi olaylarda söz konusu Direktifin gözden geçirilmesine sebebiyet vermiştir. Bu olayların başında, konuyla doğrudan olmasa da etkisi bakımından büyük ilgisi olan, 2013 yılında Edward Snowden tarafından ortaya çıkarılan mahremiyet ihlalleri gelmektedir. Söz konusu olayda başta Google, Facebook, Apple ve diğer büyük (ABD merkezli) internet aktörlerinin kullanıcıları olmak üzere milyonlarca kullanıcının erişim bilgileri de dahil pek çok kişisel verisi Ulusal Güvenlik Ajansı'nın (National Security Agency-NSA) geniş kapsamlı ve derinlikli gözetimlerine konu olmuştur. Bu somut gelişmeler Avrupa Birliği Adalet Divanı'nın (ABAD) bir dizi özgün karara imza atmasına neden olmuştur (Akıncı, 2017: 11). Bu kapsamda ABAD'ın dönüm noktası sayılan kararları, biraz sonra etraflıca incelenecek olan "Google/Unutulma Hakkı" kararı dışında, şu şekilde sayılabilir:

İrlanda Dijital Haklar Kararı: ABAD bu kararında 2006/24/EC sayılı Veri Saklama Direktifini geçersiz ilan etmiştir. Bu Direktif sabit, mobil veya internet telefonu ile e-posta iletişimi verilerinin altı aydan iki yıla kadar saklanmasını düzenlemektedir. Direktif ile söz konusu kişisel verilerin her üye devlet tarafından muhtemel bir soruşturma, araştırma ve kovuşturma da kullanılabilmesi veya kullanılabilmesi için hazır tutulması amaçlanmıştır. Ancak söz konusu veri saklama faaliyetinin makul suç şüphesi bulunmasına gerek olmaksızın yapılması ve üye devletlerin anayasal düzenlemeleri başta olmak üzere pek çok hukuki gereklilik ile çelişmesi, bahse konu Direktifin yoğun tartışmalara yol açmasına sebep olmuştur. Bu tartışmalar ABAD'ın Direktifi geçersiz ilan eden kararıyla nihayete ermiştir (ABAD, 08.04.2014 – C-293/12 ve C-594/12).

M.Schrems-Veri Koruma Komisyonu Kararı: Veri koruma kurallarına ilişkin temel yaklaşımda ve pek çok hukuki düzenlemede değişikliğe gidilmesi zorunluluğunu doğuran bir diğer önemli ABAD kararı ise 6 Ekim 2015 tarihinde verilen "Schrems Kararı"dır. Davacı Maximillian Schrems Avusturya vatandaşı olup söz konusu olayda İrlanda Veri Koruma Otoritesini dava etmiştir. Dava konusu uyuşmazlık Schrems'in daha önce, Facebook tarafından kişisel verilerinin ABD'de tutulmasının kendisi bakımından ihlale sebep olduğu gerekçesiyle yapmış olduğu başvurusunun İrlanda Veri Koruma Otoritesi tarafından reddedilmesi üzerine meydana gelmiştir. AB ve ABD arasındaki "Güvenli Liman Anlaşması" (Safe Harbour) kapsamında eşdeğer bir koruma seviyesinin bulunmasının zorunlu olmasına rağmen, bir süredir tartışmalara sebep olan NSA gözetimleri de dikkate alındığında ABD tarafından Schrems'in kişisel verilerinin AB için gerekli olan güvence şartları kapsamında korunmadığı iddia edilmiştir. ABAD yaptığı incelemede, Komisyonun üçüncü bir ülkeyi yeterli koruma düzeyini sağlar bulmasının ulusal veri koruma otoritelerinin Veri Koruma Direktifi kapsamında inceleme ve denetleme yapma gücünü azaltmaması gerektiğini, Güvenli Liman Anlaşması'nın yalnızca ABD şirketleri bakımından bağlayıcı olduğunu buna karşın kamu otoritelerini bağlamayacağını belirtmiştir. Mahkeme, ABD hukuk kurallarının incelenmesi sonucunda, AB vatandaşlarının başta kişisel verileri olmak üzere temel hakları bakımından tehlikeli sonuçların ortaya çıkabileceğini değerlendirmiş ve Güvenli Liman Anlaşması'nı geçersiz ilan etmiştir (ABAD, 06.10.2015 – C-362/14).

Veri korumasında ortak bir anlayışa ve uygulamaya ulaşmak üzere AB yasama süreçleri içerisinde AB'nin önünde iki seçenek bulunmaktaydı: Birincisi 95/46/EC sayılı Direktif gibi, üye devletleri hedef alan ve onlara belirli bir süre içinde direktifte belirtilen hususlarda ulusal hukukta düzenlemeler yapma ödevi yükleyen ve genel olarak ulusal hukukların birbirleriyle uyumlaştırılmalarına hizmet eden yeni bir direktifin yapılmasıydı; diğeri ise, yürürlüğe girmekle birlikte tüm üye ülkelerde yürürlük gücüne sahip olan ve dolayısıyla iç hukuka aktarılmak üzere bir onay kanununa ya da iç hukukta yapılacak başka düzenlemelere ihtiyaç duymayan ve böylece düzenlediği alanda tüm AB sınırları içinde yeknesak hükümlerin uygulanmasına olanak veren bir regülasyonun yapılmasıydı.

Avrupa Birliği, suçun önlenmesi, soruşturulması ve kovuşturulması noktasında 2016/680 sayılı "2008/977/JHA Çerçeve Kararı Yürürlükten Kaldıran, Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti Veya Kovuşturulması Veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin Korunmasına Ve Bu Tür Verilerin Serbest Dolaşımına

Dair Direktif" ile birinci, kişisel verilerin korunmasına ilişkin diğer hususlarda ise ikinci yolu seçmiştir. İşte, sadece 95/46/EC sayılı Direktif'i değil, aynı zamanda AB üyesi ülkelerdeki ulusal veri koruma kanunlarını da ikame eden 2016/679/EU sayılı "Gerçek Kişilere Dair Kişisel Verilerin İşlenmesine ve 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktifin Kaldırılmasına Dair Regülasyon" bu arka planla yürürlüğe konulmuştur.

Bu Regülasyonun hedefleri şu şekilde ifade edilmiştir: Özellikle küreselleşmeden kaynaklanan zorluklar ve yeni teknolojilerin kullanımı karşısında kişisel verilerin etkili bir biçimde korunması amacıyla AB hukuk sisteminin iyileştirilmesi; kişisel veriler konusunda bireysel hakların güçlendirilmesi ve aynı zamanda AB içinde ve/veya dışında kişisel verilerin serbest akışının sağlanması için bürokratik süreçlerin azaltılması; kişisel verilerin korunmasına ilişkin AB hukuku kurallarına netlik ve tutarlılık kazandırılması; bu kuralların yine tutarlı ve etkin bir biçimde uygulanması ve Birliğin tüm faaliyet alanında kişisel verilerin etkin bir biçimde korunması (Akıncı, 2017: 13).

173 paragraflık resital bölümü (başlangıç bölümü) ile 99 maddeden oluşan Regülasyonun 17. maddesi unutulma hakkını düzenlemiştir. Bu madde de özetle veri öznesi/veri süjesi olan, yani kişisel verileri özel hukuk ya da idare hukuku çerçevesinde gerçek ya da tüzel kişiler tarafından toplanan, değerlendirilen, üzerinde çalışılan, aktarılan, kişilerin, verilerinin işlenmesine artık rıza göstermemesi, istememesi veya bu verilerin uzun zamandan bu yana işleniş amaçlarına uygun olarak kullanılmaması veyahut anılan verilerin artık işlenmesi ve tutulması için gerekli hukuka uygunluk koşullarının bulunmaması veya verilerin hukuka aykırı bir şekilde işlenmesi ya da veriyi işleyen kişilere herhangi bir hukuki sebepten dolayı (örneğin bir mahkeme kararı) bu veriyi kaldırma, silme gibi bir yükümlülüğün yüklenmesi halinde, kişisel verilerin silinmesini isteyebileceği düzenlenmiştir. Bunun yanı sıra kişisel verileri işleyen ve bu bilgileri kamuya açıklayan kişilere, yani verilerin silinmesinden sorumlu olan kişiye, bazı ek külfetler yüklenmesi de bu maddeye göre mümkündür. Buna göre bu kişiler talep konusu kişisel verilere bağlantı veren ya da bu verileri kopyalayan üçüncü kişilere de veri süjesinden gelen silme talebini, teknolojinin ve mali imkânların elverdiği ölçüde bildirmekle yükümlüdür. Aynı madde de unutulma hakkının icra edilmesinden imtina edilebileceği durumlar da düzenlenmiştir. İfade özgürlüğünün korunması ya da kamusal sağlığı ilgilendiren konularda kamu yararının olması koşuluyla unutulma hakkının icra edilmesinden veri sorumlusu imtina edebilir. Ayrıca tarihsel, istatistiksel ve bilimsel amaçların gerekli kıldığı durumlarda da bu yükümlülüğün icra edilmesinden imtina edebilecektir. Avrupa Birliği'nin veya üye devletlerinin mevzuatının gerekli kıldığı durumlarda da, veri sorumlusu söz konusu kişisel verileri saklama/tutma imkânına sahip kılınmaktadır.

Öğrenme Çıktısı

2 Unutulma hakkını genel olarak tanımlayabilme, bu hakkın normatif dayanağını belirtebilme ve diğer temel hak ve özgürlükler ile ilişkisini açıklayabilme

Araştır 2	İlişkilendir	Anlat/Paylaş
Unutulma hakkının normatif dayanağı nedir?	Bilişim teknolojilerindeki gelişmeler ile unutulma hakkı arasındaki ilişkiyi değerlendiriniz.	Unutulma hakkının normatif bir dayanağa kavuşturulmasını kişisel verilerin korunması hakkı çerçevesinde anlatınız.

UNUTULMA HAKKINA İLİŞKİN YARGI KARARLARI

Yukarıda da ifade edildiği üzere unutulma hakkı yakın bir zamana kadar normatif bir dayanağa sahip olmayan, yargı organlarının içtihatlarıyla insan hakları teorisine kazandırılmış bir haktır. Bölümün bundan sonraki kısımlarında unutulma hakkına ilişkin verilen içtihatlara yakından bakmak, hakkın ortaya çıkış sürecini anlamak ve çerçevesini belirlemek için gereklidir. Bu nedenle ilk olarak ABAD'ın Google/Unutulma Hakkı kararı, daha sonra AYM'nin Unutulma Hakkı/NBB-Bireysel Başvuru kararı ve son olarak da HGK'nun bir kararı incelenecektir.

ABAD'ın Google/Unutulma Hakkı Kararı

AB içerisinde en üst mahkeme olan ve AB hukukunun uygulanmasında son sözü söyleyen, böylece AB hukukunun, hukuki denetim, yorum, uyuşmazlık çözme, hukuk yaratma ve boşluk doldurma yollarıyla, AB içinde her yerde aynı şekilde yorumlanmasını sağlayan ABAD'ın kararları her ne kadar Türkiye için resmiyette bağlayıcı değilse de; Google/Unutulma Hakkı kararı bu hakla ilgili uluslararası alanda verilmiş ilk karardır. Karar 95/46/EC sayılı Direktifin yorumlanmasını esas almaktadır. Direktifin 2018 yılında yürürlükten kalkacak olması ve yerini 2016/679/EU sayılı Regülasyona bırakacak olması, kararın önemine zeval vermemektedir; zira Regülasyonun 17. maddesi bu kararda açıklanan temel ilkeler dikkate alınarak yazılmıştır. Yine 95/46/EC ile getirilen genel ilkeler bakımından Regülasyonla bir değişikliğin olmadığı da Regülasyonun resital bölümünde, yani başlangıç bölümünde ifade edilmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun, 95/46/EC sayılı Direktifin dikkate alınarak hazırlandığının da bu noktada altı çizilmelidir.

Öyleyse ABAD'ın Google/Unutulma Hakkı kararı, ülkemizi sadece aday ülke sıfatıyla değil, aynı zamanda 6698 sayılı Kanun'un yorumlanması bakımından da ilgilendirmektedir. Son olarak belirtilmelidir ki, ABAD kararının tam ve doğru olarak anlaşılması hem 6698 sayılı Kanun'da hem de Direktifte geçen bazı normatif düzenlemelerin bilinmesiyle mümkün olacaktır. Bundan dolayı Mahkeme'nin önüne gelen somut olay ve Mahkeme'nin gerekçesinin açıklanmasına geçilmeden önce bazı temel kavramların belirtilmesi yararlı olacaktır.

Yaşamla İlişkilendir

Unutulma Hakkına İlişkin N.B.B Kararı Basın Duyurusu

Anayasa Mahkemesi Genel Kurulu, 3/3/2016 tarihinde N.B.B. tarafından yapılan bireysel başvuruda (B. No: 2013/5653), Anayasa'nın 17. Maddesinde güvence altına alınan şeref ve itibarın korunması hakkının ihlal edildiğine karar vermiştir

Olaylar

Başvurucu, hakkında ulusal bir gazetenin internet arşivinde, uyuşturucu kullandığı için adli para cezasına hükmedildiğine ilişkin 1998 ve 1999 yıllarına ait yayımlanan toplam üç haberin internet yayınının kaldırılması amacıyla ilgili basın kuruluşuna 2/4/2013 tarihinde ihtarname göndermiştir. Anılan haber içeriklerinin iki gün içinde kaldırılmaması üzerine başvurucu, içeriklerin yayından kaldırılması talebiyle ilgili basın kuruluşu aleyhine 18/4/2013 tarihinde (kapatılan) İstanbul 36. Sulh Ceza Mahkemesine başvurmuş, Mahkeme 22/4/2013 tarihinde "talebe konu yazının güncelliğini yitirdiği, haber değerinin bulunmadığı, gündemde kalmasında kamu yararı bulunmadığı ve bu haliyle muhatabının özel hayatına ilişkin incitici ve örseleyici bir bilgi niteliğinde olduğu" gerekçesiyle talebin kabulüne karar vermiştir.

İtiraz üzerine, İstanbul 2. Asliye Ceza Mahkemesinin 28/5/2013 tarihli kararıyla Mahkemenin anılan kararının kaldırılmasına hükmedilmiş ve bu karar 21/6/2013 tarihinde başvurucu vekiline tebliğ edilmiştir.

Başvurucunun İddiaları

Başvurucu, adli para cezası ödemeye mahkûm edildiği olay ile ilgili olarak internet sitelerinde yer almaya devam eden haber içeriğinin yayından kaldırılması yönündeki taleplerinin yargısal makamlar tarafından reddedilmesi nedeniyle Anayasa'nın 12., 17., 20., 25., 26., 27. ve 32. maddelerinde güvence altına alınan haklarının ihlal edildiğini iddia etmiştir.

Mahkemenin Değerlendirmesi

Anayasa Mahkemesi bu iddia kapsamında özetle aşağıdaki değerlendirmeleri yapmıştır:

Mevcut olayda başvurucunun, haberlerin hâlen internette yer alması nedeniyle müdahale edilen şeref ve itibar hakkı ile içeriğin yayından çıkarılması hâlinde müdahale edilecek olan ifade ve basın özgürlükleri arasında adil bir denge kurulması gerekmektedir. Bu dengenin değerlendirilmesinde somut olay açısından gözönünde bulundurulması gereken önemli bir husus şeref ve itibarın korunması hakkı ve unutulma hakkı karşısında sadece ifade ve basın özgürlüklerinin değil ayrıca kişilerin haber ve fikirlere ulaşma özgürlüğünün de olduğudur. Anayasa Mahkemesi anılan hak ve özgürlükler arasında adil bir denge kurulup kurulmadığı hususundaki değerlendirmesini temel olarak yetkili yargı mercilerinin ortaya koyduğu gerekçe üzerinden yapmaktadır.

Unutulma hakkı, internet ortamında bir haberin uzun süredir kolayca ulaşılabilir olması nedeniyle kişinin şeref ve itibarının zedelenmesi durumunda gündeme gelmektedir. Bu hakkın amacı, internetin yaygınlaşması ve sağladığı imkânlar nedeniyle ifade ve basın özgürlükleri ile kişilerin manevi varlığının geliştirilmesi hakkı arasında gerekli hassas dengenin kurulmasını sağlamaktır. O hâlde bu yol, internet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır.

Somut olayda, başvurucunun şikâyetine konu olan haberler 1998 ve 1999 yıllarında yayımlanmıştır ve arşiv niteliğindedir. Gazete arşivi niteliğinde olan haberler açısından arşivin sadece dijital alanda tutulmadığı ve içerik sağlayıcı tarafından saklanabileceği açıktır. Özellikle ölçülülük ilkesi temelinde yapılacak bir değerlendirme ile internet ortamında haberi ulaşılabilir kılan kişisel verilerin silinerek erişimin engellenmesi gibi yöntemler gözetildiğinde internet ortamındaki arşiv niteliğindeki haberin tamamen silinmeden sonuca ulaşılabilmesi mümkündür. Bu bağlamda bilimsel araştırmalar açısından dijital haber arşivinin tamamen silinerek geçmişteki olayların yeniden yazılması sonucunu doğuracak nitelikte basın özgürlüğüne yönelik ciddi müdahalelerin ortaya çıkması önlenebilir.

Başvurucu hakkında internet ortamındaki arşivde muhafaza edilen ve kolaylıkla ulaşılabilir kılınan haberler, 1998 ve 1999 yılındaki ceza yargılamasına ilişkindir. Bu haberlerin gerçeğe aykırı olduğu ileri sürülmemiştir. Haberler başvurucunun uyuşturucu kullanırken yakalanması ve daha sonrasında yargılanması hakkındadır. Bu bağlamda haber konusunun, haberin arşivde kolaylıkla ulaşılabilir kılınması için gerekli bulunan toplumsal açıdan haber değerinin devam etmesi veya haberin geleceğe ışık tutacak niteliğe sahip olması özelliklerini taşıdığı söylenemez.

Başvuru tarihi itibarıyla söz konusu haberin yaklaşık on dört yıl önceki bir olaya ilişkin olduğu ve böylelikle güncelliğini yitirdiği açıktır. İstatistiki ve bilimsel amaçlar yönünden de yukarıda ifade edilen gerekçelerle bu bilgilere internet ortamında kolaylıkla ulaşılmayı gerekli kılan bir neden bulunmamaktadır. Bu bağlamda kamu yararı bakımından siyasi veya medyatik bir kişiliğe sahip olmayan başvurucu hakkında internet ortamında yayınlanan haberlerin kolaylıkla ulaşılabilirliğinin başvurucunun itibarını zedelediği açıktır.

Sonuç olarak başvurucu hakkında yapılan haberler unutulma hakkı kapsamında değerlendirilmesi gereken haberlerdir. İnternet ortamının sağladığı kolaylıklar gözetildiğinde başvurucunun şeref ve itibarının korunması için anılan habere erişimin engellenmesi gerekmektedir. Bu bağlamda erişiminin engellenmesine yönelik talebin reddedilmesiyle ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu söylenemez.

Açıklanan nedenlerle başvurucunun Anayasa'nın 17. maddesinde güvence altına alınan şeref ve itibarın korunması hakkının ihlal edildiğine karar verilmiştir.

Kaynak: Basın Duyurusu No: BB 37/16, 24.08.2016.

Temel Kavramlar

Kişisel veri: Kişisel veri kavramı, İngilizce "personal data" kavramından gelmekte olup, doğrudan ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgiyi kapsamaktadır (6698 s.K. m. 3/d; Direktif m. 2/a). Görüldüğü üzere kişisel verilerin mutlaka gizli olması zorunlu olmayıp, herkes tarafından bilinen kişisel veriler de koruma altındadır; zira kişisel verilerin korunması hukukunun amacı bir bilginin gizliliğini değil, verinin ilgilisi olan kişinin kişilik haklarının korunmasıdır.

Kişisel veri kavramı geniş yorumlanmalıdır. Yargıtay'a göre kişinin; Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum tarihi, doğum yeri, nüfusa kayıtlı olunan yer, anne ve baba adı, medeni hali, nüfusa kayıtlı olduğu cilt ve aile sıra no, kan grubu, evlenme tarihi, boşanma tarihi ve mahkeme kararı bilgileri, adı-soyadı veya diğer kayıt düzeltmeleri, hakkında yapılan ceza yargılamaları, disiplin soruşturmaları, memuriyet bilgileri, vatandaşlıktan çıkarılma bilgileri, evlatlık ilişkisi, adresi, dini, bitirilen okullar, hastalıkları, hastalıkları ile ilgili tahlil sonuçları, mali durumu, ahlaki eğilimleri, zaafları, çevre ile ilişkileri, hatıra, anı ve günlükle ilgili defterindeki bilgileri, siyası görüşü, üye olduğu dernekler, alışkanlıkları, sevdiği kitaplar veya gazeteler, alışveriş eğilimleri, vergi numarası, e-posta adresi ve şifresi, banka bilgileri, bilgisayarının IP numarası, emeklilik ve kurum sicil numarası, aldığı ödüller, parmak izi, avuç içi izleri, mektupları, yazıları, kitapları, telefon numaraları, mesajları, fiziki kimliği (boy, kilo, engellilik durumu, ten rengi, göz rengi, saç rengi ve şekli), sesi, genel görünümü, ayak ve beden numarası ve daha birçok bilgi, kişisel veridir (YCGK, 17.06.2014, E. 2012/12-1510, k. 2014/331). Kişilerin Facebook, Twitter gibi sosyal paylaşım sitelerinde yazdığı ve paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları da kişisel veridir.

Kişisel verilerin işlenmesi: Kişisel verilerin işlenmesi, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak, geniş bir alanı kapsayacak şekilde tanımlanmaktadır. Kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade etmektedir (6698 s.K. m. 3/e; Direktif m. 2/b).

Veri sorumlusu (veri denetleyicisi/veri denetleyici, veri kontrolörü): Veri sorumlusu, kişisel veri işlemenin amaçlarını ve yöntemini birlikte veya tek başına belirleyen kişi, organ, ajans veya kamu kurumunu ifade etmektedir (6698 s.K. m. 3/ı; Direktif m. 2/d). Veri sorumlusu gerçek kişiler olabildiği gibi özel ve/veya kamu kurumu tüzel kişiliğini haiz kişiler de olabilir. Müvekkili hakkındaki kayıtları tutan avukat veri sorumlusunun gerçek kişi olduğu duruma örnek gösterilebilir. Bir tüzel kişi bünyesinde çalışan gerçek kişiye tüzel kişiliğin uhdesinde bulunan kişisel verileri koruma sorumluluğu yüklense dahi söz konusu somut olay bakımından veri sorumlusu olan tüzel kişiliğin kendisi olup, gerçek kişi ancak onun adına tasarrufta bulunan konumundadır. Veri sorumlusu kişisel verilerin işlenmesi konusunda hukuka uygun davranmakla yükümlü olup ortaya çıkan hukuka aykırılıklardan doğrudan sorumludur. Dikkat edilmesi gereken bir husus ise veri işleyicisi ile veri sorumlusunun her zaman aynı kişi olmayabileceğidir; zira veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişilere "veri işleyicisi" denilmektedir. Genellikle veri sorumluları, zaman ve maliyet tasarrufu sağlamak amacıyla veri işlemek üzere üçüncü bir taraftan hizmet almaktadır. Bu durumda üçüncü taraf veri sorumlusunun emri üzerine hareket etmekte ancak veri işlemenin amacını kendisi belirlememekte olduğundan bu kişi söz konusu işlem bakımından veri işleyicisi kabul edilmektedir. Bir tüzel yahut gerçek kişinin, kişisel verilerin işlenmesi bakımından aynı anda hem veri sorumlusu hem de veri işleyicisi olması mümkündür. Mesela bir avukatlık şirketi kendi çalışanları hakkındaki veriler açısından veri sorumlusu sayılırken; müvekkil şirketlerinin çalışanlarına ilişkin tutmakta olduğu kişisel veriler bakımından ise veri işleyicisi sayılmaktadır.

Kişisel verilerin işlenmesiyle ilgili genel ilkeler: Kişisel verilerin korunmasına ilişkin düzenlemelerde, verilerle ilgili yapılan işlemlerin insan onuru ve değerlerine uygun yapılması maksadıyla bazı ortak ilkeler belirlenmiştir. Bu ilkelerin birbirinden kesin çizgilerle ayrılması zordur. Bazı ilkeler diğerlerine kaynaklık ederken bazıları da tamamlayıcı rol oynamaktadır. Bu ilkelere riayet edilmemesi durumunda kişisel verilerin iyi niyetle, hukuka uygun olarak işlenmediği, ortada bir kötüye kullanımın bulunduğu kabul edilmektedir.

Söz konusu ilkelerle veri sorumlusunun kişisel verileri işlerken uyması gereken yükümlülükler belirlenmekte, işleme sırasında veri sorumlusuyla verileri işlenen kişiler (veri süjesi/veri öznesi) arasında ortaya çıkan çıkar çatışması dengelenmeye çalışılmaktadır.

Kişisel veriler ancak şu temel ilkelere uygun olarak işlenebilecektir: (1) Adil ve Yasal İşleme: Kişisel veriler adil ve yasalara uygun şekilde işlenecektir. (2) Amaç ile Sınırlılık: Kişisel veriler; kesin, belirlenmiş ve hukuka uygun amaçlara göre toplanmış olacak ve ilk toplandıkları amaca aykırı olarak daha sonradan işlemeye konu olmayacaktır. (3) İlgililik ve Orantılılık: Kişisel veriler, toplama ve/veya müteakip olarak işleme amaçları için yeterli ve bu işlemlerle ilgili olacak, aşırı olmayacaktır. (4) Doğruluk ve Güncellik: Söz konusu veriler güncel ve doğru olarak tutulacak; böylece veri kalitesi korunacaktır. Toplanma amaçları veya daha sonraki işleme için yanlış veya eksik olan verinin silinmesi veya düzeltilebilmesi için gerekli tüm makul adımlar atılacaktır. (5) Süreyle Sınırlılık: Kişisel veriler, toplama amacının veya daha sonraki işlemenin gerektirdiğinden daha uzun süre saklanmayacaktır (6698 s.K. m. 4; Direktif m. 6).

Veri işlenmesinin şartları: Kişisel verilerin işlenebilmesi ancak bazı şartların mevcut olması halinde mümkündür: Bunlar, ilgili kişinin herhangi bir kuşkuya yer bırakmayacak şekilde kişisel verilerinin işlenmesine rıza göstermesi; ilgili kişinin taraf olduğu bir sözleşmeyi yerine getirmek veya bu sözleşmeye girmeden önce ilgili kişinin isteğiyle gerekli adımları atmak için kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun konu olduğu bir yasal zorunluluğa uymak için kişisel verilerin işlenmesinin gerekmesi; ilgili kişinin hayati çıkarlarını korumak için kişisel verilerin işlenmesinin gerekmesi; kamu yararı için yapılan bir faaliyetin yerine getirilmesi veya veri sorumlusu veya verinin açıklandığı üçüncü tarafın kamu yetkisini kullanarak yaptığı bir faaliyetin yerine getirilmesi için kişisel verilerin işlenmesinin gerekli olması; ilgili kişiye tanınan haklar ağır bastığı durumlar hariç olmak üzere, kişisel verileri işlemenin, veri sorumlusu veya verilerin açıklandığı üçüncü tarafın meşru çıkarları için gerekli olması durumlarıdır (6698 s.K. m. 5; Direktif m. 7).

Kişisel verileri işlenen kişinin hakları: Kişisel verileri işlenen kişinin bazı hakları mevcuttur. Veri öznesi/veri süjesi kendisiyle ilgili verinin işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgileri talep etme, verilerin işlenme amacı ile bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurtiçinde veya yurtdışında verilerin aktarıldığı üçüncü kişileri bilme ve en önemlisi verilerin işlenmesinin genel ilkelere aykırı olması halinde (6698 s.K. m. 4; Direktif m. 6) veya veri işlemenin şartlarının mevcut olmaması halinde (6698 s.K. m. 5; Direktif m. 7) veya özellikle kişisel verilerin eksik veya doğru olmaması durumlarında, kişisel verilerin silinmesini, düzeltilmesini ve/veya erişime engellenmesini isteme hakkına sahiptir. Özellikle son sayılanlar veri öznesinin itiraz hakkı ile yakından ilintilidir (6698 s.K. m. 7, 10, 11; Direktif m. 12, 14). Zira bazı durumlarda veri sorumlusu, kişisel verileri kamu yararı gözetilerek ifa edilen bir faaliyet çerçevesinde işler ya da kişisel veriler veri sorumlusu veya verilerin açıklandığı üçüncü tarafın meşru çıkarlarının korunması (örneğin haber verme ve alma özgürlüğü) için işlenir. Bu durumlarda dahi ilgili kişiye tanınan haklar ağır bastığı hallerde (örneğin kişilik haklarının ihlali), veri öznesi/veri süjesi, işlemeye itiraz ederek kişisel verilerin silinmesini talep edebilir. Bu husus çok önemlidir; zira bu biraz sonra incelenecek mahkeme kararlarında esas rol oynamaktadır.

dikkat

28.10.2017 tarih ve 30224 sayılı Resmi Gazete'de "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik" yayınlanmıştır. Yönetmeliğin 7 ve devamı maddelerinde kişisel bilgilerin silinmesi, yok edilmesi ve anonim hale getirilmesi ile ilgili esas ve usuller düzenlenmiştir.

Karara Konu Olan Olay

Mahkemenin kararına konu olan olay şu şekilde özetlenebilir: 05.03.2010 tarihinde İspanya'da ikamet eden İspanyol vatandaşı avukat Costaja Gonzales, İspanyol Veri Koruma Kurumu'na (Agencia Espanola de Proteccion de Datos/AEPD) İspanya Katalonya'da La Vanguardia isimli yüksek tirajlı bir gazete çıkaran La Vanguardia Ediciones SL isimli şirketi ve Google Spain ve Google Inc.

şirketlerini şu nedenle şikayet etmiştir: Herhangi bir internet kullanıcısı Costaja Gonzales'in adını Google şirketinin arama motoruna (Google Search) yazdığı zaman, arama sonuçlarının en üst iki sırasında La Vanguardia adlı gazetenin 19.01.1998 ve 09.03.1998 tarihli nüshalarını içeren iki linki bulmaktadır. İnternet kullanıcısı bu linkleri tıkladığında, Costaja Gonzales'in adının açıkça zikredildiği bir ilan metnini görmektedir. Bu ilanlarda Costaja Gonzales'in gayrimenkulünün sosyal güvenlik borçlarından dolayı açık artırma yoluyla satılacağı yazmaktadır.

Karar metnine http://curia.europa.eu/juris/liste.jsf?num=C-131/12 adresinden ulaşılabilmektedir.

Bunun üzerine Costaja Gonzales, kişisel verilerinin korunması hakkına dayanarak La Vanguardia Ediciones SL şirketinden La Vanguardia gazetesine ait bu linklerin haber arşivinden çıkartılmasını talep etmiştir. AEPD nezdinde yaptığı şikayette Costaja Gonzales ayrıca kendisiyle ilgili haciz işlemlerinin yıllar önce ortadan kalktığı ve bu işlemlerle ilgili linklerin artık güncelliğini yitirdiğini gerekçe göstererek, Google Spain ve Google Inc. şirketlerinden, La Vanguardia gazetesine ait linkleri, arama motorunun gösterdiği arama sonuçlarından çıkartmasını talep etmiştir.

AEPD, 30.07.2010 tarihinde verdiği kararla, şikayetin La Vanguardia'ya ilişkin kısmını, ilanın açık artırmaya ilişkin İspanyol mevzuatına uygunluğunu gerekçe göstererek reddetmiştir. Buna karşın AEPD şikayetin Google Spain ve Google Inc. şirketlerine ilişkin kısmını kabul etmiştir; zira ilgili kişinin kişisel verilerini işleyen arama motoru işletmecisi Google Spain ve Google Inc., kişisel verilerin korunması hakkına dayanılarak yapılan başvurularda, silinmesi talep edilen bilgiler kişilik haklarını zedelemesi durumunda, üçüncü kişiler tarafından bilinmesi istenmeyen bilgileri silmek ve/veya bu bilgilere erişimi engellemekle yükümlüdür. Kişisel verilerin korunması sebebiyle arama motoru işletmecilerine yüklenen bu yükümlülük, arama sonucunda çıkan linkin içeriğinin doğru olması ve hatta somut olaydaki gibi görüntülendiği internet sitesinden silinmesinin yasal olarak mümkün olmaması halinde dahi geçerlidir; zira arama motoru işletmecilerinin kişisel verileri koruma yükümlülüğü, arama sonucu çıkan linkin içeriğini oluşturan kişilere yüklenen yükümlülüklerden ayrı ve bağımsızdır. Bu nedenle Costaja Gonzales'in Google Spain ve Google Inc. şirketlerinden bu linklerin arama sonuçlarından çıkartılmasını isteme hakkı vardır. Bu hakkın kullanılması için Costaja Gonzales'in öncelikle La Vanguardia Ediciones SL şirketine başvurması ve hatta böylesi bir başvuruda başarılı olması şart değildir. Costaja Gonzales, La Vanguardia Ediciones SL şirketine başvurmasa da ya da başvurup da şikayetiyle ilgili başarılı bir sonuç almasa da, kişisel verilerinin korunması için Google Spain ve Google Inc. şirketlerine yönelebilecektir.

Google Spain ve Google Inc. bu karara karşı yüksek mahkeme olan Audencia Nacional nezdinde ayrı ayrı dava açmıştır. Google Inc. açtığı davada şu şekilde savunma yapmıştır: Google Inc. Google Arama Motoru'nun işletmecisi olmakla birlikte, şirketin merkezi ABD'dedir. Bu nedenle Direktif kendisine uygulanamaz. Google Spain'de açtığı davada, kendisinin arama sonuçları ile bir ilgisinin olmadığını, bu arama sonuçlarına teknik olarak kendisinin bir katkısı bulunmadığını, yani veriyi kontrol etme yetkisinin bulunmadığını, kendisinin sadece Google Inc.'in İspanya'da olan müşterilerine Google Inc.'in reklam alanını tanıttığını ve sattığını belirtmiştir. Ayrıca her iki şirket Costaja Gonzales'in hukuka uygun bir veriye erişimi engelleme isteği yönünde bir hakka sahip olmadığını ifade etmişlerdir.

Audencia Nacional, davaları birleştirdikten sonra, ihtilafın 95/46/EC sayılı Direktifin yorumundan kaynaklandığını belirterek, konu hakkında görüş bildirmesi için davayı ABAD'a taşımıştır (ABAD, 13.05.2014 – C-131/12, kn. 14-20).

ABAD'ın Ulaştığı Sonuçlar ve Gerekçe

ABAD öncelikle Google Spain ve Google Inc.'in Audencia Nacional nezdinde ileri sürdükleri itirazları değerlendirmiştir. Mahkeme'ye göre, bir arama motoru işletmecisi, kendi şirket merkezi AB dışında olsa dahi, bir üye devlette arama motoru üzerinde reklam alanı sağlama ve satma amacıyla bir şirket kurduğu zaman şirket faaliyetlerinin,

kişisel verilerin korunmasına ilişkin olarak, denetiminin Direktife göre yapılması gerekmektedir. Aksinin kabulü, bu tür şirketlerin Direktifle öngörülen yükümlülük ve teminatlardan muaf tutulması anlamına gelir ki, bu da kabul edilemez (ABAD, 13.05.2014 – C-131/12, kn. 42-61).

Hemen belirtilmelidir ki, ABAD Direktifin yer bakımından uygulama alanına ilişkin yukarıda özetlenen düşüncelerini açıklamadan önce, kararında Direktifin arama motorlarının icra ettiği faaliyeti düzenleyip düzenlemediğine ilişkin de açıklamalar yapmıştır; zira Direktifin arama motoru işletmecilerine uygulanabilmesi, bunların veri sorumlusu olarak kabul edilmesine bağlıdır.

Google Spain ve Google Inc.'e göre arama motorları internette yer alan tüm bilgileri kişisel veri ve diğer bilgiler şeklinde bir ayrıma tabi tutmaksızın toplamaktadır; bu fonksiyon ise Direktif anlamında veri işleme olarak kabul edilemez. Ayrıca bu faaliyet veri işleme olarak kabul edilse dahi, arama motoru işletmecisi bu bilgilerden haberdar olmadığı ve bu bilgileri denetlemediği için veri sorumlusu değildir.

ABAD'a göre ise Direktifin ilgili maddelerinin yorumundan böyle bir sonuç çıkmamaktadır. İnternette üçüncü kişilerce yayınlanmış veya bu kişilerce bulundurulan bilgiyi konumlandırma, otomatik olarak indeksleme, geçici olarak saklama ve son olarak belirli bir tercih sırasına göre internet kullanıcısına sunmadan oluşan arama motorunun icra ettiği faaliyet, kişisel verinin işlenmesi olarak kabul edilmelidir; zira interneti otomatik, düzenli ve sistematik olarak orada yayınlanan bilgiyi bulmak için inceleyen arama motorunun işletmecisi daha sonra bu bilgileri kendi indeksleme programı çerçevesinde geri alır, kaydeder, organize eder, bu tür verileri arama sonuçları listesi formunda toplar, sunucuları üzerinde saklar, daha sonra ise ifşa eder ve kullanıcılarının kullanımına sunar. Bu tür faaliyetler, kişisel verilerin işlenmesi olarak kabul edilmelidir. Verilerin internette zaten başkalarınca yayınlanmış olması ve arama motorlarının bu verinin içeriğini değiştirmiyor olmasının bir önemi yoktur. Arama motoru işletmecisi aynı zamanda veri sorumlusudur; zira arama motoru işletmecisinin icra ettiği fonksiyon ile internet sayfalarının sahiplerinin veya yöneticilerinin icra ettikleri fonksiyon, birbirlerinden ayrı müstakil eylemlerdir (ABAD, 13.05.2014 – C-131/12, kn. 21-41).

Arama motorunun icra ettiği fonksiyonun veri işleme, arama motoru işletmecisinin de veri sorumlusu olduğunu belirttikten sonra ABAD çok önemli bir soruya yanıt aramıştır. Bu soru şudur: Direktifle bireylere sağlanan hakların korunması için arama motoru işletmecisine, üçüncü kişilerce (web sitesi sahibi) internette yayınlanmış ve/veya bulundurulan veriyi, önceden veya eş zamanlı olarak verinin yer aldığı internet sayfası sahibine başvurmaksızın, indekslerinden (arama sonuçlarından) çıkarmasını öngören bir yükümlülük yüklenebilir mi; eğer bu soruya verilecek yanıt olumlu ise, kişisel veriyi içeren internet sayfasının üçüncü kişilerce internette yayınlanmasının ve/veya bulundurulmasının meşru olduğu durumlarda da arama motoru işletmecisinin bu sorumluluğu devam edecek midir?

Google Spain ve Google Inc. bilginin kaldırılmasını ve/veya silinmesini amaçlayan bir talebin bu bilgiyi kamuoyuna sunan kişiye yöneltilmesi gerektiğini; bunun ölçülülük ilkesinin bir sonucu olduğunu ifade etmişlerdir. Kamuoyuna sunulan yayının kendisinin hukuka uygun olup olmadığını değerlendirebilecek kişi web sitesinin sahibidir. Zira bu kişi ilgili kişinin kişisel verilerinin internet sayfasından çıkartılması konusunda en etkili araçlara sahip süjedir. Ayrıca arama motoru işletmecisine internette yayınlanan yayınları indekslerinden çıkarma yükümlülüğünün yüklenmesi, web sitesi sahiplerinin ilgili kişilerin temel haklarına yeterince dikkat etmemesine neden olacaktır.

Bu noktada bir hususun altı çizilmelidir: Dikkat edilirse ABAD kararın bu bölümünde internette yer alan ve üçüncü kişilerce yayınlanan ve/veya bulundurulan verinin içeriğinin doğru, tarafsız ve meşru olması halinde, arama motoru işletmecisine ne tür sorumluluklar yükleneceği sorusuna yanıt aramamıştır; zira bu, kararın ilerleyen bölümlerinde ayrıca değerlendirilmiştir. ABAD kararının aşağıda açıklanacak bölümü temel olarak şu hususla ilgilidir: Bazen öyle somut olaylar mahkemelerin önüne gelmektedir ki, kişisel verileri internette yayınlayan üçüncü şahıslar, bu verilerin yayınlanmasında diğer temel hak ve özgürlüklere dayanabilmektedir ve böylece yayının kendisi, yayının içeriğinin ilgilinin kişisel haklarını zedeleyip zedelemediğinden bağımsız olarak, hukuka uygun hale gelmektedir. Örneğin HGK'nun önüne gelen olayda, suç mağduru olan kişinin adı kanunen zorunlu olduğu için bir Yargıtay kararında açıkça zikredilmiş, bu karar da

daha sonra Yorumlu-İçtihatlı Türk Ceza Kanunu adlı bir eserde olduğu gibi aynen okuyucuya aktarılmıştır. Suç mağduru olan kişi de, kitabın ilgili bölümünden adının çıkartılması istemiyle mahkemeye başvurmuş, Yargıtay 4. Hukuk Dairesi ise bu istemi, yayının bilim özgürlüğüne uygun olduğu gerekçesiyle reddetmiştir. İşte bu örnekte yayının kendisi hukuka uygun olduğu halde, ilgilinin kişilik haklarını zedelemektedir.

Bu noktadan hareketle ABAD ilgilinin internet sayfası sahibine yönelmeden, doğrudan doğruya arama motoru işletmecisine başvurarak, hukuka uygun ama kişilik haklarını zedeleyen yayınların bulunduğu linkleri arama motorundan çıkartmasına yönelik bir talebin kabul edilip edilemeyeceğine dair açıklamalarda bulunmuştur.

ABAD'a göre söz konusu durumla ilgili olarak Direktifin ilgili maddelerinin yorumundan çıkan sonuç şudur: Bir arama motoru işletmecesi, üçüncü kişilerce yayınlanan kişisel verileri içeren sayfalara ilişkin linkleri arama sonuçları listesinden çıkartmakla yükümlüdür. Bu yükümlülüğün doğması için ilgili kişiye ait kişisel verilerin önceden veya eş zamanlı olarak web sitesinden çıkartılması veya ilgili kişinin kendisine ait bu bilgilerin çıkartılması için web sitesi sahibine başvurması gerekmemektedir. Arama motorları işletmecisine doğrudan yüklenen bu yükümlülük ulusal mahkeme kararlarından veya ulusal ölçekte kurulan kişisel verileri korumakla yükümlü organların verecekleri kararlardan doğabilecektir; zira Direktif verilerin daha önce internette yayınlanmış olmasına ve/veya bu verilerin yayınlanmasının kendisinin hukuka uygun olup olmamasına bir önem atfetmemiştir.

Bu sonuç Direktifin amaç maddesinden çıkmaktadır. Madde 1'e göre bu Direktifin amacı kişisel verilerin işlenmesi durumunda, bireylere başta mahremiyet hakkı olmak üzere, temel hak ve özgürlüklerinin koruması için yüksek seviyede güvence sağlanmasıdır. Bu amaç doğrultusunda Direktif bir taraftan veri sorumlusuna yükümlülükler yüklemiş diğer taraftan da ilgili kişiye verilerin düzeltilmesini ve/veya silinmesini talep etme gibi haklar tanımıştır. Öyleyse Direktifle bireylere tanınan hakların kapsamına dair açıklamalar yapılırken, bu hakların temel hak ve özgürlükler açısından değerlendirilmesi zorunludur. ABTHB'nin 7. maddesi özel hayata saygıyı teminat altına alırken, 8. maddesi de kişisel verilerin korunması hakkını tanımaktadır. Bundan dolayı Direktifin söz konusu ihtilafla ilgili olan 6, 7, 12 ve 14. maddeleri (dolayısıyla 6698 sayılı Kanun'un 4, 5, 7, 10, 11. maddeleri) yorumlanırken ABTHB'nin 7 ve 8. maddelerinde tanınan hakların gerçekleşmesi amaçlanmalıdır.

Bu noktada Direktifin 12. maddesi önemlidir. Bu maddeye göre ilgili kişi veri sorumlusundan, veri işlemesinin Direktifte belirtilen esaslara uygun olmaması halinde, verilerin engellenmesini veya silinmesine veya düzeltilmesini isteyebilecektir. Her ne kadar söz konusu bu maddenin kaleme alınış şeklinden verilerin özellikle eksik veya yanlış olması durumunda bu hakların ileri sürülebileceği anlaşılmaktaysa da, söz konusu hükmün Direktifin 6. maddesiyle ilgili olduğu unutulmamalıdır. Öyleyse bireylere 12. madde ile tanınan haklar, veri işlemesinin Direktifin 6. maddesinde yer alan diğer temel ilkelere aykırılık oluşturması durumunda da söz konusu olacaktır. Diğer bir ifadeyle, ilgili kişi veri sorumlusundan kendisiyle ilgili verilerin engellenmesini, düzeltilmesini veya silinmesini, veri sorumlusunun veriyi yasal ve makul şekilde işlemediği; belirgin, meşru ve açık amaçlar için toplamadığı; hukuka uygun toplasa bile topladığı verileri daha sonra amaç dışında kullandığı veya verileri toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun süre tutması halinde de isteyebilecektir. Veri sorumlusu da verilerin silinmesi veya düzeltilmesini temin etmek için her makul adımı atmak zorundadır.

Arama motoru işletmecisine yüklenen bu yükümlülük Direktifin 7. maddesinin 14. maddesi ile birlikte okunmasından da çıkmaktadır. Kişisel verilerin işlenmesinin hangi durumlarda hukuka uygun olacağını düzenleyen 7. maddesine göre, kişisel verilerin işlenmesi veri sorumlusu veya verinin ifşa edildiği üçüncü şahıslar tarafından takip edilen meşru menfaatin gerçekleşmesi için zorunluysa (örneğin internet kullanıcılarının bilgiye ulaşmalarındaki meşru amaç gibi) ve bu menfaat ilgili kişinin temel hak ve özgürlerinden daha ağır basıyorsa, hukuka uygundur. Diğer taraftan ise Direktifin 14. maddesine göre ilgili kişi, Direktifin 7. maddesine göre hukuka uygun olan işlemeye kendi özel durumunu ileri sürerek itiraz etme hakkına sahiptir. Dolayısıyla Direktifin 7. maddesi ile veri sorumlusuna verilen işleme hakkı ile ilgili kişinin ABTHB'nin 7. ve 8. maddelerinden doğan temel hak ve özgürlükleri karşı karşıya gelmekte, birbirleriyle çatışmaktadır.

Böylesi bir durumda çatışan bu haklar arasında denge kurulmalıdır. Ne var ki, ilgili kişinin özel durumunun büyük ölçüde dikkate alınmasının zorunluluğu karşısında, bu dengenin ilgili kişi lehine bozulacağı ortadadır. Bunun istisnası, mevzu bahis bilginin toplumsal yaşamda önemli bir rol oynaması ve/veya ilgili kişinin kamusal hayatta aldığı rol nedeniyle, bu kişinin verilerine kamuoyunun ulaşmasının kamusal menfaatler için gerekli olduğunun belirlenmesi halinde mümkündür.

İlgili kişi lehine kurulan bu dengenin, arama motoru işletmecisinin salt ekonomik menfaati nedeniyle, tekrar ilgili kişi aleyhine bozulamayacağı da aşikardır. Zira arama motorunun olmadığı düşünüldüğünde, internet kullanıcıları ilgili kişi ile ilgili olarak web sitelerinin sahiplerince internette ifşa edilen kişisel verilere ya hiç ulaşamayacaklardır ya da bu verilere ulaşmak için çok büyük bir çaba harcayacaklardır. Öyleyse arama motoru işletmecisi, bu siteleri internet kullanıcısı için kolay erişilebilir kılmakta ve dolayısıyla da ilgili kişinin kişisel verilerinin yayılmasında belirleyici rol oynamaktadır ve böylece de ilgili kişinin mahremiyet hakkına en az web sitesi sahibi kadar müdahale etmektedir. Sonuç olarak ilgili kişinin doğrudan arama motoru işletmecisine başvurabilmesi ve sonuç listesinde yer alan web sitelerine ilişkin linkleri kaldırmasını isteyebilmesi temel hak ve özgürlüklerin tam olarak sağlanabilmesi için elzemdir (ABAD, 13.05.2014 – C-131/12, kn. 62-88).

ABAD son olarak ilgili kişinin, üçüncü kişilerce hukuka uygun şekilde yayınlanmış ve kendisiyle ilgili gerçek bilgiler içeren internet sayfalarına arama motoru işletmecisi tarafından Google Search aracılığıyla yapılan bağlantıların kaldırılmasını, bu bilgilerin kendisine zarar verebilecek nitelikte olduğunu ya da bu bilgilerin belirli bir zamandan sonra unutulmasını arzu ettiğini belirterek, talep edip edemeyeceğine yönelik açıklamalarda bulunmuştur.

Google Spain ve Google Inc., veri süjesinin ilgili linkin kaldırılmasını isteme hakkının ancak ve ancak işlemenin hukuka uygun olmaması durumunda mevcut olduğunu belirtmişlerdir. Buna karşın ilgili kişinin, bu kişiye ilişkin gerçek bilgiler içeren web sitelerinin linklerinin Google Search'de yapılan arama sonrası çıkan arama sonuçlarından kaldırılmasını isteme hakkı, ilgili kişinin sırf bu sitelerde yayınlanan yayınların unutulmasını arzu ettiği durumlarda, bulunmamaktadır. Bu tip durumlarda ilgili kişi web sitesinin sahibine başvurmalıdır.

ABAD bu görüşe katılmadığını şu gerekçelerle ifade etmiştir: Daha önce de belirtildiği üzere, ilgili kişi kişisel verilerinin işlenmesinin engellenmesini ya da işlenmiş verilerinin silinmesini, her ne kadar kaleme alınış şekli yanıltıcı olsa da, Direktifin 12. maddesine göre sadece bu verinin yanlış ya da eksik olması durumunda değil, işlemenin Direktifin 6. maddesinde yer alan temel ilkelerden herhangi birine uymaması halinde de isteyebilecektir. Bu noktada dikkat edilmesi gereken husus, işlemenin yapıldığı tarihte, bu işleme hukuka uygun olsa bile zamanın ilerlemesiyle bu işlemenin Direktifin 6. maddesine aykırılık oluşturabileceğidir. Diğer bir ifadeyle Google Search'de arama sonrası gösterilen ve hukuka uygun şekilde yayınlanan ve ilgili kişiyle ilgili olarak gerçek bilgi içeren internet sayfalarında yer alan bilgiler, web sitesi sahiplerince bu işlemenin ilk yapıldığı zamanda hukuka uygun olsa dahi, bu işleme bu özelliklerini zaman içinde yitirebilmektedir. İşte bu tip durumlarda kişisel veriler artık toplandığı amaca ilişkin olarak yeterli ve ilgili değildir, doğru değildir, güncel değildir ve bu veriler işlemenin amacına aykırı olarak gereğinden daha fazla süre tutulmuştur. Bütün bunlar veri kalitesine ilişkin prensiplerin belirtildiği Direktifin 6. maddesine aykırılık oluşturmaktadır. Böyle bir durumda ilgili kişi Direktifin 7. maddesini gerekçe göstererek Direktifin 14. maddesine göre kendisine dair verilerin işlenmesine itiraz edebilecektir.

Burada altı çizilmesi gereken nokta, ilgili kişinin bu talebinin kabul edilip edilmemesi değerlendirilirken, internette yer alan kendisiyle ilgili gerçek bilgilerden ilgilinin zarar görüp görmeyeceğinin değerlendirmede rol oynamayacağıdır; zira böyle bir değerlendirmeyi veri sorumlusunun objektif kıstaslar çerçevesinde yapması mümkün değildir. Ayrıca söz konusu talebin dayanağını, ilgili kişiye ABTHB'nin 7. ve 8. maddelerinde tanınan haklar oluşturmaktadır. Dolayısıyla bir kez daha internet kullanıcılarının bilgiye ulaşmalarındaki meşru menfaat ile ilgili kişinin mahremiyet hakkı çatışmaktadır. Bu tip durumlarda dengenin ilgili kişi lehine bozulduğu, eğer ki kamunun bilgiye erişmesinde ilgili kişinin toplumdaki rolü gibi bir nedenden dolayı üstün menfaatini kanıtlayan özel bir neden yoksa, yukarıda belirtilmişti.

Açıklanan tüm bu gerekçelerden dolayı Costeja Gonzalez, arama motoru işletmecisi Google Inc.'den Google Search'de ilgili gazetenin çevrimiçi arşivlerine verilen linklerin kaldırılmasını talep

edebilecektir; gazete yer alan ilanın/haberin objektif olarak doğru olması bu sonucu değiştirmemektedir. Arama motoru işletmecisi de bu talebin gereğini yerine getirmelidir; zira yaklaşık 20 yıl önceki haber güncel değildir. Haberin içeriğinde yer alan bilgilere toplumun ulaşmasında, Costeja Gonzalez'in toplumdaki rolü göz önünde alındığında, toplumsal bir yarar gibi üstün bir menfaati kanıtlayan özel bir neden de bulunmamaktadır (ABAD, 13.05.2014 – C-131/12, kn. 89-99).

Karar Çerçevesinde Unutulma Hakkının Kapsamı

İnternette yer alan kişisel verilerin çoğu bireyin yaşamını doğrudan etkilemektedir. Bireylerin yaşamında önemli rol oynayan bu veriler, örneğin bir iş veya sertifika başvurusunda, bankadan kredi çekilmesinde incelenmektedir. Dolayısıyla birey hakkında birçok önemli karar bu verilere dayanılarak verildiğinden bu verilerin doğruluğunun, güvenilirliğinin, yanlış biçimde değiştirilmemesinin ya da doğru olsa bile bireylerin özel hayatlarını yaşanılmaz hale getirecek şekilde gereksiz ve uzun süre internette tutulmamasının sağlanması çok önemlidir.

Arama motorları, büyük ölçekli metinlerden bilginin elde edilmesi veya açığa vurulması için pratik uygulamalardır. Ancak arama motorlarının işlevi bununla sınırlı kalmamaktadır. Bunlar arama hizmetinden hareketle kullanıcıların bilgilerine erişim sağlayarak internet üzerinden neye, ne kadar tıklandığı ve benzeri bilgileri kullanarak, kullanıcıların örneğin tüketim alışkanlıklarının profilini çıkartmakta ve bunu da kullanıcılarla IP adreslerinin ilişkilendirerek yapmaktadır. Ayrıca unutulmamalıdır ki, arama motorunda bir kişinin adıyla arama yapıldığında, onun özel hayatının birçok yönünü ilgilendirebilen geniş bir bilgi yelpazesine diğer kullanıcılar ulaşabilmektedir. Bu şekilde de kişi hakkında az ya da çok detaylı bir profilleme yapılabilmektedir. Oysa arama motorları olmasaydı, bu bilgilere birbiriyle ilintili olarak ulaşmak ya mümkün olmayacaktı ya da çok daha büyük güçlükle mümkün olabilirdi. İşte bundan dolayı Google, kişisel verilerin korunması konusunda en çok eleştirilen şirketlerden biridir ve hatta "gizlilik muhalifi" olarak nitelendirilmiştir.

ABAD'ın Google ve diğer arama motoru işletmecilerine dair verdiği kararı bu arka planla okumak ve kararın esas noktalarını özetlemek faydalı olacaktır:

1. İnternette üçüncü şahıslarca yayınlanmış bilgiyi konumlandırma, otomatik olarak indeksleme, geçici olarak saklama ve son olarak belirli bir tercih sırasına göre internet kullanıcılarına sunulmasından oluşan arama motoru faaliyeti, kişisel verilerin işlenmesi olarak nitelendirilmeli ve arama motoru işletmecisi de veri sorumlusu olarak bu kişisel verilerin işlenmesinden sorumlu olmalıdır.
2. Arama motoru işletmecisinin şirket merkezinin ülke dışında olması, şirketin bir şubesinin ülkede faaliyet göstermesi halinde, şirketin bu sorumluluktan kaçabilmesine olanak vermemektedir.
3. Bireyler kendilerine tanınan temel hak ve özgürlüklerden, özellikle mahremiyet hakkından, tam olarak faydalanabilmek için, arama motoru işletmecisine doğrudan başvuru yapabilmelidir. Bu yöndeki bir hakkın doğması için ilgili kişiye ait kişisel verilerin önceden veya eş zamanlı olarak web sitesinden çıkartılması veya ilgili kişinin kendisine ait bu bilginin çıkartılması için web sitesi sahibine önceden veya eş zamanlı olarak başvurması gerekmemektedir, yine aynı şekilde arama motoru işletmecisinin de ilgili sayfanın webmasterına bu hususta bilgi vermesi şart koşulmamaktadır. Dolayısıyla ilgili kişiler, arama motoru işletmecisinden, kendilerine ilişkin bilgileri içeren web sitelerine dair arama sonuçlarında yer alan linklerin kaldırılmasını isteyebilir. Bunun için şu şartlardan herhangi birinin gerçekleşmesi yeterlidir: (a) Kişisel veriler rızaya dayalı olarak yahut bir zorunluluk gereği paylaşılmasına rağmen hukuka ve dürüstlük kuralına uygun bir biçimde işlenmemişse; (b) Kişisel veriler belirli, açık, ölçülü ve meşru amaçlarla toplanmamışsa; (c) Kişisel veriler meşru amaçla toplanmasına rağmen bu amaçlarla bağdaşmayacak şekilde işlenmiş ve kullanılmışsa; (d) İşleme faaliyeti yeterli, ilgili ve amaca uygun nitelikte değilse; (e) Kişisel veriler doğru ve güncel olarak tutulmamışsa; (f) Kişisel verilerin toplanma veya işlenme amacı için gerekli olan süre aşılmışsa.
4. İlgili kişi arama sonuçlarında yer alan linklerin kaldırılmasını, bu linklerin içeriğinde kendisiyle ilgili gerçek bilgilerin bulunması

halinde dahi isteyebilecektir. Diğer bir ifadeyle unutulma hakkından yararlanabilmek için, kişisel verinin içeriğinin yanlış olması şart değildir. Gerçeği yansıtan bir verinin de kaldırılması talep edilebilir.

5. Kişinin genel olarak geçmişiyle bağlı kalmama hakkı mevcuttur. Bundan dolayı unutulma hakkı mutlaka geçmişteki hatalar veya kişiyi zor durumda bırakabilecek bilgiler bakımından değil; genel olarak mevcuttur. Bu bakımdan ilgili kişinin ilgili linkin kaldırılmasını isteyebilmesi için, kişinin linkin içeriğinden dolayı zarar görmesi veya böyle bir tehlikeyle karşı karşıya kalması gerekmemektedir.
6. Kişisel verilerin yayınlanmasının hukuka aykırı olması gerekmemektedir. Örneğin, kişinin rızasıyla vaktinde bir siteye yüklediği bilgilere ilişkin linkin kaldırılması talebi de unutulma hakkı çerçevesinde ele alınmalıdır. Zira bu ve diğer durumlarda da, kişisel veriler zaman içinde geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelebilmektedir.
7. Unutulma hakkı çerçevesinde yapılan başvurularda unutulma hakkı ile çatışan diğer temel hak ve özgürlükler arasında denge kurulmalıdır. İlgili verinin kamu hayatında oynadığı rol ve halkın ilgili veriye yönelik meşru yoğun ilgisi gibi üstün bir kamu yararını ortaya koyan özel sebepler mevcut olmadığı sürece, unutulma hakkı arama motoru işletmecileri tarafından her türlü makul tedbirlerin alınması suretiyle sağlanmalıdır.

ABAD kararından sonra Google, unutulma hakkını kullanmak isteyen AB vatandaşlarının başvurularını kabul etmeye başlamıştır. Google'dan yapılan açıklamaya göre, şirkete karardan hemen sonra günde ortalama 12.000 başvuru yapılmış, zaman içinde bu sayı bir nebze azalmıştır. Söz konusu karar çerçevesinde şirkete başvuranlar, internetteki ilgisiz ve geçersiz kişisel verilere yönelik linklerin kaldırılmasını isteyebilmektedirler. İnternetten doldurulan formda kullanıcıların hangi ülkede doğdukları, hangi linkin kaldırılmasını istedikleri ve taleplerinin nedenleri sorulurken, kullanıcılardan ayrıca geçerli bir fotoğrafı göndermeleri de istenilmektedir. Ancak ifade edilmelidir ki, unutulma hakkından şu anda sadece 28 AB üyesi ülke ve AB üyesi olmayan İzlanda, Norveç, İsviçre ve Liechtenstein ülkeleri yararlanmaktadır. Bu ülkelerin vatandaşı olmak şart olmayıp, bu ülkelerde ikamet etmek yeterlidir. Ayrıca unutulma hakkı çerçevesinde talep edilen link kaldırma talebinin kabulü halinde, karar sadece AB coğrafyasında uygulanmakta, dolayısıyla AB sınırları dışından yapılan aramalarda ilgili linklere erişim devam etmektedir.

dikkat

Türkiye'den yapılan başvurular henüz değerlendirilmeye alınmamaktadır.

Tabi ABAD kararının coğrafi sınırlamalarla uygulanmasının yetersiz olduğu belirtilmelidir. ABAD'ın yargı yetkisinin AB sınırları ile sınırlı olduğu bir gerçek ise de internetin sınır tanımayan yapısı nedeniyle, ilgili linkin tüm Google veri tabanından (google.com) çıkartılmasının unutulma hakkı ile güvence altına alınan hakkın tam olarak sağlanabilmesi için zorunlu olduğu belirtilmelidir. Ancak böylesi bir durumun ortaya çıkışında ABAD'ın konuyu ele alış şeklinin de etkili olduğu belirtilmelidir. Zira kararda tanınan hakları hayata geçirmek ve işlevsel kılmak konusunda asli yük arama motoru işletmecisine bırakılmıştır. Böylece temel bir hakkın kapsamının belirlenmesi ve içeriğinin uygulanması ve geliştirilmesi hususları, kâr amacı güden bir şirkete bırakılmıştır. Çok uluslu şirketlerin, bir insan hakkının yükümlüsü olmasının uluslararası hukuk açısından yarattığı teorik soru işaretleri bir yana, unutulmaması gereken bir diğer husus da bu şirketlerin çalışanlarının kararın yerine getirilmesine ilişkin yeterli hukuki donanıma sahip olmayabileceğidir.

Bütün bunlardan bağımsız olarak ABAD kararına getirilen eleştiriler de mevcuttur; zira ABAD kararında bazı önemli noktaları aydınlatmamıştır. Örneğin bu kararda birden fazla kişiyi içeren verilerin varlığı durumunda (örneğin grup fotoğrafı) hakkın kimin tarafından ve nasıl kullanılacağı belirtilmemiştir. Örneğin bu durumda fotoğrafta yer alan tek bir kişinin talebi üzerine veri silinecek midir ve cevap olumlu ise diğer kişilerin iradesi ne olacaktır? Ayrıca karar sadece arama motoru işlet-

mecilerine dairdir. Kararın konusu, kişisel verilerin kendisinin ilgili sayfadan silinmesi değil, arama motorunda yer alan sonucun karartılmasıdır. Buna karşın unutulma hakkı daha geniş bir şekilde, geçmişine dair bir bilgiyle bir kimsenin süresiz olarak bağlantılı kılınmama hakkı olarak ele alınabilirdi. Kararda eleştiriye açık bir başka husus da karar uyarınca yapılacak talep sonucunda alınan link kararma kararının her zaman isabetli olmayabileceği gerçeğidir. Değerlendirme, talepte bulunan kişinin verdiği bilgiler çerçevesinde yapılacaktır; fakat veriye ulaşmakta menfaati olabilecek başka kimseler süreçten haberdar bile olmayacaktır, bundan dolayı da inceleme tek taraflı bilgilere istinaden sürdürülecektir (Önok, 2017: 7738).

AYM'nin Unutulma Hakkı Kararı

Yukarıda da ifade edildiği üzere, ABAD kararı arama motoru işletmecilerinin sorumluluğuna ilişkindir. Daha da önemlisi şudur: kararın konusu kişisel verinin kendisinin ilgili sayfadan silinmesi değil, arama motorunda yer alan sonucun karartılmasıdır. Diğer bir deyişle ABAD kararı, arama motorlarından kişisel verilere link içeren sonuçların silinmesine dairdir. Buna karşın unutulma hakkı, daha geniş şekilde, geçmişine dair bir bilgiyle bir kimsenin süresiz olarak bağlantılı kılınmama hakkı olarak da ele alınabilir. AYM'nin 24.08.2016 tarihli ve 29811 sayılı Resmî Gazete'de yayınlanan 03.03.2016 tarihli ve 2013/5653 başvuru numaralı bireysel başvuru kararı bu anlamda oldukça değerlidir.

dikkat

AYM, ABAD'dan farklı olarak haber arşiv içeriğinin, dolayısıyla ilgili sayfanın kendisinin, unutulma hakkı çerçevesinde silinebileceğini belirtmiştir. Buna karşın ABAD, unutulma hakkını sadece arama motorunda gösterilen sonuçlar çerçevesinde ele almıştır.

Karara konu olan olay şu şekilde özetlenebilir: Ulusal ölçekte yayımlanan bir gazetenin internet arşivi sayfalarında, başvurucu hakkında uyuşturucu kullandığı iddiası ile yürütülen bir ceza kovuşturması neticesinde adli para cezasına hükmedilen olaya ilişkin olarak 1998 yılında iki, 1999 yılında bir olmak üzere toplam üç haber başlığı yayımlanmıştır. Başvurucu, ilgili basın kuruluşunun internet sayfasının arşiv bölümünde hakkındaki haberlerin yayınına devam ettiğini belirterek, bu tarihte 5651 sayılı Kanun'un 9. maddesi 6518 sayılı Kanun ile henüz değiştirilmediğinden, 02.04.2013 tarihinde ilgili basın kuruluşuna internet yayınının kaldırılması hakkında ihtarname göndermiştir. Bu ihtarname 03.04.2013 tarihinde tebliğ edilmiştir. İhtarnamenin içeriğinde sitede yayımlanan haberlerin başvurucunun şeref ve haysiyetini zedelediği, özel hayatına ilişkin mahremiyetini ortadan kaldırdığı, topluma mal olmuş ünlü bir kişi olmamasına rağmen başta aile yaşamı olmak üzere iş ve sosyal hayatını olumsuz etkilediği ileri sürülmüştür.

İlgili sitenin iki gün içinde anılan haber içeriklerini kaldırmaması üzerine başvurucu, içeriklerin yayından kaldırılması talebiyle ilgili basın kuruluşu aleyhine 18.04.2013 tarihinde (kapatılan) İstanbul 36. Sulh Ceza Mahkemesine başvurmuştur. (Kapatılan) İstanbul 36. Sulh Ceza Mahkemesi 22.04.2013 tarihli ve 2013/314 Değişik İş sayılı kararı ile talebin kabulüne karar vermiştir. Anılan karara karşı yapılan itiraz, İstanbul 2. Asliye Ceza Mahkemesinin 28.05.2013 tarihli ve 2013/235 Değişik İş sayılı kararlarıyla kabul edilerek (kapatılan) İstanbul 36. Sulh Ceza Mahkemesinin kararının kaldırılmasına hükmedilmiştir. Karar 21.06.2013 tarihinde başvurucu vekiline tebliğ edilmiştir. Başvurucu 22.07.2013 tarihinde bireysel başvuruda bulunmuştur.

Başvurucu, Anayasa m. 12, 17, 20, 25, 26, 27 ve 32 ile korunan haklarının ihlal edildiği iddiası ile AYM'ye başvurmuş ise de Mahkeme başvurucunun iddialarını mahiyeti itibarıyla Anayasa m. 20/3'de düzenlenen kişisel verilerin korunmasını isteme hakkı ile bağlantılı olarak Anayasa m. 17/1'de düzenlenen kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı çerçevesinde değerlendirmiştir. Daha sonra ise bu haklar ile çatışan düşünceyi açıklama ve yayma özgürlüğü ile basın özgürlüğüne dair değerlendirmelerde bulunmuş ve en son olarak da hak ihlali iddiasına konu olan olayı, çatışan menfaatler çerçevesinde incelemiştir.

Mahkemeye göre bireyin kişisel şeref ve itibarı, Anayasa'nın 17. maddesinde yer alan "manevi varlık" kapsamında yer almaktadır. Devlet, bireyin manevi varlığının bir parçası olan kişisel şeref ve itibara keyfi olarak müdahale etmemek ve üçüncü kişilerin

saldırılarını önlemekle yükümlüdür. Kamusal bir tartışma bağlamında eleştirilmiş olsa bile bir kişinin itibarı, kimliğinin ve manevi bütünlüğünün bir parçasını oluşturur ve Anayasa'nın 17. maddesinin birinci fıkrasının koruması altındadır. Öte yandan Anayasa'nın 17. maddesinin birinci fıkrasının olaya uygulanabilmesi için kişinin itibarına yapılan saldırının belli bir ağırlık düzeyine erişmiş olması gerekmektedir. Ayrıca öngörülebilir şekilde, şeref ve itibarın kendi eylemleri sonucunda zedelenmesi halinde kişinin Anayasa'nın 17. maddesinin getirdiği korumadan yararlanması söz konusu olamaz.

Ancak bu ön koşullar internet üzerinden uzun süredir devam eden yayınlar açısından farklı değerlendirilmelidir. İnternet ortamının sağladığı ulaşılabilirlik, yaygınlık, haber ve fikirlerin depolanmasındaki ve muhafazasındaki kolaylık dikkate alındığında yayımlandığı tarihte belirli ağırlık eşiğini aşmayan veya kişinin kendi eylemlerinden kaynaklanan haberlerin internet ortamında uzun süre erişebilir kalması kişilerin şeref ve itibarını zedeleyebilir; zira haberlerin internet ortamında yayınlanmasının kişisel verilerin korunması hakkı ile ilişkisi bulunmaktadır. Nitekim internet ortamına aktarılırken ve kişi ile haber arasında bağlantı kurulurken teknik olarak kişiye ait verilerin internet ortamına işlenmesi gerekmektedir. Kişisel verilerin işlenmesi 5651 sayılı Kanun kapsamında internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımlanan içerik sağlayıcısı tarafından yapılmaktadır. Bu bağlamda içerik sağlayıcılar, kişisel verileri internet ortamına aktaran ve böylelikle gazete arşivi üzerinden kişiler hakkındaki haberleri ulaşılabilir kılan kişilerdir. Şeref ve itibarın korunması hakkı ile kişisel veriler arasındaki bu ilişki internet ortamında şeref ve itibara yönelik saldırıların, kişisel verilerin korunması hakkı ile bağlantılı olarak değerlendirilmesini gerektirmektedir.

Anayasa'nın 20. maddesinin üçüncü fıkrasında herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı ifade edilmiştir. Maddede ayrıca kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Kişisel verilerin korunması hakkı, kişinin onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Öte yandan kişisel verilerin korunması hakkı sadece kişisel verilerin işlenmesi sırasında değil bu veriler işlendikten sonra da düzeltilmesini veya silinmesini talep etme hakkını içermektedir. Bu hak, sadece kamu otoritesini kullanarak işlenen kişisel verileri değil gerçek ve tüzel kişiler tarafından işlenen verileri de kapsamaktadır. Dolayısıyla internet ortamında yayınlanan bir haberin, Anayasa'nın 17. maddesinin birinci fıkrasında düzenlenen "kişinin manevi varlığının korunması ve geliştirilmesi hakkı" kapsamında kabul edilmesinin yanı sıra, kişinin kimliği ile bağlantı kurularak kişisel bir verinin alenileştirilmesi Anayasa'nın 20. maddesinin üçüncü fıkrasının dikkate alınmasını zorunlu kılmaktadır.

Kişisel verilerin işlenmesi çok geniş bir çerçevede kişisel verilerin açıklanması, kaydedilmesi, aktarılması, elde edilebilir hale getirilmesi, depolanması, muhafaza edilmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi kapsamaktadır. Dolayısıyla internet ortamında yayınlanan bir haberi ulaşılabilir kılan her türlü kişisel verilerin işlenmesi de bu kapsamda değerlendirilmelidir. Her ne kadar kişisel verilerin ancak kanunla veya kişinin açık rızası ile işlenebileceği belirtilmiş ise de Anayasa'da tanımlanan ifade ve basın özgürlükleri kapsamında yapılan bir haberin anılan sınırların istisnası olacağı açıktır.

Haber ve fikirleri iletmedeki hızı ve bunları saklama süresi ve kapasitesi gözetildiğinde internet, geleneksel iletişim araçlarından farklı, küresel olarak bilgiye erişim ve iletişim aracıdır. Dünya çapında milyonlarca kullanıcıya hizmet eden merkezi olmayan bu elektronik iletişim ağı, temel hak ve özgürlüklerin kullanımında farklı bir boyut getirmiştir. Temel hak ve özgürlüklerin kullanımında sağladığı imkânlar aynı zamanda temel hak ve özgürlüklere yönelik farklı müdahale yolları ortaya çıkarmıştır. Özellikle bireylerin özel hayatlarına ve manevi bütünlüklerine yönelik olarak çok ciddi müdahale alanları ortaya çıkmıştır. Bu nedenle geleneksel medyadan farklı olarak internet, ortaya çıkardığı riskler açısından farklı bir bakış açısı ile değerlendirilmelidir. Bu bağlamda ilgili hak ve özgürlükler açısından koruma ve ilerleme sağlayabilmek için kaçınılmaz olarak teknolojik gelişmeleri de dikkate

alacak farklı bir yaklaşım belirlenmelidir. İnternetin yaygınlaşmasından önce kişilerin geçmişlerine ilişkin özel yaşamları zaman içinde kaybolmaktaydı. Bununla birlikte bireylerin geçmişlerinde yaşadıklarına ilişkin herhangi bir kayıt tutulmuşsa da bu kayıtlara ulaşılmasının zorluğu kişilerin geçmişlerinde yaptıkları hatalardan bağımsız olarak yaşamlarını sürdürmelerine imkân tanımaktaydı. Ancak günümüzde basit bir internet araştırması, bireylerin geçmişte yaptıkları ve hatırlamak ve/veya hatırlanılmasını istemedikleri hatalarını kolayca ortaya koymaktadır. Bu bağlamda internet ortamı, arşivde kalmış ve sadece araştırmacıların veya meraklıların özel çabası ile tespit edilebilecek haberleri kolaylıkla ulaşılabilir hale getirmiştir. Haber arşivlerine erişimin kolaylaşması kişiler hakkında yapılan haberin unutulmasına fırsat vermeyen bir sanal ortam meydana getirmiştir. Bu durum internetin yaygınlığı ile birlikte değerlendirildiğinde bireylerin geçmişte yaptıkları ve hatırlanmasını istemedikleri hususların sürekli olarak kişilerin karşısına çıkması ihtimalini kuvvetlendirmiştir.

İnternetin yaygın kullanımı ile ortaya çıkan bu durum basının interneti etkin olarak kullanmasıyla beraber ifade ve basın özgürlükleri ile şeref ve itibarın korunması arasındaki dengeyi ilkinin lehine bozmuştur. İfade ve basın özgürlüğü ile şeref ve itibarın korunması hakkı, eşit düzeyde koruma gerektiren temel hak ve özgürlüklerdir. Bu nedenle bozulan dengenin her iki temel hak arasında tekrar kurulması zorunluluk olmuştur. İnternet haberciliği ile birlikte unutulmanın zor olduğu günümüzde anılan dengenin tekrar kurulabilmesi şeref ve itibar yönünden bireylerin unutulma hakkının kabul edilmesi ile mümkün olabilir. Bu bağlamda unutulma hakkı adil dengenin kurulması için vazgeçilmez niteliktedir.

Unutulma hakkı Anayasa'mızda açıkça düzenlenmemiştir. Bununla birlikte Anayasa'nın "Devletin Temel Amaç Ve Ödevleri" başlığı altında düzenlenen 5. maddesinde "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak" ifadesi ile devlete pozitif bir yükümlülük yüklenmiştir. Bu yükümlülük bağlamında Anayasa'nın 17. maddesinde düzenlenen kişinin manevi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa'nın 20. maddesinin üçüncü fıkrasında güvence altına alınan kişisel verilerin korunmasını isteme hakkı ile birlikte düşünüldüğünde, devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğu açıktır. Özellikle kişisel verilerin korunması hakkı kapsamında kişisel verilerin silinmesini talep edebilme hakkı, kişilerin geçmişlerinde yaşadıkları olumsuzlukların unutulmasına imkân tanımayı kapsamaktadır. Dolayısıyla Anayasa'da açıkça düzenlenmeyen unutulma hakkı, internet vasıtasıyla ulaşılması kolay olan ve dijital hafızada bulunan haberlere erişiminin engellenmesi için Anayasa'nın 5., 17. ve 20. maddelerinin doğal bir sonucu olarak karşımıza çıkmaktadır. Diğer taraftan unutulma hakkının kabul edilmemesi, internet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesi nedeniyle manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılmaktadır.

Bununla birlikte unutulma hakkının internet gazete arşivlerindeki her türlü haber yönünden uygulanmasını beklemek mümkün değildir. Nitekim özellikle basın özgürlüğü temelinde gazete arşivinin araştırmacılar, hukukçular veya tarihçiler için önem taşıyan veriler olduğu açıktır. Bu durumda bir internet haberinin unutulma hakkı kapsamında internetten çıkarılabilmesi için yayının içeriği, yayında kaldığı süre, güncelliğini yitirme, tarihsel bir veri olarak kabul edilememe, kamu yararına katkısı (toplumsal açıdan haberin değeri, haberin geleceğe ışık tutan niteliği) habere konu kişinin ünlü olup olmadığı, haber veya makalenin konusu, bu bağlamda haberin olgusal gerçekler ya da değer yargısı içerip içermediği, halkın ilgili veriye yönelik ilgisi gibi hususların her somut olay açısından incelenmesi gerekmektedir. Bu nedenle unutulma hakkı bağlamında ifade ve basın özgürlükleri ile şeref ve itibarın korunması hakkı arasındaki dengenin sağlanması için tedbirlerin alınması şarttır. Ancak alınacak tedbirlerin Anayasa'nın 13. maddesi gereğince ölçülülük kriteri esas alınarak yapılması gereklidir. Nitekim kişinin şeref ve itibarına yönelik müdahaleleri unutulma hakkı gereğince engellemek için arşivde arama yapmaya imkân tanıyan haber ile kişi arasında ilişki kuran kişisel verilerin silinmesi, haberin anonim hale getirilmesi, haber içeriğinin bir kısmına erişimin engellenmesi gibi birçok yöntem benimsenebilir. Bu bağlamda yargının görevinin, internet ortamı-

nın sağladığı kolaylıkla zamanla kişilerin itibarına yönelik müdahale oluşturan haberleri tamamen ortadan kaldırarak geçmişte meydana gelmiş olayların yeniden yazılmasını sağlamak olmadığı dikkate alınmalıdır. İnternet haber arşivinin bir bütün olarak basın özgürlüğünün koruması altında olduğu unutulmamalıdır. Gerçekten de haber ve fikirlerin iletilmesinde ve alınmasında önemli bir işlev gören internet, Anayasa'nın 26. maddesinde düzenlenen ifade özgürlüğünün güvencesi altındadır. Nitekim Anayasa Mahkemesi internet erişimine yönelik bir müdahalenin ifade özgürlüğü kapsamında incelenmesi gerektiğini daha önceki kararlarında kabul etmiştir. Öte yandan internet üzerinden her türlü haber ve görüşlerin iletilmesinin Anayasa'nın 28 ila 32. maddelerinde güvence altına alınan basın özgürlüğü kapsamında olduğunun kabulü mümkün değildir.

Ulaşılabilirliği, haber ve fikirlerin saklanma süresi ve kapasitesi ile hacimce büyük haber ve fikirleri iletme imkânı gözetildiğinde internet, halkın haber almasının ve bilgilerin iletilmesinin gelişiminde önemli bir role sahiptir. İnternet, herhangi bir sınırlama gözetmeksizin herkesin haber ve fikirlere ulaşması ile fikirlerini yayması noktasında çok önemli bir imkân sağlamaktadır. Bu durum ifade özgürlüğü açısından da çok geniş bir alan yaratmaktadır. Ancak internetteki bu geniş faaliyet alanı çerçevesinde, yayımlanan haber ve fikirlerin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü kapsamında değerlendirilip değerlendirilemeyeceği, her somut olay açısından ayrıca incelenmelidir. Bu kapsamda Anayasa'nın 28. maddesi ve devamı maddelerinde tanımlanan basın özgürlüğü her ne kadar temel olarak basılı kitle iletişim araçları çerçevesinde tanımlanmış ise de internette önemli bir yer işgal eden internet haberciliğinin, basının temel işlevi olan "gözetleyicilik" görevini yerine getirdiği sürece basın özgürlüğü kapsamında değerlendirilebilmesi mümkündür. Başvuru konusu olayda başvurucu hakkında haberleri internette yayımlayan şirketin ülkemizde bilinen ve ulusal ölçekte yayımlanan bir gazetenin internet yayını olması ve bu bağlamda geleneksel gazeteciliğe yakınlığı ile "gözetleyicilik" görevini yerine getirdiği değerlendirilebilir.

Öte yandan belirlenmesi gereken bir diğer husus, haber arşivinin basın özgürlüğünün korumasından yararlanıp yararlanmayacağıdır. Anayasa Mahkemesi birçok kararında ifade özgürlüğünün sadece düşünce ve fikirleri yayma özgürlüğünü değil haber ve fikirlere ulaşma özgürlüğünü de kapsadığını vurgulamıştır. Bu bağlamda haber ve fikirlerin yayılmasını ve bunlara kamunun ulaşmasını kolaylaştıran internetin toplum hayatındaki önemli rolü yadsınamaz. İnternet üzerinde arşiv oluşturma, aktüalitenin ve haberlerin saklanmasına ve erişilebilirliğine büyük ölçüde hizmet etmektedir. Bu nitelikteki arşivler özellikle doğrudan halkın erişimine açık ve genelde ücretsiz olmaları nedeniyle tarih eğitimi ve araştırma faaliyetleri için kaynak sunmaktadır. Öte yandan demokratik bir toplumda basının ilk işlevi olan "gözetleyici" rolünün bir sonucu da arşivlerin halkın erişimine sunulmasıdır. Bu nedenle internette tutulan arşivlerin, ifade ve basın özgürlükleri kapsamında olduğu açıktır. Dolayısıyla internette yayımlanan ve gazetecilik faaliyeti kapsamında kabul edilen bir haber arşivinin yayından kaldırılması basın özgürlüğüne yönelik bir müdahale teşkil eder. Bu ise kabul edilemez. Basın özgürlüğü, herkes için geçerli ve yaşamsal öneme sahip bir özgürlüktür. AİHM de birçok kez demokratik bir toplumda basının oynadığı temel rolün altını çizmiştir. Her ne kadar başkalarının şöhret ve haklarının korunmasıyla ilgili olarak bazı sınırları aşmaması gerekse de basının, görev ve sorumluluklarının bilincinde olarak kamu yararını ilgilendiren her konuyu iletme görevi vardır. Basının böyle konularda bilgi ve fikir yaymadan ibaret olan görevine kamunun bu fikir ve bilgileri alma hakkı eklenir. AİHM'e göre bu görevi olmasaydı basın, vazgeçilmez "gözetleyicilik" işlevini yerine getiremezdi.

Ancak ifade özgürlüğü ile onu tamamlayan ve ifade özgürlüğünün kullanılmasını sağlayan basın özgürlüğü, Anayasa'da yer alan temel hak ve özgürlükleri sınırlama rejimine tabidir. Anayasa'nın 28. maddesinin dördüncü fıkrasında basın özgürlüğünün sınırlanmasında 26. ve 27. madde hükümlerinin uygulanacağı belirtilmiştir. Böylece basın özgürlüğü, ifade özgürlüğü ile ilgili genel hüküm niteliğindeki 26. madde ile sanatsal ve akademik ifadelerle ilgili 27. maddedeki sınırlama rejimine tabi tutulmuştur. Basın özgürlüğüne yönelik diğer sınırlamalar ise 28. maddenin beşinci ve izleyen fıkralarında yer almıştır. Basının, Anayasa'nın 26., 27. ve 28. maddelerinde sayılan sınırlandırmalardan biri olan "başkalarının şöhret veya haklarının, özel veya aile hayatlarının" korunması için konmuş olan sınırlandırmalara uyması gerekir. Bu itibarla "başkalarının şöhret veya haklarının, özel veya aile

hayatlarının" korunması bağlamında şeref ve itibarın korunması hakkının etki alanını genişletmenin ifade ve basın özgürlüklerinin ihlali sonucunu doğurabileceği hatırda tutulmalıdır.

Öte yandan başkalarının şöhret ve haklarının korunmasıyla ilgili olarak bazı sınırların aşılmaması gerekse de basının, görev ve sorumluluklarının bilincinde olarak kamu yararını ilgilendiren her konuyu iletme görevi olduğu, onun bu tür konularda bilgi ve fikir yaymadan ibaret olan görevine kamunun bu fikir ve bilgileri alma hakkının eklendiği hatırda tutulmalıdır. Bu sebeple Anayasa'nın 17. maddesinin birinci fıkrasında koruma altına alınan şeref ve itibarın korunmasını isteme hakkı ile başvuruya konu internet haber arşivinin Anayasa'nın 28. maddesinde güvence altına alınan basın özgürlüğü ve bu özgürlükle bağlantılı olarak Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğü arasında Anayasa Mahkemesi içtihadında ortaya konulan kriterlere uygun şekilde bir denge kurulması gerekmektedir. Ancak geçmişteki olayların arşivlenmiş olması halinde çatışan haklar arasındaki dengelemenin güncel olaylara ilişkin yapılan haberlerden daha farklı yorumlanması makul kabul edilmelidir. Bu bağlamda, basının yayımladığı haberlerin gerçekliğine ilişkin olarak sorumluluk bilinci ile hareket etmesi gerekliliği, güncel haberlere nazaran doğası itibarıyla eskiyen ve yayımlanması ivedilik ve zorunluluk arz etmeyen geçmişe ilişkin haberler bakımından daha katı görünmektedir. Ancak yapılacak dengelemede haber arşivinin de Anayasa'nın 26. ve 28. maddeleri bağlamında güvence altına alındığı göz önünde tutulmalıdır.

Bütün bu açıklamalardan sonra mahkeme hak ihlali iddiasına konu olan olayı açıklanan ilkeler doğrultusunda değerlendirmiştir: Başvuru konusu olayda, şikâyete konu haberler 1998 ve 1999 yılında başvurucu hakkında yürütülen ceza yargılamasına ilişkindir. Başvurucu bu haberlerin gerçeğe aykırı veya uydurma haber olduğunu ileri sürmemiştir. Başvurucu haberlerin halen arşivde yer alması ve internet üzerinden kolayca ulaşılabilir olması nedeniyle özel ve iş hayatının olumsuz etkilendiğini ve itibarının zedelendiğini belirtmiştir. Öyleyse mevcut olayda başvurucunun, haberlerin halen internette yer alması nedeniyle müdahale edilen şeref ve itibar hakkı ile içeriğin yayından çıkarılması halinde müdahale edilecek olan ifade ve basın özgürlükleri arasında adil bir denge kurulması gerekmektedir. Bu dengenin değerlendirilmesinde somut olay açısından göz önünde bulundurulması gereken önemli bir husus şeref ve itibarın korunması hakkı ve unutulma hakkı karşısında sadece ifade ve basın özgürlüklerinin değil ayrıca kişilerin haber ve fikirlere ulaşma özgürlüğünün de olduğudur. Unutulma hakkı internet ortamında bir haberin uzun süredir kolayca ulaşılabilir olması nedeniyle kişinin şeref ve itibarını zedeleyen bir hale dönüşmesi şeklinde karşımıza çıkmaktadır. Bu hakkın amacı, internetin yaygınlaşması ve sağladığı imkânlar nedeniyle ifade ve basın özgürlükleri ile kişilerin manevi varlığının geliştirilmesi hakkı arasında gerekli hassas dengenin kurulmasını sağlamaktır. O halde bu yol, internet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır. Özellikle ölçülülük ilkesi temelinde yapılacak bir değerlendirme ile internet ortamında haberi ulaşılabilir kılan kişisel verilerin silinerek erişimin engellenmesi gibi yöntemler gözetildiğinde internet ortamındaki arşiv niteliğindeki haberin tamamen silinmeden sonuca ulaşılabilmesi mümkündür. Bu bağlamda bilimsel araştırmalar açısından dijital haber arşivinin tamamen silinerek geçmişteki olayların yeniden yazılması sonucunu doğuracak basın özgürlüğüne yönelik ciddi müdahalelerin ortaya çıkması önlenebilir.

Başvurucu hakkında internet ortamındaki arşivde muhafaza edilen ve kolaylıkla ulaşılabilir kılınan haberler 1998 ve 1999 yılındaki ceza yargılamasına ilişkindir. Bu haberlerin gerçeğe aykırı olduğu ileri sürülmemiştir. Haberler başvurucunun uyuşturucu kullanırken yakalanması ve daha sonrasında yargılanması hakkındadır. Bu bağlamda haberin konusunun, haberin arşivde kolaylıkla ulaşılabilir kılınması için gerekli toplumsal açıdan haber değerinin devam ettiği veya haberin geleceğe ışık tutacak nitelikte bir haber olduğu söylenemez. Başvuru tarihi itibarıyla söz konusu haberin yaklaşık on dört yıl önceki bir olaya ilişkin olduğu ve böylelikle güncelliğini yitirdiği açıktır. Haberin içeriği açısından uyuşturucu kullanımı ile ilgili bir haberin tarihi, istatistiksel veya bilimsel amaçlarla internet ortamında kolaylıkla ulaşılabilirliğinin sağlanmasının zorunlu olduğu da söylenemez. Bu bağlamda kamu yararı bakımından siyasi veya medyatik bir kişiliğe sahip olmayan başvurucu hakkında internet ortamında yayınlanan haberlerin kolaylıkla ulaşılabilirliğinin başvurucunun itibarını zedelediği açıktır.

Sonuç olarak başvurucu hakkında yapılan haberler unutulma hakkı kapsamında değerlendirilmesi gereken haberlerdir. İnternet ortamının sağladığı kolaylıklar gözetildiğinde başvurucunun şeref ve itibarının korunması için anılan habere erişimin engellenmesi gerekmektedir. Bu bağlamda erişiminin engellenmesine yönelik talebin reddedilmesiyle ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu söylenemez. Açıklanan gerekçelerle başvurucunun şeref ve itibarını koruma hakkının ihlal edildiği sonucuna varılmıştır.

HGK'nun Unutulma Hakkı Kararı

Gerek ABAD gerekse de AYM kararlarında unutulma hakkına ilişkin bütün açıklamalar dijital hafızada yer alan kişisel içeriklere ilişkindir. Ancak HGK unutulma hakkına yeni bir boyut getirerek, bu hakkın sadece dijital ortamda yer alan kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan her türlü kişisel verilere yönelik olarak da kabul edilmesi gerektiğine vurgu yapmıştır.

dikkat

HGK, diğer yargı organlarından farklı olarak unutulma hakkını sadece internet ortamında yer alan kişisel veriler için değil, offline işlenen kişisel veriler için de kabul etmiştir.

Karara konu olan olayda davacı 2006 yılında gerçekleşen mağduru olduğu cinsel saldırı eylemi nedeniyle şikayetçi olmuş, yapılan yargılama sonucunda yerel mahkemece verilen karar 2009 yılında Yargıtay tarafından onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama aşamasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar, mağdur ve sanığın ismi rumuzlanmaksızın 2010 yılında yayınlanan bir kitapta yer almıştır. Davacı bir ceza hukuku kitabında isminin rumuzlanmaksızın aynen kullanılması üzerine kişilik haklarının ihlal edildiği ve bu nedenle manevi zarara uğradığı iddiasıyla tazminat davası açmış; yerel mahkeme rumuzlanmaksızın kişinin ismine bir kitapta yer verilmesinin kişilik haklarını zedelediğini gerekçesiyle manevi tazminat talebinin kısmen kabulüne karar vermiştir. Temyiz üzerine Yargıtay 4. Hukuk Dairesi "bilimsel bilgi, taşıdığı özellikler dolayısıyla fikir üretiminin en yüce değer ve biçimi olma niteliğine haizdir ve her şeyden önce, insanlığın gerçekliğe ulaşması bakımından önemli bir araç sayılır. Bu durum, bilimsel bilgi ve onu üreten araştırmacının geniş bir özgürlük alanında bulunmasını gerektirir. Bilimi serbestçe öğrenme, araştırma, yayma ve öğretme haklarını içeren bilim özgürlüğü Anayasada kişisel haklar arasında düzenlenmiştir. Bu bağlamda bilimsel özgürlük, bilimsel bir etkinlikte bulunan veya böyle bir faaliyette bulunmak isteyen tüm bireylere tanınmış ve bu bireylerin kişiliğine sıkı sıkıya bağlı kalmış, öznel temel haktır. Taşıdığı önem dolayısıyla insan hakları belgelerine giren bilim özgürlüğü, araştırma özgürlüğünü, araştırma için zorunlu araçlara ve ortama sahip olma hakkını ve bilimsel üretme özgürlüğü veya bilgilendirme ve yayın hakkını içerir. Bu çerçevede bilim adamı bilimsel metotlarını kullanarak araştırma yapma hakkına ve bu araştırmanın sonuçlarını yayma hakkına sahip olacak, kural olarak bu konularda dış bir engelle karşılaşmayacaktır. Hatta bu konularda karşılaşacağı maddi ve manevi engeller devlet tarafından ortadan kaldırılacaktır. Düşünce özgürlüğünün bir alt kategorisi olan fakat, üretilmesindeki özel çabanın ya da emeğin doğal sonucu olarak, sıradan düşünceye göre daha sistematik ve derin sayılması gereken bilimsel eserler, kural olarak ancak kendi ilkeleri çerçevesinde sınır tanırlar ve istisnaen ancak insan yaşamına yönelen bir tehlike olasılığında kısıtlanabilirler. Bunun ötesine geçilerek yapılan sınırlamalar, toplumun bilimsel düşüncelerle buluşmasını önleyebilecek ve dolayısıyla gerçekliğe ulaşılmasını engelleyebilecektir. Bu bakımdan bilimsel özgürlük hukuki rejim ve yaptırım açısından diğer entelektüel özgürlüklere göre daha mutlak bir özgürlük rejiminden yararlanmasını gerektirir. Fakat tüm özgürlüklerde olduğu gibi bilimsel özgürlük de sınırsız değildir. Bilim özgürlüğü ile kişilerin, kişilik değerlerinin karşı karşıya geldiği durumlarda somut olaydaki

olgular itibariyle koruma altına alınmış bulunan bu iki değerden birinin diğerine üstün tutulması gerekecektir. Davaya konu olayda; bilimsel araştırma özgürlüğü kapsamında, aleniyet kazanmış ve kamu malı haline gelmiş Yargıtay ilamı, tarafların isimleri kodlanmadan davalıların yazmış oldukları Yorumlu-Uygulamalı Türk Ceza Kanunu adlı altı ciltlik bilimsel çalışma ürünü olan kitapta yayınlanmıştır. Adı geçen eserin bilimsel nitelikli bir çalışma olduğu, kamuya açık hale gelen Yargıtay kararının bilimsel çalışma ürünü olan kitapta olduğu gibi yer almasından dolayı yukarıda anlatılan ilkeler gereği davalıların sorumlu tutulamayacağı, çatışan yararlar dengesinin davacı aleyhine bozulmadığı, bu olayın davacının kişilik haklarına saldırı teşkil etmeyeceği gözetilerek davanın tümden reddine karar verilmesi gerekirken, yazılı biçimde karar verilmiş olması usul ve yasaya uygun düşmediğinden kararın bozulması gerekmiştir" diyerek yerel mahkemenin kararını bozmuştur. Dosyanın yerel mahkemeye gönderilmesi üzerine yeniden yapılan yargılama sonucunda; yerel mahkeme önceki gerekçelerine dayanarak kararında direnmiştir. Direnme nedeniyle dava Hukuk Genel Kurulu(HGK) önüne gelmiştir.

Yargıtay 4. Hukuk Dairesi'nin bilim özgürlüğüne dair yaptığı açıklamalar doğru olmakla birlikte, ulaştığı sonuca katılmak mümkün değildir; zira hakkın kullanılması ile işlenen haksızlık arasında bir mantıki bağlantı bulunmalıdır ve hakkın sınırı aşılmamalıdır. Mantıki bağdan kasıt, fiilin, hakkın kullanılabilmesi açısından en azından bir faydasının olması, hakkın kullanımına katkı sağlamasıdır. Oysa tacize uğrayan kişinin kimlik bilgilerinin verilmesi, eserin bilimsel içeriğine herhangi bir katkı sağlamamaktadır; bu nedenle de özel hayatın gizliliğine orantısız bir müdahale teşkil etmektedir. Hukuki konularda bilimsel eser yazılmasının amacı, teorisyenleri ve uygulamacıları konuya dair hukuki sorunlar hakkında bilgilendirmek olup, olaya karışan kişilerin kimlikleri ve diğer şahsi verilerin kamunun bilgisine sunulması bu amaca dahil ve bunu gerçekleştirmeye uygun değildir. Nitekim öğretide de haklı olarak, mağdurun isim bilgisinin, unutulma hakkı anlamında "sonradan tamamen ilgisiz hale gelmiş veri" olarak kabul edilmesi gerektiği belirtilmiştir (Önok, 2017: 7738).

HGK da bu düşüncelerden hareketle olsa gerek, yerel mahkemenin direnme kararını şu gerekçelerle haklı bulmuştur. "Unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır. Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak ifade edilebilir. Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır. Somut olaya bu kapsamda bakıldığında; davacı, kamu görevinin veya hizmet ilişkisinin sağladığı nüfuzu kötüye kullanarak, müteselsilen cinsel saldırı suçunun mağdurudur. 2006 yılında gerçekleşen eylem tarihinde davacı bekar olup maruz kaldığı eylem geleceği açısından etkilidir. Yapılan yargılama sonunda kamu görevlisi olan sanık ceza almıştır. Temyiz istemi üzerine yapılan inceleme sonunda ise hüküm 2009 yılında onanmıştır. Mağdur davacı gerek hazırlık gerekse de yargılama sırasında cinsel saldırının nasıl gerçekleştiğini açık bir şekilde anlatmış, bu anlatımlar doğal olarak karar metnine geçirilmiştir. Karar mağdur ve sanığın ismi rumuzlanmadan 2010 yılı nisan ayında yayınlanan kitapta yer almıştır. Davacı, geçmişte

yaşadığı kötü bir olayın toplum hafızasından silinmesini istemektedir. Unutulma hakkı ile geçmişindeki yaşanan talihsiz bir olayın unutularak geleceğini serbestçe şekillendirmek, diğer bir deyişle hayatında, yeni bir sayfa açma olanağı istemektedir. Kaldı ki, davacı da yargılama sırasında verdiği dilekçelerinde bu istem üzerinde ısrarla durmuştur. Davacı unutulma hakkı ile özel hayatına ilişkin kişisel verilerinin üçüncü kişiler tarafından bilinmemesini, aradan geçen süre nedeniyle toplum hafızasından silinmesini istemektedir. Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. İlgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır."

Öğrenme Çıktısı

3 Unutulma hakkına ilişkin ABAD, AYM ve HGK tarafından verilmiş kararları tartışabilme

Araştır 3	İlişkilendir	Anlat/Paylaş
ABAD'ın unutulma hakkına ilişkin kararının esas noktalarını kısaca belirtiniz.	Unutulma hakkının sadece dijital ortamda yer alan kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan her türlü kişisel verilere yönelik olarak da kabul edilmesinin gerekip gerekmediğini HGK kararı çerçevesinde değerlendiriniz.	Unutulma hakkı ile diğer temel hak ve özgürlükler arasındaki ilişkiyi AYM kararı çerçevesinde anlatınız.

UNUTULMA HAKKINA İLİŞKİN ULUSAL MEVZUAT

Ülkemizde unutulma hakkına ilişkin spesifik bir düzenleme bulunmamaktadır. Ancak Regülasyonun 17. maddesinde düzenlenen hükmün göz önünde bulundurulması ve unutulma hakkının 6698 sayılı Kanun'da yapılacak değişiklik ile açıkça düzenlenmesi üzerinde düşünülmesi gereken bir husustur. Böylesi bir düzenleme mevcut olmadığında dahi, mevzuatımızda unutulma hakkının temeli sayılabilecek ve/veya bu hakkın kullanılmasına hizmet edebilecek bazı hukuki düzenlemelerin bulunduğu da belirtilmelidir. Gerçekten de unutulma hakkının temeli olarak sayılabilecek olan hukuk devleti ilkesi (m.2), bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı (m.17), özel hayatın gizliliği hakkı (m.20), konut dokunulmazlığı (m.21), haberleşmenin gizliliği (m.22), dini ve vicdani kanaatleri açıklamaya zorlanamama (m.24), düşünce ve kanaatleri açıklamaya zorlanamama (m.25) gibi anayasal düzenlemeler Türkiye Cumhuriyeti Anayasası'nda yer almaktadır.

dikkat
Unutulma hakkı ulusal mevzuatımızda açıkça düzenlenmemiştir.

Anayasa da yer alan düzenlemelerin haricinde, kanunlarımızda da unutulma hakkıyla benzer sonuç doğurması muhtemel düzenlemeler yer almaktadır. Bu noktada konuyu yukarıdaki mahkeme kararları bağlamında ikiye ayırarak incelemek doğru olacaktır.

Arama motorları aracılığıyla yapılan aramalarda gösterilen arama sonuçlarından, kişisel verilerin yer aldığı web sayfalarına ait linklerin karartılması hususunda ülkemiz yargı organlarınca, ABAD kararı göz önünde bulundurularak, verilmiş bir karar bulunmamaktadır. Ancak 6698 sayılı Kanun aynen Direktif gibi, arama motoru işletmecilerin de veri sorumlusu olarak kabul edileceğini (m. 3/ı) ve kişisel verilerin işlenmesinin ancak işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmasını gerektiğini ve bu işlemenin de gerekli olan süre kadar muhafaza edilmesi gerektiğini belirtmektedir (m. 4/ç ve d). Kanun ayrıca işlemenin bu şartları taşımaması halinde, kişisel verilerin ilgilinin talebiyle silineceğini de hüküm altına almıştır (m. 7). Ayrıca Kanun'a göre ilgili kişi, kişisel verilerin eksik ya da yanlış olması halinde bunların düzeltilmesini isteme hakkına sahiptir (m. 11). Dolayısıyla ulusal mevzuatımız, unutulma hakkı çerçevesinde, Türkiye'den internete giren internet kullanıcılarına en az Avrupa'dan internete giren internet kullanıcılarına sağlanan haklar kadar güvenceler sunmakta ve böylece ilgili kişilerin unutulma hakkı çerçevesinde arama motoru işletmecilerine doğrudan başvuru yapabilmesini güvence altına almaktadır. Bu nedenle yüksek yargı organlarımızın, önlerine gelebilecek olaylarda unutulma hakkının bu tür şirketlerin faaliyetleri açısından da tanıması gerektiği şeklinde içtihat oluşturması için hukuki düzenlemeler mevcuttur.

Kişisel verilerin yer aldığı web sayfalarının içeriğinin silinmesi ve/veya engellenmesi hususunda da ulusal mevzuatımızda açık hüküm bulunmamakla birlikte, bu sonucu doğuracak normlar mevcuttur. Bu noktada yine 6698 sayılı Kanun göz önünde bulundurulmalıdır; zira her ne kadar bu Kanun'da unutulma hakkı adı altında bir düzenleme bulunmasa da Kanun'un 7. ve 11. maddelerinde "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi" hususları düzenlenmiştir. Bu hükümlerin unutulma hakkıyla benzer sonuç doğurması muhtemeldir. Hatta Kanun'un 17. maddesinin 2. fıkrasına göre kişisel verileri silmeyen veya anonim hale getirmeyenler Türk Ceza Kanunu (TCK) m. 138'e göre cezalandırılacaktır. Yine unutulma hakkının kullanılmasının, Türk Medeni Kanunu'nun (TMK) 23-25. maddelerinde yer alan kişiliğin korunmasına ilişkin hükümlere ve Türk Borçlar Kanunu'nun (TBK) 49 ve devamındaki haksız fiiller nedeniyle doğan sorumluluğu düzenleyen maddelere dayanılarak sağlanması mümkündür. Ancak altının çizilmesinde fayda olan husus şudur: Bu maddeler yayınlanan olayın gerçek olmaması, olayın güncel bulunmaması, olayın açıklanmasında kamu yararının bulunmaması, olayın bilinmesinin kamunun ilgisini çekmemesi, haber ile kullanılan ifadeler arasında fikri bir bağın varlığının mevcut olmaması halinde uygulama alanı bulmaktadır.

İçeriğin engellenmesi ve/veya silinmesi yoluyla unutulma hakkının kullanılmasına ilişkin mevzuatımızda yer alan en önemli madde, "içeriğin yayından çıkarılması ve engellenmesi" başlığını taşıyan 5651 sayılı Kanun'un 9. maddesidir. İlgili hüküm şöyledir: "(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir. (2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır. (3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hakim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir. (4) Hakim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hakim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi halinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir. (5) Hakimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir. (6) Hakim bu madde kapsamında yapılan başvuruyu en geç yirmi dört

saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir. (7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hakim kararı kendiliğinden hükümsüz kalır. (8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhal, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir. (9) Bu madde kapsamında hakimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi halinde mevcut karar bu adresler için de uygulanır. (10) Sulh ceza hakiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır."

Yine aynı Kanun'un 9/A maddesinin de bir nev'i benzer işlev görebileceği düşünülebilse de unutulma hakkının özel hayatın gizliliği nedeniyle erişimin engellenmesinin içeriğinden daha geniş olduğu, diğer bir ifadeyle unutulma hakkı kapsamında silinmesi talep edilebilecek içeriğin kapsamanın çok daha geniş olduğu aşikardır.

Bilindiği üzere 5651 sayılı Kanun'un 9. maddesi 2014 yılında 6518 sayılı Kanun'un 93. maddesi ile önemli değişikler geçirmiştir. Bu değişikler sonucu 5651 sayılı Kanun'un 9. maddesinin unutulma hakkının kullanılması için son derece elverişli bir ortam sunduğu kabul edilebilir.

5651 sayılı Kanunun 9. maddesinde yapılan değişiklikten önce uygulamada, güncelliğini yitiren ve yayınlanmaya devam edilmesinde kamu yararı bulunmayan habere konu kişinin önünde zorlu bir süreç bulunmakta idi. Anılan madde hükmünde, hakkında yayınlanan haberin kaldırılması talebinin muhataba iletilmesi, bu talebin ardından iki gün içinde yayının kaldırılmaması halinde sulh ceza mahkemesine başvurulabileceği öngörülmekte idi. Ancak, yayından kaldırma talebi hiçbir muhatap tarafından dikkate alınmamakta, kesinleşmiş bir mahkeme kararı olmaksızın haberin yayından kaldırılmayacağı şeklinde sorumluluk almaktan kaçınan cevaplar verilmekte idi. 6518 sayılı Kanun ile 5651 sayılı Kanunun 9. maddesinde yapılan değişiklikle, kişilerin sulh ceza hakimliğine başvuru yapabilmesi için öncelikle içerik veya buna ulaşılamaması halinde yer sağlayıcıya başvurma zorunluluğu kaldırılmış, doğrudan sulh ceza hakimliğine başvurulabileceği düzenlenmiştir. Ayrıca internet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilen kişilerin taleplerinin, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılacağı düzenlenerek, bu ihlallerin daha kısa sürede önlenebilmesi amaçlanmıştır. Geçmişte yaşanan diğer bir sorun, kişinin hakkında çıkan haberlerin kaldırılması için büyük uğraş vermek zorunda kalması idi. Çünkü bir haber temin edildiği andan itibaren internet ortamında sayısız sitede kopyalanarak yer alabilmektedir. Bu durumla başa çıkmak zor ve hatta bazen imkânsız hale gelebilmekte idi. Kişi hakkında söz konusu haberin yer aldığı internet sitelerinin her birisinin tespit edilmesi ve her bir adres yönünden ayrıca talepte bulunulması gerekliliği, kişilik hakkı ihlalleri ile mücadelede zaman kaybına sebep olmakta, kişiyi manevi yönden olumsuz etkilemekte ve yargının iş yükünü artırmakta idi. 5651 sayılı Kanun'un 9. maddesinde yapılan değişiklikle, sulh ceza hakimliği tarafından bu madde kapsamında verilen erişimin engellenmesi kararına konu yayının başka internet adreslerinde de yayınlanması durumunda, ilgili kişi tarafından Erişim Sağlayıcıları Birliği'ne müracaat edilmesi halinde, mevcut kararın bu adresler için de uygulanacağı düzenlenerek, bu olumsuzlukların giderilmesi amaçlanmıştır.

5651 sayılı Kanun'da yapılan değişiklikler isabetli olmakla birlikte, uygulamada söz konusu maddenin hayata geçirilmesinde bazı sıkıntıların mevcut olduğu da bilinen bir gerçektir; zira 9. maddeye göre yapılan istem yalnızca yurt içinden içerik sağlayan ve/veya yer sağlayanlar için uygulama alanı bulabilmektedir. Yurt dışından kişilik haklarını ihlal eden yayınlar yapanlar ve/veya şirket merkezi yurt dışında bulunan yer sağlayıcılar (örneğin Facebook, Twitter) hem yasanın uygulama alanı açısından hem de bunlara yaptırım uygulanmasının olanaksızlığı bakımından yasanın kapsamı dışında bulunmaktadır. Ancak bu tür eksiklikler yasa koyucunun elinde olan imkânlarla çözebilece-

ği hususlar değildir. Aksine bu durum konunun uluslararası boyutunu ortaya koymakta, internetle ilgili hususlarda uluslararası adli yardımlaşmanın önemine dikkat çekmekte ve daha da önemlisi ulusal mahkemelerin ve diğer ulusal mercilerin uluslararası yer sağlayıcıları ile doğrudan irtibat kurabilmesinin ne denli önemli olduğunu belli etmektedir. Bu noktada Türkiye'nin, internetin büyük aktörleri şirketlere, yurt içi irtibat büroları kurmaları yönündeki çağrısının, sadece unutulma hakkının kullanılabilmesi için değil, bilişim hukukuyla kesişen diğer tüm hukuk dallarında yaşanan problemlerin hızlı çözümü için de doğru ve önemli bir adım olduğunun altı çizilmelidir.

Öğrenme Çıktısı

4 Mevzuatımızda yer alan normları unutulma hakkı çerçevesinde değerlendirebilme

Araştır	İlişkilendir	Anlat/Paylaş
Unutulma hakkının kullanılmasına ilişkin mevzuatımızda yer alan en önemli madde hangisidir?	6698 sayılı Kanun ile AB normları arasındaki ilişki çerçevesinde, arama motoru işletmecisine doğrudan başvurunun ulusal mevzuatımıza göre mümkün olup olmadığını değerlendiriniz.	Unutulma hakkının ulusal mevzuatımızda açıkça düzenlenmesinin gerekip gerekmediğini anlatınız.

öğrenme çıktıları ve bölüm özeti

1 İnternete erişim hakkını insan hakları teorisi çerçevesinde açıklayabilme ve dördüncü kuşak insan haklarını tanımlayabilme

İnsan Hakları Teorisine İlişkin Temel Bilgiler

İnsan hakları, kişinin sırf insan olduğu için sahip olduğu haklardır. Anayasa'nın 12. maddesi "herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez haklara sahiptir" diyerek bu hakların niteliğini açıklamıştır. İnsan hakları öğretisinin oluşmaya başladığı tarihten bu yana, insan haklarını sayan ve sınıflandıran çok sayıda liste ortaya çıkmıştır. Bunlardan en önemlisi Karel Vasak tarafından ortaya konan üç kuşak haklar teorisidir. Birinci kuşak hakların temel özelliği, kişilere, devletin karışmayacağı özel bir alan yaratmasıdır. İkinci kuşak haklar, devlete karışmama ödevi değil, aksine eylemde bulunma, harekete geçme yani hizmet sağlama ödevi yüklemektedir. Üçüncü kuşak haklar ise ilk iki kuşak haklardan farklı olarak belirli bir grubun değil, bir toplumdaki tüm sosyal grupların ihtiyaçlarına cevap vermeyi amaçlayan haklardır. Üçüncü kuşak haklara örnek olarak "internete erişim hakkı" verilebilir.

Son yıllarda dördüncü kuşak insan haklarından bahsedilmektedir. Bunlar bilişim teknolojisinde yaşanan gelişmelerin insan onurunun korunması bakımından yarattığı riskler nedeniyle ortaya çıkmıştır. Bu bağlamda, dördüncü kuşak hakların bilimin ve teknolojinin olası kötüye kullanımına karşı insan onurunun korunması amacına dayandığı kabul edilmektedir. Diğer bir ifadeyle bilişim teknolojisinin günümüzde eriştiği düzeyin ortaya çıkardığı, insan onurunu tehdit eden yeni tehlikelere karşı yeni hakların güvence altına alınması veya mevcut hakların yeni durumları kapsayacak biçimde ek güvencelerle desteklenmesi dördüncü kuşak hakların tanınmasının temel nedenidir. 2010 Anayasa Referandumu ile kabul edilen 2010 değişikliğiyle, dördüncü kuşak haklardan biri olarak kabul edilen kişisel verilerin korunması hakkı, ülkemizde de anayasal güvenceye bağlanmıştır (m. 20/3).

2 Unutulma hakkını genel olarak tanımlayabilme, bu hakkın normatif dayanağını belirtebilme ve diğer temel hak ve özgürlükler ile ilişkisini açıklayabilme

Unutulma Hakkı

Dördüncü kuşak haklardan kabul edilen unutulma hakkı, bireyin dijital hafızada yer alan kişisel verilerinin kendi talebi üzerine bir daha geri getirilemeyecek şekilde ortadan kaldırılması şeklinde tanımlanmaktadır. Bireylerin hayatlarında yeni bir sayfa açma hakkı bulunduğunun kabulü unutulma hakkının çıkış noktasıdır.

Unutulma hakkı, 2016/679/EU sayılı "Gerçek Kişilere Dair Kişisel Verilerin İşlenmesine ve 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktifin Kaldırılmasına Dair Regülasyon"nun ya da bilinen adıyla Genel Veri Koruma Regülasyonu'nun (Generel Data Protection Regulation/GDPR) 17. maddesinde düzenlemeden önce herhangi bir kadar normatif bir dayanağa sahip olmayan, yargı organlarının içtihatlarıyla insan hakları teorisine kazandırılmış bir haktır.

Unutulma hakkı ile bu hakkın çatıştığı diğer haklar arasındaki ilişki şu şekilde özetlenebilir: Kamu yararı ile birey yararı arasındaki denge, ilk bakışta güncellik, görünür gerçeklik, kamuoyu ilgisi sebebiyle haber, fotoğraf ve görüntülerin üçüncü kişilerin bilgisine sunulması lehine kurulduğu halde; unutulma hakkı sayesinde bu bilgilerin güncelliğini yitirdiği andan itibaren denge bu defa birey lehine değişmektedir.

3 Unutulma hakkına ilişkin ABAD, AYM ve HGK tarafından verilmiş kararları tartışabilme

Unutulma Hakkına İlişkin Yargı Kararları

ABAD unutulma hakkını kabul etmiş ve hakkın şartlarını ve sınırlarını şu şekilde belirlemiştir: 1. Arama motoru faaliyeti, kişisel verilerin işlenmesi ve arama motoru işletmecisi de veri sorumlusu olarak kabul edilmelidir. 2. Bireyler kendilerine tanınan temel hak ve özgürlüklerden, özellikle mahremiyet hakkından, tam olarak faydalanabilmek için, arama motoru işletmecisine doğrudan başvuru yapabilmelidir. Bu yöndeki bir hakkın doğması için ilgili kişiye ait kişisel verilerin önceden veya eş zamanlı olarak web sitesinden çıkartılması veya arama motoru işletmecisinin ilgili sayfanın webmasterına bu hususta bilgi vermesi gerekmemektedir. Dolayısıyla ilgili kişiler linklerin kaldırılmasını, kişisel verilerin doğru ve güncel olarak tutulmaması veya kişisel verilerin toplanma veya işlenme amacı için gerekli olan süreden daha uzun süre saklanması halinde isteyebilirler. 3. İlgili kişi arama sonuçlarında yer alan linklerin kaldırılmasını, bu linklerin içeriğinde kendisiyle ilgili gerçek bilgilerin bulunması halinde dahi isteyebilecektir. 4. Kişinin genel olarak geçmişiyle bağlı kalmama hakkı mevcuttur. Bu bakımdan ilgili kişinin ilgili linkin kaldırılmasını isteyebilmesi için, kişinin linkin içeriğinden dolayı zarar görmesi veya böyle bir tehlikeyle karşı karşıya kalması gerekmemektedir. 5. Kişisel verilerin yayınlanmasının hukuka aykırı olması gerekmemektedir. 6. Unutulma hakkı çerçevesinde yapılan başvurularda unutulma hakkı ile çatışan diğer temel hak ve özgürlükler arasında denge kurulmalıdır. İlgili verinin kamu hayatında oynadığı rol veya halkın ilgili veriye yönelik meşru yoğun ilgisi gibi üstün bir kamu yararını ortaya koyan özel sebepler mevcut olmadığı sürece, unutulma hakkı arama motoru işletmecileri tarafından her türlü makul tedbirlerin alınması suretiyle sağlanmalıdır.

ABAD kararı arama motoru işletmecilerinin sorumluluğuna ilişkindir. Kararın konusu kişisel verinin kendisinin ilgili sayfadan silinmesi değil, arama motorunda yer alan sonucun karartılmasıdır. Diğer bir deyişle ABAD kararı, arama motorlarından kişisel verilere link içeren sonuçların silinmesine dairdir. Buna karşın unutulma hakkı, daha geniş şekilde, geçmişine dair bir bilgiyle bir kimsenin süresiz olarak bağlantılı kılınmama hakkı olarak da ele alınabilir. İşte AYM'nin unutulma hakkı kararı bu anlamda oldukça değerlidir. Bu kararda AYM, haber arşivinin içeriğinin de unutulma hakkı çerçevesinde silinebileceğini belirtmiştir.

Gerek ABAD gerekse de AYM kararlarında unutulma hakkına ilişkin bütün açıklamalar dijital hafızada yer alan kişisel içeriklere ilişkindir. Ancak HGK unutulma hakkına yeni bir boyut getirerek, bu hakkın sadece dijital ortamda yer alan kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan her türlü kişisel verilere yönelik olarak da kabul edilmesi gerektiğine vurgu yapmıştır.

öğrenme çıktıları ve bölüm özeti

4 Mevzuatımızda yer alan normları unutulma hakkı çerçevesinde değerlendirebilme

Unutulma Hakkına İlişkin Ulusal Mevzuat

Ülkemizde unutulma hakkına ilişkin spesifik bir düzenleme bulunmamaktadır. Ancak yine de unutulma hakkının temeli sayılabilecek ve/veya bu hakkın kullanılmasına hizmet edebilecek bazı hukuki düzenlemeler mevcuttur. Unutulma hakkına ilişkin mevzuatımızda yer alan en önemli madde, "içeriğin yayından çıkarılması ve engellenmesi" başlığını taşıyan 5651 sayılı Kanun'un 9. maddesidir. Uygulamada söz konusu maddenin hayata geçirilmesinde bazı sıkıntıların mevcut olduğu ise bilinen bir gerçektir; zira 9. maddeye göre yapılan istem yalnızca yurt içinden içerik sağlayan ve/veya yer sağlayanlar için uygulama alanı bulabilmektedir. Ancak bu tür eksiklikler yasa koyucunun elinde olan imkânlarla çözebileceği hususlar değildir. Aksine bu durum konunun uluslararası boyutunu ortaya koymakta ve internetle ilgili hususlarda uluslararası adli yardımlaşmanın önemine dikkat çekmektedir. 5651 sayılı Kanun'un 9. maddesinin uygulanmasında yaşanan problemler ayrıca mahkemelerin ve diğer ulusal mercilerin uluslararası yer sağlayıcılar ile doğrudan irtibat kurabilmesinin ne denli önemli olduğunu da belli etmektedir. Bu noktada Türkiye'nin, internetin büyük aktörleri olan şirketlere, yurt içi irtibat büroları kurmaları yönündeki çağrısının, sadece unutulma hakkının kullanılabilmesi için değil, bilişim hukukuyla kesişen diğer tüm hukuk dallarında yaşanan problemlerin çözümü için de doğru ve önemli olduğunun altı çizilmelidir.

1 İnternete erişim hakkının bir insan hakkı olarak tanınması yönündeki en önemli belge aşağıdakilerden hangisidir?

A. Avrupa Birliği Adalet Divanı'nın Google/Unutulma Hakkı Kararı
B. İnsan Hakları Evrensel Beyannamesi
C. Birleşmiş Milletler Raporu
D. İnsan Hakları Avrupa Sözleşmesi
E. Avrupa Birliği Temel Haklar Bildirgesi

2 Kişisel verilerin korunması hakkı kaçıncı kuşak haklar arasında kabul edilmektedir?

A. Üçüncü kuşak haklar
B. Dördüncü kuşak haklar
C. İkinci kuşak haklar
D. Birinci kuşak haklar
E. Beşinci kuşak haklar

3 Üç Kuşak Haklar Teorisi aşağıdakilerden hangisine aittir?

A. Karel Vasak
B. Georg Jellinek
C. Avrupa Birliği Adalet Divanı
D. Anayasa Mahkemesi
E. Hukuk Genel Kurulu

4 Aşağıdakilerden hangisi üçüncü kuşak haklara örnek olarak gösterilebilir?

A. İnanç ve ibadet özgürlüğü
B. Düşünceyi açıklama ve yayma hürriyeti
C. Yaşam hakkı
D. Unutulma hakkı
E. İnternete erişim hakkı

5 Dördüncü kuşak haklarla ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. Bu hakların temel özelliği, kişilere, devletin karışmayacağı özel bir alan yaratmasıdır.
B. Bu haklar devlete karışmama ödevi değil, aksine eylemde bulunma, harekete geçme yani hizmet sağlama ödevi yüklemektedir.
C. Dördüncü kuşak hak mevcut değildir.
D. Bunlar bilişim teknolojisinde yaşanan gelişmelerin insan onurunun korunması bakımından yarattığı riskler nedeniyle ortaya çıkmıştır.
E. Bu haklara dayanışma hakları da denilmektedir.

6 Unutulma hakkı ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır?**

A. Üçüncü kuşak haklardan kabul edilir
B. Dördüncü kuşak haklardan kabul edilir.
C. Kişisel verilerin korunması hakkıyla ilişkilidir.
D. Ülkemizde bu hakka ilişkin spesifik bir düzenleme bulunmamaktadır.
E. Diğer temel hak ve özgürlükler ile bazen kesişme bazen ise çatışma şeklinde ilişki halindedir.

7 Unutulma hakkı aşağıdaki hukuki metinlerin hangisinde açıkça düzenlenmiştir?

A. 2016/680 sayılı "2008/977/JHA Çerçeve Kararı Yürürlükten Kaldıran, Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti Veya Kovuşturulması Veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin Korunmasına Ve Bu Tür Verilerin Serbest Dolaşımına Dair Direktif"
B. 2016/679/EU sayılı "Gerçek Kişilere Dair Kişisel Verilerin İşlenmesine ve 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktifin Kaldırılmasına Dair Regülasyon"
C. 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif"
D. 2006/24/EC sayılı "Veri Saklama Direktifi"
E. Avrupa Birliği Temel Haklar Bildirgesi

8 ABAD kararı uyarınca unutulma hakkıyla ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A. İnternette üçüncü şahıslarca yayınlanmış bilgiyi konumlandırma, otomatik olarak indeksleme, geçici olarak saklama ve son olarak belirli bir tercih sırasına göre internet kullanıcılarına sunulmasından oluşan arama motoru faaliyeti, kişisel verilerin işlenmesi olarak nitelendirilemez.
B. Arama motoru işletmecisi veri sorumlusu olarak kişisel verilerin işlenmesinden sorumlu tutulamaz.
C. Unutulma hakkı çerçevesinde başvuru yapılabilmesi için ilgili kişiye ait kişisel verilerin önceden veya eş zamanlı olarak web sitesinden çıkartılması veya ilgili kişinin kendisine ait bu bilginin çıkartılması için web sitesi sahibine başvurması gerekmektedir.
D. Üçüncü kişilerce yayınlanan verilerin hukuka aykırı olması gerekmektedir.
E. Karar, arama motorlarından kişisel verilere link içeren sonuçların silinmesine dairdir.

9 Ulusal yüksek yargı organlarınca verilen kararlar ışığında unutulma hakkı ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır?**

A. AYM'ye göre bu hak, kişisel verilerin bulunduğu içeriğin kaldırılmasına da olanak sağlamaktadır.
B. HGK'na göre bu hak, sadece dijital ortamda yer alan kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan her türlü kişisel verilere yönelik olarak da kabul edilmelidir.
C. AYM'ye göre bu hak, sadece dijital ortamda yer alan kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan her türlü kişisel verilere yönelik olarak da kabul edilmelidir.
D. AYM'ye göre bu hak, Anayasa m. 20/3'de düzenlenen kişisel verilerin korunmasını isteme hakkı ile bağlantılı olarak Anayasa m. 17/1'de düzenlenen kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı çerçevesinde değerlendirilmelidir.
E. HGK'na göre bu hak, ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığı sürece kabul edilmelidir.

10 Türkiye'de unutulma hakkı ile ilgili spesifik bir düzenleme bulunmamakla birlikte, unutulma hakkıyla benzer sonuç doğurması muhtemel en önemli hukuki düzenleme aşağıdakilerden hangisidir?

A. 4721 sayılı Türk Medeni Kanunu'nun 23 ve devamı maddeleri.
B. 6098 sayılı Türk Borçlar Kanunu'nun 49 ve devamı maddeleri.
C. 5237 sayılı Türk Ceza Kanunu'nun 132 ve devamı maddeleri.
D. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9. maddesi.
E. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nun 9/A maddesi.

1. C	Yanıtınız yanlış ise "İnsan Hakları Teorisine İlişkin Temel Bilgiler" konusunu yeniden gözden geçiriniz.
2. B	Yanıtınız yanlış ise "Dördüncü Kuşak Haklar" konusunu yeniden gözden geçiriniz.
3. A	Yanıtınız yanlış ise "Üç Kuşak Haklar Teorisi" konusunu yeniden gözden geçiriniz.
4. E	Yanıtınız yanlış ise "Üç Kuşak Haklar Teorisi" konusunu yeniden gözden geçiriniz.
5. D	Yanıtınız yanlış ise "Dördüncü Kuşak Haklar" konusunu yeniden gözden geçiriniz.
6. A	Yanıtınız yanlış ise "Unutulma Hakkı" konusunu yeniden gözden geçiriniz.
7. B	Yanıtınız yanlış ise "Unutulma Hakkının Normatif Dayanağı" konusunu yeniden gözden geçiriniz.
8. E	Yanıtınız yanlış ise "ABAD'ın Google/Unutulma Hakkı Kararı" konusunu yeniden gözden geçiriniz.
9. C	Yanıtınız yanlış ise "AYM'nin Unutulma Hakkı Kararı" ve "HGK'nun Unutulma Hakkı Kararı" konularını gözden geçiriniz.
10. D	Yanıtınız yanlış ise "Unutulma Hakkına İlişkin Ulusal Mevzuat" konusunu yeniden gözden geçiriniz.

8 Araştır Yanıt Anahtarı

Araştır 1

Dördüncü kuşak haklar bilişim teknolojisinde yaşanan gelişmelerin insan onurunun korunması bakımından yarattığı riskler nedeniyle ortaya çıkmıştır. Bu bağlamda, dördüncü kuşak hakların bilimin ve teknolojinin olası kötüye kullanımına karşı insan onurunun korunması amacına dayandığı kabul edilmektedir. Bunlara örnek olarak kişisel verilerin korunması hakkı ve unutulma hakkı örnek olarak gösterilebilir.

Araştır 2

Unutulma hakkının normatif temeli 2016/679/EU sayılı Gerçek Kişilere Dair Kişisel Verilerin İşlenmesine ve 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktifin Kaldırılmasına Dair Regülasyonun 17. maddesidir.

8 Araştır Yanıt Anahtarı

Araştır 3

ABAD'a göre arama motoru faaliyeti, kişisel verilerin işlenmesi olarak nitelendirilmeli ve arama motoru işletmecisi de veri sorumlusu olarak bu kişisel verilerin işlenmesinden sorumlu olmalıdır. Bireyler kendilerine tanınan temel hak ve özgürlüklerden, özellikle mahremiyet hakkından, tam olarak faydalanabilmek için, verilerin doğru ve güncel olarak tutulmaması veya verilerin toplanma veya işlenme amacı için gerekli olan süreden daha uzun süre tutulması halinde arama motoru işletmecisine doğrudan başvuru yapabilmelidir. Unutulma hakkı çerçevesinde yapılan başvurularda unutulma hakkı ile çatışan diğer temel hak ve özgürlükler arasında denge kurulmalıdır. İlgili verinin kamu hayatında oynadığı rol ve halkın ilgili veriye yönelik meşru yoğun ilgisi gibi üstün bir kamu yararını ortaya koyan özel sebepler mevcut olmadığı sürece, unutulma hakkı arama motoru işletmecileri tarafından her türlü makul tedbirlerin alınması suretiyle sağlanmalıdır.

Araştır 4

Unutulma hakkına ilişkin mevzuatımızda yer alan en önemli madde, "içeriğin yayından çıkarılması ve engellenmesi" başlığını taşıyan 5651 sayılı Kanun'un 9. maddesidir.

Kaynakça

Akgül, A. (2015). Kişisel Verilerin Korunmasında Yeni Bir Hak: Unutulma Hakkı ve AB Adalet Divanı'nın Google Kararı. *Türkiye Barolar Birliği Dergisi*, 2015(116), ss. 11-38.

Akıncı, A. N. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi*. Kalkınma Bakanlığı, Yayın No: 2968, Ankara.

Başalp, N. (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21(1), ss. 77-103.

Elmalıca, H. (2016). Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 65(4), ss. 1603-1636.

Gören, Z. (2014). İnternet Özgürlüğünün Koruma Alanı ve Sınırları. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 13(26), Güz 2014/2, ss. 9-25.

Gözler, K. (2017). İnsan Hakları Hukuku. Ekin Yayıncılık, Bursa.

Önok, M. (2017). Kişisel Verilerin Korunması Bağlamında Unutulma Hakkı ve Türkiye Açısından Değerlendirmeler. İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, 2017(1), ss. 155-188 (jurix, 7738).

Şen, E. (2016) Unutulma Hakkı. http://www.haber7.com/yazarlar/prof-dr-ersan-sen/2100122-unutulma-hakki.

Uygun, O. (2014). *Devlet Teorisi*. XII Levha Yayıncılık, İstanbul.