



ANADOLU ÜNİVERSİTESİ

e-öğrenme ortamları

Yepyeni deneyimler sunan
birbirinden farklı eğitim materyalleri

etkileşimli e-kitap

Video ve seslerle desteklenmiş bir öğrenme ortamı sunan etkileşimli e-kitap ile öğrenmek artık daha kolay! Masaüstü ve dizüstü bilgisayarlarınızda görüntüleyebileceğiniz etkileşimli e-kitaplara mobil ortamlardan da erişebilirsiniz.

deneme sınavları

Ünite sonu çalışma soruları ve Ara sınav/Dönem sonu deneme sınavları ile kendinizi test edebilirsiniz. Soruları bilgisayar ve mobil cihazlardan görüntüleyebilir, isterseniz yazdırabilirsiniz.

ünite çalışma notları

Üniteyi okuyarak öğrendiklerinizi pekiştirmek ve bilgilerinizi kalıcı hale getirmek için, çalışma notlarından yararlanarak tekrar yapabilirsiniz. Ayrıca çalışma notlarının dökümünü alarak istediğiniz zaman çalışabilirsiniz.

e-seminer

Eşzamanlı e-seminer dersleri ile hepimiz sanal sınıflarda buluşabiliyoruz. Canlı derslerde sorularınızı sorabilirsiniz. Derse katılmadığınızda tüm e-seminerlerin video kayıtlarına istediğiniz zaman erişebilirsiniz.

çıkış sınav soruları

Derslerinize ait geçmiş yıllarda yapılan sınavlarda çıkmış sorulara erişebilirsiniz.

ders anlatım videoları

Derslerinize ait konu anlatım videolarına bilgisayarınızdan veya mobil cihazınızdan istediğiniz zaman istediğiniz yerden ulaşabilir, videoları dilediğiniz kadar izleyebilirsiniz.



444 10 26

0850 200 46 10-19 (10hat)

www.anadolu.edu.tr



[/anadoluuniversitesi](https://www.facebook.com/anadoluuniversitesi)



[/Anadolu_Univ](https://twitter.com/Anadolu_Univ)



[instagram.com/anadoluuniv](https://www.instagram.com/anadoluuniv)

www.eogrenme.anadolu.edu.tr





ANADOLU ÜNİVERSİTESİ



- AÖF sınavları
- sınav giriş belgesi
- sınav sonuçları
- itunes u
- duyurular
- sor/izle/öğren
- ders kitabı
- sesli kitap
- deneme sınavları
- konu anlatım videoları
- TRT okul videoları
- e-seminer dersleri
- takvim



444 10 26

0850 200 46 10-19 (10hat)
www.anadolu.edu.tr

www.eogrenme.anadolu.edu.tr



/anadoluuniversitesi



/Anadolu_Univ



instagram.com/anadoluuniv

T.C. ANADOLU ÜNİVERSİTESİ YAYINI NO: 3220
AÇIKÖĞRETİM FAKÜLTESİ YAYINI NO: 2091

BİLİŞİM HUKUKU

Yazarlar

Arş.Gör. Murat ARABACI (Ünite 1)
Yrd.Doç.Dr. Elif KÜZECİ (Ünite 2, 3)
Doç.Dr. Hakan KARAKEHYA (Ünite 4, 5)
Prof.Dr. Tekin MEMİŞ (Ünite 6, 7)
Av. Burçak ÜNSAL (Ünite 8)

Editör

Yrd.Doç.Dr. Gökhan GÜNEYSU



ANADOLU ÜNİVERSİTESİ

Bu kitabın basım, yayım ve satış hakları Anadolu Üniversitesine aittir.
“Uzaktan Öğretim” tekniğine uygun olarak hazırlanan bu kitabın bütün hakları saklıdır.
İlgili kuruluştan izin almadan kitabın tümü ya da bölümleri mekanik, elektronik, fotokopi, manyetik kayıt
veya başka şekillerde çoğaltılamaz, basılamaz ve dağıtılamaz.

Copyright © 2015 by Anadolu University
All rights reserved

No part of this book may be reproduced or stored in a retrieval system, or transmitted
in any form or by any means mechanical, electronic, photocopy, magnetic tape or otherwise, without
permission in writing from the University.

UZAKTAN ÖĞRETİM TASARIM BİRİMİ

Genel Koordinatör

Prof.Dr. Müjgan Yazıcı Bozkaya

Genel Koordinatör Yardımcısı

Yrd.Doç.Dr. İrem Erdem Aydın

Öğretim Tasarımcısı

Yrd.Doç.Dr. İrem Erdem Aydın

Grafik Tasarım Yönetmenleri

Prof. Tevfik Fikret Uçar

Yrd.Doç. Nilgün Salur

Öğr.Gör. Cemalettin Yıldız

Dil ve Yazım Danışmanı

Okt. Ezgi Aslan

Okt. Gönül Yüksel

Ölçme Değerlendirme Sorumlusu

Biriçim Altınordu

Kitap Koordinasyon Birimi

Uzm. Nermin Özgür

Kapak Düzeni

Prof. Tevfik Fikret Uçar

Öğr.Gör. Cemalettin Yıldız

Grafikerler

Özlem Çayırılı

Ayşegül Dibek

Kenan Çetinkaya

Dizgi

Açıköğretim Fakültesi Dizgi Ekibi

Bilişim Hukuku

ISBN

978-975-06-1843-7

1. Baskı

Bu kitap ANADOLU ÜNİVERSİTESİ Web-Ofset Tesislerinde 4900 adet basılmıştır.
ESKİŞEHİR, Aralık 2015

İçindekiler

Önsöz	ix
-------------	----

Bilişim, İnternet ve Hukuk	2
BİLİŞİM VE BİLİŞİM HUKUKU	3
Bilişim Kavramı	3
Bilişim Kavramının Türk Hukukundaki Gelişimi	4
Bilişim Suçu	4
İNTERNET'İN TANIMI, TARİHİ GELİŞİMİ, YÖNETİMİ VE İNTERNET'LE İLGİLİ BAZI ÖNEMLİ KAVRAMLAR	5
İnternet'in Tanımı	5
İnternet'in Tarihi Gelişimi	6
İnternetin Yönetimi	6
İnternet'le İlgili Bazı Önemli Kavramlar	7
TÜRKİYE'DE İNTERNET'İN YÖNETİMİ; YETKİLİ VE SORUMLU KURUMLAR	11
Ulaştırma Bakanlığı	12
İnternet Kurulu	12
Bilgi Teknolojileri ve İletişimi Kurumu	12
Telekomünikasyon İletişim Başkanlığı	13
TİB'in Kuruluş Amacı	13
TİB'in Bilgisayar Ağlarına İlişkin Görev ve Yetkileri	13
İnternet Daire Başkanlığı	14
Özet	17
Kendimizi Sınayalım	18
Yaşamın İçinden	19
Okuma Parçası	20
Kendimizi Sınayalım Yanıt Anahtarı	22
Sıra Sizde Yanıt Anahtarı	22
Yararlanılan Kaynaklar	23

1. ÜNİTE

Bilişim, İnsan Hakları ve Kişisel Verilerin Korunması.....	24
BİLİŞİM TEKNOLOJİLERİ VE İNSAN HAKLARI	25
KİŞİSEL VERİ VE KİŞİSEL VERİLERİN İŞLENMESİ	27
KİŞİSEL VERİLERİN KORUNMASININ ÖNEMİ	29
KİŞİSEL VERİLERİN KORUNMASI HAKKI	30
Genel Olarak	30
İnsan Onuru, Bireysel Özerklik ve Bilgilerin Geleceğini Belirleme Hakkı	31
Özel Yaşamın Gizliliği Hakkı	32
Düşünceyi Açıklama Özgürlüğü	35
Özel Haberleşmenin Gizliliği	37
Diğer Bazı Hak ve Özgürlükler	38
KİŞİSEL VERİLERİN KORUNMASINDA HÂKİM OLANTEMEL İLKELER..	38
Genel Olarak	38
Kişisel Verilerin Niteliğine İlişkin İlkeler	40
İlgili Kişinin Katılımı ve Denetimine Yönelik İlkeler	40
Özel Kategorideki Verilerin Nitelikli Korunması	41
Veri Güvenliğinin Sağlanması	41

2. ÜNİTE

Bağımsız Organlarca Denetim	42
İstisnalar ve Sınırlamalar	42
Özet	43
Kendimizi Sınayalım	45
Yaşamın İçinden	46
Okuma Parçası	46
Kendimizi Sınayalım Yanıt Anahtarı	47
Sıra Sizde Yanıt Anahtarı	47
Yararlanılan Kaynaklar	48

3. ÜNİTE

Türkiye’de Kişisel Verilerin Korunması..... 50

GİRİŞ	51
TÜRKİYE CUMHURİYETİ ANAYASASI	52
AVRUPA İNSAN HAKLARI SÖZLEŞMESİ	55
TÜRK CEZA KANUNU	57
TÜRK MEDENİ KANUNU	58
TÜRK BORÇLAR KANUNU	58
ELEKTRONİK HABERLEŞME KANUNU	59
ELEKTRONİK TİCARET KANUNU	60
KİŞİSEL VERİLERİN KORUNMASI KANUN TASARISI	60
Özet	65
Kendimizi Sınayalım	67
Yaşamın İçinden	68
Okuma Parçası	68
Kendimizi Sınayalım Yanıt Anahtarı	69
Sıra Sizde Yanıt Anahtarı	69
Yararlanılan Kaynaklar	69

4. ÜNİTE

Bilişim Alanında Suçlar ve Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El

Koyma Tedbiri 70

GİRİŞ	71
BİLİŞİM ALANINDAKİ SUÇLARA İLİŞKİN TÜRKİYE’DE YAŞANAN SÜREÇ	72
BİLİŞİM SUÇLARINA İLİŞKİN TEMEL KAVRAMLAR	73
Genel Olarak	73
BİLİŞİM SİSTEMİ	73
Genel Olarak	73
Şifreli Yayınların Konumu	74
Program ve Veriler	74
İnternet	74
BİLİŞİM SİSTEMİNE GİRME SUÇU	75
Genel Açıklamalar	75
Suçla Korunan Hukuki Değer	75
Tipik Maddi Unsur	76
Tipik Manevi Unsur	77
Hukuka Aykırılık	78
Kusurluluk	78
Suçun Özel Görünüş Biçimleri	79

Teşebbüs	79
İştirak	79
İçtima	79
Ceza	80
SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU	81
Genel Açıklamalar	81
Suçla Korunan Hukuki Değer	81
Tipik Maddi Unsur	81
Tipik Manevi Unsur	83
Hukuka Aykırılık	83
Kusurluluk	84
Suçun Özel Belirîş Biçimleri	84
Teşebbüs	84
İştirak	84
İçtima	84
Ceza	85
BANKA VE KREDİ KARTLARININ KÖTÜYE KULLANILMASI SUÇU	85
Genel Olarak	85
Suçla Korunan Hukuki Değer	86
Tipik Maddi Unsur	86
Tipik Manevi Unsur	88
Hukuka Aykırılık	88
Kusurluluk	88
Şahsi Cezasızlık Sebepleri	88
Etkin Pişmanlık	88
Suçun Özel Belirîş Biçimleri	89
Teşebbüs	89
İştirak	89
İçtima	89
Ceza	90
BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE EL KOYMA	90
Kavram	90
Tedbire Başvurmanın Koşulları	90
Tedbire Karar Vermeye Yetkili Merciler	91
Tebdirin Uygulanma Usulü	91
Özet	92
Kendimizi Sınayalım	94
Kendimizi Sınayalım Yanıt Anahtarı	95
Sıra Sizde Yanıt Anahtarı	96
Yararlanılan Kaynaklar	96

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

5. ÜNİTE

GİRİŞ	99
TEMEL KAVRAMLAR, BAŞKANLIĞIN GÖREVLERİ VE ERİŞİM SAĞLAYICILAR BİRLİĞİ	100

Genel Olarak	100
Temel Kavramlar	100
Başkanlığın Görevleri	101
Erişim Sağlayıcılar Birliği	102
İÇERİK, YER VE ERİŞİM SAĞLAYICILAR BAKIMINDAN ÖNGÖRÜLEN BİLGİLENDİRME YÜKÜMLÜLÜĞÜ	102
İÇERİK SAĞLAYICININ KULLANIMA SUNDUĞU İÇERİKTEN SORUMLULULUĞU VE YÜKÜMLÜLÜKLERİ	103
YER SAĞLAYICININ YÜKÜMLÜLÜKLERİ	103
ERİŞİM SAĞLAYICININ YÜKÜMLÜLÜKLERİ	104
TOPLU KULLANIM SAĞLAYICININ YÜKÜMLÜLÜKLERİ	104
İÇERİĞİN ÇIKARTILMASI VE/VEYA ERİŞİMİN ENGELLENMESİ TEDBİRLERİNE İLİŞKİN GENEL AÇIKLAMALAR	105
ERİŞİMİN ENGELLENMESİ KORUMA TEDBİRİ	105
Genel Olarak	105
Tedbirin Uygulanabilmesi İçin Gerekli Olan Şüphe Derecesi	106
Erişimin Engellenmesi Kararı Verilebilmesi Bakımından Katalog Suçlar	107
Tedbire Karar Verebilecek Merciler	107
Tedbirin Süresi ve Tedbire Karşı Kanun yolu	107
Tedbirin Uygulanması	108
İçeriğin Yayından Çıkartılmasının Tedbire Etkisi	108
Erişimin İdari Bir Tedbir Olarak Engellenmesi	108
ÖNLEME AMAÇLI OLARAK İÇERİĞİN ÇIKARTILMASI VE/VEYA ERİŞİMİN ENGELLENMESİ TEDBİRİ	109
Genel Olarak	109
Tedbire Başvurulmasının Koşulları	109
Tedbire Karar Verebilecek Merciler ve Tedbirin Uygulanması	109
KİŞİLİK HAKLARININ İHLALİNE BAĞLI OLARAK İÇERİĞİN YAYINDAN ÇIKARTILMASI VE ERİŞİMİN ENGELLENMESİ	110
ÖZEL HAYATIN GİZLİLİĞİNİN İHLALİ NEDENİYLE İÇERİĞE ERİŞİMİN ENGELLENMESİ	111
Özet	113
Kendimizi Sınayalım	114
Kendimizi Sınayalım Yanıt Anahtarı	115
Sıra Sizde Yanıt Anahtarı	115
Yararlanılan Kaynaklar	115

6. ÜNİTE

E-Ticaret..... 116

ELEKTRONİK ORTAMDA SÖZLEŞMELER	117
Genel Olarak Elektronik Sözleşmeler	117
Elektronik Ortamda Yapılan Sözleşmelerin Yasal Çerçevesi	118
Sözleşmelerin Kurulmasında İrade Açıklamaları	119
Genel Olarak	119
İrade Açıklamalarının Tasnifi: Öneri ve Kabul	120
Elektronik Ortamda Açık ve Örtülü İrade Açıklaması	121
Hazır Olanlar ve Olmayanlar Arasında İrade Açıklamaları	122
İrade Açıklamasında Bozukluklar ve İptal Edilebilirlik	124
İrade Açıklamasının Yorumu	124
Sözleşmelerin Kurulmasında Şekil	124

Şekil Serbestisi	124
İstisna: Şekil Şartı	125
Sözleşmelerin ya da Elektronik İrade Açıklamalarının İspatı	126
Belge - Senet Kavramları	126
Mevcut Hukuk Sisteminde Elektronik Dokümanların İspat Gücü	127
Elektronik Dokümanların İspat Değerine Sahip Olma Gereksinimi	127
Güvenli Elektronik İmza ve İspat Gücü	128
Elektronik Ortamda Kurulan Sözleşmelerde Akdin Zayıf Tarafının	
Korunması	129
Genel Olarak	129
Tüketicinin Korunması Hakkında Kanun'da Mesafeli Sözleşmeler	129
Elektronik Ticaret Kanunu'nda Sözleşmelere İlişkin Düzenlemeler	131
Sözleşmelere İlişkin Düzenlemeler	131
ELEKTRONİK ORTAMDA REKLAMLAR	132
İnternet Reklamlarının Avantajları	132
Başlıca İnternet Reklam Türleri	133
Elektronik Ortamdaki Reklamlara İlişkin Hukuki Düzenlemeler	133
Elektronik Ortamdaki Reklamların Hukuki Çerçevesi	133
Kural: Reklam Serbestisi	134
Elektronik Ortamda Yapılacak Reklamlara İlişkin Genel İlkeler	134
Reklam Yasakları	135
İnternette Reklamlara İlişkin Özel Sorunlar	136
İzinsiz Elektronik Postalar	136
Arama Motorlarında Kelime Tabanlı Reklamlar (Adwords Reklamlar)	136
ELEKTRONİK ORTAMDA HAKSIZ REKABET	138
Genel Olarak	138
İnternette Haksız Rekabet Örnekleri	139
Alan Adı Kullanımı Yolu ile	139
Yanlış ve Yanıltıcı Beyanlar	141
Başlık Tekniği (Meta-Tag)	141
Haksız Rekabette Sorumluluk	141
Özet	143
Kendimizi Sınayalım	144
Kendimizi Sınayalım Yanıt Anahtarı	145
Sıra Sizde Yanıt Anahtarı	145
Yararlanılan Kaynaklar	146

Bilişim Ortamında Fikrî ve Sınai Haklar..... 148

7. ÜNİTE

İNTERNET ORTAMINDA FİKRÎ HAKLAR VE KORUNMASI	149
Giriş ve İlgili Mevzuat	149
İnternet Ortamında Eser	149
İnternet'te Eserlerin Yer Alma Türleri	149
Eserin Niteliği Olarak Dijitalleşme	150
Dijitalleşmenin Tehlikeleri	150
İnternete Mahsus Eser Görünümleri: Çoklu Ortam (Multimedya)	
Eserleri	150
İnternette Fikri Hukuk Bakımından Özellik Arz eden Uygulamalar	151
Genel Olarak	151
Link ve Frame Kullanılması	152

İnternet (Web) Sayfalarının Korunması	159
Widget Programlarının Kullanımı	160
Değişim Programları	161
Paylaşım Programları	162
Kanunda Eser Sahipleri İçin Getirilen Özel Koruma Usulü	163
Fikri Hak İhlallerinde Uygulanacak Hukuk	163
İNTERNET ORTAMINDA SINAİ HAKLARIN KORUNMASI	164
Genel Olarak	164
Alan Adı ve Markasal Kullanım	164
Alan Adının Niteliği ve Sorunun Ortaya Konulması	164
Ortaya Çıkan Sorunlar	165
Marka Hakkına Tecavüz	166
Alan Adlarına Karşı Açılacak Davalarda Üst Düzey Alan Adının Önemi	169
Ticaret Unvanı ve İşletme Adının Korunması	170
Alan Adının Korunması	170
Markanın Adwords Reklamlarda ve Başlıklarda (Meta Tag) Kullanılması	171
Özet	172
Kendimizi Sınayalım	173
Kendimizi Sınayalım Yanıt Anahtarı	174
Sıra Sizde Yanıt Anahtarı	174
Yararlanılan Kaynaklar	174

8. ÜNİTE

Bilişim Hukuku Alanındaki Son Gelişmeler	176
TEMEL HAK VE HÜRRİYETLER	177
TEMEL HAK VE HÜRRİYETLERİN KISITLANMASI	178
TEMEL HAK OLARAK İNTERNET ERİŞİMİ	179
DÜNYADA VE TÜRKİYE'DE İNTERNET ERİŞİMİNİN ENGELLENMESİ VE İSTİHBARAT AMAÇLI GÖZLENMESİ	181
ÜLKEMİZDE İNTERNET	183
ARAMA MOTORLARI	189
UNUTULMA HAKKI	191
Özet	196
Kendimizi Sınayalım	197
Kendimizi Sınayalım Yanıt Anahtarı	198
Sıra Sizde Yanıt Anahtarı	198

Önsöz

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

Yrd.DoçDr. Gökhan GÜNEYSU

1

Amaçlarımız

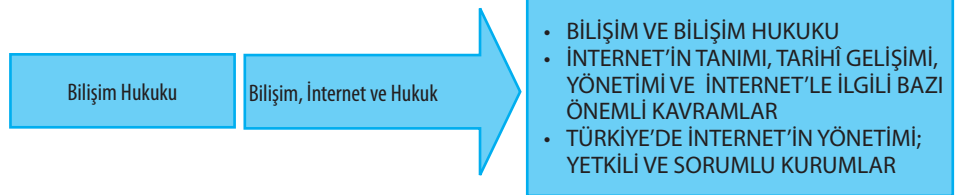
Bu üniteyi tamamladıktan sonra;

- Bilişim ve bilişim hukuku kavramlarını tanımlayabilecek,
- İnternet'in tarihsel gelişimi ve yönetimini açıklayabilecek,
- İnternet'e dair önemli bazı teknik ve hukuki kavramları açıklayabilecek,
- Türkiye' de İnternet'i yönetmekle sorumlu kurumların hangileri olduğunu ve bu kurumların yetki ve sorumluklarını açıklayabilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Bilişim
- Bilişim Hukuku
- İnternet
- İnternet Ağları
- World Wide Web
- Veri
- Ulaştırma Bakanlığı
- Telekomünikasyon İletişim Başkanlığı

İçindekiler



Bilişim, İnternet ve Hukuk

BİLİŞİM VE BİLİŞİM HUKUKU

Bilişim Hukuku, bilişim teknolojilerindeki gelişmeler ve yenilikler sebebiyle mevcut yasal düzenlemelerin yetersiz kalması ile ortaya çıkmış bir hukuk dalıdır. Bu hukuk dalını, siber/elektronik ortamın düzenlenmesi ve bilişim konusundaki ihtilafların çözümü ile uğraşan multi-disipliner bir hukuk dalı olarak tanımlamak mümkündür.

Bilişim hukukunun uğraş alanı, multi-disipliner bir yapıya sahip olması sebebiyle çok geniş olup birçok hukuk dalı ile iç içe geçmiştir. Bu karmaşık ilişkiye örnek vermek gerekirse; yazılımların korunması, kullanılması, bunlara ilişkin sözleşmeler ve ihlaller fikrî mülkiyet hukukunun konusuna girmektedir. Bilişim aracılığıyla işlenen suçlar, özel hayatın gizliliği, kişisel verilere karşı işlenen suçlar, banka veya kredi kartları aracılığıyla işlenen suçlar gibi konular ceza hukukunun konusudur. Kamu kurum ve kuruluşlarında bilgisayarların kullanılmasına ilişkin sorunlar idare hukukunun alanına girmektedir. Verilerin uluslararası kullanımından doğan sorunlar devletler hukukunun ve bilişim hukukundaki soruşturma, kovuşturma ve yargılama yöntemleri ise medeni usul hukuku ile ceza muhakemesi hukukunun kapsamına girmektedir(Özkan,2014).

Bu örnekleri çoğaltmak pek tabii mümkün olup birkaç örnek ile açıklamak gerekirse: Son yıllarda hızla yaygınlaşan İnternet üzerinde yapılan alışverişler normalde borçlar hukuku ve tüketici hukuku dallarını konusudur. Fakat İnternet üzerinden yapılan alışverişlerde kullanılan İnternet altyapısı sebebiyle bazı sorunlar ortaya çıkmaktadır. Benzeri sebeplerle ortaya çıkan hukuki uyumsuzlukları çözmek için ek hukuki düzenlemelere ihtiyaç vardır. Yine aynı şekilde bilişim suçlarının işleniş biçimini diğer klasik suçlara nazaran daha karmaşık bir yapıya sahip olduğundan özel hukuki düzenlemeleri gerekli kılmıştır (Özkan, 2014). İşte bu düzenlemelerle birlikte bilişim hukuku isimli yeni bir hukuk dalı ortaya çıkmıştır.

Bilişim hukukunu tam olarak anlatabilmek için öncelikle bilişim kavramının tanımlanması gerekmektedir. Bu sebeple ünitenin devam eden bölümlerinde bilişim kavramı üzerinde durulacak ve Türk hukukuna bu kavramın nasıl girdiği anlatılacaktır.

Bilişim Kavramı

“Bilişim” sözcüğü, bilgi ve iletişim sözcüklerinin bir araya getirilerek kullanılmasıyla ortaya çıkmıştır. Bilgisayar ve bilişim sözcükleri zaman zaman birbirleri yerine kullanılmagelmıştır. Fakat her ikisi de farklı anlamlara sahiptir. Bilgisayar, bilgileri (verileri) depolayan ve işleme tabi tutan bir sistemi, bir makineyi ifade etmektedir. “Bilişim” sözcüğü ise bilgisayara göre daha üst bir kavramı ifade etmek için kullanılmaktadır. Bilişim kavramı çeşitli eserlerde ve mahkeme kararlarında farklı tanımlanmıştır.

Türk Dil Kurumu Bilişimi: “İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik” olarak tanımlamıştır (tdk.gov.tr, 2015).

Bilişim hukuna dair birçok önemli eserde benzer tanımlara rastlamak mümkündür. Fakat bütün tanımları vermek yerine Türk hukuk sistemi içerisinde önemli bir yere sahip olan Yargıtay Ceza Genel Kurulu’nun tanımına bakmak gerekirse;

Yargıtay Ceza Genel Kurulu’nun (YCGK) 19 Haziran 2007 tarihli vermiş olduğu E. 2007/6-36 K. 2007/150 sayılı kararında (Kazancı, 2015) bilişim sözcüğü ile “bilginin otomasyona tabi tutulması sonucunda işlenmesini, başka deyişle, verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılmasını” ifade ettiği belirtilmiştir. Yine anılan karar ile, “Bilgisayar, (kompüter, elektronik beyin) aritmetik ve mantık işlemi dizileriyle oluşturulmuş programlara göre verileri (bilgileri) otomatik işleme tabi tutan sistemlere verilen ortak isim iken, bilişim (enformatik) ise, bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesine konu olan akademik ve mesleki disipline verilen addır; yani başka bir deyişle, bilgisayar kullanma ilmidir.”denilerek, bilişim kelimesinin bilgisayarla göre daha geniş anlam ihtiva ettiği belirtilmiştir.

Bilişim bilginin (verilerin) bilgisayarlar aracılığıyla elektronik olarak depolanması yanında işlenmesini ve iletilmesini kapsamaktadır. Bir başka ifadeyle, bilişim, bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır bir hale gelmesinin konu alan akademik ve mesleki disipline verilen isimdir. Aynı zaman bilgisayar kullanma bilimi “computer science” ın Türkçedeki karşılığıdır (Özen, Baştürk, 2011).

Bilişim Kavramının Türk Hukukundaki Gelişimi

Bilişim kavramı Türk hukuk sisteminde ilk kez 1989 tarihli Türk Ceza Kanunu ön tasarısında kullanılmıştır. Bu ön tasarının 342. maddesinin gerekçesinde bilişim alanının tanımı; “... bilgileri depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinde oluşan alan...” olarak yapılmıştır. Bu tanım, TCK’ya “Bilişim Alanında Suçlar” başlıklı 11.babı ekleyen 14.06.1991 tarih ve 3756 sayılı yasanın gerekçesinde olduğu gibi aktarılmıştır. 1997 tarihli TCK tasarısında bilişim tanımı; “... verileri toplayıp, yerleştirdikten sonra bunları otomatik işlemlere tabi tutma imkanı veren manyetik sistemler...” olarak yapılmıştır. 2000 tarihli TCK tasarısında da aynı tanım yer almaktadır. Son olarak 2003 yılında TBMM’ye sunulan TCK tasarısında da bilişim aynı şekilde değişiklik yapılmadan tanımlanmıştır (Dülger, 2014). Bahsi geçen bu son tasarı 1 Haziran 2015 tarihi itibarıyla yürürlüğe girmiş ve hâlihazırda aynı tanım 5237 sayılı Türk Ceza Kanunu’nda da bulunmaktadır.

Bilişim Suçu

Bilişim suçları literatürde çok farklı sınıflandırmalara ve tanımlamalara tabi tutulmaktadır. İlerleyen ünitelerde bu suçlar detaylı bir şekilde inceleneceği için burada kısa bir tanım ile dar ve geniş anlamda bilişim suçları ayırımına değinilecektir. Bilişim suçunu, verilere karşı ve/veya veri işlemekle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar olarak tanımlamak mümkündür (Dülger, 2014).

Dar anlamda bilişim suçları: Bilişim sisteminin güvenliğini veya veri işlemini hedef alan eylemlerdir. Geniş anlamda bilişim suçları ise bilişim sistemi ve ağı marifetiyle veya bu sistem veya ağda gerçekleşen herhangi bir hukuk dışı eylemi ifade eder (Yazıcıoğlu, 2002).

Sadece bilişim ortamında işlenebilen, klasik suçlar arasında sayılmayan, bilgisayar ve İnternete özgü suçlar dar anlamda suçlardır. Bu suçlar, daha önce hiç görülmemiş ve bilinmeyen, bilgisayarın icadı ve yaygınlaşması sonucu ortaya çıkan İnternetin yaygınlaş-

masıyla da işlenmeleri kolaylaşan ve artan suçlardır. Bu suçları ortadan kaldırmak veya sınırlandırmak mümkün değildir. Her geçen gün çok değişik yöntemler kullanılarak bu suçlar çoğaltılmaktadır. Dar anlamda bilişim suçlarına örnek olarak yetkisiz erişim (hacking), verilere yönelik suçlar, bilişim ağlarına yönelik suçlar ve sanal tecavüz gösterilebilir.

Geniş anlamda bilişim suçları; bilişim sistemleri kullanılarak veya bilişim sistemlerinden yararlanılarak işlenen klasik suçlardır. Birçok klasik suçun bilişim sistemlerinde veya bilişim sistemlerinden yararlanılarak işlenmesi mümkündür. Bilişim sistemleri üzerinden işlenmesi mümkün olan suçlara örnek olarak; Tehdit ve şantaj, hakaret ve sövme, taciz, röntgencilik, manüpilasyon, dolandırıcılık, hırsızlık, sahtekârlık ve siber terör gösterilebilir.

Bilişim sistemleri İnternetle birlikte çok yoğun bir etkileşimin merkezi olmuştur. İnternetin karmaşık yapısı ve kullanımının bu kadar yaygınlaşması beraberinde birtakım ciddi sorunları da gündeme getirmiş ve İnternetin kötü amaçlarla kullanılması sonucunda yukarıda kısaca açıklamaya çalıştığımız “bilişim suçları” olarak adlandırılan yeni suç türleri ortaya çıkmıştır. İnternetin günümüzde hukuki sorunlar bakımından da irdelenmesi, çıkabilecek yeni sorunların önüne geçmek ve bilişim suçlarıyla etkin mücadele bakımından önem taşımaktadır. Bilişim hukukunu ve bilişim suçlarını daha iyi anlayabilmek adına ünitenin devam eden bölümlerinde “İnternet” kavramı üzerinde durulacaktır.

Dar anlamda bilişim suçlarına örnek veriniz?



SIRA SİZDE

1

Bilişim suçlarını anlamak için yararlı bir kaynak olarak: Bilişim Suçları ve İnternet İletişim Hukuku’na bakabilirsiniz. (Murat Volkan Dülger Seçkin Yayınevi, 2014)



K İ T A P

İNTERNET’İN TANIMI, TARİHİ GELİŞİMİ, YÖNETİMİ VE İNTERNET’LE İLGİLİ BAZI ÖNEMLİ KAVRAMLAR

İnternet’in Tanımı

Tek başına bilgisayarın icadı elbette önemli bir keşif olma özelliğine sahiptir. Fakat bilgisayarların çeşitli yöntemlerle birbirine bağlanabilir hâle gelerek bilgisayar ağlarını oluşturmaya başlaması, bilişim teknolojisinin, dünyada bilginin küreselleşmesini ve kendisini daha hızlı üretmesini ve dönüştürmesini sağlayan bir gelişme olmuştur. Hiç şüphesiz, son 40 yılda teknolojik gelişmeleri tetikleyen en önemli olay, dünya çapındaki küçüklü büyüklü bilgisayar ağlarının kurulması ve varlığı değil, bütün bilgisayar ağlarını kapsayan genel bir ağ olan “İnternet”in tesis edilmesi ile olmuştur. (Akıncı, Alıç, Er,2002)

Bilgisayar ağlarından birisi olan İnternet, günümüzde dünyadaki en yaygın ve en çok kullanılan ağ olma özelliğine sahiptir. “İnternet” kelimesi, **Interconnected Networks** (kendi aralarında bağlantılı ağlar) kelimesinin kısaltması olarak kullanılmaktadır (Özen, Baştürk, 2011). İnternet, birden fazla haberleşme ağının, birlikte meydana getirdikleri bir iletişim ortamıdır. Bu iletişim ağları, bilgisayarlar ile örülmüştür. Yani, İnternet bilgisayarlar arasında kurulmuş bir haberleşme ağıdır. İnternet, kişilerin dünya üzerinde birbirleri ile çok geniş amaç ve içerikte iletişim kurmalarını, bilgi alışverişinde bulunmalarını sağlayan ortak iletişim alt yapısıdır. Özet, olarak nasıl ki vücudumuzun her yanını atar ve toplardamarlar vasıtasıyla kılcal damarlar sarmışsa, İnternet ağı da dünyayı aynı şekilde sarmıştır. İnternette iletişim için, ağı meydana getiren bilgisayarlar arasında bağlantı kurulması gerekmektedir. Bu bağlantılar, omurga (backbone) adı verilen ana iletişim hatları vasıtasıyla yapılır. Yapılan bu bağlantı, yani iletişim, bir takım kurallara göre yapılır. Bunun için ortak bir dil kullanılmaktadır. Bu ortak dile “İnternet protokolü” denilmektedir. Bilgisayarlar bu yolla iletişim kurarak bilgi alışverişinde bulunabilmektedir (Oğuz,2012).



İnternet kelimesi hangi İngilizce kelime öbeğinin kısaltmasıdır?

İnternet'in Tarihi Gelişimi

İnternetin ortaya çıkışı soğuk savaş döneminde ABD ve Sovyetler Birliği arasında yaşanan kıyasıya rekabete dayanmaktadır. Söz konusu bilgisayar ağı projesi, olası bir nükleer savaşta, herhangi bir askerî bilgisayarda bulunan bilgilerin bir diğerine aktarılması düşüncesine dayanmaktadır. Yüksek teknoloji rekabetinin çok yoğun yaşandığı bu dönemde Sovyetler Birliği, 1957 yılında Sputnik uydusunu uzaya göndermiş bu gelişme üzerine Amerikan Hükümeti, tek bilgisayardan bağımsız olarak çalışabilen bir ağ kurma fikrini ulusal güvenlik gerekçesiyle geliştirmek için çalışmalara başlamıştır. Amerikan Hükümeti, Savunma Bakanlığına bağlı olan ve birbirinden uzakta olan bazı askerî birliklerin geliştirdiği projelerin ortak bir ağ üzerinden birleştirilmesi temeline dayanan ARPA (Advanced Research Project Agency) adlı bir birim oluşturmuş ve daha sonraki süreçte bu farklı sistemleri birbirine bağlamak için ARPANET adlı bir askerî bilgisayar ağı kurulmuştur (Taşkın, 2008).

Zaman içerisinde önce bu sistemdeki farklı özellikteki bilgisayarların birbirini tanımasına yarayan ve aralarındaki uyumsuzlukları çözmeye yarayan, günümüzde de dünyadaki milyonlarca bilgisayarın ve yerel ağların birbiriyle iletişim kurmasına yarayan kurallar bütünü olan TCP/IP (Transport Control Protocol/Internet Protocol) kuralları gibi kurallar geliştirilmiştir. Bu sistem bir süre sonra sivil bilgisayarların kullanımına açılmış ve 1990 yılında daha da geliştirilerek bugünkü hâlini almıştır (Taşkın, 2008).

Türkiye'de ise ilk İnternet bağlantısını 12 Nisan 1993 tarihinde Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) destekli bir proje ile Orta Doğu Teknik Üniversitesi (ODTÜ) gerçekleştirmiştir.

Türkiye'de ise ilk İnternet bağlantısını 12 Nisan 1993 tarihinde Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) destekli bir proje ile Orta Doğu Teknik Üniversitesi (ODTÜ) gerçekleştirmiştir.

İNTERNET



İnternet'in tarihçesi ile ilgili detaylı bilgiye <http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/İnternet'in-tarih%C3%A7esi> adresinden ulaşabilirsiniz.

İnternetin Yönetimi

İnternet'in belirli bir sahibi yoktur. Bir anlamda, dünya üzerindeki posta hizmetlerine benzer. Ülkeler, belirli kurallara uyarak kendi topraklarında küresel posta akışını sağlayınca, dünya ölçeğinde iyi işleyen bir posta hizmeti doğmuştur. Benzer olarak, küresel olarak konulan bazı kurallar çerçevesinde İnternet trafiği dünya ölçeğinde oldukça iyi yönetilmektedir. Hemen belirtelim ki, İnterneti küresel olarak yöneten kuruluşlar ticari değil, bir anlamda yapılması gereken zor işleri üstlenen gönüllü kuruluşlardır (Karaçay, 2013).

Bu kuralları ve kuruluşların yapısını, artan İnternet trafiğinin ihtiyaçları belirlemektedir. Dolayısıyla, zaman içerisinde bu kuruluşların yapısı değişmektedir. Bu günkü duruma göre tepede iki organ vardır. Birisi, İnternet numaralarının tahsisini yöneten IANA (Internet Assigned Numbers Authority) kurumudur. Ötekisi ise, İnternetin yönetim ve gelişme politikalarını belirleyen ICANN (Internet Corporation for Assigned Names and Numbers) kurumudur. ICANN 1998 yılında kurulmuştur ve merkezi Marina Del Rey, Kaliforniya'dadır (Karaçay, 2013).

Her iki kurumun altında dünyanın beş bölgesi için İnternet kaynaklarını ICANN'nın belirlediği politikalara göre yöneten kuruluşlar vardır. Bunlara Bölgesel İnternet Kayıt Merkezi (Regional Internet Registry- RIR) denir. Bu kuruluşların hiçbirisi ticari amaç gütmeyen ve hükümetlerin organı değildir (NGO-nongovernment organization). Ayrıca, bu merkezler ICANN politikalarının oluşmasında rol oynarlar. Böylece, dünya çapında, katılımcı ve demokratik bir İnternet yönetimi oluşur (Karaçay, 2013).



İnternet'i büyük geniş otobanlar ve bunlara bağlı sayısız küçük yan yollar olarak düşünürsek bu kuruluşlar işte bu otoban ve yollardaki trafikle ilgili olarak çeşitli düzenlemeler yaparlar. Bu kuruluşların yönetimi herşeye hâkim olmak anlamına gelmemektedir. İnternet içeriğiyle birlikte merkezî bir otorite tarafından yönetilemez. Buna şimdilik teknik imkânlar el vermemektedir. Bu uçsuz bucaksız alan insanlara muazzam bir özgürlük alanı açmasının yanı sıra birçok yasa dışı faaliyetin de bu alana kaydığı görülmüştür. İnterneti merkezî bir denetim kuruluşu tarafından denetleme düşüncesi çeşitli zamanlarda ABD gibi önemli ülkelerde projelendirilmiş fakat ciddi muhalefetler karşısında kabul görmemiştir.

Bu projelerden birisi ABD'de hazırlanmıştır. İnternet suçluluğuyla mücadele etmek için özel yaşamı ihlal etmeyi göze alan Amerika Birleşik Devletleri (ABD), 2000 yılında Federal Bureau of Investigation'ın (FBI) kullanımına "Carnivore" adlı bir sistemi sunmuş ve böylece bireylerin İnternet 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 (Taşkın, 2008).

Sanal ortamda işlenebilecek ya da sanal ortam aracı olarak işlenebilecek suçların önlenmesi için 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 Avustralya 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 (Taşkın, 2008).

Her ne kadar merkezî bir yönetime sahip olmasa da önemli devletler İnterneti merkezî bir denetime sokmaya çalışmaktadır. Bu çabanın her geçen gün artarak devam ettiği bilinmektedir.



ECHELON projesi Patrick Radden KEEFFE tarafından romana uyarlanmıştır. (Echelon: Dünyayı Dinleyen İstihbarat Örgütleri, Defne Yayinevi, 1. Baskı, Mayıs 2003, Çeviren: Sinem Gül)



K İ T A P

İnternet'le İlgili Bazı Önemli Kavramlar

Bilişim hukuku ve İnternet'in daha iyi anlaşılabilmesi için bazı önemli kavramların açıklanması gerekmektedir. Bu kavramlar, bilişim hukuku mevzuatını oluşturan birçok kanunda tanımlaması yapılmış kavramlardır.

Bilgisayar, kullanıcılardan aldığı verilerle aritmetik ve mantıksal işlemleri yapabilen ve yaptığı işlemlerin sonuçlarını saklayabilen, saklanan bilgilere istenildiğinde ulaşılabilen elektronik bir makinedir. Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesi "bilgisayar sistemi" kavramına yer vererek bunu, "dijital verilerin otomatik olarak işlenmesi için geliştirilmiş donanım ve yazılımdan oluşan cihaz" olarak tanımlamıştır (Avrupa Konseyi Siber Suçlar Sözleşmesi md.1/a).

Veri, bilişim sistemlerinin en temel birimidir. Bilişim sistemlerinin amacı, veriyi saklamak, işlemek ve sonuç çıkarmaktır. Veri, bilgisayar tarafından üzerinde işlem yapılan her türlü değeri ifade etmektedir (Eralp, 2012). Başka bir tanımla "...bilgisayar tarafından iletişim, açıklama ve işlem amacıyla herhangi bir amaç, konu, durum, koşul, fikir ya da diğer unsurları açıklamak için (ve) sayıları, harfleri, simgeleri belirtmek üzere kullanılan genel terim"dir. Veri; her türlü bilginin, bilgisayarın işlem yapabileceği, sonuçlar ürete-

bileceği, saklayabileceği ve gerektiğinde yeniden okuyabileceği şekilde sayısal birimlere dönüştürülmüş hâlidir. (Dülger, 2014)

Bilişim Alanı, bilgisayarları da kapsayan ve özellikle bilgisayar ve bu tür aygıtların yer aldığı bir alan, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma imkânı veren manyetik sistemlerdir (Akıncı, Alıç, Er,2002).

Bilişim Sistemi, Yeni Türk Ceza Kanunu'nun 243. madde gerekçesinde, bilişim sistemi, "veri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir" şeklinde tanımlanmıştır. Avrupa Konseyi Siber Suç Sözleşmesi'nin "Tanımlar" başlıklı 1. maddesinde "bilgisayar sistemi" terimi, "bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı ifade edecektir" şeklinde tanımlanmıştır. Bilişim sisteminin biri maddi diğeri de soyut olmak üzere iki bileşeni bulunmaktadır. Bilişim sisteminin, verileri depolamaya, işlemeye, kullanmaya ve nakletmeye yarayan cihazlarına donanım, bunların bu şekilde çalışmasını sağlayan programlara da yazılım denmektedir. Bilişim sistemi, yazıcı, modem gibi tüm çevre birimleri de dâhil olmak üzere bilgisayardan beklenen tüm amaçları gerçekleştirmeye elverişli donanım ve yazılım öğelerinin bütünüdür (Avşar, Öngören, 2010).

Bilgisayar programı, bilgisayara ne yapması gerektiğini söyleyen bir dizi komuttur. Bir başka tanımla, bilgisayarın çalışmasının temelinde işletim sistemi adı verilen ve bilgisayarın çalışabilmesi için gerekli veriler, komutlar ve dosyaları içeren ana program vardır. Bilgisayar açıldığı zaman harekete geçen ve otomatik olarak yüklenen dosyalar ve komutlar, kullanıcının bilgisayarda işlem yapabilmesini sağlayan zemini oluştururlar. İşletim sistemine bilgisayarın ruhu denilebilir. Dos, Windows, Linux, Zenix gibi farklı işletim sistemleri mevcuttur. İşletim sistemi de temelde bir bilgisayar programıdır ve bilgisayarın hangi durumda nasıl davranması gerektiğini bildiren komutlar içerir. Bilgisayar komutlarla hareket eder, Bilgisayar programları da bilgisayara komut veren ve belli durumlarda belli şekilde çalışmasını düzenleyen, işlemleri sıraya koyan, belli yapılar oluşturabilen komut dizilimleridir. (Avşar, Öngören, 2010)

TCP/IP Protokolü, "Bilgi ağı" üzerindeki bilgi iletimi ve paylaşımı bazı kurallara göre yapılmaktadır. Bu kurallara, İnternet protokolleri ya da TCP/IP (Transmission Control Protocol/ İnternet 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 mesajların doğru yere ulaştırılmasından; IP ise adresleme sisteminden sorumludur. TCP/IP protokolünün dışında bazı anlaşma dilleri oluşturulmuşsa da genel olarak kabul görmediğinden şu an için İnternet ağında en çok kullanılan anlaşma dili TCP/IP protokolüdür. (Eralp, 2005).

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, İnternet üzerindeki bilgisayarlar arasında dosya alma/ gönderme protokolü (FTP, File Transfer Protocol), Elektronik posta iletişim protokolü (SMTP Simple Mail Transfer Protocol), TELNET protokolü (İnternet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen *login* protokolü) verilebilir. Adını sıkça duyduğumuz WWW (ya da web) ortamında birbirine bağlanmış farklı türden objelerin iletilmesini sağlayan protokol ise Hyper Text Transfer Protocol (HTTP) olarak adlandırılmaktadır (Oğuz, 2012).

World Wide Web (www) kısaca web; dünyanın her yerindeki yüzbinlerce sunucuda kayıtlı, milyarlarca dosyadan oluşan bir bütündür. Birçok İnternet 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. Bütün bu farklı yapılarıdaki veriler uygun bir standart ile bir arada kullanılarak bir web tarayıcısında görüntülenebilir (Oğuz, 2012). Hiper ortam, bir dökümandan başka bir dökümanın çağırılmasına (navigate) imkan verir (iç içe dökümanlar). Bu ortamdaki her veri (object), başka bir veriyi çağırabilir (link). Link, aynı döküman içinde başka bir yerde olabildiği gibi, fiziksel olarak başka bir yerde de (İnternet üzerindeki herhangi bir makinede) olabilir. Bütün bu farklı yapıdaki veriler uygun bir standart ile bir arada kullanılıp bir web tarayıcısında (web browser) görüntülenebilir. Web'in diğer bir işlevi de öteki bazı İnternet servislerini kendi içerisinde barındırmasıdır (ftp, gopher, news, wais gibi). Web uygulamaları (Web sayfaları), web listeleycilerinde/tarayıcılarında (Browser, Gezgin, Tarayıcı) görüntülenir. Web sayfaları, başka sayfalara ve değişik türden verilere hiper linkler içermektedir. Buralara fare (mouse) ile tıklayarak başka sayfalara, oradan da başka sayfalara geçmek mümkündür. Bu aslında çok basit bir bilgiye ulaşım modelidir. Web Sistemleri, kullanılan platformdan bağımsızdır. Bir Macintosh, Pc ya da Unix Web listeleycisi aynı sayfaları, aynı şekilde alır. Sayfaların alındığı web servisleri de farklı bilgisayar platformlarında olabilir. Web listeleycileri ve web servis sağlayıcı ortamlar hemen hemen tüm dünyada her yerde vardır ve global olarak kullanımları üstel bir şekilde artmaktadır. Web yapısının bu kadar çok kabul görmesinin bazı sebeplerini sıralamak gerekirse, her şeyden önce 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 (Oğuz, 2012).

Web Browser (web tarayıcısı), İnternet üzerindeki tüm bilgilere bakabilmek ve bu bilgilerle etkileşim halinde olabilme imkânı veren bir uygulama programıdır. Web tarayıcısı ile web adreslerine erişilir. Bilgisayar kullanıcısının İnternet aracılığıyla bir Web hizmet merkezine bağlandıktan sonra tek seferde ekranına aktarabildiği yazı resim grafik veya ses bilgilerini içeren farklı verilerden de oluşabilen web sayfası, HTML (Hypertext Markup Language) adı verilen işaretleme dili kullanılarak oluşturulur. Bu işaretleme dili sayesinde bir web sayfasında hangi kelime veya cümleye tıklandığında hangi sayfaya bağlanacağı web sayfasındaki resimlerin nereden alınacağı ve sayfaya ilişkin diğer unsurlar işlev kazanırlar. 1994'ün sonlarında en popüler ve yaygın kullanımı olan Web Browser Mosaic idi. Bu yüzden Web denildiğinde Mosaic akla gelirdi. Netscape Navigator. Netscape'in ilk sürümü (1.0) 1994 sonlarında çıktı. 4.0 sürümünde, Netscape Composer (html editörü), Netscape Messenger (e-posta programı), Netscape Collabra (News Programı), ve Netscape Conference ile Navigator birlikte gelmektedir. 7.0 çıktı(2000) Netscape'in dışında 1995'in ortalarında, Microsoft, Mosaic tabanlı bir Web Listeleycisi çıkardı Microsoft İnternet Explorer. Diğer adıyla ağ tarayıcısı, kullanıcıların ağ sunucuları üzerinde yer alan HTML sayfalarını açmasını sağlayan yazılımdır. Günümüzde en yaygın kullanılan tarayıcılar, Microsoft İnternet Explorer, Mozilla, Firefox, ve Safari'dir (Avşar, Öngören, 2010).

Domain Name, (DNS, Domain Name System/ alan adı sistemi) olarak adlandırılan hiyerarşik bir isimlendirme sistemi ile (alan adı sistemi), İnternete bağlı bilgisayarlara ve bilgisayar sistemlerine isimler verilir. DNS de aslında bir TCP/IP servis protokolüdür. DNS, 'host' olarak adlandırılan İnternete bağlı tüm birimlerin yerel olarak bir ağaç yapısı içinde gruplandırılmasını sağlar. Bu şekilde, bütün adreslerin her yerde tanımlı olmasına gerek kalmaz. Her bir İnternet adresine 4 haneli bir numara karşılık gelir, a.b.c.d şeklindeki bu numaralara IP (İnternet Protocol) numaraları denir. Burada, a,b,c ve d 0-255 arasında değişen bir tam sayıdır.(32 bit adresleme sistemi). Her İnternet adresinin ilk kısmı bulunduğu Domain'in network adresini, son kısmı ise makinenin (host) numarası verecek şekilde ikiye bölünür. (http://www.heweso.com/newsdetails/57/İnternet_adresi_nedir.html) (Erişim Tarihi: 15.08.2015) İnternet üzerindeki her bilgisayarın o anda sadece

kendisine ait olan bir adresi vardır. Statik IP sürekli size ait olan bir IP adresinin olması ve bilgisayarınıza tanımlanmasıdır. 1992 yılından beri Avrupa’da IP numarası dağıtımı Yerel İnternet Kayıt Merkezleri (Local Internet Registries) tarafından yapılmaktadır. ABD’de bulunan Global Internet Registry, Avrupa bölgesindeki IP numarası dağıtım yetkisini RIPE NCC (Réseaux IP Européens Network Coordination Center) organizasyonuna vermiştir. RIPE NCC de elindeki IP numarası bloklarını Avrupadaki ülkelerde Yerel İnternet Kayıt Merkezleri aracılığı ile dağıtmaktadır. Türkiye’de ise IP numarası dağıtım yetkisi RIPE tarafından ULAKBİM’e verilmiştir. Ülkemizde hâlihazırda alan adı ODTÜ alan adlarının dağıtımını yapmaktadır. IP numaralarının dağıtımını ise ULAKBİM tarafından yapılmaktadır (Karaçay, 2013).

İnternet alanı oluşturan her birim sadece kendine ait bir IP adresine sahiptir. Bu IP adresleri kullanıcıların kullanımı için `www.site_adı.com` gibi kolay hatırlanır adreslere karşılık düşürülür. DNS sunucuları, İnternet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır. Sistem makine isimlerini IP adreslerine, IP adreslerini ise makine isimlerine çevirir. Bir DNS istemci bir bilgisayarın ismine karşılık IP adresini bulmak istediği zaman isim sunucuya başvurur. İsim sunucu, yani DNS sunucu da eğer kendi veritabanında öyle bir ad varsa bu ada karşılık gelen IP adresini istemciye gönderir. DNS veritabanına kayıtların elle, tek tek girilmesi gerekir. DNS üstlendiği görev gereği hızlı olmak zorundadır. Bu yüzden sorgulamalar 512 byteden küçük ise UDP üzerinden çalışacaktır. İnternet adresleri ilk önce ülkelere göre ayrılır. 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 çünkü DNS ve benzeri uygulamaları yaratan ülke ABD’dir. Öte yandan, ABD’ye özel kuruluşlar için `us` uzantısı yaratılmıştır. İnternet adresleri ülkelere ayrıldıktan sonra `com`, `edu`, `gov` gibi daha alt bölümlere ayrılır. Bu ifadeler DNS’de üst düzey (top-level) alan adlarına karşılık gelir. Üst düzey alan adları aşağıdaki gibidir:

- `com`: Ticari kuruluşları,
- `edu`: Eğitim kurumlarını,
- `org`: Ticari olmayan, hükümete de bağlı bulunmayan kurumları,
- `net`: İnternet omurgası işlevini üstlenen ağları,
- `gov`: Hükümete bağlı kurumları,
- `mil`: Askeri kurumları gösterir.
- `num`: Telefon numaralarını bulabileceğiniz yerleri,
- `arpa`: Ters DNS sorgulaması yapılabilecek yerleri göstermektedir.
- Bu isimlere yakın zaman önce `biz` veya `tv` gibi isimler de eklenmiştir.

Alan adları, ağaç yapısı denilen ve belli bir kurala göre dallanan bir yapıda kullanılmaktadır. Amerika haricinde, İnternete bağlı olan tüm ülkelerdeki adresler, o ülkenin ISO3166 ülke kodu ile bitmektedir. Türkiye’deki tüm alt alan adresleri, `.tr` ile bitmektedir. Örneğin; `marine.ulakbim.gov.tr` adresinde: `tr` Türkiye’yi, `gov` alt alanın devlet kurumu olduğunu, `ulakbim` bu devlet kurumunu `marine` bu kurumda bulunan bir makineyi göstermektedir (Avşar, Öngören, 2010).

İnternet Servis Sağlayıcısı, (İnternet Service Provider, ISS) İnternet servis sağlayıcıları, kullanıcıların İnternete bağlanmasını sağlayan, yani kullanıcılar ile İnternet arasında köprü vazifesi gören gerçek veya tüzel kişilerdir. İnternet sistemi içerisinde en önemli aktör İnternet servis sağlayıcılardır. İnternet servis sağlayıcıları kendi bilgisayarlarını, kullanıcıların İnternet’e erişebilmeleri için giriş kapısı olarak kullanırlar. Bu sebeple bir İnternet kullanıcısı, bir İnternet servis sağlayıcısının yardımı olmadan İnternete bağlanamaz (Oğuz, 2012).

İnternet bağlantıları telefon hatları aracılığıyla gerçekleştirilmektedir. Telefon/telekomünikasyon idareleri telefon hatları üzerindeki özel hatları İnternet bağlantıları için tahsis etmişlerdir. Bu, özel hatlar arası veri trafiğinin akmasını sağlamaktadır. İnternet servis sağlayıcıları, İnternet kullanım hizmeti vermek istediklerinde telefon/telekomünikasyon idareleri ile bir sözleşme akderer bu özel üzerinde kullanım/kullandırma hakkı elde eder ve genellikle ücret karşılığında bu hakkı İnternet kullanıcılarına kiralar (Oğuz, 2012).

İnternet servis sağlayıcıları İnternet'e bağlantı sağlamak için çeşitli teknolojileri kullanırlar. Bunlar; Dial-up (çevirmeli ağ), DSL, ADSL, Kablosuz İnternet, Kablolı İnternet, Uydu İnternet vb. teknolojilerdir.

İnternet Erişim Sağlayıcısı, (İnternet Acces Provider) (İES), İnternet Erişim sağlayıcıları, İnternet toplu kullanım sağlayıcılarına ve abone olan kullanıcılara İnternet 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.

İnternet erişim sağlayıcıları, çoğu kez İnternet servis sağlayıcıları ile aynı anlamda kullanılmaktadır. Ancak İnternet servis sağlayıcısı sadece erişim hizmeti veriyor ise yani başkalarına ait bilgileri sunucularında barındırmıyorsa erişim sağlayıcısı adını alır.

5651 sayılı Kanun'un 6. maddesinde erişim sağlayıcılarına önemli yükümlülükler getirilmiştir. Buna göre; "Erişim sağlayıcı;

- a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu kanun hükümlerine uygun olarak haberdar edilmesi hâlinde (...) (1) 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 usûllere uygun olarak kuruma teslim etmekle,
- ç) Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,
- d) Başkanlığın talep ettiği bilgileri talep edilen şekilde başkanlığa teslim etmekle ve başkanlıkça bildirilen tedbirleri almakla, yükümlüdür.

(2) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

İnternet Yer Sağlayıcısı (Web Host Provider) (İYS), Host kelime anlamı olarak "barındırmak" anlamına gelmektedir. İnternetin aktif bir elemanı olan host'un İnternet ortamındaki anlamı da tam olarak budur. Host, İnternet yoluyla erişilebilen dijital bir depolama birimidir. Yani web sayfalarının sanal ortamda barındırıldığı yerdir. İnternet sayfaları için hazırlanan yazı, resim, ses vb. dosyaların İnternet ortamında bir sürücü üzerinde saklanması gerekir. Bu işi de genellikle servis sağlayıcıları üstlenmektedir.

İnternet üzerindeki tüm bilgilere bakabilmek ve bu bilgilerle etkileşim hâlinde olabilmek imkanı veren uygulama programına ne ad verilir?



SIRA SİZDE

TÜRKİYE'DE İNTERNETİ'N YÖNETİMİ; YETKİLİ VE SORUMLU KURUMLAR

Bu bölümde Türkiye'de İnternetin düzenlenmesi konusunda yetkili ve sorumlu olan kurum ve kurullar incelenecektir.

Ulaştırma Bakanlığı

Ülkemizde, bilişim ve bilgisayar denilince ilk akla gelen kurum Ulaştırma Bakanlığıdır. 3348 Sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun'a göre, devletin ulaştırma ve haberleşme hedef ve politikalarının tespiti ve uygulanması amacıyla gerekli araştırmaları yapmak ve yaptırmak evrensel hizmet politikalarını, ilgili kanunları hükümleri dahilinde ülkenin sosyal, kültürel, ekonomik ve teknolojik şartlarına göre belirlemek, hükümetin genel politikasını uygulamaya yönelik tedbirleri almak, evrensel hizmetin yürütülmesini sağlayacak esasları tespit etmek uygulanmasını takip etmek ve net maliyetiyle ilgili hesapları onaylamak görevleri Ulaştırma Bakanlığının tarafından yerine getirilecektir. Böylece, bilgisayar ağları ve hizmetlerinin düzenlemesi konusunun Ulaştırma Bakanlığının görevi kapsamında bulunması nedeniyle, bu alanın ilk ve en yetkili kuruluşun Bakanlık olduğunu, alandaki diğer kuruluşların ise, Bakanlığa doğrudan bağlı ya da gözetiminde olan kuruluşlardan oluştuğunu görmekteyiz.

İnternet Kurulu

Ulaştırma Bakanlığı bünyesinde ilk olarak 1998 yılında "İnternet Üst Kurulu" oluşturulmuştur. Bu kurul başlangıçta Ulaştırma Bakanlığının başkanlığını yaptığı, kamu kurum ve kuruluşlarının yoğunluklu olarak temsil edildiği bir görünümde idi. İlk hâliyle İnternet Kurulu şimdikinden daha farklı bir yapıya sahip, katılımın az olduğu ve Ulaştırma Bakanının başkanlık yaptığı bir kurul yapısı taşıyordu.

İnternet Kurulu, 5651 sayılı İnternet Ortamında Yapılan yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un kapsamında, yeniden düzenlenmiştir. Böylece, İnternet Kurulu; Devlet, Adalet, İçişleri, Ulaştırma Bakanlığı temsilcileri, Üniversiteler, Radyo Televizyon Üst Kurulu, Telekomünikasyon Kurumu, TÜBİTAK, İnternet Servis Sağlayıcılar, erişim sağlayıcılar, altyapı hizmeti veren kuruluşlar ve teknoloji sektörü temsilcileri ve ilgili sivil toplum kuruluşları temsilcilerini oluşturduğu geniş katılıma sahip bir kurul hâlini almıştır.

İnternet ağı alanında ulusal politikanın belirlenmesi görevini üstlenen İnternet Kurulu, ülkemizde İnternet ağı ile ilgili planlama, koordinasyon, izleme, öneri oluşturma, eğitim v.b. alanlarda projeler yürütmektedir. Bu alanda izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti ve benzeri konularda öneriler yapmak Kurulun başlıca görevlerindendir. Kurul kararlarının icrası ise, TİB tarafından yerine getirilecektir. 5651 sayılı Kanun TİB'e "İnternet Kurulu" ile gerekli işbirliği ve koordinasyonu sağlama; bu Kurulca benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alma hususlarını bir görev olarak yüklemiştir. Bu yasal düzenleme göz önünde bulundurulduğunda, İnternet Kurulu kararlarının istişari nitelikte kalmayıp, icrai yönünün de bulunduğunu söylemek mümkündür (Özen, Baştürk, 2011).

Bilgi Teknolojileri ve İletişimi Kurumu

5809 sayılı Elektronik Haberleşme Kanunu ile Telekomünikasyon Kurumunun adı "Bilgi ve Teknolojileri ve İletişim Kurumu" şeklinde değiştirilerek görev ve yetkileri yeniden düzenlenmiştir. Anılan Kanunun'un 3/1-h maddesinde, "Elektronik Haberleşme: Elektiriksel işaretlerle dönüştürülebilen her türlü, işaret, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını ifade eder." şeklinde tanımlanmıştır. Bu tanım karşısında, bilgisayar ağları ve İnternet ağı, 5809 sayılı Kanun anlamında "elektronik haberleşme" olarak değerlendirilecek ve 5809 sayılı Kanun hükümlerine tabi olacaktır.

Ülkemizde elektronik haberleşme alanına ilişkin olarak “regülasyon-düzenleme” yapma yetkisi Bilgi Teknolojileri ve İletişim Kurumuna aittir. Kurumun 5809 sayılı Kanun çerçevesinde en önemli yetkisi, İnternet başta olmak üzere elektronik haberleşmede “yetkilendirme” ve “denetleme” işlevine sahip olmasıdır.

5369 sayılı Evrensel Hizmetin Sağlanması Hakkında Kanun’un 2.maddesi ile bir elektronik haberleşme türü olarak İnternet erişimi de “evrensel hizmet” kabul edilerek, Kanun kapsamına alınmış ve Kurum’a bazı görevler verilmiştir.

Telekomünikasyon İletişim Başkanlığı

TİB’in Kuruluş Amacı

23 Temmuz 2005 tarihinde 5397 sayılı Kanun ile Bilgi Teknolojileri ve İletişim Kurumu bünyesinde, Telekomünikasyon İletişim Başkanlığı kurulmuştur. TİB’in kuruluşunun temel amacı, telekomünikasyon yoluyla yapılacak iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması işlemlerini istihbari amaçlı olarak merkezî bir kuruluştan yürütme düşüncesidir. Gerçekte, 5397 sayılı Kanun’un genel gerekçesinde, 11 Eylül 2001 den sonra artan terör olaylarına vurgu yapılarak, istihbarat amaçlı iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması işlemlerinin terörle ve suçlulukla mücadelede önemine değinmektedir. Nitekim, 5397 sayılı Kanun, belirtilen amacına uygun olarak, 2559 sayılı Polis Vazife ve Salahiyet Kanunu, 2803 sayılı Jandarma Teşkilat, görev ve Yetkileri Kanunu ile 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilat Kanunlarında değişiklikler getirmiştir. Belirtilen görevleri gerçekleştirmek üzere, Bilgi Teknolojileri ve İletişim Kurumu Başkanına doğrudan bağlı, “Telekomünikasyon İletişim Başkanlığı” adıyla merkezî bir kuruluş oluşturulması da yine aynı Kanun ile düzenlenmiştir. (5397/ md. 1/9)

TİB, ilk kuruluşunda bilgisayar ağlarına ilişkin hiçbir yetki ve görevi bulunmayıp sadece telekomünikasyon yoluyla yapılan iletişim alanında yetkileri bulunan bir kuruluş kimliğinde idi. Fakat 2007 yılında 5651 sayılı Kanun’un yürürlüğüne girmesi ile birlikte İnteret Sujelerinin sorumluluklarının yerine getirilmesi ve “İnternet ortamında işlenen suçlarla mücadele” anlamında tüm görevler TİB’e verilmiştir. TİB’in belirtilen İnternet alanına ilişkin görevlerini yerine getirmek üzere 5607 sayılı Kanun’un yürürlüğe girmesini müteakip, TİB nezdinde, İnternet Dairesi Başkanlığı adında bir birim oluşturulmuştur. Böylelikle, telekomünikasyon yoluyla yapılan iletişimin tek bir merkezden denetlenmesi amacıyla kurulan TİB, 2007 yılında İnternet ağı alanına ilişkin görevleri de yüklenmiş olan bir kurum hüviyetine dönüşmüştür(Özen, Baştürk, 2011).

TİB’in Bilgisayar Ağlarına İlişkin Görev ve Yetkileri

5651 sayılı kanun, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde kurulan Telekomünikasyon İletişim Başkanlığına birçok görev vermiş ve yetki tanımıştır. Bu görev ve yetkiler arasında, İnternet ağı ile ilgili olmayanlar da yoğun olarak bulunmakla birlikte, konumuz açısından bakıldığında, bilgisayar ağları ve İnternetle ilgili olanların oldukça önem taşıdıkları göze çarpmaktadır.

5651 sayılı Kanun’un 10/4. maddesine göre, kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, TİB’in bu kanun kapsamındaki görev ve yetkileri şunlardır:

(4) Kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Başkanlığın bu Kanun kapsamındaki 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 İnternet ortamında yapılan ve bu kanun kapsamına giren suçları oluşturan içeriğe

sahip faaliyet ve yayınları önlemeye, İnternetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usûller dâhilinde Kurumca karşılanacak çalışma kurulları oluşturmak.

- b) İnternet ortamında yapılan yayınların içeriklerini izleyerek bu kanun kapsamına giren suçların işlendiğinin tespiti hâlinde, 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 usûlleri belirlemek
- d) İnternet ortamındaki yayınların izlenmesi suretiyle bu kanunun 8'inci maddesinin birinci fıkrasında 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 İnternet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak
- g) Bu kanun'un 8'inci maddesinin birinci fıkrasında sayılan suçların, İnternet 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

İNTERNET



TİB'in yetki ve sorumlulukları ile ilgili detaylı bilgiye <http://www.tib.gov.tr/tr/> adresinden ulaşabilirsiniz.

İnternet Daire Başkanlığı

TİB bünyesinde, bilgisayar ağları ile ilgili işlevleri yerine getirmekle görevlendirilmiş olan, İnternet Daire Başkanlığı adıyla faaliyet gösteren birim bulunmaktadır.

İnternet Daire Başkanlığının görevleri, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik'te gösterilmiştir. Anılan yönetmeliğin 22/A maddesinde İDB'nin görevleri,

a) 17 nci maddenin (j), (k), (l), (m), (n), (o), (p), (r), (s), (t), ve (u) bentleri kapsamında sayılan görevleri yerine getirmek ve buna ilişkin iş ve işlemleri yürütmek, Bu yönetmeliğin ilgili bentleri şöyledir:

- j) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kapsamında Ulaştırma Bakanlığı, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak İnternet ortamında yapılan ve 5651 sayılı Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak;

bu amaçla gerektiğinde, her türlü giderleri kurumca karşılanacak çalışma kurulları oluşturmak,

- k) İnternet ortamında yapılan yayınların içeriklerini izleyerek, 5651 sayılı Kanun kapsamına giren suçların işlendiğinin tespiti hâlinde, İnternet ortamında yapılan yayınlara erişimin engellenmesine yönelik olarak 5651 sayılı Kanun’la öngörülen tedbirleri almak,
- l) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek,
- m) 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,
- n) İnternet ortamındaki yayınların izlenmesi suretiyle, 5237 sayılı Türk Ceza Kanunu’nda yer alan; intihara yönlendirme (madde 84), çocukların cinsel istismarı (madde 103, birinci fıkra), 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 ile 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun’da yer alan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dâhil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak,
- o) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgarî kriterleri belirlemek,
- p) (n) bendinde sayılan suçların, İnternet 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 dâhilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak,
- r) İnternet Kurulu ile gerekli işbirliği ve koordinasyonu sağlamak; İnternet Kurulunca izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları almak,
- s) İlgili mevzuat kapsamında hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararlarını uygulamak ve buna ilişkin iş ve işlemleri yürütmek,
- t) İçeriği, (n) bendinde belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması hâlinde veya içerik veya yer sağlayıcısı yurt içinde bulunsan bile, içeriği çocukların cinsel istismarı (madde 103, birinci fıkra) ve müstehcenlik (madde 226) suçlarını oluşturan yayınlara ilişkin olarak resen erişimin engellenmesi kararı vermek ve bu kararı, erişim sağlayıcısına bildirerek gereğinin derhal ve en geç kararın bildirilmesi anından itibaren yirmi dört saat içinde yerine getirilmesini istemek,
- u) (t) bendine göre verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi hâlinde, Cumhuriyet Başsavcılığına suç duyurusunda bulunmak,

b) Başkanlığın bilişim ve İnternet alanındaki faaliyetleri için gerekli sistemleri oluşturmak, altyapıyı kurmak, kurdurmak, geliştirmek, işletmek, bakım ve onarımlarını yapmak veya yaptırmak ve bu alandaki teknolojik gelişmeleri takip etmek ve Başkana görüş bildirmek,

- c) Erişim sağlayıcılar ve yer sağlayıcılar ile ilgili iş ve işlemleri yürütmek,
 - d) İnternet toplu kullanım ve sağlayıcılarıyla ilgili olarak mevzuatta Başkanlığa verilen görevleri yerine getirmek,
 - e) Başkanlığın bilişim ve İnternet alanındaki faaliyetleri ile ilgili yurt içi ve yurt dışı gelişmeleri takip etmek, bu kapsamda ulusal ve uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak ve gelişmelerin Başkanlık hizmetlerine yansıtılması için önerilerde bulunmak,
 - f) Başkan tarafından verilen diğer görevleri yerine getirmek olarak düzenlenmiştir.
- Yönetmelik ile tanınan ve tek başına sahip kılındığı yetkiler (Yön. Md.22/A) yönüyle bakıldığında, Ülkemizde İnternet alanına özgülenmiş ve “uygulayıcı” tek birimin İnternet Daire Başkanlığı olduğu söylenebilecektir.

Özet

Bilişim Hukuku, bilişim teknolojilerindeki gelişmeler ve yenilikler sebebiyle mevcut yasal düzenlemelerin yetersiz kalması sebebiyle ortaya çıkmış bir hukuk dalıdır. Kısa bir tanım vermek gerekirse: Bilişim hukuku; siber/elektronik ortamın düzenlenmesi ve bilişim konusundaki ihtilafların çözümü ile uğraşan multi-disipliner hukuk dalıdır. Bilişim, bilginin (verilerin) bilgisayarlar aracılığıyla elektronik olarak depolanması yanında işlenmesini ve iletilmesini kapsamaktadır. Bir başka ifadeyle, bilişim, bilgisayarda da faydanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır bir hâle gelmesini konu alan akademik ve mesleki disipline verilen isimdir. Bilgisayar kullanma bilimi “computer science” in Türkçedeki karşılığıdır.

İnternet, birden fazla haberleşme ağının (network), birlikte meydana getirdikleri bir iletişim ortamıdır. Bu iletişim ağları, bilgisayarlar ile örülmüştür. Yani, İnternet bilgisayarlar arasında kurulmuş bir haberleşme ağıdır. İnternet, kişilerin dünya üzerinde birbirleri ile çok geniş amaç ve içerikte iletişim kurmalarını, bilgi alışverişinde bulunmalarını sağlayan ortak iletişim alt yapısıdır. Ancak, İnternet dünyadaki bilgisayar ağlarına bağlantı kurabilen ve bunu dünya çapında kabul edilen ilgi ağları protokolüne bağlı olarak özel bir ağ mimarının tanınması vasıtasıyla gerçekleştirerek bilgiye erişim sağlayan bir bilgi ağıdır.

İnternetin ortaya çıkışı soğuk savaş döneminde Sovyetler Birliği'nin 1957'de Sputnik uydusunu uzaya göndermesiyle başlamıştır. Bu gelişme üzerine Amerikan Hükümeti, tek bilgisayardan bağımsız olarak çalışabilen bir ağ kurma fikrini ulusal güvenlik gerekçesiyle geliştirmek için çalışmalara başladı. Amerikan Hükümeti, Savunma Bakanlığına bağlı olan ve birbirinden uzakta olan bazı askerî birliklerin geliştirdiği projelerin ortak bir ağ üzerinden birleştirilmesi temeline dayanan ARPA (Advanced Research Project Agency) adlı bir birim oluşturmuş ve daha sonraki süreçte bu farklı sistemleri birbirine bağlamak için ARPANET adlı bir askeri bilgisayar ağı kurulmuştur.

Zamanla önce bu sistemdeki farklı özellikteki bilgisayarların birbirini tanımaya yarayan ve aralarındaki uyumsuzlukları çözmeye yarayan, günümüzde de dünyadaki milyonlarca bilgisayarın ve yerel ağların birbiriyle iletişim kurmasına yarayan kurallar bütünü olan TCP/IP (Transport Control Protocol/Internet Protocol) kuralları gibi kurallar geliştirilmiştir. Bu sistem sonradan sivil bilgisayarların kullanımına açılmış ve 1990'da sistem daha da geliştirilerek bugünkü hâlini almıştır.

Türkiye'de ise ilk İnternet bağlantısını 12 Nisan 1993 tarihinde Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) destekli bir proje ile Orta Doğu Teknik Üniversitesi (ODTÜ) gerçekleştirmiştir.

Bilişim Sistemi, Yeni Türk Ceza Kanunu'nun 243. madde gerekçesinde, bilişim sistemi, “veri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir.” şeklinde tanımlanmıştır. Avrupa Konseyi Siber Suç Sözleşmesi'nin “Tanımlar” başlıklı 1. maddesinde “bilgisayar sistemi” terimi, “bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı” ifade etmektedir.

World Wide Web (www) kısaca web; birçok İnternet 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. Domain Name, (DNS, Domain Name System/ alan adı sistemi) olarak adlandırılan hiyerarşik bir isimlendirme sistemi ile (alan adı sistemi), İnternete bağlı bilgisayarlara ve bilgisayar sistemlerine isimler verilir.

Türkiye'de İnterneti yönetmekle sorumlu kurumlar sırasıyla Ulaştırma Bakanlığı, İnternet Kurulu, Bilgi Teknolojileri ve İletişimi Kurumu, Telekomünikasyon İletişim Başkanlığı ve İnternet Daire Başkanlığıdır. Ulaştırma bakanlığı her düzenlemede söz sahibi başat kurumdur. Günümüzde adını en sık duyduğumuz kurum ise yetkilerinin çokluğu ve önemi yüzünden Telekomünikasyon İletişim Başkanlığıdır. İnternetle ilgili her türlü yargı kararının ve aynı zamanda 5651 sayılı yetkinin kendisine verdiği erişim engelleme vb. kararların yoğun bir şekilde uygulandığı bir kurum olma özelliğine sahiptir.

Kendimizi Sınavalım

1. Bilgisayarda faydanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır bir hâle gelmesini konu alan akademik ve mesleki disipline ne ad verilir?
 - a. İnternet
 - b. Veri
 - c. Bilişim
 - d. Akademi
 - e. Üniversite
2. Dünya çapında İnternet numaralarının tahsisini yöneten kurum aşağıdakilerden hangisidir?
 - a. IASSR
 - b. IANA
 - c. NASA
 - d. ISS
 - e. IES
3. Aşağıdakilerden hangisi “gov” uzantılı İnternet sitesi açma hakkına sahiptir?
 - a. Askeri kurumlar
 - b. Ticari kuruluşlar
 - c. Sivil toplum örgütleri
 - d. Hükümete bağlı kuruluşlar
 - e. Eğitim kurumları
4. İnternet’in ortaya çıkışında önemli rol oynamış olan ABD’ de hazırlanan askerî proje aşağıdakilerden hangisidir?
 - a. World Wide Web
 - b. Echelon
 - c. Carnivore
 - d. Arpanet
 - e. Telnet
5. Türkiye’ de İnternete ilk olarak kaç yılında bağlantı yapılmıştır?
 - a. 1990
 - b. 1991
 - c. 1992
 - d. 1993
 - e. 1994
6. Türkiye’ de IP numarası vermekle yetkili kurum aşağıdakilerden hangisidir?
 - a. Ulaştırma Bakanlığı
 - b. TİB
 - c. Ulakbim
 - d. Emniyet Genel Müdürlüğü
 - e. Bilim, Sanayi ve Teknoloji Bakanlığı
7. Türkiye’ de İnternete ilk olarak nereden giriş yapılmıştır?
 - a. İstanbul Teknik Üniversitesi
 - b. Orta Doğu Teknik Üniversitesi
 - c. Gebze Yüksek Teknoloji Enstitüsü
 - d. Bilim, Sanayi ve Teknoloji Bakanlığı
 - e. Ulaştırma Bakanlığı
8. Türkiye’ de 5651 sayılı yasa ile kendisine İnternet erişim engeli yetkisi verilen kurum hangisidir?
 - a. Ulaştırma Bakanlığı
 - b. Bilim, Sanayi ve Teknoloji Bakanlığı
 - c. Tübitak
 - d. İnternet Kurulu
 - e. Telekomunikasyon İletişim Başkanlığı
9. Aşağıdakilerden hangisi Türkiye’ de İnternetin yönetiminde yetki ve sorumluluk sahibi kurumlardan biri **değildir**?
 - a. Telekomunikasyon İletişim Başkanlığı
 - b. Ulaştırma Bakanlığı
 - c. Bilim, Sanayi ve Teknoloji Bakanlığı
 - d. İnternet Kurulu
 - e. Bilgi Teknolojileri ve İletişim Kurumu
10. Bilgi ağı üzerindeki bilgi iletimi ve paylaşımını düzenleyen kurallar bütününe ne ad verilir?
 - a. World Wide Web
 - b. TCP/IP Protokolü
 - c. İnternet Erişim Sağlayıcı
 - d. İnternet Servis Sağlayıcı
 - e. İnternet Yer Sağlayıcısı

Yaşamın İçinden

İnternet dolandırıcılığı tırmanışta!

Emniyet Genel Müdürlüğü, İnternet üzerinden evlilik vaa-diyle dolandırıcılık olaylarına karşı uyardı. Emniyet tespitlerine göre Bulgaristan ve Romanya uyruklu iyi derecede Türkçe konuşan bayanlar, evlenebileceklerini söyleyerek dolandırıcılık olayına karışıyorlar.



Emniyet Genel Müdürlüğü Asayiş Dairesi Başkanlığı'ndan yapılan açıklamada, iyi derecede Türkçe konuşan yabancı uyruklu bayanların sanal alem veya televizyon kanalları vasıtasıyla ulaştıkları Türk erkeklerine Türkiye'ye veya bulundukları ülkeye gelmeyi düşündüğünü, gelmek için paralarının olmadığını, pasaport ve uçak bileti masrafları için yardımcı olmalarını istedikleri belirtildi.

İnternette en yaygın 7 dolandırıcılık yöntemleri; sahte avukatlara dikkat edin, faturanız ödendi yazısına güvenemeyin, şüpheli e-postaları açmayın, sahte iş ilanlarına güvenmeyin, her soruyu yanıtlamayın, sosyal medyada arkadaşlarınıza dikkat edin ve dolandırıcı sitelere dikkat edin.

1. Sahte Avukatlara Dikkat: İnternette dolaşan "Kredi kartı aidat masraflarını geri alın. Geçmişe dönük kapansın veya kapanmasın tüm kredi kartı aidatlarınızı bankadan sizin adınıza tahsil ediyoruz" ilanları ile aslında avukat olmayan ya da sahte avukat isimleri kullananlar vatandaşları yanıltıp bu ilanlara başvuranlara form gönderip 150 TL gibi bir para talep ediyorlar. Parayı dilerseler banka havalesi, kredi kartı ya da kapıda ödemeli tahsil ediyorlar. Avukatlık desteği para tahsil edildikten sonra tamamen kesiliyor. Banka ödemeyi ret ettiği için bundan olumlu bir cevap alınamıyor. Ayrıca başvuru formunda istenilen kişisel bilgilerin ve TC numaralarının ne yapıldığı ise bilinmiyor.

2. 'Faturanız Ödendi' Yazısına Güvenmeyin: Online ödenen faturalar dolandırıcıların iştahını kabarttı. İnternette cep telefonu ve elektrik faturasını ödeyenler ya da kontör yükleyenler "kontör satın alma, fatura tahsilatı, fatura sorgulama" adıyla bulunan sahte sitelere dikkat. Sahte sitelere kart bilgilerini giren birçok vatandaşın bilgileri ve hesapları dolandırıcıların eline geçti.

3. Şüpheli E-Postalara Dikkat: Kredi kartı kullanan kişilerin e-posta adreslerine gönderilen banka tarafından gönderilmiş görüntüsü verilen e-postalar birçok kişiyi dolandırdı. Bu e-postada bankanın yeni bir güvenlik sistemi oluşturduğu, bu nedenle de müşterinin eksik olan kimlik veya kredi kartı bilgilerini e-postada belirtilen İnternet adresine girerek güncellemesi gerektiği ifade ediliyor. Kişiler, maildeki adresi tıkladığında sahte banka sitesine yönlendiriliyor ve İnternet bankacılığı şifreleri elde ediliyor. Daha sonra ise hesapları boşaltılıyor.

4. Sahte İş İlanlarına Dikkat: İşsiz vatandaşlar e-postalarına gelen gönderilen "İnternette bıraktığınız özgeçmişinizden size ulaştık. Bünyemizde size göre boş pozisyon var." ilanı ile dolandırıldı. Maaş hesabı açmak için vatandaşların hesap ve kart bilgilerini ele geçiren dolandırıcılar hesaplardan para çektikten sonra ortadan kayboldular.

5. Ödül Kazanmadınız: İnternette dolaşırken karşısına çıkan anketi yanıtlayıp bir de cep telefonu numaralarını verenler aşırı yüksek cep faturaları ile karşılaştılar. İnternette arama yaparken sizi başka bir sayfaya yönlendiriliyor ve karşınıza yanıtladığınızda ödül kazanacağınızı belirten bir anket çıkıyorsa sakın bu anketi yanıtlamayın. Anketi yanıtlayan faturalı hat kullanıcıları faturalarının birden arttığından faturasız hat sahipleri ise hesaplarındaki bakiyenin sürekli düşmesini şikayet etti.

6. Facebook'taki Arkadaşlarınıza Dikkat: Facebook kullanıcılarının hesabını ele geçiren dolandırıcılar, arkadaş listesindekilerle normal konuşmaya başlıyor. Daha sonra kişilerden para göndermelerini ya da çeşitli mesaj dolandırıcılıkları ile hesaplarından para çekiyorlar.

7. Dolandırıcı Sitelere Dikkat Edin: Dolandırıcılar İnternet üzerinde açtıkları başta alışveriş siteleri olmak üzere vatandaşların banka hesapları ve kredi kartı bilgilerini ele geçiriyorlar. Sitelere girip İnternet üzerinden kredi kartı ile ya da bankacılık işlemi yapmak istenildiği sırada verilen komutlar takip edilerek kart yada banka hesap bilgilerinin girilmesi yeterli oluyor. Bütün bilgiler girildiğinde son tuşa yani enter'e basıldığında karşınıza "error" yazısı çıkarak sistemin hata verdiği uyarısı yapılıyor. O anda hata verdiği sanılan sistem aslında işlem yapanların kart ve banka bilgilerinin dolandırıcıların eline geçmesini sağlıyor ve bilgilere ulaşan dolandırıcılar da amacına ulaşmış oluyor."

İnternet ortamında her geçen gün yeni bir dolandırıcılık yöntemi ortaya çıkıyor. Dolandırıcılar işi daha da ilerletip yeni yöntemler buluyor. Son olarak yabancı uyruklu kızların İnternette tanıştıkları kişilerle Türkiye'de mal varlığın olduğunu bunu gelip paylaşabileceğini tapo, senet gibi belgelerle

güven vererek karşısındaki kişiden maddi destekte bulunmasını istiyor.

İstanbul'da bir kişi, sosyal medya aracılığıyla Romanya Braşov'dan tanıştığı kadının, kendisini dolandırdığı iddiasıyla savcılığa şikayette bulundu. Sevindzhan Marinova adlı yabancı uyruklu kız tarafından dolandırılan kişi ifadesine göre; "Dürüst insanları aldatmak kadar kolay bir şey yoktur. Birçok özdeyiş gibi bu da kısmen doğrudur. Her gün birçok dürüst insan dolandırıcıların kurbanı oluyor. Dürüst olmak onları korumaya yetmiyor. Dünyanın en zeki kişilerinden bazıları insanlardan para koparmak için planlar tasarlayıp bunları hayata geçiriyor. O kadar iyi tasarlanmış hileler var ki, onlara kanmamak elden değil. Ben kandırıldım 3 Milyar param gitti. Benden sonra başkaları yanmasın." dedi.

Kaynak: Milliyet Gazetesi: <http://www.milliyet.com.tr/Internet-dolandiriciligi-gundem-1943378/>

Okuma Parçası

BİLGİ ÇAĞININ HUKUKUNA GENEL BAKIŞ

Değişen ve dönüşen hukuk...

Alt yapıdaki değişim, nasıl "ikame, yayılma" ve "dönüşüm" aşamalarından geçilerek hayata geçiriliyorsa[i] onun biçimlendirdiği bir üst yapı kurumu olarak "hukuk" da aynı aşamaları izliyor. Endüstri devriminin, tarım toplumu hukuk düzeninin değişmesine yol açması gibi bilgi ekonomisi de endüstri toplumunun hukukunu şimdiden zorluyor. Bilgi ekonomisinin ürünleri, yakınsanmış iletişim teknolojileri aracılığıyla, hangi gelişmişlik düzeyinde olursa olsun dünyanın her yerinde, toplumları kendine "taraf" kılıyor. Buna "yenilikçilik" de eklendiğinde, bir taraf lehine artan "rekabet edebilirlik", diğer tarafı iyice "edilgin tüketici" haline getiriyor. Ancak aynı "yenilikçilik", az gelişmiş çoğunluk içinden bunu farkedip doğru politikalarla harekete geçebilenleri, "edilgin tüketiciler" olmaktan çıkarıp "üreticiler"e dahil edilebilen bir fırsat. Yale hukuk profesörü Jochai Benkler (2006) [ii], ister zengin ister fakir ülkelerden olsun, sermayesi "zi-hinsel emek", ürünü "bilgi" olan ve "yenilikçi bir eko-sistem" içinde ağlar yoluyla birbirleriyle etkileşime giren "bilgi endüstrisi üretici"lerinden çok umutlu. Onların merkezi piyasalara bağımlı olmayan üretim biçimlerinin yaratacağı yeni değerlerin, endüstri dönemi hukukunu da tüm insanlığın yararına dönüştüreceğine inanıyor.

Erken yola çıkanın hukuku mu?

Şurası açık ki bilgi çağının hukukuna, bilgi ekonomisinin altyapısını kuran toplumlar yön vermekteler. Bu alanda erken yola çıkan ABD -özellikle Clinton döneminde- bilgi ekonomisinin hukukunu oluşturmada önemli adımlar attı. Öte yandan Birleşmiş Milletler, OECD, Dünya Ticaret Örgütü gibi kuruluşlar tip düzenlemeler ortaya koyarak küresel ekonomiyi yaygınlaştırma çabalarını sürdürüyorlar. Avrupa Birliği'nin de 2000'li yıllardan başlayarak gündeme getirdiği, hem altyapısal hem üstyapısal köklü değişim ve dönüşüm programlarının temelinde, üye devletleri bilgi ekonomisinin "edilgin tarafı" olmaktan çıkarmak kaygı ve telaşesi var. Avrupa Birliği, hepsi "Avrupalı" olsalar da başta hukuk düzenleri olmak üzere üstyapıda farklı kültürel yaklaşımlar sergileyen "üye"lerini, ortak kurallarda birleştirebilmek için, her topluma uyarlanabilecek düzenlemeler yaparak "minimalist" bir tutum izliyor. Bir taraftan da küresel rekabete karşı, AB vatandaşlarının kişisel verilerinin transferi konusunda olduğu gibi, "hukuk"u bir kalkan olarak kullanıyor. [iii]

Bir kamusal alan olarak Internet

Ağırlıklı olarak "küresel elektronik ticaret" bağlamında seyyeden ve daha çok "özel hukuk" düzenlemelerini ilgilendiriyormuş gibi gözüken bilgi çağı hukukunun, aslında hem kamu hukuku ile kesişen hem de evrensel insan hakları hukuku alanına giren çok önemli boyutları var. İfade özgürlüğü, bilgiye erişim özgürlüğü gibi üçüncü kuşak haklar geniş ölçekte bir kamusal alan olarak Internet ortamında kullanı-

labilirken, “9/11” hadisesinin ardından başlayan sınırlamacı eğilimler ve kişisel bilgilerin gizliliğinden “feragat” gerekti- ren yaklaşım, kıta Avrupası hukuku ile Anglo-Sakson huku- ku arasında teoride ve pratikte gerilimlere yol açıyor.

Bu olgu, bilgi çağıının hukukunun biçimlendirilmesinde “İnternet’in yönetimi ve yasal düzenlenmesi gibi” çok hayati bir gündem maddesinin ortaya çıkmasının da en önemli et- kenlerinden biri. Aynı olguyla birlikte yasal düzenleme yak- laşımları da değişiyor, dönüşüyor. Dr. Yaman Akdeniz (2003) “Beyaz Kitap”ta^[iv] İnternet’in “ulusötesi, merkezi olmayan ve sınır tanımayan” doğası gereği, bu küresel ortamdaki iliş- kileri ve işlenen suçları “hiç bir devletin tek başına ve yeterli düzeyde düzenleyemeyeceğini, bu yüzden, devletlerin, kendi hukuk politikalarını bilgi çağıının alt yapısına paralel olarak çağdaştırmaları gerektiği”ne dikkat çekiyor. Dr. Akdeniz, yasal düzenlemeler alanında devletin rolü her ne kadar hâlâ hayati öneme ve yönlendirici niteliğe sahip ise de çağın gere- ği, devletin yasa yapmadan önce “risk çözümlemeleri” yap- ması, tek başına yasal düzenleme yerine; “işbirliği”, “koordi- nasyon”, “danışma”, “birlikte düzenleme” ve “öz-düzenleme” gibi yeni kavramlara daha fazla önem vermesini salık veriyor. Avrupa Konseyi Bakanlar Kurulu’nun “İnternet Üzerinde İle- tişim Özgürlüğü Bildirgesi”nde ^[v] de benimsenen Politika sürecinin açık ve saydam olmasını, ilgili tüm tarafların gö- rüşlerinin sürece katılmasını da gerektiren bu “çok katmanlı” yaklaşımın uygulanması her toplumun kendi kültürüne göre farklılıklar arz ediyor.

Kültürel farklılıklar ve yeni hukuk

Üst yapıları bilgi çağıına uyarlanmakta olan toplumlarda bu farklılıkları hukukun hemen her alanında görmek mümkün. Örneğin “bilgiye erişim” hakkı ABD’de “şeffaflık ve hesap sorulabilirlik” bağlamında ve bir “özgürlük” olarak ele alı- nırken, Avrupa Birliği konuyu “kamunun elindeki bilgile- ri –hem de bir an önce!- ekonomik dolaşıma sokma hakkı” bağlamında gündeme getiriyor. Hatta kimi Avrupa devletleri, örneğin Birleşik Krallık, kendini bunu yapması umulan “özel sektör”e bir rakip gibi görüp, “bilgi”yi vermekte cimri dav- ranarak, AB’nin bilgi ekonomisi hedeflerine hızla ulaşması- nı da geciktirebiliyor. “Gizlilik kültürü”nün baskın, devletle birey arasındaki mesafenin “uzun” olduğu toplumlar da bu konuyu toptan görmezden geliyorlar. ^[vi]

Keza, ceza hukuku alanında İnternet’te işlenen suçlardan hangisinin düzenlenmesine öncelik verileceği toplumdan topluma değişiyor. Sonuncusuna ülkelerin egemenlik hak- larına klasik yaklaşım paradigması ile insan hakları savunu- cusu sivil toplum örgütlerinin haklı muhalefeti de eklenince, örneğin Avrupa kökenli bir “Siber Suçlar Konvansiyonu” yıl- lardır uygulamaya geçemiyor. Küresel bir düzenleme olması amaçlanan bu Konvansiyon ^[vii] insan hakları ve ceza huku- kunun temel ilkeleri açısından gerçekten de “sakıncalı” dü- zenlemeler içerdiği için “hukukun üstünlüğü”ne bağlı klasik

Avrupa demokrasileri tarafından hemen imzalanmadığı ya da çekince konarak imzalandığı halde, “9/11 sonrası ABD’si” ile AB’ne yeni giren Sovyetler sonrası devletler tarafından “gözü kapalı” imzalanabiliyor...

İnternet gerçekten “sınırsız” mı?

İnternet’in doğası gereği “ulusötesi, merkezi olmayan, sınırsız” özellikleri geniş çaplı kabul görmüşken, Goldsmith ve Wu (2006) ^[viii] ise “İnternet’i Kim Denetliyor: Sınırsız Bir Dünya Yanılsamaları” başlıklı ortak kitaplarında İnternet’e yakıştırılagelen “sınırsız”lığın tam bir yanılsama olduğunu, günümüzde ekonomik bakımdan kim güçlü ise İnternet’i de kendi sınırları içinde ve hatta ötesinde onun denetim altın- da tuttuğu savını ileri sürüyorlar. Harvard hukuk profesörü Goldsmith, “güç blokları” diye nitelendirdiği bu ülkelerin şimdilik “ABD, Avrupa’nın kuzeyindekiler ve Çin” olduğunu vurgularken, zamanla bunların dışındaki blokların devreye girmesinin “soğuk savaşın bir teknolojik versiyonu” nun baş- langıcı ile eşanlamlı olacağını belirtiyor.

İşte bir değişik yaklaşım daha!

Sonuç olarak, bilgi çağıının hukukunu yaratacak olanların alt yapıda yaşanan çok boyutlu değişimi anlamak ve izleyebil- mek için öncelikle bilgi okur-yazarı olması ve disiplinlerarası bir yaklaşımı benimsemesi kaçınılmaz görünüyor...

Kaynaklar

- [i] Eczacıbaşı, F., “Değişebilenler Dönüşebiliyor”, Bilgi Çağı Dergisi, Mayıs, 2007 <http://www.bilgicagi.com/sayi33/>
- [ii] Benkler, J., “The Welfare of Networks: : How Social Pro- duction Transforms Markets and Freedom”, ISBN-13: 978-0-300-11056-2, Yale University Press, 2006, <http://www.benkler.org/>
- [iii] Tansuğ, A., “AB’nin yeni ekonomik silahı: “Veri Saklama Hukuku”, Güncel Hukuk Dergisi, Nisan 2005
- [iv] Akdeniz, Y., “Beyaz Kitap - İnternet’in Çok Taraflı Yö- netimi: Türkiye’deki Politika Yaratma Sürecinin Çağdaşlaş- masına Doğru”, ISBN: 975-6797-44-4, TBV Dizisi:1, Papatya Yayıncılık, 2003 <http://www.papatya.gen.tr/beyazKitap.htm>
- [v] “DECLARATION on freedom of communication on the Internet”, 28 May 2003 <https://wcd.coe.int/ViewDoc.jsp?id=37031>
- [vi] Bu konuda Türkiye’deki uygulama için: <http://www.bilgiedinmehakki.org/>
- [vii] Konvansiyon’un Türkçe metni: <http://www.ivhp.net/> “Bilgi Belge” / “Avrupa”
- [viii] Goldsmith, J., and Wu, T., “Who Controls the Internet? Illusions of a Borderless World”, ISBN: 13: 978-0-19-515266-1 ISBN-10: 0-19-515266-1, Oxford University Press, 2006

Kaynak: Avniye Tansuğ, Bilgi Çağı Dergisi, Temmuz 2007: <http://bilgicagininhukuku.blogspot.com.tr/search/label/Bilgi%20%C3%87a%C4%9F%C4%B1%20Dergisi>

Kendimizi Sıyalım Yanıt Anahtarı

1. c	Yanıtınız yanlış ise “Bilişim” konusunu yeniden gözden geçiriniz.
2. b	Yanıtınız yanlış ise “İnternetin Yönetimi” konusunu gözden geçiriniz.
3. d	Yanıtınız yanlış ise “İnternetle İlgili Bazı Önemli Kavramlar” konusunu gözden geçiriniz.
4. d	Yanıtınız yanlış ise “İnternetin Yönetimi” konusunu gözden geçiriniz.
5. d	Yanıtınız yanlış ise “İnternetin Tarihçesi” konusunu gözden geçiriniz.
6. c	Yanıtınız yanlış ise “İnternetle İlgili Bazı Önemli Kavramlar” konusunu gözden geçiriniz.
7. b	Yanıtınız yanlış ise “İnternetin Tarihçesi” konusunu gözden geçiriniz.
8. e	Yanıtınız yanlış ise “Telekomünikasyon İletişim Başkanlığı” konusunu gözden geçiriniz.
9. c	Yanıtınız yanlış ise “Türkiyede İnternetin Yönetimi: Yetkili ve Sorumlu Kurumlar” konusunu gözden geçiriniz.
10. b	Yanıtınız yanlış ise “İnternetle İlgili Bazı Önemli Kavramlar” konusunu gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Dar anlamda bilişim suçlarına örnek olarak yetkisiz erişim, verilere yönelik suçlar, bilişim ağlarına yönelik suçlar gösterilebilir.

Sıra Sizde 2

Interconnected Networks

Sıra Sizde 3

Web Tarayıcısı

Sıra Sizde 4

Ulaştırma Bakanlığı, İnternet Kurulu, Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı

Yararlanılan Kaynaklar

- Akıncı, H; Alıç, E; Er, C, (2002).**Türk Ceza Kanunu ve Bilişim Suçları, İnternet ve Hukuk**, Der: Yeşim M. Atamer, İstanbul, Bilgi Üniversitesi Yayınları
- Avşar Z, Öngören G. (2010). **Bilişim Hukuku**, Ankara: Türkiye Bankalar Birliği Yayınları
- Bayram, M. H. (2011). **Avrupa Birliği ve İnternet Hukuku**, Ankara: Seçkin Yayınevi
- Dülger, M. V. (2014). **Bilişim Suçları ve İnternet İletişim Hukuku**, Ankara: Seçkin Yayınevi
- Eralp, Ö. (2012). İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu, Ankara: Eralp Kitap
- Eralp, Ö. (2004). **Bilişim Suçlusuna Giden Yol - IP**, <http://www.ozgureralp.av.tr/web/makaleler/bilisim-suclusuna-giden-yol-ip/> (Erişim T: 15.08.2015)
- Karaçay, T (2013). İnternet Yönetimi, Bilişim Dergisi 2013, Eylül
- Oğuz H, (2012). İnternet Ortamında Kişilik Haklarının İhlali ve Korunması, Adalet: Ankara
- Öngören, G. (2006). **İnternet Hukuku**, İstanbul: Öngören Yayıncılık
- Özen M, Baştürk, İ. (2011). **Bilişim-İnternet ve Ceza Hukuku**, Ankara: Adalet Yayınevi
- Özkan, H. (2014). **Sorularla Bilişim Hukuku Mevzuatı**, Ankara: Adalet Yayınevi
- Tansuğ, A. (2007). **Bilgi Çağının Hukukuna Genel Bakış**, Bilgi Çağı Dergisi, Temmuz2007:<http://bilgicaginhukuku.blogspot.com.tr/search/label/Bilgi%20%C3%87a%C4%9F%C4%B1%20Dergisi> (Erişim T: 15.08.2015)
- Taşkın, Ş. C. (2008). **Bilişim Suçları**, İstanbul: Beta Yayınevi
- Tevetoğlu, M. (2006). (Editör).**Bilişim Hukuku**, İstanbul: Kadir Has Üniversitesi Yayınevi
- Yazıcıoğlu, R, Y, (1997) **Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları**, İstanbul: Alfa Yayınevi
- www.tdk.gov.tr
- Milliyet Gazetesi: <http://www.milliyet.com.tr/İnternet-dolandiriciligi-gundem-1943378/>
- (http://www.heweso.com/newsdetails/57/İnternet_adresi_nedir.html) (Erişim T:15.08.2015)

2

Amaçlarımız

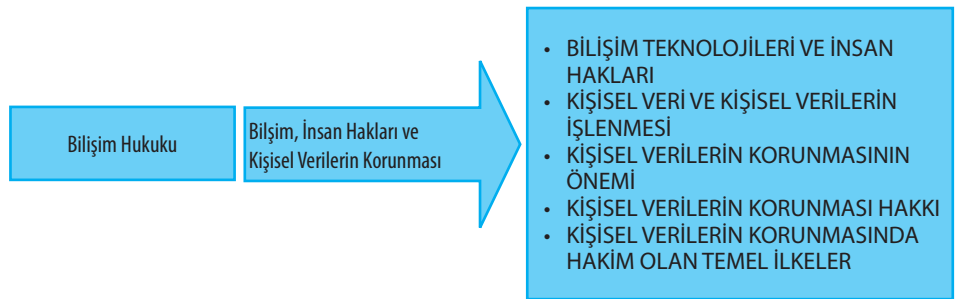
Bu üniteyi tamamladıktan sonra;

- İnsan hakları ile bilişim teknolojileri arasındaki ilişkiyi açıklayabilecek,
 - Kişisel veri ve kişisel verilerin işlenmesini tanımlayabilecek,
 - Kişisel verilerin korunması hakkının diğer temel hak ve özgürlüklerle ilişkisini açıklayabilecek,
 - Kişisel verileri korunmasında hakim olan temel ilkelerin neler olduğunu açıklayabilecek
- bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- İnsan Hakları
- Kişisel Veri
- Kişisel Verilerin Korunması
- Özel Yaşamın Gizliliği
- Düşünceyi Açıklama Özgürlüğü
- Özel Haberleşmenin Gizliliği

İçindekiler



Bilişim, İnsan Hakları ve Kişisel Verilerin Korunması

BİLİŞİM TEKNOLOJİLERİ VE İNSAN HAKLARI

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.

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 kağıdır. 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 bulunmaktadır. 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 işbirliği 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 işbirliği 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 öngöründe 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 hakim olan temel ilkeleri belirlemek gerekir.

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 gereken ilkelerin hukuksal güvence altına alınmasını gerektirir. Nitekim bu gereksinim, dünyada 100’ ün üzerinde devlette kişisel verilerin korunmasına yönelik hukuksal düzenlemelerin kabul edilmesine neden olmuştur.

Kişisel verilerin korunması hakkı, bilişim teknolojilerindeki gelişmeler ile ortaya çıkan bir insan hakkıdır. Bu yeni 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 deyimssel 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 ayırım 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 gerçekleştirilmesi 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 ayırım yapmak gerekir. Buna göre, kamusal alanların kişilerin görüntülerini alan araçlarla izlenmesi ancak bu görüntülerin kayıt edilmemesi durumunda özel yaşama müdahale sayılmaz. Nitekim burada kamera ile yapılan izlemenin, kamusal alanda, örneğin bir meydana, 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, uyarılma 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.

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 başladı. Bunda teknolojiye, 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, teknolojiye ilişkin 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 olmaktadır. 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 tanıır. Bu tehlikeleri bertaraf etmek ve sözünü ettiğimiz dengeyi sağlayabilmek için 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.

KİŞİSEL VERİLERİN KORUNMASI HAKKI

Genel Olarak

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 işleminin 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 denge- nin yeniden kurulmasının gerekliliklerini titizlikle ortaya koymasındır.

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 öngörülmişti (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 (informationelle 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 zedelemeyiz. 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 tür 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 öngörül-müş 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 adlandırılacak 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):

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

Tablo 2.1



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 ilgilendirmedeği”* 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 suçların 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 yönetimdekilerin 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 ve-

rir. 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 araştırarak, değerlendiren, yayınlayan basın kuruluşları, diğer yanda, kişisel bilgilerinin paylaşılmasını 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 ögesidir. 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 anonimlik (complete 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 Milletler 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, gözetimindeki 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, saklanması, işlenmesinin ve yayılmasının doğurabileceği zararın daha büyük olduğu düşüncesidir.

Bu noktada ilk akla gelen “*ayrımcılık yasağı*”dır. Kişilerin ırkları, etnik kökenleri, cinsel tercihleri dolayısıyla bu kimselere ayrımcılık yapılamayacağı ilkesi, insan haklarının eksen kavramlarından “*eşitlik*”in bir gereğidir. Bu ilke, pek çok devlette anayasal düzeyde korunmaktadır. Özellikle genetik araştırmaların hız kazanması ve kişilerin genetik yapılarına ilişkin bilgilerin toplandığı gen bankalarının kurulması ile ayrımcılık yasağının yeni bir boyutta tartışılmaya başlandığını da belirtmek gerekir.

Hassas veriler kapsamında değerlendirilen önemli bir hak kategorisi de kişilerin dinsel inançlarına ilişkin verilerdir. Din ve inanç özgürlüğü, kişisel verilerin korunması hakkının tartışılmaya başlanmasından çok daha eskilere dayanan bir geçmişe sahiptir. Din ve inanç özgürlüğünün kapsamında dinini açıklamaya zorlamama da yer alır. Gerçekten kimsenin dini inanç ve kanaatlerini açıklamaya zorlanamayacağı konuya ilişkin pek çok metinde de belirtilmiştir. Böylece inanç ve kanaate öğrenme biçiminde bile olsa müdahale edilemeyeceği saptanmıştır (Kaboğlu, 2002). Bu bağlamda din ve inanç özgürlüğü ile kişisel verilerin korunması hakkının birbirinin desteklediği söylenebilir.

Bunun yanında örneğin sağlık verilerinin gizli tutulması, hekimin sır saklama yükümlülüğü hasta-hekim arasındaki ilişkinin bir gereği olarak binlerce yıldır kabul edilen bir gerekliliktir. Hipokrat yemininde de yer alan bu ilke, sağlık hizmetlerine ilişkin pek çok ülkedeki yasal düzenlemelere de yansımıştır.

Ancak bu temel hak ve özgürlüklerin kişisel verilerin korunmasına katkısı oldukça sınırlıdır: Ayrımcılık yasağı, kişilerin hangi etnik kökene, dinsel gruba dahil olduklarının ya da cinsel tercihlerinin, genetik yapılarının ne olduğunun kayıt altına alınmasını değil, bu bilgilerden hareketle farklı işlem görmelerini önlemeyi amaçlamaktadır. Sağlık verilerine ilişkin hekimlerin ulaştıkları bilgileri gizli tutmaları gerekliliği de kişisel verilerin korunması hakkı kapsamında yer alan ilkelerin yalnızca birinin güvencesini oluşturur. Bunun gibi din ve inanç özgürlüğünün getirdiği koruma da bu konudaki verilerin işlenmesi karşısında zayıf kalmaktadır.

Kişisel verilerin korunmasına yönelik yasal düzenlemenin yokluğunda bunlar ve benzeri diğer ilkeler sınırlı da olsa bir koruma sağlamaktadır. Ancak tam bir güvence için kişisel verilerin korunması hakkının tanınması gerekir. Ayrıca bu güvence yukarıda belirtilen diğer hak ve özgürlüklerin de etkin bir şekilde sağlanmasına hizmet edecektir.

KİŞİSEL VERİLERİN KORUNMASINDA HÂKİM OLAN TEMEL İLKELER

Genel Olarak

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 ünite de 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, Birleşmiş 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. Avrupadaki 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 Birleşmiş 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 doğrudan 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 işleme 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 anlaşılabilceği 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 yönelmesi 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 işleme 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 yükümlülükler 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,
- siyasi 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.

Hassas sayılan veriler hangileridir?



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 yönelik 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 sınırlandırılmasına ilişkin ilkeler burada da uygulanacaktır. Avrupa İnsan Hakları Sözleşmesinde ve demokratik devletlerin Anayasalarında temel hak ve özgürlüklerin ancak yasa ile sınırlandırılabilceği 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 aşılması 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.

Özet

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. 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 tanımında "her türlü" bilgi ifadesinin kullanılması oldukça geniş bir alanın hedeflendiğinin işaretidir. Burada bilginin türüne ilişkin herhangi bir ayırım 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.

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 Bilemiş 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.

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 işleme 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 anlaşılabilceği 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.

İlgili kişinin katılım ve denetimine yönelik ilkeler çok çeşitlidir. Bu kapsamda kişiye bazı haklar tanındığı, veri işleyenlere ise yükümlülük yüklendiği görülür. Bu hak ve yükümlülükler 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

Kendimizi Sıneyalım

- Aşağıdakilerden hangisi bilişim teknolojilerinin gelişmesinden etkilenen temel insan haklarından biri **değildir**?
 - Düşünceyi açıklama özgürlüğü
 - İnternet'e erişim hakkı
 - Kişisel verilerin korunması
 - Örgütlenme hakkı
 - Yaşam hakkı
- Aşağıdakilerden hangisi kişisel verinin tanımıdır?
 - Bir kişi için özel olarak hazırlanmış veri demetidir.
 - Bir kişinin kendi başına hazırladığı veri demetidir.
 - Belirli ya da belirlenebilir bir kişiye ilişkin her türlü bilgidir.
 - İstatistik amacıyla toplanan anonim bilgidir.
 - Bir tür bilgisayar yazılımıdır.
- Aşağıdakilerden hangisi kişisel veri **değildir**?
 - TC kimlik numarası
 - Bir kişinin sabıka kaydı
 - Bir kişinin akciğer filmi
 - Bir limited şirketin ticaret ünvanı
 - Bir kişinin pasaport numarası
- Kişisel verilerin işlenmesi kısaca nasıl tanımlanabilir?
 - Kişisel verilerden anlamlı sonuçlar çıkarılmasıdır.
 - Kişisel verilere ilişkin konuların değerlendirilmesidir.
 - Kişisel veriler üzerinde gerçekleştirilen her türlü işlemdir.
 - Kişisel verilerin bilişim sistemlerinden basılı dosyalara aktarılmasıdır.
 - Kişisel verilerin başka bilgiler katılarak zenginleştirilmesidir.
- Alman Anayasa Mahkemesi, "bilgilerin geleceğini belirleme hakkını" hangi temel ilkelere dayandırarak geliştirmiştir?
 - İnsan onuru ve kişiliğın korunması
 - Düşünceyi açıklama özgürlüğü
 - Özel yaşamın gizliliğı hakkı
 - Bilgi edinme hakkı
 - Din ve vicdan özgürlüğü
- Avrupa İnsan Hakları Mahkemesi kişisel verilerin korunmasına ilişkin kararlarını Avrupa İnsan Hakları Sözleşmesinin aşağıdaki hükümlerinden hangisi çerçevesinde değerlendirir?
 - Yaşam hakkı (Madde 2)
 - Özel yaşamın gizliliğı hakkı (Madde 8)
 - İşkence yasağı (Madde 3)
 - Düşünceyi açıklama özgürlüğü (Madde 10)
 - Adil yargılanma hakkı (Madde 6)
- Aşağıdaki metinlerden hangisinde kişisel verilerin korunması açıkça tanımlanmış ve ayrı bir hak alanı olarak düzenlenmiştir?
 - Avrupa İnsan Hakları Sözleşmesi
 - Alman Temel Yasası
 - Birleşmiş Milletler Evrensel İnsan Hakları Beyanname
 - Avrupa Birliğı Temel Haklar Şartı
 - Amerika Birleşik Devletleri Anayasası
- Aşağıdakilerden hangisi düşünceyi açıklama özgürlüğü kapsamında **korunmaz**?
 - Özel yaşamın gizliliğı hakkı
 - Serbestçe düşünce ve bilgilere ulaşabilme
 - Düşünce ve kanaatlerden dolayı kınanmama
 - Çeşitli yollarla düşüncelerini savunabilme
 - Düşüncelerini yayabilme
- Aşağıdakilerden hangisi kişisel verilerin kaliteli olması ilkesinin gereklerinden biri **değildir**?
 - Hukuka ve dürüstlük kurallarına uygun işleme
 - Belirli, açık ve meşru amaçlar için toplanma
 - Doğru ve eğer gerekli ise güncel olarak tutulma
 - Amacın gerektirdiğinden uzun süre tutulmama
 - Yüksek ekonomik değeri olma
- Kişisel verilerin korunmasıyla ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?
 - Özel nitelikli kişisel veriler (hassas veriler) veri koruma ilkelerinin uygulanmadığı veri kategorilerini nitelemek için kullanılan bir deyimdir.
 - Veri güvenliğı kişisel verilerin korunmasından hakim olan temel ilkelere biridir.
 - Kişisel verilerin korunmasında hakim olan temel ilkeler uyarınca ilgili kişinin otomatik kararların konusu olmama hakkı bulunur.
 - Kişisel verilerin toplanma amaçlarına uygun bir şekilde işlenmesi gerekir.
 - Kişisel verilerin korunması hakkı Avrupa Birliğı Temel Haklar Şartı'nda açıkça düzenlenmiştir.

Yaşamın İçinden

“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 baskısını 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 bireyle-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 – NCTA)'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>

Okuma Parçası

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 sorumlulukları 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 kritik kaynaklarla ilgili eylemlere ve enformasyon teknolojisi tasarımına hem de hükümet eylemlerine dayanır.
5. Özellikle, erişim ve İnternet kullanımı, teknik nedenlerden dolayı ağır istikrarlı ve sürekli biçimde işleminin 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, ilkelere 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.

(Ünite'nin 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/>

Kendimizi Sınyalım Yanıt Anahtarı

- | | |
|-------|---|
| 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. |

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Kişinin, ırksal veya etnik kökenine, siyasal görüşüne, dinsel ya da felsefi inancına, sendika üyeliğine, sağlık ya da cinsel yaşamına ilişkin bilgiler bu kategoride sayılmaktadır.

Yararlanılan Kaynaklar

- Bu Ünite kapsamında bazı bölümler “Elif Küzeci, Kişisel Verilerin Korunması, Turhan, Ankara 2010” künyeli eserden özetlenerek aktarılmıştır.
- 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 Knows, Safeguarding Privacy in a Networked World, ABD.
- Kaboğlu, İ. (2002). Özgürlükler Hukuku, Ankara: İmge.
- Küzeci, E. (2010). Kişisel Verilerin Korunması, Ankara: Turhan.
- 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.

3

Amaçlarımız

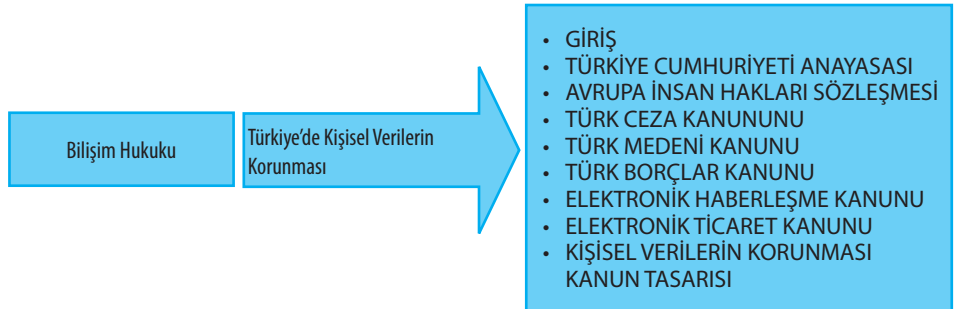
Bu üniteyi tamamladıktan sonra;

- Türkiye Cumhuriyeti Anayasası'nda kişisel verilerin korunmasına ilişkin sağlanan güvenceleri açıklayabilecek,
- Kişisel verilerin hukuka aykırı işlenmesi ile ilişkili suçları tanımlayabilecek,
- Türk Medeni Kanunu ve Türk Borçlar Kanunu'nda yer alan kişisel verilerin korunması ile ilgili düzenlemeleri açıklayabilecek,
- Elektronik ticaret ve elektronik haberleşme sektörlerinde kişisel veriler işlenirken uyulacak temel kuralları açıklayabilecek,
- Kişisel Verilerin Korunması Kanun Tasarısını çeşitli yönleri ile tartışabilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Kişisel Verilerin Korunması
- Avrupa İnsan Hakları Sözleşmesi
- Elektronik Haberleşme
- Elektronik Ticaret
- Hassas Kişisel Veri

İçindekiler



Türkiye’de Kişisel Verilerin Korunması

GİRİŞ

Bir önceki ünite de 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 oluşturmaya neden olmaktadır. Nitekim 21. yüzyılda bireylerin bu konudaki kaygılarının arttığı da görülmektedir.

Örneğin 2011 yılında yayınlanan bir araştırma, Kuzey Amerika’da 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 yönetsel 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 girmeye yeterliliğini taşıyan onlarca partiye 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 kullanıcılar 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 işbirliği 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 değer 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 ünitelerde 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 anlaşılabılır.

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 anlaşılrsa 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 “istatistiki 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 yeniden Anayasa Mahkemesi önüne götürülmüş ve Anayasa Mahkemesi yürütmenin durdurulmasına karar vermiştir (E.: 2013/114, K.: 2014/22, 6/12/2014). Bu ünite 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 bulunmamıştır (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 korunmasının 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 andlaşmalar kanun hükmündedir”. Dolayısıyla Türk hukuk sisteminde uluslararası andlaşmalar iç hukuk sisteminin bir parçasıdır. Bu andlaşmanın 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 andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma 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.

Anayasa’nın 90. maddesi milletlerarası andlaşmaları nasıl düzenlemektedir?



SIRA SİZDE

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 kapsamalarını belirleyebilmek için AİHM’in yorumlarının önemi açıktır. O hâlde hem Anayasa’nın 90. madde hükmünün bir gereği olarak hem de bu konuda geliştirilen içtihatlarla 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 ihlalinin 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. fıkarda 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 amaçla 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.

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 Kanununda (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 ünite de 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 yaptırımı 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 yaptırımı 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 hükmüne 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 “*kışisel veri*”nin tanımı konusunda mevzuatımızda açıklayıcı hükümlerin son derece sınırlı olması ve temel ilkelerin düzenlenmemesi nedeniyle “*hukuka aykırılık*”ın belirlenmesinde yaşanan güçlükler özellikle dikkat çekicidir.

TÜRK MEDENİ KANUNU

Türk hukuk mevzuatında medeni hukukun kişilik haklarına yönelik düzenlemelerinin kişisel verilerin korunmasına açısından bazı olumlu sonuçlar sağlayabileceği söylenebilir. Nitekim kişilik hakları, kişisel değerlerin bütününe kapsayan bir hukuksal alandır. Alman Anayasa Mahkemesi de bir önceki üniteye 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. Mevzuatın 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.

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 artırmaktadır. Bütün bunlar, işçinin kişisel verilerinin korunmasının yakından incelenmesine ve kimi yerlerde özel düzenlemelerin konusu olmasına neden olmuştur. Uluslararası düzenlemelere bakıldığında ise Uluslararası Çalışma Örgütü’nün (International Labour Organization-ILO) konuya ilişkin bir sözleşme kabul etmediği ancak işçinin kişisel verilerinin korunmasına ilişkin uygulama ilkelerini belirlediği görülmektedir.

Yeni Borçlar Kanununda 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.

ELEKTRONİK 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 hükmeye 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 ünite 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 dolayısıyla 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.

ELEKTRONİK TİCARET 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 saklanması 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.

KİŞİSEL VERİLERİN KORUNMASI KANUN TASARISI

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 beklentiye 1981 yılına kadar geriye götürmek olanaklıdır. Nitekim Türkiye, taraf

devletlerin metinde yer alan ilkeleri mevzuatlarına yansıtma 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 teknolojiadaki 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 ile-geç kalınmış da olsa-ihlallerin asgari ve denetlenebilir bir düzeye indirilmesi için yeni bir fırsat doğmuştur. Bu fırsatın değerlendirildiğini söyleyebilmemiz için ise elbette Tasarı, 1. maddede belirlenen “kişisel verilerin işlenmesinde kişinin temel hak ve özgürlüklerini korumak”, amacını gerçekleştirebilecek nitelikte olmalıdır. Bu, Anayasa’nın da bir gereğidir.

Tasarının hükümlerini değerlendirirken Avrupa uygulamasını dikkate almak yararlı olacaktır. Bunun bir nedeni, Avrupada 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 işbirliği gerçekleştirilememesine ve ekonomik kayıplara neden olmaktadır.

Kişisel Verilerin Korunması Kanun Tasarısı dokuz 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. Tasarının “kişisel verilerin işlenmesi” kenar başlıklı ikinci bölümünde ise veri işlemede hakim olan temel ilkelere, kişisel verilerin işleme şartlarına, özel nitelikli(hassas) kişisel verilere, verilerin silinmesi yok edilmesi ve anonim hâle getirilmesi düzenlenmiştir. Bu noktada belirtmek gerekir ki metin olarak düşünülmüştür, ancak pek çok maddesi ile diğer kanunlarda yer alan hükümlerin saklı tutulduğu görülmektedir. Örneğin, Tasarı kapsamında kişilerin “ırkı, kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf ya da sendika üyeliği, sağlığı veya cinsel hayatıyla ilgili veriler” özel nitelikli (hassas) kişisel veri olarak kabul edilmiş ve işlenmesi yasaklanmıştır (m.6/1). Ancak ikinci fıkrada altı bent altında belirlenen istisnalardan biri “yeterli önlemlerin alınması şartıyla (...) kanunlarda

açıkça öngörülmesi” hâlidir. Bu hüküm istisnayı kural, kuralı istisna hâline getirebilecek bir genişliktedir. Nitekim yeterli önlemlerin ne olduğunun tam olarak belirli olmaması bir yana, diğer istisna hükümleri ile birlikte değerlendirildiğinde hassas verilerin işlenmesinde nitelikli bir koruma sağlanmasını önleyebilir.

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(m. 6/2,c). 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.8/4,a,b). Diğer hiçbir özel nitelikli veri için böylesine bir koşul belirlenmemiştir. Nitekim kişinin açık rızasının bulunduğu hâllerde, bunun yeterli görülmeyle bir de Kurulun onayının gerekmesinin nedeni açık değildir. Bu hüküm dolayısıyla bir dernek-İlgililerin açık rızası ile-yönetim kurulunu İnternet sitesinde yayınlamayacak 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.

Tasarının ikinci bölümünde ayrıca kişisel verilerin üçüncü kişilere ve yurt dışında aktarımına ilişkin hükümler yer almaktadır. Bu hükümleri de bir örnek üzerinden değerlendirilebilir. Nitekim Tasarıda yer alan bir diğer istisna hükmü “İlgili 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: “İlgili kişi tarafından alenileştirilen ve böylelikle herkes tarafından bilinen bu tür verilerin işlenmesinde, korunması gereken hukuki yararın ortadan kalktığı kabul edilmektedir”. Öncelikle “alenileştirme” ile neyin kastedildiği belirlenmelidir. Örneğin bir kişinin İnternet sitesinde e-posta adresini yazması, kartvizitinde telefon numarasının bulunması, İnternet’te yayımlanan bir bildiriye imza atması, kamusal alanda gerçekleştirilen bir gösteri yürüyüşüne katılması, bir sokak röportajında siyasal görüşünü söylemesi kendisi tarafından ilgili bilgilerin alenileştirildiği anlamına mı gelir? Bu noktada herkes tarafından bilinen bilgiler açısından korunması gereken hukuki yararın ortadan kalkmadığı belirtilmelidir. Nitekim kişisel verilerin korunmasının bir temel hak alanı olarak kabul edilmesi; veri tabanlarındaki ve kayıt etme, ilişkilendirme, arama yapma, aktarma gibi veri işleme teknolojilerindeki gelişmeler ile yakından ilişkilidir.

Tasarının üçüncü bölümünde veri sorumlusunun aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülükler ile birlikte ilgili kişinin hakları düzenlenmiştir. Bu düzenlemelerdeki temel hedef kişinin kendisi ile dijital ortamlarda her gün artan oranda işlenen verileri arasındaki bağın korunmasıdır. Bu açıdan önemli başka bazı hükümler de dördüncü bölümde yer alır. Nitekim burada özellikle altıncı bölümde oluşum ve işleyiş prensipleri benimsenen Kişisel Verilerin Korunması Kuruluna 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.

Tasarının 18. maddesi ile “görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak” yerine getireceği belirtilen bir Kişisel Verileri Koruma Kurulu oluşturulması öngörülmektedir. Tasarının 20/1 hükmü uyarınca:

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

Belirtmek gerekir ki Kurulun Adalet Bakanlığı ile ilişkili olması(m.18/3), üyelerinin Bakanlar Kurulu tarafından belirlenmesi (m.20/1), kurul üyelerinin görevleri sebebiyle işledikleri iddia edilen suçlara ilişkin soruşturma iznini Adalet Bakanının vermesi (m.20/11) gibi hususlar bağımsızlığın sağlanması noktasında kuşku yaratmaktadır. Kurulun kompozisyonu ve idare teşkilatındaki yeri, ilişkili olduğu Adalet Bakanlığının (UYAP gibi) veri işleyen sistemlerini ya da Sağlık Bakanlığı gibi hassas nitelikteki verileri işleyen diğer Bakanlıkları denetimi açısından sorun yaratabilir. Belirtmek gerekir ki Avrupa mevzuatı uyarınca denetim organı “tam bağımsız” olmalıdır. Avrupa Adalet Divanı da sırasıyla Almanya, Avusturya ve Macaristan uygulamalarının bazı yönleriyle tam bağımsızlık koşulunu karşılamadığına ilişkin kararlarında konunun kritik önemine işaret etmiştir.

Öte yandan tasarının sekizinci bölümünde yer alan istisnalar, yani Kanun yürürlüğe girdikten sonra bütüncül olarak kapsam dışında kalacak alanlar en çok tartışılan hükümleri arasındadır. Bu noktada ilk dikkat çeken istisna istihbarat gibi bazı etkinliklerin kapsam dışında 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 (m.4/2) bu alanda da öncelikle ve mutlaka geçerli olmalıdır. 2014 AB İlerleme Raporunda da MİT’in ve TİB’in yetkilerini genişleten düzenlemelerin kabul edilmesinin “kişisel verilerin korunmasına ilişkin bir mevzuatın ve bağımsız bir denetleme organının olmaması ile birlikte, Türkiye’de kişisel verilerin yeterli düzeyde korunmadığı” yönündeki endişeleri artırdığı belirtilmektedir. Bu noktada, elbette işaret edilen mevzuat bu alanları da kapsar niteliktedir.

Konuyu bütüncül olarak düzenleyen tasarının, başta beşinci bölümde yer alan yaptırım sistemi olmak üzere değerlendirilmesi ve düzenlenmesi gereken başka hükümleri de bulunmaktadır. Bu değerlendirmeler yapılırken 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 ilkedен 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 teknolojiye 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 artırılması 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 teknolojiye 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.

Türkiye’de Anayasal bir hak olan kişisel verilerin korunması hakkının etkin bir biçimde yaşama geçirilebilmesi için Kişisel Verilerin Korunması Kanun tasarısının yeniden gözden geçirilerek bir an önce yürürlüğe girmesi ve kurulacak bağımsız veri koruma otoritesinin belirtilen yeni yaklaşımları da dikkate alarak farkındalık artırıcı çalışmalar yürütmesi son derece önemlidir.

Özet

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 yönetsel 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 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 işbirliği alanlarında çeşitli kayıplar yaşamasına neden olmaktadır.

Ancak bu, konuya ilişkin Türkiye’de hiçbir bir düzenleme olmadığı anlamına gelmez. Başta Türkiye Cumhuriyeti Anayasası olmak üzere iç hukukumuzda kişisel verilerin korunmasını açıkça tanıyan bazı düzenlemeler bulunmaktadır.

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. 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.

Türk Anayasa Mahkemesi bir kararında göre insan onuru kavramını şu şekilde tanımlamıştır: “İnsanın ne durumda, hangi şartlar altında bulunursa bulunsun sırf insan oluşunun kazandırdığı değer 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. 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”.

Bu 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 ilkelere hükümde sayılanlar ile sınırlı değildir. Hüküm metninden bu kolaylıkla anlaşılabılır.

Kişisel verilerin korunmasının 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 andlaşmalar kanun hükmündedir”. Dolayısıyla Türk hukuk sisteminde uluslararası antlaşmalar iç hukuk sisteminin bir parçasıdır. Bu andlaşmanın 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 andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma 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 Anayasanın 90. maddesinde de bulunmaktadır. 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.

Türk 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. 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. 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.

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 onayla-
rı 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.”

Kendimizi Sınavalım

- Aşağıdakilerden hangisi kişisel verilerin işlenmesinin Anayasa ile belirlenmiş meşru temelidir?
 - İlgili kişinin açık rızası
 - Yönetmelikle öngörülmüş olma
 - İlgili kişinin eşinin onay vermesi
 - Veri işleme gereksiniminin ortaya çıkması
 - İdarenin veri işlemenin gerekliliğine karar vermesi
- Aşağıdakilerden hangisi Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi uyarınca özel yaşama müdahale-nin hukuka uygun kabul edilebilmesi için gerçekleşmesi ge-rekli olan koşullardan biri **değildir**?
 - Veri işleme koşullarının yasa ile belirlenmiş olması
 - Veri işlemenin 8. maddenin 2. fıkrasında belirlenen nedenlerden birine yönelik olması
 - Müdahalenin demokratik bir toplumda gerekli olması
 - Müdahalenin orantılı olması
 - Müdahalenin idarenin bir kararına dayanması
- Türk Ceza Kanunu'nda göre aşağıdaki eylemlerden han-gisi suç olarak **düzenlenmemiştir**?
 - Kişisel verilerin hukuka aykırı olarak kayıt edilmesi
 - Kişisel verilerin hukuka aykırı olarak yok edilmesi
 - Kişisel verilerin hukuka aykırı olarak yayılması
 - Kişisel verilerin hukuka aykırı olarak ele geçirilmesi
 - Kişisel verilerin kanunda belirlenen süre geçmiş ol-masına karşın sistem içerisinde yok edilmemesi
- İşçinin kişisel verilerinin korunması ile ilgili aşağıdaki ifadelerden hangisi doğrudur?
 - İşveren işçinin kişisel verilerini dilediği gibi işleyebilir.
 - İşveren işçiye ilişkin olarak iş yerinde topladığı veri-leri dilediği gibi aktarabilir.
 - İşveren işçinin kişisel verilerini hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir.
 - İşveren işçinin kişisel verilerini hiç bir durumda işle-yemez.
 - İşveren işçinin verilerini gerekçe göstermek kaydıyla her durumda işleyebilir.
- Aşağıdaki yasa metinlerden hangilerinde kişisel verilerin korunmasına yönelik düzenlemelere yer **verilmemiştir**?
 - Türk Ceza Kanunu
 - Türk Borçlar Kanunu
 - Elektronik Ticaret Kanunu
 - Elektronik Haberleşme Kanunu
 - Karayolları Trafik Kanunu
- Türk Ceza Kanunu'nda kişisel verilerin korunmasına yönelik hükümlerde aşağıdaki yaptırımlardan hangisi öngörülmüştür?
 - Uyarma
 - İdari para cezası
 - Para cezası
 - Hapis cezası
 - Meslekten men etme
- Kişisel verilerle ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?
 - Türkiye'de çerçeve nitelikte kapsayıcı bir Kişisel Veri-lerin Korunması Kanunu yürürlüktedir.
 - Türkiye, kişisel verilerin korunmasına ilişkin 108 sa-yılı Avrupa Konseyi Sözleşmesini imzalamış ancak onaylanmamıştır.
 - Türkiye Cumhuriyeti Anayasası uyarınca Avrupa İn-san Hakları Sözleşmesi yasa hükmündedir.
 - Türk Medeni Kanunu'nun kişilik haklarının korunma-sına ilişkin 24 ve 25. madde hükümleri bazı konularda kişisel verilerin korunmasını destekleyici niteliktedir.
 - Elektronik Ticaret Kanunu uyarınca hizmet sağlayıcı elektronik ticaret işlemleri dolayısıyla elde ettiği kişi-sel verilerin güvenliğinden sorumludur.
- Aşağıdakilerden hangisi kişisel verilerin etkin korunma-sını destekleyici unsurlardan biri **değildir**?
 - Çerçeve nitelikte bir yasal düzenleme
 - Veri korumayı destekleyici teknik önlemlerin alınması
 - Veri korumaya yönelik bireysel önlemlerin alınması
 - Veri koruma alanında farkındalık artırıcı çalışmala-rın yapılması
 - Kişisel verilerin sınırsız şekilde işlenmesini sağlayıcı hukuksal düzenlemelerin yapılması
- Kişisel Verilerin Korunması Kanun Tasarısı uyarınca Ki-şisel Verileri Koruma Kurulu üyeleri nasıl belirlenir?
 - Bakanlar Kurulunca seçilir.
 - TBMM tarafından seçilir.
 - Yüksek Öğretim Kurulu (YÖK) seçer.
 - Türkiye Barolar Birliği tarafından seçilir.
 - Halk seçer.
- Aşağıdakilerden hangisi Türkiye'de kişisel verilerin ko-runması alanında yaşanan sorunlardan biri **değildir**?
 - Kişisel verilerin güvenliğine ilişkin eksiklikler
 - Çerçeve niteliğinde bir yasal düzenlemenin bulunmaması
 - Konuya ilişkin bazı düzenlemelerde yaptırım siste-mindeki eksiklikler
 - Kolay ulaşılabilir bazı anahtar bilgiler aracılığıyla başka bilgilere erişilebilmesi
 - Kişisel verilerin hukuka aykırı ele geçirilmesine karşı herhangi bir yaptırımın öngörülmemesi

Yaşamın İçinden



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.

Karearda, "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" süreç 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

Okuma Parçası

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 güvenceler 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".



Kendimizi Sınavalım Yanıt Anahtarı

- | | |
|-------|---|
| 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”, “Türk Ceza Kanunu” ve “Türk Borçlar Kanunu” konularını yeniden gözden geçiriniz. |
| 6. d | Yanıtınız yanlış ise “Türk Ceza Kanunu” konusunu yeniden gözden geçiriniz. |
| 7. a | Yanıtınız yanlış ise “Kişisel Verilerin Korunması Kanun Tasarısı” konusunu yeniden gözden geçiriniz. |
| 8. e | Yanıtınız yanlış ise “Kişisel Verilerin Korunması Kanun Tasarısı” konusunu yeniden gözden geçiriniz. |
| 9. a | Yanıtınız yanlış ise “Kişisel Verilerin Korunması Kanun Tasarısı” konusunu yeniden gözden geçiriniz. |
| 10. e | Yanıtınız yanlış ise “Kişisel Verilerin Korunması Kanun Tasarısı” konusunu yeniden gözden geçiriniz. |

Yararlanılan Kaynaklar

- 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.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Anayasaya göre “Usulüne göre yürürlüğe konulmuş Milletlerarası andlaşmalar kanun hükmündedir”. Dolayısıyla Türk hukuk sisteminde uluslararası andlaşmalar iç hukuk sisteminin bir parçasıdır. Bir andlaşmanın 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 andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınır”.

4

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Bilişim suçlarına ilişkin Türkiye’de yaşanan süreci ve temel kavramları açıklayabilecek,
- Bilişim sistemine girme suçunu analiz edebilecek,
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun unsurlarını açıklayabilecek,
- Kredi kartlarının kötüye kullanılması suçunu analiz edebilecek,
- Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbirinin uygulanma koşullarını belirleyebilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- 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 El Koyma

İçindekiler



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

GİRİŞ

Bilişim alanında son çeyrek asırda yaşanan devrim niteliğindeki gelişmelerle birlikte, insanlık bundan yüzyıl önce yaşayan insanların hayal bile edemeyeceği bir yaşam standardına 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 hâle getirilmiştir ki, onların girmedeği, götürülemediği veya kullanılmadığı yaşam alanı yok denecek kadar azalmıştır.

Bilişim alanındaki gelişmelerin hukuk alanında da önemli birtakım sorunlara neden olduğu aşikârdır. 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 birtakım 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 Avrupası ceza hukuku sistemlerinde biçimsel kanunilik ilkesi kabul edilmiştir. Dolayısıyla ceza hukukunda kıyasa başvurulması suretiyle suç sayılmayan birtakım antisosyal 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 İnternete ilişkin oldukça kapsamlı bilgilere de sahip olması gerekmektedir.

Bu ünite de dar anlamda bilişim suçlarının CMK m.135'teki koruma tedbirinin incelenmesi uygun görülmüştür. Bu bağlamda öncelikle TCK'nin 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 geldiğinde 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 hâller ünite kapsamında değerlendirilmeyecektir. Aynı şekilde Fikir ve Sanat Eserleri Kanunu ile Elektronik İmza Kanunu'nda yer alan bilişim suçları da ünite içerisinde değerlendirilmeyecektir. Buna karşın CMK m.135'te düzenlenen bilgisayarlar, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma koruma tedbiri de ünite içerisinde incelenecek konulardandır.

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'ye 1991 yılında girmiş ve 3756 sayılı kanun'la 765 sayılı TCK'nın ikinci kitabına bazı bilişim suçlarını öngören "Bilişim Alanında Suçlar" başlıklı 11. Bap ilave edilmiştir.

3756 sayılı kanun'dan 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'nin 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'de 1991 yılında yapılan söz konusu düzenlemeyi takiben 1995 yılında ise 4110 sayılı kanun'la Fikir ve Sanat Eserleri Kanunu'nda bilgisayar programlarının da eser sayılacağına ilişkin bir değişiklik yapılmış; bilgisayar programlarına karşı gerçekleştirilen birtakım eylemler de yaptırım altına alınmıştır.

Daha sonra ise iletim ağlarının ticarete 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'de ise bilişim alanında işlenen suçlara, önceki 765 sayılı kanundan daha ayrıntılı düzenlemeler yapılarak yer verilmiştir. Kanunda söz konusu suçlara, özel hükümlerin yer aldığı TCK'nin 2. kitabının topluma karşı suçların düzenlendiği 3. kısmının 10. bölümünde "Bilişim Alanında Suçlar" başlığı altında yer verilmiştir. Görüldüğü üzere 765 sayılı TCK'nin söz konusu suçlara ilişkin olarak 11. babında kullanılan başlık ile 5237 sayılı yeni TCK'nin 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'de hırsızlık, dolandırıcılık gibi bazı suçların bilişim sistemleri vasıtasıyla işlenmesi hâli de söz konusu suçların nitelikli hâli olarak ayrıca hükme bağlanmıştır. Ayrıca Fikir ve Sanat Eserleri Kanunu ile Elektronik İmza Kanunu'nda düzenlenen bilişim suçları da bulunmaktadır.

Son olarak ise İnternet vasıtasıyla işlenen suçlarla mücadelenin etkiliğini 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 İnternet 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 birtakım cezai fiiller söz konusu kanunda kabul edilmiştir.

BİLİŞİM SUÇLARINA İLİŞKİN TEMEL KAVRAMLAR

Genel Olarak

Gerek 765 sayılı önceki TCK'de gerekse 5237 sayılı yeni TCK'de 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 düzenlemenin anlamını orta koyma bakımından zorunluluk teşkil etmektedir. Bu nedenle aşağıda gerek inceleyeceğimiz suç tipine ilişkin kanuni düzenlemede geçen gerekse anlatılarımız sırasında bizim sıklıkla kullanacağımız birtakım terimlerin içeriklerini belirlemeyi uygun buluyoruz.

BİLİŞİM SİSTEMİ

Genel Olarak

765 sayılı eski TCK'de 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'de 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'nin "bilgileri otomatik olarak işleme tabi tutmuş sistem" ibaresi yerine 5237 sayılı TCK'de aynı anlamı taşımak üzere tercih edilen "*bilişim sistemi*" tabirinden bir veya birden fazla ünitelerden oluşan ve belirli bir sonuca ulaşmak için işbirliği sistemiyile 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 sayılmaz.

Şifreli Yayınların Konumu

Yayıcılık 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'nin 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 sahiptir.

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'nin 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 reddetmekteydi. Buna karşın ceza hukukumuzda bu konuda bir ihtiyaç olduğu açıktı. Bu sebeple kanunkoyucu yeni TCK'de 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 hâlde belirli bir formata dönüştürülmüş hâlidir.

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.

İnternet

Her ne kadar kanunda yer alan suça ilişkin düzenlemede geçen kavramlardan biri olmasa da bilişim sistemleri arasında bağlantı sağlanmasında ve bu tür sistemlere erişimde önemli bir araç olan İnternet 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 İnternete “ağlar arası ağ” da denilmektedir. İnternet sanıldığıının aksine veri iletim ağlarının yalnızca bir türü, dolayısıyla sanal alanın yalnızca bir parçasıdır. Ancak dünya üzerinde bugün kullanılan en yaygın ve en geniş ağıdır. Sanal alan ise bilişim sistemleri ile bunları birbirine bağlayan her türlü veri işletim ağından oluşan, fiziksel yapısı sayısal verilerden ibaret bir alandır.

İnternet nedir?



SIRA SİZDE

BİLİŞİM SİSTEMİNE GİRME SUÇU

Genel Açıklamalar

765 sayılı TCK’de 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.

5237 sayılı TCK’de *izinsiz bilişim sistemine girme* suçunun düzenlemesiyle birlikte, hukuk sistemimizde, Avrupa Siber Suç Sözleşmesi’nin 2. maddesinde öngörülen *hukuka aykırı erişim* düzenlemesiyle de paralellik sağlanmıştır.

Bilişim sistemine girme suçunun düzenlendiği ve 5237 sayılı TCK’nin 243. maddesinin metni şu şekildedir:

Madde 243 - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, 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.

Görüldüğü üzere madde üç fıkradan oluşmaktadır. Birinci fıkra suçun temel şekli düzenlenirken; ikinci ve üçüncü fıkralarda nitelikli hâllerine yer verilmiştir. Bu hâllerden ilkinin gerçekleşmesi hâlinde faile suçun temel şekline nazaran daha az, ikincisinin gerçekleşmesi hâlinde ise daha fazla ceza verilmesi öngörülmüştür.

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.

Aşağıda suça ilişkin inceleme gerçekleştirilirken suçun unsurları maddi unsur, manevi unsur ve hukuka aykırılık unsuru olmak üzere üç tür üzerinden incelenmiştir. Bu inceleme şekli, konunun daha rahat anlaşılabilmesi amacıyla yönelik pragmatik gerekçelere dayanmaktadır.

Suçla Korunan Hukuki Değer

Suçun hukuki konusu; 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 mal varlığına ilişkin hem de kamunun itimatına ve özel hayatın korunmasına ilişkin yararlar koruma altına alınmaktadır.

Bilişim sistemine izinsiz girme suçu kapsamında ise 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 suç ile korunan hukuki menfaat dijital alandaki özel alan olarak ifade edilebilir 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.

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 maddi konusu, bir bilişim sistemi veya ona ait parçalardan herhangi birisidir. Nitekim suç tipiyle yasaklanan davranışlar bir bilişim sistemi veya onun parçaları üzerinde gerçekleştirilmelidir ki suç oluşabilsin.

Fail: Suçun faili tipik eylemleri gerçekleştiren kişidir. Söz konusu suç bakımından fail olmanın gerektirdiği herhangi bir özellik söz konusu değildir. Herkes suçun faili olabilir. Bu bağlamda suçun özgü suç olma niteliği vs. bulunmamaktadır.

Mağdur: Suçla korunan hukuki değer ait olduğu kimse mağdur olarak nitelendirir. Girilen bilişim sistemini kullanan kimse bu suçun mağdurdur. Suçun mağduru olabilmek bakımından aranan herhangi bir özellik bulunmamaktadır.

Fiil: Kanunda tanımlanan maddi fiil, bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek ve orada kalmaya devam etmektir. Sisteme hukuka aykırı olarak girip orada 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 birtakım sonuçların gerçekleşmesi gerekmez.

Bununla birlikte, davranışın devamlılığı bakımından da suç kesintisiz (mütemadi) bir suçtur. Yani davranış gerçekleştirildiğinde suç oluşur ancak hemen sone 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 orada bir süre kalmayı da gerekli görmüştür. Suçun oluşması bakımından failin ne kadar sistemde kalmasının gerektiği somut olayın özelliklerine göre belirlenmelidir. Bu bağlamda sisteme girip suçla korunan hukuki menfaatlere zarar vermeksizin derhâl çıkan kimsenin fiili bakımından maddi unsurun gerçekleşmediğinin kabulü gerekir.

Kanunkoyucunun sadece sistemi girmeyi değil; bununla birlikte orada kalmayı da suçun gerçekleşmesi bakımından zorunlu kabul etmesi, bireylerin dijital ortamdaki özel alanını ihlale yönelik bir amaç olmaksızın, salt deneme veya başarıyı testetme amaçlı olarak sisteme kısa süreli girişleri cezalandırmama düşüncesine dayanmaktadır.

Bir görüşe göre, deneme veya başarıyı testetme amaçlı olarak bilişim sistemine yapılacak kısa süreli girişler tamamlanmış suçtan olmasa da teşebbüsten cezalandırılacaktır. Ancak



bu görüşü paylaşmadığımızı ifade etmek isteriz. Nitekim teşebbüs hâlinde kalmış suçla, tamamlanmış suç arasında manevi unsur bakımından hiçbir fark yoktur. Her iki durumda da fail suç teşkil eden davranışı gerçekleştirme niyetindedir. Bu bağlamda dijital ortamdaki özel alana müdahale etme amacı olmayan ve sistemde çok kısa süreli kalan kimseyi, sanki amacı sistemde kalmakmış da başaramamış gibi cezalandırmak mümkün değildir.

Suçun maddi unsurunun gerçekleşmesi bakımından sisteme doğrudan doğruya girilebileceği gibi, örneğin İnternet 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, İnternet 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 birine 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 hâllere 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 hâlinde failin temel tip için kabul edilen ceza ile cezalandırılmasını uygun görmemiştir. Örnek vermek gerekirse İnternet 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 hâlden 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 hâlin varlığı için, verilerin yok olması veya değişmesi failin kastı kapsamında olmamalıdır. Aksi takdirde, yani bu hâllerin kasten gerçekleştirilmesi hâlinde, ayrıca TCK m.244/2'de düzenlenen suç vücut bulacaktır. Burada düzenlenen nitelikli hâl, netice sebebiyle ağırlaştırılmış bir suç tipi olarak karşımıza çıkmaktadır. Dolayısıyla netice sebebiyle ağırlaştırılmış 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 hâlden sorumlu olacaktır.

Tipik Manevi Unsur

Suçun manevi unsuru kasttır. Suçu oluşturan fiillerin hangi amaçla gerçekleştirildiğinin bir önemi yoktur. Bu bağlamda suçun gerçekleşmesi bakımından özel kast aranmaz. Do-

layısıyla zarar verme veya menfaat sağlama gibi bir amacı olmaksızın, sadece bakmak için hukuka aykırı olarak bir bilişim sistemine giren ve orada kalan kimse bu madde gereğince sorumlu olacaktır.

Suçun taksirli hâli kanunda düzenlenmemiştir. Bu itibarla İnternette gezinirken dikkatsiz davranıp, kastı olmaksızın gerçekleştirdiği bazı davranışlarla bir bilişim sistemine giren kimseler bakımından cezai sorumluluk doğmayacaktır.

Kusurluluğu kaldıran hâllerden herhangi birisinin bulunmasına bağlı olarak failin kınanabilirliği ve bu bağlamda kusuru söz konusu olamayacağından suç oluşmayacaktır. Bu bağlamda örneğin cebir veya tehdit altında, İnternet vasıtasıyla, girilmesi yasak bir sisteme giriş yapan bilişim sistemi uzmanı kimse bakımından kusurun varlığından ve dolayısıyla cezai sorumluluktan söz edilemeyecektir.

Hukuka Aykırılık

Ceza normu ile yasaklanmış tipik davranışların gerçekleştirilmesi hukuka aykırılığın karinesini oluşturur. Ancak bazı hâllerde hukuk düzeni, tipiklikte formüle edilmiş olan yasağı hukuka uygunluk nedenleri denilen müsaade edici durumların mevcudiyeti hâlinde kaldırır. Böylece herhangi bir fiilin hukuka aykırı olduğu konusundaki kesin hüküm, ancak herhangi bir hukuka uygunluk nedeninin somut olayda bulunmaması hâlinde verilebilir.

Bilişim sistemine girme suçu bakımından hukuka uygunluk nedenlerine ilişkin özellikler arzeden bir durum söz konusu değildir. Bu bağlamda genel ilkeler bu suç tipi 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 İnternet üzerinden erişilebilen İnternet sayfalarına ilişkindir. Nitekim bazı İnternet sayfalarında kişilere ait birtakım bilgiler bulunmakta ya da bireylere birtakım hizmetler sunulmaktadır. Herhangi bir şifreli koruma olmaksızın bu tür sayfalara erişim sağlanması hâlinde 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 İnternet ortamına koymakla, aleniyetini sağlamış ve kamunun bilgisine/hizmetine sunmuş olmaktadır. Bu nedenle bu tür erişimler söz konusu suçu oluşturmaz.

Buna karşın sadece belirli kimselerin içeriğini görmesini sağlamaya yönelik olarak bir İnternet sayfası oluşturulur ve bu sayfaya fail tarafından şifre kırılmak suretiyle erişim sağlarsa; bu suçun oluştuğunun kabulü gerekir. Nitekim söz konusu İnternet 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 hâllere ilişkin söz konusu suç bakımından özellikler arzeden bir durum söz konusu değildir. Bu bağlamda zorunluluk hâli 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

Teşebbüs

Teşebbüs kişinin işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamamasıdır. Bu bağlamda bilişim sistemine girme suçu teşebbüse müsait bir suçtur. Sisteme girmeye çalışmak veya girdikten sonra orada kalmayı başaramamak teşebbüs hâlidir. Ancak bu hâlde teşebbüsten cezai sorumluluğun söz konusu olabilmesi bakımından da genel ilkeler geçerlidir. Dolayısıyla mutlak elverişsiz davranışlarla veya mutlak elverişsiz vasıtalarla sisteme girilmeye çalışılması, işlenemez suçun vücudunu oluşturacak; bu da cezai sorumluluk doğurmayacaktır. Ancak davranışların ve kullanılan vasıtaların nisbi elverişsizliğinden kaynaklanan nedenlerle suçun işlenememesi hâlinde failin teşebbüsten cezalandırılması gereklidir.

Bir örnekle konuyu somutlaştırmak gerekirse İnternet 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 hâlde, İnternet adresinin giriş sayfasında yer alan şifre kutusuna rastgele birtakım rakamlar yazar ancak sisteme giriş konusunda başarılı olamaz. Bu durumda failin sisteme girme suçuna teşebbüsten sorumluluğu söz konusu olmaz kanaatindeyiz. Çünkü rastgele rakamlarla son derece güvenli kodlanmış bir sisteme girmek son derece düşük bir olasılıktır. Her ne kadar sisteme girişin olasılık dâhilinde 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 işbirliği içerisinde işlenmesine iştirak denir. İştirake ilişkin genel kurallar suç bakımından özel bir önem arz etmeksizin 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 isteyen, ancak kendisinin bilişim sistemleri hakkında yeterli bilgisi olmadığından, bu konuda uzman bir arkadaşını, bu sisteme girme konusunda ikna eden ve bu fiilin gerçekleşmesini sağlayan kimse bakımından azmettiren olarak cezai sorumluluk doğacaktır. Bu karşın sisteme giren kimse ise fail olarak suçu gerçekleştirmiş sayılacaktır.

Yukarıda manevi unsur başlığı altında verdiğimiz örnek üzerinden devam edersek cebir veya tehdit kullanarak bilişim sistemleri konusunda uzman birinin, İnternet vasıtasıyla girilmesi yasak bir sisteme giriş yapmasının sağlanması hâlinde, cebir veya tehdit altında onu 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 ve 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 hâlinde 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'te 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 hâlinde ne şekilde hareket edileceği konusunda tereddüt doğabilir. Örneğin bilişim sistemini kullanmak vasıtasıyla gerçekleştirilecek dolandırıcılığın söz konusu olduğu hâllerde, 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

Suçun temel şeklinin gerçekleştirilmesi hâlinde faile seçenekli bir yaptırım öngörülmüştür. Bu bağlamda fail bir yıla kadar hapis cezasıyla veya adli para cezası ile cezalandırılabilir. Kanunun açık hükmü gereği hakim her iki cezaya da aynı anda hükmetmesi mümkün değildir.

Suçun ikinci fıkrada düzenlenen daha az cezayı gerektiren nitelikli hâlinin 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 hâlin söz konusu olması durumunda yarı oranına kadar indirilecektir.

Suçun üçüncü fıkrasında daha fazla cezayı gerektiren nitelikli hâl 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 hâlinde uygulama alanı bulmayacaktır.

TCK'ye 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, bu suç bağlamında tüzel kişiler hakkında güvenlik tedbirinin uygulanabileceği sonucuna ulaşılmaktadır.

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU

Genel Açıklamalar

TCK'nin 244. maddesinde bilişim alanındaki bir diğer suç tipi olarak *sistemi engelleme, bozma, verileri yok etme veya değiştirme* düzenlenmiştir. Maddenin birinci ve ikinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızzar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkra seçimsel hareketli bir suç meydana getirilmiştir.

Üçüncü fıkra, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde, verilecek cezanın artırılması öngörülmüştür. Dördüncü fıkra ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımına altına alınmıştır.

Suçla 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 hâlinde, 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 hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

Suçla Korunan Hukuki Değer

Suçla korunan hukuki değer bireyin gerek mal varlığı gerekse de bilişim sisteminin güvenliğidir. Nitekim söz konusu suç tipiyle hem bilişim sisteminin işleyişinde meydana gelebilecek zararlar hem de bilişim sistemindeki verilerin bozulması, değiştirilmesi, başka yere gönderilmesi gibi eylemler cezai yaptırıma tabi tutulmuştur. Doktrinde söz konusu düzenlemenin, bilişim sistemlerine özgü özel bir mala zarar verme suçunu hükme bağladığı da 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: Suçun faili bakımından kanunda herhangi bir özellik aranmamıştır. Bu bağlamda suç 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 suçun 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 kulla-

nımındaki bir bilgisayara virüs yüklenerek tüm verilerin kaybına neden olduğunda, kardeşlerin her ikisi de mağdur olacaktır.

Suçun Konusu: Suçun konusu bilişim sistemi veya sistemdeki verilerdir. Nitekim birinci fıkradaki fiiller bilişim sistemi üzerinde işlenirken ikinci fıkradaki fiillerin bilişim sisteminde yer alan veriler üzerinde işlenmesi aranmıştır. Bu nedenle duruma göre suçun maddi konusu bazen bilişim sisteminin kendisiyken bazen de sistemde yer alan veriler olabilecektir.

Fiil: TCK m.244'ün birinci fıkrasında sistemin işleyişini engelleme ve bozma, ikinci fıkra verileri bozma, yok etme, değiştirme veya verileri başka yere gönderme, dördüncü fıkra ise bilişim sistemini aracı kılarak yarar sağlamak fiilleri düzenleme altına alınmıştır. Doktrinde ağırlıklı olarak bunlardan her birinin ayrı bir suç olduğu yönünde görüşler bulunmaktadır (Katılmadığımız görüş için bkz. Yaşar-Gökcan-Artuç, 2014:7309). Ancak kanaatimizce bunlar ayrı suçları değil, bilakis aynı suçun temel şeklini ve nitelikli hâllerini oluşturmaktadır.

Birinci fıkradaki düzenleme bakımından bilişim sisteminin işleyişinin engellenmesi ve bozulması hükme bağlanmıştır. 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 işleminin 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 gerçekleştiremiyordu.

İkinci fıkradaki düzenlemeyi birinci fıkradan ayıran en önemli farklılıklardan biri, 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 virüs bulaştırılması ve çalışmaz hâle 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 tümünden 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-Artuç, 2014:7311 vd.).

Düzenlemenin üçüncü fıkrasında yukarıda bahsedilen fiillerin, *bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi cezaı arttıran bir neden olarak kabul edilmiştir*. Böyle bir arttırmaya yer verilmesinin temel nedeni, gerçekleştirilecek eylemler nedeniyle bu kurum ve kuruluşların hizmetlerinin aksamamasının, 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'nin 158/1/j maddesinin gerekçesinde, banka olmamasına karşın kanunen borç vermeye yetkili kurumlar olarak ifade edilmiştir. Bağlayıcı olmakla birlikte söz konusu kavramın içeriğini tespitte gerekçe metninin de yol gösterici olduğu kanaatiniz taşımaktayız.

Suçla ilişkin düzenlemenin dördüncü fıkrasında ise yukarıda açıkladığımız *fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde*, 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 olma zorunluluğudur. Bununla birlikte fail, gerçekleştirdiği bu eylemlere bağlı olarak kendisi veya başkası yararına haksız bir çıkar sağlamış olmalıdır. Çıkarın mutlaka maddi olmasına gerek yoktur. Örneğin kişi sisteme girerek 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 İnternet bankacılığı şifresini kırarak hesaptaki parayı başka hesaba aktarma eyleminin m.244/4'teki suçu değil; bilakis 142/2/e kapsamında bilişim yoluyla hırsızlık oluşturduğunu kabul etmiştir ((Yaşar-Gökcan-Artuç, 2014:7315 vd.).

Tipik Manevi Unsur

Söz konusu suç kasten işlenebilen bir suçtur. Kanunda taksirli şekline açıkça yer verilmediği için, suçun 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 suç olası kastla da işlenebilir. Örneğin sisteme girince muhtemelen bazı verilerin bozulacağını öngören fail, bu riski kabullenerek sadece kendini arkadaşlarına ispatlamak amacıyla sisteme giriş yapar ve bu şekilde bazı verilerin kaybolmasına neden olursa, bu suça ilişkin olası kast sorumluluğu doğacaktır.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun tipik manevi unsuru nedir?



SIRA SİZDE

Hukuka Aykırılık

TCK m.244'te tanımlanan suç bakımından hakkın icrası, ilgilinin rızası ve görevin ifası hukuka uygunluk sebeplerin ortaya çıkaması 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 el koyma işlemlerini gerçekleştiren kolluk görevlisi bakımından görevin ifasına dayalı hukuka uygunluk nedeni oluşacaktır. Son olarak bir bilişim sisteminden faydalanmak konusunda ödeme yapıp sistemdeki verileri kullanma ve nakletme hakkı kazanan kişi de, bu eylemleri gerçekleştirdiğinde hakkın icrası kapsamında hukuka uygun bir eylem gerçekleştirmiş olacaktır.

Kusurluluk

Kusurluluk ve kusurluluğu ortadan kaldıran hâllere ilişkin söz konusu suç bakımından özellik arz eden bir durum söz konusu değildir. Bu bağlamda zorunluluk hâli veya karşı konulamayacak bir cebir veya ağır bir tehdit altında buradaki fiilleri gerçekleştirenler bakımından kınanabilirlik söz konusu olmayacağından cezai sorumluluk doğmayacaktır.

Suçun Özel Belirli Biçimleri

Teşebbüs

TCK m.244'te düzenlenen suça teşebbüs mümkündür. Bu bağlamda örneğin bilişim sistemine girip verileri bozmaya yönelik icra hareketlerine başladıktan sonra, verileri bozmayı başaramadan yakalan kimse, ikinci fıkra kapsamında bu suça teşebbüsten sorumlu olacaktır.

İştirak

İştirake ilişkin olarak bu suç bakımından özellik arzeden bir durum söz konusu değildir. Herkes tarafından işlenebilen suçta, özel bir faillik niteliği de aranmamaktadır. Bu bağlamda bir bilişim sistemini bozmak konusunda fiil üzerinde ortak hakimiyet kurmak suretiyle suçu birlikte işleyenler müşterek fail olarak sorumlu olacaklardır. Bunun yanında yardım etme ve azmettirme şeklinde suçun işlenişine şerik olarak katılmak da mümkündür.

İçtima

Eğer TCK m.244'ün birinci ve ikinci fıkralarındaki düzenlemeler ayrı suç tipi olarak kabul edilirse bu durumda fail sisteme girip verileri başka yere nakledip sonra da sistemi bozarsa birinci fıkraya ve ikinci fıkraya göre ayrı ayrı iki suç işlemekten cezalandırılacaktır. Ancak biz kanaatimizin bu düzenlemelerin ayrı ayrı suçları değil, suçun temel şeklini ve nitelikli hâllerini düzenlediği yönünde olduğunu fiile ilişkin açıklamalarımızda ifade etmiştik. Bu nedenle sistemden verileri nakledip sonra sonra sistemi bozan kişi sadece en ağır cezayı gerektiren suçtan sorumlu tutulmalıdır.

Ayrıca belirtmek gerekir ki birinci ve ikinci fıkra kapsamına giren eylemleri gerçekleştiren kişi bundan menfaat sağlamışsa sadece dördüncü fıkra kapsamında sorumluluk doğacaktır. Ancak menfaati elde edemeden yakalanmışsa bir başka deyişle suçu dördüncü fıkra kapsamında gerçekleştirmeye yönelik davranışları teşebbüs aşamasında kalmışsa, birinci ve ikinci fıkra kapsamındaki işlenmiş suçla, dördüncü fıkra kapsamındaki teşebbüs aşamasında kalmış suç arasında fikri içtima hükümleri uygulanmalı ve fail çıkacak sonuca göre cezalandırılmalıdır.

Bununla birlikte dördüncü fıkra kapsamında hileli davranışlarla kişilerin İnternet hesaplarından başka hesaba para aktaran kimse de bilişim yoluyla dolandırıcılıktan (TCK m.158) sorumlu olacaktır. buna karşın TCK m.244/4'e göre göre ayrı sorumluluğu söz konusu olmaz. Nitekim düzenlemede fiilin ayrıca başka bir suç oluşturmaması aranmıştır. Bu durumda fiil dolandırıcılık suçunu oluşturduğundan, TCK m.244/4'ten sorumluluk doğmayacaktır.

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 uygun görülmüştür. Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hâlinde ise verilecek cezanın yarı oranında arttırılması hükme bağlanmıştır. Son olarak suçun dördüncü fıkra kapsamında gerçekleştirilmesi hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacağı düzenlenmiştir. bu son fıkraya giren hâlde kanunkoyucu fail bakımından hem hapis hem de adli para cezası uygulanmasını tercih etmiştir.

Bununla birlikte söz konusu suçun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler varsa, bunlar hakkında da tüzel kişilere özgü güvenlik tedbirlerine hükmolunur (TCK m.246; m.60).

BANKA VE KREDİ KARTLARININ KÖTÜYE KULLANILMASI SUÇU

Genel Olarak

Gerek banka kartları gerekse kredi kartları son dönemde gündelik hayatta giderek daha fazla yer tutmaya başlamıştır. Birçok insan artık yanında para taşımamakta, doğrudan veya İnternet üzerinden yaptığı alışverişlerde 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 alışverişlerde kullanımı, harcama ve satışların kayıt altında tutulmasını kolaylaştırmaktadır. Böylelikle söz konusu kartlarının kullanımı vergilendirmeyi etkili kıldığı için, bu şekilde alışveriş 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 kullanılması suçunu 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 kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli 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 adli 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 edilen veya evlâtlığın,

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

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

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.

K İ T A P



Banka ve Kredi Kartlarını kötüye kullanılması suçuna ilişkin ayrıntılı bir inceleme için bkz. Baş, E. (2015) Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, Ankara

Suçla Korunan Hukuki Değer

Söz konusu suç 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 suçla korunan hukuki değer karma bir niteliktedir. Hırsızlık, dolandırıcılık, güveni kötüye kullanma, sahtecilik suçlarının tamamının düzenleniş amaçlarını bir yönüyle içeren bu suç tipi, uygulamada ortaya çıkabilecek içtihat farklılıklarını ve duraksamaları önlemek amacıyla ayrıca hüküm altına alınmıştır.

Tipik Maddi Unsur

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

Mağdur: Bu suçun mağduru kural olarak herkes olabilir. Kural olarak mağdur bakımından özellik arzeden bir durum bulunmamaktadır. Ancak yargıtay'a göre ikinci fıkra-daki suçun mağduru "kartın henüz kullanılmamış olması nedeniyle" hesap sahibi değil, bilakis bankadır. Kanaatimizce bu durumda hesap sahibinin de bankayla birlikte mağdur olduğunun kabulü gereklidir.

Suçun Konusu: Suçun konusunu banka ve kredi kartları oluşturmaktadır. Nitekim suç teşkil eden eylemler bunlar üzerinde gerçekleştirilmektedir. Banka ve kredi kartlarının hukuki tanımına ilişkin olarak 5464 sayılı Banka ve Kredi Kartları Kanunu'ndaki düzenlemelere bakmak gereklidir.

Fiil: Hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının kanuni düzenlemeye bağlanmasını gerekli kılan nedenler bu suçun kanuni düzenlemeye bağlanması bakımından da geçerlidir. Kanunkoyucu bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmelerini uygun görmüştür.

TCK'nın 245. maddesinin birinci, ikinci ve üçüncü fıkralarının ayrı ayrı suçları düzenlediği şeklindeki doktrindeki yaygın görüşe katılmamaktayız (Katılmadığımız görüş için bkz. Özen ve Baştürk, 2011:114). Nitekim kanunkoyucunun bu yönde bir iradesi olsa tek bir suç adı altında bu tür düzenlemeler yapmazdı ya da bunların ayrı ayrı suçları oluşturduğuna ilişkin ayrı bir ifadeye düzenleme içerisinde yer verirdi. Bu bağlamda söz konusu fıkraların suçun temel şekli ve nitelikli hâllerini düzenleme altına aldığı düşüncesinde olduğumuzu ifade etmek isteriz (Benzer şekilde bkz. Baş, 2015 :140 vd.). Ancak Yargıtay'ın uygulamada bu düzenlemelerin her birini ayrı ayrı suçlar olarak kabul ettiğini de ifade etmek gerekir.



Birinci fıkra kapsamında suçun oluşması için öncelikle sahte olmayan, gerçek bir kredi kartının bulunması gereklidir. Eğer kart sahte ise bu durumda ancak ikinci ve üçüncü fıkra kapsamında suç oluşabilecektir. Başkasına ait 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 kredi kartını kötüye kullanmaktan hem de hırsızlık ayrı ayrı cezai sorumluluğa sahip olacaktır. Bununla birlikte failin kartı sadece ele geçirmiş olması, banka ve kredi kartlarını kötüye kullanma veya bu suça teşebbüsü de 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 Kanunu 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 hâlinde bu suç oluşmayacaktır. Yargıtay da banka kart numarası ele geçirilerek İnternet ortamında işlem yapılması ve yarar elde edilmesi hâlinde 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 hâlinde 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 zorunludur.

İkinci fıkradaki 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, bunu kullanmasa bile ikinci fıkra kapsamında cezai sorumluluğa sahip olacaktır.

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

Sahte oluşturulan bir banka ve kredi kartının kullanılması suretiyle failin kendisine veya üçüncü bir kimseye yarar sağlaması ise üçüncü fıkra kapsamında 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 suçta vücut verecektir.

Üçüncü fıkra kapsamında sahte bir kartın ele geçmesi yetmez. Bu durumda ikinci fıkrada kapsamında sorumluluk doğar. Ancak ele geçirilen sahte kartın kullanılması hâlinde 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 kart 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 fıkrada kapsamında değil, daha ağır ceza gerektiren suçtan sorumluluk oluşacaktır. Bu husus ilgili düzenlemede açıkça ifade edilmiştir.

Tipik Manevi Unsur

Suç kasten işlenebilen bir suçtur. Kanunda taksirli hâline yer verilmediğinden bahsi geçen eylemlerin taksirle yapılması suça vücut vermeyecektir.

Hukuka Aykırılık

Söz konusu suçun birinci fıkra kapsamında oluşması bakımından ilgilinin rızası hukuka uygunluk sebebinin varlığı söz konusu olabilir. Ancak rıza tipik düzenlemede açıkça ifade edildiğinden, burada artık hukuka uygunluk sebebi olan değil, bilakis tipikliği kaldıran bir rıza söz konusu olacaktır. Bunun dışında diğer hukuka uygunluk sebepleri söz konusu fiil bakımından oluştuğu ölçüde uygulama alanı bulabilecektir.

Kusurluluk

Kusurluğu kaldıran sebepler bu suç 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 söz konusu suçun birinci fıkra kapsamında işlenmesi hâlinde, bazı şahsi cezasızlık sebeplerine yer vermiştir. Bu bağlamda söz konusu cezasızlık sebepleri sadece fiilin birinci fıkra kapsamında kalması hâlinde 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 hâlinde, 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. Aynı evlerde yaşayan kardeşlerden biri diğerinin kredi kartını rızası olmaksızın kullandığında, şahsi cezasızlık sebebi geçerli olmaz.

Etkin Pişmanlık

Kanunkoyucu, yine birinci fıkra kapsamına giren fiillerle ilgili olarak etkin pişmanlık hâlini de kabul etmiştir. Buna göre söz konusu fiiller bakımından malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanacaktır. Yine vurgulamak da fayda vardır ki birinci

fıkra kapsamı dışında kalan fiillerle ilgili olarak etkin pişmanlık hükümlerinin uygulanması 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 hâlinde, verilecek cezanın üçte ikisine kadarı indirilir. Bu etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi hâlinde, verilecek cezanın yarısına kadarı indirilir. Kısmen geri verme veya tazmin hâlinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır (TCK m.168).*

Suçun Özel Belirîş Biçimleri

Teşebbüs

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

İştirak

Bu suçta iştirakin her türlü 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 gerçekleştirme düşüncesi olmayan birisine, sahte kart üretme fikrini aşıl原因an kişi ise, bu düşüncayı oluşturduğu kişinin fiili gerçekleştirmesi hâlinde azmettiren olarak sorumlu olacaktır. Fiili gerçekleştiren kişi ise müstakil fail olarak cezai sorumluluğa sahip olur.

İçtima

Öncelikle belirtmek gerekir ki TCK m.245 kapsamında birinci, ikinci ve üçüncü fıkradaki düzenlemelerin ayrı ayrı suçları düzenlediği konusunda doktrinde ağırlıklı görüş vardır. Bu ağırlıklı görüş Yargıtay tarafından da kabul görmektedir. Dolayısıyla bu görüşe göre, bir kimse hem sahte kart oluşturur hem de bu sahte kartı kullanmak suretiyle kendisine yarar sağlarsa hem ikinci fıkra göre hem de üçüncü fıkra göre cezalandırılacaktır. Yargıtay uygulaması da bu yöndedir (Yaşar-Gökcan-Artuç, 2014:7342 vd.). Kanaatimize göre ise kanunkoyucu birden farklı fiili tanımlamış olsa bile, bunları tek bir maddede ve tek bir suç (banka ve kredi kartlarının kötüye kullanılması suçu) adı altında toplamışsa burada tanımlanan farklı fıkralardaki fiilleri aynı suçun temel şekli ve nitelikli hâlleri olarak kabul etmek gereklidir. Dolayısıyla yukarıda bahsedilen hâlde tek suçun olduğu ve en ağır cezayı gerektiren üçüncü fıkra hükmüne göre cezai sorumluluğun doğduğu kabul edilmelidir. Ancak söylediğimiz üzere bizim görüşümüz azınlık görüşüdür.

Ayrıca belirtmek gerekir ki 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.

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 bir miktar arttırma 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).

BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE EL KOYMA

Kavram

Bilişim sistemlerinin ve dolayısıyla bilgisayarların sosyal ve ticari alanda giderek yaygınlaşması ve bireysel yaşamda da giderek daha fazla önem arz etmesine bağlı olarak kanunkoyucu bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve el koyma faaliyetlerini ayrıca düzenleme ihtiyacı hissetmiştir. Bu bağlamda söz konusu tedbir, CMK'nın birinci kitap, dördüncü kısım, dördüncü bölümünde, "arama ve el koyma" başlığı altında, m.134'te hükme bağlanmıştır.

Tedbir sadece soruşturma sırasında başvurulabilen bir tedbirdir. Kanun koyucunun bu tedbirin uygulanmasına kovuşturma bakımından da cevaz verdiğine ilişkin bir düzenleme kanunda bulunmamaktadır. Temel haklara sınırlama getiren bir muhakeme işlemini düzenliyor olması nedeniyle, CMK m.134'teki hükmü kıyasen kovuşturmaya da uygulamak mümkün değildir.

Aşağıda özel olarak ayrı bir maddede hük bağlanmış olan söz konusu tedbir alt başlıklar hâlinde 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 hâlinde 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 tanır. Eğer tedbirin uygulama alanının kovuşturmayı da kapsar şekilde genişletilmesi isteniyorsa, bunun ayrıca düzenleme altına alınması zorunluluktur kanaatindeyiz.

Hangi merci, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbirine karar vermeye yetkilidir?



SIRA SİZDE

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 hâline getirilmesine hakim tarafından karar verilir (CMK m.134/1). Ancak bazen şifreleme nedeniyle söz konusu işlemlerin gerçekleştirilmesi mümkün olmayabilir. Kanunkoyucu bu ihtimale binaen ilgili araç ve gereçler üzerinde el koyma işleminin yapılmasına cevaz vermiştir. Buna göre “bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülmemesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir (CMK m.134/2).” Bilgisayarların ticari ve gündelik yaşamda giderek daha fazla yer almaları ve önem arz etmeleri dolayısıyla kanunkoyucu öncelikle bunlar üzerinde el koyma işlemi yapılırsa, gerekli arama, kopya çıkarma ve metin hâline getirme işlemlerinin yapılmasını öngörmüştür. Bu şekilde söz konusu bilgisayarın şüphelinin kullanımından alınması söz konusu olmayacaktır. Ancak şifreleme nedeniyle bu işlemler yapılamazsa mecburen el koymaya 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 el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır (CMK m.134/3). Alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. (CMK m.134/4).” Nitekim kendisinden alınıp el konulan donanımdaki veriler üzerinde sonradan değişiklik yapılması ihtimaline binaen, bir kopyanın şüpheliye verilmesi onun bakımından önemli bir güvence oluşturmaktadır.

“Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kağıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır (CMK m.134/5).”

Özet

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 öngörülen ve dolayısıyla suç tipleri arasında düzenlenmeyen birtakım 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. Kanun'da 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'de hırsızlık, dolandırıcılık gibi bazı suçların bilişim sistemleri vasıtasıyla işlenmesi hâli de söz konusu suçların nitelikli hâli olarak ayrıca hükme bağlanmıştır. Ayrıca Fikir ve Sanat Eserleri Kanunu ile Elektronik İmza Kanunu'nda düzenlenen bilişim suçları da bulunmaktadır.

765 sayılı TCK'de 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.

Bilişim sistemine girme suçunu düzenleyen TCK'nın 243. maddesinin metni şu şekildedir:

Madde 243 - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (2) Yukarıdaki fıkralarda tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, 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.

Görüldüğü üzere madde üç fıkradan oluşmaktadır. Birinci fıkra suçun temel şekli düzenlenirken ikinci ve üçüncü fıkralarda nitelikli hallerine yer verilmiştir. Bu hallerden ilkinin gerçekleşmesi hâlinde faile suçun temel şekline nazaran daha az, ikincisinin gerçekleşmesi hâlinde ise daha fazla ceza verilmesi öngörülmüştür. Suçun manevi unsuru ise kasttır. Suçu oluşturan fiillerin hangi amaçla gerçekleştirildiğinin bir önemi yoktur. Bu bağlamda suçun gerçekleşmesi bakımından özel kast aranmaz.

TCK'nın 244. maddesinde bilişim alanındaki bir diğer suç tipi olarak, *sistemi engelleme, bozma, verileri yok etme veya değiştirme* düzenlenmiştir. Maddenin birinci ve ikinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızzar fiilleri özel bir suç hâline getirilmiştir. Üçüncü fıkra, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde, verilecek cezanın artırılması öngörülmüştür. Dördüncü fıkra ise bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımını altına alınmıştır. 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 hâlinde, 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 hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur. Söz konusu suç kasten işlenebilen bir suçtur. Kanunda taksirli şekline açıkça yer verilmediği için, suçun taksirle işlenmesi mümkün değildir. Kast bakımından ise genel kast yeterlidir.

Gerek banka kartları gerekse kredi kartları son dönemde gündelik hayatta giderek daha fazla yer tutmaya başlamıştır. Birçok insan artık yanında para taşımamakta, doğrudan veya İnternet üzerinden yaptığı alışverişlerde çoğunluk banka kartı veya kredi kartı kullanmayı tercih etmektedir. 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 kullanılması suçunu hüküm altına almıştır.

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 kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli 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 adli 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 hâlinde, ilgili akraba hakkında cezaya hükümlenmez.

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

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. Suç kasten işlenebilen bir suçtur. Kanun'da taksirli hâline yer verilmediğinden bahsi geçen eylemlerin taksirle yapılması suça vücut vermeyecektir.

Son olarak bilişim sistemlerinin ve dolayısıyla bilgisayarların sosyal ve ticari alanda giderek yaygınlaşması ve bireysel yaşamda da giderek daha fazla önem arz etmesine bağlı olarak kanunkoyucu bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve el koyma faali-

yetlerini ayrıca düzenleme ihtiyacı hissetmiştir. Bu bağlamda söz konusu tedbir, CMK'nin birinci kitap, dördüncü kısım, dördüncü bölümünde, "arama ve el koyma" 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 işlemi düzenliyor olması nedeniyle, CMK m.134'teki hükmü kıyasen kovuşturmayaya da uygulamak mümkün değildir.

Kendimizi Sıneyalım

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

- Herkes suçun faili olabilir.
- Yalnız kamu görevlileri suçun faili olabilir.
- Yalnız erkekler suçun faili olabilir.
- Yalnız kadınlar suçun faili olabilir.
- Yalnız on sekiz yaşından büyükler suçun faili olabilir.

2. Şifreli televizyon yayınlarını, şifreyi kırmak suretiyle ödeme yapmaksızın izleyen kimse aşağıdaki suçlardan hangisinden sorumlu olacaktır?

- Hırsızlık
- Karşılıksız yararlanma
- Bilişim sistemine girme
- Dolandırıcılık
- Güveni kötüye kullanma

3. Aşağıdakilerden hangisi bilişim sistemine girme suçunun daha fazla cezayı gerektiren nitelikli hâli olarak düzenlenmiştir?

- Kamu görevlisine karşı işlenmesi
- Ticari işletmelere karşı işlenmesi
- Mağdurun on sekiz yaşından büyük olması
- Fiil nedeniyle verilerin yok olması veya değişmesi
- Fiilin bir örgütün faaliyeti kapsamında gerçekleştirilmiş olması

4. Aşağıdakilerden hangisi sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun ağırlaştırıcı sebebi kapsamında yer alır?

- Suçun örgütün faaliyeti kapsamında işlenmesi
- Suç sonucunda herhangi bir tüzel kişiliğe menfaat sağlanması
- Suçun bir bankaya karşı işlenmesi
- Suçun mağdurunun otuz yaşından büyük olması
- Suçun failinin otuz yaşından büyük olması

5. Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun tipik manevi unsuru ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

- Genel kast gerekli ve yeterlidir.
- Failin özel bir kastla hareket etmesi aranır.
- Suç kasten veya taksirle işlenebilir.
- Basit taksir gerekli ve yeterlidir.
- Suç ancak bilinçli taksirle işlenebilir.

6. Başkasına ait kredi kartını çalıp alışverişte kullanan kimse- nin cezai sorumluluğu ile ilgili aşağıdaki ifade doğrudur?

- Sadece banka ve kredi kartlarının kötüye kullanılması suçundan sorumludur.
- Sadece hırsızlıktan sorumludur.
- Sadece bilişim sistemine girmekten sorumludur.
- Hırsızlık ile banka ve kredi kartlarının kötüye kullanılması suçlarından sorumludur
- Bilişim sistemine girme, hırsızlık ve banka ve kredi kartlarının kötüye kullanılması suçlarından sorumludur.

7. 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 kullandırarak kendisine veya başkasına yarar sağlayan kişi bakımından aşağıdaki hâllerden hangisinde şahsi cezasızlık sebebi söz konusudur?

- Suçu babasına karşı işlemişse
- Suç nedeniyle ortaya çıkan zararı gidermişse
- Yargılama sırasında pişmanlığını açıkça ifade etmişse
- Kamu kurumu yararına suç işlemişse
- Hukuki alacağının tahsili amacıyla suç işlemişse

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

- Basit şüphe
- Makul şüphe
- Yeterli şüphe
- Kuvvetli şüphe
- Kesin şüphe

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

- Tedbire sadece hakim karar verebilir.
- Tedbire kural olarak hakim, gecikmesinde sakınca bulunan hallerde ise Cum. Savcısı karar verebilir.
- Tedbire kural olarak hakim, gecikmesinde sakınca bulunan hallerde Cum. Savcısı, Cum. Savcısına ulaşamıyorsa da kolluk amiri karar verebilir.
- Tedbire kural olarak hakim, gecikmesinde sakınca bulunan hallerde ise mülki amir karar verebilir.
- Tedbire yalnızca Cum. Savcısı karar verebilir.

10. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbirine karar verilebilecek muhakeme süreci ile ilgili aşağıdaki ifade hangisi doğrudur?

- a. Yalnızca soruşturma sırasında başvurulabilen bir tedbirdir.
- b. Yalnızca duruşma sırasında başvurulabilen bir tedbirdir.
- c. Yalnızca iddianamenin değerlendirilmesi aşamasında başvurulabilir.
- d. Yalnızca duruşma aşamasında başvurulabilir.
- e. Hem soruşturma hem de kovuşturma da başvurulabilir.

Kendimizi Sıneyalım 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 Değişirme Suçu” konusunu yeniden gözden geçiriniz. |
| 5. a | Yanıtınız yanlış ise “Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değişirme 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 El Koyma” konusunu yeniden gözden geçiriniz. |
| 9. d | Yanıtınız yanlış ise “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma” konusunu yeniden gözden geçiriniz. |
| 10. a | Yanıtınız yanlış ise “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma” konusunu yeniden gözden geçiriniz. |

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

“İnternational” 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 İnternete “ağlar arası ağ” da denilmektedir. İnternet sanıldığıının aksine veri iletim ağlarının yalnızca bir türü, dolayısıyla sanal alanın yalnızca bir parçasıdır. Ancak dünya üzerinde bugün kullanılan en yaygın ve en geniş ağıdır. Sanal alan ise bilişim sistemleri ile bunları birbirine bağlayan her türlü veri iletim ağından oluşan, fiziksel yapısı sayısal verilerden ibaret bir alandır.

Sıra Sizde 2

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu kasten işlenebilen bir suçtur. Kanunda taksirli şekline açıkça yer verilmediği için, suçun taksirle işlenmesi mümkün değildir. Kast bakımından ise genel kast yeterlidir. Nitekim kanunda failin belirli bir saikle hareket etmesi zorunluluğu aranmamıştır. Bununla birlikte suç olası kastla da işlenebilir.

Sıra Sizde 3

Tedbire Cumhuriyet Savcısının istemi üzerine sulh ceza hakimisi 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 hakiminin başka bir adli merciin de herhangi bir koşula bağlı olarak bu tedbire karar vermesi söz konusu değildir.

Yararlanılan Kaynaklar

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

5

Amaçlarımız

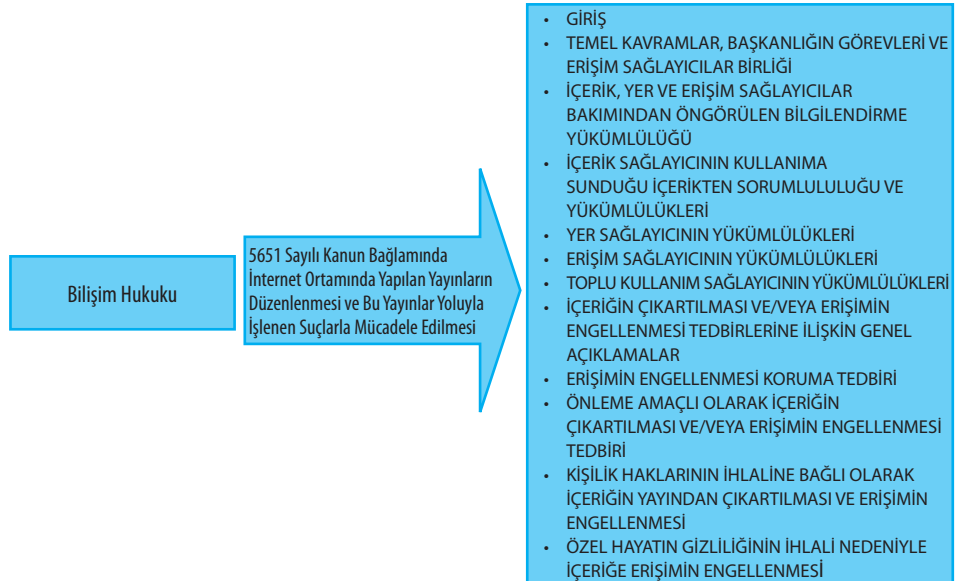
Bu üniteyi tamamladıktan sonra;

- 5651 sayılı Kanun kapsamındaki temel kavramları açıklayabilecek,
- İçerik, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerini belirleyebilecek,
- Farklı kapsamdaki içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirlerinin uygulanma koşullarını analiz edebilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- 5651 Sayılı Kanun
- İçerik Sağlayıcı
- Yer Sağlayıcı
- Erişim Sağlayıcı
- Toplu Kullanım Sağlayıcı
- İçeriğin Çıkartılması
- İçeriğe Erişimin Engellenmesi
- Siteye Erişimin Engellenmesi

İçindekiler



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

GİRİŞ

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

Bununla birlikte İnternet insanoğlunun hayatını sadece kolaylaştırmakla kalmamış aynı zamanda asosyalleşme, İnternet bağımlılığı gibi bazı dezavantajları da beraberinde getirmiştir. Ancak her halükarda modern dönemin bu görelî yeniliğinin insanlık bakımından dezavantajlarına nazaran çok daha büyük faydalar sağladığı aşîkârdır kanaatindeyiz. Bu nedenle İnternet'i sosyal hayattan çıkarmak artık mümkün olmadığına göre, onun toplumsal menfaat bakımından getirdiğı zararları mümkün olduğunca aza indirmeye gayret etmelidir.

İnternet'in toplumsal menfaat bakımından ortaya çıkardığı en önemli dezavantajlardan birisi yeni suç işleme yöntemlerine imkân tanınması ve ortaya çıkardığı yeni bireysel menfaatlere bağılı olarak yeni suç biçimlerinin ortaya çıkması olarak sayılabilir. Gerçekten de İnternet 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 edemediğı yeni imkânlar ve haklar ortaya çıkartan İnternet, bu haklara karşı işlenecek suçlarda da önemli bir araç hâline gelebilmektedir. Buna rağmen İnternet'i suçla özdeşleşmiş bir araç olarak görmekten de kaçınmak gerekir (Gedik, 2008:180).

İnternet sosyal hayat bakımından zararlı bir araç mıdır?



SIRA SİZDE

Bu bağlamda İnternet yoluyla işlenen suçlarla mücadele adına kanunkoyucunun da bir takım özel düzenlemeler yapması kaçınılmazdır. Çünkü modern dönemin getirdiğı bu yeni araç, klasik suç, ceza ve muhakeme anlayışının öngöremediğı toplumsal zararlar ve suç işleme yöntemleri ortaya çıkarmıştır. Bunlarla mücadele edebilmek ise ancak İnternet'in özellikleri ve yapısı gözönünde bulundurularak yapılacak özel hukuki düzenlemelerle mümkün olabilecektir.

İnternet yoluyla işlenen suçlardan önemli bir kısmı ise İnternet yayınları vasıtasıyla gerçekleştirilmektedir. Dolayısıyla bu tür suçlarla mücadele adına özel birtakım düzenlemelerin yapılması kaçınılmazdır. Bu gereklilikler karşısında kanunkoyucumuz da İnternet

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.K.). Söz konusu kanunun amacı 1. maddede; *içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemek* olarak belirlenmiştir.

Bu ünite de söz konusu kanunun öngördüğü düzenlemeler ve bunların içeriği inceleme konusu yapılacaktır. Nitekim bilişim hukukuna ilişkin bir kitapta, söz konusu düzenlemenin ele alınması sistematik açıdan bir zorunluluktur.

TEMEL KAVRAMLAR, BAŞKANLIĞIN GÖREVLERİ VE ERİŞİM SAĞLAYICILAR BİRLİĞİ

Genel Olarak

Ünitenin başında, ünite de kullanılacak ve ilgili kanunda geçen temel kavramların açıklanmasının, 5651 s. K'nın uygulanmasında çok önemli bir rolü bulunan başkanlığın görevlerinin belirlenmesinin ve Kanun'un 8. maddesi kapsamı dışında kalan hâllerde 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. Kanun'un ikinci maddesinde kanunda geçen bazı kavramların tanımlanması yoluna gidilmiştir. Böylelikle kanunkoyucu içeriği konusunda tereddüte düşülebilecek bazı kavram ve eterimlerden 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);

- a. *Bakanlık: Ulaştırma Bakanlığı,*
- b. *Başkanlık: Kurum bünyesinde bulunan Telekomünikasyon İletişim Başkanlığını,*
- c. *Başkan: Telekomünikasyon İletişim Başkanını,*
- ç. *Bilgi: Verilerin anlam kazanmış biçimini,*
- d. *Erişim: Bir İnternet ortamına bağlanarak kullanım olanağı kazanılmasını,*
- e. *Erişim sağlayıcı: Kullanıcılarına İnternet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,*
- f. *İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,*
- g. *İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan İnternet üzerinde oluşturulan ortamı,*
- ğ. *İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,*
- h. *İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,*
- ı. *Kurum: Telekomünikasyon Kurumunu,*
- i. *Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre İnternet ortamı kullanım olanağı sağlayanı,*
- j. *Trafik bilgisi: Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,*



- k. Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,
- l. Yayın: İnternet ortamında yapılan yayını,
- m. Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,
- n. Birlik: Erişim Sağlayıcıları Birliğini,
- o. Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,
- ö. İçeriğin yayından çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını,
- p. URL adresi: İlgili içeriğin İnternet'te bulunduğu tam İnternet adresini,
- r. 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.

Başkanlığın Görevleri

Kanun'la verilen görevler, Kurum bünyesinde bulunan Başkanlıkça yerine getirilir (5651 s.K. m.10/1). Kanun'larla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Başkanlığın 5651 s.K. 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 İnternet ortamında yapılan ve bu Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye, İnternet'in güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usûller dahilinde Kurumca karşılanacak çalışma kurulları oluşturmak.
- b. İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti hâlinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanun'da 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 ticari amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usûlleri belirlemek.
- d. İnternet ortamındaki yayınların izlenmesi suretiyle Kanun'un 8 inci maddesinin birinci fıkrasında 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 İnternet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak.
- g. Bu Kanun'un 8 inci maddesinin birinci fıkrasında sayılan suçların, İnternet 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 başkanlık; 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 İnternet'in yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli kullanılması gibi konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır. 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 alınması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar (5651 s.K. m.10/5,6).

Erişim Sağlayıcılar Birliği

Temel kavramlar ve başkanlığın görevleri açıklandıktan sonra kanunkoyucunun 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 kanunkoyucu 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 İnternet servis sağlayıcıları ile İnternet 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 satış 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 İnternet servis sağlayıcıları faaliyette bulunamaz (5651 s.K. m.6/A/9, 10).

İÇERİK, YER VE ERİŞİM SAĞLAYICILAR BAKIMINDAN ÖNGÖRÜLEN BİLGİLENDİRME YÜKÜMLÜLÜĞÜ

İnternet ortamındaki yayınlarda düzenin sağlanması bakımından kanunkoyucu içerik, yer ve erişim sağlayıcılarına bilgilendirme yükümlülüğü getirmiştir. Bu bağlamda söz konusu sağlayıcılar, yönetmelile belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait İnternet 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). Bununla birlikte söz konusu yükümlülüğü yerine getirmeyen sağlayıcılar bakımından iki bin TL' den elli bin TL' ye kadar idari para cezası verilmesi öngörülmüştür. Söz konusu yaptırım uygulamakla yetkili merci ise başkanlıktır (5651 s.K. m.3/2). Başkanlığın bu idari para cezasına karşı

6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine kanun yoluna başvurulması da mümkündür (5651 s.K. m.8/12).

Kanunkoyucu 5651 s. Kanun kapsamındaki faaliyetleri yurt içi veya yurt dışından yürütenlere, İnternet 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 kanunkoyucu, bu kanun kapsamında faaliyet yürütenlere de İnternet sayfalarında paylaşılan bilgiler ve sayılan diğer araçlarla bildirim yapılmasına da cevaz vermiştir.

İÇERİK SAĞLAYICININ KULLANIMA SUNDUĞU İÇERİKTEN SORUMLULUĞU VE YÜKÜMLÜLÜKLERİ

Kanunkoyucu içerik sağlayıcının İnternet 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 İnternet ortamına koyduğu içeriğin hukuki sorumluluğunu taşır. Ancak içeriğin yayınının aynı zamanda suç teşkil etmesi hâlinde, 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 kanunkoyucu 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, Başkanlığın 5651 sayılı Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında talep ettiği bilgileri, talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla da yükümlüdür (5651 s.K. m.4/3).

YER SAĞLAYICININ YÜKÜMLÜLÜKLERİ

Kanunkoyucu yer sağlayıcının, kural olarak yer sağladığı içerik bakımından denetim sorumluluğunu 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, Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça 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, Başkanlık tarafından on bin Türk lirasından yüz bin Türk lirasına kadar idari para cezası verilmesi de hükme bağlanmıştır. Başkanlığın 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).

ERİŞİM SAĞLAYICININ YÜKÜMLÜLÜKLERİ

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 bağlanmıştır. 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 İnternet ortamına girebilmelerine imkân sağlayan erişim sağlayıcılar bakımından da kanunkoyucu bir takım yükümlülükler getirmiştir. Bu doğrultuda *erişim sağlayıcı* (5651 s.K. m.6/1);

- Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi hâlinde erişimi engellemekle,*
- 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,*
- 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,*
- Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,*
- Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür.*

Bu sayılanlardan (b), (c), (ç) ve (d) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkanlık 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 KULLANIM SAĞLAYICININ YÜKÜMLÜLÜKLERİ

5651 s. K'da özellikle İnternet kafeler 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 İnternet 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 biri-ne karar vermeye mahalli mülki amir yetkilidir (5651 s.K. m.7/4).

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 tedbidir. Bunun dışında önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi tedbiri farklı koşullara bağlı olarak düzenleme altına alınmıştır. Ayrıca kişilik haklarının İnternet 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 İnternet 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 sistematigi açısından daha uygun olacaktır. mevcut durumda kanunkoyucu 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 artırılması, kamuoyunda tepkiyle karşılanmakta, doktrinde de yer yer sert biçimde eleştirilmektedir (Bkz. Dülger, 2014:757). Bu eleştirilerden bazılarını 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.

5651 sayılı Kanun'da hangi tür içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirlerine yer verilmiştir?



SIRA SİZDE

İnternet yayınları yoluyla işlenen hukuka aykırılıklarla mücadele gerçekten zordur. Nitekim başlangıç kısmında da belirttiğimiz üzere, İnternet yayınları vasıtasıyla klasik adalet ve muhakeme anlayışının öngöremediği şekillerde suç işlenmesi veya kamusal düzenin tehlikeye düşürülmesi söz konusu olabilmektedir. Kanunkoyucu 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.

ERİŞİMİN ENGELLENMESİ KORUMA TEDBİRİ

Genel Olarak

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, hâlâ suçsuzluk karinesinden faydalanmakta olan şüpheli veya sanık ile bazı üçüncü kişilerin temel haklarına önemli müdahaleler gerçekleştirilmektedir. Bu tedbirler 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 gerekir; *şüpheli veya sanığı ya da bir delili elde etmek, duruşmanın yapılmasını yahut hükmün infazını teminat altına almak amacıyla başvurulmuş, 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 bir kaçını 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 mahkumiyet hükmü kurulduktan sonra sanığın kaçma tehlikesi varsa, hükmen tutukluluğuna karar verilmesi suretiyle, hüküm kesinleşinceye kadar el altında tutulması sağlanabilir. Böylelikle sanığın kaçmasına engel olunarak mahkumiyet hükmünün infazı teminat altına alınır.

Bu bağlamda belirtmek gerekir ki kanunkoyucu 5651 s.K'da da İnternet yayınları yoluyla işlenen suçlarla mücadele adına erişimin engellenmesi koruma tedbirine yer vermiştir. Kanunkoyucunun bu uygulamayı koruma tedbiri olarak gördüğü konusunda tereddüt yoktur. Nitekim 5651 s.Kanun'un 8. maddesinin 2 ve 10. fıkrasında bu kurumu açıkça koruma tedbiri olarak nitelendirmiştir. Ancak söz konusu tedbirin klasik bir koruma tedbiri olmadığı da aşîkardır. 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 İnternet yoluyla işlendiği düşünülen bazı suçların devamlılığına engel olmaktadır. Örneğin bir İnternet 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

Kanunkoyucu erişimin engellenmesi tedbirine karar verilebilmesi bakımından yeterli şüphe derecesini gerekli görmüştür. Yeterli şüphe İnternet ortamında yapılan yayınlara

rın içeriğinin Kanun'da 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 İnternet 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, *İnternet 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 hâllerde 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 hakim onayına sunar ve hakim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması hâlinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır (5651 s.K. m.8/2).*

Tedbirin Süresi ve Tedbire Karşı Kanunyolu

Erişimin engellenmesi kararının uygulanması bakımından Kanun'da belirli bir süre öngörülmemiştir. Dolayısıyla muhakeme devam ettiği bu tedbirin uygulanması mümkün görünmektedir. Bununla birlikte amacı gerçekleştirebilecek nitelikte 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 merciin inceleme yapacağı CMK m.267 vd. maddelerde hükme bağlanmıştır.

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

Tedbirin Uygulanması

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

Soruşturma sonucunda kovuşturmayaya yer olmadığı veya kovuşturma sonucunda beraat kararı verilmesi hâlinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda soruşturma sonunda Cumhuriyet savcısı kovuşturmayaya yer olmadığı kararının bir örneğini, kovuşturma sonunda ise mahkeme beraat kararının bir örneğini Başkanlığa 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 kanunkoyucu 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 Çıkarılmasının Tedbire Etkisi

Konusu yukarıda saydığımız katalog suçlardan biri veya birkaçını oluşturan içeriğin yayından çıkarılması hâlinde; 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 İdari Bir Tedbir Olarak Engellenmesi

Kanun'da belirli hâllerde erişimin engellenmesinin idari bir tedbir olarak 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 bulunsun 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 Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir (5651 s.K. m.8/4).

İdari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık 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 ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir (5651 s.K. m.8/11). Başkanlığın 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 Millî Piyango İdaresi gibi), kendi görev alanına giren suçların İnternet ortamında işlendiğini tespit etmeleri halinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilirler. Erişimin engellenmesi kararları uygulanmak üzere Telekomünikasyon İletişim Başkanlığına gönderilir (5651 s.K. m.8/14).

ÖNLEME AMAÇLI OLARAK İÇERİĞİN ÇIKARTILMASI VE/VEYA ERİŞİMİN ENGELLENMESİ TEDBİRİ

Genel Olarak

Kanunkoyucu 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 İnternet sitesi üzerinden suç işlemeye yönelik haberleştiklerine dair makul sebepler varsa henüz ortada işlenmiş bir suç olmamasına rağmen İnternet sitesine erişimin engellenmesine ve/veya bazı içeriklerin çıkartılmasına karar verilebilecektir. Bununla birlikte İnternet sitesi üzerinden halkı kin ve düşmanlığa tahrik ederek, suç teşkil edecek eylemlerde bulunma çağrısı yapılıyorsa; hem halkı kin ve düşmanlığa tahrik suçları işlenmiş hem de ileride başka suçların işlenecek olması tehlikesi ortaya çıkmış olacaktır. Dolayısıyla bu tür hâllerde de tedbirin uygulanması söz konusu olabilecektir.

Tedbire Başvurulmasının Koşulları

Kanunkoyucu 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 bir kaçına 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 başkanlık da bu tedbire karar vermeye yetkilidir. Ancak başkanlığın re'sen bu kararı verebilmesi mümkün değildir. Bunun için belirli nedenlere bağlı olarak başbakanlık 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, **Başbakanlık** veya millî güvenlik ve kamu düzeninin korunması,

suç işlenmesinin önlenmesi veya genel sağlığın korunması ile **ilgili bakanlıkların** talebi üzerine Başkanlık tarafından tedbire karar verilebilecektir (5651 s.K. m.8/A/1). Gecikmesinde sakınca bulunan hallerde yukarıda belirtilen tüm sebeplere bağlı olarak başbakanlık 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, *Başkanlık 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 Başkanlık tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkanlık 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 yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, İnternet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir (5651 s.K. m.8/A/3).* Dolayısıyla kanunkoyucu içeriğin sadece ihlale ilgili kısmına erişimin engellenememesi durumunda, ilgili İnternet sitesini erişimin tümüyle engellenmesine de imkân tanımıştır.

Bu tedbirin uygulanmasına neden olan suça konu İnternet içeriklerini oluşturan ve yayanlar hakkında Başkanlık 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.

Kanunkoyucu 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 elli bin Türk lirasından beş yüz bin Türk lirasına kadar idari para cezası verilmesini de hükme bağlamıştır (5651 s.K. m.8/A/5).

SIRA SİZDE



3

Önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirine hangi merciler karar vermeye yetkilidir?

KİŞİLİK HAKLARININ İHLALİNE BAĞLI OLARAK İÇERİĞİN YAYINDAN ÇIKARTILMASI VE ERİŞİMİN ENGELLENMESİ

5651 s.K.'da İnternet 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 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 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 İnternet 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 İnternet 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, İnternet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir (5651 s.K. m.9/2,3,4). Kanunkoyucu öncelikle kişilik haklarını ihlal eden yayına erişimin engellenmesini öngörmüş; ancak bunun mümkün görülmemesi halinde, ilgili İnternet 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 kanunkoyucu, kişilik haklarını ihlal eden içeriğin yayından çıkartılması hâlinde, 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 hakimın verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka İnternet adreslerinde de yayımlanması 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 İnternet 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 İnternet sitesindeki içerik için tekrar tekrar aramak yersiz olacaktır. Bu bağlamda kanunkoyucunun 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 kanunkoyucu kararın yerine getirilmemesini adli para cezasına tabi kasıtlı bir suç olarak düzenleme altına almıştır.

ÖZEL HAYATIN GİZLİLİĞİNİN İHLALI NEDENİYLE İÇERİĞE ERİŞİMİN ENGELLENMESİ

Kanunkoyucu 5651 s.K'da İnternet 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 ihlalinin 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 *İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğini iddia eden kişiler, Başkanlığa 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. Başkanlık, 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, İnternet 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, İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararı en geç kırk sekiz saat içinde açıklar ve doğrudan Başkanlığa gönderir; aksi halde, erişimin engellenmesi tedbiri kendiliğinden kalkar* (5651 s.K. m.9/A/5). Hakim tarafından verilen bu karara karşı Başkanlık 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 Başkanlık tarafından yapılacağı da hükme bağlanmıştır. Bu kapsamda Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hakim, kararını kırk sekiz saat içinde açıklar (5651 s.K. m.9/A/8,9).

Özet

Modern zamanların en önemli keşiflerinden birisi olan İnternet insanlığa sağladığı faydalar yanında birçok olumsuzluğu da beraberinde getirmiştir. Dolayısıyla İnternet insanoğlunun hayatını sadece kolaylaştırmakla kalmamış aynı zamanda asosyalleşme, İnternet bağımlılığı gibi bazı toplumsal sorunları da beraberinde getirmiştir. Ancak her halükarda modern dönemin bu önemli yeniliğinin insanlık bakımından dezavantajlarına nazaran çok daha büyük avantajlar sağladığı açıktır. Bu nedenle İnterneti sosyal hayattan çıkarmak mümkün olmadığına göre, onun toplumsal menfaat bakımından getirdiği zararları mümkün olduğunca aza indirmeye gayret etmelidir. İnternet'in toplumsal menfaat bakımından ortaya çıkardığı en önemli dezavantajlardan birisi yeni suç işleme yöntemlerine imkân tanınması 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 İnternet, bireysel haklara karşı işlenecek suçlarda önemli bir araç haline de gelebilmektedir.

Bu bağlamda İnternet yoluyla işlenen suçlarla mücadele adına kanunkoyucunun da bir takım özel düzenlemeler yapması kaçınılmazdır. Bu gereklilikler karşısında kanunkoyucumuz da İnternet 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.K. ile verilen görevlerin, Kurum bünyesinde bulunan Başkanlıkça yerine getirileceği hüküm altına alınmıştır. Söz konusu kanunun 10/4. maddesinde, kanun ayrıca görevlendirdiği haller saklı kalmak üzere Başkanlığın görevleri sayılmıştır. Ayrıca Kanunun 8. maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur.

İnternet ortamındaki yayınlarda düzenin sağlanması bakımından kanunkoyucu içerik, yer ve erişim sağlayıcılarına bilgilendirme yükümlülüğü getirmiştir. Bu bağlamda söz konusu sağlayıcılar, yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait İnternet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

Ayrıca içerik sağlayıcının İnternet ortamında kullanıma sunduğu her türlü içerikten sorumlu olacağı da hükme bağlanmıştır. Düzenlemede sadece sorumluluktan bahsedildiği için ve cezai sorumluluk ayrıca vurgulanmadığından, bahsi geçen sorumluluktan 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 yüklenmesi fiilin ve cezanın kanunla açıkça düzenlenmesi gereklidir. Kanunkoyucu kural olarak yer sağlayıcının, yer sağladığı içerik bakımından denetim sorumluluğunu olmadığını kabul etmiştir. Bu bağlamda yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. 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. 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 bağlanmıştır. İçeriği denetim yükümlülüğü olmamakla birlikte kullanıcıların İnternet ortamına girebilmelerine imkân sağlayan erişim sağlayıcılar bakımından da kanunkoyucu bir takım yükümlülükler getirmiştir.

5651 s. K'da özellikle İnternet cafeler gibi ticari amaçlı olanların giderek yaygınlaştıkları görülen toplu kullanım sağlayıcılara da bir takım 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.

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 tedbidir. Bunun dışında önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi tedbiri farklı koşullara bağlı olarak düzenleme altına alınmıştır. Ayrıca kişilik haklarının İnternet 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 İnternet 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 sistematigi açısından daha uygun olacaktır. Mevcut durumda kanunkoyucu 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 artırılması, kamuoyunda tepkiyle karşılanmakta, doktrinde de yer yer sert biçimde eleştirilmektedir.

İnternet yayınları yoluyla işlenen hukuka aykırılıklarla mücadele gerçekten zordur. Nitekim başlangıç kısmında da belirttiğimiz üzere, İnternet yayınları vasıtasıyla klasik adalet ve muhakeme anlayışının öngöremediği şekillerde suç işlenmesi veya kamusal düzenin tehlikeye düşürülmesi söz konusu olabilmektedir. Kanunkoyucu 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.

Kendimizi Sıyalım

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

- Yer sağlayıcı
- Toplu kullanım sağlayıcı
- Erişim sağlayıcı
- Fiziksel sağlayıcı
- 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. Kanun'da öngörülen gerekli tedbirleri almak aşağıdakilerden hangisinin görevidir?

- Başkanlık
- Bakanlık
- Yer sağlayıcı
- Erişim sağlayıcılar birliği
- Başbakanlık

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

- Erişim Sağlayıcıları Birliği
- Telekomünikasyon İletişim Başkanlığı
- Yer Sağlayıcılar Birliği
- İçerik sağlayıcılar Birliği
- Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı

4. Yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait İnternet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurma yükümlülüğünü ihlal eden yer sağlayıcılar bakımından öngörülen yaptırım aşağıdakilerden hangisidir?

- İdari para cezası
- Adli para cezası
- Hapis cezası
- Müsadere
- Sürgün

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

- Ulaştırma Bakanlığından
- Belediye başkanından
- Emniyet Müdürlüğünden
- Telekomünikasyon İletişim Başkanlığından
- Mülki amirden

6. Erişimin engellenmesi koruma tedbirine başvurulabilmesi bakımından kanunkoyucu katalog suçların işlendiği hususunda en az hangi şüphe derecesine ulaşmış olmalıdır?

- Basit şüphe
- Makul şüphe
- Yeterli şüphe
- Kuvvetli şüphe
- Kesin şüphe

7. Aşağıdakilerden hangisi erişimin engellenmesi koruma tedbirine karar verilebilmesi bakımından İnternet yayının içeriğinin oluşturması gereken katalog suçlardan biridir?

- Soykırım
- İntihara yönlendirme
- Görevi kötüye kullanma
- Rüşvet
- Sahtecilik

8. Aşağıdakilerden hangisi önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirine başvurma nedenlerinden birini oluşturur?

- Milli güvenlik ve kamu düzeninin korunması
- Suç işlenmesinin önlenmesi
- Yaşam hakkının korunması
- Genel Sağlığın korunması
- Suç faillerinin yakalanması

9. Normal şartlarda önleme amaçlı olarak içeriğin çıkartılması ve/veya erişimin engellenmesi tedbirine karar verecek merci aşağıdakilerden hangisidir?

- Hakim
- Cum. Savcısı
- Ulaştırma Bakanlığı
- Telekomünikasyon İletişim Başkanlığı
- Başbakanlık

10. Özel hayatın gizliliğinin ihlali nedeniyle içeriğe erişimin engellenmesi tedbirinin uygulanması bakımından doğrudan emir verme yetkisi aşağıdakilerden hangisine aittir?

- Telekomünikasyon İletişim Başkanı
- Ulaştırma Bakanı
- Başbakan
- Erişim Sağlayıcılar Birliği
- Cumhurbaşkanı

Kendimizi Sınavalım Yanıt Anahtarı

1. e Yanıtınız yanlış ise “Temel Kavramlar” konusunu yeniden gözden geçiriniz.
2. a Yanıtınız yanlış ise “Başkanlığın 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 Çıkarılması ve/veya Erişimin Engellenmesi Tedbiri” konusunu yeniden gözden geçiriniz.
9. a Yanıtınız yanlış ise “Önleme Amaçlı Olarak İçeriğin Çıkarılması 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.

ması ve/veya erişimin engellenmesi hüküm altına alınmıştır. Son olarak aslında kişilik hakları kapsamında yer alan özel hayatın gizliliğinin ihlaline yönelik İnternet yayınlarına erişimin engellenmesi de ayrıca düzenlemeye tabi tutulmuştur.

Sıra Sizde 3

Tedbire karar vermeye yetkili merci kural olarak hakimdir. Bununla birlikte gecikmesinde sakınca bulunan hâllerde başkanlık da bu tedbire karar vermeye yetkilidir. Ancak başkanlığın re’sen bu kararı verebilmesi mümkün değildir. Bunun için belirli nedenlere bağlı olarak başbakanlık 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, **Başbakanlık** veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile **ilgili bakanlıkların** talebi üzerine Başkanlık tarafından tedbire karar verilebilecektir (5651 s.K. m.8/A/1). Gecikmesinde sakınca bulunan hâllerde yukarıda belirtilen tüm sebeplere bağlı olarak başbakanlık talepte bulunabilirken; ilgili bakanlıklar sadece millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerine bağlı olarak tedbirin uygulanması talebinde bulunabileceklerdir.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

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

Sıra Sizde 2

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 İnternet yayınları yoluyla ihlali ne bağlı olarak ilgililerin başvurusu üzerine içeriğin çıkartıl-

Yararlanılan Kaynaklar

- 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**, C.14, S.1-2
- Özen, M. ve Baştürk, İ. (2011) **Bilişim-İnternet ve Ceza Hukuku**, Ankara

6

Amaçlarımız

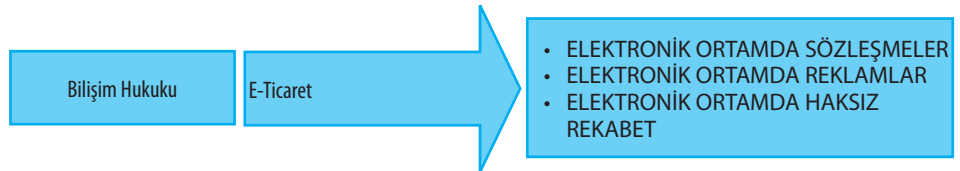
Bu üniteyi tamamladıktan sonra;

- Sözleşme kavramının elektronik ortamda ne anlama geldiğini açıklayabilecek,
- Sözleşmelerde dikkat edilmesi gereken noktaların ne olduğunu sıralayabilecek,
- Sözleşmelerin nasıl yapılması gerektiğini ifade edebilecek,
- Sözleşme taraflarının nasıl korunacağını açıklayabilecek,
- İnternet’te yeni reklam imkânlarını ifade edebilecek,
- Haksız rekabetin yeni formlarını sıralayabilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Öneri
- Kabul
- İrade Açıklamaları
- Hata-Hile
- Sözleşmeden Dönme
- Tarafların Korunması
- Tüketici
- Mesafeli Satım
- Cayma
- Sipariş
- Hata
- Senet
- Belge
- Elektronik İmza
- Spam

İçindekiler



E-Ticaret

ELEKTRONİK ORTAMDA SÖZLEŞMELER

Genel Olarak Elektronik Sözleşmeler

İnsanoğlunun var olduğu günden bu yana hayatını devam ettirmek için yaptığı ilk işlemlerin **sözleşme** olduğu kabul edilir. Sözleşme kavramı öylesine derin ve güçlü bir anlamı 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.

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. İnternette 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.

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 derecellemek 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.

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.

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 bi rev kiralamamız ya da bir konser bileti satın almamız da bir sözleşmedir.

Neden elektronik ortamda sözleşme?

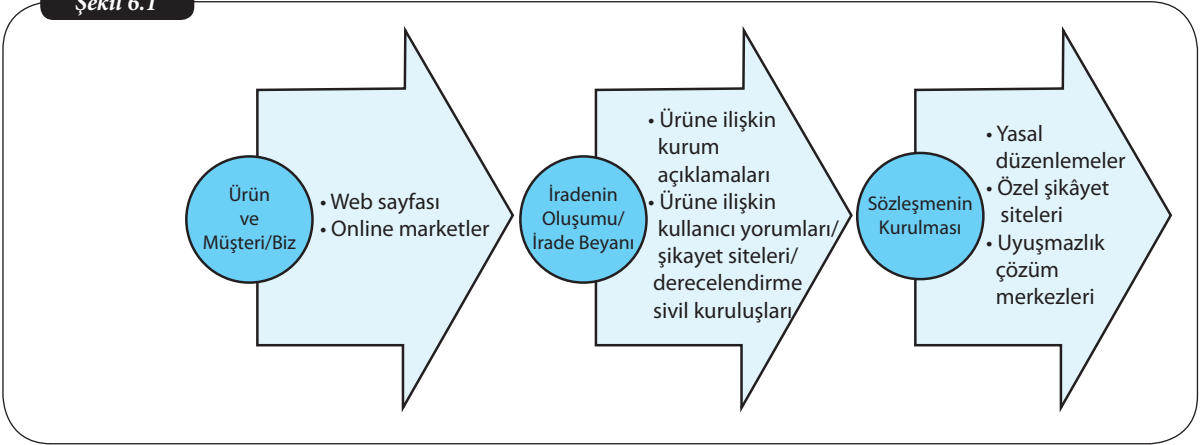
- 1) zamandan tasarruf
- 2) kolay karşılaştırma
- 3) mal ve hizmetlere kolay ulaşım
- 4) mesafelerin engel olmaktan çıkması
- 5) ve diğer bir çok neden...

Nitekim, Türkiye'de e-ticaret hacminin yıllara göre büyüme oranları:

2009-2010: %40,61,
2010-2011: %46,32,
2011-2012: %34,35,
2012-2013: %37,44,
2013-2014: %35

E-Sözleşme: Taraf iradelerinin elektronik ortamda yani yüz yüze gelmeksizin karşılaştığı ve uyduğu 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, vaad 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

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 dönebilmeye 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.

Şekil 6.2

Elektronik ortamda yapılan sözleşmelerin yasal çerçevesi



Sözleşmelerin Kurulmasında İrade Açıklamaları

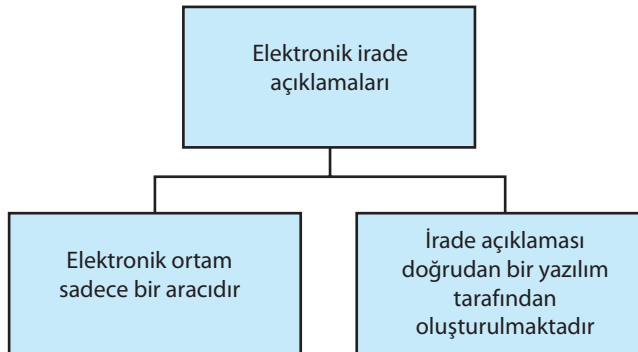
Genel Olarak

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 araçtır. 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 araçtır. 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 'elektronik 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 Language Standart (HTML) ve Hper 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.

Belirli olmayan kişilere yapılan öneri.

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 ayırım 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. İnternet 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 du-

rumlar 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 iletişimidir. 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 hâlde 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 canlandırılabilmesine 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.

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 görecektir. 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 öğretilerde 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 yaygınlaş-

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

ması 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 ayırım 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 yüz yüze 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 yönlendirilmesini 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 mauseun 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 Şekil

Şekil Serbestisi

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 resmi 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 yapılması 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 uyarılmanın yapılması mümkündür. Uyarılmanın 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.

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, gayrimenkul 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 koymasındır (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

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

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 resmi 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 üretilmemektedir. 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 problemidir. 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

HMK m. 199: 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.

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.

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.

Bu problemin önemini burada özellikle vurgulamak istiyorum. 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

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.

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 güven-sizliğin 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 bulunmakta 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 yapıp 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 eden 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 imzalanırsa 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

Genel Olarak

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

Tüketicinin Korunması İhtiyacı

İnternetle birlikte tüketicilerin korunması özel bir önem kazanmıştır. Mal ve hizmet sürümünün İnternette 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, vaad 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 problemlidir. 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 ayrım yapmak 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 ettiği. Şayet tüketici Türkiye içinde ikâmet etmekte ise sorun tüketici açısından daha kolay çözülebilmektedir. Fakat Türkiye dışında bir satıcı ile işlem yapan tüketicinin haklarının korunması 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.

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.

Satıcı ya da sağlayıcı, sipariştten 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 aşılar 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 sonuza kadar da devam etmez, her hâlükârda cayma hakkının bittiği ilk 14 günlük süreden bir yıl sonra sona erer.

Tüketicinin cayma hakkını kullanacağı sürede malın mutlak 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 hesaplanmıyor ise buna ilişkin ek ödeme çıkabileceği uyarı, ilave maliyetler, şikâyetlerin çözüm yöntemleri, cayma hakkının varlığında bunun kullanım usulü, cayma hakkının kulla-

TKHK m.28/1: Mesafeli sözleşme, 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.

TKHK m.3: Sağlayıcı: 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.

nilmadığı 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

Genel Olarak

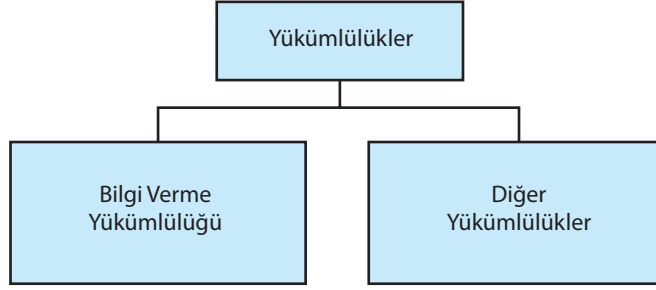
Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (ETK), genel itibarıyla bugüne kadar Türk hukukunda düzenlenmemiş alanları ele alıp düzenlemiştir. Kanun'un asıl amacı, elektronik ortamda icra edilen ticarete ve sözleşmelere güvenin sağlanmasıdır. Kanun koyucunun temel düşüncesi, güvenin sağlandığı hâllerde 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 taraflardan 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



ETK m.2/ç; Hizmet Sağlayıcı: Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişileri... ifade eder.

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 uyumsuzluk çözüm mekanizmalarına ilişkin bilgileri sunar. Yine hizmet sağlayıcı, varsa mensubu olduğu meslek odası ile meslekle ilgili davranış kurallarını ve bunlara elektronik olarak ne şekilde ulaşabileceğini belirtir (m.3).

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).

ELEKTRONİK ORTAMDA REKLAMLAR

İnternet Reklamlarının Avantajları

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.

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 teknikleridir.

Araştırmalara göre televizyonun 13 yılda, radyonun 38 yılda geçirdiği aşamayı İnternet sadece 5 yılda geçirmiş ve bir reklam mecrası olmayı başarmıştır.

Pazarlama, mal, hizmet ya da ürün ve fikirlerin üreticilerden tüketicilere ulaştırılması ve tüketici ihtiyacı 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 mecra olmaması, İnternet mecrasında vardır. Maliyetler diğer mecralara göre son derece ucuzdur ve reklamın etkisi bu mecra da 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.

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 teknolojiye ve teknolojinin yakınsaması nedeniyle karşımıza yeni dönemlerde çıkacak yeni reklam türlerine hazırlıklı olmalıyız.

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. 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. (Vikipedi).

Yakınsama, tek bir cihazda birden fazla teknolojik cihazın işlevlerinin birleştirilmesidir. Örneğin cep telefonunda televizyon, radyo ve bilgisayarın birleştirilmesi gibi.

Elektronik Ortamdaki Reklamlara İlişkin Hukuki Düzenlemeler

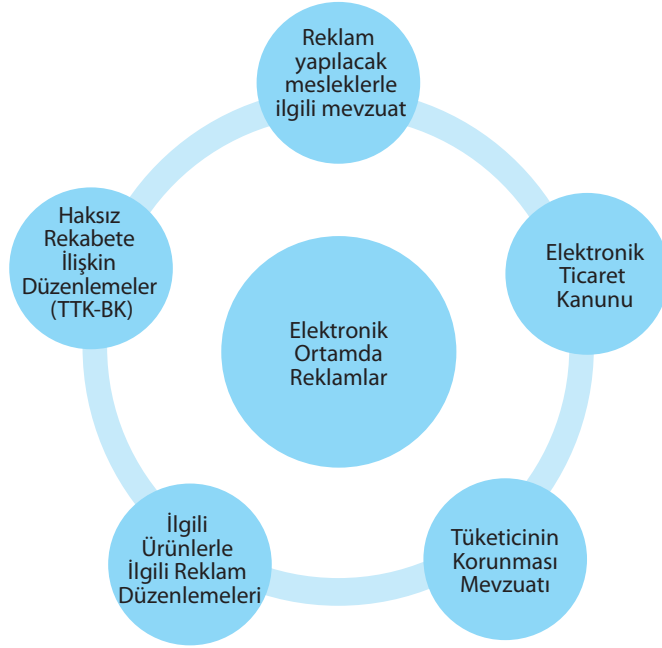
Elektronik Ortamdaki Reklamların Hukuki Çerçevesi

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 mecra ya 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:

- Reklamların aldatıcı, yanıltıcı ve haksız rekabete yol açar nitelikte olmaması,
- Karşılaştırmalı reklam yapılıyor ise karşılaştırılan ürünlerin aynı nitelikte olması ve müşteriye yarar karşılaştırmaların yapılması, karşılaştırılan hususların ölçülebilir olması,
- Reklamı yapılan mal ve hizmetlerin toplam bedeli hakkında yanıltıcı bilgilerin verilmemesi,
- Sayısal verilere dayanan reklam unsurlarının bilimsel test ve raporlara dayanması,
- Rakiplerin kötülenmemesi, karalanmaması,
- Rakiplerin itibarından haksız yararlanmaya yol açılmaması,
- Örtülü reklamlarla bilinçaltı reklamların yapılmaması,
- Çocuklara yönelik reklamlarda onların zihni durumlarını sömürecek, onları gerçek dışı beklentilere ya da şiddete itecek reklamlara yer verilmemesi,
- Kişisel hesaplarına istenmeyen reklam içeriklerinin gönderilmemesi,
- Kişisel verileri esas alan reklamlarda ilgisinden izin alınması,

- k. Bir başkasına ait fikri ya da sınai hakkın kullanımına riayet etmek,
- l. Ayrımcı, aşağılayıcı ya da saldırgan ifadelerle 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 yanıtılması endişesidir.

Normal mesleki hayatlarında reklam yaşağına 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 yaşağına 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 yaşağı getirilmiştir. Bu yaşağın amacı, tüketicinin zarar görmesinin engellenmesidir. İspençiyari ve Tibbi Müstahzarlar Kanunu'nun 13. maddesine göre ilaçların övülmesi veya aslında sahip olunmayan özellikleri ile reklamının yapılması yasaklanmıştır. Sadece tıpla ilgili dergilerde reklama izin verilmiştir.

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

İzinsiz Elektronik Postalar

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.

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 gerekçeyle 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 Gümrük ve Ticaret Bakanlığı özel bir sistemi devreye sokmuştur: <http://tiss.gtb.gov.tr/gtb/giris.xhtml>

SIRA SİZDE



Ticari elektronik postalar hakkında bilgi veriniz.

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 verdiği için, reklamların kaçınıcı 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 faydalandığı, 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 hükmeye 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 aşîkârdır. 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 kullanılabilir.

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.

ELEKTRONİK ORTAMDA HAKSIZ REKABET

Genel Olarak

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 arzulan 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 görünümelerini 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 görünümü 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

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.

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.muhasibe.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.

İnternet Alan Adları Yönetmeliği m. 3: İnternet üzerinde bulunan bilgisayar veya İnternet sitelerinin adresini belirlemek için kullanılan İnternet protokol adresini tanımlayan adları... ifade eder.

Frankfurt Temyiz Mahkemesinin bu kararının sorunun tartışılmasında merkezî bir yere sahiptir. Öncelikle alan ismi olarak seçilen bir isim teknik olarak sadece bir kez kullanılabilir. 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 "rechtsanwalte-koeln.de" (avukatlık bürosu-koeln.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 Könlü 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 tek el oluşturma bir değişik görünümü olarak değerlendirmiş ve iktisadi rekabetin her türlü kötüye kullanımını 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.

Alan isminin stoklandığı nasıl ispat edilecektir? ICANN'ın iyi niyete aykırı bir şekilde tescil edilen bir alan isminin varlığını tesbitte koymuş olduğu kriterlerden faydalanılabilir¹:

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),

¹ www.icann.org/udrp/udrp-poly.24oct99.htm.

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.

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 teknikte 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) manipüle 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.

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.

Bilgisayara yüklenen programlar yolu ile normal İnternet bağlantısını kopararak daha pahalı programlara aktaran yazılımlara verilen isimdir.

Başlık Tekniği (Meta-Tag)

Browserlerin hazırlanan sayfaya yönlenebilmesi için arama mekanizmalarının meta-tagging denilen bir yöntemle manipüle edilmesi gerekmektedir. Danimarka mahkemesi, bir kararında Melitta Grubu'nu arayan İnternet kullanıcılarının, meta-tagging 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 Canon ürünlerini satıyoruz. Siemens ürünleri de iyi olmasına karşın bunları satmıyoruz", şeklinde bir ibareyi web sayfasında kullanmıştır. Arama motorlarına "Siemens" 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 Siemens müşterilerini yanlış yönlendirebilmekte ve uyumsuzluklara sebep olabilmektedir.

Arama motorlarının taradığı başlık tekniği.

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 açılmaz. 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 açılmaz; 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 ölçsüz bir tedbir olurdu.

Özet

Sözleşmenin kurulması için gerekli irade açıklamaları, irade açıklamalarının sonuçları, irade açıklamalarından dönembilme 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 araçtır. 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 si-

parişinin 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, sipariştten 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 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 uyumsuzluk çözüm mekanizmalarına ilişkin bilgileri sunar.

Kendimizi Sıyalım

1. Elektronik irade açıklaması ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

- İnternette yapılan açıklamayı ifade eder.
- Bir icaba davet şeklindedir.
- Bir bilgisayar yazılımı yolu ile yapılan icap ve kabul-leri ifade eder.
- Karşı tarafa varması gerekli bir icaptır.
- Bu tür öneri ve kabullerle bağlı olunmaz.

2. Ürün ve fiyatların da belirtildiği web sayfaları ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

- Öneridir.
- Herkese açık bir öneridir.
- Kabuldür.
- Bir irade açıklaması olarak değerlendirilemez.
- Sadece bir reklamdır.

3. Aşağıda sayılan sözleşmelerden hangisi elektronik ortamda yapılabilir?

- Gayrimenkulün devrine ilişkin sözleşme
- Evlilik sözleşmesi
- Resmî şekil şartına tabi sözleşmeler
- Bütün sözleşmeler
- Şekle bağlı olmayan sözleşmeler

4. Elektronik ortamda yazılı şekil şartına tabi tutulan bir sözleşmenin yapılabilmesi için aşağıdakilerden hangisi gerekir?

- Tarafların ayrıca kağıt ortamında da sözleşmeyi yapması
- Tarafların tanık göstermesi
- Tarafların yemin beyanında bulunması
- Elektronik imza ile sözleşmeyi imzalamaları
- Güvenli elektronik imza ile sözleşmeyi imzalamaları

- Bu sözleşme geçerli olur.
- Taraflarca inkâr edilemez.
- İspat problemi yaşanmaz.
- Geçerliliği için elektronik imza ile imzalanması da gerekir.
- Bu sözleşmeye dair elektronik ortamdaki veriler belge sayılır.

Elektronik ortamda yapılan şekil şartına tabi olmayan bir sözleşme ile ilgili yukarıdaki ifadelerden hangisi doğrudur?

- I ve II
- I ve IV
- I ve V
- II ve III
- 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?

- Sözleşmenin geçerliliğini sağlar.
- Sözleşmenin damga vergisine tabi olmasını gerektirir.
- Sözleşmenin yazılı şekil şartına tabi olduğunu gösterir.
- Borcun ispatını sağlar.
- Borca ilişkin tanık dinleme imkânını verir.

7. Elektronik ortamda kurulan sözleşmelerle ilgili aşağıdaki ifadelerden hangisi doğrudur?

- E-posta yolu ile sözleşme kurulamaz.
- E-posta karşı tarafa ulaşsa bile öneriden dönülebilir.
- Elektronik ortamda irade açıklamasında bulunanların irade açıklamasında hata kabul edilemez.
- Sözleşmelerin kurulmasında teknik hatalara kullanıcı katlanır.
- Bilişim sisteminde sadece ekrandaki teklifin belli bir zaman içinde reddedilmemesi irade açıklaması olarak kabul edilemez.

8. Mesafeli sözleşmelerin kurulmasında cayma hakkı kaç gündür?

- 1 hafta
- 8 gün
- 14 gün
- 1 ay
- 1 yıl

9. Tüketici mesafeli sözleşmelerde cayma hakkı konusunda bilgilendirilmezse bunun sonucu aşağıdakilerden hangisidir?

- Satıcı idari para cezası ile cezalandırılır.
- Cayma hakkını 1 yıl içinde kullanabilir.
- Cayma hakkı verilmemiş olur.
- Satım sözleşmesi geçersiz olur.
- Satım sözleşmesindeki aleyhe şartlar geçersiz olur.

10. Elektronik ortamdaki reklamlar ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?

- Reklamların aldatıcı, yanıltıcı ve haksız rekabete yol açar nitelikte olmamalıdır.
- Reklamı yapılan mal ve hizmetlerin toplam bedeli hakkında yanıltıcı bilgilerin verilmemelidir.
- Bir web sayfasında kesintisiz reklam yapılmamalıdır.
- Rakiplerin kötülenmemeli, karalanmamalıdır.
- Rakiplerin itibarından haksız yararlanmaya yol açılmamalıdır.

Kendimizi Sınyalım Yanıt Anahtarı

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.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Reklam yasağı uygulanan mal ve hizmetler arasında alkollü içecekleri, tütün mamüllerini ve ilaçları sayabiliriz. Ayrıca tıp sektöründe (hekimlik) de bu yasak geçerlidir.

Sıra Sizde 2

Esnaf ve tacirlerin ilk e-posta gönderimi serbesttir. E-posta almayı red üç iş günü içinde uygulanmalıdır. Önceden izin verilmiş e-postalar sonradan reddedilebilir. Ayrıca izinsiz ticari e-postalar için idari para cezası öngörülmüştür.

Yararlanılan Kaynaklar

- Acar, F.: Uzağa Satış Sözleşmesi Yapımında Tüketicinin Korunması Hakkındaki Avrupa Topluluğu Direktifi (Die neue Richtlinie 97/7/EG), İstanbul Barosu Dergisi, C. 74, S. 1, 2000
- Afra, S.: Dijital Pazarın ortak Noktası E-Ticaret: Dünyada Türkiye'nin Yeri, Mevcut Durum ve Geleceğe Yönelik Adımlar, Tüsiad, İstanbul 2004 (bkz. http://www.tusiad.org/_rsc/shared/file/eTicaretRaporu-062014.pdf).
- Arkan, S.: Marka Hukuku, C.II, Ankara 1998
- Arslanlı, H.: Kara Ticareti Hukuku Dersleri, Umumi Hükümler, İstanbul 1960
- Ayhan, R.: Haksız Rekabet Münasebetiyle Elde Edilen Menfaatin İadesi, Konya 1990
- Bettinger, T.: Kennzeichenrecht im Cyberspace: Der Kampf um die Domain-Namen, GRUR-Int 1997, H.5,
- Bettinger, T.: Kennzeichenrecht im Cyberspace: Der Kampf um die Domain-Namen, GRUR-Int 1997, H.5
- Bielfeldt, M./Slink, T./Pernice, M./Rappelmund, H./Scheinpflug, J.: Electronic Commerce, 2. Aufl. Berlin 2000
- Bugiel, A.: Rechtliche Rahmen des E-Commerce in Deutschland und Europa, TOBB, 11, 12 Mayıs 2000,
- Demir, M.: Mesafeli Sözleşmelerin İnternet Üzerinden Kurulması, Ankara 2004
- Eichhorn, B.: "İnternet-Recht, Ein Lehrbuch für das Recht im World Wide Web", Köln 2000
- Eichhorn, B.: Internet-Recht, Ein Lehrbuch für das Recht im World-Wide-Web, Köln 2000, s. 16 vd.
- Fikentscher, W./Möllers, M.J.T.: "Die (negative) Informationsfreiheit als Grenze von Werbung und Kunstdarbietung", NJW, 1998/18
- Fröhlich, M.: "Zentrale Institutionen des deutschen Urheberrechts und französischen Droit d'auteur auf dem Prüfstand der elektronischen Netzwerke", Frankfurt am Main 2001
- Funk, A.: "Wettbewerbliche Grenzen von Werbung per E-Mail", CR, 1998/7
- Göle, C.: Ticaret Hukuku Açısından Aldatıcı Reklamlara Karşı Tüketicinin Korunması, Ankara 1983
- Halbscheid, W.J.: Schweizerisches Zivilprozes –und Gerichtsorganisationsrecht, 2. Aufl. Basel/Frankfurt. A Main, 1988
- Hanika, H.: "Internetrecht versus Schutz der öffentlichen Gesundheit und Standesrecht", MedR 2000, Heft 5
- Heun, S. E.: Die Elektronische Willenserklärung, CR. 1994
- Hoeren, T.: "Cybermannes und Wettbewerbsrecht-Einige Überlegungen zum Lauterkeitsrecht im Internet", WRP, 1997/11
- Hoeren, T.: "Werberecht im Internet am Beispiel der ICC Guidelines on Interactive Marketing Communications", Internet und Multimediarecht (Cyberlaw) (Hrsg. Lehmann, M.) Stuttgart 1997
- İmre, Z.: Şahsiyet Hakkının Korunmasına İlişkin Genel Esaslar, Özellikle İsim Hakkı ve isim Hakkının Korunması, A. Recai Seçkin'e Armağan, Ankara 1974
- İnal, E.: E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması, İstanbul 2005
- Jaeger-Lenz, A.: Werberecht-Recht der Werbung in Internet, Film, Funk und Printmedien, Weinheim 1999
- Karayalçın, Y.: Ticaret Hukuku, C.1, Giriş-Ticari İşletme, Ankara 1968
- Kolb, A.: "Cyberethik: Verantwortung in einer digital vernetzten Welt", World Congress Safety of Modern Technikal Systems, Saarbrücken 2001
- Körner, R./Lehment, C.: "Allgemeine Wettbewerbsrecht", (Hoeren, T./ Sieber, U.: Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs", München 1999)
- Ladeur, K.: "Neue Werbeformen und der Grundsatz der Trennung von Werbung und Programm, Virtuelle Werbung, Split Screen und Vernetzung von Medien als Herausforderung der Rundfunkregulierung, ZUM 1999/10
- Laga, G.: Internet im rechtsfreien Raum?, Dissertation, Wien 1998, Geschichte, s. 10 vd.
- Lettl, T.: "Rechtsfragen des Direktmarketings per Telefon und E-Mail", GRUR, 2000
- Leupold, A.: "Die massenweise Versendung von Werbe-e-Mails: Innovatives Direktmarketing oder unzumutbare Belaestigung des Empfängers" WRP, 1998/3
- Maibach, M.C.: "The Internet: The Great Equalizer", Economic Reform Today, Number 2, 1999
- Mankowski, P.: Besondere Formen von Wettbewerbsverstößen im Internet und Internationales Wettbewerbsrecht, GRUR Int. 1999
- Mayer, F.C.: "Recht und Cyberspace", NJW 1996, Heft 28, s. 1782.
- Mehner, A.: "Wettbewerbliche Bewertung geschäftlicher Aktivitäten im Internet und in sonstigen Online Plattform", Cyberlaw (Hrg. Schwerdtfeger/Everyz/Kruezer/Peschel-Mehner/Poeck) Weisbaden 1999
- Müko/Kramer, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1 3. Aufl. 1993
- Naumann, T.: "Präsentationen im Internet als Verstoß gegen §§ 1, 3 UWG, Unter besonderer Berücksichtigung der Online-Angebote von Rechtsanwälten", Frankfurt am Main, 2001

- Özdemir, H.: Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara 2009
- Öztekin, S.: “Haksız Rekabete İlişkin Yeni İsviçre Düzenlemesinin Öngördüğü Bazı Haksız Rekabet Halleri”, Prof. Dr. Jale G. Akipek’e Armağan, Konya 1991.
- Palant/Heinrichs, Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Kommentar, 55. Aufl. 1996
- Peschel-Mehner, A.: “Wettbewerbsrechtlicher Bewertung geschäftlicher Aktivitäten im Internet und in sonstigen Online-Plattform”, (Schwerdtfeger/Evertz/Kreuzer/Peschel-Mehner/Poeck: “Cyberlaw”, Wiesbaden 1999)
- Reich, N.: Die Neue Richtlinie 97/7/EG über den Verbraucherschutz bei Vertragsschlüssen im Fernabsatz, EuZW, Heft 19/97
- Reichelsdorfer, J.: “eMails zu Werbezwecken-ein Wettbewerbsstoss?”, GRUR, 1997
- Rosenthal, D.: “Unverlangte Werbe E-Mail ohne Rechtsfolgen?” MediaLEX, 1999/4
- Rosenthal, D.: “Unverlangte Werbe E-Mail ohne Rechtsfolgen”, Media Lex, 4/99
- Rüßmann, H.: “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.: İnternet Üzerinden Akdedilen Sözleşmeler, Ankara 2008
- Schneider, J.: Handbuch des EDV-Rechts, 2. Aufl. München 1997
- Schwarz, M.: Merkmale, Entwicklungstendenzen und Problemstellungen des Internet, http://www.jura.uni-muenchen.de/Institute/Internet_I.html,
- Taşkın, A.: Tüzel Kişilerin Kişilik Haklarının Korunması, AÜHFD., C. 42, 1991-1992
- Vehslage, T.: “Auswirkungen der Fernabsatzrichtlinie auf die Telefon- und E-Mail-Werbung”, GRUR 1999, H. 8/9
- Von Herget, H./Reimer, M.: Rechtsformen und Inhalte von Verträgen im Online-Bereich, DStR 1996
- Wattel, J.: “Le problème du Spamming ou comment guérir le cancer de l’internet”, Jurpc Web-Dok. 163/2001, (www.jurpc.de).
- Weber, R. H.: “Internet als Subventionsnetz? Wettbewerbsrechtliche Rahmenbedingungen von Internet-Dienstleistungsangeboten durch öffentlich kontrollierte “Einheiten” CR1997
- Yasaman, H.: Tanınmış Markalar, Halil Arslanlı’nın Anısına Armağan, İstanbul 1978
- Ziem, C.: “Spamming, Zulaessigkeit nach § 1 UWG, Fernabsatzrichtlinie und E-Commerce Richtlinienentwurf”, MMR 2000/3, s. 131 vd.; Schrick, A.: “Direktmarketing mittels E-Mail und seine Entwicklung”, MMR 2000/7

7

Amaçlarımız

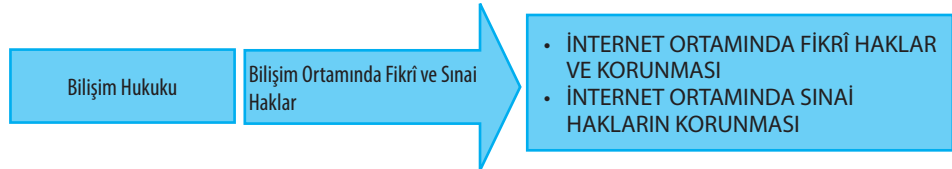
Bu üniteyi tamamladıktan sonra;

- Fikrî ve sınai hakların korunması konusunda İnternet’te ne tür özelliklerin olduğunu açıklayabilecek,
- İhlallerin nasıl niteleneceği ifade edebilecek,
- İhlallerin en kısa nasıl ortadan kaldırılacağını ifade edebilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Eser Türleri
- Dijitalleşme
- Eser Sahibinin Hakları
- Multimedya
- Meta-tag
- Adwords
- Alan Adı
- Alan Adı Stoklama
- Yarışan Haklar
- Önce Gelen Önce Alır
- P2P-filessharing
- Mp3
- DivX
- Senkron-asenkron

İçindekiler



Bilişim Ortamında Fikrî ve Sınai Haklar

İNTERNET ORTAMINDA FİKRÎ HAKLAR VE KORUNMASI

Giriş ve İlgili Mevzuat

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 yayınlatabilme 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 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

İnternet'te Eserlerin Yer Alma Türleri

İnternette telif haklarının korunması 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 Management 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 olmadığı 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 ayırım 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 farklı zamanlarda sunulanlara erişme ve onları tüketme imkânına sahiptir.

	Çevrimiçi	Çevrimdışı
Senkron	Radyo, televizyon	-----
Asenkron	İnternette web sayfasının çağırılması	Veri taşıyıcılarla kullanım (CD, DVD)

Tablo 7.1
Multimedya Kullanımının
Tasnifi

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

Genel Olarak

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, eserin işlenmesi, çoğaltılması ve yayınlaması 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

Bağlantı (Link)

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 yapılabilir. 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 hyper-link, web sayfasından internet kullanıcıını, 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, de-eplinks, 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 diğerkimsenin 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 diğersayfaya ulaşmaktadır. Bu, doğrudan diğersitesinin ana sayfası olabileceği gibi, o site içinde bulunan bir diğersayfa 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 serveri meşgul edilmeksizin kullanılmaktadır. Bu tür linkler, bir eserin sahibinin link veren kimse olduğu görünümü verilerek kötüye kullanılabilir.

Çerçeve (Frame)

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 çekişme 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 itibarıyla 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

Genel Olarak

Link ve frame verilmesinde ortaya çıkacak sorunlara genel bir bakıştan önce link türleri arasında başlangıçta bir ayırım 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 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 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 bir takım haklarından bahsetmek mümkündür. Zira bu link türünde link verilen sayfa (eser) bağımsız bir sayfa olarak açılmamakta, link veren sayfanın içinde görüntülenmekte; link veren sayfanın adeta bir parçası görünümü verilmektedir. Bu durumda eser sahibinin korunmaya değer menfaatlerinden bahsetmek gerekmektedir. Öncelikle eser sahibinin manevi haklarından adının belirtilmesi hakkının çiğnenmesi söz konusu olabilir (FSEK m. 15).

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 kullanılabilir. 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 bulunmak-

tadır. Eser sahibinin eserinde zorunlu hallerde değişiklik yapılabilir. 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 kullanılabilir ve miras yolu ile intikale yahut üçüncü şahıslara devredilmeye elverişli bulunmamaktadır.

Normal olarak hangi tür olursa olsun linklerde ve frameelerde eserin değiştirilmesi sözü konusu değildir. Ancak bazı hallerde eserin belirli bir parçasının frame ve dahili linklerle bir başka sayfaya bitleştirilmesi halinde eser sahibinin eserinin bütünü veya parçasında belirli bir değişiklik yapıldığının kabul edilmesi gerekmektedir.

Mali Haklar

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 işleme sayılmaz. Bir roman veya hikâyenin kısaltılması, bir tablodan belirli bir kısmın çıkarılması, senaryonun rejisör tarafından kısaltılması birer işleme 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 işleme eserin varlığından bahsetmek mümkün olmayacaktır. Mesela bir tablonun değişik ışıklandırılmalar altında sergilenmesi gibi. Esere bir başka buut kazandırılması durumlarında da işleme eser mevcut değildir. Bir müzik parçasına yeni bir güftenin yazılması da işleme eser olarak kabul edilemez. Böyle bir durumda eserin metni değişmemekte, ilave ve ikame bir metin daha esere bitleştirilmektedir. Burada işleme 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 işleme 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 frameelerde 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 frameyi veren kimsenin eylemi olarak düşünülmelidir.

Amerikâda 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 bir çok 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 framerde 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.

Almanyada 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 framerde çoğaltma hakkının ihlal edilmediği sonucuna varılmalıdır. Ancak kullanıcı tarafından hangi sayfanın link ve frame sonucu kullanıldığı bilinmiyorsa 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 serverinde meydana gelmesi 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 framer 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.

SIRA SİZDE



Eser sahibinin manevi ve mali hakları nelerdir?

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 Milneum Copyright Act'a da aykırı bulunmuştur. DMCA bölüm 1201 (a) (2) hükmü, fikri 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 serveri 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 itibarıyla 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 subjektif şartın yerine gelmesi gerekir. Eserin sahibinin hususiyetini taşıması, subjektif 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 multimedia 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 bulundurdıkları münferit unsurlarına ayrılarak pekala 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 kullanılmışsa 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 kul-

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.

lanıcının 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.

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

Genel Olarak

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 Fraunhofer 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 değişmemekte, 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 kullanıcıları olacağı tahmin edilmektedir. Böylece dünya adeta her gün genişleyen bir dijital müzik kütüphanesine dönüşmektedir.

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 haklarından (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 imkanı 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 ta-

Müzik alanında ihlalin boyutlarına örnekler vermek gerekirse:

- Arama motorlarında en fazla aranan kavram "Mp3" kavramıdır, hatta "sex" kavramını dahi geçmiş ve onu ikinci sıraya itmiştir.
- Bugün net rakamlar bilinmemekle birlikte 1988 yılında 30 ayrı ülkede 2 binin üzerinde sitede 200 bin müzik parçası sunulmuştur. IFPI'nin son rakamlarına göre illegal müzik sunumu yapan 700 bin web sayfası bulunmaktadır.
- IFPI'ye göre bir güne 1 milyon 100 bin müzik verisi serverlerden 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.

nımlanmaktadır. 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 Kaza'a'yı ilişkindir.

Napster, merkezi serveri olan ve kullanıcılarına müzik değişim imkanı 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 bulunduğu 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 Kaza'a'ya karşı Hollanda'da dava açılmıştır. Hollandalı Hâkim, müzik değişim platformu olan Kaza'a'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 Kaza'a, günlük 40 bin-80 bin dolar ceza ödemek zorunda kalacaktır.

Kaza'a, bu karara karşı temyize gitmiş ve temyiz merciinde verilen kararda hem ihtiyati tedbir kararı kaldırılmış hem de Kaza'a'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 paylaşılabilir. Yine değişik internet platformlarında da sadece müzik, video, film ya da fotoğraf paylaşılabilir.

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.

Örneğin: Facebook, Youtube, Instagram vb.

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 bir çok 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 hakim 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.

İNTERNET ORTAMINDA SINAI HAKLARIN KORUNMASI

Genel Olarak

Bilişim sistemlerinde sinai 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

Alan Adı Sistemi

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 yazdığı anda 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 nitelenmesi 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

yardımla 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 kullanılabilir. 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 kullanılabilir. 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 ad’larına 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 iddiası.” 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

Tescilli Markaların Alan İsmi Olarak Seçilmesi

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. Örneğin; www.nestle.com adresi altında reklam edilen malların İsviçre Nestle Ortaklığına ait olduğunu düşünebilmektedir. 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 Hükümünde 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 çağrıştırmacı işaretlerin kullanılması hallerinde söz konusu olmaktadır. Markanın aynen alan ismi olarak kullanımı ne anlama gelmektedir? Markalar esas ve yardımcı unsurlar olmak üzere iki kısımdan oluşmaktadır. 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 kullanıldığına tespitinde esas unsuru teşkil eden şekil veya kelimenin aynının veya benzerinin kullanımı dikkate alınır. Esas unsuru teşkil eden şekil ve kelimelere yapılacak cüz'î 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 karşılaşmaktadır. 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 tesbitinde kullanılan ölçünün müşteri kitlesinin yanılgıya 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 yanılgıya 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 kullanılabilir. Fakat farklı iş kollarında faaliyet gösterecekler 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 harfli 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 yanıltma 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 kişiler 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 yanıltmayı 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 bulunmasına 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 imkanı 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 uzantsız 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 bir çok kişi ve kuruluş haksız yere başkalarının 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 Kanununda 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 bir çok 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 kapsamaması 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-tagging denilen bir yöntemle manipüle edilmesi gerekmektedir. Bu manipüle, 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 kullanımıdır.

Gerek meta-tag kullanımı, gerekse adwords reklam yolu ile marka sahibi dışında bir kullanım marka ihlalidir (MarKHK.m.9).

Webde yayınlanan bilgiyi aramak için kullanılan bir yazılım paketi; en çok kullanılan Microsoft Internet Explorer ve Netscape’dir.

Bu konular için bkz. 6. Ünite.

Keyword advertising, bir üst kavram olarak adwords ve adsense reklamlarını da kapsayan, başta Google olmak üzere, Yahoo ve Microsoft gibi önde gelen arama motorlarında kullanılan, arama içeriğine bağlı, anahtar sözcüklerle yapılan reklam sistemini ifade etmektedir.

Özet

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 yayınlatabilme 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 sahibinin hakları ve haklarının korunması bakımından eserin bilişim ortamına taşınması, uygulanacak olan kuraları değiştirmez. Eser sahibi, eseri üzerinde eserinin umuma arz edilmesi, eserinde değişiklik yapılması, eserinin işlenmesi, çoğaltılması ve yayımlanması konusunda münhasıran hak sahibidir. Eser sahibine Kanun ile tanınan bu haklar, eserin elektronik ortamda kullanılması hâlinde de aynen geçerlidir. 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 kullanılabilir 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 tabloda 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, nakil sonucuna ise yine ortada bir işlenme eserin varlığından bahsetmek mümkün olmayacaktır. Mesela bir tablonun değişik ışıklandırılmaları 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 bitştirilmektedir. 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.

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. fıkra da genişletilmiştir: "Eserlerin aslından ikinci bir kopyasının çıkarılması ya da eserin işaret, ses ve görüntü nakil ve tekrarıyla 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.

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 umuma yaralanmasına sunulmasıdır. Umuma arz kavramında önem taşıyan kavram "umum" kavramına yüklenecek anlamdır. Fikir ve Sanat Eserleri Kanunu'muzda umum kavramı tanımlanmamıştır.

Kendimizi Sınavalım

- Aşağıdakilerden hangisi internet teknolojisinin eser sahibi için getirdiği tehlikelerden biridir?
 - Eserlerin hızlı yayılması
 - Eserlerin kopyalanması
 - Dijitalleşme
 - Multimedya olması
 - Arama motorlarından bulunması
- Değişim programlarında bir eserin kullanılması halinde eser sahibi ya da hak sahibinin aşağıdaki haklarından hangisi ihlal edilir?
 - Mali haklarının tümü
 - Manevi haklarının tümü
 - Çoğaltma hakkı, umuma iletim hakkı
 - İşleme hakkı, adın belirtilmesi hakkı
 - Eserde değişiklik yapılmasını men hakkı
- Link tekniği ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?
 - Link, internet kullanıcılarına bir başka içeriği işaret eder.
 - İnternet kullanıcısının bir diğer sayfaya geçişini mümkün kılar.
 - Harici ve dahili link olarak iki kısma ayrılabilir
 - Bir sayfada diğer sayfanın da görüntülenmesini sağlar.
 - Çoğaltmalar kullanıcının bilgisayarında gerçekleşir
- Frame teknolojisi ile ilgili aşağıdaki ifadelerden hangisi doğrudur?
 - Bir sayfadan diğerine geçişi sağlar.
 - İnternet kullanıcısının tek bir sayfasında bir çok işlevi yüklemesini mümkün kılar.
 - Verilerin sıkıştırılmasını sağlar.
 - Verilerin hızlı transferini sağlar.
 - Bir internet sayfasında bir başka sayfanın görüntülenmesini sağlar.
- Değişim programları ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?
 - Merkezi olan ve olmayan değişim programları vardır.
 - Her türlü verinin değişimi mümkündür.
 - Kullanıcının yaptığı fikri ürüne ilişkin değişimler FSEK.m.38 kapsamında yasaldır.
 - Değişimlerde eserin çoğaltılması söz konusudur.
 - Eserlerin umuma iletimi de vardır.
- Paylaşım platformlarının sorumluluğu ile ilgili aşağıdaki ifadelerden hangisi doğrudur?
 - Aracı hizmet sağlayıcı olan paylaşım platformu kural olarak sorumlu değildir.
 - Eser sahiplerinin haklarının ihlalden sorumludur.
 - Eser sahiplerinin hak ihlalleri nedeniyle sitelerinin erişime engellenmesi mümkündür.
 - Eser sahiplerinin platforma koydukları eserleri kontrol yükümlülüğündedir.
 - İhlal teşkil eden eserlere ilişkin tazminat davasının tarafıdır.
- Alan adı ile ilgili aşağıdaki ifadelerden hangisi doğrudur?
 - Alan adı bir markadır.
 - Alan adı bir ticaret unvanıdır.
 - Alan adı bir coğrafi işaretir.
 - Alan adı kendine özgü bir isimdir.
 - Alan adı, sayılardır.
- İnternet alan adının bir başkası tarafından marka olarak tescili halinde aşağıdakilerden hangisi yapılabilir?
 - Marka tesciline öncelik verilir ve marka tescili korunur.
 - Markanın hükümsüzlüğü talep edilir.
 - Marka sahibine tazminat davası açılır.
 - Hem marka hem de alan adı birlikte var olmaya devam eder.
 - Marka sahibi alan adı sahibine markasının korunması için dava açabilir.
- Aşağıdakilerden hangisi marka ihlali **sayılmaz**?
 - Siemens markasının Bosch şirketi tarafından meta-tag olarak kullanımı
 - AEG tarafından Grundig markasının adwords reklamlarda kullanımı
 - Arçelik markasının Profilo olarak alan adı olarak kullanımı
 - Regal markasının bir web sayfasında asıl unsur olarak kullanılması
 - Arçelik tamircisinin, arceliktamircisierkan.com şeklinde bir alan adı alması.
- Bir eserin web sayfasında yayınlanması halinde eser sahibinin yararlanabileceği özel usul aşağıdaki kanunlardan hangisinde bulunur?
 - Türk Ticaret Kanunu
 - Fikir ve Sanat Eserleri Kanunu
 - Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
 - Borçlar Kanunu
 - Elektronik İmza Kanunu

Kendimizi Sınavalım Yanıt Anahtarı

- | | |
|-------|--|
| 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” konusunu yeniden gözden geçiriniz. |

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Eser sahibinin adının belirtilmesi, eserde değişiklik yapılmasını yasaklama hakkı, işleme hakkı, çoğaltma hakkı ve umuma iletim hakkı

Yararlanılan Kaynaklar

- 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.: “Urheberrechtliche Zulaessigkeit privaten Downloadings von Musikdateien”, CR 2001/3
- Bozbel, S.: “Mukayeseli Hukukta ve Türk Hukukunda Karşılaştırmalı Reklam Hukuku”, Ankara 2006
- Burmeister, K.: “Urheberrechtsschutz gegen Framing im Internet- eine rechtsvergleichende Untersuchung des deutschen und US-amerikanischen Urheberrechts”, Köln 2000
- Burmeister, K.: “Urheberrechtsschutz gegen Framing im Internet: eine rechtsvergleichende Untersuchung des deutschen und US-amerikanischen Urheberrechts”, Köln 2000.
- Çabuk, S./Bağcı, M.İ.: “Pazarlamaya Çağdaş Yaklaşım”, İstanbul 2003
- Decker, U.: “Urheberpersönlichkeitsrecht im Internet”, (Hoeren, T./ Sieber, U.: Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschaeftsverkehrs”, München 1999)
- E. M. Haas, Die Französische Rechtsprechung zum Konflikt zwischen Domaninnamen und Kennzeichenrechten, GRUR-Int. 1998, s. 939).
- Eichhorn, B., Internet-Recht, Ein Lehrbuch für das Recht im World-Wide-Web, Köln 2000
- Eichhorn, B.: “Internet-Recht, Ein Lehrbuch für das Recht im World-Wide-Web”, Köln 2000
- Erel, Ş.: “Türk Fikir ve Sanat Hukuku”, Ankara 2009
- Eren, F.: “Borçlar Hukuku Genel Hükümleri” Ankara 2015
- Federrath, H., “Multimediale Inhalte und technischer Urheberrechtsschutz im Internet”, ZUM, 2000
- Fröhlich, M.: “Zentrale Institutionen des deutschen Urheberrechts und des fransözischen Droit d’auteur auf dem Prüfstand der elektronischen Netzwerke”, Frankfurt am Main 2001
- Gabel, D.: “Anmerkung zum Urteil des LG Düsseldorf vom 29.4.1998,” K&R 1988
- Gahrau, E.: “Einleitende Überlegungen”, (Hoeren, T./ Sieber, U.: Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschaeftsverkehrs”, München 1999)
- Hüsch, M.: “Der Gebrauch geschützter Kennzeichen als Advertising Keywords (AdWords)”, K&R 2006, 223 vd.
- Ilde, R.: “Hyperlinks”, www.graefe-partner.de/ecom/hyperlinks.html; Ernst, NJW-CoR
- Junker, M.: “Anwendbares Recht und internationale Zustaendigkeit bei Urheberrechtsverletzungen im Internet”, Kassel 2002

- Karahan, S./Suluk, C./Saraç, T./Nal, T.: Fikri Mülkiyet Hukukunun Esasları, Ankara 2013
- Klett, A.: "Urheberrecht im Internet aus deutscher und amerikanischer Sicht", Baden-Baden 1998
- Kur, A.: Namens- und Kennzeichenschutz im Cyberspace, CR 1996
- Kur, A.: Neue Perspektiven für die Lösung von Domainnamenkonflikten: Der WIPO-Interim Report, GRUR, Int. 1999, Heft 3
- Laga, G.: "Neue Techniken im World Wide Web - Eine Spielwiese für Juristen?", JurPC Web-Dok. 25/1998, Abs. 1 - 50 (www.jurpc.de)
- Lehmann, M., Digitalisierung und UrhR, Internet und Multimediarecht (Cyberlaw), Stuttgart 1997
- Lehmann, M./v. Tucher, T., "Urheberrechtlicher Schutz von multimedialen Webseiten" CR1999,
- Leistner, M./Bettinger, T.: "Immaterialgüterrechtlicher und wettbewerbsrechtlicher Schutz des Web-Designers", CR 1999
- Leupold, A./ Demisch, D.: "Bereithalten von Musikwerken zum Abruf in digitalen Netzen", ZUM 2000, s. 385.
- Mankowski, P.: "Besondere Formen von Wettbewerbsverstößen im Internet und Internationales Wettbewerbsrecht", GRUR Int. 1999, Heft 12, s. 998.
- Memiş, T., Alan İsmi Etrafında Ortaya Çıkan Hukuki Sorunlar, Bilişim Toplumuna Giderken Psikoloji, Sosyoloji ve Hukuka Etkiler Sempozyumu, Ankara 2001.
- Memiş, T.: "İnternette Cins ve Meslek İsimlerinin Alan İsmi Olarak Kullanılması ve Ortaya Çıkan Hukuki Sorunlar", Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, Erzincan 2000, C. VI, S. 1-2.
- Memiş, T.: Fikri Hukuk Bakımından İnternet ortamında Müzik Sunumları, Ankara 2003.
- Memiş, T.: FSEK Değişikliği İle İnternet Ortamında Fikri Hak İhlallerinin Engellenmesi İçin Getirilen Usul" Fikri Mülkiyet Hukuku Dergisi, Sayı 1, 2006.
- Memiş, T./ Bozbel, S.: "Marka Ve Haksız Rekabet Hukuku Bakımından Adwords Reklamlar", E-Akademi Dergisi, Kasım 2008, Sayı 81 (www.e-akademi.org).
- Meyer, S.: „Google & Co. – Aktuelle Rechtsentwicklungen bei Suchmaschinen“, K&R (Kommunikation und Recht), 2007.
- Nordemann, W.: "Urheberrecht, Kommentar zum Urheberrecht und zum Urheberrechtswahrnehmungsgesetz", Stuttgart 1998.
- Öztek, S.: "Haksız Rekabete İlişkin Yeni İsviçre Düzenlemesinin Öngördüğü Bazı Haksız Rekabet Halleri", Jale G. Akipeke Armağan, Konya 1991.
- Peter Mankowski, "Besondere Formen von Wettbewerbsverstößen im Internet und Internationales Wettbewerbsrecht", GRUR Int. 1999.
- Plass, G.: "Hyperlinks im Spannungsfeld von Urheber-, Wettbewerbs- und Haftungsrecht", WRP 2000/6
- Saacke, A., Saacke, Astrid-"Schutzgegenstand und Rechtsinhaberschaft bei Multimediaprodukten-Grundfragen des Rechtsschutzes und der Lizenzierung", in: Götting, Horst-Peter (Editor)-"Multimedia, Internet und Urheberrecht", 1998
- Sabih Arkan, Marka Hukuku, C.II, Ankara 1998.
- Schack, H.: "Urheber- und Urhebervertragsrecht", 2. Aufl. Tübingen 2001.
- Schack, H.: "Urheberrechtliche Gestaltung von Webseiten unter Einsatz von Links und Frames", MMR 2001.
- Schuster, F./Müller, U.: "Entwicklung des Internet- und Multimediarechts von Januar 1999 bis Juni 2000", MMR-Beilage 2000/10.
- Selim Kaniti, "İsviçre Federal Mahkemesinin Markalar Arasında İltibasla İlgili Kararları", Batider 1961, C.II, S.2.
- Sosnitz, O.: "Das Internet im Gravitationsfeld des Rechts: Zur rechtlichen Beurteilung so genannter Deep Links", CR 10/2001.
- Strömer, T. H.: "Online Recht, Rechtsfragen im Internet", 2. Auflage, Heidelberg 1999.
- Tekinalp, Ü.: "Fikri Mülkiyet Hukuku", İstanbul 2012.
- Tekinay, S.S. : "Esas Unsurları Dolayısıyla Koruma Dışı Bırakılan Markalar", Prof. Dr. Yaşar Karayalçın'a Armağan, Ankara 1988____.
- Ünal Tekinalp, "Markanın Üçüncü Kişi Tarafından Kullanılması", Prof.Dr. Selahattin Sulhi Tekinay'ın Hatırasına Armağan, İstanbul 1999.
- Von Bonin, A./Köster O.: "Internet im Lichte neuer Gesetze", ZUM 1997, s. 823.
- Völker, S./Lührig, N.: "Abwehr unerwünschter Inline-Links", K&R 2000/1.
- Zscherpe, Urheberrechtsschutz digitalisierter Werke im Internet, MMR 1998____.

8

Amaçlarımız

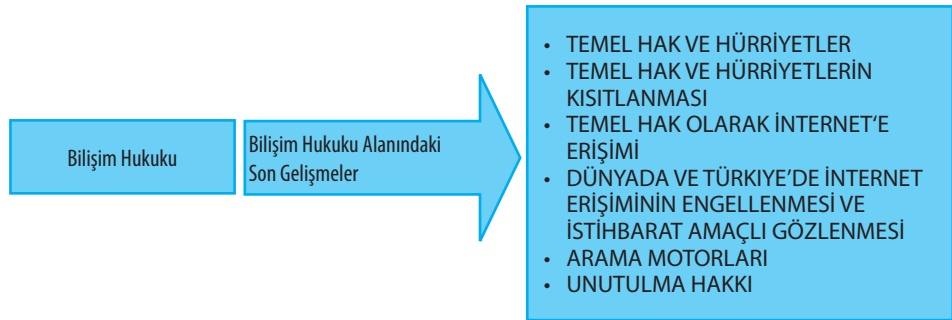
Bu üniteyi tamamladıktan sonra;

- Temel hak ve hürriyetler kavramlarını tanımlayabilecek,
 - Temel hak ve hürriyetlerin kısıtlanması konusunu açıklayabilecek,
 - İnternet'e Erişimi bir temel hak olarak açıklayabilecek,
 - Arama Motorları kavramını açıklayabilecek,
 - Unutulma Hakkını tanımlayabilecek
- bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Temel Haklar ve Hürriyetler
- Temel Hak ve Hürriyetlerin Kısıtlanması
- İnternet'e Erişim Hakkı
- İnternete Erişimin Engellenmesi
- Arama Motorları
- Unutulma Hakkı

İçindekiler



Bilişim Hukuku Alanındaki Son Gelişmeler

TEMEL HAK VE HÜRRİYETLER

Hakkında birçok kaynakta açıklama bulunabilecek temel hak ve hürriyetler, kısaca insan olarak doğmakla elde edilen¹, anayasa tarafından tanınarak güvence altına alınmış ve aynı zamanda devletin temel organlarının yetkilerinin de sınırını oluşturmakla² yasama ve yürütme tarafından keyfi biçimde ortadan kaldırılamayacak olan haklardır.

Temel hak ve hürriyetler sadece Magna Carta³ ile değil farklı medeniyetlerin farklı metinleriyle, insanoğlunun dünya savaşları, soykırımlar, insanlığa karşı işlenmiş yüzlerce suç gibi acı tecrübeleriyle birlikte bin yılı aşkındır süzülerek, rafineleşerek gelen bir anlayış ve farkındalık sonucu İnsan Hakları Evrensel Beyannamesi (“İHEB”)⁴, Avrupa İnsan Hakları Sözleşmesi (“AİHS”)⁵, Avrupa Birliği Temel Haklar Bildirgesi (“ABTHB”)⁶ ve Anayasamızda yer alan, kişinin doğumuyla kazandığı, vazgeçilmez ve feragat edilmez haklardır.

Bu incelememiz bakımından özellikle İnternet’in etkilediği ve İnternet ile birlikte kullanılması çok farklı bir hâl alarak artık İnternet’siz kullanılabilmesi dahi düşünülmemeyen temel hak ve hürriyetlerin bir kısmını düşünce hürriyeti, ifade hürriyeti, basın hürriyeti, eğitim hakkı, gelişim hakkı, iletişim hürriyeti, fırsat eşitliği, kültürel faaliyetlere erişim hakkı, toplanma ve örgütlenme hakkı, mahremiyet ve veri korunması hakları olarak sıralayabiliriz. Temel hak ve hürriyetler bir bütündür ve bu haklar bir arada var olmadıktan, kullanılmadıktan sonra özgürlükten söz edilemez.

Temel hak ve hürriyetler çalışılırken negatif-pozitif⁷, aktif; sosyal, ekonomik, kültürel ya da kuşaksal çeşitli kategorizasyonlar yapıldığı görülse de bu kategorizasyonlar temel hak ve hürriyetlerin önemine veya önceliğine ilişkin bir ayırım değil, kronolojik, akademik ve doktrinsel tanımlama ve açıklama amacıyla yapılan ayrımlardır.

Bizim ana konumuz İnternet ekseninde kalacağından biz de kuşaksal olarak özetle temel hak ve hürriyetleri aşağıdaki şekilde kategorize edebiliriz:

¹ Kapani, Kamu Hürriyetleri, s.20.

² Gözler, Anayasa Hukukunun Temel Teorisi, s.37.

³ British Library, <http://www.bl.uk/magna-carta>

⁴ 10.12.1948, Birleşmiş Milletler Genel Kurulu, <http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=trk>

⁵ 04.11.1950, Avrupa Konseyi, http://www.yargitay.gov.tr/abproje/belge/temelbelge/AIHS_Tr_A6format.pdf

⁶ 02.10.2009Lizbon Anlaşması, <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2007:303:TOC>

⁷ Jellinek, c.II, s.51-57

Birinci kuşak haklar: Vücut bütünlüğü ve yaşam güvenliği, konut dokunulmazlığı, düşünce hürriyeti, siyasal haklar.

İkinci kuşak haklar: Çalışma ve hayatını idame ettirme, dinlenme, emeklilik, sağlık, barışçı toplanma, seyahat ve mülkiyet gibi sosyal ve ekonomik haklar.

Üçüncü kuşak haklar: Çevre hakkı, barış hakkı, gelişme ve fırsat eşitliği hakları.

Dördüncü kuşak haklar: İnternete erişim ve birlikte gelişecek şu anda tartışılan haklar.

TEMEL HAK VE HÜRRİYETLERİN KISITLANMASI

Temel hak ve hürriyetlerin bu ünite bakımından da en önemli niteliklerinden biri prensip olarak dokunulmaz olmasıdır⁸. Yani, temel hak ve hürriyetlerin sınırlandırılması ancak aşağıdaki unsurlar dahilinde ve bunlara uygun olarak yapılabilir:

1. Savaş, sıkı yönetim, seferberlik, olağanüstü hâl gibi mutlak gerektirici ve yakın bir tehdit bulunmalıdır.
2. Sınırlama söz konusu tehdidi giderme amaçlı olmalı ve bu amaçla orantılı bir sınırlama yapılmalıdır.
3. Sınırlama kanunla yapılmalı ve sınırlamanın çerçevesi amaç, araç ve süre bakımından belirlenmelidir.
4. Bu şekilde belirlenen sınırlama, amacını aşmamalı ve amacı dışında kullanılmamalıdır.

2001 yılında Anayasa'da yapılan bir değişiklikle temel hak ve hürriyetlerin kamu güvenliği, ülkenin bölünmez bütünlüğü, özel hayatın ve meslek sırlarının korunması gibi amaçlarla da sınırlandırılabileceğine ilişkin bir hüküm getirilmiştir⁹.

Temel hak ve hürriyetler ancak bu şekilde sınırlandırılabilecek olsa da getirilebilecek kanuni sınırlar bakımından da mutlak anayasal çerçeve vardır.

Savaş ve olağanüstü hallerde dahi kimse düşünce ve kanaatlerinden ötürü suçlanamaz ve bunları açıklamaya zorlanamaz. Her hâlükârda, uluslararası hukuktan kaynaklanan yükümlülükler ihlal edilemez.

Hukukumuzda da sınırlamaların demokratik toplum düzeninin gereklerine aykırı olamayacağı ve öngördükleri amaç dışında kullanılamayacağı kabul edilmiştir. Burada altı çizilmesi gereken nokta “demokratik toplum/rejim” anlayışıdır. Türkiye, Strasbourg ruhunu, Avrupa Birliği (“AB”) Kopenhag siyasi kriterlerini benimsemekle, yukarıda değindiğimiz uluslararası sözleşmelere taraf olmakla ve AB müktesebatına uyum gayretiyle zaten aslında “demokratik toplum” derken neyi anladığını ortaya koymaktadır. Bu anlayış Anayasa Mahkememiz tarafından da kararlarında atıfta bulunulan batı uygarlığında benimsenen demokrasi anlayışıdır.

Uluslararası hukuktan kaynaklanan yükümlülükler dediğimizde aklımıza İHEB ve AİHS hükümleri, Avrupa İnsan Hakları Mahkemesi (“AİHM”) kararları ve bunlardan kaynaklanan yükümlülüklerimiz gelir. Ancak, yine temel hak ve özgürlükler çerçevesi içinde olan angaryayı önleme, çocuk işçiliğini önleme, işçi hakları, işçi sağlığı ve iş güvenliği esasları, ağır ve tehlikeli işlerde insani çalışma şartlarına ilişkin standartları getiren Uluslararası Çalışma Örgütü (“ILO”) ve onun sözleşmeleri ve ek sözleşmeleri gibi farklı uluslararası enstrüman ve angajmanlardan kaynaklanan yükümlülüklerimiz de vardır.

AİHS de bazı hallerde temel hak ve hürriyetlerin kısıtlanmasını öngörmektedir. Ancak, AİHM bu kısıtlama şartları testini ulusal varlığı tehdit eden durumlar kavramı üzerinden yapmaktadır. Savaş ve ulusal varlığı tehdit eden sair haller sadece belli bir gruba ya da grupları veya kişi ya da kişileri değil tüm nüfusu tehdit etmeli ve tüm toplumun kamu

⁸ Kaboğlu, Kolektif Özgürlükler., s.25-26

⁹ Fendoğlu, 2001 Anayasa Değişikliği Bağlamında Temel Hak ve Özgürlüklerin Sınırlaması, s. 144

düzenini ve kamu sağlığını olağanüstü bir boyutta, gerçekleşmesi kesin ve yakın bir tehlike olması hâlinde bunun temel hak ve özgürlüklerin kısıtlanmasında meşru zemin teşkil edeceği ilkesini tesis etmiştir.

Hem temel bir hak ve hürriyet olan hem de diğer tüm hak ve hürriyetlerin garantisini olan en önemli husus da hakkı ihlal edilen herkesin siyasi ve ekonomik olarak bağımsız yetkili yargı makamında, kanun önünde idareyle yani kamu otoritesiyle eşit şekilde, idarenin yani kamu otoritesinin işlemlerinin suistimalini iddia ederek durdurulması ve zararlarının giderilmesini talep edebilmesidir.

İdarenin işlemleriyle yargı denetimine tabi olması erkler ayrılığının bir gereği ve tüm temel hak ve hürriyetlerin garantisidir. Anayasa Mahkemesi'nin varlık sebebi Türkiye Büyük Millet Meclisi tarafından insan haklarının ihlal edilmesini önlemektir. AİHM kararları da ülkemiz ve insanımız için temel hak ve hürriyetlerin tanımlanması, sınırlandırılması, kullanılması ve idarenin işlemlerinin hukuka uygunluğunun tespiti bakımından çok büyük bir arzuetmektedir. Bununla birlikte AİHM kararları cebren icra edilemez ancak tazminat ile mümkün olduğunca zararları giderme noktasında bir etkisi olur. Ayrıca bir kısım mevzuatımıza göre bir Türk mahkemesinin kararı AİHS'ne aykırı olduğu AİHM tarafından tespit edilmişse mağdur AİHM kararının kesinleşmesinden itibaren bir yıl içinde yargılanamın yenilenmesini isteyebilir.

AİHM, 1976 tarihli *Handyside v. UK* kararında¹⁰ ifade hürriyetinin sadece rahatsız edici olmayan bilgi ve fikirlere değil, devleti veya toplumun bir kısmını rahatsız edebilecek veya şoke edebilecek fikir ve yorumlara da uygulanacağını belirterek çoğulculuk, hoşgörü ve açık görüşlülüğü demokratik toplumun olmazsa olmaz unsurları olarak saymış; çoğulculuğu, ifade ve toplanma ve dernekleşme hürriyetini garantine altına alan, siyasi ve toplumsal farklılıklara izin veren, devletin farklı görüşlere karşı eşit mesafe durmasını ifade eden siyasal tarafsızlık ilkesini demokratik toplumun vazgeçilmez bir unsuru olarak ortaya koymuştur.

Anayasamızda temel hak ve hürriyetlerin kısıtlanması için nasıl bir sistem öngörülmüştür?



SIRA SİZDE

TEMEL HAK OLARAK İNTERNET ERİŞİMİ

2003 yılının Aralık ayında yapılan Bilgi Toplumu Dünya Zirvesi'nde¹¹, Birleşmiş Milletler Kurucu Belgesi ve İHEB çerçevesinde sürdürülebilir gelişim ve yaşam kalitesini artırma yönünde insanların ve toplumların potansiyellerini azami ölçüde kullanabilmeleri için herkesin bilgi yaratma, bilgiye ulaşma, bilgiyi kullanma ve paylaşma hakkı olduğu ve bu hakları kullanabilmelerini sağlayacak şartların yaratılması hususunda katılımcı devletler, özel sektör ve sivil toplum temsilcileri bir sonuç bildirisi yayımlamışlardır.

Bildiride gelişim hakkının kullanılmasının ayrılmaz bir parçası olan fikir ve ifade hürriyetlerinin ve bu hürriyetlerin hiçbir müdahale olmaksızın, millî sınırlardan bağımsız olarak her türlü media (aracı platform) kullanılarak ifade edebilmesi ve paylaşabilmesinin gerekli olduğu belirtilmiştir. İletişim sadece temel bir hak değil aynı zamanda temel bir insan ihtiyacı, toplumsal bir süreç ve toplumsal organizasyonun da temelidir.

Nitekim İHEB dahi daha o yıllarda son derece öngörülü davranarak 19. Maddesinde her türlü medya (aracı) kullanımına atıfta bulunmuştur.

BBC, 2009 – 2010 arasında, aralarında Türkiye'nin de bulunduğu 26 ülke ve 14 bini İnternet kullanıcısı dahi olmayan 27 bin yetişkin nezdinde yaptığı bir araştırma sonucunda, her beş kişiden birinin yani %79'luk bir kesimin İnternet erişimini temel bir insan hakkı olarak gördüğü ortaya çıkmıştır¹².

¹⁰ 5493/72, 07.12.1976, [http://hudoc.echr.coe.int/eng?i=001-57499#{"itemid":\["001-57499"\]}](http://hudoc.echr.coe.int/eng?i=001-57499#{)

¹¹ <https://www.itu.int/wsis/docs/geneva/official/dop.html>

¹² http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/08_03_10_BBC_Internet_poll.pdf

İnternet'in çok ciddi kısıtlamalarla karşılaştığı Çin'de oran %87 çıkmış, bir başka İnternet'le çok sorunlu ülke olan Rusya'dan katılanların %71'i ise İnternet'in devlet tarafından düzenlenmemesi gerektiğini belirtmiştir.

Ülkemiz bakımından sonuç çok enteresandır. İnternet'e erişimin temel insan hakkı olduğunu düşünenlerin oranı Portekiz hariç tüm Avrupadan daha yüksek bir oranla %91 çıkmıştır.

16 Mayıs 2011 tarihi bundan on yıllar sonra hukuk kitaplarına ve literatüre girecek olan bir miladın tarihidir. BM Genel Kurulu İnsan Hakları Komisyonu, özel raportörünün katkılarıyla hazırlanarak yayınladığı bir raporla¹³ İnternet erişiminin temel bir insan hakkı olduğunu ve bu sayede insanların fikir ve ifade hürriyetlerini kullanabildiğini ifade etmektedir. Rapordan, bu sonucunun yanında İnternet alanı hakların gasp edildiği, insanlara ve toplumlara zarar veren bir alan olsun gibi bir anlam çıkarılamaz, zira raporda daha önce işaret ettiğimiz sınırlandırma koşullarına da yer verilmiştir. Buna göre İnternet'e içerik veya erişim bakımından bir kısıtlama yapılacaksa yani bu kısıtlamanın doğrudan sonucu olarak ifade hürriyetine ve başta saydığımız temel hak ve hürriyetlere herhangi bir sınırlandırma getirilecekse bu sınırlandırmanın sadece tehlikeyi gidermeye yönelik, en asgari şekilde kısıtlayıcı, süre ve çerçevesi belirli şekilde kanunla yapılmalı, amacı dışında kullanılmamalı, başkalarının haklarını ve ulusal güvenlik, kamu düzeni ve kamu sağlığını koruma amaçlı olarak gerekliliği "proven" yani ispatlanmış olmalıdır. Kısıtlamaya ilişkin çıkarılan düzenleme ve bu düzenlemenin uygulaması siyasi ve ekonomik olarak bağımsız yargı denetimine tabi olmalıdır.

Bu çok önemli raporda altı çizilmesi gereken hususlar şunlardır:

- Keyfi olarak İnternet sitesi veya içerik bloklama ve filtreleme adli veya tamamen bağımsız düzenleyici makam tarafından kanuni sınırlamalara uygun olarak yapılmalıdır. Şahsi yorumuma göre düzenleyici kurumun bu yetkisi ani bloklama veya filtreleme için yargılamayı gerektiren haller dışındaki çocuk pornosu, dolandırıcılık ve terör suçları gibi zararın çok büyük ve hukuk ihlalinin çok açık olduğu hâllerle sınırlı olmalıdır.
- Meşru fikir ve ifade hürriyeti kullanımları ceza hukuku kapsamından çıkarılmalıdır.
- Hizmet sağlayıcılara gayri makul sorumluluklar yüklenmemelidir. İnternet hizmet sağlayıcıları dediğimiz, erişim sağlayıcılara ve hizmet sağlayıcılara, İnternet'teki içeriği kendileri sağlıyormuşçasına hukuki ve cezai sorumluluklar yüklenmekte ve bu sorumluluklar çerçevesinde hizmet sağlayıcıların yöneticileri cezai sorumlulukla yargılanmakta veya hukuki sorumluluklar ve idari cezalar söz konusu olabilmektedir.
- Yetersiz mahremiyet ve gizli bilgi koruması. Mahremiyet de bir insan hakkıdır. Ne yazık ki kişisel bilgiler, hassas bilgiler, gizli bilgiler, tıbbi bilgiler, ticari sırlar gibi hususlar ve bunların saklanması ile korunmasına ilişkin ülkemizde spesifik düzenlemeler bulunmamaktadır. Bu da sadece İnternet ve temel haklar bakımından değil her bakımdan büyük sorunlar yaratmaktadır. Devletlerin veya şirketlerin, kişilerin İnternet veya sair araçlar üzerinden yaptıkları veri alış verişini gözetlemeleri ve kullanmaları, trafik bilgilerinin tespiti gibi hususlar tüm dünyada ortak bir sorundur.

Netice itibarı ile BM'in bu raporu dünyada büyük bir yankı uyandırmış ve heyecanla karşılanmıştır.

"İnternet'in Babası" olarak adlandırılan, Google başkan yardımcılarında ünlü Vinton Cerf bu raporu New York Times'daki bir yazısı ile değerlendirmiştir. İnternet'in mutla-

¹³ Birleşmiş Milletler Genel Kurulu İnsan Hakları Komisyonu, Fikir ve İfade Özgürlüğünün Korunması ve Geliştirilmesi Üzerine Özer Raportör Raporu, A/HRC/17/27, 16.05.2011 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

ka geliştirilmesinin, yayılmasının ve korunmasının insanlık için yapılması gereken bir şey olduğunu ancak İnternet'e erişimin temel bir insan hakkı olmadığını yazmıştır¹⁴.

Bugün eğitim, sağlık, gelişim ve ticaret için elzem olan iletişim ve bilgiye ulaşma, ifade ve fikir ve tabii ki basın hürriyeti için İnternet olmazsa olmaz bir şart ve araç olduğundan bu görüşe iştirak etmek mümkün değildir.

Doğru ve dengeli var olan veya iyi niyetle getirilmek istenen, hakların lüks veya bol görünmeye başlanarak özgürlük alanlarının daraltma hevesi veya temayülü otokratik bir yaklaşımdır ve insan haklarının, temel hak ve hürriyetlerin temel felsefesi ile çelişir. Nitekim, Uluslararası Af Örgütü, İstanbul'da bir İnternet cafede çekilmiş bir fotoğrafla verdiği cevapta¹⁵ de Cerf'in insan hakları algısının çok dar olduğunu belirtmiştir. Kendi verdikleri bir örnekte nasıl ki bir kişinin bir şehrin meydanına veya merkezine fiziksel erişimi olmadan, gösteri ve toplanma hakkını kullanamayacaksa, İnternet'e erişim olmadan da ifade hürriyeti, basın hürriyeti ve eğitim hürriyetinin kullanılmasının imkânsız ve anlamsız olacağını anlatmaya çalışmışlardır.

Avrupa Konseyi Genel Sekreterliği, İnsan Hakları ve Hukukun Üstünlüğü ve Bilişim Toplumu Genel Müdürlüğü, 2012 - 2015 İnternet Yönetim Stratejisi Gözetimi, Kasım 2014 İnternet Yönetim Stratejisi Uygulama Sekreterlik Raporu'nda¹⁶ İnternet erişiminin, ifade hürriyetinin, eğitim hakkının, kültürel hayatta yer alma hakkının, siyasi hakların, toplanma, örgütlenme ve dernekleşme haklarının kullanılabilmesini gerçekleştiren bir olgu olduğunu kabul etmiştir. İnternet'i bu sebeple AİHS'nin 10. Maddesi çerçevesinde değerlendirdiklerini bildirmiştir.

AB, BM'e ve üye devletlere de bu konuda uyum hâlinde kodifikasyon çağrısı yapmıştır. Estonya, Finlandiya, Fransa gibi ülkeler İnternet erişimini *temel bir hak* olarak kabul edip kendi iç mevzuatlarına dercetmişlerdir.

DÜNYADA VE TÜRKİYE'DE İNTERNET ERİŞİMİNİN ENGELLENMESİ VE İSTİHBARAT AMAÇLI GÖZLENMESİ

İdarenin işlemlerinin yargı denetimine tabi olması ve bireysel hakların korunması demokrasinin ve hukukun üstünlüğünün *conditio sine quo non*'u yani, olmazsa olmaz şartıdır.

Ancak bu yaklaşımın en eskiye dayandığı batılı ülkelerde dahi son yirmi yıldır yargıçlar temel hakların sınırlanması noktasında hukuk ile çoğunlukçu yasama faaliyeti arasında sıkışmıştır. Bu çelişki tüm ülkelerde benzer özellikler arz etmektedir.

Özellikle İnternet ve telekomünikasyon noktasında devlet gücünün suistimali veya devletin kişilik haklarının ihlalleri 2013 yılında büyük bir skandal ile zirveye çıkmıştır.

Edward Snowden'in 2013'te başlattığı bilgi akışı sayesinde¹⁷ dünya inanılması güç bazı gerçeklerin farkına varmaya başlamış ve bu gerçekler ABD'yi ve Birleşik Krallığı 2014 itibarı ile Sınır Tanımayan Gazetecilerin "İnternet Düşmanı Ülkeler" listesine sokmuştur¹⁸.

ABD'nin başta Birleşik Krallık olmak üzere Almanya, Kanada, Avusturalya ve Yeni Zelanda ile çok ciddi bir İnternet ve iletişim gözetlemesi ve milyonlarca doküman ve varılan teknoloji itibarı ile akılların alamayacağı büyüklükte veri topladıkları ortaya çıkmıştır.

1946'da İkinci Dünya Savaşı sonunda kurulan ve soğuk savaş süresince bir istihbarat işbirliği öngören, içinde ABD, Birleşik Krallık, Kanada, Avusturalya ve Yeni Zelanda'nın

¹⁴ New York Times, The Opinion Pages, İnternet Access is Not a Human Right, 04.01.2012, http://www.nytimes.com/2012/01/05/opinion/Internet-access-is-not-a-human-right.html?_r=0

¹⁵ <http://blog.amnestyusa.org/middle-east/is-Internet-access-a-human-right/>

¹⁶ [http://www.coe.int/t/dghl/standardsetting/media/CDMSI/CDMSI\(2014\)016_en.pdf](http://www.coe.int/t/dghl/standardsetting/media/CDMSI/CDMSI(2014)016_en.pdf)

¹⁷ Greenwald, No Place to Hide: Edward Snowden, the NSA and the US Surveillance, 13.05.2014

¹⁸ <http://en.rsrf.org/enemies-of-the-Internet-2014-11-03-2014,45985.html>

bulunduğu Five Eyes¹⁹ isimli istihbarat ağı yürüttüğü ortak veya ulusal istihbarat programlarıyla milyonlarca Amerikalı'nın ve Amerikalı olmayan İnternet kullanıcısının metadata ve içerik paylaşımlarını, gözetlediği ve topladığı ve telefonlarını dinlediği ortaya çıkmıştır.

Bu gözetlemelere ve dinlemelere Hotmail ve MSN Messenger'ın sahibi Microsoft, British Telecom, Verizon ve Vodafone gibi şirketin ticari ortak olarak katıldıkları ortaya çıkmıştır.

Örneğin Guardian, çok gizli bir mahkeme kararına istinaden Ulusal Güvenlik Kurumu, National Security Agency'nin ("NSA") 120 milyon Verizon abonesinin telefon kayıtlarını toplandığını ortaya koymuştur.

NSA, yürüttüğü PRISM²⁰ adındaki gözetleme programı çerçevesinde bilinmeyen sayıda Amerikalı'nın ve diğer ülke vatandaşlarının e-maillerini, video görüşmelerini, chatlerini Google, Microsoft, Yahoo, Apple gibi devlerin veri merkezlerine veri taşıyan iletim sistemlerine sızmak suretiyle yüz milyonlarca kullanıcıdan metadata ve içerik toplama kabiliyeti kazanmış ve yine tam olarak bilinmeyen hacimde bilgi depolamıştır. Aynı tarz bir gözetleme sistemini Birleşik Krallık da MUSCULAR²¹ adı ile tesis ederek benzer istihbarat faaliyetleri gerçekleştirmiştir.

Bu ortaya çıkan skandalın tam boyutunu her yönüyle anlatmak bu ünitenin amacının dışındadır. Neticede, o demokratik toplum standardını belirleyen batı yüz milyonlarca vatandaşının ve vatandaşı olmayan İnternet kullanıcısının iletişim özgürlüğünü ve mahremiyetini ihlal etmiştir.

Bu faaliyetlerin savaş tam-tamları çalan bir neo-con olmakla suçlanan Cumhuriyetçi George W. Bush veya selefi bir Cumhuriyetçi başkan döneminde değil de Demokrat ve ABD tarihinin ilk siyahi başkanı Obama döneminde yapılmış olması da kaderin acı bir cilvesidir.

Bütün bu süreçler kaçınılmaz olarak bir takım hukuki sonuçlar doğurmuş ve çok ilginç iki mahkeme kararı ortaya çıkmıştır.

*Klayman v. Obama*²² davasında Verizon aboneleri Karry Klamann'ın açtığı davaya müdahil olmuşlardır. 16 Haziran 2013'te Federal Hakim Richard Leon verdiği kararlar uygulamanın yüksek teknolojinin ihlali bakımından daha keyfi ve rastgele kullanılamayacağını, uygulamanın ABD anayasasını ihlal ettiğini ve herhangi bir yakın ve ciddi bir saldırıyı önlediğine dair de herhangi bir delil de bulunmadığını ifade etmiştir.

Hükümetin topladığı bilgilerin imha edilmesine karar verilmiş olmasına rağmen, kararın yürütmesi ABD hükümetinin çok ciddi millî güvenlik sebeplerini ve anayasaya uygunluk denetiminde durumun özellik arzettiği sebebiyle yaptığı temyiz başvurusu ile durdurulmuştur.

Bu arada Amerikan Temel Haklar Birliği ile New York Temel Haklar Birliği, Ulusal İstihbarat ve NSA direktörleri ile bir kısım üst düzey ilgili bürokrat aleyhine dava açmıştır.

ACLU v. Clapper davasında²³, Federal Hakim William Pauley, NSA tarafından telefon şirketlerinden alınan verinin telefon şirketleri tarafından mahkeme kararına dayanarak veya istemli iş birliği çerçevesinde verildiğini ve Anayasa'nın Dördüncü Maddesi (Fourth Amendment Rights) çerçevesinde kullanıcıların bir gizlilik beklentisi içinde makul olarak bulunamayacaklarını belirtmiştir.

Hakim ayrıca bu uygulamanın başarılı olduğunu, bir takım terörist saldırıları önlediğini, NY metrosuna bombalı saldırı planlayan Najibullah Zazi'nin, New York Borsası'na

¹⁹ ABD Ulusal Arşivi, 1946, https://www.nsa.gov/public_info/declass/ukusa.shtml

²⁰ Gellman & Poitras, US, British Intelligence Mining Data from Nine US İnternet Companies in Broad Secret Program, Washington Post, 07.07.2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-İnternet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

²¹ Gellman, Soltani & Peterson, How We Know the NSA Had Access to Internal Google and Yahoo Cloud Data, Washington Post, 04.11.2014, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-İnternet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

²² US District Court for the District of Columbia, 13-0851 (RJI), 16.12.2013, https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48

²³ US District Court Southern District of New York, 13-3994 (WHP), 27.12.2013 <http://www.nysd.uscourts.gov/cases/show.php?db=special&id=364>

bombalı saldırı planlayan Khalid Ouzzani'nin bu çalışmalar sayesinde tespit edildiğini belirterek, yargılama sonucunda davayı reddetmiştir.

ÜLKEMİZDE İNTERNET

Ülkemiz hiçbir ülkenin özgürlüğünü de hukuk sistemini de cezasını da taklit etmek, başkasına benzemek zorunda değildir. Türkiye, en özgür diye bildiğimiz ülke kadar özgür olabilirken, aynı zamanda gerçek suçla en etkin mücadele eden ülke kadar dirayetli, güçlü ve neticede gerek insanların suça yönelmesini engellemekte gerekse de suç oranlarının düşürmekte başarılı olabilir. Hukuk sistemimizde ve uygulamamızdaki bir kısım problem yabancı mevzuatın üzerine oturduğu felsefe, kültür ve tarihi hiç anlamadan, hatta çoğu zaman niye çıkarıldığını dahi bilmeden sırf çıkarmış olmak için çıkarılan ve çoğu zaman da bazı menfaatler gözetilerek, içlerine işimize geldiği gibi hükümler serpiştirerek işimize geldiği gibi mevzuat yapmamızdan kaynaklanmaktadır.

Alt yapı olan hukuka yaklaşım kesinlikle bu şekilde olmamalıdır.

Türkiye bugün filtreleme ve bloklaama sonucu sayısı tam olarak bilinemeyen ve öğrenilemeyen 84,000'den fazla URL/web sitesi bulunmaktadır²⁴.

20 Haziran 2013'te Resmi Gazete'de Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem planı yayımlanmıştır²⁵. Eylem planı açıkça İnternet'te anonimlik ve inkâr edilebilirlik zaafiyetleri olduğundan söz etmekte ve bunlarla mücadele amacı gütmektedir. Siber güvenlik alanında paydaş kurumlar arasında ulusal koordinasyon eksikliğini risk olarak ortaya koyan madde gibi bir kısım parametrelerin anlamı tam olarak açık değildir. Uluslararası iş birliği ve bilgi paylaşımı için diplomatik, teknik ve kolluk iletişim kararlarının sürekli ve etkin kullanılması gerektiği belirtilmektedir. Belgenin en can alıcı noktaları ise, İnternete olumsuz ve şüpheli gözle bakarken 2013-14 döneminde “gerekli” mevzuatların çıkarılacağını, adli süreçler için “kayıt” mekanizmalarının kurulacağını belirtilmesi, siber olaylara müdahale organizasyonu oluşturulacağını ifade etmesi. Faaliyet Planı Eylül 2013'te kanun yapım çalışmalarının tamamlanacağını öngörmektedir. Siber olayların delillendirilmesinde MİT, Jandarma, Emniyet Müdürlüğü, TÜBİTAK ve BTK sorumlu kuruluşlar olarak gösterilmektedir.

Nitekim, kamuoyunda İnternet Kanunu olarak bilinen 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da (“**5651 S.İ Kanun**”), MİT Kanunu'nda, HSYK Kanunu'nda ve en son 10 Eylül 2014 tarihinde yasalaşan 6552 Sayılı Torba Kanun²⁶ içinde 5651 S.İ Kanun'da yapılan değişikliklerle Eylem Planında öngörülen tüm bu “geliştirmeler” yapılmıştır ve yapılmaya devam edilmektedir.

Ülkemizde İnternet üzerinden işlenen suçlarla mücadele konusunda özel hüküm getirme ve Avrupa Birliği mevzuatı ile uyum sağlama ihtiyaçları kabul tarihi 4 Mayıs 2007 olan 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'la giderilmeye çalışılmıştır.

5651 Sayılı Kanun gerek teknik ve hukuki gelişmeler gerekse suçla mücadele noktalarında son derece yetersiz kalmış ve özetle yanlış tanımlar getirmiş, katalog suçları yanlış belirlemiş, idareye yargılama gerektiren bir takım yetkiler vererek anayasal yetki gaspına sebebiyet vermiş, Uyar – Kaldır yöntemini çok yetersiz şekilde düzenlemiştir.

²⁴ <http://engelliweb.com/>

²⁵ <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2013/06/20130620.htm&main=http://www.resmigazete.gov.tr/eskiler/2013/06/20130620.htm>

²⁶ <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2014/09/20140911m1.htm&main=http://www.resmigazete.gov.tr/eskiler/2014/09/20140911m1.htm>

Ne yazık ki 5651 Sayılı Kanun'un yorumlanması ve uygulanması mahkemeden mahkemeye farklılık göstermekte, kanunu uygulamakla yükümlü kurumlar tarafından çok sınırlı anlaşılabilmekte ve sonuç olarak uygulamasında büyük eksiklikler yaşanmaktadır. Konunun teknik mahiyetinin yanı sıra, itiraf etmeliyiz ki bazen bu kanun işe geldiği gibi uygulanmakta ve haber alma hürriyeti ile ifade hürriyetini sınırlamak gibi niyetler de gözlemlenmektedir.

YouTube'a Türkiye'den erişim, 2007 ile 2010 yılları arasında verilen çeşitli mahkeme kararlarıyla toplamda iki yıl kadar engellenmişti. YouTube'un kapatılmasına sebep olan içerikler, dünyanın her yerinden ulaşılabilir iken absürd bir biçimde sadece Türkiye'den ulaşamaz hâle getirilmiştir.

Google Sites, her bireyin ve işletmenin tamamen ücretsiz olarak ve profesyonel yardım almadan kendi web sitesini kurmasına imkan sağlayan bir üründür. 2009 ortasına kadar ülkemizde milyonlarca kişi ve işletme Google Sites'i hem web sitelerini kurmak için, hem de bu kurulmuş olan sitelerden faydalanmak için kullanmakta iken, Google Sites alanının (ürününün) tamamına erişim milyonlarca web sitesi içinde sadece tek bir sitede bulunan içerik sebebiyle tamamen engellenmiştir. Bir sabah uyandıklarında binlerce web sitesi sahibi sitelerine ulaşamaz olmuş, kullanıcılar binlerce siteden elde ettikleri içeriklere de ulaşamaz olmuştur.

Yargı süreci içinde bu karar en sonunda AİHM'nin önüne gelmiş²⁷ ve AİHM 18 Aralık 2012 tarihli ve 3111/10 sayılı kararıyla, 5651 sayılı Kanun'un 8. Maddesinin Avrupa İnsan Hakları Sözleşmesi'nin 10. Maddesine aykırı bulmuş, kanunun demokratik hukuk devletin sağlama gereken hukuki korumayı sağlamadığını belirtmiş ve Türkiye'yi kınayarak tazminata mahkûm etmiştir. Bu karara rağmen bu alana Türkiye'den erişim halâ yasaktır.

Ne yazık ki ülkemizde *yer sağlayıcı* dediğimiz, içeriği kendisi oluşturup yüklemeyen ancak sadece platformu sağlayan YouTube, Blogger, Blogspot gibi tüzel kişiler; uygulamada yazıyı yazan, videoyu çeken ve bunları platforma yükleyen içerik sağlayıcısıymışçasına sorumlu tutulmaya çalışılmaktadır.

Mevzuatımız *yer sağlayıcı* için platforma yüklenen içeriği denetleme yükümlülüğü öngörmemesine rağmen (sadece YouTube'da saniyede yüklenen 100 saatlik içerik nasıl denetlenebilir?) mahkemeler uygulamada kanuna açıkça aykırılık teşkil edecek şekilde bu yönde kararlar verebilmektedir.

Uyar – kaldır dediğimiz bir içeriğe erişimi engellemek üzere yargıya başvurmadan önce yapılacak ihbar sistemi çok muğlaktır ve uygulanmamaktadır.

Müstehcenlik, hakaret suçu, siyasi söylem gibi kavramların yorumlanmasında standart bulunmamakta ve haber alma hürriyeti ile kamu yararı faktörlerinin değerlendirilmesinde sorunlar hissedilmektedir. Müstehcenlik gibi herkese göre farklı olabilecek bir kavram katalog suç tipi iken terör suçu, ağır mali suçlar, ticaret ve finans hayatını etkileyecek sermaye piyasası ve bankacılık suçları, kamu sağlığını ve düzenini etkileyecek suçlar gibi konuların katalog suçlar içinde bulunmaması anlaşılacak gibi değildir.

Yıllardır uygulamacılar, akademisyenler ve İnternet aktörleri 5651 Sayılı yasanın ilgili mevzuatın düzeltilmesi için çok önemli girişimlerde bulunmuş, sayısız toplantılar yapmış, değişiklik tekliflerini ilgili makamlara iletmiştir. İyi niyetle tüm ülke bunların dinlenmesini ve bunun üzerine ülkenin ekonomik, sosyal, hukuki ve eğitim menfaatlerine yönelik adımlar atılmasını beklerken ne yazık ki bu beklentilerimizin sonu hüsrana olmuştur.

²⁷ Yıldırım v. Turkey, 3111/10, 18.12.2012, [http://hudoc.echr.coe.int/fre?i=001-115705#{"itemid":\["001-115705"\]}](http://hudoc.echr.coe.int/fre?i=001-115705#{)

7 Ocak 2014 Salı günü öğleden sonra TBMM Plan ve Bütçe komisyonunda görüşülmeye başlanarak, gece yarısına doğru Genel Kurul'a sunulma kararı alınan "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Bazı Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı" isminde bir Torba Yasa'nın 92. ile 108. Maddeleri ile 5651 Sayılı Kanun değiştirilmiş aynı hafta içinde kanun ikinci bir defa daha değiştirilmiştir.

Zaten hemen her tarafında ciddi problemler olan 5651 Sayılı Kanun'un, Torba Yasa ile getirilen yeni hükümlerinin hepsi de çok ciddi problemlere gebe hatta bence Anayasa Mahkemesi tarafından iptal edilebilir niteliktedir.

Özetle ifade etmek gerekirse, Mahkeme eğer arzu edilen amaca ulaşamayacağını düşünürse sadece URL (sayfa sayfa) bazlı değil, bütün bir web sitesine veya İnternet hizmetine (YouTube, Facebook, Twitter, Ekşi Sözlük, Vimeo gibi) erişimi engelleyebilir. Diğer bir deyişle, YouTube, Facebook, Twitter farklı kullanıcılar tarafından defalarca yüklenen videolar-dan ötürü tamamen kapanabilir.

Telekomünikasyon İletişim Başkanlığı ("TİB") Başkanı, re'sen ve tamamen kendi takdirleriyle özel hayatın ihlali olarak nitelediği bir sitenin kapatılmasını emredebilir. Bu emrini Erişim Sağlayıcılar Birliği'ne ("**Birlik**")²⁸ gönderir ve Birlik bu emri derhal ve her hâlükârda en geç dört saat içinde uygulamak zorundadır. Başkan bu kararına 24 saat içinde mahkemeden onay almalıdır. Mahkeme kararını 48 saat içinde vermek zorunda olacaktır.

Özel hayatının ihlal edildiğini iddia eden kimse mahkemeye dahi gitmeden doğrudan TİB'e *içerikten çıkarma* talebiyle başvurabilir. TİB bu talebi Birlik'e gönderir. Birlik bu talebi derhal ve her halukarda en geç dört saat içinde uygulamak zorundadır. Başvuruyu yapan kimse 24 saat içinde kapatılma uygulaması için mahkemeden onay almalıdır.

Özel hayatının gizliliği dışında sebeplerden mağdur olduğunu iddia eden kimse doğrudan mahkemeye başvurabilir. Mahkeme talep ile ilgili 24 saat içinde içeriği koyanı ve yer sağlayıcıyı (YouTube, Facebook, Twitter vb.) dinlemeden karar verir. Ancak kapatılma kararından sonra içerik veya yer sağlayıcı bir üst mahkemeye itiraz edebilir.

Erişim Sağlayıcılar, bir özel hukuk tüzel kişisi mahiyetinde olacak olan Erişim Sağlayıcılar Birliği'ni kurmak zorundadır. Birlik'e katılmayan erişim sağlayıcının lisansı iptal edilir.

Yer sağlayıcılar iki yıla kadar trafik bilgisini (IP adresi, hizmetin başlangıç ve bitiş zamanını, yararlanılan hizmetin türünü, aktarılan veri miktarını, abone kimlik bilgilerini) iki yıla kadar saklamak zorundadır. Siber güvenlikle ilgili bilgileri TİB yer sağlayıcıdan isteyebilir.

Yukarıda açıklanan yirmidört saatlik süreler 11 Eylül 2014 tarihinde yürürlüğe giren yine bir Torba Yasa (No. 6552) hükmüne göre dört saate indirilmiştir.

Müstehcenlik, nefret suçu, özel hayatın ihlali gibi kişiden kişiye, yerden yere, zamandan zamana değişebilecek münferit olarak her davada mahkemeler tarafından ayrı ayrı ele alınması gereken en müphem kavramlar idareye filtreleme ve sansür bahanesi olarak sunulmakta ve yargı denetiminden çıkmaktadır. Yukarıda gerekçeleri ile belirttiğimiz üzere zaten ülkemizin taraf olduğu uluslararası sözleşmelere, Anayasaya ve erkler ayrılığına aykırı olan 5651 Sayılı Kanun düzeltilmesi gerekirken, ülkemizi hem ekonomik hem de hukuki bakımdan çok zor durumda bırakacak hükümler içerirken, diğer yandan da ne yazık ki tüm temel hak ve hürriyetleri de ihlal etmektedir.

Nitekim son olarak 30 Mart 2014 tarihli Yerel Seçimlerden hemen önce hem Twitter hem de YouTube tamamen hukuki temelden yoksun olarak kapatılmıştır. Her iki hizmet / web sitesi de ancak Anayasa Mahkemesi'ne yapılan "bireysel" başvuruların^{29,30} kazanılmasıyla yeniden açılabilmiştir.

²⁸ Kurulması öngörülen Erişim Sağlayıcıları Birliği'nin tüzüğünün uygulamasını Danıştay 13. Dairesi 20.01.2015'te durdurmuştur.

²⁹ <http://www.resmigazete.gov.tr/eskiler/2014/06/20140606-10.pdf>

³⁰ <http://www.resmigazete.gov.tr/eskiler/2014/04/20140403-18.pdf>

Anayasa Mahkemesi, verdiği gerekçeli kararda, TİB'in Twitter'a erişimin tümüyle engellenmesine ilişkin kararının, ilgili kanun hükümlerine açık aykırılık oluşturduğunu, ayrıca bu yönde herhangi bir mahkeme kararı olmadığı gibi Ankara 15. İdare Mahkemesi'nin engelleme kararının yürürlüğünü durduran kararının da idare tarafından uygulanmadığına işaret etmiştir.

Mahkeme, İnternet'in modern demokrasilerde başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin kullanılması bakımından önemli bir araçsal değere sahip bulunduğu belirterek İnternet'in sağladığı sosyal medya zemini kişilerin bilgi ve düşüncelerini açıklama, karşılıklı paylaşma ve yaymaları için vazgeçilmez nitelikte olduğu tespit etmiştir.

Mahkeme, sosyal paylaşım sitesine erişimin kanuni dayanağı olmaksızın ve sınırları belirsiz bir yasaklama kararı ile engellenmesinin demokratik toplumların en temel değerlerinden biri olan ifade özgürlüğüne ağır bir müdahale oluşturduğunu, kamu otoritesince yapılan müdahalenin haklı sebeplere dayanması, hak ve özgürlüklerin sınırlandırılması sırasında hakların özüne dokunulmaması ve ölçülü olunması gerektiğini belirtmiştir.

Anayasa Mahkemesi'nin bu iki kararından sonra hem 5651 Sayılı Karar yeniden değiştirilmiş, hem de Twitter, Facebook, Google ve bir çok basın kuruluşunun URL'lerine daha erişim engeli getirilmiştir.

27 Mart 2015'in ilk saatlerinde TBMM Genel Kurulu'nda yine birbiriyle ilgili ilgisiz bir çok mevzuatta yer alan bir çok hükmü değiştiren bir Torba Yasa daha³¹ kabul edildi.

6637 Sayılı Torba Yasa'dan da haftalardır mecliste neredeyse ölümle sonuçlanacak yalaranmalı kavgalarla, basında da gece gündüz tartışılan, hayatımızın merkezine oturan iç güvenlik paketi hükümleri ve İnternet yasakları çıktı. Yasalaşan metinde bir de sürpriz vardı. TBMM Genel Kurulu'na sunulan taslağında yer almayan, genel kurul görüşmeleri sırasında İçişleri Bakanı tarafından teklif edilen, Cumhurbaşkanı'na kapalı istihbarat ve kapalı savunma hizmetleri, devletin milli güvenliği için örtülü ödenek olanağı veren önerge kabul edildi ve Torba Yasa içinde kanunlaştı.

6637 Sayılı Torba Yasa'nın 16. Maddesi, 5651 sayılı Kanunun 8. Maddesi'ne getirdiği ek hükümlerle;

- Başbakan veya ilgili Bakan'ın vereceği 'milli güvenlik, kamu düzeni, suç işlemesini önlemek, genel sağlık' gibi sebeplerle bir web sitesine içerikten çıkarma ve/veya erişimi engelleme kararını, Telekomünikasyon İletişim Başkanlığı (TİB) tarafından derhal ve en geç dört saat içinde uygulanması;
- Başkanlık'ın içerikten çıkarma ve/veya erişimi engelleme kararını 24 saat içinde Sulh Ceza Hakimi onayına sunması ve hakimın 48 saat içinde karar vermesi;
- İçeriğin çıkarılması ve/veya içeriğe erişimin engellenmesi teknik olarak yapılamaz ise içeriğin yer aldığı hizmetin (örneğin YouTube veya Twitter hizmetinin tamamı) tamamen engellenmesi;
- Suç olduğu değerlendirilen içeriği yayanlar (yani retweet veya facebook share gibi) hakkında, içeriği oluşturanlar gibi suç duyurusunda bulunulabilmesi;

yönünde düzelemeler getirilmiştir.

2014'ün başından beri yapılagelen ve büyük eleştirilere, büyük gösterilere maruz kalan, bu torba yasayla yeni bir boyut kazanan İnternet yasakları Türkiye Cumhuriyeti Anayasası'na, Ceza Hukukumuzun temel prensiplerine, Türkiye bakımından bağlayıcı olan İnsan Hakları Evrensel Beyanname'si'ne, Avrupa İnsan Hakları Sözleşmesi'ne, AB Temel Haklar Bildirgesi'ne Anayasa Mahkememizin ve Avrupa İnsan Hakları Mahkemesi'nin yerleşik içtihatlarına uygunluk bakımından çok tartışılmalıdır.

Eleştiriler özellikle bazı noktalarda yoğunlaşmaktadır. Bir içeriği, bir tweet'i veya bir Facebook postunu herhangi bir vatandaşın, paylaşırken suç olup olmadığını bilmesi mümkün

³¹ 6637 Sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına İlişkin Kanun, <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2015/04/20150407.htm&main=http://www.resmigazete.gov.tr/eskiler/2015/04/20150407.htm>

değildir. Kişinin hürriyeti en temel ve en kutsal hakkıdır. Hukuk öngörülebilirliği, güvenliği olmazsa devletin varlık sebebi ortadan kalkar. Devlet vatandaşını sindirmek, püştürmek ve hapsedmek için değil, özgür kılmak, fikri, vicdani zenginliğini geliştirmek, korumak ve göndirmek için vardır. Bu sebeple bir içeriği veya tweeti paylaşırken, onun suç olup olmadığını takdir imkânı olmayan, suç işleme saiki ve kastı olmayan bir kişinin, *suçu işleme saik ve kastı ile hareket eden* asıl içerik sağlayıcı ile bir tutularak hakkında cezai kovuşturma açılması ceza hukukunun ve insan haklarının temel prensipleriyle çelişkilidir.

Milyarlarca farklı içeriği, veriyi barındıran web hizmetlerine (forumlar, Twitter, YouTube, Facebook, Ekşi Sözlük, basın kuruluşlarının web platformları vb) erişimin, hukuka aykırı olduğu iddia edilen tek bir içerik veya bazı içerikler yüzünden engellenmesi amaca uygunluk ve orantılılık ilkesine aykırıdır. Sonucu, haber alma hürriyetinin, ifade hürriyetinin ve basın hürriyetinin ihlalidir.

Başbakan veya bakanlar, savcı veya hakim değildirler. Başbakan veya ilgili bakan kendisini bir hakim veya bir mahkeme heyeti yerine koyarak bir içeriğin milli güvenliğe, kamu düzenine, kamu sağlığına aykırı olduğuna karar vermemelidir. Bu hususların hepsi yargılamayı gerektirir. Bir başbakanın veya bakanın kendisini polis, savcı, hakim yerine koyarak bir suç işlendiğinden, işlenmekte olduğundan veya işleneceğinden emin olarak bir içeriği kaldırtması veya ona erişimi engellemesi Anayasamızın ve demokratik hukuk devleti rejimimizin temel unsurlarından olan erkler ayrılığı ile bağdaşmaz, idare içinde iş yükünü arttırmış olur.

Başbakanlık veya bakanlık talepleri kanunda 'idari emir' mahiyetinde düzenlenmiştir. İdari emir yargı kararı yerine geçemez. Sulh Ceza Mahkemesinden aranacak onay da ilgili sulh ceza mahkemesinin adeta 'özel teşkil edilmiş bir mahkeme' gibi özel olarak Hakimler ve Savcılar Yüksek Kurulu tarafından belirlenecek olması sebebiyle eleştirilmektedir. Nitekim, sonradan 15.02.2014 tarihinde kabul edilen hükümlerin bir kısmı Anayasa Mahkemesi tarafından 11.04.2014'te iptal edilmiştir.

Bu yasama faaliyetlerinin yanı sıra, İnternet yer sağlayıcılık ve arama motoru hizmetleri veren sosyal medya sitelerine ve medya kuruluşlarının web portallarine erişim engellenmeye devam edilmiş, Twitter, Google, Facebook gibi sitelere erişim engellenmiştir.

Yukarıda özetlediğimiz durum, adeta bir fotoğraf gibi Twitter tarafından 11.08.2015'te yayınlanan Şeffaflık Raporu'na da yansımıştır. Buna göre 2015 senesinin ilk altı ayında Twitter'ın 37 farklı ülkeden aldığı 1003 içerik kaldırma talebinin 718'i Türkiye'ye aittir. İkinci sırada 68 taleple Rusya bulunmaktadır. Bu taleplerinin 442'si mahkeme kararı olup bunların 408'i Türkiye'dendir. Twitter bunların %60'ına itiraz etmiş ve bu itirazların %5'i yerinde görülmüştür. Twitter'ın bu taleplere uyma oranı önceki altı ayda %50 iken, son altı ayda %34'e gerilemesi de çok dikkat çekicidir. Zira, ülkemizdeki yaygın kanının aksine Twitter, Amerika Birleşik Devletleri'nde dahi anayasal olmadığına inandığı bazı mevzuat düzenlemelerine ya da bazı uygulamalara hukuk çerçevesinde direnmekte, meşru zeminde kalarak bunlara karşı hukuk yollarına başvurmaktadır. Örneğin Foreign Intelligence Surveillance Act'e (Yabancı İstihbarat İzleme Yasası) dayanarak mahkemeler tarafından kendisine gönderilen kararları ve talep edilen bilgileri ve ulusal güvenlik çerçevesinde kendisine gönderilen talepleri ve bunlar çerçevesinde istenen bilgileri şeffaflık raporunda yayımlayabilmesine ilişkin kısıtlamaları ABD anayasasına aykırı olduğu gerekçesiyle 07.10.2014 tarihinde California'da ABD Adalet Bakanlığı'na karşı bir dava açmıştır³².

³² Twitter v. US Department of Justice, US District Court Northern District of California, 14-cv-4480, 07.10.2014, <https://g.twimg.com/blog/blog/attachments/Complaint.pdf>

Bu bölümde ülkemiz bakımından ifade ettiğimiz yasa değişikliklerinin ve erişim engellemesi uygulamalarının Anayasamıza ve uluslararası sözleşmelerden kaynaklanan yükümlülüklerimize aykırı olduğu iddia edilebilir³³. Şöyle ki,

- Hükümlerde yer alan ifadelerin muğlak ve keyfi uygulamalara sebep olabilir nitelikte olması, hukuki belirlilik ilkelerinden uzak olması, idareyi yargı organı görev ve yetkileriyle donatması ve bu sayede yetki aşımına imkân vererek anayasal düzenin temeli olan erkler ayrılığını zedelemesi sebebiyle Anayasa'nın 2. Maddesi'ne aykırılık söz konusudur.
- Esas itibarı ile ancak toplumun tamamına yönelmiş, varlığını tehdit eden, gerçekleşmesi kesin bir tehdit karşısında, sadece bu tehdidi gidermeye yönelik olarak usul, içerik ve süresi sınırlandırılmış, kendisi ve uygulaması bağımsız yargı denetimine tabi olmasına gereken kanunla getirilebilecek bir önlem olan, erişim engelleme yetkilerinin kapsamı ve bu yetkilerin kullanılması bakımından yürütme organına tanınan geniş yetkiler sebebiyle, Anayasa'nın 5. Maddesi'nde yer alan "Devletin yükümlülüklerine" aykırı bir düzenlemedir.
- Birleşmiş Milletler Konseyi, Avrupa Birliği, Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkememiz tarafından dördüncü kuşak temel haklardan biri olarak kabul edilmiş ve artık ifade hürriyeti, basın hürriyeti, haber alma hürriyeti, haberleşme hürriyeti, iletişim hürriyeti ve ticari faaliyette bulunma hürriyetinin ayrılmaz bir unsurunu teşkil eden "İnternet'e erişim" hakkının sınırlandırma ölçütleri konusunda Anayasa'nın 13. Maddesi ihlal edilmiştir.
- İnternet'in ifade, basın, haber alma, haberleşme, iletişim ve ticari faaliyette bulunma hürriyetlerinin kullanılmasında günümüzde elzem, ikame edilemez ve en önemli araç özelliği teşkil etmesine ve bu durumun Türkiye'nin de üyesi olduğu uluslararası topluluklar tarafından kabul edilmesine rağmen erişim engelleme kararlarının tamamen idarenin takdirine tabi olarak keyfi, ölçüsüz ve orantısız kısıtlamalara tabi tutulması Anayasa'nın 22. ve 26. Maddeleri'ni ihlal etmektedir.
- Kanun ile düzenlenmiş ve cezai soruşturma gerekçesi gösterilen eylemlerin gerek Anayasa gerekse hukukun evrensel ilkeleri ile bağdaşmaması sebebiyle Anayasa'nın 36. ve 38. Maddeleri ihlal edilmiştir.
- Erişim engelleme kararlarına içeriği engellenen kişinin başvurabileceği etkili bir başvuru yolunun bulunmaması Anayasa'nın 40. Maddesi'ni ihlal etmektedir.
- Eklenmesi teklif edilen hükümler Anayasa Mahkemesi'nin 2 Ekim 2014 tarihli ve E.2014/149, K. 2014/151 sayılı kararıyla iptal edilen 5651 Sayılı Kanun'un milli güvenlik ve kamu düzeninin korunmasına dair gecikmesinde sakınca bulunan hallerde erişimin engellenmesine ilişkin Telekomünikasyon İletişim Başkanlığına keyfi uygulamalara yol açabilecek nitelikte ölçüsüz ve orantısız kısıtlama serbestisi tanıyan 8. Maddenin 16. Fıkrasında iptal edilmiş kanun maddesi ile özdeş ve hatta sınırları daha da genişletilmiş şekilde yetki düzenlemeleri içeren bir hüküm olması sebebi ile Anayasa Mahkemesi kararlarının bağlayıcı olması özelliğini düzenleyen Anayasa'nın 153. Maddesi'ni ihlal etmiştir.

³³ Ünsal, 5651 Sayılı Kanunda Yapılan Değişikliklerin Anayasaya Aykırılığına İlişkin Beyaz Rapor, CNNTürk.com, 15.04.2015, <http://www.cnntrk.com/haber/turkiye/Internet-yasasindaki-degisiklikler-anayasaya-aykiri-mi>

ARAMA MOTORLARI

Arama motoru kavramının kabul edilmiş standart bir tanımı olmasa da sade şekilde İnternet'te bilgi aramak için kullanılan bir yazılım sistemi olduğunu söyleyebiliriz. Dünyanın en çok kullanılan arama motoru olan Google üzerinden İnternet'te arama yapmak artık İngilizce'ye "to google" olarak giren bir fiille karşılanmakta³⁴, aynı fiil Türkçe'de de yerini bulmaktadır. Günümüz dünyasını arama motorları olmadan hayal etmek imkansızdır.

1960'lı yıllarda, en sonunda adına İnternet diyeceğimiz birbirleri ile iletişim içinde olan bilgisayarlardan oluşan geniş bir ağ kurma fikri ortaya çıkmış ve bu yönde çalışmalar başlamıştı³⁵.

1970'li yıllarda İnternet'in atası diyebileceğimiz ARPANET (Advanced Research Projects Agency Network) Amerika Birleşik Devletleri'nde esas itibarı ile askeri bir iletişim projesi olarak meydana çıkmış, 1980'lerin sonunda proje sivilleşmiştir³⁶. 1980'lerin başında birden fazla bilgisayar ağı var ise de bunların birbirleriyle iletişim içinde olarak veri iletmesi ortak protokol olmadığından kolay sağlanamamıştır. 1982 ABD Savunma Bakanlığı ortak protokol olarak Veri Kontrol Protokolü/İnternet Protokolü'nü (TCP/IP) tüm askeri bilgisayar ağının ortak protokolü kabul etmiş, 1985'te de İnternet Danışma Kurulu da TCP/IP'yi özel şirketlerin ticari kullanımına sokmak üzere harekete geçmiş ve ilk olarak IBM, DEC ve AT&T bu protokolü kullanmıştır.

Birbirlerine bağlı bilgisayarlardan oluşan ağlar da bu şekilde birbirlerine bağlanınca, bu geniş veri kaynağı içinde aranan spesifik bir verinin bulunması ihtiyacı sonucu ilk arama motorları doğmuştur. İlk arama motorları, daha doğrusu ilk veri listeleri (endeksleri) bizzat kişiler tarafından elle hazırlanmaktaydı.

İnternet üzerinde dosya iletim protokolü (FTP) arşivlerini listeleyen ilk arama motoru olan Archie, 90'lı yıllarda kullanılmaya başlanmıştır ve ancak "dosya ismi" ile arama yapabilen bir sistemdir³⁷.

İlk web sitesi ve world wide web (www) CERN'de HTML formatı kullanır biçimde geliştirilince İnternet sadece bilgisayar mühendislerinin değil, herkesin kullanımına açılmış oldu.

Bu durum 1990 ile 2000 arası bir çok arama motoru denemesini ortaya çıkardı. 1993'de Excite, 1995'te Alta Vista ve 1997'de Ask.com en çok hatırd kalanlar old. Bunlardan bir kısmı halka arz edildi ve iyi paralar kazandı. Yine bir kısmı dotcom balonu dediğimiz spekülasyon balonu olarak patladı.

2000 yılından itibaren Google, arama sonuçlarının doğruluğundan ve tamlığından daha öte geliştirdiği *page rank* yani öne çıkma veya üstte yer alma teknolojisi ile öne çıktı. Bu teknoloji tamamen matematik formüllere dayanan bir algoritmanın belli parametrelere göre daha iyi ve arzu edilebilen arama sonucunun listede daha üstte yer almasını sağlayan bir teknolojiydi.

Google ayrıca daha sade bir ara yüz geliştirdi. Yahoo gibi rakipleri, İntomi teknolojisi kullanıp, bir web portal olarak arama motorunu dizayn ederken Google sadece sade ve beyaz bir arayüz üzerinde bulunan sade bir arama çubuğunu (search bar) koyarak herşeyi çok basitleştirdi³⁸.

Microsoft da İntomi kullanırken bir süre sonra "msnbot" isminde kendi ağ tarama örümceklerini (web crawler) geliştirerek 2009'da arama motorunu Bing olarak yeniden markalaştırdı. Şu anda ise Yahoo da Microsoft teknolojisi ile hizmet vermektedir.

³⁴ <http://www.merriam-webster.com/dictionary/google>

³⁵ Abbate, *Inventing the Internet*, 1999

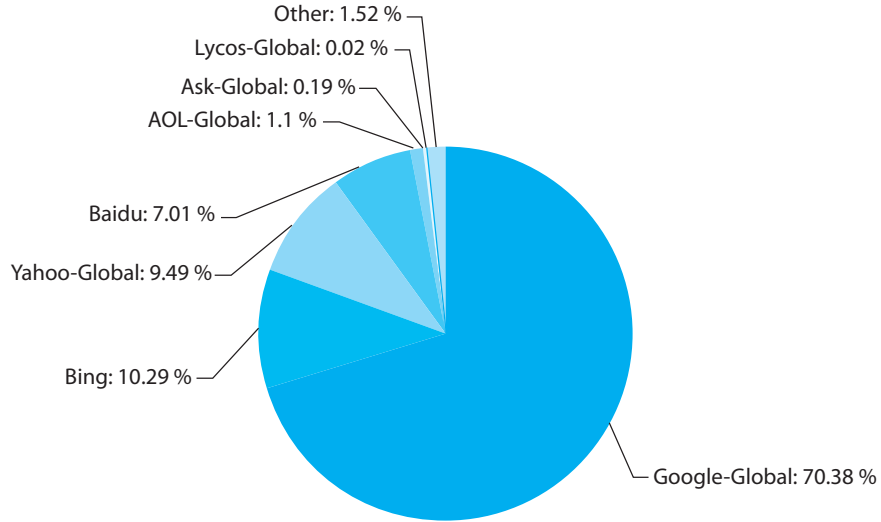
³⁶ Salus, *Casting the Internet, From ARPANET to İnternet*, 1995

³⁷ Books LLC, *İnternet Search Engines*, 2010

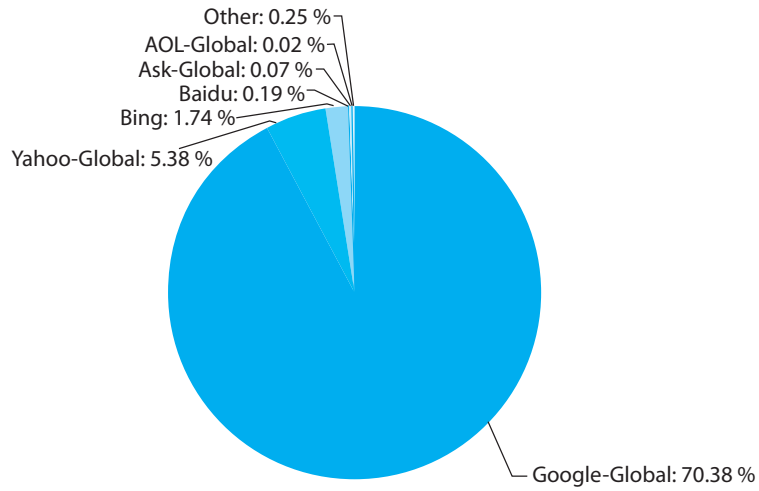
³⁸ Brin & Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, Computer Science Department, Stanford University, 1998

Bu teknoloji beraberinde bir takım etik ve hukuki sorunlar getirdi. Bunların en başında, arama motorlarının taraflı olup olmadığı, arama sonuçlarının manipüle edilip edilmediği, online (çevrimiçi) reklam stratejileri, aramaları etki altında bırakarak yönlendirmek, mahremiyet, kişisel verilerin istem dışı ifşası veya elde edilmesi, gözetlenme, takip edilme, izlenme, fikri mülkiyet ihlalleri, haksız fiil ve suçlar ile kişilik haklarına ve demokrasiye yönelen tehditler gelmektedir.

Temmuz 2015 itibarı ile masa üstü bilgisayarlarda pazar payının arama motorları arasındaki dağılımı aşağıdaki gibi iken,



mobil ve tabletlerde arama motorları pazar payları ise aşağıdaki gibidir³⁹:



Arama motorların uygulanacak esasa ve usule ilişkin hukuk ve bunların hukuki sorumlulukları, sadece ülkemizde değil tüm dünyada bir problemidir. Arama motorlarının diğer İnternet sùjelerinden farklılığı, yayıncı olarak kabul edilebilip edilemeyeceği, İnternet'te sağladığı hizmetin evsafı noktalarında fikir ayrılıkları olabilmektedir.

Biz, bu çalışmamızda arama motorlarının ülkemizde ve dünyada *unutulma hakkı* yönünden sorumluluğu üzerinde duracağız.

³⁹ <https://www.netmarketshare.com/>

UNUTULMA HAKKI

2006 senesinde Arjantin'de Google ve Yahoo aleyhine aralarında ünlü futbolcu Armando Diego Maradona, manken Yesica Toscanini'nin de bulunduğu çoğunluğu ünlü isimlerinden oluşan kişiler tarafından içerikten kaldırma talepli birbirine benzer en az 130 tane dava açılmıştır.

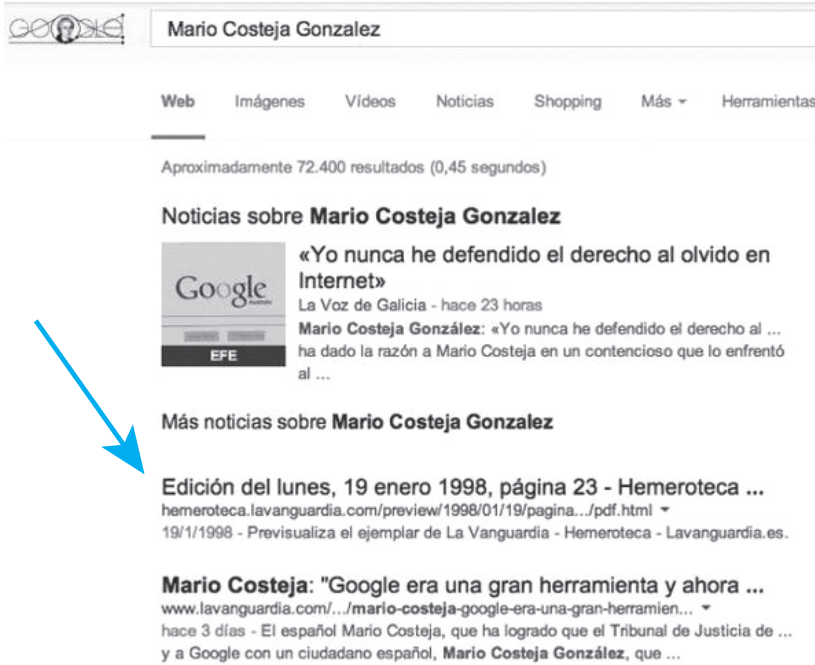
Pilot davada, birinci derece mahkeme, 2009 yılında Google ve Yahoo aleyhine, davacı Virginia Da Cunha ismi ile yer verilen cinsel, erotik ve pornografik içeriğin tahkir suçunu teşkil ettiğine, arama sonuçlarından kaldırılmasına ve tazminata hükmetmiştir.

Temyiz mahkemesi, 2010 yılında ilk derece mahkemenin bu kararını bozmuş ve arama motorlarının hukuka aykırı içerikten haber olmalarına rağmen, kaldırmakta ihmal göstermeleri hâlinde sorumlu tutulabileceği sonucuna varmıştır⁴⁰.

2013 senesinde Avrupa Birliği Genel Veri Koruma Yönetmeliği Teklifi ve Unutulma Hakkı'nın Kökleri isimli çalışmada⁴¹ unutulma hakkı talebinin ve ihtiyacının bireylerin geçmişte yaptıkları spesifik bir davranıştan ötürü, belli aralıklarla ve sürekli olarak yaf-talanmak zorunda kalmadan, hayatlarının gelişimini kendi iradeleriyle belirleyebilme arzusundan geleceği belirtilir. Ancak aşağıda açıklanacağı üzere "geçmişte olanlardan yaf-talanmama" arzusu çoğu zaman geçmişte ne olduğu ve bugün nasıl hatırlandığı veya hatırlanması gerektiği gibi sorularla karşı karşıya kalabileceği gibi haber alma, öğrenme ve ifade hürriyetleri ile de çelişebilir.

La Vanguardia isimli bir İspanyol gazetesi, diğer bir çok yayın, hatta kütüphane gibi eski sayılarını taratarak bir online arşiv kurmuş ve İnternet'te eski sayılar ve içeriği aran-dığında bulunabilmesi için gerekli etiketlemeleri yapmıştır.

Costeja Gonzales isimli İspanyol avukat, Google'da kendi ismiyle bir arama yaptığında La Vanguardia'nın 19 Ocak 1998 sayısının 23. Sayfında yer alan aşağıdaki arama sonucu ile karşılaşır⁴².



⁴⁰ Da Cunha v. Yahoo and Google, <http://law.emory.edu/eilr/content/volume-27/issue-1/recent-developments/argentinas-right-to-be-forgotten.html>

⁴¹ Mantelero, The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten', Computer Law & Security Review, s. 229 – 235.

⁴² <http://hemeroteca.lavanguardia.com/preview/1998/01/19/pagina-23/33842001/pdf.html>

Bu arama sonuçlarından ilgili olana tıkladığında ise kendisi hakkındaki aşağıdaki ilanı görür.

- **Les dues meitats indivises d'un habitatge al carrer Montseny, 8, propietat de MARIO COSTEJA GONZÁLEZ i ALICIA VARGAS COTS, respectivament. Superfície: 90 m². Càrregues: 8,5 milions de ptes. Tipus de subhasta: 2 milions de ptes. cadascuna de les meitats.**

Burada Gonzales'in borçlarını ödeyemediği için gayrimenkulünün açık artırma ile satılacağı yönünde, azami sayıda katılımcı sağlayabilmek amaçlı bir ilandır. Gonzales Kasım 2009'da La Vanguardia gazetesine başvurarak bu içeriğin kaldırılmasını talep eder ancak olumsuz yanıt alır.

12 yıl sonra böyle bir ilanın, kendi ismiyle yapılan bir arama sonucunda Google tarafından listelenmesini istemediğinden Şubat 2010'da Google İspanya'ya başvurarak söz konusu linkin arama sonucu listesinden çıkarılmasını talep eder. Google İspanya, talebi California merkezli Google Inc.'e gönderir ancak bir sonuç çıkmaz.

Bunun üzerine aynı sene (2010) İspanyol Ulusal Veri Koruma Kurulu'na başvurarak söz konusu sürecin çok uzun zaman önce tamamlanmış olduğunu, günümüz bakımından bir önemi, geçerliliği ve ilgisi kalmadığını, bu haberin arama sonuçlarında kalmasının kendi kişisel verisinin kendi saygınlığını gayrimakul şekilde haleldar ettiği iddia ederek hem gazeteyi hem de Google'ı şikayet eder.

30 Temmuz 2010'da Ulusal Veri Koruma Kurulu gazete hakkındaki içerik kaldırma talebini reddeder ancak Google hakkında ilgili linkin arama sonuçlarından çıkarılmasına ilişkin talebi kabul ederek Google'a bu yönde talimat verir.

Bunun üzerine Google İspanya ve Google Inc. karara karşı hukuk yollarına başvurarak İspanyol Ulusal Yüksek Mahkemesi nezdinde dava açar⁴³. Davasında, Google Inc.'in AB mevzuatına (EU Directive 95/46/EC, Veri Koruma Yönetmeliği) tabi olmadığını, kendi iştiraki olan Google İspanya'nın ise arama motoru hizmeti vermediğini ve bu faaliyet ile ilgisiz olduğu iddia eder. Ayrıca arama motoru hizmeti çerçevesinde veri işleme söz konusu olmadığını, Google Inc.'in ve Google İspanya'nın veriyi kontrol etme durumu ve sıfatı bulunmadığını, Gonzales'in de hukuka uygun olarak yapılmış bir yayına erişimi engelleme hakkı bulunmadığını iddia eder.

İspanyol Yüksek Mahkemesi, AB Veri Koruma Yönetmeliği'nin yetkisel uygulama alanının ne olduğunun belirlenmesi bir arama motorunun Yönetmelik çerçevesinde sorumluluğunun ne olduğunun belirlenmesi, ve Yönetmeliğin bir unutulma hakkı bahşedip bahşetmediğinin belirlenmesi amacıyla uyuşmazlığı Avrupa Adalet Divanı'na sevkeder.

13 Mayıs 2014 tarihinde Avrupa Adalet Divanı aşağıdaki şekilde karar verir⁴⁴:

AB Mevzuatının uygulama alanı bakımından: Bir şirketin sunucuları AB sınırları dışında olsa dahi, o şirketin AB üyesi ülkeler dahilinde arama motorunun sunduğu reklam alanını pazarlayan bir şubesi veya iştiraki varsa, AB mevzuatı söz konusu arama motoruna uygulanır.

AB Veri Koruma Yönetmeliği'nin bir arama motoruna uygulanıp uygulanmayacağı bakımından: Arama motorları şahsi veriyi kontrol eder ve elinde tutar pozisyonadadır. Bu sebeple arama motorları, AB Veri Koruma Yönetmeliği ve unutulma hakkı bakımından sorumludur.

⁴³ Google Spain S.L. and Google Inc. v Agencia Española de Protección de Datos, C – 131/12

⁴⁴ http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

Unutulma hakkı bakımından: Bireyler belli şartlara tabi olmak kaydı ile arama motorlarından şahsi verilerinin arama sonuçlarından çıkarılmasını talep edebilir. Arama sonuçlarından çıkarılması talep edilebilecek şahsi verinin hatalı, yetersiz, geçersiz veya aşırı ve ölçüsüz olması veya o hale gelmiş olması gerekir.

Adalet Divanı, unutulma hakkının mutlak olmadığını ve diğer temel hakların üzerinde olmadığını, tam tersine, ancak ifade ve basın özgürlükleri karşısında bir teraziye konarak dengesinin gözetilmesi gerektiğine hükmetmiştir. Bu dengenin her olayda ayrı ayrı gözetilmesi gerektiği ve münferit dava adaletinin tesis edilmesi gerektiğine karar vermiştir. İlgili şahsi verinin saklanması neredeyse “gereksiz” olduğu durumlar için geçerli olabileceği açıklanmıştır⁴⁵.

Adalet Divanı kararı ile birlikte ortaya çıkabilecek yanlış anlaşılımları ve belirsizlikleri gidermek için bir de basın bildirisi yayınlamış⁴⁶ ve kararına temel teşkil eden kriterlerin üzerinden geçmiş, arama motorlarının bu tür içerikten çıkarma talepleri alması hâlinde nasıl bir denetleme yapması gerektiğine ilişkin de yol göstermeye çalışmıştır.

Söz konusu karar okyanus ötesinde büyük yankı uyandırmış ve önemli bir tartışmaya sebebiyet vermiştir. Google, karardan hemen sonra, bu çerçevede başvuru yapmak isteyen kullanıcılar için bir başvuru sistemi ve formu hazırlamış ve devreye sokmuştur⁴⁷. Bu imkandan 28 AB ülkesi⁴⁸ ve AB üyesi olmayan İzlanda, Norveç, İsviçre ve Liechtenstein faydalanabilmektedir. Ülkemiz bu imkandan faydalanamamaktadır.

Search removal request under European Data Protection law

You will need a copy of a valid form of photo ID to complete this form. Fields marked with an asterisk * must be completed for your form to be submitted.



We're working to finalize our implementation of removal requests under European data protection law as soon as possible. In the meantime, please fill out the form below and we will notify you when we start processing your request. We appreciate your patience.

Please select the country whose law applies to your request *

Please select one

Your information

Name *

The full name for which you are requesting search results to be removed

Your name ?

Your own name, if different

Your relationship to the person you represent, if not yourself (for example: "spouse" or "attorney")

Contact email address *

(where confirmation email will be sent)

Links associated with your name that you want removed

For us to evaluate your request, you must:

(a) Provide the URL for each link appearing in a Google search for your name that you request to be removed. (The URL can be taken from your browser bar after clicking on the search result in question).

(b) Explain, if not clear, why the linked page is about you (or, if you are submitting this form on behalf of someone else, the person named above).

(c) Explain how this URL in search results is irrelevant, outdated, or otherwise inappropriate

URLs you want removed *

⁴⁵ Avrupa Komisyonu, C-131/12 Unutulma Hakkı Kararı Bilgi Formu, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

⁴⁶ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf>

⁴⁷ https://support.google.com/legal/contact/lr_eudpa?product=websearch

⁴⁸ http://europa.eu/about-eu/countries/member-countries/index_en.htm

Karar çıktıktan sonraki iki yıl Google, unutulma hakkı başvurularının çoğunluğunun yolsuzluk, çocuk pornografisi veya çocuk istismarı gibi suçlardan hüküm giyenlerin buna ilişkin haberleri arama sonuçlarından çıkarmak için yaptığını iddia etse de Google Temmuz 2015'te yanlışlıkla unutulma hakkı taleplerine ilişkin verileri dışarı sızdırmış ve yapılan 220 bin başvurunun sadece %5'inin bu mahiyette içeriklere ilişkin olduğu, %95'inin ise toplumdaki normal vatandaşların kendi şahsi verilerine ilişkin olduğu ortaya çıkmıştır⁴⁹.

Google yapılan başvuruları aşağıdaki şekilde kategorize etmiştir:

Mayıs 2014, Mart 2015 arası alınan başvuru: 218,320. %95,6'sı "şahsi/mahrem". Bunların %48'i kabul edilmiş, %37'si reddedilmiş. Kalanı ile ilgili inceleme devam ediyor.

Başvurusu reddedilen kişiler, ülkesinin yetkili mahkemesinden içeriğin çıkarılmasını talep edebilmektedir.

Google, bir talebi kabul ettiğinde söz konusu sonuç tüm dünyada geçerli global arama sonuçlarından çıkacak anlamına gelmemektedir. Tam tersine Google, ülkesel IP kısıtlamaları teknikleri uygulayarak çıkarılması talep edilen içeriği sadece talebin geldiği ülkede görünmeyecek şekilde sınırlandırmaktadır.

Karar, Twitter'ı da etkiliyor ve bu yazı kaleme alınmadan sadece iki gün önce Politwoops isimli siyasilerin sildikleri eski tweetlerini ulaşılabilir kılan hesabı kapatmıştır⁵⁰.

Twitter ayrıca, 17 Nisan 2015⁵¹'te açıkladığı ve 18 Mayıs 2015'te yürürlüğe giren bir ilke değişikliği ile hesapları, ABD hesabı ve ABD harici hesaplar olmak üzere iki farklı sisteme uygun olarak yöneteceğini açıklamıştır. Bu değişiklikler çok moda haline gelen Persicope için de söz konusudur.

Buna göre ABD'de yaşayanların hesapları San Francisco'da bulunan Twitter Inc. tarafından, ABD harici ülkelerde yaşayanların hesapları ise Dublin'de bulunan Twitter International tarafından yönetilecektir.

Bu ilke değişikliği, Twitter'ın, yukarıda da değindiğimiz, Ekim 2014'te ABD Federal Hükümetinin hesap ve kullanıcı bilgi taleplerinin ABD Anayasası'na aykırı olduğu gerekçesi ile New York'ta dava etmesinden sonra çok daha fazla anlam kazanmıştır.

ABD'de yaşayanların hesapları, NSA'nın (Milli Güvenlik Kurumu) ve mevzuatının etkili olduğu kararları çıkaran ABD mahkemelerine ve ABD hukukuna tabi olacaktır. Ancak ABD'de bulunmayanların hesapları İrlanda şirketi tarafından yönetilecek, veriler İrlanda'da saklanacak ve AB mevzuatına ve İrlanda Veri Koruma Kurumu'nun düzenlemelerine tabi olacaktır.

Burada herkesin gözden kaçırdığı en önemli nokta ise bu değişiklik sayesinde ABD mahkemelerinin ve makamlarının ABD'de olmayanların hesapları hakkında talep ettiği bilgi ve verdiği kararlar bakımından Twitter'ın bu talep ve kararlara uymaktan imtina edebilecek olmasıdır. Bundan sonra ABD makamları, ABD'li olmayan hesaplar bakımından kendi kanunlarını ancak uluslararası anlaşmaların izin verdiği usul ve esaslar çerçevesinde uygulatabildiği kadar uygulatacaktır.

Bu değişikliğin reklam ilkeleri bakımından da Twitter'ın hem leyhine, hem de aleyhine olabilecek bazı sonuçları da olabilecektir. AB içinde nisbeten daha gevşek mahremiyet düzenlemeleri olduğu bilinen İrlanda dijital pazarlama bakımından avantajlı olabilse de reklam ilkeleri bakımından AB mevzuatı, ABD'ye göre daha muhafazakar sayılabilir. Bu arada belirtmekte fayda var ki, İrlanda, Veri Koruma Kurumu'nun bütçesini 1,9 milyon Avro'dan, 3,85 milyon Avro'ya çıkardı ve yeni bir veri koruma ve mahremiyet düzenlemesi yapmaktadır. Bunu da İrlanda'nın kendisini baz olarak kullanan Twitter, Facebook, Google gibi şirketlerin mahremiyet politikalarını daha yakından takip edeceği şeklinde yorumlamaktayız⁵².

⁴⁹ <http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests>

⁵⁰ <http://fortune.com/2015/08/24/twitter-right-to-be-forgotten/>

⁵¹ <https://support.twitter.com/articles/20172527>

⁵² Twitter'ın 21 Nisan 2015'te ilan ettiği bir diğer ilke değişikliği de Twitter'ın istismara karşı açtığı savaşın bir sonucudur. Twitter, kullanıcıların en güvendiği, mutlu olduğu ve emniyette olduğu dijital platform olmak istemektedir. Bu sebeple bundan sonra seri olarak alacağı ilk tedbir olarak doğrudan şiddet ve tehdit söylemi yasağına, şiddeti ve tehdidi kışkırtacak, teşvik edecek söylemleri yasaklamayı eklemek olmuştur.

Ülkemizdeki duruma geçmeden önce bir cümleyle belirtelimki yukarıdaki açıklamalardan da görülebileceği gibi unutulma hakkı ve bu çerçevede şirketlerin attığı adımlar sadece AB bölgesi içindir ve bu zorunluluklar veya hassasiyetler, ifade ve basın hürriyetinin mutlak olduğu ve unutulma hakkı şeklinde formüle edilen beklentiye çok ağır bastığı Amerika Birleşik Devletleri için geçerli değildir⁵³.

Unutulma hakkı bakımından, şu ana kadar incelediğimiz anlamıyla bir Türk Yargı kararına rastlamış olmasak da Yargıtay 4. Hukuk Dairesi'nin 3 Temmuz 2013 tarihli E:2013/6256, K:12821 sayılı kararını bu çerçevede incelemek mümkündür⁵⁴.

Buna göre, bir kitapta, cinsel suça ilişkin Yargıtay incelemesine konu olmuş bir uyuşmazlığa yer verilirken, suçun mağduru olduğunu iddia eden şahsın ismi alenen yazılmış, ismi yazılan şahıs konunun hassasiyeti sebebiyle ismi kodlanması gerekirken açıkça yazılmış olmasından bahisle kişilik haklarının ihlal edildiğini iddia ederek tazminat talep etmiştir.

Talebi kısmen kabul eden Asliye Hukuk Mahkemesinin kararını, Yargıtay 4. Hukuk Dairesi kitabın bilimsel eser olduğu, içeriğin bilimsel özgürlük alanında kaldığı, karar aleniyet kazandığından kişilik haklarına saldırı teşkil etmeyeceği gerekçesiyle kararın bozulmasına karar vermiştir. Temyiz kararının düzeltilmesi talebi de oy çokluğu ile reddedilmiştir.

Burada gerek karşı oy yazısı, gerekse makale sahibinin üzerinde durduğu gibi, kişinin ismi bireysel verisidir. Yargılama aleni yapılmış olsa da bilimsel bir kitapta yer alan yargı kararı incelemesinde, kişinin isminin yazılması hiçbir menfaat sağlamadığı gibi, güdülen amaca da hizmet etmez, ilgisiz ve geçersizdir. Kaldı ki, cinsel saldırı mağduru olma kavramı çerçevesinde, özellikle içerik dijitalize edilip İnternet üzerinden ulaşılabilir kılınması halinde, mağdur bakımından “sürekli ve düzenli aralıklarla tekrar eden bir yaftalamaya” sebebiyet verebilecek mahiyettedir.

Ülkemizde henüz veri korumasına ilişkin spesifik bir kanun ve buna bağlı tali mevzuat olmadığından, konu çeşitli mevzuat parçaları içinde ayrıışık biçimde bazen genel hükümlerle, bazen de özel hükümlerle düzenlenmeye çalışıldığından, başta Amerika Birleşik Devletleri ve Avrupa Birliği içindeki mevzuat ve içtihat gelişmeleri, tarafı olduğumuz bağlayıcı uluslararası sözleşmeler, Anayasamız ve yasalarımız çerçevesinde incelenerek, teknolojinin baş döndürücü ilerleme hızıyla ortaya çıkabilecek durumları karşılayabilecek nitelikte yasama faaliyetleri yapmamızın mümkün olabileceğini, doğru ve vizyoner uygulama ve içtihatlarla bu çabayı yaşatabileceğimizi düşünüyoruz.

⁵³ Gates v. Discovery Communications, California Supreme Court, S115008, 06.12.2004 ve diğer kararlar <https://cei.org/blog/european-right-be-forgotten-eats-free-speech-rights-google-and-its-users-rights-too>

⁵⁴ Akgül, TBB Dergisi 2016 (116), s. 11 – 38

Özet

Temel hak ve hürriyetler, kısaca insan olarak doğmakla elde edilen, anayasa tarafından tanınarak güvence altına alınmış ve aynı zamanda devletin temel organlarının yetkilerinin de sınırını oluşturmakla yasama ve yürütme tarafından keyfi biçimde ortadan kaldırılamayacak olan haklardır.

Temel hak ve hürriyetlerin sınırlandırılması ancak aşağıdaki unsurlar dahilinde ve bunlara uygun olarak yapılabilir: Savaş, sıkı yönetim, seferberlik, olağanüstü hâl gibi mutlak gerektirici ve yakın bir tehdit bulunmalıdır. Sınırlama söz konusu tehdidi giderme amaçlı olmalı ve bu amaçla orantılı bir sınırlama yapılmalıdır. Sınırlama kanunla yapılmalı ve sınırlamanın çerçevesi amaç, araç ve süre bakımından belirlenmelidir. Bu şekilde belirlenen sınırlama, amacını aşmamalı ve amacı dışında kullanılmamalıdır.

Keyfi olarak Internet sitesi veya içerik blokla ve filtreleme adli veya tamamen bağımsız düzenleyici makam tarafından kanuni sınırlamalara uygun olarak yapılmalıdır. Şahsi yorumuna göre düzenleyici kurumun bu yetkisi ani blokla veya filtreleme için yargılamayı gerektiren haller dışındaki çocuk pornosu, dolandırıcılık ve terör suçları gibi zararın çok büyük ve hukuk ihlalinin çok açık olduğu hallerle sınırlı olmalıdır. Meşru fikir ve ifade hürriyeti kullanımları ceza hukuku kapsamından çıkarılmalıdır. Hizmet sağlayıcılara gayri makul sorumluluklar yüklenmemelidir. Internet hizmet sağlayıcıları dediğimiz, erişim sağlayıcılara ve hizmet sağlayıcılara, Internetteki içeriği kendileri sağlıyormuşçasına hukuki ve cezai sorumluluklar yüklenmekte ve bu sorumluluklar çerçevesinde hizmet sağlayıcıların yöneticileri cezai sorumlulukla yargılanmakta veya hukuki sorumluluklar ve idari cezalar söz konusu olabilmektedir. Yetersiz mahremiyet ve gizli bilgi koruması da sıkıntılı bir başka meseledir. Hâlbuki mahremiyet de bir insan hakkıdır. Ne yazık ki kişisel bilgiler, hassas bilgiler, gizli bilgiler, tıbbi bilgiler, ticari sırlar gibi hususlar ve bunların saklanması ile korunmasına ilişkin ülkemizde spesifik düzenlemeler bulunmamaktadır. Bu da sadece Internet ve temel haklar bakımından değil her bakımdan büyük sorunlar yaratmaktadır. Devletlerin veya şirketlerin, kişilerin Internet veya sair araçlar üzerinden yaptıkları veri alış verişini gözetlemeleri ve kullanmaları, trafik bilgilerinin tespiti gibi hususlar tüm dünyada ortak bir sorundur.

Ülkemizde, Internet Kanunu olarak bilinen 5651 Sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da, MİT Kanunu'nda, HSYK Kanunu'nda ve en son 10 Eylül 2014 tarihinde yasalaşan 6552 Sayılı Torba Kanun içinde 5651 Sayılı Kanun'da yapılan değişikliklerle, "geliştirmeler" yapılmıştır.

Arama motoru kavramının kabul edilmiş standart bir tanımı olmasa da, sade şekilde Internet'te bilgi aramak için kullanılan bir yazılım sistemi olduğunu söyleyebiliriz. Bu teknoloji beraberinde bir takım etik ve hukuki sorunlar getirdi. Bunların en başında, arama motorlarının taraflı olup olmadığı, arama sonuçlarının manipüle edilip edilmediği, online (çevrimiçi) reklam stratejileri, aramaları etki altında bırakarak yönlendirmek, mahremiyet, kişisel verilerin istem dışı ifşası veya elde edilmesi, gözetlenme, takip edilme, izlenme, fikri mülkiyet ihlalleri, haksız fiil ve suçlar ile kişilik haklarına ve demokrasiye yönelen tehditler gelmektedir. Arama motorlarının uygulanacak esasa ve usule ilişkin hukuk ve bunların hukuki sorumlulukları, sadece ülkemizde değil tüm dünyada bir problemdir. Arama motorlarının diğer Internet süjelerinden farklılığı, yayıncı olarak kabul edilebilip edilemeyeceği, Internette sağladığı hizmetin vasıfları noktalarında fikir ayrılıkları olabilmektedir.

Unutulma hakkı bakımından: Bireyler belli şartlara tabi olmak kaydı ile arama motorlarından şahsi verilerinin arama sonuçlarından çıkarılmasını talep edebilir. Arama sonuçlarından çıkarılması talep edilebilecek şahsi verinin hatalı, yetersiz, geçersiz veya aşırı ve ölçüsüz olması veya o hale gelmiş olması gerekir. Avrupa Adalet Divanı, unutulma hakkının mutlak olmadığını ve diğer temel hakların üzerinde olmadığını, tam tersine, ancak ifade ve basın özgürlükleri karşısında bir teraziye konarak dengesinin gözetilmesi gerektiğine hükmetmiştir. Bu dengenin her olayda ayrı ayrı gözetilmesi gerektiği ve münferit dava adaletinin tesis edilmesi gerektiğine karar vermiştir. İlgili şahsi verinin saklanmasıyla neredeyse "gereksiz" olduğu durumlar için geçerli olabileceği açıklanmıştır. Avrupa Adalet Divanı kararı ile birlikte ortaya çıkabilecek yanlış anlaşılımları ve belirsizlikleri gidermek için bir de basın bildirisi yayınlamış ve kararına temel teşkil eden kriterlerin üzerinden geçmiş, arama motorlarının bu tür içerikten çıkarma talepleri alması halinde nasıl bir denetleme yapması gerektiğine ilişkin de yol göstermeye çalışmıştır.

Kendimizi Sınavalım

1. “İnsan olarak doğmakla elde edilen, anayasa tarafından tanınarak güvence altına alınmış ve aynı zamanda devletin temel organlarının yetkilerinin de sınırını oluşturan” haklara ne ad verilir?
 - a. Temel Hak ve Hürriyetler
 - b. Sosyal Haklar
 - c. Mülkiyet Hakkı
 - d. Unutulma Hakkı
 - e. Özel Hayatın Gizliliği Hakkı
2. Aşağıdaki hukuk metinlerinden hangisi doğrudan temel insan haklarıyla ilgilidir?
 - a. Magna Carta
 - b. İnsan Hakları Evrensel Beyannamesi
 - c. Türkiye Cumhuriyeti Anayasası
 - d. Hukuk Muhakemeleri Kanunu
 - e. Avrupa Birliği Temel Haklar Bildirgesi
3. Aşağıdakilerden hangisi “birinci kuşak haklar”dan biri **değildir**?
 - a. Vücut Bütünlüğü
 - b. Konut Dokunulmazlığı
 - c. Düşünce Hürriyeti
 - d. Yazardan istenebilir
 - e. İnternete Erişim Hakkı
4. Temel hak ve hürriyetlerin kısıtlanması ile ilgili aşağıdaki ifadelerden hangisi doğrudur?
 - a. Savaş bir kısıtlama nedeni değildir.
 - b. Sıkıyönetim bir kısıtlama nedeni değildir.
 - c. Sınırlama ancak kanunla gerçekleştirilmelidir.
 - d. Seferberlik bir sınırlama nedeni değildir.
 - e. Sınırlama söz konusu ise ilgili hak tamamen ortadan kaldırılabılır, sınırlamanın sınırlandırılması öngörülmemiştir.
5. Temel hak ve hürriyetlerin sınırlandırılması hakkındaki aşağıdaki ifadelerden hangisi **yanlıştır**?
 - a. Savaş ve olağanüstü hallerde dahi kimse düşünce ve kanaatlerinden ötürü suçlanamaz.
 - b. Sınırlama amacını aşmamalı ve amacı dışında kullanılmamalıdır.
 - c. Sınırlamalar demokratik toplum düzeninin gereklerine aykırı olamaz.
 - d. Sınırlamalar söz konusu olduğunda uluslararası huktan kaynaklanan yükümlülükler ihlal edilebilir.
 - e. Sınırlama ancak belli tehdit veya tehditleri giderme amaçlı olmalı ve bu amaçla orantılı bir sınırlama yapılmalıdır.
6. İnternete erişim hakkı ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?
 - a. Fikir ve ifade hürriyeti ile bağlantısı olan bir haktır.
 - b. Hak olduğu kadar temel bir insan ihtiyacı olarak da tanımlanmaktadır.
 - c. Cinsiyete bağlı olarak sınırlandırılması mümkün olan bir haktır.
 - d. Bilgiye ulaşma kadar bilgi yaratma ile de yakından ilişkili bir haktır.
 - e. Bilgiye ulaşma kadar bilgiyi paylaşma ile de yakından ilişkili bir haktır.
7. Türkiye’deki İnternet ve İnternete ilişkin mevzuat hakkında aşağıdakilerden hangisi **söylenemez**?
 - a. Ülkemizde şimdiye kadar bir “Ulusal Siber Güvenlik Stratejisi” hazırlanmış değildir.
 - b. 2013-2014 Eylem Planı’na göre mücadele edilmesi gereken, anonimlik ve inkâr edilebilirlik gibi zaafılar söz konusudur.
 - c. Siber Güvenlik alanında koordinasyon eksikliği tespit edilmiştir.
 - d. Siber olayların delilendirilmesinde MİT, Jandarma, Emniyet Genel Müdürlüğü gibi kuruluşlar sorumlu olarak belirlenmiştir.
 - e. Konuyla ilgili olarak 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hazırlanmıştır.
8. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile ilgili aşağıdaki ifadelerden hangisi **yanlıştır**?
 - a. Bu Kanun ile İnternet üzerinden işlenen suçlarla mücadele konusunda özel hüküm getirilmesi amaçlanmıştır.
 - b. Bu Kanun ile Avrupa Birliği mevzuatı ile uyum sağlanması hedeflenmiştir.
 - c. Kanun’un uygulanmasında mahkemeden mahkemeye farklılık gözlenmemiş, istikrarlı bir uygulama geliştirilebilmiştir.
 - d. Söz konusu Kanun’un 8. Maddesi AİHM tarafından Avrupa İnsan Hakları Sözleşmesi’nin 10 maddesine aykırı bulunmuştur.
 - e. Kanun’un uygulanması sırasında ifade hürriyeti gibi bazı temel hakların sınırlandırıldığı gözlenmiştir.

9. “İnternet’te bilgi aramak için kullanılan yazılım sistemi”ne ne ad verilir?

- Blog
- Web Sayfası
- Bilişim Sistemi
- Virüs Programı
- Arama motoru

10. Unutulma hakkı ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

- Hiçbir uluslararası, ulus-üstü veya ulusal metinde düzenlenmemiştir.
- Böyle bir hak mevcut değildir.
- Arama motorları tarafından ihlal edilmesi mümkün olmayan bir haktır.
- Avrupa Adalet Divanı kararı gereği, arama motorlarının da koruması şart olan bir haktır.
- Google bu hakkı tanımayı reddetmiştir.

Kendimizi Sınavalım Yanıt Anahtarı

1. a	Yanıtınız yanlış ise “Temel Hak ve Hürriyetler” konusunu yeniden gözden geçiriniz.
2. c	Yanıtınız yanlış ise “Temel Hak ve Hürriyetler” konusunu yeniden gözden geçiriniz.
3. e	Yanıtınız yanlış ise “Temel Hak ve Hürriyetler” konusunu yeniden gözden geçiriniz.
4. c	Yanıtınız yanlış ise “Temel Hak ve Hürriyetlerin Sınırlandırılması” konusunu yeniden gözden geçiriniz.
5. d	Yanıtınız yanlış ise “Temel Hak ve Hürriyetlerin Sınırlandırılması” konusunu yeniden gözden geçiriniz.
6. c	Yanıtınız yanlış ise “Temel Hak Olarak İnternet Erişimi” konusunu yeniden gözden geçiriniz.
7. a	Yanıtınız yanlış ise “Ülkemizde İnternet” konusunu yeniden gözden geçiriniz.
8. c	Yanıtınız yanlış ise “Ülkemizde İnternet” konusunu yeniden gözden geçiriniz.
9. e	Yanıtınız yanlış ise “Arama Motorları” konusunu yeniden gözden geçiriniz.
10. d	Yanıtınız yanlış ise “Unutulma Hakkı” konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Temel hak ve hürriyetlerin en önemli niteliklerinden biri prensip olarak dokunulmaz olmasıdır. Yani, temel hak ve hürriyetlerin sınırlandırılması ancak aşağıdaki unsurlar dahilinde ve bunlara uygun olarak yapılabilir:

1. Savaş, sıkı yönetim, seferberlik, olağanüstü hâl gibi mutlak gerektirici ve yakın bir tehdit bulunmalıdır.
2. Sınırlama söz konusu tehdidi giderme amaçlı olmalı ve bu amaçla orantılı bir sınırlama yapılmalıdır.
3. Sınırlama kanunla yapılmalı ve sınırlamanın çerçevesi amaç, araç ve süre bakımından belirlenmelidir.
4. Bu şekilde belirlenen sınırlama, amacını aşmamalı ve amacı dışında kullanılmamalıdır.

2001 yılında Anayasa’da yapılan bir değişiklikle temel hak ve hürriyetlerin kamu güvenliği, ülkenin bölünmez bütünlüğü, özel hayatın ve meslek sırlarının korunması gibi amaçlarla da sınırlandırılacağına ilişkin bir hüküm getirilmiştir.

Yararlanılan Kaynaklar

- AKGÜL, Aydın. “Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın Google Kararı, *Türkiye Barolar Birliği Dergisi*, Sayı 116.
- Birleşmiş Milletler Genel Kurulu İnsan Hakları Komisyonu, Fikir ve İfade Özgürlüğünün Korunması ve Geliştirilmesi Üzerine Özer Raportör Raporu, A/HRC/17/27, 16.05.2011 http://www2.ohchr.org/english/bodies/hrco-uncil/docs/17session/A.HRC.17.27_en.pdf.
- GÖZLER, Kemal. *Anayasa Hukukunun Genel Teorisi*, Ekin Yayınevi, Bursa 2011, 2 Cilt.
- KAPANİ, Münci. *Kamu Hürriyetleri*, Yetkin Yayınları, Ankara 2007.