T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU PROGRAMI
YÜKSEK LİSANS TEZİ

SOSYAL MEDYADA PAYLAŞILAN VERİLERİN CEZA HUKUKU YOLUYLA KORUNMASI

Dilara ALGÜL

Danışman
Dr. Öğretim Üyesi Pınar BACAKSIZ

İZMİR-2022

TEZ ONAY SAYFASI

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Sosyal Medyada Paylaşılan Verilerin Ceza Hukuku Yoluyla Korunması” adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

02/02/2022

Dilara ALGÜL

ÖZET

Yüksek Lisans Tezi

Sosyal Medyada Paylaşılan Verilerin Ceza Hukuku Yoluyla Korunması

Dilara ALGÜL

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

Kamu Hukuku Anabilim Dalı

Kamu Hukuku Programı

Çalışmamızın konusu günümüzde birçok kişi için vazgeçilmez hale gelen sosyal medya olmuştur. Sosyal medyanın yaygınlaşması ve milyonların bu platformlara olan ilgilisinin gün geçtikçe artması sosyal medyada paylaşılan verilerin nasıl korunması gerektiği sorusunu ortaya çıkarmıştır. Meydana gelen insan hakları ihlallerin hukuki ve cezai sonuçları ise ulusal ve uluslararası düzenlemelerle tayin edilmeye çalışılmaktadır.

Çalışmamızın birinci bölümünde öncelikle sosyal medyaya ve kişisel verilere ilişkin temel kavramları ele alınmıştır. Günümüzde sosyal medyaya ilişkin terimlerin değiştiği ve bu terimlerin yerlerini farklı terimlerin aldığı görülmektedir. Bu sebeple kavramsal açıklamalar çalışmamızın hangi durumlar ve tanımlamalar altında yapıldığının tespiti açısından gereklidir.

İkinci bölümde ise uluslararası ve ulusal düzenlemeler ele alınmıştır. Uluslararası düzenlemelerden Avrupa Birliği Yönergeleri ve Avrupa Birliği Genel Veri Koruma Tüzüğü ulusal mevzuatımızın şekillendirilmesinde esas alınan kaynaklardandır. Ulusal düzenlemelerimiz Kişisel Verilerin Korunması Kanunu ve 5651 sayılı Kanun (Sosyal Medya Kanunu olarak adlandırılan 7253 sayılı Kanun Değişiklikleri) çalışmamızda önemle üzerinde durduğumuz hususlardır. Çalışmamızda sosyal medyada gerçekleştirilen hukuka aykırı eylemler Türk Ceza Kanunu 135 ve 136. maddelerinde yer alan suç tiplerine uygunluk açısından ele alınmıştır. Bu kısımda sosyal medya da işlenen suçlar ve paylaşılan kişisel verilerin korunmasına ilişkin yargı kararlarına yer verilmeye

çalışılmıştır. Çocukların kişisel verilerinin korunması konusunda da ayrıca bir değerlendirme yapılmıştır.

Anahtar Kelimeler: İnternet, Sosyal Medya, Sosyal Medya Süjeleri ve Yükümlülükleri, Veri, Kişisel Verilerin Korunması, Ceza Hukukunda Kişisel Verilerin Korunması, Çocukların Kişisel Verilerinin Korunması, Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu, Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu.

ABSTRACT

Master's Thesis

Protection of Data Shared on Social Media Through Criminal Law

Dilara ALGÜL

Dokuz Eylül University

Graduate School of Social Sciences

Department of Public Law

Public Law Program

The subject of our study has been social media, which has become indispensable for many people today. The spread of social media and the increasing interest of millions in these platforms day by day have revealed the question of how the data shared on social media should be protected. The legal and criminal consequences of human rights violations are tried to be determined by national and international regulations.

In the first part of our study, first of all, the basic concepts of social media and personal data are discussed. Today, it is seen that the terms related to social media have changed and these terms have been replaced by different terms. For this reason, conceptual explanations are necessary in order to determine under which conditions and definitions our study was conducted.

In the second part, international and national regulations are discussed. Among the international regulations, the European Union Directives and the General Data Protection Regulation of the European Union are in the shaping of our national legislation. Our national regulations, the Law on the Protection of Personal Data and the Law No. 5651 (Law Amendments No. 7253, called the Social Media Law) are the issues we focus on in our work. In our study, unlawful actions on social media are discussed in terms of compliance with the types of crimes in the 135 and 136 articles of the Turkish Penal Code. In this section, the crimes committed in social media and the judicial decisions on the protection of shared personal data are tried to be included. An evaluation has also been made on the protection of children's personal data.

Keywords: Internet, Social Media, Social Media Subjects and Obligations, Data, Protection of Personal Data, Protection of Personal Data in Criminal Law, Protection of Personal Data of Children, The Crime of Unlawful Recording of Personal Data, The Crime of Unlawfully Giving or Obtaining Personal Data.

SOSYAL MEDYADA PAYLAŞILAN VERİLERİN CEZA HUKUKU YOLUYLA KORUNMASI

İÇİNDEKİLER

TEZ ONAY SAYFASI ii
YEMİN METNİ iii
ÖZET iv
ABSTRACT vi
İÇİNDEKİLER viii
KISALTMALAR xiii
TABLOLAR LİSTESİ xiv

GİRİŞ 1

BİRİNCİ BÖLÜM
SOSYAL MEDYA VE KİŞİSEL VERİ KONUSUNDA TEMEL KAVRAM VE İLKELER

I. SOSYAL MEDYA 5
A. Sosyal Medya Kavramı 5
1. Genel Olarak Sosyal Medya Kavramı ve Sosyal Medyanın Özellikleri 5
a. Erişilebilirlik 8
b. Kullanıcı/Katılımcı 8
c. İnteraktif Paylaşım, Etkileşim ve İçerik 9
d. İletişim 10
2. Sosyal Medyanın Bileşenleri 12
a. Sosyal Ağlar 12
b. Fotoğraf, Ses ve Video Paylaşım Siteleri 14
c. Bloglar 15
d. Mikro Bloglar 15

e. Wikiler 16
f. Sosyal İşaretleme Siteleri 16
g. Sanal Oyun ve Sanal Gerçeklik (Yaşam) Platformları 17
3. Sosyal Ağlardaki Başlıca Kısımların, İşlevlerin ve İşlemlerin, Kişisel Veri Kapsamına Giren Alanları 17
a. Profil 19
b. Gönderi, Paylaşım, Hikaye, Reels, Tweet, Retweet 22
c. Zaman Tüneli (Zaman Akışı) ve Duvar (Haber Kaynağı) 23
d. Yorum Yapma ve Duygu Belirtme (Beğenme) 24
e. Konum Bilgisi Ekleme 25
f. Etiketleme 25
g. Doğrudan/Direct Mesaj 26
h. Konu Başlığı/Hashtag(Sosyal Medya Künyesi) 27
II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL KAVRAMLAR 29
A. Veri ve Kişisel Veri Kavramı 29
1. Kişisel Veri Kavramı ve Unsurları 29
a. Veri Kavramı ve İçeriği 32
b. Kimliğin Belirli veya Belirlenebilir Olması 33
c. Kişiye İlişkin Olma 37
2. Özel Nitelikli Kişisel Veri (Hassas Veri) 37
3. Özel Hayatın Gizliliği ve Mahremiyet 39
III. KİŞİSEL VERİLERİN KORUMASINDA TEMEL İLKELER 44
A. Veri Korumanın Esasına Dair İlkeler 44
1. Veri Güvenliği ve Mahremiyeti 44
2. Hassas Verilerin İşlenmesi ve Özellikli Olarak Korunması 48
B. Verinin İşlenme Usulüne Dair İlkeler 49
1. Hukuka ve Dürüstlük Kurallarına Uygunluk 49
a. Açık Rızanın Kapsamında Verilerin İşlenmesi 51
b. Kanunlarda Açıkça Öngörülmesi 52
c. Diğer Haller 53
2. Amaçla Bağlılık 53
3. Ölçülülük 55

4. Doğruluk ve Güncellik 56
C. Veri Sahibi Kişinin Haklarına İlişkin İlkeler 57
1. Bilgi Edinme, Erişim ve Düzeltme Hakkı 57
2. Unutulma Hakkı 60
3. İşlemenin Sınırlandırılması Hakkı 67
4. Verilerin Taşınması Hakkı 68
5. İtiraz ve İrade Sergileyebilme Hakkı 69
D. Kişisel Veri, İnternet ve Sosyal Medya İlişkisi 70

İKİNCİ BÖLÜM

ULUSLARARASI VE ULUSAL DÜZENLEMELER

I. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ULUSLARARASI DÜZENLEMELER 72
A. OECD Düzenlemelerinde Kişisel Verilerin Korunması 72
B. Birleşmiş Milletler Temel Metinlerinde Kişisel Verilerin Korunması 74
C. Avrupa Konseyi Düzenlemelerinde Kişisel Verilerin Korunması 76
1. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme (108 sayılı Sözleşme) 77
2. AİHS 8. Maddesi Kapsamındaki Koruma 79
D. Avrupa Birliği Dahilinde Kişisel Verilerin Korunması 86
1. Avrupa Birliği Temel Haklar Şartı 86
2. Avrupa Birliği Veri Koruma Direktifi (95/46/AT) 87
3. Özel Yaşamın ve Elektronik İletişimin Korunması Yönergesi (2002/58/AT) 90
4. 29 Madde Veri Koruma Grubunun 5/2009 Sayılı Çevrimiçi Sosyal Ağlar Konusundaki Tavsiye Raporu 92
5. Avrupa Birliği Veri Koruma Regülasyonu (2016/679- GDPR Avrupa Birliği Genel Veri Koruma Tüzüğü) 94
II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL ULUSAL DÜZENLEMELER 95

A. Anayasa' da Kişisel Verilerin Korunması 95
B. Kişisel Verilerin Korunması Kanunu Kapsamında Kişisel Veriler 96
C. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651 Sayılı Kanun) 99
1. Sosyal Medya Ağ (Site) Sahipliği ve Yükümlülükleri 99
a. Sosyal Medya Ağ Site Sahipliği Hukuki Niteliği 102
b. Sosyal Medya Ağ Site Sahipliği Hukuki Niteliği Yer Sağlayıcı Sıfatıyla Tabi Olduğu Özel Yükümlülükler 104
c. Sosyal Medya Ağ Site Sahipliği Hukuki Niteliği ve 7253 Sayılı Kanun "Sosyal Ağ Sağlayıcı" Sıfatıyla Tabi Olduğu (Ek) Özel Yükümlülükler 106
2. Sosyal Medya Kullanıcısı ve Yükümlülükleri 111
a. Sosyal Medya Kullanıcısının Hukuki Niteliği: İçerik Sağlayıcı Kavramı 111
b. İçerik Sağlayıcının Özel Yükümlülükleri 112
3. Erişim Sağlayıcı ve Toplu Kullanım Sağlayıcılar: İnternet Erişimi Sağlayanlar 115
a. Erişim Sağlayıcı Kavramı ve Yükümlülükleri 115
b. Toplu Kullanım Sağlayıcı Kavramı ve Yükümlülükleri 116
D. Ceza Hukuku Kapsamında Kişisel Verilerin Korunması 117
1. Ceza Hukuku Kapsamında Değerlendirilecek Sosyal Medyada Paylaşılan Veriler 117
2. TCK m. 135 ve m. 136 Açısından Sosyal Medya Paylaşımlarının Değerlendirilmesi 120
a. Kişisel Verilerin Kaydedilmesi, Kişisel Verileri Verme, Yayma ve Ele Geçirme Suçlarının Maddi Unsuru 125
b. Kişisel Verilerin Kaydedilmesi, Kişisel Verileri Verme, Yayma ve Ele Geçirme Suçlarının Manevi Unsuru 136
c. Kişisel Verilerin Kaydedilmesi, Kişisel Verileri Verme, Yayma ve Ele Geçirme Suçlarının Hukuka Aykırılık Unsuru 137
3. TCK m. 135 ve 136 Açısından İçtima 148

4. TCK m. 135 ve m. 136 Açısından Çocukları Konu Alan ya da Çocuklar Tarafından Yapılan Sosyal Medya Paylaşımlarının Değerlendirilmesi 153
SONUÇ 165
KAYNAKÇA 169

KISALTMALAR

AB	Avrupa Birliği
ABAD	Avrupa Birliği Adalet Divanı
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
Ay.	Anayasa
AYM	Anayasa Mahkemesi
Bkz.	Bakınız
BM	Birleşmiş Milletler
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CD.	Ceza Dairesi
C.	Cilt
CMK	Ceza Muhakemesi Kanunu
E.	Esas Numarası
ESB	Erişim Sağlayıcıları Birliği
E.T	Erişim Tarihi
GDPR	AB Veri Koruma Tüzüğü
K.	Karar Numarası
KVKK	Kişisel Verileri Koruma Kanunu
m.	Madde
RG	Resmi Gazete
s.	Sayfa
ss.	Sayfa Aralığı
S.	Sayı
TBB	Türkiye Barolar Birliği
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
YCGK	Yargıtay Ceza Genel Kurulu

TABLOLAR LİSTESİ

Tablo 1: Hane Halkı Bilişim Teknolojileri Kullanımına İlişkin Temel Göstergeler, 2009-2020 s.7

Tablo 2: Sosyal Medya ve Geleneksel Medya Karşılaştırması s.11

Tablo 3: Facebook, Twitter, İnstagram Aracılığı ile İşlenen Suçlardan 2016-2019 Yılları Arasında Yargıtay Tarafından Karara Bağlanan Suçlar s.119

GİRİŞ

Günümüzde sosyal medya günlük hayatın bir parçası halinde gelmiştir. Milyonlarca kullanıcısı olan bu mecraların ortaya çıkması internetin gelişimi sonucunda olmuştur. İnternet bireylerin hayatlarını kolaylaştırmış aynı zamanda sayısız verinin deposu haline gelmiştir. İnternet kullanıcıları tarafından ise bu durumun idrak edilmesi bir hayli zaman almıştır. Bilinçsiz kullanımlar bireylerin hayatında önemli izler bırakmıştır. İnternetin ortaya çıkardığı bu sonuçlar sosyal medya diye adlandırdığımız sosyal ağ siteleri açısından da kaçınılmaz bir sonuç olmuştur. Facebook'un ortaya çıkışı ile başlayan bu süreç özellikle son yıllarda sayısız sosyal medya platformunun kurulması ile hız kazanmıştır.

Çalışmamızda, günümüzde mevcut birçok sosyal ağ arasından ülkemizde ve dünyada en çok kullanıcısı olan facebook, instagram ve twitter esas alınmıştır. Facebook ve instagram daha çok görsel ögeler içeren paylaşımlar için kullanılmakta iken twitter ise düşünsel ögeler içeren paylaşımların daha yoğun olarak yapıldığı bir mecra olarak değerlendirilmektedir. Ancak her üç sosyal medya platformunda da hem görsel ögelerin hem de işitsel ögelerin paylaşılmasına imkan tanıyan özellikler bulunmaktadır. Her platformun kendi paylaşım türleri ve bu türlerin farklı isimleri bulunmaktadır. Ancak sonuç olarak bu platformlarda paylaşımların altına açıklamalar yapılması ya da doğrudan paylaşımda düşünce yazılarının yer almasının yanında sadece kişinin kendi fotoğrafını paylaşması ya da bir video şeklinde düşüncelerini sesli olarak açıklaması da mümkündür. Bu platformlarda yapılan paylaşımlar veri niteliğindedir. Ancak çalışmamız kapsamında her veriyi değil de kişisel verileri esas almış bulunmaktayız. Her verinin kişisel veri niteliğine sahip olmadığı ve kişisel verinin tespiti önemli bir husustur. Örneğin kişinin kendisinin çektiği bir doğa fotoğrafını sosyal medya hesabından paylaşması durumunda fotoğrafın veri olduğu kabul edilebilmekle birlikte kişisel veri niteliğinde olduğu söylenemeyecektir. Kişilerin bu şekilde yaptığı paylaşımların niteliğine göre fikri ve sınai haklar kapsamında bir değerlendirmeye tabi tutulma imkanı elbette bulunmaktadır ancak kişisel veri niteliğine sahip olabilmesi için gerçek bir kişiye ait veri olmalıdır. Ayrıca gerçek kişiye ait verinin de o kişi belirli kılabilir nitelikte olması aranmalıdır.

Kişisel verilere ilişkin uluslararası düzenlemeler ulusal düzenlemelerimiz için önemli kaynak niteliğindedir. Özellikle Kişisel Verilerin Korunması Kanunu, kanun koyucu tarafından hazırlanırken Avrupa Birliği düzenlemeleri esas alınmıştır. Avrupa Birliği Genel Veri Koruma Tüzüğü özellikle kişisel verilerin korunması konusunda internet ve sosyal medyanın günümüzde oluşturduğu sorunlara yönelik çözümler sunmaktadır. Kişisel Verilerin Korunması Kanunumuz sosyal medya kullanımına açıkça yer vermese de kişisel veriler konusunda hukukumuzda yapılan en önemli yasal düzenleme olarak yer almaktadır. Kişisel Verilerin Korunması Kanunu kişisel verilere ilişkin tanımlamalara, ilkelere, verilerin işlenmesi ve aktarılması konusunda düzenlemelere yer vermiştir. Kanunumuzda yer alan en önemli düzenlemelerden birisi ise veri işleme ve verileri aktarma konusundaki açık rıza, alenileştirme ve diğer hukuka uygunluk sebepleridir. Kamuoyunda sosyal medya kanunu adıyla bilinen 5156 sayılı Kanunda yapılan düzenleme ise sosyal medya şirketlerine getirilen özel yükümlülükler kişisel verilerin korunmasına yönelik önemli tedbirleri içermektedir. İlgili kanun internette ilişkin temel düzenlemeleri içermekte ve suç unsuru içeren eylemlerin mağdurların mağduriyetlerinin daha fazla artmadan geçici tedbirler alınmasına hizmet etmektedir.

Kişisel verilerin korunması kavramında verilerin hukuki koruması kadar cezai hükümlerle korunması da büyük önem arz etmektedir. Çalışmamızın esas konusu ceza hukuku yoluyla kişisel verilerin korunması olsa da temel kavramlar ve kişisel verilerin korunmasının hukuki yönü de büyük önem arz etmektedir. Önemi doğrultusunda öncelikle bu hususa ilişkin düzenlemelere yer verilmesi tercih edilmiştir. Türk Ceza Kanunu'nda yer alan kişisel verilerin hukuka aykırı olarak kaydedilmesi, kişisel verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçlarının değerlendirilmesinin yapılabilmesi için kişisel verilerin korunması konusundaki ulusal ve uluslararası mevzuata değinilmesi bir zorunluluk olmuştur. Sosyal medyada paylaşılan bir kişisel verinin hangi durumlarda hukuka aykırılık teşkil ettiğinin tespiti yalnızca ceza hukukunu ilgilendiren bir durum olmayıp hukukumuzda kişisel verilere ilişkin olan tüm mevzuat hükümlerini kapsayan bir durumdur. Sosyal medya konusunun yeni bir konu olması suç tipleri konusunda hukuka aykırılık değerlendirmesi yapılırken yalnızca Yargıtay Ceza Dairelerinin

kararlarının değil de Yargıtay Hukuk Dairelerinin kararlarının da dikkate alınmasını gerektirmektedir.

Sosyal medyada kullanıcılar tarafından rıza ile paylaşılan kişisel verilerin kaydedilmesi işleminin hukuka aykırı olup olmadığına karar verilmesi gerekir. Çalışmamızda herkese açık olan yani korumalı olmayan hesaplar esas alınmıştır. Verinin paylaşıldığı hesabın herkese açık bir hesap mı ya da yapılan paylaşımın türü kaydedilme eylemine izin verecek şekilde mi gibi sorular sorularak hukuka aykırılık hususunda değerlendirmeler yapılabilecektir. Kişisel Verilerin Korunması Kanunu kapsamında olan kişisel verinin, kişinin bizzat kendisi tarafından alenileştirmesi halinde hukuka uygunluk sebebinin oluşup oluşmadığının tespiti önem arz etmektedir. Ayrıca bazı durumlarda paylaşımın niteliğinin ve failin kastının tespiti de gerekir. Ancak bu noktada şu tespitin yapılması gerekir: Verilerin alenileştirilmesi bu verilerin başkaları tarafından kaydedilmesi ya da yayılması eylemine verilen bir rıza mıdır? Örneğin kullanıcıların sınırlı sayıda kişi ile paylaştığı ya da süreli olarak paylaştığı verilerin sınırlı sayıya dahil olmayan üçüncü kişilerce kaydedilmesine yönelik rızasının olmadığı kabul edilmelidir. Kullanıcının herkese açık sosyal medya hesabından paylaştığı bir fotoğrafının başka bir kullanıcı tarafından bu fotoğrafta yer alan kişi kendisiymiş gibi paylaşılmasına rıza vermiş olduğu kabul edilebilir mi? Bu sorunun cevabına olumlu yanıt vermek hakkaniyete uygun değildir. Kullanıcı kişisel verisi olan yüzünü paylaştığında bunu aleni hale getirmekle birlikte bu verinin kendisine ait olduğu hususunun başkalarınca göz ardı edilmesine yönelik kabulü bulunmamaktadır. Söz konusu kişisel verinin sahibinin kim olduğu gösterilerek ya da etiketlenerek paylaşımının tekrar paylaşılması esasen sosyal medya platformlarında bir paylaşım özelliği olarak zaten mevcuttur. Bunun dışındaki verme, yayma ya da ele geçirme eylemleri hukuka aykırı olarak değerlendirilebilmeye daha uygundur.

Çocuklara ait kişisel verilerin sosyal medyada paylaşılması oldukça yaygındır. Çocukların rızası nasıl olabilir ve hangi yaşlarda rıza açıklayabilirler konusu hukukumuzda doğrudan düzenlenmemiş bir husustur. Bu konuda Avrupa Birliği Genel Veri Koruma Tüzüğü düzenlemeleri ve buna uygun olarak sosyal medya platformlarının topluluk kuralları 13 yaş sınırını ön plana çıkarmaktadır. Sosyal medya platformlarındaki içeriklerin birçoğunun pedagojik açıdan çocuklar için uygun olmadığı değerlendirilmektedir. Çocukların bu platformları yaş sınırına

uygun olmadan kullandığı araştırmalar sonucunda açıkça tespit edilmektedir. Çocuğun kişisel verilerini paylaştığı durumlarda bu verilerin korunması bir yetişkine oranla daha önemlidir. Çocukların bizzat kendilerinin kişisel verilerini paylaşması durumu haricinde ebeveynleri tarafından çocuklarının özelikle fotoğraflarının paylaşılması oldukça yaygındır. Bu paylaşımlar bazen günlük hayata ilişkin normal paylaşımlar bazen de ticari amaçlarla markalarla yapılan iş birlikleri çerçevesinde olan paylaşımlardır. Her iki durumda da çocuğun kendi iradesi ile yapılan paylaşımlar olduğu söylenemeyecektir. Bu paylaşımlar konusunda ebeveynlerin çocuk yararına davranması, onun duygusal zihinsel gelişimine zarar verebilecek ya da yıllar sonra çocuk için travmatik olabilecek eylemlerden kaçınması gerekir. Verilerin bir defa dijital dünyaya aktarılması ile artık kalıcı bir şekilde silinmesi mümkün olmamaktadır. Bu durumda çocuklarının verilerini paylaşan ebeveynlerin çocuğunun kendi kişisel verileri üzerinde tasarrufta bulunabilmesi hakkını elinden almasına sebep olacaktır. Özellikle ayırt etme gücüne sahip olan çocuğun rızasına tamamen aykırı olan bir kişisel verisinin paylaşılmaması bir gerekliliktir.

Çalışmamızda, yukarıda açıkladığımız hususları daha da ayrıntılı ele alacak şekilde açıklamaya, bir anayasal hak olan kişisel verilerin korunması hakkının sosyal medyadaki yansımalarına ve hangi durumların ceza hukuku konusu olabileceğine ilişkin tespitler yapmaya çalıştık. Sosyal medyanın yeni ve güncel bir alan olması sebebi ile olabildiğince güncel kaynaklardan ve yargı kararlarından yararlanmaya özen gösterdik. Umarım çalışmamız sosyal medyada paylaşılan kişisel verilerin korunması olgusuna, kullanıcıların eylemlerinin cezai sonuçlarının değerlendirilmesine yönelik çalışmalara ve farklı düşüncelerin ortaya konulmasına katkı sağlayan bir çalışma olmuştur.

BİRİNCİ BÖLÜM
SOSYAL MEDYA VE KİŞİSEL VERİLER KONUSUNDA TEMEL KAVRAMLAR

I. SOSYAL MEDYA

A. Sosyal Medya Kavramı

1. Genel Olarak Sosyal Medya Kavramı Ve Sosyal Medyanın Özellikleri

Sosyal medya birçok alan da farklı tanımları yapılmış bir kavramdır. Her alan sosyal medyanın farklı özellikleri ön plana çıkarak tanımlama yapmaktadır. İletişim temelli yaklaşımlarda paylaşma esasına yönelik açıklamaların ön planda olduğu görülmektedir. Örneğin *"Kullanıcılarına karşılıklı paylaşım imkanı sağlayan, kullanıcılarının kişisel veya gruplar içinde medya içeriği oluşturmasına imkan veren dijital medya ve teknolojileridir."* tanımlanmıştır. Teknoloji temelli yaklaşımlara bakıldığında sosyal medyanın içerik ekleme özelliğine dikkat çekmektedir. Web 2.0 teknolojisi ile web 1.0 teknolojisindeki asıl farklılık yalnızca okuyucu olmanın aksine kişilerin kendi içeriklerini de yazarak başkalarının okumasına imkan sağlayabilmeleridir[1].

Öncelikle internetin tanımı yapmak yararlı olacaktır. İnternet, tüm bilişim ağlarının ve bilgisayarların TCO/IP[2] adıyla adlandırılan protokollerle birbirine bağlayan bit ağ sistemidir[3].

Esasen sosyal medya son tanımda da kısaca ifade edildiği üzere aslında tek taraflı bilgi paylaşımı değil de çift taraflı ve eşzamanlı bilgi paylaşımı elde etmemizi sağlayan web 2.0 teknolojisidir. Sosyal medya kişilerin internet üzerinden yaptıkları paylaşımlar ve diyalogları kapsamaktadır. Ayrıca sosyal ağlar olarak adlandırdığımız

---

[1] Sami Akkurt, **Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması**, 2. Baskı, Seçkin Yayınları, Ankara, 2020, ss. 95, 96.

[2] TCP/IP (Transport Control Protokol/Internet Protokol) Kısaca TCP, ileti ve mesajların doğru yere ulaşmasından, IP ise adresleme sisteminden sorumludur. Berrin Akbulut, **Bilişim Alanında Suçlar**, 2. Baskı, Adalet Yayınları, Ankara, 2017, (Bilişim Alanında Suçlar) s. 18; Murat Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 8. Baskı, Seçkin Yayıncılık, Ankara, 2020, s.81.

[3] Dülger, s. 78, Berrin Bozdoğan Akbulut, "Bilişim Suçları" **Selçuk Üniversitesi Hukuk Fakültesi Dergisi,** Milenyum Armağanı, Cilt:8, Sayı:1-2, 2000, ss. 546-547.

internet siteleri ve uygulamalar insanların içerik paylaşmalarının ve bu paylaşımlara arayan herkesin ulaşabildiği platformlar vardır. Bu platformlarda kullanıcı bazlı içeriklere ve küçük grupların paylaşımlarına değer atfedilmektedir. Sosyal medya günümüzde dünyada azımsanmayacak kadar önemli bir kesim tarafından kullanılmaktadır[4]. Başka bir tanıma göre ise sosyal medya internet aracılığı ile kişilerin birbiri ile etkileşim içinde olduğu, topluluklar oluşturduğu, duygu ve düşüncelerini içeren paylaşımlar yaptığı bir sosyalleşme aracıdır[5]. Aslında daha sade bir tanımla sosyal medyanın online ortamlarda katılımcılar tarafından yorum yapılabilmesi, katılımcıların birbirleri ile iletişim kurabilmesi, bu ortamlara çeşitli şekillerde katkı sunabilmesine imkan tanıyan "sosyal içerikli web siteleri" olarak tanımlanması mümkündür[6].

Medya kelimesi ise Latince kökenlidir. Bu kelime, medium kelimesinden yani "ortada bulunan, aradaki, araç" anlamına gelen kelimesinin çoğuludur[7]. TDK'ye göre medya, iletişim ortamı ve araçları anlamına gelmektedir[8].

Sosyal medya, mahkemelerce örneğin Anayasa Mahkemesi (AYM) tarafından *"...dünyadaki bütün kullanıcıların toplu olarak iletişim kurabildiği ve haberleştikleri bir mecra..."* olarak tanımlamıştır, AYM sosyal medyayı dünyadaki tüm insanların iletişim kurabildiği, mesaj, yorum, bilgi, eleştiri, satış ve tanıtımların paylaşılabildiği etkili bir mecra olduğunu belirtmektedir. Bu şekilde toplumun gündem belirlemesine, gündemin izlenmesini ve bilgi dolaşımını kolaylaştırmaya önemli düzeyde katkı sunmaktadır[9].

> *Kısacası sosyal medya; basit, yalın bir tema içeren, kullanımı kolay olan, içerik oluşturma ve oluşturulan içeriği okumada gönüllülük esasına dayalı olan, her*

---

[4] Servet Yetim, **Ceza Muhakemesi Hukuku Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (Facebook Örneği**), Seçkin Yayıncılık, Ankara, 2016, s. 268.

[5] Mine Kaya, **Elektronik Ortamda (Elektronik Haberleşme- İnternet- Sosyal Medya) Kişilik Hakkının Korunması**, Seçkin Yayınları, Ankara, Eylül 2015, s.76.

[6] Yüksel Köksal ve Şuayb Özdemir "Bir İletişim Aracı Olarak Sosyal Medya'nın Tutundurma Karması İçerisindeki Yeri Üzerine Bir İnceleme", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt:18, Sayı:1, 2013, s. 325.

[7] https://www.kokeni.com/medya-kelimesinin-anlami-kokeni-ve-tarihcesi/ (E.T:27/09/2021).

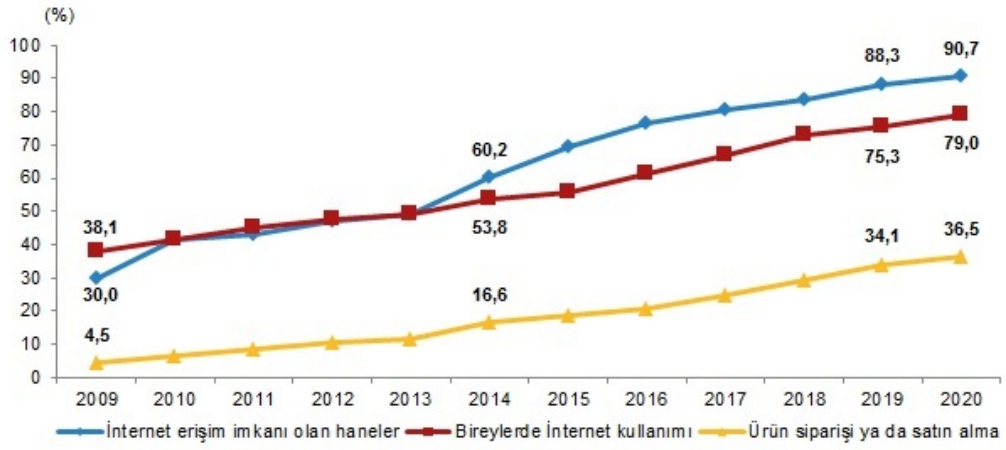
[8] https://sozluk.gov.tr/ (E.T:27/09/2021).

[9] Anayasa Mahkemesi'nin 07/02/2018 tarih ve 30325 sayılı R.G.'de yayımlanan, 15/11/2017 T., 2015/76 E. ve 2017/153 K. sayılı Kararı, AYM, Youtube Llc Corporatıon Servıce Company ve diğerleri [GK], 29/05/2014 tarihli Bireysel Başvuru No: 2014/4705, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/4705?BasvuruNoYil=2014&BasvuruNoSayi=4705, (E.T:27/09/2021).

türlü paylaşım için zemin hazırlayan, yöneticisi editörü ve sahibi hiç kimsenin olmadığı ya da herkesin olduğu, kendine has kuralları olan, aynı zamanda herkese eşit bit şekilde demokratik ortamı sağlayan sanal ortamın adıdır[10].

We are Social 2020 Türkiye İnternet, Sosyal Medya ve Mobil Kullanım İstatistiklerine göre Türkiye'de 62 milyon internet kullanıcısı (Türkiye nüfusunun yüzde 74'ü) ve Türkiye'de 54 milyon sosyal medya kullanıcısı bulunmaktadır. Ayrıca yapılan çalışmada Türkiye'de en çok ziyaret edilen siteler sıralamasında ilk sırada google, ikinci sırada youtube, dördüncü sırada facebook, yirminci sırada instagram gibi sosyal medya platformları yer almaktadır. Türkiye'de en çok kullanılan sosyal medya platformları sıralamasında ise ilk sırada youtube yer alırken onu sırayla instagram, whatsapp, facebook, twitter takip etmektedir. Sosyal medya kullanımında yaş dağılımı konusunda gelindiğinde ise en yüksek kullanım oranı 25-34 yaş aralığında bulunmaktadır[11].

TÜİK verilerine göre İnternet kullanım oranı 2020 yılında 16-74 yaş grubundaki bireylerde %79,0 oldu. Bu oran, 2019 da %75,3'tü. İnternet kullanım oranı erkeklerde %84,7 iken kadınlarda %73,3 oldu. Verilere bakıldığında hanelerin %90,7'sinin evden İnternete erişim imkanına sahip olduğu görülmüştür. Bu oran 2019 yılında %88,3 idi. Ayrıca TÜİK söz konusu verileri aşağıdaki şekilde tablo şeklinde yayınlamıştır[12]:



Tablo 1: Hanehalkı bilişim teknolojileri kullanımına ilişkin temel göstergeler, 2009-2020.

[10] Yetim, s. 271.

[11] https://www.webtekno.com/turkiye-de-kac-kisinin-ne-kadar-ve-hangi-amacla-internet-kullandigi-aciklandi-h107112.html (E.T:03/08/2021).

[12] https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679 (E.T:27/09/2021).

Sosyal medyanın başlıca özelliklerini şu şekilde sıralayabiliriz:

a. Erişilebilirlik

Esasen bir sosyal medya platformundan bahsedebilmek için onun zaman ve mekan sınırlaması olmadan geniş bir kitle tarafından ulaşılabilir olması gerekmektedir. Ancak belli meslek grubunda olmanın şart koşulması ya da belli kurumda çalışıyor olunması gerekmesi bu özelliğin yitirilmesi anlamına da gelmemektedir[13].

> *Sosyal paylaşım siteleri teknik olarak kullanım basitliği, maddi anlamda erişilebilirlikteki ucuzluğu, akıllı telefon üzerinden mobil sosyal medya uygulamaları ile bireyler arasındaki birincil ilişkilerin yerini almaya başlamıştır…gerçek yaşam ilişkilerini bu mecraya taşıma ve dolayısıyla gerçek yaşam örüntülerinden kopma düzeyleri de artmaktadır*[14].

b. Kullanıcı/Katılımcı

Sosyal medya içerikleri daha çok kullanıcıların oluşturduğu içeriklerin bütünüdür. Yani kullanıcı ve katılımcılar sosyal medyayı diğer web sitelerinden ayırmaktadır. Bu sosyal medya platformundaki kullanıcılar büyük oranda içerik üreticisi konumundadır. Kullanıcı adları, avatar ya da profil adı verilen sanal kimliklerle tanınırlar. Bu kimlikler bazen kendi adları iken bazen başkaca isimlerden oluşmaktadır. Kişinin kendi adı dışında isimler kullanması hukuk tekniği açısından müstear ad niteliğinde olup bu konuda mevcut hukuk kurallarına tabi olacaktır[15]. Kişilerin kimliklerine ilişkin paylaştığı veriler twitter, facebook, instagram gibi sosyal medya sitelerinde rızayla paylaşıyor olmasına rağmen bu bilgiler özel hayat ve kişisel verilere ilişkin hükümlerle ilişkilidir[16]. Sosyal medyada kullanıcılar ve

---

[13] Akkurt, s. 100.
[14] Hatice Budak, "Sosyal Medya İletişiminde Mahremiyet Serüveni**" İnsan ve Toplum Bilimleri Araştırmaları Dergisi**, Cilt:7 Sayı:1, 2018, s. 147.
[15] Akkurt, s. 101.
[16] Jan H. Kietzmann, Kristopher Hermkens, Jan P. Mccarty, Bruno S. Silvestre, "Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media" **Busines Horizons**, Cilt: 54, Sayı: 3, 2011, ss. 243, 244;

kullanıcıların oluşturduğu topluluklar aslında bu platform aracılığı ile sosyalleşmektedir. Her kullanıcı bunu farklı biçimlerde yapmaktadır. Örneğin üretici konumundaki kullanıcılar kendi sayfalarında fotoğraf, video ya da başka paylaşımlarla içerik üretmektedirler. Bu paylaşımların amacı kullanıcıların duygu ve düşüncelerini ifade etme, tanınma, şöhret, insanları etkileme ve onları harekete geçirme ya da kendini gerçekleştirme içgüdüsü gibi sebeplerledir. Tüketici konumundaki kullanıcılar ise sadece sosyale medyada okuma ve izleme faaliyetini gerçekleştirir. Bu kullanıcıların amacı üretmek değildir. Yalnızca bilgi edinme ya da eğlenme amacı güder. Katılımcı kullanıcı olarak adlandırılan kesim ise kullanıcıdan kullanıcıya ya da içeriğe doğru etkileşim sağlamaktadır. Bu işlevi yorum yapma, post atma, beğenme ve favorilere ekleme gibi şekillerle gerçekleştirebilirler. Bu kullanıcılar tüketici konumundaki kullanıcıları etkilemekte ve doğal olarak üretici kullanıcıların davranış ve paylaşımlarını da şekillendirmektedir[17].

Sanal alemden insanlar her türlü bilgi ve içeriğe akıllı telefonlar, dizüstü bilgisayarlar ve tabletler aracılığı ile ulaşabilir hale gelmişlerdir. Kişilerin daha önce televizyon izleme alışkanlıkları varken artık bu durum internette gezinme alışkanlığına dönüşmüştür. Bu husus ağ vatandaşlığı (netizenship) olarak adlandırılmaktadır. Ayrıca vatandaşların faaliyetleri ile açık kaynak gazeteciliği olarak adlandırılan halk gazeteciliği de ortaya çıkmıştır. Çünkü bu teknoloji ile halk sadece okuyan değil aynı zamanda haber veren, yorum yazan, gazeteci kimliği olmaksızın şahit olduklarını sosyal medyadan yazı, resim, video gibi araçlarla aktarabilen bir konumda yer almıştır. Özellikle günümüzde bu kullanıcılar vatandaş gazeteciliği (citizen journalizm) ile birçok toplumsal harekette haber verme ve örgütlenmede etkin rol oynamıştır[18].

c. İnteraktif Paylaşım, Etkileşim ve İçerik

Sosyal medya kullanıcılara çift yönlü iletişim ve etkileşim sağlar yani kişilerin ilgilendikleri konularda daha etkin ve hızlı bir şekilde bir araya

---

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.687.4642&rep=rep1&type=pdf (E.T:15/01/2022); Kaya, s. 85.

[17] Kaya, 78.

[18] Yetim, s. 285, 286.

gelebilmeleri ya da o içeriğe ulaşabilmelerini sağlar. Kullanıcıların duygu, düşünce, kişisel bilgilerini ve hallerini bildiren yazı, fotoğraf ve videoları gibi paylaşımlar içerik olarak adlandırılmaktadır. Sosyal medyanın asıl amaçlarından biri de içerik paylaşımı yapılmasıdır[19]. Sosyal meydanın bir diğer özelliği de alıcı ve kaynak arasındaki statü farkı söz konusu olmamasıdır [20]. Ayrıca sosyal medya paylaşımı yapılabilmesi için site ya da platform olarak adlandırdığımız web 2.0 destekli internet platformlarının olması gereklidir[21].

d. İletişim

Sosyal medya platformunda iletişim başkaları ile içerik paylaşabilme, yorum yapabilme, sesli ve görüntülü konuşma, yazışma yapılabilmesi örneğin chat, direkt mesaj (dm) gibidir. İletişim özel ikili diyaloglar ya da kitlesel gönderiler yapılabilmesi şeklinde olabilir[22]. İletişim ortamında arkadaşlar, bağlantılar ve tanıdıklar gibi isimler vardır. Sosyal medyada tanınma olgusu firmalar için önemlidir. Ancak bu konuda bir mesajının okunmasında o kişinin takipçi sayısı tek kriter değildir. Farklı uygulamalarla kullanıcıların tanınma düzeyleri değerlendirilebilir. Ayrıca sosyal medyada kullanıcı grupları mevcuttur. Bu grupların oluşumu iki şekilde olabilir: İlki kullanıcının bağlantı kurduğu yakınları, arkadaşları ya da takipçilerinden oluşur. İkincisi ise kişiler gruplara davet edilerek bu şekilde herkese kapalı ya da gizli ile oluşturulan gruplardır[23].

Mayfield'e göre sosyal medyanın başlıca özellikleri şunlardır: Sosyal medya ilgi alanı olan herkesi katılım sağlamaya yönlendirmektedir. Kullanıcılar hem katkı sağlamaya hem de cevap verme gereksinimi duymaktadırlar. Katılım sağlayıcı özelliği ile kullanıcılar arasında tüketici ve üretici kullanıcı olarak yapılan sınıflandırma da üreticiye doğru kaymaktadır. Ayrıca sosyal medyada açıklık hakimdir. Şifreli alanlar azdır. Bu sebeple yorum, beğenme ya da etkileşimde bulunma teşvik edilmektedir. Kullanıcılar arası etkileşim birebir konuşma ya da

[19] Akkurt, s. 102.
[20] Cansel Güzel, "Sosyal Medyanın Neliği, Gelişimi Ve Kullanım Alanları Üzerine Kuramsal Bir İnceleme", **Sosyolojik Düşün**, Cilt:5 Sayı:2 Aralık 2020, s.97.
[21] Akkurt, s. 103.
[22] Akkurt, s. 103.
[23] Kaya, s. 86, 87.

topluluklar oluşturma şeklinde meydana gelmekte ve geleneksel medyanın aksine iki yönlü iletişim vardır. Bütün bunlara ek olarak sosyal medyada linkler aracılığı ile bağlantılar kurulmaktadır[24]. Sosyal ağların geleneksel iletişim yöntemlerinden en temel farkı geri bildirim imkanı sağlamasıdır[25]. Geleneksel medya[26] olarak adlandırdığımız medyadan farklı olarak sosyal medya ya da diğer bir ismiyle yeni medyada iletiler kitleler için oluşturulur ve aktarılırken, etkileşim çağındaki medyayı ifade eden yeni medyada bireye özel içerikler hazırlanır veriler kişiselleştirilmiştir. Bu şekilde sosyal medya da etkileşim, eş zamanlılık ve kitlesizleştirme[27] özellikleri vardır[28]. Bu özellikler sosyal medyayı hem küresel hem de etkin bir alan haline getirmiştir. Geleneksel medya ile sosyal medya arasındaki benzerlik ve farklılıklar şunlardır[29]:

Erişebilirlik, Kullanabilirlik ve Üretim Yetkisi	• Sosyal medya herkesin erişimine açıktır. Bu kişilerin belli bir yetenek ve eğtime sahip olması gerekmemektedir. Ayrıca sosyal medyada herkes üretim ve değişiklik yapabilmektedir. • Gelneksel medya da herkesin erişimine açık olmakla birlikte belli eğitim ve uzmanlığa sahip kişilerce kullanılıp üretim yapılabilmektedir.
Değişime Uyarlama ve Esneklik	• Sosyal medya sürekli değişimin olduğu ve kısa sürede buna uyarlama yapılmasının mümkün olduğu bir platfotmdur. Yapılan yorumlar silinebilir yada üretimler anlık olarak değiştirilebilir. • Geleneksel medyada ise değişim genellikle uzun sürede gerçekleşir ve örneğin makale üretimi yapıldıktan sonra değiştirilmesi kolay değildir.
Serbestlik ve Özgürlük	• Sosyal medyada hareket alanı oldukça özgürdür. Ancak son yıllarda bu alana ilişkin yasal düzenlemeler yapılmaya çalışılmaktadır. • Geleneksel medya üzerinde siyasi ve ekonomik çıkar gruplarının baskısı vardır.

Tablo 2: Sosyal Medya ve Geleneksel Medya Karşılaştırması

[24] Antony Mayfield**, What is Social Media**, United Kingdom, 2010, s. 5, Yetim, s. 33.
[25] Ebru Çetin, "Sosyal Paylaşım Ağlarında Fotoğraf, Yer/Mekan Bildirimi Paylaşımları Ve Mahremiyet: Facebook Örneği" **Uluslararası Sosyal Araştırmalar Dergisi**. Cilt:8 Sayı:41, 2015, s. 780.
[26] Geleneksel medya endüstriyel medya, broadcast veya mass medya gibi türlerden oluşmaktadır. Gazete, televizyon, dergi ve filmler örnek olarak verilebilir. Geleneksel medya endüstri haline gelmiş çıkar ilişkilerine dayanmaktadır. Sosyal medyaya göre daha pahalı ve herkesin yayın yapamayacağı bir türdür. Dülger, s. 140-141.
[27] *"Kitlesizleştirme, iletişimde bir kitleye yönelik akışın geniş kitlelerden küçük gruplara yönelmesidir. Geleneksel medya ile gönderilen iletiler tüm hedef kitleyi kapsayacak şekilde gönderilirken, yeni medya hedef kitlede yer alan kişilere özel mesaj gönderme olanağına sahiptir."*; Kaya, s. 79.
[28] Güzel, s. 97.
[29] Metin Turan, **Bilişim Hukuku**, 5. Baskı, Seçkin Yayıncılık, Ankara, 2021, s. 316; Dülger, s. 141.

Castells'in "İsyan ve Umut Ağları" adlı eserinde günümüz sosyal medyanın özellikleri ile ilgili açıklamaları vardır. İletişim internet ve kablosuz ağların kullanımı ile kitlesel bir hale dönüşmüştür. Kendisinin ifadesi ile kitlesel öz iletişim *"birçok kişiden birçok kişiye iletilen, çok sayıda kişiye ulaşma ve dijital haldeki bilgiyi yakın çevre ya da sonsuz ağlara bağlanma ihtimali olan mesajlarla işler."* şeklinde açıklamaktadır. Gönderici mesaj oluştururken bu konuda bir özerkliğe sahiptir. Aynı şekilde alıcı da bu mesajı alma konusunda öz seçime sahiptir[30].

2. Sosyal Medyanın Bileşenleri

Sosyal medyanın bileşenlerinin sınıflandırılmasında farklı düşünceler vardır. Örneğin Kaplan ve Haenlein sosyal medya araçlarını; işbirlikçi projeler, bloglar, içerik toplulukları, sosyal ağlar, sanal oyun dünyaları, sanal sosyal dünyalar olarak sınıflandırmaktadır. Mayfield ise bu araçları sosyal ağlar, bloglar, wikiler, podcastler, forumlar, içerik toplulukları, mikrobloglar olarak yedi sınıfa ayırmaktadır. Akar'ın sınıflandırmasında ise sosyal ağ siteleri, medya paylaşım siteleri, bloglar, mikro bloglar, wikiler, sosyal işaretleme ve etiketleme, podcasting ve sanal dünyalardır[31].

Çalışmamızda Akkurt'un yaptığı sıralamaya uygun şekilde "sosyal ağlar", "fotoğraf, ses ve video paylaşım siteleri", "bloglar", "mikro bloglar", "wikiler", "sosyal işaretleme siteleri", "sanal oyun ve sanal gerçeklik (yaşam) platformları", "elektronik posta grupları", "kurumsal inranet", "ekstranet" olarak sınıflandırma yapılmıştır.

a. Sosyal Ağlar

Kullanıcılar herkesin görebileceği şekilde açık-yarı açık kişisel profiller oluşturarak başka kullanıcıları davet ederek gruplar oluşturarak çeşitli paylaşımlarda

[30] Manuel Castells, **İsyan ve Umut Ağları**, çev. Ebru Kılıç, Koç Üniversitesi Yayınları, İstanbul, 2013, s. 21.
[31] Kaya, ss. 87, 88.

bulunmaları bu katılımcılarla özel ya da genel olarak anlık yazışmalarda bulundukları web tabanlı platformlara sosyal ağ denilmektedir[32].

Sosyal ağlar bireyler arasındaki kişisel veya profesyonel ilişkilerin oluşturduğu ağlardır. Bu ağlar kural olarak herkese açıktır ve kullanıcı sıfatı ile kişiler ücretsiz kullanabilecektir. Temel amaç paylaşım yapmak ve iletişim kurmaktır. Ancak her sosyal ağın kendine özgü kullanım, erişim ve güvenlik konusunda kuralları vardır[33]. Sosyal ağlar zaman zaman sosyal medya kavramı ile karıştırılmaktadır. Sosyal ağlar sosyal medyanın araçlarından biridir. Bu siteleri diğer sitelerden ayıran en temel özelliği olan profil oluşturması ve paylaşım yapılması özelliklerinin yanında arkadaş listesi göstermesi, herkese açık yorumlama ve gizli mesajlaşma sisteminin olmasıdır. Ayrıca bu sitelerde görünürlük açısından farklı seçenekler de sunulmaktadır[34].

Sosyal ağ siteleri, kullanıcıların oluşturdukları profil etrafında sosyal medya platformunun kendilerine sağladığı özellikleri kullanmaktadır. Bu profil kullanıcıyı temsil etmekte ve sosyal ağlar da profil üzerinde kullanıcılara bazı yetkiler tanımaktadır. Kullanıcının profilindeki bilgilerin kimler tarafından görülebileceği ve kimlerin kendisi ile bağlantı kurabileceğine dair ayarlarda değişiklikler yapabilmektedir[35]. Kullanıcılar sosyal medya hesabı açtıklarında otomatik olarak profilleri ve içerikleri diğer kullanıcılara açıktır. Ancak gizlilik ve görünürlük gibi konularda kullanıcılara sağlanan çeşitli seçenekler bulunmaktadır.

En çok bilinen sosyal ağları şu şekilde sıralayabiliriz: Facebook[36], Google Plus, LinkedIn, MySpace, Windows Live, Reddit, MyYahoo, Odnoklassniki, FourSquare, Swarm.

Facebook 4 Şubat 2004 tarihinde kurulmuş bir sosyal ağ sitesidir. Harvard Üniversitesi öğrencisi olan Mark Zuckerberg tarafından Harvard öğrencileri arasında

---

[32] Andreas M. Kaplan ve Michael Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media" **Business Horizons**, Cilt: 53, Sayı:1, 2010, s. 63; Kaya s. 91.
[33] Akkurt, s. 105.
[34] Kaya, s. 91; Akar, s.36; N. Gizem Koçak, **Bireylerin Sosyal Medya Kullanım Durumlarının ve Motivasyonlarının Kullanımlar ve Doyumlar Yaklaşımları Bağlamında İncelenmesi: Eskişehir'de Bir Uygulama**, (Yayınlanmamış Doktora Tezi), Anadolu Üniversitesi, Eskişehir 2012, s. 22.
[35] Zeynep Tüfekçi, "Can you see me now? Audience and Disclosure Regulation in Online Social Network Sites". **Bulletin of Science, Technology & Society**, Cilt: 28, Sayı:1, 2008, ss. 22-23.
[36] https://www.facebook.com/policy.php?locale=tr_TR (E.T:12/09/2021).

iletişim kurmak için kurulmuştur. Facebook ismi ise üniversitelerin yönetimlerin verdiği "Paper Facebooks" olarak adlandırılan form ile verilmiştir. Öğrenciler bu formlarda yer verdikleri bilgilerle birbirlerinin tanıyor ve birbirleri ile iletişim kurabiliyorlardı. İlk başta yalnızca Harvard Üniversitesi öğrencileri bu şekilde iletişim kullanabiliyorken 2006 yılı Eylül ayından itibaren e posta adresine sahip olan kişiler üye olabilir hale gelmiştir[37].

Sosyal ağlar günümüzde iletişim bazında çağımıza önemli katkılar sağlamakla birlikte hukuki ve cezai sorumluluklar doğuran sorunlar da ortaya çıkarmaktadır. John Cooper QC'ya göre sosyal medya kullanıcıları içinde bulunduğumuz toplumdan farklı değildir. Toplumun büyük çoğunluğu akıllı, kültürlü, düzgün kişilerden oluşur ancak toplumda gördüğümüz gibi sorunlar genellikle bazı şeyleri kötüye kullanan azınlıktan kaynaklanır. Toplumsal hayatta görülen bu durumlar da bu hayatın tezahürü olan sosyal medyada da sürmesi abes değildir[38].

b. Fotoğraf, Ses ve Video Paylaşım Siteleri

Kullanıcıların bizzat kendilerince oluşturulan veya başkalarının oluşturdukları fotoğraf, video ve sair çoklu ortam (multimedia) içeriklerini paylaşmaya ya da paylaşımlar hakkında yorum yapmaya yarayan sitelerdir. Bu sitelerin en yaygın olanları Youtube (Kullanıcıların video izleyebildikleri, istenildiğinde kendi videolarını yükleyebildikleri ve yorum yapabildikleri bir sosyal ağdır.), İnstagram[39] (Fotoğraf paylaşma ve bu fotoğrafları düzenleme uygulamasıdır ayrıca uygulamada kullanıcılara fotoğraflara yorum yapabilme ve fotoğrafları beğenebilme özelliği de sunmaktadır.), Vimeo, Dailymotion ve Flickr örnek verilebilir[40]. Sosyal paylaşım sitesi YouTube 2005 yılında kurulmuştur. Çeşitli yöntem ve formatta dosya yükleme;

[37] Wikipedia Online Encyclopedia (E.T:12/08/2021).
[38] Güliz Uluç, Bilal Süslü, "Örnek Yargıtay Kararlarıyla Sosyal Medya Hukuku", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi** Cilt:8 Sayı:17, Aralık 2016, s. 351.
[39] İnstagram: https://help.instagram.com/519522125107875 (E.T:18/09/2021).
[40] Akkurt, s. 106, Wikipedia Online Encyclopedia (E.T:07/08/2021).

yüklenilen içeriğe erişebilecekleri seçme özellikleri taşıyan video paylaşım sitesidir[41].

c. Bloglar

Bloglar kısaca ağ ya da web günlüğü olarak açıklanmaktadır. Kelime aslında web ve log kelimelerinin birleşmesi ile oluşmuştur. Bloglar web sayfası üzerinden kolaylıkla oluşturulabilir. Okuyucu kitlesine yorumlar ve fikirler sunan günlüklerdir[42].

Bloglar sosyal medyanın en eski türüdür. Genellikle tek yazar tarafından yönetilir. Paylaşımlar ise ters kronolojik sıra ile yani güncelden eski tarihli olana göre sıralanır[43]. Paylaşımların sonunda yazarın adı ve paylaşımın yapıldığı zamana ilişkin bilgiler verilir. Ayrıca yazar okuyucuların hangi paylaşım için yorum yapabileceğini de belirler. En bilinen bloglar; blogspot, wordPress ve Tumblr gibi uygulamalardır[44].

d. Mikro Bloglar

Mikro bloglar, blogların daha küçük çaplı, sınırlı ve anlık özellik gösteren bir çeşididir. Kişiler için sınırlı sayıda karakterle mesajlaşma ve anlık fotoğraf, link ya da küçük çaplı içerik göndermesine imkan sağlar. Kaya'ya göre karmaşık yapıda olmaması, hızlı ve mobil araçlarla ulaşılabilir olması ve anlık iletişim sağlayan özelliği ile oldukça yaygın bit kullanım alanı olmuştur. Twitter, İnstagram ve Foursquare mikro blogların en bilinen türlerindendir. Ayrıca bu mikro blog üzerinden kişiler hem tanıdığı kişilerle iletişim kurabilir hem de ünlü kişileri takip edip onların düşünce ve paylaşımlarını görebilir. Twitter tweet adı verilen 10 karakterle sınırlı metinler yazıp paylaşmaya izin vermektedir. Kullanıcılar paylaştığı twettlere yorumlar yazılabilir ve twettleri retweetlenerek başka kişilerce yayılabilir.

[41] Wikipedia Online Encyclopedia (E.T: 12/08/2021).
[42] Erkan Akar, **Sosyal Medya Pazarlaması- Sosyal Webde Pazarlama Stratejileri**, Efil Yayınevi, Ankara, 2011, s. 45.
[43] Kaplan ve Haenlein, s. 63.
[44] Akkurt, s. 106, 107.

Twitterda kullanıcıların bahsettiği konular gündem olabilmektedir. Toplumun düşüncelerini öğrenmek açısından, siyasi veya ticari açıdan şirketler ve siyasetçilerin twitter da bulunma gereği duydukları söylenebilir. Kaya Instagram'ı da mikro blog başlığı altında değerlendirmektedir. İnstagram fotoğraf paylaşım mikro bloğu olarak değerlendirilebilir. Bu mikro blog da kullanıcılar fotoğraflarını düzenleyerek paylaşmaktadırlar[45]. Son zamanlarda farklı özelliklerle video paylaşımı konusunda da oldukça yeni özellikleri de mevcuttur. Fotoğraf özelliği yanında video paylaşımı ve fotoğraflı metin paylaşımları da yaygın olarak yapılmaktadır.

e. Wikiler

Wikiler, bloglara benzer ancak temel farklılığı birden çok yazara sahip olmaları ve gönderilerin kronolojik yapıda sıralanmamasıdır. Ayrıca wikilerde kullanıcılar içeriklerde sonradan değişiklik yapabilmektedirler[46]. Kısacası wikiler kullanıcılar için yorum yapıcı geniş katılım sağlayıcı içerik ekleme, düzenleme ve kategorize etme gibi imkanlar sağlamaktadır. Wikilerin en bilineni Wikipedia'dır. Wikipedia geleneksel ansiklopedilerin aksine bir ansiklopedi oluşturmuştur. Geniş içeriği ve içeriğin kullanıcılar saye sinde düzenlenebilir olması nedeni ile farklılaşmıştır. Ulaşılabilirlik ve farklı dil seçenekleri açısından kullanışlı olması iyice yaygınlaşmasını sağlamıştır[47].

f. Sosyal İşaretleme Siteleri

Sosyal işaretleme siteleri, bazı ögeleri kullanıcılar tarafından ulaşabilir kılan, saklayan, organize eden aynı zamanda yorum ve paylaşma gibi etkinlikler yapılmasına izin veren sitelerdendir. En önemli özellikleri ise online içeriği "izi sürülebilir" hale getirmeleridir. Kaydedilen yer işaretleri birçok kullanıcı tarafından

[45] Kaya, ss. 89-90
[46] Hawaii dilinde wiki hızlı anlamına gelmektedir. Wikipedia Online Encyclopedia (E.T: 12/08/2021); Akkurt, s. 108; Kaya, s. 94; Akar, ss.67- 69; Koçak, s. 61.
[47] Kaya s. 95; Akkurt, s. 108.

okunup yeni kaynakların keşfedilmesine imkan vermektedir[48]. Delicious adındaki site sosyal işaretleme sitelerinden en bilinenidir[49].

Kullanıcılar işaretlemek istedikleri web sitesi linklerini etiket bulutuna göndermekte ve bu şekilde diğer kullanıcılarla paylaşmaktadır. Diğer kullanıcılar bu etiketlemeler ve anahtar kelimeler ile bunlara ulaşabilmektedir[50].

g. Sanal Oyun ve Sanal Gerçeklik (Yaşam) Platformları

Sanal oyun platformları, kullanıcıların birbiri ile oyun oynaması ve bunu yaparken diğer kullanıcılarla anlık mesajlaşma ve grup kurma şekilden iletişimde olmalarını sağlamaktadır. Kullanıcıların avatar adı verilen kişiselleştirilmiş karakterleri sanal dünyada gerçek yaşamdaki birçok nesne ile ilgili kendi isteklerine göre değişimler yapabilirler. Özellikle bazı oyun türlerinde sanal dünyada kazanılan paraların gerçek dünyada karşılığı olmaktadır[51].

3. Sosyal Ağlardaki Başlıca Kısımların, İşlevlerin ve İşlemlerin, Kişisel Veri Kapsamına Giren Alanları

Devletlerin vatandaşlarını gözetlemesi ve sermaye gruplarının tüketicilerini gözetlemesi günümüzde yaygın bir durum iken son zamanlarda sosyal medya sayesinde bireylerin birbirlerini gözetlemesi olgusu ortaya çıkmıştır. Bu durum "gözetimin bireyselleşmesi" olarak adlandırılmaktadır. Sosyal medya kullanımının yaygınlaşması, iletişim teknolojilerinin küçülmesi ve cebe girecek boyutlara gelmesi ile birlikte kullanıcılar birbirlerinin nerede, ne yaptığından anlık olarak haberdar olabilmektedir. Ulaşımın bu kadar kolay olması mahrem ilişkilerde önemli değişimlere ve bir takım toplumsal sorunlara yol açmaktadır[52]. Söz konusu olan

---

[48] Akar, ss. 78, 80.
[49] Kaya, s. 95; Wikipedia Online Encyclopedia (E.T:12/08/2021)
[50] Akkurt, s. 108.
[51] Akkurt, s. 109; Kaya, ss. 96, 97.
[52] "*Pek çok kişi bloglarda, facebookta ve benzeri sitelerde sınırlı olduğunu düşündüğü bir grup için hayatını sergimektedir. Teşhir ve narsizmin söz konusu olduğu bir görülme arzusu ortaya çıkmıştır. Bu konudaki en meşhur örnek 1996'da Jennifer Ringley adındaki bir genç kızın evine yerleştirdiği kamerayla bütün özel hayatını internetten yayınlamasıdır ki bu durum "Jennicam" olarak kavramlaşmıştır. Hal Niedzvieck "Dikizleme Günlüğü" adlı kitabında pek çok benzer örnek*

sorunların da hukuki düzenlemelerin yapılması gerekliliğini doğurduğu anlaşılmaktadır.

Sosyal medyada yapılan paylaşımların hukuki ve cezai sorumluluğu konularından söz edebilmek için bu alana özgü paylaşımların niteliklerini daha iyi açıklamak gereklidir. Örneğin yapılan paylaşımın kimlerce görülebileceği yani aleni olup olmadığı ve rıza büyük önem arz etmektedir[53]. Bu konu çalışmamızda ceza hukuku yönünden yapacağımız değerlendirmelerin de dayanak noktasını teşkil edecektir.

Sosyal medyada saklanan veriler çeşitli şekillerde elde edildiği görülmektedir. Bunları kısaca üç grupta incelemek mümkündür. Birinci grup üye kişilerin kendi rızaları doğrultusunda kullanıcı olarak sosyal medya hesaplarında ekledikleri bilgilerdir. Şirketler bu verileri sunucularında saklamaktadır. Diğer kullanıcılar tarafından da bu veriler genellikle görülüp kaydedilebilir şekilde açıktır. Ancak bazı istisnai bilgiler erişime açık değildir. İkinci grup ise kullanıcı sosyal medyayı kullanırken bu uygulama tarafından otomatik olarak elde edilen bilgilerdir. Bu veri trafiği muhafaza edilmektedir. Kısaca bunlara log kayıtları veya kütük bilgileri denilmektedir. Üçüncü grup ise bir sosyal medya kullanıcısının bizzat kendisinin sosyal medya platformunda paylaştığı ve kaydettiği verilerdir. Bunlar her türlü yazı, resim, video, ses, beğenme, etiketleme, dürtme, konum paylaşımı gibi verilerdir. Bahsedilen veri grupları silinmediği sürece sosyal medyada kayıtlı bulunmaktadır. Hatta bazı verilerin silinmesi mümkün değildir. İkinci grupta bahsettiğimiz üzere veri trafiklerinin kullanıcı tarafından silinmesi mümkün değildir. Yani bu gruptaki veriler ve otomatik tutulan veriler üzerinde kullanıcının inisiyatifi bulunmamaktadır[54]. Örneğin Facebook 69 kategoride veri bulundurmaktadır[55].

Sosyal medyada milyonlarca kullanıcı bulunmaktadır. Bu kullanıcıların suçlu olup olmadığı ya da psikolojik sorunları olan insanlar olup olmadığı hakkında kimsenin net bilgisi yoktur. Bu mecrada yapılan paylaşımlar izlenir, kaydedilir ve

---

vermektedir." Bkz. Kübra Kuruoğlu, "Dijital Ortamda Panoptisizm", **Akademik Sosyal Araştırmalar Dergisi**, Sayı: 31, Ekim 2016, ss. 260-261.

[53] Akkurt, s. 111.

[54] Yetim, s. 303.

[55] Ayrıntılı bilgi için bkz. Yetim, ss. 299-300.

bazen de başka kişilere yayılır[56]. Sosyal medyada bazı "fenomen" olmaya çalışan kişiler için sık sık gönderi paylaşmak ve daha görülür hale gelmek amaçlanmaktadır. Bu kişilere özenen diğer kullanıcılar da benzer şekilde davranarak önemli ya da önemsiz nitelikte olan verisini paylaşır. Ancak bu aşamada kişi paylaştığı verinin kontrol edilemez hale geleceğini düşünmez. Daha sonra bu paylaşımı hakkında fikri değişen kullanıcının gönderisi binlerce kişiye ulaşmış olacaktır. Özellikle bilinçsiz kullanıcılar verisinin niteliğini değerlendirmeden paylaşım yapmakta bu şekilde bazen kimlik numaralarını, kredi kartı bilgilerini, ev adreslerinin ya da mahrem görüntülerini paylaşmaktadırlar. Kişilerin sonradan pişman olarak ya da farklı sebeplerle kendi paylaşım sayfasından sildiği veriler kişilerce ya da şirketlerce çoktan depolanmış olmaktadır. Kişilerin paylaşımlarını yaptıkları platformlardan bu verilerini silmeleri dijital dünyada bu verilerin silindiği anlamına gelmemektedir[57].

Sosyal medyada veri paylaşımı yapılan başlıca işlemler ise şunlardır:

a. Profil

Sosyal medya hesabı açmak isteyen her kullanıcı adayı kendisinden talep edilen bazı bilgiler vardır. Bu bilgilerin bir takımı zorunlu iken bir kısmı ihtiyaridir. Zorunlu bilgiler olarak genellikle e posta adresi, ad, soyadı ya da daha önce açıkladığımız gibi müstear ad, doğum tarihi ve en sonunda da hesap şifresi talep edilir. Bu bilgiler hesap açılması için verilmesi gereken verilerdir. Bunlar dışında cinsiyet, medeni durum, resim, yaşanılan şehir, eğitim, okul, çalışılan kurumlar gibi ihtiyari olarak paylaşılacak veriler de bulunmaktadır[58].

Kullanıcıların profilleri kendisi bizzat gizleme özelliğini kullanmazsa herkes tarafından görülebilir halde olur. Ancak kişi profilindeki gizlilik ayarlarını kullanarak profilini gizleyebilir bu durumda sadece arkadaşı olan kişiler kullanıcının profilindeki bilgi ve paylaşımlarını görebilecektir[59]. Ancak kişilerin profili ne de

[56] Ali Büyükarslan ve Murat Kırık, **Sosyalleşen Birey, Sosyal Medya**, Çizgi Kitapevi, Konya, 2014, s. 47.
[57] Güney Nair ve Emine Balta, "Bilgi İletişim Teknolojileri Kullanımında Sınırları Aşan Bir Sosyal Sorun Alanı Olarak Unutulma Hakkı" **CÜ Sosyal Bilimler Dergisi**, Aralık 2017, Cilt: 41, Sayı: 2, s. 118.
[58] Akkurt, ss. 111-113. Yetim, s. 302.
[59] Akkurt s. 114.

kadar gizli olsa da son dönemde gizli hesapları görüntüleme amacıyla çeşitli yazılımlarla uygulamalar oluşturulmuştur. Bu tarz uygulamalar, uygulamayı kullanan kişilerin arkadaşı olan ve kendi profilleri herkese açık olamayan kullanıcıların profillerini rıza dışı alenileştirmektedir. Yazılımlar virüs gibi hareket ederek uygulamayı indiren kullanıcının sosyal medyadaki tüm bilgilerini ve arkadaşlarının profil bilgilerini elde etmektedir. Bu yazılımların çoğu belli bir noktada hizmet alanlarında ücret istemektedir[60]. Söz konusu durumun sosyal medyada hesaplarını gizli tutmak isteyen kullanıcıların verilerinin rızaları dışında bu şekilde paylaşıma açıldığı ve ticari amaçlarla kullanıldığı görülmektedir.

Yapılan bir araştırma facebook ve twitter kullanıcıların herkese açık hesaplarını inceleyerek kullanıcıların ilerdeki paylaşımlarının nasıl olabileceğini analizlerin etmektedir. Çalışma kullanıcıların arkadaşlarının hesapları, kullanıcıların hesaplarından arkadaşlarına attığı bağlantılar ve mesajları analiz edilerek yapılmıştır. Bu analizler sonucunda kullanıcının ileride yapacağı paylaşımlar yüzde 95 oranında doğru tahmin edilmiştir. Bu bizi kullanıcılar sosyal medya hesabından herhangi bir paylaşım yapmasa dahi sosyal medyada arkadaş listesinde yer alan kişilerin tek başına yaptığı paylaşımlarla ya da bu arkadaşları ile etkileşimlerine bakılarak kişinin özel hayatına dair önemli verilerin elde edilebileceği sonucuna ulaştırmaktadır. Şu cümleler durumu özetlemektedir: *"Sosyal medya platformlarında mahremiyetinizi tek başınıza kontrol edemezsiniz. Bu konuda arkadaşlarınıza da iş düşüyor."* [61]

Sosyal medya içerik sağlayıcıların kişisel veriler noktasındaki sorumlulukları kullanıcı adaylarının profil oluşturmak için paylaşması zorunlu olan bilgileri ile sınırlı olmaktadır. Kişinin rızası ile herkesçe görüntülenmesini engellemediği yani hesap ayarlarında bazı verilerini gizlemediği müddetçe bunlardan dolayı içerik sağlayıcının sorumluluğu doğmayacaktır. Örneğin kişinin e posta adresi ya da fotoğrafı herkesçe görünebilir şekilde hesap ayarlarında düzenlenmiş olabilir. Ancak bunlar gizlendiği halde üçüncü kişilerce bu ihlal edilirse içerik sağlayıcının da

[60] İlgili uygulamalara ilişkin örnekler:
https://webhakim.com/instagram-gizli-hesap-gorme-uygulamasi.html,
https://www.webtekno.com/instagram-gizli-profilleri-gosteren-web-sitesi-ortaya-cikti-h98955.html
(E.T:12/09/2021).

[61] Andrew Griffin, "Sosyal Medyada Henüz Yazmadıklarımız Bile Gizli Değil", (Çev. Demrikol, Elvide) **İndependent Türkiye**, 22/01/2019,
https://www.indyturk.com/node/10186/haber/sosyal-medyada-hen%C3%BCz-yazmad%C4%B1klar%C4%B1n%C4%B1z-bile-gizli-de%C4%9Fil (ET:14/06/2021).

sorumluluğu doğacaktır. Söz konusu sorumluluğu TMK, TBK, KVKK ve FSEK kapsamında olmaktadır[62].

Sosyal medya platformlarında kişiler profil oluştururken aslında başta profilinde paylaştığı bilgiler daha sonrasında da bu platformların olanak sağladığı paylaşım türleri ile kendisine bir kimlik oluşturmaktadır. Bu noktada kişilik ve kimlik kavramlarına değinmek gerekir. Kişiliğin bireysel ve bireye özgü olan manevi nitelikleri olduğunu ancak kimliğin toplumsal, politik ve ekonomik etkenlerle şekillenen bir husus olduğu ifade edilmektedir. Kullanıcılar oluşturdukları profilde yaptıkları paylaşımlarla sosyal medya aracılığı ile kimlik oluşturmaya çalışmaktadır. Kişiler oluşturdukları kimliklerle tanınır hale gelmektedir. Günümüzde kişiler bu mecrada tanınırlıklarını arttırmak ve takipçi sayılarını arttırmak için farklı kimlikler oluşturmaktadır. Kişiler nasıl tanınmak ve anılmak isteniyorlarsa ona uygun bir vitrin yani bir profil oluşturup bu vitrinde *"cinsiyet, yaş, ırksal özellikleri, boy, görünüş, duruş şekli, konuşma kalıpları, yüz ifadeleri, konum, meslek"* gibi hususları sergilemektedir. Bu kişisel özellikler sosyal kimliğin inşasını sağlamaktadır [63].

Facebook ve instagram gibi uygulamaların hesaplar silinse bile veri saklama süresi için kendi kuralları bulunmaktadır[64]. Aynı şekilde twitter da bu konuda bazı kurallara sahiptir. Buna göre twitter da temel hesap bilgileri ve kamusal bilgiler ayrımı yapmaktadır. Profilleri oluştururken girilen e posta adresi, telefon numarası, ad ya da takma adları temel hesap bilgileri olarak adlandırmaktadır. Hesabın aleni olup olmaması kullanıcının takdirindedir. Twitter gizlilik politikasında kamuya açık hale getirilen verilerden ve atılan tweetler, retweet, beğenilerinizden kullanıcı olarak

---

[62] Akkurt, ss. 114, 115.

[63] Çetin, s. 780.

[64] *"Hizmetlerimizi ve Facebook Ürünleri'ni kullanımınıza sunmamız için gerekli olduğu süre boyunca ya da hesabınız silinene kadar (hangisi önce gerçekleşirse) verileri saklıyoruz. Verinin niteliği, toplanma ve işlenme nedeni, ilgili yasal veya idari saklama gereklilikleri gibi unsurlar göz önünde bulundurularak her veri için duruma özel bir karar verilir. Örneğin Facebook'ta bir şeyi aradığınızda, yaptığınız sorguyu istediğiniz zaman arama geçmişinizden silebilirsiniz. Ancak yaptığınız aramanın kaydı 6 ay sonra silinir. Hesabınızın doğrulanması için bir devlet kurumu tarafından verilmiş kimliğinizin kopyasını gönderirseniz aksi belirtilmediği takdirde bu kopyayı inceledikten 30 gün sonra sileriz. Paylaştığınız içeriklerin silinmesi ve sosyal eklentiler aracılığıyla elde edilen çerez verilerinin silinmesi hakkında daha fazla bilgi alın .Hesabınızı sildiğinizde, fotoğraflarınız ve durum güncellemeleriniz gibi paylaşmış olduğunuz içerikleri sileriz. Bu bilgileri daha sonra geri alamazsınız. Başkalarının sizin hakkınızda paylaştığı bilgiler hesabınızın bir parçası değildir ve dolayısıyla silinmez. Hesabınızı silmek istemiyor ama Ürünleri kullanmayı geçici olarak bırakmak istiyorsanız hesabınızı silmek yerine dondurabilirsiniz. Hesabınızı silmek isterseniz lütfen Facebook Ayarları'nı ve Instagram Ayarları'nı ziyaret edin."* https://help.instagram.com/519522125107875 (E.T:12/09/2021).

kendiniz sorumlusunuz demektedir[65]. Her üç sosyal medya uygulamasının en önemli özelliği kişiselleştirilmiş reklamlardır. Özellikle facebook ve instagram ortak facebook (Meta) şirket birliği altında aldığı onaylarla bu konuda ticari amaçlı veri paylaşımı yapmalarıdır. Yakın tarihte söz konusu şirketle ilgili facebook skandalı kişisel verilerin güvenliğinin önemini ortaya koymuştur[66].

b. Gönderi, Paylaşım, Hikaye, Reels, Tweet, Retweet

Gönderiler sosyal medyada kullanıcılarının duygu, bilgi ve düşüncelerini yazılı, görsel ya da işitsel olarak yaptıkları paylaşımlardır. Her sosyal medya ağında farklı isimlerle adlandırılsa da gönderi özel yazışma niteliği olamayan genellikle herkese yönelik olan temel paylaşım şeklidir. Kullanıcılar bu paylaşımlara ulaşabilir, katkıda bulunabilir ve bu paylaşımlar diğer kullanıcıların yeni paylaşımlar yapmasına aracılık edebilir[67]. Paylaşım yapma sosyal medya platformlarında farklı isimlerle adlandırılmaktadırlar.

Facebook ve instagramda fotoğraf, video paylaşma özelliklerinin çeşitleri vardır. Örneğin instagramda hikayeler adlı gönderi seçeneği ile süreli paylaşım yapma ya da instagram kamerası kullanarak 60 saniyelik özel efektli veya müzikli videolar düzenleyip bunları paylaşma imkanı sağlamaktadır[68]. Bu özellikler uygulamaya özgüdür. Benzer özellikler facebook uygulamasında da bulunmaktadır.

Twitter da ise temel gönderi şekli tweet olarak adlandırılmaktadır. Kullanıcılar tweetle butonuna tıklayarak en fazla 280 karakterden oluşan yazı yazabilir. Tweetlerde doğrudan yazı dışında en fazla 4 fotoğraf paylaşılabilir. Ayrıca bir gif veya bir de video paylaşılabilir. Ayrıca twitterda da herkese açık ya da korumalı hesap seçeneği bulunmaktadır. Herkese açık olması sosyal medya platformlarında varsayılan ayardır ve bu ayar değiştirilerek hesap korumalı hesap haline dönüştürülebilir. Korumalı hesap olduğunda kullanıcıların tweetleri, retweetleri gibi gönderileri yalnızca kullanıcının takipçileri tarafından

[65] https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-aug-19th-2021/Twitter_Privacy_Policy_EN.pdf (E.T:12/09/2021).
[66] https://www.webtekno.com/mark-zuckerberg-den-veri-skandali-aciklamasi-hata-yaptik-ayrica-bunlar-buz-daginin-gorunen-kismi-h42795.html (E.T:12/09/2021).
[67] Kietzmann/Hermkens/Mccarthy/Silvestre s. 245; Kaya, s. 85; Akkurt, s. 116.
[68] https://help.instagram.com/519522125107875 (E.T:12/09/2021).

görüntülenebilir. Kullanıcı kendisine gönderilen takip isteklerini onaylayabilir ya da reddedebilir. Bu şekilde gönderilerini kimlerin görebileceğini belirlemektedir[69]. Retweet etmek kısaca başka bir kullanıcının tweetini paylaşmak anlamına gelmektedir. Bu işlem kullanıcının profilinde arkadaşları (takipçileri) tarafından ya da herkese açık hesapsa diğer kullanıcılar tarafından da görülebilecektir[70].

Günümüzde retweet yoluyla yapılan paylaşımların cezai sorumluluğa sebep olup olmayacağı konusu tartışılmaktadır. Kullanıcı tarafından bir gönderi retweetlendiğinde cezai sorumluluğu değerlendirilirken suç tipine bakmak önemlidir. Örneğin Müstehcenlik Suçu konusunda düzenlemenin yer aldığı TCK m. 226/2'de *"Müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi altı aydan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır."* düzenlemesi bulunmaktadır. Mevzuatta düzenlenen aracılık etme ifadesi retweetleme ile oluşan duruma uygun görünmektedir. Kullanıcı retweet yaparak gönderi içeriğin yayınlanmasına ve yayılmasına önemli bir etki sağlamaktadır[71].

Gönderilerin varsayılan şekli genellikle herkese açık olduğu için kişilerin şeref ve haysiyetine, özel hayatın gizliliğine, fikri mülkiyet hakkına, iktisadi bütünlüğe, ifade özgürlüğünün sınırlarına aykırı ya da kişilik hakkı ihlallerine yol açabilecek içerikler barındırmaktadır. Hesabın korumalı olması kullanıcının gönderilerinde yer alacak olan verilerinin korunması açısından önem arz etmektedir. Hukuki karşılığı rıza kavramına denk gelmektedir. Verilerin üçüncü kişilerce öğrenilmesine rıza gösterilmediği anlamına gelmekte ve içerik sağlayıcıların ve üçüncü kişilerin buna aykırı eylemlerinin hukuki ve cezai sorumlulukları doğabilecektir[72].

c. Zaman Tüneli (Zaman Akışı) ve Duvar (Haber Kaynağı)

[69] https://help.twitter.com/tr/using-twitter/how-to-tweet (E.T:14/09/2021).
[70] Yetim, s. 275.
[71] Rıdvan Yıldız, Sosyal Medyada Konusu Suç Teşkil Eden İçeriğin Paylaşılması, https://www.bartin.info/sosyal-medyada-konusu-suc-teskil-eden-icerigin-paylasilmasi-makale,1772.html (14/11/2021).
[72] Akkurt, s. 117, 118.

Zaman tüneli kavramı sosyal medya platformlarında facebook da kullanılmaktadır. Kısaca kullanıcının gönderilerinin listelendiği paylaşım sayfası olarak açıklanabilir. Kullanıcı önceki gönderilerini bir albüm haline getirebilir. Twitter ve instagram da olduğu gibi burada da kullanıcı gönderi sayfasının herkese açık olup olmayacağı konusunda karar verebilmektedir. Zaman tünelinde kullanıcı geçmişte paylaşılanları görüntüleyebilir, yapılanların genel dökümlerinin inceleyebilir, kişisel albümüne görsel ekleyebilir, anlık durum güncellemeleri yapabilir bu gibi farklı seçenekler bulunmaktadır[73].

Facebook kullanıcılarının zaman tünelinde duygularını paylaşmak istediğinde aklından neler geçiyor şeklinde yazan kısma yazı ve emojiler kullanarak paylaşım yapmasına duvara yazmak denilmektedir[74]. Başka bir tanımda ise kullanıcıların gönderilerinin ve paylaşımlarının kullanıcının belirlediği önem sırasına ya da kronolojik sıraya göre sıralanan paylaşım sayfasına duvar (haber kaynağı) denilmektedir. Bu alan da herkese açıktır ancak kullanıcılar için bu alanda da farklı gizlilik ayarı alternatifleri sunulmaktadır. Kullanıcının özel alanı olacağı ya da herkese açık bir alanı olacağı konusunda seçim hakkı burada da bulunmaktadır[75].

d. Yorum Yapma Ve Duygu Belirtme

Yorum yapma twitter, facebook ve instagram adlı sosyal medya platformlarının hepsinde bulunmaktadır. Kullanıcılar başka bir kullanıcının herkese açık gönderisine yorum yapabilir. Kullanıcılar herkese açık gönderilerine kullanıcıların yorum yapmasını da ayarlardan engelleyebilir. Örneğin kullanıcılar yalnızca arkadaşlarım yapabilir ya da arkadaşlarımın arkadaşları gibi seçenekleri kullanabilir[76].

Yorum yaparken kullanıcılar yazı ile gönderi sahibi kişilere karşı küçük düşürücü ifadeler veya özel hayatın gizliliğinin ihlaline yönelik açıklamalar

[73] https://tr-tr.facebook.com/help/search?query=zaman%20t%C3%BCneli (E.T:17/09/2021); Akkurt, s. 120, 121; Yetim, s. 274.
[74] Yetim, s.274.
[75] Akkurt, s. 121.
[76] https://tr-tr.facebook.com/help/1719980288275077/?helpref=hc_fnav (E.T:14/09/2021). https://help.instagram.com/519522125107875 (E.T:12/09/2021). https://help.twitter.com/tr/using-twitter/how-to-tweet (E.T:14/09/2021).

yapabilirken ayrıca emoji olarak ifade edilen insan duyguları karikatürize etmeye yarayan şekiller aracılığı ile de olumsuz yorum yapabilirler. Söz konusu emojiler olumlu veya olumsuz birçok duyguyu ifade edebilecek şekilde tasarlanmıştır[77].

Sosyal medya platformlarının yapılan yorumları sınırlandırmaya yarayan özellikleri bulunmaktadır. Bu özellik sayesinde bazı kullanıcıların yorum yapması ya da yapılan yorumların görülmesinin engellenmesi mümkündür[78].

e. Konum Bilgisi Ekleme

Sosyal medya kullanıcılarının bulundukları yeri ifade etmek, bir resmin ya da videonun nerede çekildiğini belirtmek gibi amaçlarla kullanılmaktadır. Akıllı cihazlardaki GPS özelliği ya da uygulamaların kendi özellikleri kullanılarak kullanıcıların yaklaşık konumunun belirlenmektedir. Sosyal medya şirketleri konum bilgileri ile kullanıcılara bulundukları konuma uygun olarak kişiselleştirilmiş hizmetler sunmaktadır[79].

Kullanıcıların bu şekilde paylaşmış oldukları konum bilgisi paylaşılma şekillerine göre değerlendirilmelidir. Kullanıcı konum bilgilerini herkese açık olacak şekilde bir gönderide paylaşması ile yalnızca doğrudan belli bir kullanıcıya göndermesi farklı sonuçlar doğurmaktadır. Herkese açık hesabı üzerinden konum bilgisini twitter da tweet atmış, instagram da bir gönderisinde paylaşmış ya da facebook duvarına yazmış ise bu verisini rızayla açıklamıştır[80].

f. Etiketleme

---

[77] Akkurt s. 122.

[78] İnstagram kişilerin yorum yapma özelliğinin sınırlanabileceğini belirtmektedir. *"Birinin yorum yapmasını engellediğinizde bu kişi fotoğraf ve videolarınızı görmeye devam edebilir. Bu kişinin yapacağı yeni yorumları, kendisinden başka kimse göremez."* https://help.instagram.com/234506470408555/?helpref=related_articles (E.T:22/01/2022).
"Birisinin gönderilerime yorum yapmasını geçici olarak sınırlayabilir miyim?
Evet. Tacize uğradığınızı hissederseniz hesap gruplarından istenmeyen yorumları ve mesajları geçici olarak sınırlayabilirsiniz. Bunlar ya son bir haftada sizi takip etmeye başlamış hesaplar ya da sizi takip etmeyen ancak spam, sahte olabilecek veya sizi taciz etmek için oluşturulmuş hesaplardır.
Kişileri bir seferde dört haftaya kadar sınırlayabilirsiniz ancak bu süreyi istediğiniz kadar uzatabilirsiniz."
https://help.instagram.com/4106887762741654/?helpref=search&query=yorum%20kapat&search_session_id=ae3cff9c95bd55542431b695948f40e5&sr=19 (E.T:22/01/2022).

[79] Yetim, s. 276.

[80] Akkurt, s. 124.

Etiketleme (@ işareti) bir kullanıcının başka bir kullanıcıyı bir gönderi ile gönderiye ulaşabilecek herkesin anlayabileceği şekilde ilişkilendirmesidir. Etiketleme ile diğer kullanıcılar etiketlenen kullanıcının profiline ulaşabilmektedir. Bir nevi köprü görevi görmektedir[81].

Kullanıcılar facebook yüz tanıma sistemini kullanıldığında facebook tarafından gönderilerin içinde resimde yer alan kullanıcı belirlenip bu kişi size önerilmektedir. Bu şekilde kullanıcılar daha hızlı etiketlenmektedir. Ayrıca facebook yüz tanıma özelliğini kullanarak kullanıcıdan habersiz resminin başka bir kullanıcı tarafından paylaşıldığında bunu tespit edip kullanıcının haberdar olmasını sağlamaktadır[82].

Etiketleme ile kişilerin rızası dışında bir paylaşımda yer alması ihtimali oldukça fazladır. Kişilerin resimleri etiketlenerek paylaşılmasına rıza göstermedikleri kişilerin kişisel ilişkileri ifşa edilebilir veya özel hayatının gizliliği ihlal edilebilir[83].

g. Doğrudan/Direct Mesaj

Sosyal medya platformlarında kullanıcıların özel yazışma alanları olan kısımlar doğrudan ya da direct mesaj olarak adlandırılmaktadır. Bu alanlarda sohbet grupları da oluşturulabilmektedir[84].

---

[81] Akkurt, ss. 124, 125.

[82] *"Yüz tanıma, sizin için şablon adında benzersiz bir numara oluşturmak üzere, Facebook'ta içinde olduğunuzu düşündüğümüz, profil fotoğrafınız ve etiketlendiğiniz fotoğraf ve videolar gibi fotoğraf ve videoları analiz etmek için kullanılır…Unutmayın, şablonunuzu hiç kimseyle paylaşmayız…Yüz tanıma ayarınızı açarsanız, hesabınız aktif olduğu sürece şablonunuzu tutacağız ama yüz tanıma ayarınızı kapatırsanız şablonunuzu sileceğiz. Şablonunuzu sizin dışınızda hiç kimseyle paylaşmayız. Bir fotoğraf veya videodan etiketiniz kaldırılırsa, o fotoğraf veya videoyu yüz tanıma şablonu kapsamında sizi tanımak için kullanmayız. Yüz tanıma, sadece 18 yaşından büyük kişilere sunulur. 18 yaşından küçük kişilerde yüz tanıma ayarı bulunmaz. Tanımadığınız kişilere kim olduğunuzu söyleyen yüz tanıma özelliklerimiz yoktur."* https://tr-tr.facebook.com/help/122175507864081/?helpref=search (E.T:17/09/2021).

[83] Akkurt, s. 125.

[84] *"Facebook'taki herkese mesaj gönderebilirsiniz. Arkadaş olmadığınız kişilere gönderdiğiniz mesajlar bu kişilerin Mesaj İstekleri klasörüne düşebilir.*
Ayrıca mesajlarınız Facebook sohbetinde veya Messenger'da sizi engellemiş olan kişilere ulaşmaz."
https://tr-tr.facebook.com/help/438779846195810/?helpref=search (E.T:17/09/2021).
https://help.twitter.com/tr/using-twitter/direct-messages#things-to-know (E.T:17/09/2021).
"*Instagram Direct, bir veya birden fazla kişiye mesaj göndermenize olanak tanır. Instagram Direct'te şunları mesaj olarak gönderebilirsiniz: Çektiğiniz ya da kütüphanenizden yüklediğiniz fotoğraflar veya videolar, Akışta gördüğünüz gönderiler, Kaybolan fotoğraf ve videolar, Profiller, Metin, Konu*

Direct mesajın kullanıcıların özel hayatı ile ilgili bir alan olduğu söylenebilecektir. Kişilerin özel alanı olarak değerlendirilmekte hatta mesaj içeriklerine göre mahrem alan olarak da değerlendirilebilecektir. Örneğin günlük hayata ilişkin rutin konuşmaların yapıldığı bir durumda bu konuşmalar özel hayat alanı olarak kategorize edilecekken mesaj içeriklerinin kişilerin cinsel hayatına ilişkin olması bu konuşmaları mahrem hayat alanına ilişkin kategorize etmeyi gerektirecektir. Kullanıcıların bu kısımda yaptığı konuşmalar üçüncü kişilere açıklanmasına ya da paylaşılmasına ilişkin açık rızalarının olmadığı şeklinde değerlendirilmelidir. Ancak kişilerin rıza vermesi de mümkündür. Rıza dışı olarak bu konuşmaların ekran görüntüsü alınarak sosyal medyada başka kullanıcılarla paylaşılması hukuki ve cezai sorumluluk doğuracak TCK anlamında özel hayatın gizliliğine ilişkin suç tiplerini oluşturabilecektir[85].

h. Konu Başlığı/Hashtag (Sosyal Medya Künyesi)

Sosyal ağ künyesi kullanarak yapılan paylaşımlar bulunmaktadır. Bu paylaşımların herkese açık olması durumunda ilgili hashtag (# işareti) kullanılarak paylaşımlara ulaşmak oldukça kolaydır. Özellikle yapılan faaliyetlere ilişkin kullanılan sosyal ağ künyeleri altında büyük etkileşimlerin olduğu görülmektedir[86]. Kişiler hakkında düşünce bildiren yazılar ya da resim video gibi paylaşımlar bu konunun önüne # işareti kullanılarak yapılmaktadır. Anayasa Mahkemesine bireysel başvuru konusu olan olayda Twitter'da siyasetçinin ve siyasetçinin görüşleri karşısında kullanıcıların herkese açık olacak şekilde düşüncelerini paylaşılması ve bu paylaşımlar sonucunda siyasetçinin hakkında hashtag başlığı altında yapılan yorumlar yapılması olayında ilk derece mahkemesinde hakaret suçunun oluştuğunda dair karar vermiştir. Bireysel başvuru incelemesinde olayın herkese açık bir sosyal medya platformunda ve tarafların da herkese açık bir şekilde paylaşımlar yaptığının

---

*etiketleri, Konumlar. Instagram Direct ile gönderilen fotoğraflar ve videolar, Instagram aracılığıyla Facebook veya Twitter gibi diğer internet sitelerinde paylaşılamaz ve konu etiketi ve konum sayfalarında görünmez."*https://tr-tr.facebook.com/help/instagram/684926628219030/?helpref=search (E.T:17/09/2021).
Kaya, s. 85; Akkurt, s. 125.

[85] Akkurt, s. 126, 127.

[86] Turan, s. 308.

yani somut olayın iyi değerlendirilmesi gerektiğini ve ifade özgürlüğünün ihlali kararı vermiştir[87].

Bahsettiğimiz kategorilerde açıkladığımız üzere genel olarak sosyal medya içerik sağlayıcılarında tutulan verileri şu şekilde sayabiliriz[88]:

Birinci kategoride verinin üretim durumuna göre üç durum ortaya çıkmaktadır.

a. Sosyal medya kullanıcısının bizzat kendisi tarafından paylaşılan veriler,

b. Sosyal medya platformu tarafından otomatik olarak tutulan veriler,

c. Sosyal medya platformları tarafından analiz edilerek çıkartılan veriler.

İkinci kategoride:

a. Sadece sosyal medya platformunda tutulan veriler,

b. Sosyal medya platformu ve sosyal medya kullanıcısında ortak tutulan veriler.

Üçüncü kategoride:

a. Herkesin erişimine açık olan veriler,

b. Sınırlı kişinin/grubun erişimine açık olan veriler.

Dördüncü kategoride:

a. Sadece mahkeme kararı ile verilecek veriler,

b. Mahkemeler tarafından arama kararı ile verilerek elde edilebilen veriler,

c. Güvenlik amacıyla sosyal medya platformları tarafından devlet kurumları ile paylaşılan veriler.

d. Herhangi bir şekilde mahkeme arama kararı verilmeksizin ulaşılabilecek veriler

Beşinci kategoride:

a. Veri bütünlüğü zayıf olan veriler,

b. Veri bütünlüğü ve doğrulaması kuvvetli olan veriler.

Altıncı kategoride:

---

[87] AYM Başvuru No: 2015/13431 Tarih 23/05/2021; Mahkeme siyasetçilere yönelik eleştirilerin sınırlarının daha geniş olduğundan ve bu konuda daha hoşgörülü olunması gerektiğinden bahsetmiştir. *"45. Öte yandan başvuruya konu olay, tarafların yaşamının diğer bireylere kapalı ve mahrem alanına ilişkin değildir. Başvurucunun paylaşımı, basında ve kamuoyunda kürtaj konusuyla ilgili devam eden tartışmalarla ilgili olarak davacının paylaşımı üzerine yapılmıştır.*
46. Başvuru konusu olayın şartları ve arka planı dikkate alındığında başvurucu tarafından yapılan paylaşım ve paylaşımda kullanılan ifadeler olgusal bir temele sahiptir. Şöyle ki…şeklindeki doğrudan mesajının sosyal medyada yayılması üzerine yapılmıştır. Başvurucu, paylaşımıyla davacının paylaşımına yönelik eleştirilerini ifade etmiştir.
48. Açıklanan gerekçelerle başvurucunun Anayasa'nın 26. maddesinde güvence altına alınan ifade özgürlüğünün ihlal edildiğine karar verilmesi gerekir."

[88] Yetim, ss. 298, 299.

a. Hassas kişisel veri niteliği taşıyan,

b. Hassas kişisel veri niteliği taşımayanlar.

Yedinci kategoride:

a. Paylaşılması bizzat suç olanlar,

b. Paylaşılması bizzat suç olmayanlar.

Sekizinci kategoride:

a. Hesap sahibi tarafından paylaşılanlar,

b. Diğer kullanıcılar tarafından paylaşılanlar.

Dokuzuncu kategoride:

a. Sosyal medya kullanıcısı tarafından üzerinde tasarruf hakkı olan veriler,

b. Sosyal medya kullanıcısı tarafından üzerinde tasarruf hakkı olmayan veriler.

Onuncu kategoride:

a. Yoruma açık olanlar,

b. Yoruma açık olmayanlar.

On birinci kategoride:

a. Sistem tarafından şifreli olarak tutulan veriler,

b. Sistem tarafından şifreli olarak tutulmayan veriler.

On ikinci kategoride:

a. Yazılı olanlar,

b. Görsel olanlar,

c. İşitsel olanlar.

Bu şekilde kategori oluşturmak veri türlerini anlamak açısından yararlı olmaktadır.

II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL KAVRAMLAR

A. Veri ve Kişisel Veri Kavramı

1. Kişisel Veri Kavramı ve Unsurları

Anayasamızın[89] 20. maddesinin 3. fıkrasında kişisel verilerin korunmasına ilişkin anayasal ilkelere yer verilmiştir. Maddede *"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."* denilmektedir. Söz konusu Anayasal düzenleme 2010 yılında yapılmıştır. Anayasa değişikliği özel hayatın gizliliği başlığını içeren maddede altında yapılmıştır. Öncesinde hukukumuzda kişisel veriler konusuna doğrudan değinen anayasal bir düzenleme bulunmamaktaydı.

Kişisel veriler kavramının uluslararası bir belgede ortaya konuluşu 1980'de Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından yayınlanan Kişisel Verilerin Sınır Aşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri ile olmuştur. Bu ilkeler bağlayıcı nitelikte değil de konsey tavsiyesi niteliğinde kararlar olmuştur. Ancak bu belge öncesinde özellikle ABD'de kredi notlandırma gibi ekonomik konularla ilgili düzenlemeler yapılmıştır. 1970 yılında Almanya'nın Hessen eyaletinde kişisel verilere ilişkin kanuni düzenleme yapılmıştır[90]. Daha sonraki yıllarda ülkeler bazında olan düzenlemeler daha fazla uluslararası boyut kazanmış ve bağlayıcı nitelikte olmaya başlamıştır.

Avrupa Konseyi kaynaklı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme" üye ülkelerin dağınık ve bölünmüş mevzuatını uyumlaştırmayı ve belli standartlar oluşturmayı amaçlamaktadır. 108 sayılı Sözleşme veri koruma alanındaki bağlayıcı ilk uluslararası hukuksal belge niteliğindedir. Avrupa İnsan Hakları Sözleşmesi'nde ise kişisel veriler konusunda boşluk vardır. 28 Ocak 1981 tarihinde Strazburg'da imzaya açılmış ve 1 Ekim 1985'te yürürlüğe girmiştir. Türkiye ise 28 Ocak 1981 yılında

[89] https://mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5 (E.T:30/09/2021).

[90] Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Bata Yayınları, İstanbul, 2008, s. 10-12.

imzalamıştır[91]. Sözleşmenin Resmi Gazetede yayınlanarak yürürlüğe girdiği tarih ise 17 Mart 2016'dır.

Kişisel veri kapsamına giren hususlar ulusal ya da uluslararası mevzuatta sınırlı sayıma sahip değildir. Anayasa Mahkemesinin 25/12/2014 tarihli 2014/74 Esas ve 2014/201 Karar numaralı kararında kişiye ilişkin olan ve onu belirleyen ya da belirlenebilir kılan bütün bilgiler kişisel veri olarak açıklanmıştır. Bunlara örnek olarak; kişinin adı, soyadı, ev ve iş adresi, doğum tarihi, medeni durumu, uyruğu, etnik kökeni, görüntüsü, fiziksel özellikleri, mesleği, eğitim durumu, özgeçmiş, çalışma şartları[92], motorlu taşıt plakası, sağlık bilgileri, vücut ölçüleri, aile ilişkileri, kanaatleri[93], inançları, gündelik yaşam alışkanlıkları, alışveriş alışkanlıkları, banka ve emniyet bilgileri, adli sicil kaydı, yaptığı yolculukların listesi[94], kamuya açık alanlardaki kameraların çektiği görüntüler[95], vergi numarası, pasaport ve sosyal güvenlik numarası, tercihleri, hobileri, cinsel hayatı, yüz yapısı[96], parmak izi, kişinin DNA'sının içeren hücre ve doku örnekleri[97], vakıf ve dernek üyelikleri, fotoğrafı, çevrimiçi kimlik ve internette ziyaret edilen sitelerden elde edilen çerezler, bilgisayarının IP numarası, telefon numarası[98], haberleşme içerikleri, grup üyelikleri ve etkileşimde bulunduğu kişiler[99], telefon rehberi ve mesajları, facebook, instagram, twitter[100] ve kişisel blog sayfasında paylaştığı yazı, fotoğraf, ses ve videoları verebiliriz[101]. Yargıtay Ceza Genel Kurulu Kararında ayrıca ad-soyad düzenlemelerinin, vatandaşlıktan çıkarılmanın, kişilerin mali durumlarının, anı

[91] Şimşek, s. 23.
[92] Avrupa Adalet Divanı 06/10/2003 tarihli C-101/101 sayılı Lindquivist Kararı.
[93] Şimşek, s. 121.
[94] Hayrünnisa Özdemir, "Haberleşmenin Gizliliği ve Kişisel Veriler", **Erzincan Hukuk Fakültesi Dergisi**, Cilt:13 Sayı:1-2, 2009, s. 290.
[95] AİHM Peck v. United Kingdom, Başvuru No:44647/98.
[96] Songül Atak, "Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri", **Kazancı Hakemli Hukuk Dergisi**, Sayı:57-60, 2009, s. 207.
[97] Avrupa Veri Koruma Hukuku El Kitabı, s. 29. (E.T: 16/10/2021)
[98] Ersan Şen ve Yasemin Yurttaş, "Bilgisayar Programları Karşısında Özel Hayatın Korunması" **Terazi Hukuk Dergisi**, 5(42), 2010, s. 3; AİHM Case Of X v. United Kingdom, Başvuru No: 9072/82.
[99] AYM 2014/74 Esas, 2014/201 Karar, 25/12/2014 tarihli (E.T: 16/10/2021).
[100] Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığından Kişisel Verilerin Korunması,** 2. Baskı, Beta Yayıncılık, İstanbul, 2016, ss. 8-9.
[101] İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayıncılık, 2. Baskı, Ankara, 2019, s.31; Melike Köse Aysun, **Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135),** Seçkin Yayıncılık, Ankara, 2018, s. 27; Şeyma Sert, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2019, s. 24; Batuhan Aktaş, **Özel Hayatın Gizliliğini İhlal Suçu**, Der Yayınları, İstanbul, 2017, s. 66.

günlük defterlerinin, mektuplarının, alışveriş eğilimlerinin, engellilik durumlarının ve daha sayılması mümkün olmayan birçok bilginin kişisel veri kapsamında değerlendirilmesinin mümkün olduğunu belirtmektedir[102]. Kişinin imzası, ailesine ilişkin bilgiler, aile bireylerinin işyerine ve su aboneliklerine ilişkin bilgiler de kişisel veridir[103]. Elde edilen bilgi ve verilerin doğru ya da yanlış olması; objektif ya da sübjektif nitelikteki değer yargıları olması kişisel veri olarak kabul edilmesine engel değildir[104].

Kişisel veri konusuna geçmeden önce veri kavramının üzerinde durulması gerekmektedir. Veri ve bilgi hususuna sosyal medya konusunu açıkladığımız bölümde kısaca değinmiştik.

a. Veri Kavramı ve İçeriği

"Data" ve information" kelimeleri dilimizde veri olarak tercüme edilmektedir. Ancak yapılan bir tercüme hatasıdır. Data sözcüğü bilişim anlamındaki bilgileri ifade etmekte iken information aslında her türlü bilgiyi yani günlük hayatımızda

---

[102] *"…kişinin; Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum tarihi, doğum yeri, nüfusa kayıtlı olunan yer (İl, İlçe, mahalle veya köy), anne ve baba adı, medeni hali (Evli, bekâr, boşanmış), nüfusa kayıtlı olduğu cilt ve aile sıra no, kan grubu, evlenme tarihi, boşanma tarihi ve mahkeme kararı bilgileri, adı-soyadı veya diğer kayıt düzeltmeleri, vatandaşlıktan çıkarılma bilgileri, evlatlık ilişkisi, adresi, dini, bitirilen okullar (ilk-orta-yüksek), hastalıkları, hastalıkları ile ilgili tahlil sonuçları (DNA bilgileri), mali durumu (servet, aldığı ücretler), ahlaki eğilimleri, zaafları, çevre ile ilişkileri, hatıra, anı ve günlükle ilgili defterindeki bilgileri, siyasi görüşü (oy verdiği partiler, üye olduğu dernekler), alışkanlıkları, sevdiği kitaplar veya gazeteler, alışveriş eğilimleri, vergi numarası, e posta adresi ve şifresi, banka bilgileri, bilgisayarının IP numarası, emeklilik ve kurum sicil numarası, aldığı ödüller, parmak izi, avuç içi izleri, mektupları, yazıları, kitapları, telefon numaraları, mesajları, fiziki kimliği (boy, kilo, engellilik durumu, ten rengi, göz rengi, saç rengi ve şekli, sesi, genel görünüm, ayak ve beden numarası ve çok daha fazla bilgi kişisel veri kapsamında değerlendirilebilecektir…"* Yargıtay Ceza Genel Kurulu, 2012/12-1510 E, 2014/331 K, 17/06/2014. https://kararara ma.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:27/11/2021).

[103] AYM Aylin Nazlıaka Başvurusu Bireysel Başvuru No:2018/24439); Söz konusu kişisel verilerin başvurucunun rızası dışında elde edilmiş ve Twitter adlı sosyal medya sitesi üzerinden yayınlanmış olması gibi sebeplerle ile Ay. m. 20 kapsamında ihlal kararı verilmiştir. https://kararlarbilgibankasi.anayasa.gov.tr/Ara?BasvuruNoYil=2018&BasvuruNoSayi=24439 (E.T:27/11/2021).

[104] Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010, ss.14-15; Elif Mendos Kuşkonmaz, "Kişisel Verilerin Türk Ceza Kanunu Kapsamından Korunması"**, İstanbul Üniversitesi Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi**, İstanbul, 2013, ss. 6-7; İlknur Deniz, **Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2021, s. 74.

edindiğimiz basit bilgileri dahi kapsamaktadır[105]. Bilgi, *"İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat"* olarak tanımlanmaktadır[106]. Veri, *"Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done, bilgi, data"* olarak tanımlanırken Türk Dil Kurumu bilişim konusunda "*Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*" şeklinde ayrıca bir tanım yapmıştır[107].

Veri, her türlü bilginin bilgisayar ortamında çeşitli işlemler için kullanılabilir hale getirilmesidir. Veri halinde getirilen bilgiler okunabilir, saklanabilir ve iletilebilir. Bu işlemleri yapmaya yarayan teknik alfabeye de yazılım dili denilmektedir[108]. Anayasa Mahkemesi *"veri, bir araştırmanın, bir tartışmanın, bir /muhakemenin temeli olan ana öğe, muta, done"* anlamına gelmekte olup bilimsel, istatistiki, ekonomik, kişisel bilgileri de içine alan bir kavram olduğunu ifade etmiştir[109]. Her ne kadar birbirlerinden farklı yönlerine değinilmiş olsa da dilimizde tanımları konusunda net bir ayrımın ortaya konulmaması sebebi ile bilgi ve veri kelimelerini birbirlerinin yerine kullanmaktayız[110].

Veri kavramı sosyal medya konusunu açıkladığımız ilk bölümde 5651 sayılı kanunda m.2/1-k'da veri *"Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri*" olarak açıklandığına değinmiştik.

b. Kimliği Belirli veya Belirlenebilir Gerçek Kişi Olması

Kişi tabirinin ortaya çıkışı Roma da oyuncuların sahnede kullandıkları maskeyle olmuştur. Bu maskenin karşılığı Latince "persona"dır.[111] Hukukumuzda

---

[105] Yavuz Erdoğan, "Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi (MADDE 135, 136, 137, 138)" **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:8, Sayı:2, Aralık 2013, ss. 569-632.
[106] https://sozluk.gov.tr/ (E.T:21/11/2021).
[107] https://sozluk.gov.tr/ (E.T:21/11/2021).
[108] Dülger, s. 76.
[109] AYM, E. 2010/40, K. 2012/8, T. 19/01/2012, https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2012/8?EsasNo=2010%2F40 (E.T:12/11/2021).
[110] Elif Küzeci, **Kişisel Verilerin Korunması**, On İki Levha Yayıncılık, 4. Baskı, İstanbul, 2021(2021), ss. 9-12.
[111] Kaya, s. 29; Sinan Sami Akkurt, "Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlâli Hâlinde Ortaya Çıkacak Cezaî Sorumluluğa Medeni Hukuk Bağlamında Bir Bakış" **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:25, Sayı:2, 2017, s. 15

kişi, hak sahibi varlık olarak açıklanır. Bu varlık haklara sahip olma ve borç altına girme ehliyetine sahiptir[112].

Kişilik hakkı *"hukukun korunmaya değer bulduğu, hukuki, manevi nitelikteki varlıkların tümü"* olarak tanımlanabilirken[113] daha ayrıntılı bir şekilde kişinin kişiliğini oluşturan hayat, vücut bütünlüğü, ad, resim, özel hayatın gizliliği, ekonomik özgürlük gibi maddi ve manevi değerlerin tümü üzerinde sahip olduğu hak şeklinde de tanımlanabilecektir[114]. Kural olarak kişisel verilerin korunması hakkı bir insan hakkıdır ve yalnızca gerçek kişiler yararlanabilecektir. Tüzel kişilerin bu korumaya dahil edilmesi gerçek kişilerin bu alandaki korumasını zayıflatacağı düşünülmektedir[115]. Kişilik hakkına tüzel kişiler de sahiptir ancak onların kişilik hakkı korumalarından yararlanması gerçek kişiler gibi değildir. Gerçek kişilere özgü olan yaşam hakkı, vücut bütünlüğü gibi değerler tüzel kişilerin kişilik hakkı kapsamında yer almaz[116]. Öğretide farklı görüşler mevcut olmakla birlikte Gönen'in düşüncesine göre tüzel kişiler de kişilik hakkı kapsamındaki korumalardan yararlanmalıdır. Örneğin İsviçre Verileri Koruma Kanunu tüzel kişilerin de kişisel verilerinin korunduğu görülmektedir[117]. Ancak uluslararası düzenlemeler ve Kişisel Verilerin Korunması Hakkındaki Kanunumuz m.3/1-d bendinde yapılan kişisel veri tanımında yalnızca kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak açıklanmıştır. TCK m.135'te yer alan kişisel verileri kaydedilmesi suçunda da madde gerekçesinde kişisel veri gerçek kişiye ait her türlü bilgi açıklaması yapılmaktadır.

Tüzel kişilerin verilerinin hem KVKK hem de TCK m. 135 kapsamında değerlendirilmesinin pratik bir yararının olmadığının düşünülmektedir. Türk Hukuku açsısından ticaret şirketlerinin, dernek ve vakıfların birçok işleminin aleniyet gerektirdiği hususu dikkate alındığında bu verilerin korunmasının temel mantığı da

---

[112] Kemal Oğuzman, Özer Seçili, Saibe Oktay Özdemir**, Kişiler Hukuku (Gerçek ve Tüzel Kişiler),** 12. Baskı, Filiz Kitabevi, İstanbul 2012, s. 2.
[113] Mustafa Dural ve Tufan Öğüz, **Türk Özel Hukuku Cilt II Kişiler Hukuku,** 14. Baskı, Filiz Kitabevi, İstanbul, 2013, s. 8.
[114] Beyza Aka, "Sosyal Medyada Kişilik Hakkı İhlalleri ve Hukukî Korunma Yolları", **İzmir Barosu Dergisi**, Mayıs 2017, s. 234; Doruk Gönen, **Tüzel Kişilerde Kişilik Hakkı ve Korunması**, On İki Levha Yayıncılık, İstanbul, 2011, s. 19.
[115] Şimşek, s. 122-123.
[116] Gönen, s. 29; Oğuzman, Seçili, Özdemir, s. 155.
[117] Gönen ss. 90, 99; Korkmaz, s. 39; Akgül, s. 15.

ortaya konulamamaktadır[118]. Tüzel kişilere ait verilerde gerçek kişilerin de verilerinin bulunması halinde örneğin şirket temsilcilerinin bazı verileri kendilerini belirli ya da belirlenebilir kılması durumunda kişisel verilerin korunması hükümleri uygulama alanı bulabileceği düşünülmektedir[119]. TCK m. 135 gerekçesinde gerçek kişilerden bahsediliyor olsa bile öğretide bazı görüşler tüzel kişilerin ticari hayatının da gerçek kişiler kadar olmasa da özel hayat kapsamında korunması gereklidir. Bu sebeple bu suçun mağduru hem gerçek kişiler hem de tüzel kişilerin olabileceği düşünülmüştür[120]. Ancak Anayasa Mahkemesinin 2014 tarihli farklı kararının da bulunduğunu söylemek gerekir[121].

Belirli kişi olması konusunda öğretide farklı açıklamalar bulunmaktadır. Kişinin belirli olması bir görüşe göre *"o kişinin bulunduğu grubun diğer üyelerinden ayırt edilebilmesi"*dir[122]. Kişiyi farklı prosedür ve işlemlerden geçirmeye gerek kalmadan eldeki bilgilerle bağlantı kurulup belirli bit kişinin kimliğinin ortaya çıkabilmesidir. Bu şekilde isim ya da kimlik numarası veyahut açık adres gibi bilgiler kişiyi belirli kılmaktadır[123]. Belirlenebilir olma ise kişiye doğrudan ulaştıran değil ama ek verilerle kişinin belirlenmesi mümkün olma durumudur. Kişiyi belirlenebilir kılan veriler de bu özellikleri sebebi ile kişisel verilerin korunması kapsamındadır[124].

Belirlenebilir olmanın nasıl olacağı konusunda farklı görüşler bulunmaktadır. Örneğin bilgisayarların IP adresleri değişken de olabilir ya da sabit olabilir. IP adresi sabit olan ve sadece bir kişi tarafından kullanılan bir bilgisayarın IP adresinin kişiyi

---

[118] Kerim Kılıç, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)", **Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:25, Sayı:1 Haziran 2021, s. 15.

[119] Elif Küzeci, **Kişisel Verilerin Korunması**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2010, s. 364; Şimşek, s. 123, 207; Kişisel Verilerin Korunması Hakkında Kanun tasarı halinde tüzel kişiler de yasal korumaya dahil edilmişken son durumda uluslararası düzenlemelere uygun olarak yalnızca gerçek kişiler düzenleme kapsamı altına alınmıştır.

[120] Ersan Şen, "Kişisel Verilerin Korunması Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi" **İstanbul Barosu Dergisi**, Cilt: 83 Sayı: 3, 2009, s. 1201-1202; Sert, s. 30; TCK Madde Gerekçesi, s. 220; Suç konusunun gerçek kişiye ait veriler olabileceğine ilişkindir. https://docplayer.biz.tr/1257504-Turk-ceza-kanunu-madde-gerekceleri.html (E.T:05/01/2022).

[121] Anayasa Mahkemesi 2013/84 E. 2014/183 K. 04/12/2014 T.; Kararda Anayasa Mahkemesi Ay. m.20'de herkes ibaresinin yer almasından dolayı tüzel kişilerin de bu korumadan yararlanması gerektiğine hükmetmiştir. Berrak Yılmaz, **Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, (Yayınlanmamış Doktora Tezi) Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, 2019, s. 14.

[122] Rezzan İtişgen, "Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu", **Türkiye Adalet Akademisi Dergisi**, Yıl: 6, Sayı:23, Ankara, Ekim 2015, s. 183.

[123] Şimşek s. 122; Sert, s. 32.

[124] Akgül, s. 17.

belirlenebilir kılacağı için kişisel veri kabul etmek gerekecektir[125]. IP adresi konusunda şunu da söylemek gerekir: Yargıtay kararlarında da değinildiği gibi IP numarası doğrudan bilgisayarı göstermez. IP esasen internetle olan bağlantıyı göstermektedir. Ayrıca kişilerin haberleri olmadan bilgisayarlarına indirilen programlar sayesinde bilgisayarları zombi bilgisayar halinde getirildiği durumlarda bilgisayarı kullanan kişinin haberi dahi olmadan IP numarası ile siber saldırılar düzenlenebilir. Yani kullanıcının haberi olmadan bilgisayarlarının IP adresleri kullanılarak suç işlenmesi mümkündür. Bu sebeple IP adresi o bilgisayarı kullanan kişinin eylemi gerçekleştirdiğini kesin olarak kanıtlamamaktadır. Yargıtay da birçok kararında özellikle IP adresleri konusunda doğru ve gerekli araştırmaların yapılaması gerektiği düşüncesindedir[126].

İnternet cafe ya da toplu bilgisayar kullanımı olan herkese açık yerlerde IP yoluyla kullanıcı olan kişinin tespiti mümkün olmayacaktır[127]. Görüşlerden biri kişinin kimliğine ulaşmaya yarayabilecek her türlü verinin kişisel veri olacağı düşüncesidir. Bu görüş kişisel veri işleyen kurum ve kişilerin, kişisel verileri korunması hakkındaki mevzuata tabi olmaları ve mevzuatın yüklediği sorumluluk ve yükümlülüklere uygun davranmaları gerektiği sonucuna götürmektedir. Çok basit verilerin dahi bu sonuca sebep olması hem veri işleyenler hem de denetim makamları için göz ardı edilmeyecek kadar önemli bir iş yükü oluşturacaktır. Başka bir görüş ise elde edilen verinin kişi ile bağlantı kurmaya imkan sağlayıp sağlamadığının değerlendirilmesi gerektiğini değerlendirmektedir. Burada çift yönlü bir değerlendirme yapılmalıdır. Elde edilen veriyi kullanacak kişinin imkan ve gücü ile elde edilen verinin kişi ile bağlantı sağlayabilecek kadar güçlü olup olmadığı değerlendirilecektir. Veriyi elde tutan kişi bağlantı kurma gücüne ve imkanına sahip değilse söz konusu veri kişisel veri olarak değerlendirilmeyecektir. Örneğin TÜİK gibi istatistik çalışmaları sebebi ile elde edilen veriler anonimleştirilme ile kişisel veri sayılmayacaktır. Bu verilerin en başta isimsiz olarak kaydedilmesi ya da isim olsa

[125] A. Çiğdem Ayözer, **Kişisel Verilerin Korunması**, Beta Yayıncılık, İstanbul, 2016, s. 11; Şen ve Yurttaş, s. 33.

[126] Dülger, ss. 595-596; IP adreslerini dinamik ve statik şeklinde sınıflandırabiliriz. İnternete bağlanmak isteyen bir kişiye internet sağlayıcısı geçici olarak IP atar bu durumunda dinamik IP adresi söz konudur. Statik IP ise sunucu bilgisayarlarda kullanılır. Ayırıca Yerel Ağ (LAN) da kullanılabilen özel IP adresleri bulunmaktadır.

[127] Yasemin Durak, "İnternet Yoluyla Kişilik Haklarına Saldırı ve Hukuki Koruma" **Selçuk Hukuk Fakültesi Dergisi**, Yıl:2014, Cilt:22, Sayı:1, s. 104.

bile bunların kişiler tespit edilemeyecek şekilde bir düzene tabi olmadan yayınlanması ya da paylaşılması halinde bir sorun oluşmayacaktır[128].

c. Kişiye İlişkin Olma

Bir verinin kişiye ilişkin olması demek söz konusu verinin "içerik", "amaç" veya "sonuç" yönünden kişi ile bağlantıya sahip olmasıdır. Bilginin kişi hakkında olması demek bu bağlantının var olmasıdır[129]. Verinin kişisel veri niteliğinde olup olmadığının tespitinde kişi ile verinin bağlantı noktasının tespiti gerekir. Burada bağlantı kurulma yöntemi önemlidir. Kullanılması gereken araçlar ya da yapılması gerekenler bağlantı kurulma yöntemi olarak ifade edilir[130].

Kişilik hakkının konusu kişisel değerlerdir. Bunların hepsinin sayılması ve bunların sınırlandırılması mümkün değildir. Mevzuatta sınırlı bir sayım yapılmaması isabetli bir düzenleme kabul edilmektedir. Bu alanda olan değişim ve dönüşüm sürecin doğal sonucu olarak sınırlı sayım yapılmamasını zorunlu kılmaktadır. Somut olaylar doğrultusunda hakimlerin takdir yetkisi kapsamında bu kişisel değerlendirilmesi kişilik hakkına giren değerler üçe ayrılmaktadır: Bu değerlerin ilki fiziksel kişilik değerleri, ikincisi duygusal kişilik değerleri ve son olarak sosyal kişilik değerleri olarak sayılabilir. Fiziksel kişilik değerleri kişinin yaşamı, vücut bütünlüğü, ruhsal sağlığı, hareket özgürlüğü ve cinsel özgürlüklerinden oluşmaktadır. Kişilerin özellikler ailesi ile ve yakınlarıyla olan ilişkileri duygusal kişilik değeri olarak değerlendirilir. Sosyal kişilik değerleri ise kişinin kimliği, görüntüsü, sesi, şeref ve haysiyeti, özel hayatı, ekonomik özgürlüğü gibi değerlerden oluşturmaktadır. Şeref ve haysiyet konusunda mesleki, ekonomik ve toplumsal haysiyet dikkate alınmalıdır. Yargıtay'a göre kişilerin onuru ve şerefi o kişinin yaşadığı çevredeki manevi değerlerinin bütünüdür[131].

2. Özel Nitelikli Kişisel Veri (Hassas Veri)

[128]Aksoy, ss. 25-27.
[129] Mendos Kuşkonmaz, s. 11.
[130] Lee Bygrave, Data Protection Law - Approaching Its Rationale, Logic and Limits**, Kluwer Law International**, Hollanda, 2002, s. 45. (Data Protection)
[131] Hasan İşgüzar, "Kişilik Hakkının İhlali Nedeniyle Manevi Tazminat Davasının Şartları", **Ankara Barosu Dergisi,** Sayı:6, 1990, ss. 857-859.

Kişisel Verilerin Korunması Kanunu[132] 6. maddesi 1. fıkrasına göre, *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."* Bu verilerin işlenebilmesi için açık rıza gereklidir. Aksi takdirde hassas verilerin işlenmesi yasaktır. Bu düzenleme ile birlikte kanunda ayrıca istisnai haller de düzenlenmiştir. Sağlık ve cinsel hayata ilişkin veriler haricindeki diğer hassas verilerin kanunlarda öngörülen hallerde açık rıza aranmaksızın işlenebileceği şeklinde bir istisnai durum düzenlenmiştir.

Söz konusu kanun maddesinde sınırlı sayı esası benimsemiş görünmektedir. Ancak farklı ülkelerde milli köken, siyasi partilere veya hareketlere aidiyet, engellilik, bağımlılık, alkol ve uyuşturucu kullanımı, destek ve sosyal refah yardımları, WEB tarama geçmişleri, e-ticarette satın alma ve mal arama trafiği gibi bilgiler de özel nitelikli kişisel hassas veri türleri içinde kabul edilebilmektedir[133]. Esasen hassas veriler kişilerin ayrımcılığa ya da toplumsal baskıya maruz kalabileceği hususları içeren verilerdir[134].

TCK[135] m. 135/2'de ise hukuka aykırı yollarla kişisel verileri kaydeden kimseye suça konu olan kişisel verinin kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda ceza yönünden ağırlaştırıcı sebep olduğu düzenlenmiştir. İçerikler hassas verileri tarif etmekte ve bu konuda özel bir bilinç oluşmasına hizmet etmektedir. Düzenleme uluslararası eğilimi yansıtmış ve bu özel kategori ile hassas veriler yasal himaye altına alınmıştır[136].

AİHM'nin M.S/İsveç Kararında hassas verilere ilişkin açıklamalara yer verilmiştir. Başvurucu geçirdiği iş kazası sebebi ile bel ağrıları yaşamıştır. Bu sebeple açtığı tazminat davasında SGK talebi ile başvurucunun tedavi olduğu

[132] https://mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (E.T:10/10/2021).
[133] Metin Bulut, "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", **Ankara Barosu Dergisi**, Yıl: 78, Sayı: 2020/3, ss. 110-111.
[134] Türkay, Henkoğlu, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, 1. Baskı, Yetkin Yayınları, Ankara 2015, s. 28.
[135] https://mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5 (E.T:10/10/2021).
[136] Bulut, s. 120.

klinikten tıbbı kayıtlar SGK'ye gönderilmiştir. Ancak tıbbi kayıtlarda başvurucunun daha önce yaşadığı kürtaj hakkında bilgilere de yer verilmiştir. Bu verilerin de gönderilmesinin özel hayatın gizliliğini ihlal ettiği gerekçesi ile AİHM'ye başvurulmuştur. AİHM kişinin kürtaj konusundaki verilerinin hassas veri niteliğinde olduğunu tespit etmekle beraber tazminat davası konusunda karar verilmesi için tüm bu verilere ihtiyaç olduğuna karar vermiştir. Sonuç olarak bu olayda AİHM başvurucuya ait sağlık verilerinin tazminat hesabı için gerekli olduğuna ve ihlalin olmadığı kanaatine varmıştır[137].

Kişisel Verileri Koruma Kurumu[138] özel nitelikli veriler hakkında bir kararında bir hastanede kayıtlı olan hastaya ilişkin verinin farklı bir cihazla fotoğrafının çekilip sosyal medyada paylaşılmasına ilişkin olayı incelemiştir. Bu olayda Kurulca KVKK m.12/1-c kapsamında veri sorumlusu hakkında idari para cezası uygulamıştır. Kurula göre somut olayda kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin edilmemiştir[139].

Sonuç olarak mevzuatta "hassas veri", "özel nitelikli kişisel veri" gibi çeşitli isimler kullanılarak kişisel veriler, nitelikleri gereği diğer kişisel verilerden daha özel bir konuma ve korumaya sahip kılınmıştır[140].

3. Özel Hayatın Gizliliği ve Mahremiyet

Özel hayat *"Kişinin kendine özgü yaşayışı, yaşama tarzı, kendisini ilgilendiren tutum ve davranışı, öz yaşam, özel yaşamı[141]"* olarak tanımlanmaktadır. Bu tanımlamalar *"Kişinin sadece kendisi için saklı tuttuğu ve başkalarının bilgisinden uzak kalmasını istediği yaşam görünümleri"*, *"Herkes tarafından bilinmeyen, özel araştırma ve bilgi edinmeyle sağlanan kişiye ait hususlar"*,

[137] AİHM M.S./İsveç Başvuru No: 20837/92, Karar Tarihi: 27/08/1997; Mendos Kuşkonmaz ss. 109-110.
[138] Kişisel Verileri Koruma Korunması Kanunu'nun 19. maddesinde Kişisel Verileri Koruma Kurumu, 21. maddesinde Kişisel Verileri Koruma Kurulu düzenlenmiştir. Kişisel verilerin korunması konusunda önemli yetki ve görevleri bulunmaktadır.
[139] https://kvkk.gov.tr/Icerik/5408/Ozel-Nitelikli-Kisisel-Verilerin-Kanuna-Aykiri-Sekilde-Internet-ve-Sosyal-Medya-Mecralarinda-Paylasilmasi (E.T: 14/11/2021).
[140] Korkmaz, s. 112.
[141] Türk Dil Kurumu, sozluk.gov.tr (E.T:07/09/2021).

"Kişilerin gizli hayat alanlarında yapmış oldukları faaliyetlerin başkaları tarafından bilinmemesini istedikleri taraflar" şeklinde çoğaltılabilir[142].

Özel hayat kavramının ortaya çıkışı ve korunması ihtiyacını çok eski çağlardan beri mevcuttur. İlkel toplumlarda ve dini metinlerde buna yönelik ibarelere ve uygulamalara rastlamak mümkündür. Kişilerin soyut bir mahrem alanı daima var olagelmiştir. Henüz özel hayat kavramı bir hak olarak tanınmadan önce tarihsel gelişimde İngiltere'de 1361'de kişilerin özel hayatının gizliliğinin ihlal edenleri tutuklama yetkisi veren "Justices of the Peace Act" ön plana çıkmaktadır. Sulh yargıcına verilen tutuklama yetkisi başkalarını gizlice dinleyen ve izleyen insanlara yönelik verilmiştir. Özel hayat kavramının bir hak olarak tanımlanmasında 1890 yılında Amerika'da Harvard Law Review'de yayımlanan ve Samuel D. Warren-Louis D. Brandeis tarafından kaleme alınan "The Right to Privacy" (Mahremiyet Hakkı) isimli makalenin etkisinin büyük olduğu düşünülmektedir. Bu makalede özel hayatın gizliliği hakkının "the right to be let alone" (yalnız kalabilme hakkı) olarak tanımlanmıştır. Makalenin yazılmasına ise fotoğrafçılığın ve basının ortaya çıkması, yaygınlaşması etkili olmuştur. Uluslararası alanda bu hakka yer verilmesi ise 10 Aralık 1948 tarihli ve 217A(III) sayılı Birleşmiş Milletler Genel Kurulu kararı ile kabul edilen İnsan Hakları Evrensel Beyannamesi, Avrupa Konseyine üye devletlerce 4 Kasım 1950 tarihinde imzalanan İnsan Haklarının ve Temel Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi ve 16 Aralık 1966'da New York da kabul edilen Medeni ve Siyasi Haklara Dair Uluslararası Sözleşmesi bu hakkın tanınması ve devletlerin iç hukuklarına aktarmasında etkili olmuştur[143].

Avrupa İnsan Hakları Sözleşmesi 8. maddedeki düzenleme özel hayata dairdir[144]. Maddede özel hayat kavramının tanımı yapılmamıştır. Avrupa İnsan Hakları Mahkemesi de özel hayata ilişkin kesin bir tanım yapmaktan kaçınmaktadır. Bir tanımın olmaması bu alanın içtihatlarla gelişmesine de olanak tanımıştır. Ancak AİHM kararları incelendiğinde hangi hakların bu kapsamda değerlendirilmesi

[142] Ali Korkmaz, "İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması", **KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi**, Sayı: 16 (Özel Sayı I), 2014, s. 2. (Ali Korkmaz)

[143] Yaşar Salihpaşaoğlu, "Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme", **Gazi Üniversitesi Hukuk Fakültesi Dergisi** Cilt: 17, Sayı: 3, 2013, ss. 228-229.

[144] https://www.anayasa.gov.tr/tr/mevzuat/aihs/ (E.T:06/01/2021).

gerektiğine ilişkin yol gösterici açıklamaları bulunmaktadır. AİHM'ye göre özel hayatın kapsamı şunlardır

a. Kişinin Kimliği: Bu kapsamda kişinin ismi, cinsel kimliği, etnik kimliği ve yaşam biçimi, kişinin görüntüsü özel hayatın parçasını oluşturmaktadır[145]. Günümüzde özellikle kadının kendi ailesinden gelen soyadını tek başına kullanıp kullanamayacağı konusu tartışmalara sebep olmuş ve bu hususu AYM Neşe Akbıyık Başvurusunda özel hayata saygı hakkına ve ayrımcılık yasağına aykırılık olarak değerlendirmiştir. Daha önce AİHM önüne gelen bu tarz başvurularda hem madde 8 özel hayata saygı hem de m. 14 ayrımcılık yasağı konularında ihlal kararı vermiştir[146].

b. Kişinin Onur ve Şöhreti: Kişinin onur ve şöhreti; kişilik ve manevi bütünlükle ilgilidir. Bu sebeple de onur ve şöhret özel hayat kapsamında değerlendirilmesi gerekmektedir. Ancak mahkeme özel hayat konusunda sözleşmenin ifade özgürlüğüne ilişkin 10. maddesi ile adil denge kurulmasının gerektiğinin de altını çizmektedir[147].

c. Kişisel Veriler: Kişisel verilerin toplanması, saklanması ve kullanılması özel hayatın gizliliği kapsamındadır. Devletler kişisel veriler konusunda pozitif ve de negatif yükümlülüklerle karşı karşıyadır. Daha önce de bahsettiğimiz üzere bu kişisel veriler Avrupa İnsan Hakları Sözleşmesinde doğrudan düzenlenmediği halde bu konu AİHM tarafından m. 8 kapsamında değerlendirilmektedir[148]. AİHM kararında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmesine atıfta bulunmaktadır. Sözleşmenin 2. maddesinde kişisel veriler kişinin kimliğini belirten ya da belirtmeye elverişli olan her türlü bilgi olarak tanımlanmaktadır. Sözleşmenin "özellikli veri kategorileri" başlığını taşıyan 6. maddesine göre, "*iç hukukta uygun güvenceler sağlanmadıkça, ırk menşeini, politik düşünceleri, dinî veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkûmiyetleri, otomatik bilgi işlemine tâbi tutulamazlar.*"

[145] Salihpaşaoğlu, ss. 237-239.
[146] Aktaş, s.55.
[147] Salihpaşaoğlu, s. 242.
[148] Mustafa Ruhan Erdem, Tezcan Durmuş, Oğuz Sancakdar, R. Murat Önok, **İnsan Hakları El Kitabı**, 8. Baskı, Seçkin Yayıncılık, Ankara, 2019, s. 282; Salihpaşaoğlu, s.244; Aktaş, s. 66.

d. Kişinin Cinsel Hayatı: Kişinin cinsel hayatı özel hayatın en mahrem alanlarını oluşturmaktadır. Ancak AİHM'e göre ensest ve bazı sado-masochistic ilişkiler sözleşmenin 8. maddesinin sağladığı korumadan yararlanamayacaktır. Ancak AİHM Laskey, Joggard and Brown v. United Kingdom Kararında sado-mazoşist eylemlerin özel hayat kapsamında kaldığını düşünmüş fakat somut olayda gruba yeni üye kazandırma maksadı ile cinsel ilişkinin kayda alınması durumunun 8. madde kapsamındaki korumdan yararlanıp yararlanmayacağının tartışmalı bir durum olduğunu açıklamıştır[149]. AİHM, yetişkin erkekler arasındaki rızaya dayalı aleni olmayan eşcinsel ilişki yasakları 8. maddeye aykırı bulurken ensest[150] ve sado-mazoşist ilişki[151] gibi farklı cinsel ilişki şekillerinin devletler tarafından ulusal hukuk düzenlemelerinde yasaklanmış olmasını ve suç kabul edilmesini AİHS 8. maddeye aykırı bulunmamıştır[152]. Kısacası genel olarak mahkeme bu konuda taraf devletlerin takdir yetkisinin olduğunu ve bu tür ilişkilerin yasaklanmasının, yaptırıma bağlanmasının özel hayatın ihlali olmadığını düşünmektedir[153].

e. Kişinin Fiziksel ve Psikolojik Bütünlüğü: Kişilerin maddi ve manevi bütünlüğü özel hayat kapsamı altında değerlendirilmektedir. AİHS'nin işkencenin yasaklanması başlığı altında yer alan 3. maddesi de fiziksel ve psikolojik bütünlüğe ilişkindir. Mahkeme bu konuda belli bir asgari şiddet düzeyine ulaşıp ulaşmama şeklinde bir ayrıma gitmektedir. Bu şiddet düzeyine ulaşılmışsa m. 3 uygulanacaktır. Belli bir asgari şiddet düzeyine ulaşmaması halinde ya da ulaşması halinde de m. 8'in uygulanması mümkündür. Ancak kişinin fiziksel ve psikolojik bütünlüğüne yönelik şiddet düzeyi çok hafif olursa m. 8 dahi uygulanmayacaktır. *"Belli bir asgari şiddet düzeyine"* ulaşan kötü muameleler daha çok 3. maddenin ihlali olarak düşünülmektedir. Buna göre aynı eylem muamelenin süresi, doğurduğu fiziksel ve ruhsal etkiler, mağdurun cinsiyeti, yaşı ve sağlık durumu gibi çeşitli faktörler dikkate alınmaktadır. Örneğin AİHM, Juhnke v. Türkiye davasında, *"herhangi bir tıbbi sebep olmaksızın ilgilinin rızası dışında"* yapılan jinekolojik muayeneyi, 8. maddenin ihlali olarak görmüşken Yazgül Yılmaz v. Türkiye davasında yaşı 16 olan

[149] Aktaş, s. 59.
[150] Stübing v. Germany, Başvuru No: 43547/08, 12/04/2012.
[151] Laskey, Jaggard and Brown v. the UK, Başvuru No: 21627/93, 21826/93, 21974/93.
[152] Gülay Arslan Öncü, **Özel Yaşama ve Aile Yaşamına Saygı Hakkı Anayasa Mahkemesi Bireysel Başvuru El Kitabı-8,** Avrupa Konseyi, Epamat Basım Yayın, Ankara, 2019, s. 63.
[153] Salihpaşaoğlu, ss. 239-240.

başvurucuya karşı gerçekleştirilen aynı eylemi 3. maddenin ihlali olarak görmüştür[154].

Maddi ve manevi varlığını koruma ve geliştirme hakkı, Anayasamızın 17. maddesine yer almakta ve herkese tanınmış bir haktır. Bireyin kişisel şeref ve itibarı da AYM içtihatlarına göre Anayasa'nın 17. maddesinde yer alan manevi varlık kapsamındadır. Bu sebeple devlet, kişilerin manevi varlığı olan şeref ve itibara keyfi olarak müdahale etmemeli ve de üçüncü kişilerce gerçekleştirilebilecek saldırıları önlemelidir. (Abdullah Doğtaş, B. No:2013/1123, 2/10/2013) Bu noktada devletin yükümlülüğü sadece önlemek değil aynı zamanda bu hakların güvence altına alınmasını sağlayacak pozitif koruyucu tedbirler almak da olacaktır. (Kadir Sağıç, B. No: 2013/6617, 8/4/2015) Avrupa İnsan Hakları Mahkemesi (AİHM) de 2006 tarihindeki H.M./Türkiye kararında arama kararı olmadan yapılan aramaya iddiasına ilişkin savcılığın gerekli incelemeyi yapmadan takipsizlik kararı vermesi sonucunda Türkiye'nin AİHS m. 8'den kaynaklanan hakları korumada yetersiz kaldığını tespit etmiştir[155]. Açıklayacağımız TCK hükümleri özel hayata yönelik bu saldırıların korunmasına yöneliktir.

Kişilerin görüntüsü kişinin ayıt edilmesini sağlayan bir özelliktir. AİHM birçok kararında[156] bu hususa dikkat çekerek kişilerin mahremiyeti ve kişiliğinin geliştirilmesi konusunda kişinin görüntüsünün önem arz ettiğini belirtmektedir. Bu sebeple görüntüler de özel hayat kapsamında korunmaya muhtaçtır. Özellikle ünlü kişilerin görüntülerinin yayınlanmasında kamu yararı olması ya da fotoğraflarının çekilmesine katlanmak zorunda olduklarına dair farklı görüşler bulunmaktadır. Ancak Avrupa İnsan Hakları Mahkemesi'nin Prenses Caroline kararında sürekli takip edilerek magazinciler tarafından fotoğrafları çekilen Prensesin özel hayatının gizliliğinin ihlal edildiğine yönelik karar verilmiştir.

Yargıtay kararlarında kişiler de bu kişilerin mağdurların bilgisi dışında kişilerin fotoğraflarının örneğin facebook adlı sosyal medya sitesinde rızası dışında profil fotoğrafı yapılması ve de kişinin isminin de paylaşılması halinde kişinin özel

[154] Salihpaşaoğlu, s. 247.
[155]Erdem, Tezcan, Sancakdar, Önok, ss. 396, 397.
[156] Avrupa İnsan Hakları Mahkemesi Von Hannover v. Germany Kararı, Başvuru No:59320/00, Paragraf 50.

hayatının gizliliğinin ihlal edildiğine karar vermiştir[157]. Öğretide bu şekilde kişinin fotoğraflarının kullanılmasının ayrıca kişilik hakkının ihlali oluşturduğu düşünülmektedir.

III. KİŞİSEL VERİLERİN KORUMASININ TEMEL İLKELERİ

A. Veri Korumanın Esasına Dair İlkeler

1. Veri Güvenliği ve Mahremiyeti

Veri güvenliği ilkesi idari ve teknik tedbirlerin alınmasının sağlanmasıdır. Veri güvenliği ilkesi ile kişisel verilerin korunması aynı anlama gelmemektedir. Veri güvenliği ilkesi verilerin bizatihi kendisinin korunmasına endekslidir. Verinin kaybedilmesi, yetkisiz kişilerce ele geçirilmesi, tahrip edilmesi, ifşa edilmesi gibi durumlar için getirilen güvenlik önlemleri sayesinde verinin korunması amacına hizmet eden düzenlemelerdir. Kişisel verilerin korunması ise esasen kişisel verilerin korunması için verilerin işlenmesindeki hukuksal korumaları düzenlemektedir. Veri güvenliği ilkesinin kişisel verilerin korunması ile aynı olmadığını belirtmekle beraber veri güvenliği ilkesinin kişisel verilerin korunmasına hizmet ettiğini de söylemek mümkündür[158]. Veri güvenliğinin asıl amacı verilerin kötü niyetli kişilerce elde edilmesinin önlenmesi ve buna yönelik gerekli idari-teknik tedbirlerin alınmasını sağlamaktır[159].

Veri güvenliği için ilgilerin verilerinin korunmasına yönelik makul önlemlerin alınması hususu OECD Rehber İlkeleri m.11'de Avrupa Konseyi Verilerin Korunması Sözleşmesinde 7. maddede yer almaktadır. Avrupa Konseyinin

---

[157] Yargıtay 12. CD, 2014/7338 E. 2014/24862 K. 08/12/2014 T.; 12.CD, 2013/1045 E. 2013/28322 K. 09/12/2013 T.
https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/pf/sorgula.xhtml
(E.T:22/01/2022).

[158] Şimşek, s. 95; Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", **International Journal of Law and Information Technology**, 1998, Cilt:6, (Data) s. 253. https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf
(E.T:10/01/2022).

[159] Hale Akdağ, **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,** (Yayınlanmamış Yüksek Lisans Tezi) Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 83.

108 Sayılı Verilerin Korunması Sözleşmesinde de otomatik olarak kaydedilen verilerin korunması için uygun güvenlik önlemlerinin alınması gerektiği çünkü verilerin imhası, kaybolması, iziniz aktarılması veya değiştirilmesi gibi ihtimallerin var olduğunun altını çizmektedir. Söz konusu düzenlemeler verilerin güvenliğinin sağlanması ile aslında kişisel verilerin korunmasına hizmet eden bir mekanizmanın gerekliliği ve önemine işaret etmektedir[160].

AT Kişisel Verilerin Korunmasına İlişkin Direktifinde (95/46/AT)[161] veri güvenliği ilkesinin kişisel verilerin korunmasında verilere yapılacak müdahalelere ya da herhangi bir şekilde hukuka aykırı bir işlem yapılaması karşısında veri işlem sorumlusunun gerekli tedbirleri alması gerektiğini düzenlemektedir. Veri işlem sorumlusu işlenen verinin özelliği ve çıkabilecek sorunları da dikkate alarak makul bir koruma düzeyi garanti etmelidir. Yönergenin 46 numaralı gerekçesinde bu tedbirlerin alınmasının hukuka uygun veri işlemenin ve ilgilinin haklarının korumanın sadece bir boyutu olduğu belirtilmektedir. Bu sebeple veri güvenliğinin sağlamış olması kişisel veriler üzerinde tam bir koruma sağlanmış olduğu anlamına gelmemektedir[162].

KVKK'de veri güvenliği ilkesine yer verilmiştir. Bu ilke kanunda 12. maddede veri güvenliğine ilişkin yükümlülükler başlığı altında düzenlenmiştir. Veri sorumlularının kişisel verilerin muhafazasını sağlaması, hukuka aykırı şekilde işlenmesi ve verilere hukuka aykırı şekilde erişilmesini önleme için gerekli tedbirleri almakla yükümlü kılmıştır. Ayrıca veri sorumlularının ve veri işleyen kişilerin, öğrendikleri kişisel verileri başkasına açıklaması ve işleme konusu dışında kullanmaları açıkça yasaklanmıştır. Bu yükümlülüklerinin kapsamına görev sonrası da dahil edilmiştir. Avrupa Birliği Genel Veri Koruma Tüzüğünde (GDPR) de veri güvenliği konusuna yer verilmektedir. Veri işleme güvenliği ile ilgili düzenlemelere göre verinin türü, risk durumu ve ihtimaller göz önüne alınarak maliyet ve de teknolojik gelişmeler doğrultusunda veri işleyen ve veri sorumlusu gerekli tedbirleri almak zorundadır. Bu önlemler veri işleme faaliyeti sırasında takma adların

[160] Şimşek, s. 96.
[161] Söz konusu yönerge 95/46/AT adı Direktif olarak anılmaktadır. Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından yapılan tüzük (Genel Veri Koruma Tüzüğü-GDPR) 2016 yılında kabul edilmiş olup, 25 Mayıs 2018 tarihinde 95/46 sayılı Direktif'i ilga ederek yürürlüğe girmiştir.
[162] Şimşek, ss. 96, 97.

kullanılması, veri işlenen sistemlerin düzenli olarak güncellenmesi, erişim durumlarının kontrol edilmesi, şifreleme yapılmış olması gibi olabilir[163]. KVKK 12. maddenin birinci fıkrası şu şekilde düzenlenmiştir: Veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini önleme, bu verilere yine hukuka aykırı olarak erişilmesini önleme ve de verilerin güvenli bir şekilde saklanmasını sağlamakla yükümlüdür. Bu yükümlülükleri yerine getirmesi ve "uygun güvenlik düzeyini" sağlaması için gereken teknik ve idari tedbirler veri sorumlusu tarafından alınacaktır.

Verilerin güvenliği veri gizliliği ile bağlantılıdır. Verilerin gizliliğinin sağlanması ve gerekli tedbirlerin alınması ile kişisel verilerin korunmasına hizmet edecek gerekli yöntemler uygulanmış olacaktır. Solove veri güvenliğini ihlallerini açıkladığı piramidinde en üste çeşitli yöntemlerle kişilerin verilerinin kimlik bilgilerinin elde edilerek bunların kötüye kullanılmasını koymuştur. İkinci sırada ise veri sorumlularının sızıntıları örneğin şirket görevlilerince verilerin ifşa edilmesine yer vermiştir. Son sırada piramidin en geniş noktası olan en altta ise verilerin güvenli şekilde saklanmıyor olması hususuna yer vermektedir. Verilerin bizzat veri sorumlusu tarafından işlenmediği durumlarda ise bu kişiler adına veri işleyenler veri güvenliğini sağlamakla yükümlüdür[164]. KVKK m. 12/2'de bu husus açıklamaktadır. Veri güvenliği konusundaki yükümlülükler söz konusu olduğunda veri sorumlusunun kendisi adına veri işleme faaliyetini gerçekleştiren kişilerle birlikte müştereken sorumlu olacaktır.

Kanunda veri sorumlularına ve de veri işleyen kişilere öğrendikleri bilgileri işlerinden ayrılsalar dahi saklama yükümlülüğü yüklenmiştir. Ayrıca bu verilerin işlenme amacına aykırı bir şekilde kullanılmasını da yasaklanmıştır. Kanun koyucu özellikle verilere bir şekilde görevleri dolayısıyla ulaşan kişilere yönelik bir düzenleme yapmaya çalışmıştır. Maddenin son fıkrasına göre yasa dışı bir biçimde verilere ulaşılması halinde veri sorumlularının Kurulu ve ilgilisini en kısa sürede haberdar etmesi gerekir. Sonuç olarak verilerin hukuka aykırı biçimde başkaları tarafından elde edilmesi ihtimalinde derhal gerekli tedbirlerin alınması için veri sorumlularına bildirim yükümü getirilmiştir.

---

[163] Sert, ss. 94, 95.

[164] Daniel J. Solove, "The New Vulnerability: Data Security and Personal Information" **GW Law Faculty Publications**, 2008;
https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2090&context=faculty_publications

Günümüzde büyük şirketlere yönelik siber saldırılar oldukça yaygınlaşmıştır. Yakın zamanda da Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik A.Ş. tarafından "yemeksepeti.com" web sitesi üzerinden uygulama sunucusu açığından yararlanılarak saldırı yapıldığı ve veri sızıntısı olduğunu tespit edilmiştir. Veri sızıntısının yaklaşık 7 gün[165] içinde tespit edilip KVKK m.12/5 hükmündeki yükümlülüğü uyarınca Kişisel Verileri Korunma Kurumuna bildirdiği görülmektedir. Veri sorumlusu sıfatını taşıyan şirket kurma veri ihlal bildirimi göndermiştir. İlgili bildirime göre saldırıyı yapanlar tarafından sunucu üzerinde kullanıcı oluşturularak veri toplanmaya çalışıldığı ve uzaktaki sunuculara trafik göndermiştir. Bu şekilde yapılan saldırıdan 21.504.083 kişinin etkilenmiş olduğunu, şirket tarafından belirlenebildiği kadarıyla söz konusu verilerin kullanıcı adı, adres, telefon, e-posta, şifre, IP bilgilerinin olduğu belirtilmiştir. Konuya ilişkin Kişisel Verileri Koruma Kurumu inceleme başlatmıştır[166]. İlgili şirket yemek sipariş hizmeti vermektedir. Son dönemlerde bu hizmeti sunan en popüler çevrimiçi uygulamalardan olduğu etkilenen kişi sayısının büyüklüğünden de anlaşılmaktadır. Şirkete en üst sınırdan idari para cezası kesilse bile 21 milyondan fazla kişinin verisinin çalınmış olması ihtimalinde kişi başına düşen rakamların oldukça düşük rakamlar olduğu görülmektedir. Ayrıca veri ihlali olmasına rağmen durumu kuruma bildirmeyen şirketlerin bulunduğu da görülmektedir[167].

Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/58 sayılı Kararına veri sorumlusu olan bir sigorta acentesinin facebook ve instagram paylaşımında müşteri adları ve adresleri görünür şekilde paylaşımlar konusu olmuştur. Kurul, sigorta şirketinin paylaşım yaparken müşterilerinin açık rızasını almadığını ve müşterilerinin ad soyadı, adresleri ve de araçlarının plaka bilgilerini içeren kişisel verisinin paylaştığını tespit etmiştir. Veri sorumlusunun KVKK m. 12'de düzenlenen yükümlülüklerin yerine getirilmediği ve müşterilerinin rızası

[165] Kişisel Verileri Koruma Kurumu 2019/10 Sayılı Kararı uyarınca bildirme süresi öğrenmeden itibaren 72 saattir. Ayrıca verileri etkilenen kişiler tespit edildiğinde bu kişiler makul sürede bildirim yapılması gereklidir. Bu bildirim yöntemi önce ilgiliye doğrudan ulaşmaya çalışma ancak ulaşılamıyorsa veri sorumlusunun sitesinde uygun şekilde yayımlama ile olabilir. https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi (E.T:29/11/2021).

[166] https://kvkk.gov.tr/Icerik/6936/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Yemek-Sepeti-Elektronik-Iletisim-Perakende-Gida-Lojistik-AS (E.T: 25/11/2021).

[167] https://www.gercekgundem.com/ekonomi/267745/kisisel-bilgiler-calinmisti-yemek-sepeti-krizinde-kafa-karistiran-sorular (E.T:25/11/2021).

alınmadan onlara ait kişisel verileri herkese açık sosyal medya meralarında reklam yapma amacıyla paylaşması sebebi ile veri sorumlusu hakkında idari para cezası verilmiştir. Benzer şekilde Kurul başka bir kararında spor eğitmeni olarak bir kurumda çalışan ilgilinin işten çıktıktan sonra ve rızası alınmadan fotoğraflarının kurumun herkese açık sosyal medya hesaplarından paylaşılmasına ilişkin olayda da hukuka aykırı bir şekilde veri işlendiği kararı vermiştir[168].

2. Hassas Verilerin İşlenmesi ve Özellikli Olarak Korunması

Hassas verilerin ancak gerekli olduğunca toplanması ve sınırlı koşullar altında işlenmesi ilkesi geçerlidir. Bu tür veriler kişiler arasında ayrımcılık yapılması ihtimali oldukça yüksek olan verilerdir. Kişilik haklarına ağır müdahale barındırabilecek ihlaller söz konusu olması nedeni ile özellikli bir korumaya ihtiyaç duyulmaktadır. Bu verilerin işlenmesinin ancak kamu yararının gerektirdiği hallerde mümkün olması gerekir. OECD Rehber İlkelerine bu verilere ilişkin özel bir koruma türü getirilmemiştir. Ancak Avrupa Konseyi Verilerin Korunması Sözleşmesinin 6. maddesinde bu tür verilere ilişkin özel bir korunmuş ve bu verilerin işlenebilmesi için iç hukukta bunlara ilişkin uygun korumanın sağlanması gerektiği düzenlenmiştir. Mülga 95/46/AT Numaralı Avrupa Toplulukları Direktifinde hassas veriler sayılmış ve bu tür verilerin işlenmesinin kural olarak yasak olduğunu ancak bazı istisnalar da getirilmiştir. Bu istisnalar kısaca ilgilinin açık rızası, ilgili devlet tarafından yeterli garantilerin sağlanması halinde iş hukuku çerçevesinde gerekli olması halinde, hayati durumlarda ilgili kişi veya üçüncü kişinin rıza verebilecek durumda olmaması ve zorunluluk olması halinde, ticari amaç gütmeyen vakıf ve ya derneklerin kendi alanları ile ilgili verilerin gerekli garantiler sağlanması halinde, özel nitelikli verilerin kamuya açılmış olması veya mahkeme önünde hukuksal taleplerde ya da savunma yaparken kullanılması zorunlu olması halinde, sağlık hizmetleri konusunda sır saklama yükümlülüğü olan hekimler ve sağlık personelleri tarafından yapılan faaliyetlerin olması halinde, suçların ceza mahkumiyetinin ve güvenlik tedbirlerinin

[168] https://kvkk.gov.tr/Icerik/6716/2020-58 (E.T:14/11/2021).
Benzer nitelikte karar başka bir karar olan Kişisel Verileri Koruma Kurulunun 27/04/2021 tarihli 2021/442 sayılı kararı.

işlenmesinde resmi makamların gözetimi ve denetimi altından olması halinde mümkündür [169].

B. Verinin İşlenme Usulüne Dair İlkeler

1. Hukuka ve Dürüstlük Kurallarına Uygunluk

Verilerin hukuka ve dürüstlük kuralına uygun olarak işlenmesi gerekmektedir. Yasalarla toplama ve işleme amacı belirli olan kişisel veriler yasalara uygun şekilde toplanıp işlenecektir. Yetkisiz kişilerce elde edilemeyecek ya da aktarılamayacaktır. İlgililere verileri üzerinde ne tür işlemlerin yapıldığı ne için nasıl kullanıldığı bilebilme ve verilerinin kontrolünü sağlama imkanı verilecektir. Verinin oluşturulmasında, kaydedilmesinde, kullanılmasında sınırlar gözetilmeli ve bu işlemlerin minimum düzeyde tutulması gerekmektedir. Belirli ve sınırlı olma özelliği taşıması verilerin korumasında önemli bir noktadır. Amaca aykırı olacak şekilde gereksiz ve fazla veri toplanması ya da amaç hasıl olduktan sonra dahi veriyi saklanmaya devam edilmesi bu ilkelere aykırı bir davranış olacaktır. Bu gibi durumlarda veriler daha fazla muhafaza edilmemeli ve silinmelidir. Böylece veriler hukuka ve dürüstlük kuralına uygun olarak işlenmiş olacaktır[170]. Veriler işlenirken işlemlerin baştan sona hukuka uygun şekilde işlenmesi gerekir. Ancak bu şekilde veri işleme faaliyeti hukuka uygun olabilecektir[171]. Hukuka uygun bir şekilde kişisel verinin işlenmesi bilinmesini için meşru veya kabul edilebilir kılan sebeplerin olması nedeniyle o verinin kişisel olma özelliğini değiştirmemektedir. Bu sebepler sadece kişisel verinin başkalarınca öğrenilmesini hukuka ve dürüstlük kuralına uygun kılabilecektir. Fakat verinin niteliğini değiştirmez[172].

---

[169] Şimşek, ss. 86-89.
[170] Şimşek, ss.84, 85.
[171] Hayrünnisa Özdemir, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayınları, Ankara, 2009, (Elektronik), s. 137.
[172] Akdağ, s. 38.

Kişinin işlenmiş olan kişisel verileri için sonradan onay vermesi işlemi hukuka uygun yapmamaktadır. Bu durumda kişinin sonra yapılacak olan işleme onay verdiği ve bu sebeple sonraki işlemlerin hukuka uygun olduğu kabul edilmelidir[173].

Dürüstlük kuralına uygun olunması verilerin yasal düzenlemelere uygun şekilde gizlice olmadan bilgi ve ilgi dahilinde şeffaf bir şekilde işlenmesi ile sağlanacaktır. Şeffaflığın sağlanabilmesi adına veri işlenirken açık ve anlaşılır bir dil kullanılması da önemlidir. Hukuka uygunluk ve dürüstlük kuralı aslında veri sorumlusunun kişilerin özel hayatına, maddi manevi bütünlüğüne yönelik fiillerini en asgariye indirmeye yöneliktir[174]. Hukuka aykırı olarak veri işlenmesi halinde tazminat talep edilmesi söz konusu olacaktır. Zarara uğrayanlar kişisel verinin hukuka aykırı şekilde işlenmiş olması sebebi ile maddi ve manevi tazminat ödemek zorunda kalabilecektir[175].

Kişisel Verilerin Korunması Hakkında Kanunun 4. maddesinde hukuka ve dürüstlük kuralına uygun olma ilkesine yer verilmiştir. Ayrıca 108 sayılı Avrupa Konseyi Sözleşmesinde 5. maddenin a bendinde ve GDPR 5. maddede yasaya uygun veri işleme, kanunilik, dürüstlük ve şeffaflık ilkelerine yer verilmiştir[176]. KVKK 5. maddesinde kişisel verilerin işlenmesi için gerekli şartların neler olduğundan bahsedilmiştir. Kanunda verinin işlenebilmesi için ilgilinin açık rızasının aranması gerektiği belirtilmiştir. Ancak maddenin devamında ikinci fıkrada açık rızaya ihtiyaç duyulmayan veri işlenebilmesinin şartları düzenlenmiştir.

Sosyal medyada örneğin Facebook ve İnstagram veri ilkesini açıklarken hangi tür verileri topladığından bahsetmektedir. Kullanıcının sağladığı veriler olarak kategorize edilen kısımda yoruma açık ifadeler yer almaktadır. Hesap açılması veya paylaşım yapılması durumunda bu paylaşımların içeriği, hesap açılırken verilen bilgiler, atılan mesajların içerikleri, paylaşılan bir fotoğrafın hangi konumda ve tarihte çekildiği gibi bilgiler kullanıcının sağladığı veriler olarak açıklanmaktadır [177].

Bu hususlar dışında iletişim kurulan kişiler, bağlantılar, konu etiketleri, sayfalar, kullanıcının tercih etmesi halinde bir cihazda yer alan rehber ya da çağrı

[173] Şimşek, s. 107.
[174] Küzeci, 2021, s. 230; Bygrave, Data Protection, s. 58.
[175] Şimşek s. 109.
[176] Korkmaz, ss. 121-122; Sert, ss. 75-76; Atak, Songül, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", **Türkiye Barolar Birliği Dergisi**, S.87, 2010, (AB), s. 96.
[177] https://help.instagram.com/519522125107875 (E.T:18/01/2022).

kayıtları, görüntülenen içerikler, etkileşimde bulunulan kişiler, kullanım sıklığı, facebook ürünlerini alışveriş yapmak amacıyla kullanılması halinde kredi kartı, ödeme bilgileri, kimlik doğrulama bilgileri, finansal kayıtlar, kullanılan cihaz bilgileri, cihaz sinyalleri, çerez verileri de toplanan veriler arasında sayılmaktadır. Ayrıca bir diğer önemli husus başkalarının yaptığı şeyler ve sizin hakkınızda verdiği bilgilerin de toplanıp işleniyor olmasıdır. Bu veriler başka kullanıcılar tarafından yüklenen ama size ait olduğu tespit edilen bir fotoğraf, yapılan bir yorum ya da verilen iletişim bilgisi gibi verilerdir. Verilerin indirilmesi ile verilerin görülebilmesi imkanı vardır. Söz konusu verilerin silinmesine dair ise uygulama ayarları "verilerine eriş" seçeneğinde görünen hesap verilerinde silinme işlemi yapılabilmektedir. Ancak bu seçenekte çıkan veri türleri veri ilkesinde uygulamanın toplayacağını belirtilen tüm veriler değildir. Verilerine eriş seçeneği ile kullanıcı hesap bilgileri, profil bilgileri, bağlantılar, hesap hareketleri, hikaye hareketleri ve reklamlara ait veriler görülebilmekte silinebilmektedir[178]. Benzer şekilde twitter da verileri işlemekte ve bu verilere ulaşım imkanı sağlamaktadır[179].

a. Açık Rızanın Kapsamında Verilerin İşlenmesi

Kişisel verilerin kamu organları tarafından veri işlenmesi için ya bu kamusal organların yetkilendirilmiş olması ya da ilgili kişilerin veri işleme faaliyetine rıza göstermesi gerekmektedir. Yasal bir yetkilendirmenin ya da ilgilinin rızasının olması gerekliliği izin kaydı olarak adlandırılmaktadır[180].

Veri işleme faaliyetinde ilk olarak bakılacak şey ilgilinin rızasının var olup olmadığıdır. Ancak rızanın olması tek başına yeterli değildir. Rızanın gerçekten ki verinin toplanmasındaki somut amaca ve bu verilerin elde edilmesi halinde ortaya çıkacak sonuçlara yönelik olması gerekir. Yani doğru bir bilgilendirme yapılmış olmalı ve rıza da bu şekilde verilmiş olmalıdır.[181]. Birden fazla amaç söz konusu

[178] İnstagram tarafından verilerinizi indirme ve verilerinize ulaşma imkanı tanınmaktadır. İnstagram tarafından bu durum "verilerinizin kontrolü sizde" olarak lanse edilmektedir.
https://help.instagram.com/181231772500920 (E.T:22/01/2022).
https://help.instagram.com/519522125107875 (E.T:18/01/2022).
[179] https://help.twitter.com/tr/managing-your-account/accessing-your-twitter-data (18/01/2022).
[180] Şimşek, s. 106.
[181] Özdemir, s. 292; Atak, s. 211.

olduğunda ilgiliye bu amaçların da bildirilmiş olması gereklidir. İlgili tüm bu hususlarda bilgilendirilmiş olmalıdır. Ayrıca alınan rıza da yazılı olarak ve ilgilinin özgür iradesi doğrultusunda verilmelidir.

Veriler işleneceği sırada ilgiliye ortalama bir kişinin anlayabileceği şekilde ve ilgilinin farklı bir milliyete tabi olması halinde uygun dil seçeneği ile bilgilendirme yapılmalıdır. Özellikle veri işlemenin amacının, süresinin ve nerelerde kullanılacağının açıklanması önemlidir[182].

Rıza elektronik ortamda alınıyorsa o hususstaki kurallara uygun şekilde alınmalıdır. Kişilerinden hassas verilere ilişkin rıza alınırken bu rıza hassas veri ile açıkça ilişkilendirilmelidir. Veri işlem sorumlusu bu durumlarda yalnızca bir iletişim adresi vererek ilgilinin gerekli denetimi yapmasını sağlayamaz. Bu sebeple ilgililerin haklarını kullanabilmesi ve verilerini takip edebilmesi için veri işlem sorumlusunun "kimliğini ve adresini" bildirmesi gereklidir. Yasal temeli ve ilgilinin rızası olmadıkça veri işlenmemesi kuraldır. Kişinin susması ya da rıza vermek istememesi halinde haklı bir gerekçe sunması gerekmez. Temel kural veri işleme özgürlüğü olmadığı içim ilgililerin kişisel verilerinin kaydedilmesine rıza vermemesi halinde bunu gerekçelendirmesi gerekmemektedir. Bir görüşe göre kişinin kendisinin rızası ile kişisel verilerin toplanmasının kişisel verilerin korunmasını hakkının sağlayıcısıdır. Başka bir görüşe göre ise kişinin rızası aslında kişisel verilerin korunması temel hakkından vazgeçmesidir. Ancak farklı görüşlerin düşüncelerini barındıran temel husus rıza ile kişinin kendi kişisel verilerinin akıbetini belirleme hakkına sahip olduğu ve bunun garanti altına alınmaya çalışıldığıdır[183].

b. Kanunlarda Açıkça Öngörülmesi

Açık rıza dışında yasal düzenlemelerde veri işlenmesini hukuka uygun hale getiren durumlar düzenlenmiştir. Örneğin adli sicil ve nüfus kayıtlarının tutulması

[182] Özdemir, s. 293.
[183] Şimşek, ss. 106-108.

veya parmak izi alınması gibi durumlara ilişkin rıza aranmayan kanuni düzenlemeler bu kapsamda değerlendirilecektir[184].

c. Diğer haller:

-Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

-Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

-Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

-İlgili kişinin kendisi tarafından alenileştirilmiş olması,

-Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,

-İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olmasıdır.

Bu hukuka uygunluk hallerinden ilgili kişinin kendisi tarafından kişisel verisinin alenileştirilmesi hususu sosyal medyada paylaşılan veriler açısından önemlidir. Alenileştirme hususunun TCK açısından hukuka uygunluk sebebi olarak değerlendirilip değerlendirilemeyeceği ceza hukukuna ilişkin açıklamaların yapıldığı kısımda irdelenecektir.

2. Amaçla Bağlılık

Amaca bağlılık ilkesi verilerin kaliteli olması ilkesi ile bağlantılıdır. Çünkü verilerin kaliteli olması, önceden verilerin kullanılma amacının belli olması ve toplanan verilerin bu amaca bağlı olarak işlenmesi anlamına gelmektedir[185]. Özellikle genel ifadelerin kullanılması ve belirsizlik oluşturulması kişisel verilerin

[184] Bahri Öztürk, Elif Altınok Çalışkan, Serkan Seyhan, **Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı**, Seçkin Yayınları, Ankara, 2021, ss. 64-65.
[185] Şimşek, s. 83.

toplanırken bu toplanma amacının belirli olması ve de bu amaçla sınırlı olacak şeklide olması gerekliliğini ihlal edebilecektir. Bu sebeple verilerin toplanma amacı belirli ve açık olmalıdır[186]. İlkenin uygulanması aynı zamanda kişisel verilerin hukuka ve dürüstlük kuralına uygun olarak işlenmesi ve tutulması anlamına gelecektir[187].

OECD Veri Koruma İlkelerinde 9. maddede, Avrupa Konseyi Sözleşmesi 5. maddede ve yürürlükten kaldırılan 95/46/AT Avrupa Toplulukları Verilerin Korunması Yönergesinde 6. maddede bu ilkeye yer verilmiştir. Düzenlemelerde kişisel verilerin toplanması ve işlenmesinden önce verilerin belirli bir amacın olması gerektiği ifade edilmektedir. Bu belirli olan amaç doğrultusunda işlem yapılacakken amacın ilgililerce bilinmesi ve veriler üzerinde kontrol imkanı sağlanması gerekmektedir[188].

Amaca bağlılık ilkesi, "asgarilik ilkesi" ile de bağdaştırılmaktadır. Asgarilik ilkesi ancak veri işleme amacı için zorunlu olan miktarlarla sınırlı olacak şekilde veri işlenmesi ve toplanması anlamına gelmektedir. Belirli amaç için veri toplanırken amaç için yeterli olduğu tespit edilen veriler dışında veriler toplanmalıdır. Örneğin güvenlik kameralarının güvenliğe hizmet etmeyecek şekilde farklı açılarda yerleştirilmesi halinde Almanya'da kişilerin gereksiz yere görüntülerinin kaydedildiğine karar vermiştir[189]. GDPR m. 5/1-c hükümlerinde de benzer şekilde verilerin olabildiğince azaltılması, toplanan verinin toplanma amacı için gerektiği kadarı ile sınırlı kalması ve gereklilik barındırmayan verilerin işlenmemesi gibi hususlara yer verilmiştir[190].

Sosyal medyada kullanıcıların şirketlerle paylaştığı örneğin doğum tarihi ya da telefon numarası gibi verileri şirketlerce işlenme amacı doğrultusunda saklanması gereklidir. Veri sorumlusu olan şirketlerin bu yükümlülükleri de amaca bağlılık ilkesinin bir gereğidir. Sosyal medya şirketlerinin kullanıcıların kişisel verilerini işleme amacı dışında ticari amaçlarla kullanmaması gerekir.

---

[186]Mendos Kuşkonmaz, s. 89; Akgül, s. 72.
[187] Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008, s. 225.
[188] Şimşek, s. 83.
[189] Küzeci, s. 203; Akgül, s. 158.
[190] Hüseyin Murat Develioğlu**, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, İstanbul, 2017, s. 47.

Federal Alman Veri Koruma Yasası amaca bağlılık ve olabildiğince az veri işlenmesine yönelik hükümlerinde veriler toplanırken amaca göre tasarlanması ve seçilmesi gerektiğinden bahsetmektedir. Ayrıca zorunluluk olmamakla birlikte amaç için uygunsa maliyetli ve zahmetli olmaması halinde bu verilerin anonimleştirilmesi veya takma adlaştırılması öngörülmüştür. İnternette özellikle de sosyal medya da kullanıcı adını takma ad olarak seçen kişilere oldukça sık rastlanmaktadır. Bu takma adlar ya da takma adı olarak IP adreslerinin kullanılması halinde bunların kişisel veri olarak değerlendirilip değerlendirilemeyeceği tartışılan bir husustur. Web sitelerinin kullanıcının etkinliklerini izleyerek bir profil oluşturması mümkündür. Bu konuda tartışmalar olmakla birlikte Avrupa Adalet Divanı dinamik IP adreslerini kişisel veri olarak değerlendirdiği kararlarının vaarlığı da bilinmektedir. GDPR'de IP adreslerini de kişisel veri olarak değerlendirmiştir[191].

3. Ölçülülük

Kişisel verilerin korunmasındaki temel amaç, bir bütün olarak temel hak ve özgürlüklerin korunmasıdır. Hak ihlallerinin meydana gelmeden önce engellenmesi için gerekli tedbirleri alarak mümkünse olmamasını, olmuşsa da ihlalin devamını engellemek, sonuçlarını ortadan kaldırmaya yöneliktir[192]. Kişisel verileri korurken yapılan müdahaleler ölçülü olmalıdır. Ölçülülük ilkesi bu noktada önem arz etmektedir. Bu ilke hukuk devleti olma ile bağlantılıdır. Kamu gücü sınırlanırken ya da hak ve özgürlükler korunurken ölçülü olunması gerekir[193]. Ölçülülük ilkesi temel hak ve özgürlüklerin sınırlanmasındaki amaç ile buna yarayan araçlar arasındaki ilişkiyi incelemektedir. "*Ölçülülük ilkesi, sınırlamayla güdülen amaca erişmek için hak ve özgürlüklerin ne ölçüde sınırlanmasının yeterli olacağını belirleyen bir ilkedir*[194]." Bu ilke özgürlüğün kural ve sınırlamanın istisna olması ilkesini de içinde barındırmaktadır. Verilerin işlenirken özel makamlar ya da kamu makamları da yasal sınırları içinde kalarak bu ilke doğrultusunda yapılan düzenlemelere uygun

[191] Küzeci, 2021, ss. 239-241; ABAD Breyer v Bundesrepublic Deutschland C-582/14, 19/10/2016.
[192] Şimşek, ss. 98-99
[193] O. Korkut Kanadoğlu, **Türk ve Alman Anayasa Yargısından Değerlerin Çatışması ve Uyumlaştırılması**, Beta Yayınları, İstanbul, 2000, s. 162.
[194] Yüksel Metin, "Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?", **SDÜHFD,** Cilt: 7, Sayı 1, 2017, s. 4.

davranacaktır. Ölçülülük ilkesi içinde birçok ilkeyle bağlantılıdır. Örneğin veri kaydedilirken meşru bir amaçla işlenmeli bu işlemin yasal bir dayanağı olmalı, her veri değil gerekli olan veriler toplanmalı ve işlenmeli ayrıca kişinin haklarına en az zarar verme ihtimali olan yani uygun aracın seçilmelidir. Ayrıca oranlılık ilkesi gereği yapılan müdahale ve bu müdahalede kullanılan araçlarla ulaşılmak istenen amaç arasında makul bir bağlantı olması gerekir[195]. Ölçülülük ilkesi aslında 3 alt ilke ile bağlantılıdır. Bu ilkeler elverişlilik, gereklilik ve orantılılık ilkesidir. Ölçülülüğe ilişkin bir değerlendirme yaparken sınırlama için kullanılan aracın bu amaç doğrultusunda ulaşılmak istenen için elverişli olması, sınırlamanın amacına ulaşması için bu aracı kullanılmasının gerekli olması, araç ve amaç arasında bir orantının olması aranmaktadır[196].

Ölçülülük ilkesi KVKK m. 4/2'de sayılan genel ilkelerden c, ç ve d bentleri *"c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.*" ölçülülük ilkesi ile ilgilidir.

4. Doğruluk ve Güncellik

Kişiler hakkında tutulan verilerin doğru olması önemlidir. Yanlış verilerin dikkate alınması halinde kişinin temel hak ve özgürlükleri açısından olumsuz sonuçlar doğurabilecektir. Verilerin işlenmesinin ve toplanmasının belli bir amacı bulunmaktadır. Yanlış verileri bu amacın gerçekleşmesini önleyip maddi manevi zararlara sebebiyet verebilecektir[197]. Verilerin doğru ve güncel tutulması hususunun sağlanması için ilgilinin bu verilere erişiminin mümkün olması ve kontrol edebilme olanağının sağlanması gereklidir. Dolayısıyla doğruluk ve güncellik için ilgiliye erişim hakkının verilmiş olması meselesi birbiri ile bağlantılıdır. Veri sorumlularının web siteleri aracılığı ile ilgilileri kendi verilerine ulaşabilir kılması gibi şekillerle bu yükümlülüklerini yerine getirmeleri mümkündür[198]. Sosyal medya profili ve site üyeliklerinde profil bilgilerinde ilgililerin verilerini görme ve düzeltme imkanı

[195] Şimşek, ss. 98-99.
[196] Metin, s. 7.
[197] Küzeci, 2021, s. 243.
[198] Şimşek, s. 85.

bulunmaktadır. Kullanıcıların hesaplarına giriş çıkış işlemlerinde doğrulama işlemi yaptıkları telefon numarası ya da e mail bilgileri bu yönden önem arz etmektedir. Sosyal medya platformlarının belli aralıklarla iletişim bilgilerinin doğrulanmasını istediği ya da güncelleme yapılasını talep ettiği görülmektedir.

OECD Rehber İlkeleri m. 8'de verilerin doğru ve güncel şekilde tutulması gerektiği hususu yer almaktadır. GDPR m.5/1-d bendine ve 108 Sayılı Avrupa Konseyi Sözleşmesinde de bu yükümlülüklere yer verilmiştir[199].

Kişisel verilerin amacını gerçekleştirilmesi sonrasında veriler daha fazla tutulmadan silinmelidir. Özellikle kişinin tespitine doğrudan yarar sağlayan veriler konusunda silinme işleminin yapılması kişisel verileri koruyucu bir işlem niteliğinde olacaktır. Verilerin uzun süre tutulmasının "potansiyel bir tehlike" yarattığı kabul edilmelidir. AİHM verilerin uzun süre tutulması konusunda S ve Marper/Birleşik Krallık davasında bu husus değerlendirilmiştir. AİHM bazı verilerin belirsiz süre tutulmasını sağlayan uygulama ile AİHS m. 8 ihlali gerçekleştirildiğine karar vermiştir. Dava konusu veriler de parmak izi, DNA gibi hassas verilerdendir. Bu veriler suç soruşturması sebebi ile elde edilmiş veriler olmasına rağmen suçun türü ve ağırlığından bağımsız olarak belirsiz süre tutulması AİHM açısından bir ihlal kabul edilmiştir[200].

C. Veri Sahibi Kişinin Haklarına İlişkin İlkeler

1. Bilgi Edinme, Erişim ve Düzeltme Hakkı

Kişisel verilerin korunmasının gerçek manada sağlanmış olması için ilgili kişiye verilerinin işlendiğini ve ne şekilde kullanılacağı konusunda bilgi verilmesini gerektirmektedir. Verinin üçüncü kişiden elde edilmesi durumunda ilgili kişiye bilgilendirme yapılır. Bilgilenme hakkı aslında hukuk devleti ve dürüstlük ilkesi ile bağlantılıdır[201]. Kişinin rızası ile veri işleme faaliyetinde bilgilendirme işlemi önem arz etmektedir. Ancak rıza dışında kanuni gerekçelerle yapılan veri işleme

[199] Küzeci, s. 208.
[200] Mendos Kuşkonmaz, s. 93; Akgül, s .158; Küzeci, ss. 210-211.
[201] Şimşek, ss. 88, 89.

faaliyetinde ise ilgilinin hiçbir şekilde bu konu ile ilgili bilgisi olmayacağı için daha da önemlidir. Her iki durumda da yapılan işlemlerin hukuka uygun olabilmesi için bilgilendirilmesi gerekmektedir.

Kişinin bilgilendirilmesinin, veri işleme süreci ve devamında bilgi edinme hakkına sahip olmasının önemi kişisel verilerin korunması meselesinde "altın kural" ve işlemin "Magna Charta"sı kabul edilmesi ile açıklanabilir. Veri işleme faaliyetini gerçekleştiren kişinin bilgi verme yükümlülüğüne sahip olması ile ilgili kişinin bilme hakkı farklı olsalar da birbirini tamamlayan haklardır. Kişiye hiçbir bilgilendirme yapılmaması ilgilinin bilgi alma ya da verilerinde düzeltme, silinme gibi taleplerde bulunması ve bu hakları kullanması önünde bir engeldir[202].

Yürürlükten kaldırılan Avrupa Toplulukları Verilerin Korunması Direktifinin 10. maddesinde ilgili kişilere asgari olarak bilgilendirilmesi gereken hususlara değinilmiştir[203]: Bunlarda ilki veri sorumlusunun ve ayrıca değişen duruma göre temsilcisinin kimliğidir. İkincisi ise belirli bir veri işleme amacının varlığıdır. Üçüncüsü sunulan verileri kabul edeninin hangi kategoride olduğudur. Dördüncü olarak ilgiliye sorulan sorulara cevap vermenin zorunlu veya isteğe bağlı olduğunu bildirilmeli ve de ilgilinin cevap vermeme halinde bunun sonuçlarının ne olacağını bilmesi gerekir. Son olarak ilgiliye kendisini ilgilendiren veriler hakkında bilgi alma ve düzeltme haklarının mevcut olduğu açıklanmalıdır.

İlgili Yönergenin/Direktifin 11. maddesinde ise bildirim yükümlülüğünün istisnaları olabilecek durumların olduğundan bahsedilmektedir. Verisi toplanan kişiye ulaşmak mümkün değilse, aşırı masraf gerektiriyorsa, kanunda açıkça düzenlenen bir hususta işlem yapılıyorsa bildirim yükümlülüğünün olmayacağı belirtilmektedir. Ancak böyle durumlar için devletin gerekli koruyucu önlemleri de almış olması gerekir. Direktifin 12. maddesinde de veri işleme faaliyeti sırasında ilgili kişi kendisi hakkındaki verilerin neler olduğunu, veri işlemenin amacını, verilerin hangi kategorideki veriler olduğunu, verilerinin aktarılması ihtimalini ya da

---

[202] Şimşek, s. 90.

[203] Öztürk, Altınok Çalışkan, Seyhan, s. 47; Ayşe Nur Akıncı, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi", **Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Çalışma Raporu**, Haziran 2017, s. 6;
http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf (E.T:15/11/2021).

verilerinin otomatik işleme faaliyetine tabi tutulup tutulmayacağını gibi konularda veri işlem sorumlusundan anlaşılır ve makul sürelerde bilgi alma hakkına sahiptir. Aynı zamanda bu verilerde düzeltme, silinme ve engelleme gibi talepleri olabilecektir. Daha önceden bu verileri üçüncü kişilere aktarıldıysa yapılan değişiklik ve düzenlemenin üçüncü kişiye bildirilmesini isteme hakkı da vardır. Ancak bu taleplerin imkanlar dahilinde gerçekleştirilmesi ve aşırı masraf oluşturmaması da gereklidir[204].

OECD Rehber İlkeleri m. 13'te ilgili kişinin makul sürede veriler hakkında bilgi edinme hakkının olduğu ayrıca kişinin anlayabileceği bir şekilde bunu ücretsiz ya da makul ücretlerle öğrenmesi imkanı sağlanması gerektiği yer almaktadır. Kişinin bilgi edinme hakkı yanında öğrendiği bilgilerde düzeltme yapılmasını ya da silinmesini istemesi gibi hakları da garanti edilecektir.

Erişim hakkı konusunda düzenlemeler GDPR, 108 sayılı Avrupa Konseyi Sözleşmesi, OECD İlkelerinde yer almaktadır. AİHM'nin erişim hakkını 8. madde kapsamında değerlendirmektedir. Leander-İsveç Kararında mahkeme ulusal güvenlik gibi sebeplerle başvuranın kendisine ait polis kayıtlara ulaşamamasını 8. maddenin ihlali olarak değerlendirmiştir. Ayrıca AİHM'nin şöyle bir değerlendirme yaptığını da ifade etmek gerekir. Söz konusu verilerin kişisel veri olması halinde ve bunlara ulaşılmasının devlet tarafından engellenmesi m. 8 ihlali oluşturacakken zaten aslında erişilebilir nitelikte olan verilere devlet tarafından erişimin engellenmesi halinde bu m. 10 kapsamında ifade özgürlüğü konusunda bir ihlal oluşturmaktadır. Mahkeme bu değerlendirme ve kıstası Gaskin- Birleşik Krallık Kararında yapmıştır[205]. Kişisel verilere erişim hakkı konusundaki bu karar her türlü veriye ulaşım hakkı olduğuna dair değildir. AİHM kararında sınırlı bir yorum yapmıştır. Mahkeme bireyin gelişimi için önemli olan verilere ulaşımı hakkının olduğuna dikkat çekmektedir[206].

Düzeltme hakkı özellikler verilerin hatalı elde edilmiş olması durumunda söz konusu olacaktır. Eksik veya hatalı olan verilerin düzeltilmesi halinde bunun veri

[204] Küzeci ss. 215-216; Mendos Kuşkonmaz, ss. 98-99; Şimşek, ss.88-90.
[205] Korkmaz, s.137; Cavidan Soykan "Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı" **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:56, Sayı:2, 2007, ss. 68-69; Gaskin davası devlet tarafından tutulan kayıtlara ilişkindir. Annesine-babasına ait bilgileri öğrenmek isteyen ve sosyal hizmetler tarafından tutulan kayıtlara ulaşmak isteyen oğulun talebi kurumlarca reddedilmiştir. Mahkemece AİHS bilgi edinme hakkı değil de m. 8 açısından olayda ihlal kararı vermiştir.
[206] Mendos Kuşkonmaz, s. 60.

aktarımı yapılan üçüncü kişilere bildirilmesi önemli bir husustur. Çünkü veri aktarılan üçüncü kişilere bildirilmemesi halinde düzeltme yapılmasının bir anlam ifade etmediği durumlar olabilir. Düzeltme hakkı kullanılırken *"maddi bakımdan doğru ve gerçek"* olma esas alınacaktır[207].

KVKK 11. maddenin ilk beş bendinde herkesin, veri sorumlusuna başvurarak verilerinin işlenip işlenmediğine, işlenmişse hangi amaçla işlendiğine, hani amaçlar doğrultusunda kullanıldığına, kimlere aktarıldığına ilişkin bilgileri talep etme ve da hatalı bilgilerin düzeltilmesini isteme hakkı olduğu gibi hususlar düzenlenmiştir.

Daha önce bahsettiğimiz üzere sosyal medya da kullanıcıların verilerine erişimini sağlayan özellikler bulunmaktadır. Kullanıcılar bu verilere erişip kendilerine verilerine ilişkin döküm alabilir, bazı verilerini silebilir ya da düzeltebilir. Ancak şunu söylemek gerekir ki verilerin hepsine erişme ya da düzeltme yapılmasına imkan verilmemektedir. Verilerine eriş seçeneği ile kullanıcı hesap bilgileri, profil bilgileri, bağlantılar, hesap hareketleri, hikaye hareketleri ve reklamlara ait verilere erişilebilmektedir[208].

2. Unutulma Hakkı

Verileri sildirme hakkı genellikle verilerin yetkisiz kişilerce toplanması ya da verilerin kaliteli olması ilkesine aykırılık ortaya çıktığında kullanılmaktadır[209]. Günümüzde sosyal medya platformların da yaygınlaşması ile kişilerin rızaları ya rızaları dışında kişisel bilgilerini içeren paylaşımlar yıllar sonra hayatlarının beklenmedikleri anlarda önlerine çıkar hale gelmiştir. Bu veriler kişilerin unutmak istedikleri veriler olabilmektedir. Örneğin Amerika Birleşik Devletleri'nde görülen Snyder Davasındaki olayda üniversiteden mezun olmak üzere olan bir stajyer öğretmenin sosyal medya platformunda alkol içeren bir resminin öğrencileri içkiye

---

[207] Şimşek, s. 93.

[208] *"Instagram'daki verilerinizin kontrolü sizdedir. İstediğiniz zaman hesap verilerinizi görebilir ve Instagram'daki verilerinizin bir kopyasını indirebilirsiniz."*
https://help.instagram.com/181231772500920 (E.T:22/01/2022).
https://help.instagram.com/519522125107875 (E.T:18/01/2022).

[209] Şimşek, s. 94.

özendirdiği ve bu sebeple üniversitesi tarafından mezun edilmediği görülmüştür[210]. Unutulma hakkı kısaca dijital geçmişin silinmesini isteme hakkıdır. Modern çağın getirdiği teknolojik gelişmeler kişilerin bir tıkla bilgiye ulaşmasını mümkün kılar hale getirmiştir. Kişilerin geçmişlerine ait olan kendileri tarafından ya da başka kişi ya da kurumlarca paylaşılan kişisel verileri yıllar sonra kişi için rahatsızlık verici nitelikte olabilecektir. Bu gibi "*dijital hafızada yer alan bireylere ait rahatsız edici her türlü kişisel içeriğin, yine bireylerin talebi üzerine bir daha geri getirilemeyecek biçimde ortadan kaldırılması/silinmesi"* hakkı unutulma hakkı olarak literatürde yer almıştır. Unutulma hakkından bahsedebilmek dijital bir ortam söz konusu olmalıdır. Fiziki ortamda tutulan veriler için unutulma hakkı konusunda değerlendirme yapılabilecektir. Sonuç olarak kişisel veri ve bu verinin dijital ortamda olması gerekir[211]. Yargıtay'ın 2015 tarihli Hukuk Genel Kurulu Kararına göre unutulma hakkının tanımı, daha üstün bir kamu yararının gerekliliğinin olmadığı durumlarda kişinin geçmişinde yaşadığı olumsuz durumların dijital hafızadan silinmesini isteme hakkı olarak yapılabilir[212].

Unutulma hakkının dayanak noktası konusunda farklı düşünceler vardır. Bu konuda üç anlayış şu şekildedir: İlki kişisel verilerin belli süreler sonra silinmesi gerektiğini düşünen görüştür. Bu ilk görüş baskın olan görüştür. İkinci görüş sosyal perspektifli olan kişilerin hakkındaki olumsuz bilgilerin kullanılmaması gerektiği görüşüdür. Üçüncüsü ise bireylerin kendilerini bir kısıtlamaya tabi olmadan geliştirebilmesi ve bu konuda endişe duymamasının sağlanması gerektiği görüşüdür. Son iki görüş temelde beyaz sayfa yaklaşımı adı verilen yaklaşımdan yola çıkan görüşlerdir. Unutulma hakkı bu görüşlerden de yola çıkarak aslında amaç ne olursa olsun ulaşılabilir kılınan kişilerin geçmişlerindeki belli bilgilerin hatırlanmamasını isteme imkanı sağlayan bir hak olarak ortaya çıkmaktadır. Bu hakla "İnternet asla unutmaz" diye ifade edilen husus karşısında bireye bu platformdaki verilerini kontrol edebilme imkanı sunulmaktadır. Yargıtay kararlarında unutulma hakkının ve kişisel verilerin belli sürelerle ve ölçülerle tutulmasının kişisel verilerin korunması hakkının

[210] İrem Laçin, "Unutulma Hakkı", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, Doç. Dr. Melike Batur Yamaner'in Anısına Armağan, Cilt:1, 2014, ss. 392-393.
[211] Seray Nalbantoğlu, "Bir Temel Hak Olarak Unutulma Hakkı", **Türkiye Adalet Akademisi Dergisi**, Yıl:9, Sayı: 35, 2018, s. 589.
[212] Yargıtay HGK Kararı, 2014/4-56 E. 2015/1679 K. 17/06/2015 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:15/12/2021).

çatısını oluşturduğu belirtilmektedir. Yargıtay unutulma hakkı konusunda şu açıklamaları yapmaktadır: Bu hak kişilerin bizzat kendisi tarafından gerçekleştirilmiş ya da üçüncü kişinin etkisi ile ortaya çıkmış bir olay sebebi ile geleceğinin olumsuz etkilenmesinin önlenmeye çalışılmasına hizmet etmektedir. Kişilerin geçmişlerinde yaşadıkları olumsuz olaylar onların kendilerini geliştirmesine ve geleceğini şekillendirmeye çalışmasına engel olmamalıdır. Bu şekilde bireyin yararı gözetildiği gibi aslında toplum kalitesinin artmasına da olumlu etki sağlanacaktır. İsviçre'de 1983 yılında verilen bir karar da unutulma hakkı konusunda önem arz etmektedir. Dava konusu olay 1939 yılında babası ölüm cezası alan ve daha sonra resmi kayıtlar aracılığı ile düzenlenen belgeselin yayınlanmasının önlenmesine yönelik mahkumun oğlunun talebini içermektedir. Mahkeme bu dosyada kullandığı *"basının, yargılanan bir sanığın kimlik bilgilerini yayımlama hakkı muhakemenin devamı süresince mevcuttur ve bu noktadan sonra basının ve kamuoyunun resmi kayıtlara erişimi olmamalıdır çünkü suçlular ilelebet kamunun ilgisine mazhar değildir"* şeklindeki açıklaması unutulma hakkının temel dayanaklarını henüz 1980'li yıllarda ortaya koymaktadır[213].

Verilerin silinmesi konusunda Avrupa Adalet Divanı (ABAD) "Google Spain SL and Mario Costeja Gonzáles Kararı" özellikle arama motorları hususuna değinen önemli bir karardır. Söz konusu olay başvurucunun arama motoruna adını yazdığı zaman La Vanguardia gazetesinin kendisi hakkında sosyal güvenlik borçlarının ödenmesi amacıyla taşınmazının açık arttırma yoluyla satılmasına ilişkin ilan sebebiyledir. Başvuruya sebep olan gazete haberleri de 1988 tarihinde yapılmıştır. Başvurunun başvuru tarihi ise 2010 yılındadır. Kendisi de avukat olan Costeja Gonzáles öncelikle iki başvuruda bulunmuştur ilk başvurusu doğrudan İspanya Veri Koruma Kurumuna şikayet yoluyla bu güncelliğini yitiren bu ilanı içeren haberin kaldırılmasına ya da düzeltilmesine yönelik kurumca gerekli araçların kullanılmasını talebi şekildedir. İkinci başvurusu ise "Google" tarafından arama motorundan bu haberlerin kaldırılmasını ya da bağlantının gizlenmesini gibi taleplerle yaptığı başvuru olmuştur. Her iki başvuruda olumsuz sonuçlanmıştır. İspanya Veri Koruma

[213] Murat Önok, "Kişisel Verilerin Korunması Bağlamında 'Unutulma Hakkı' Ve Türkiye Açısından Değerlendirmeler", **İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:16, Sayı:1, 2017, ss. 159-162.

Kurumu ilanın bakanlık kararı ile yapılması nedeniyle gazeteden kaldırılması gerektiği yönündeki talebi reddetmiştir. Ancak bu süreçte İspanya Veri Koruma Kurumu "Google"ı veri sorumlusu olarak değerlendirerek yaptığı işlemin kişisel veri işleme faaliyeti olması gerektiği sonucuna varmıştır. Kendisinin veri sorumlusu olarak değerlendirilmesi üzerine karar Google İspanya ve Google İnc tarafından mahkemelere taşınmıştır. İspanya Mahkemeleri tarafından görüş alınmak için ABAD'a başvurulmuştur[214].

ABAD değerlendirme sonucunda ana şirket olan Google İnc İspanya da yerleşik olmamasına rağmen Google İspanya aracılığı ile İspanya sınırları içerisinde veri işleme faaliyeti gerçekleştirdiğini kabul etmiştir. *"Google Arama dünya çapında 'www.google.com' web sitesi üzerinden sunulmaktadır. Çok sayıda Devlette, ulusal dile uyarlanmış yerel bir versiyon vardır. Google Arama'nın İspanyolca sürümü, 16 Eylül 2003'ten beri kayıtlı olan 'www.google.es' web sitesi aracılığıyla sunulmaktadır."*[215] Sonuç olarak ABAD 95/46/AT Direktifini dikkate alarak arama motorlarının veri işlediklerini ve bu sebeple veri sorumlusu olacakları değerlendirmesini yapmıştır. Direktifin veri kalitesine ilişkin prensipleri uyarınca verilerin tarihi, istatiksel ya da bilimsel gerekçelerle tutulması gereken haller haricinde uzun sürelerde ilgisiz ya da amacını aşan şekilde tutulması halinde bunların silinmesi gereklidir. Tabi ki silinme için kamu yararı gibi durumların olmaması gerekir[216]. Kamu yararının bulunduğu haller incelenirken ilgili verinin kamusal etkisi ve rolü ayrıca halkın bu veriye olan ilgisi gibi hususlar dikkate alınabilir. Bu şekilde kamunun üstün yararının olduğu tespit edilirse unutulma hakkı uygulanmayabilecektir[217]. Sonuç olarak ABAD'ye göre veriler internet sitelerinden kaldırılmasa bile arama motorlarında çıkan sonuçlardan silinmesi veri sorumlusu olan arama motoru işletenlerden istenebilir[218].

---

[214]Develioğlu, s. 89; Nalbantoğlu, s. 590; Muhammed Emin Karakaş, "Dijital Geçmişin İnternet Erişiminden Kaldırılması 'Unutulma Hakkı' ve Türk Hukukunda Görünümü", **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 3 Sayı: 2 Yıl: 2020, s. 267; İrlanda Dijital Haklar Kararı, M.Schrems-Veri Koruma Komisyonu Kararı da örnek olarak verilebilecek kararlardır ayrıntılı için bkz. Akıncı, ss. 11-12.

[215] Cvria. InfoCuria - Case-law of the Court of Justice, Judgment of the Court C131/12 https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en (E.T:25/11/2021).

[216] Aydın Akgül, "Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' ve AB Adalet Divanı'nın 'Google Kararı'", **TBB Dergisi**, Sayı: 116, 2016, (Google) ss. 30–31; Karakaş, s. 268.

[217] Önok, s. 164.

[218] Develioğlu, s. 89.

Ancak bu kararda kararın konusuna dikkat çekmek gerekir: *"kararın konusu, kişisel verinin kendisinin ilgili sayfadan silinmesi değil, arama motorunda yer alan sonucun 'karartılması'dır."* Yani ABAD'nin bu kararı arama motorlarından silinmeyi içerir. Bu karar doğrultusunda silinen şey kişisel verileri içeren link sonuçları olacaktır[219].

ABAD kararının Avrupa Birliği dahilinde hizmet veren Google dışındaki diğer her bir arama motoru için bağlayıcı nitelikte olduğu görülmektedir. Google Avrupa Birliği vatandaşlara ve Avrupa Birliği sınırları içinde erişimi sınırlasa bile AB sınırları dışı için erişimi sınırlamamaktadır. Ancak ülkeler bazında sınırlama yapmak yerine tüm Google sunucularından kaldırılma yapılmasının unutulma hakkının daha doğru bir şekilde uygulanmasını sağlayacağını söylemek mümkündür[220]. Bu tartışma Google ile Fransa Veri Koruma Otoritesi (CNIL) arasında yaşanmıştır. Google tarafından ülkesel bazda bağlantının kaldırılmasının sağlandığı ancak bağlantıya küresel çapta erişilebildiği yani google.com'dan kaldırılmadığı için kendisine idari para cezası kesilmesi öngörülmüştür. Google sınırlı ve özerk internetin (splinternet) kullanıldığı alanlarda ya da unutulma hakkının tanınmadığı ülkeleri de kapsayacak şekilde küresel çapta bir kaldırma işlemini yapmasının mümkün olmadığını savunmaktadır. Bunun yerine Avrupa sınırlarını değil de aramayı yapan kişiyi esasa alarak o kişinin bulunduğu coğrafi konumda yapılan aramayı engellemeyi teklif etmektedir. Ancak bu şekilde coğrafi engelleme yöntemi adı verilen yöntemin kullanılmasının da sakıncaları bulunmaktadır. Fransa tarafından da kabul görmemiştir[221].

İlkeye ilişkin asıl düzenleme ise GDPR ile yapılmıştır. Tüzükte silinme hakkı[222] "right to erasure" olarak unutulma hakkı ise "right to be forgetten" olarak yer almıştır. Tüzüğün 17. maddesinde "Unutulma ve Silinme Hakkı" başlığı altında düzenlenmiştir.

---

[219] Önok, s. 164.
[220] Hasan Elmalıca, "Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, 2016, ss. 1617-1618.
AB Gizlilik Gereği İçerik Kaldırma başlıklı Google formu için bkz. https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637202230061146146-20083139&rd=1 (E.T:26/11/2021).
[221] Nalbantoğlu, s. 596.
[222] Akıncı, s. 19.

Tüzükte 17. maddenin ikinci fıkrasında kamuya açıklanmış olan ve birinci fıkra kapsamında verilerde yapılan silinmelerde veriyi işleyen diğer sorumlulara da imkanlar dahilinde bilgi verilmesi gereklidir. Üçüncü fıkrada ise veri işlemenin gerekli olduğu durumlar izah edilmiştir. Bu durumlar ifade özgürlüğünün kullanıldığı, veri sorumlusunun bir görev ya da resmi yetkinin kullanması, kamu sağlığı, silinme hakkının kullanılması durumunda veri işlemenin amacının engellenmiş olması, kamu yararı amacı arşivleme yapılan bilimsel ve teknik incelemelerde veri işlenmesi, bir hakkın tesisi halleri olarak sayılmıştır[223].

Unutulma hakkı kapsamında kişinin bu hak gereğince işlem yapılmasını talep etmesinde hukuki yararın olduğu haller vardır. Sayacağımız hallerden herhangi biri gerçekleştiğinde kişi kişisel verileri hakkında unutulma hakkı gereği talepte bulunabilir. Bu haller şu şekilde örneklendirilebilir[224]: Kişisel veriler daha önce hukuka uygun şekilde elde edilmiş olsa bile daha sonra hukuka ve dürüstlük kuralına aykırı şekilde işlenirse; en başta veriler meşru bir amaç olmadan, ölçüsüz, işleme amacı için gerekli süreye riayet edilmeden toplanmışsa; işlenen veriler doğru ve güncel değilse unutulma hakkı kapsamında talepte bulunulabilir.

GDPR ile unutulma hakkının düzenlenmesindeki amaçlardan biri de dijital dünyanın getirdiği veri işleme hızına sınırlar çekmek ve gerektiğinde bunların güncellenmesini sağlamaktır. GDPR'da çocuklara ilişkin düzenlemeler de mevcuttur. Tüzüğün 8. maddesinde çocuğun bilgi toplumu hizmetlerine[225] ilişkin rızası açısından geçerli koşullara yer verilmiştir. Düzenlemeye göre madde:

> *1. 6(1) maddesinin (a) bendinin uygulandığı hallerde, doğrudan bir çocuğa bilgi toplumu hizmetleri sağlanması ile ilgili olarak, çocuğun en az 16 yaşında olması halinde, ilgili çocuğun kişisel verilerin işlenmesi hukuka uygundur. Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak*

[223] Korkmaz, s. 141; Akıncı, ss. 19-20; Karakaş, s. 271.
[224] Elmalıca, ss. 1619-1620.
[225] Bilgi toplumu hizmeti ifadesinin tanımı GDPR'de bulunmamaktadır. Ancak GDPR m.3/25 de ifadenin tanımının 2015/1535 sayılı direktifte yer aldığı belirtilmekle yetinilmiştir. Bilgi Toplumu Hizmeti: Teknik Düzenlemelerin Bildirimi ve Bilgi Toplumu Hizmetlerine İlişkin Kurallar Hakkında Bir Usul Belirlenmesine Yönelik 2015/1535 Sayılı Direktif m.1/1-b'ye göre: "*(b) 'hizmet' herhangi bir Bilgi Toplumu hizmetidir; bir başka deyişle, belirli bir mesafede, elektronik araçlarla ve hizmet alıcısının münferit talebiyle normal olarak ücret karşılığı sunulan herhangi bir hizmettir*. Bkz. Avrupa Birliği Düzenlenmemiş Alan Yasal Çerçevesi, s. 60; https://ugdgm.ticaret.gov.tr/data/5f450c3f13b8761320144cdc/Avrupa%20Birli%C4%9Fi%20D%C3%BCzenlenmemi%C5%9F%20Alan%20Yasal%20%C3%87er%C3%A7eve.pdf (E.T:23/12/2021).

rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde ve verildiği veya onaylandığı ölçüde hukuka uygundur. Üye devletler, 13 yaştan küçük olmamak kaydıyla, bu amaçlara yönelik olarak kanunla daha küçük bir yaş belirleyebilir.

2. Bu durumlarda, kontrolör mevcut teknolojiyi dikkate alarak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verildiğini veya onaylandığını doğrulamak adına makul çaba sarf eder[226].

Çocukların rızaları ile yapılan işlemlerde unutulma hakkı büyük önem arz etmektedir. Çocukların verdikleri rızaların yaşamların ilerleyen dönemlerinde pişmanlıklara ve kayıtlı geçmişe yönelik olumsuz psikolojik sorunlara yol açması mümkündür. Rıza alınma için m.40/2-g'de *"çocuklara sağlanan bilgiler ve çocukların korunması ve çocuklar üzerinde velayet hakkına sahip olanların rızasının alınma şekli;"* konusunda Tüzüğün uygulanmasına yönelik davranış kuralları hazırlanabileceği ya da kurallarda değişikliklerin yapılabileceği veya kapsamda genişlemelerin yapılabileceği düzenlenmiştir. Ayrıca 57. maddede ülkelerin bu tüzük kapsamında özellikle çocuklara yönelik faaliyetlerde ihtimam gösterilmesi gerektiği belirtilmiştir[227]. Çocukların rızası konusuna rıza ile paylaşılan sosyal medya verilerinin korunmasına ilişkin değerlendirmemizi yaptığımız bölümde tekrardan değineceğiz.

Unutulma hakkı özellikle ifade özgürlüğünün korunması hakkının gözetilerek ölçülü bir şekilde uygulanması gereken bir alandadır. Haklar dengesi doğru kurulmalıdır. Arama motorlarına yapılan başvurularda yer alan taleplerin değerlendirilmesi sorumluluğu yüklenmiştir.

Kişisel verilerin silinmesi konusunda KVKK m. 7'de düzenlemelere yer verilmiştir. Kanunun 11. maddesinde 7. maddede öngörülen koşullar dahilinde kişisel verilerinin silinmesini ya da yok edilmesini isteme hakkının ilgililere tanındığı belirtilmektedir. İlgili 7. maddede hukuka uygun olarak işlenen bir veri için düzenleme yapılmıştır. Yani hukuka uygun olarak işlenen bir veri olması ve yapılan

[226] https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (E.T:26/11/2021).

[227] Nalbantoğlu, s. 594; https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (E.T:26/11/2021).

işleme faaliyetini gerektiren sebepler ortadan kalktığında veri resen ya da ilgilinin talebi ile veri sorumlusu tarafından kaldırılacaktır. Kanun metninde silinir, yok edilir veya anonim hale getirilir denilmektedir. Konuya ilişkin 28/10/2017 tarihli Resmi Gazetede (RG) Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik[228] yayınlanmıştır. Yönetmeliğin 11. maddesinde veri sorumlularına periyodik imha politikası hazırlama zorunluluğu olanlar için en fazla 6 aylık sürelerde; periyodik imha politikası hazırlama zorunluluğu olmayanlarda ise 3 aylık sürelerle kişisel verilerin resen silme, yok etme veya anonim hale getirme zorunluluğu getirmiştir. Yönetmeliğin 12. maddesinde ise KVKK m. 11 ve 13 kapsamında ilgili kişinin veri sorumlusuna başvurusu halinde veri sorumlusunun yerine getirme ve cevap verme sürelerine yer verilmiştir. Bu maddedeki süreler veri işleme şartlarının ortadan kalkıp kalmadığına göre düzenlenmiştir. Verileri işleme şartları ortadan kalktığı durumlarda veri sorumlusu ilgilinin talebi en geç 30 gün içinde sonuçlandırılacak ve ilgiliye bilgi verecektir. Ayrıca bu şartlar atında veri üçüncü kişiye aktarılmışsa veri sorumlusunun üçüncü kişiye bildirme yükümlülüğü bulunmaktadır. Verinin işleme şartlarının tamamen ortadan kalkmadığı durumda ise veri sorumlusu kanunun 13. maddesinin 3. fıkrası hükümlerine göre ret kararı verebilir. Ancak ret kararını gerekçesi ile ilgiliye yazılı veya elektronik ortamda bildirilir. Bu halde de bildirme süresi en geç 30 gün olarak düzenlenmiştir. Kanunda yer alan süre ile uyumlu düzenleme yapıldığı görülmektedir. Kanunun 13. maddesinin 2. fırkasında da veri sorumlusunun kendisine başvuranların talepleri en geç 30 gün içinde ücretsiz cevaplaması şeklinde bir yükümlülüğü bulunmaktadır.

Kişisel Verilerin Korunması Kanunumuzda yer alan düzenlemeler mülga 46/95/AT Yönergesi düzenlemelerine GDPR'den daha yakındır[229].

3. İşlemenin Sınırlandırılması Hakkı

Veri işlemenin kısıtlanması GDPR m. 4/3'te tanımlanmıştır. Fıkrada yer alan düzenlemeye göre ilgili kişiler veri işlemenin sınırlandırılmasını talep edebilecektir.

[228] https://resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm (E.T:27/11/2021).
[229] Develioğlu, s. 93.

Bu sınırlama depolanmış olan verilerin işlenmesini sınırlama amacıyla işaretlenmesi şeklinde olmaktadır. İşaretleme yapılınca bu kişisel verileri bir süre yani akıbetleri belli oluncaya kadar işlenmeyecektir.

Tüzüğün 18. maddesinde kişisel veri işlemenin kısıtlanması hakkının kullanılabileceği durumlar açıklanmıştır. İlgili verilerin doğruluğuna itiraz edebilir ve bu süreçte verinin doğruluğu doğrulanana kadar veri işleme kısıtlanabilir. Bir diğer durum yasa dışı veri işleme faaliyeti nedeni ile verilerin silinmesine itiraz edilerek bunların kullanılmasının kısıtlanması talep edilebilir. Veri sahibinin bazı yasal iddiaları nedeniyle normalde bu verilere artık ihtiyaç duyulmamasına rağmen veri sahibinin ihtiyacı nedeni ile kısıtlanabilir. Veri sahibinin m.21/1 uyarınca itiraz hakkını kullanması durumunda veri sorumlusunun meşru gerekçelerinin daha ağır olup olmadığının tespiti amacıyla kısıtlama yapılabilir. Sayılan bu durumlar 18. maddenin 1. fıkrasında a-b-c-d bentlerinde sayılmıştır. Bu hükümlere göre yapılacak sınırlama nedeni ile verinin saklanması dışında işlenmesi ilgilinin rızası, başka gerçek veya tüzel kişinin korunması ya da üye devletler için kamu yararı adına işlenebilecektir. Yapılan sınırlamaların kaldırılması halinde kısıtlama kaldırılmadan önce veri sorumlusunca ilgili kişinin bilgilendirilmesi gerektir[230].

Kişisel Verilerin Korunması Kanunu'nda bu hakka yer verilmemiştir.

4. Verilerin Taşınması Hakkı

Bu hakka GDPR m. 20 hükmünde yer verilmiştir. Söz konusu hak için m.20/1-a bendi uyarınca işleme faaliyetinin m. 6/1-a veya m. 9/2-a bentlerine göre bir rızaya ya da m. 6/1-b bendine göre bir sözleşmeye dayanması halinde ve 20/1-b bendi uyarınca işleme faaliyetinin otomatik yollarla gerçekleştirilmesi halinde tanınmıştır. Bu bentlerde belirtilen durumların olması halinde veri sahibinin kendisi ile ilgili olarak veri sorumlusuna verdiği verileri kullanılabilir şekilde ve teknolojik duruma uygun formatta alma hakkına sahiptir. Ayrıca bu veriler başka bir veri sorumlusuna iletme hakkı bulunmaktadır. Böyle bir talep olduğunda veri sorumlusunun engellemesi olmamalıdır. Bu düzenlemenin amacı kişileri farklı bir

[230] Korkmaz, s. 142.

hizmet sağlayıcısını kullanmak istediklerini verilerini o hizmet sağlayıcısına aktarabilmesini sağlamaya yöneliktir. Örneğin bir kişinin kullandığı e-postasında bulunan verileri başka bir e -posta açtığında ve verilerin o e-posta aktarılmasını istediğinde bu hak sayesinde verileri taşınabilecektir[231].

Kanun koyucu Kişisel Verilerin Korunması Kanunu'nda bu hakka yer vermemiştir.

5. İtiraz ve İrade Sergileyebilme Hakkı

İtiraz hakkı ilgililerin hukuka aykırı işlemler sebebi ile başvurabileceği denetim mekanizmaları veya yargı yollarına başvurabilmesine olanak sağlanmasıdır. Avrupa Konseyinin 108 sayılı Sözleşmesinde ilgilinin verileri üzerindeki taleplerinin yerine getirilmemesi halinde ilgiliye itiraz hakkının tanınmasına yönelik imkanların sağlanması gerektiği yer almaktadır. Mülga 95/46/AT Direktifinde de itiraz hakkının garanti altına alınması gerektiğinden bahsedilmiştir[232].

İlgililere itiraz hakkı verilmesine dair GDPR 21. maddede itiraz hakkı düzenlemesine yer verilmiştir. Maddenin 1. fıkrasında veri sahibinin m. 6 uyarınca hukuka uygun şekilde yapılan veri işleme faaliyetine herhangi bir zamanda itiraz hakkı vardır. İtiraz edilmesi halinde veri işlenemez. Veri işlenmeye devam edilebilmesi ilgili kişinin menfaati olduğu ya da temel hak ve özgürlükler açısından gerekli olduğu iddiası olmalı ve de zorlayıcı meşru gerekçeler ortaya koyulmalıdır. Verilerin pazarlama amaçlı olarak işlenmesi hallerinde de pazarlama amacı ile kişisel verilerin işlenmesine her zaman itiraz edilmesi mümkündür. Bu halde doğrudan pazarlama amaçlı işlemeye itiraz edilmesi artık verinin bu amaçla işlenmesi mümkün değildir. Yine aynı maddenin son fıkrasına göre kamu yararı sebebi ile bir görev yürütülmesi haricinde bilimsel, tarihi veya istatistiki amaçlar dahilinde verilerin işlenmesi halinde de itiraz mümkündür.

KVKK m. 11/1-g bendine göre ilgililerin *"İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,"* hakkı bulunmaktadır.

---

[231] Korkmaz, ss. 142-143.
[232] Şimşek, s. 94.

D. Kişisel Veri, İnternet ve Sosyal Medya İlişkisi

İnternet belli ülke ve sınırlara bağlı olmadan birçok kişinin kullanım sağladığı bir iletişim aracıdır. Bu şekilde geniş bir kullanıma sahip olan internet hakkında uluslararası bir düzenleme ve kontrol mekanizması bulunmamaktadır. İnternet sayesinde bilgisayarlar aracılığı ile kişiler birçok veri paylaşımında bulunmaktadır. Söz konusu verileri tutan hizmet sunucuları çeşitli olduğu için denetimi ve verilerin güvenliğini tek elden sağlamak mümkün değildir[233].

Sosyal medyada yer alan kişilik hakları ihlalleri açısından ikinci bölümde kısaca bahsedeceğimiz ihlallerin yayılmasını önleyici hızlı tedbirler yer almaktadır. Söz konusu mekanizmalar bazen önleyici bazen ihlal olması muhtemel durumlar için tedbirler alıcıdır. Sulh ceza hakimliklerince verilen kararlar da bu yöndedir. Ancak bu süreçte sulh ceza hakimliklerinin mahkumiyet ya da beraat hükmü içeren bir yargılama yapmadıkları açıktır. Sosyal medya internet aracılığı ile kişilerin birçok verisini rızayla ya da rızası dışında diğer kullanıcıların bilgisine ve ilgisine sunulduğu bir ortamdır. Bu ortamda bazen otomatik işlemlerle veriler işlenmekte bazense kullanıcının bizzat kendisi tarafından başta fotoğraflar olmak üzere kişisel veri niteliğinde birçok verisini paylaşılmaktadır. En başta kişi bir sosyal medya hesabı açarken kullanıcı adı oluşturmakta ve e mail bilgisini sosyal medya şirketi ile paylaşmaktadır. Başka herhangi bir veri kullanmasa dahi bu verileri paylaşması zorunludur. Bunun yanı sıra kullanıcıların çoğunlukla ad soyadlarını, eğitim bilgilerini, yaşadıkları şehirleri ya da konum bilgilerini paylaştıkları görülmektedir. Sosyal medya şirketlerinin ticari amaçlarla kendi ürünlerinin satışını yaptıkları da görülmektedir. Bu ürünleri satın almak isteyen kullanıcılar satın alma işlemleri sırasında hem kredi kartı bilgilerini hem de adreslerini paylaşmak durumundadır. Ayrıca sosyal medya şirketleri kullanıcılara daha iyi hizmet sunma amacıyla olarak adlandırdıkları faaliyet kapsamında topladıkları verileri kullanmaktadır. Kişilerin izledikleri ya da tıkladıkları gönderiler değerlendirilerek yapay zeka sistemleri ile istek ve tercihleri tespit edilebilmektedir. Bu veriler sürekli kayıt altında tutulmakta

[233] Şimşek, ss. 176-177.

ve kolay kolay silinmemektedir. Örneğin sürekli belli ırkı konu alan içerikleri arayan ve buna ilişkin paylaşımları takip eden kullanıcıya bu ırka ilişkin paylaşımlar daha çok gösterilmektedir. Aslında sosyal medya şirketi kullanıcının bu ırka karşı bir duyarlılığını olduğunu basit bir şekilde tespit edebilmektedir. Bazen de çeşitli verilerin toplanmasını sağlayan anketler ve düşünce paylaşımları içeren uygulamalarla bağlantılı şekilde hizmet sunmaktadır. Bu hususun en önemli örneği bir veri analiz şirketi olan Cambridge Analytica skandalıdır. Söz konusu olay 50 milyon Facebook kullanıcısının verilerinin toplaması, Global Science Research şirketi ile Cambridge Analytica arasında verilerin paylaşılmasına ilişkin anlaşma yapılmış olması ve de bu verilerin çeşitli seçimler dahil çeşitli siyasal olaylarda kullanılmış olması şüphesine ilişkindir. Facebook, Global Science Research şirketinin sahibi olan Aleksandre Kogan'a bu verilere erişim izni verdiğini doğrulamakla birlikte bu verilerin facebook kullanıcıların kendi rızaları ile paylaşmış oldukları veriler olduğunu belirtmektedir. Cambridge Analytica şirketi ise verileri kullanılmadığını ve facebook hizmet kullanım şartları gereği verileri sildiklerini iddia etmektedir[234]. Kişilerin veriler, özellikle analiz şirketlerince sosyal olayların yönlendirilmesinde kullanılabilecek etkili argümanlar olmaktadır.

Belirttiğimiz üzere sosyal medya alanında kesin sınırlar koyan mevzuat hükümleri yoktur. Gelişime ve değişime oldukça açık olan bu alanda zaten kesin sınırlar koymak mümkün değildir. Uluslararası hukukta kişisel verilere ilişkin temel ilkeler ve internete ilişkin yasal düzenlemeler yeni yeni yapılmaktadır. Sosyal medyaya dolayısıyla da internet olarak adlandırdığımız dijital ortama bir defa giren verinin artık korunmasının ve korunmasının denetlenmesinin ne kadar güç olduğu açıktır. Ancak sonuç olarak kişisel verilerin korunmasına yönelik temel ilkeler ve yasal düzenlemeler yine de en etkin koruyucu mekanizmalardır. Ticari amaç güden sosyal medya şirketlerinin verileri ticari meta olarak görmesi elbette kaçınılmaz bir sonuçtur. Sosyal medya uygulamalarının önemli bir kısmının sadece kullanmak için belli bir ücret talep etmemesi bu uygulamadan kazanç elde edebilmesinin farklı yöntemlerini geliştirmesine sebep olmaktadır. The Social Dilemma adlı belgeselde

[234] https://www.bbc.com/turkce/haberler-dunya-43469094 (E.T:17/01/2021).

"Bir ürüne para ödemiyorsanız ürün sizsinizdir." ifadesi kişisel veriler ve sosyal medya ilişkisini özetler niteliktedir.

İKİNCİ BÖLÜM

I. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ULUSLARARASI DÜZENLEMELER

A. OECD Düzenlemelerinde Kişisel Verilerin Korunması

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) ilk olarak II. Dünya Savaşı sonrasında Marshall Planı uygulamasına yönelik olarak ve Avrupa Ekonomik İşbirliği Örgütü adı ile kurumuştur. Daha sonra OECD'ye dönüştürülmüştür[235].

OECD temelde üye devletlerinin demokrasisini ve insan haklarının gelişmesine yardımcı olma, halklarının ekonomik sorunlarını analiz ederek çözümler üretme amacındadır. OECD bu amaçlarla 1961 yılında kurulmuştur. Üyeleri arasında gelişmiş Avrupa ülkeleri dışında ABD ve birçok kıtadan farklı ülke bulunmaktadır. OECD kuruluşu altında bir araya gelen devletler özellikle ekonomik anlamda işbirliği sağlayarak büyümeyi sağlamak ve iş alanları oluşturup ülkelerin ekonomik ve insani standartlarını yükseltmeyi hedeflemektedirler[236]. Geniş çapta olan bu işbirlikleri kişisel verilerin kullanımı ve korunması konusundaki sorunlar hakkında standartlar ortaya konulmasını gerekli kılmıştır.

OECD ülkelerinin veri mahremiyeti konusunda yasal düzenlemeler yapması gerekirken üye ülkelerin birçoğunda kişisel verilerin korunması için yasal düzenlemeler yapılmamıştır. Bu sebeple Örgüt belli insan hakları ve verilerin güvenliği için belli ilkelerin ortaya konulması ihtiyacı daha da artmıştır. 23 Eylül 1980 tarihinde Konsey Tavsiyesi niteliğinde olan "Kişisel Verilerin Sınıraşan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeler" kabul edilmiştir. Bu düzenleme kişisel veriler konusunda yapılan ilk uluslararası düzenleme olma özelliğine

[235] Sedat Erdem Aydın, **AİHM İçtihatları Bağlamımda Kişisel Verilerin Kaydedilmesi Suçu**, On iki Levha Yayınları, İstanbul, 2015, ss. 25-26.
[236] Korkmaz, s. 157; Mendos Kuşkonmaz, s. 38.

sahiptir[237]. Söz konusu ilkeler üye devletler için tavsiye niteliğindedir yani bağlayıcı değildir. Ancak bu ilkeler doğrultusunda düzenlemelerin yapılması üye devletler arasında yasal düzenlemelerin daha uyumlu olmasının sağlayacaktır[238].

Rehber ilkelerde şu sekiz temel ilkeye yer verilmiştir[239]:

-Veri toplamanın sınırlı olması ilkesi: Bu ilke 7. maddede düzenlenmiştir. Bu ilkeye göre veri toplanması faaliyetine sınırlar getirilmelidir. Veriler hukuka uygun amaç ve araçlarla toplanmalı gerekli hallerde veri sahibinin rızasına ve bilgisine sunulmalıdır.

-Verilerin belirli bir niteliği karşılaması ilkesi: Bu ilkeye 8. maddede yer verilmiştir. Toplanan verilerin belli bir amaçla toplanması ve bu amaca doğru hizmet edebilecek durumda tutulmasını ifade etmektedir.

-Amacın belirliliği ilkesi: 9. maddede de bu ilke düzenlenmiştir. Veriler toplanmadan önce bir amacın var olması gerekir. Amacın belirlenmiş olması zorunluluğu en geç toplama anıdır. Bu amaç dışında başka amaçlar dışında kullanılmaması gerekir. Ancak asıl amaçla bağdaşan ve amaçtaki değişikliğin veri sorumlusuna usulünce bildirilmesi durumunda bu veriler kullanılabilecektir.

-Kullanımın sınırlı olması ilkesi: Düzenlemenin 10. maddesinde de bu ilkeye yer verilmiştir. Veri sahiplerinin rızası veya kanunla verilen yetki gibi haller dışında veri işleme amacına aykırı bir kullanım yapılamaz.

-Veri güvenliği ilkesi: Rehber ilkelerden bir diğeri de 11. madde de düzenlenen veri güvenliği ilkesidir. Bu ilke verilerin çeşitli ihlallere yönelik korunması ve makul önlemlerin alınmasını öngörmektedir. Kişilerin verilerine yetkisiz kişilerce erişim sağlanması ya da zarar verilmesi gibi ihtimalleri barındırır.

-Açıklık ilkesi: Düzenlemenin 12. maddesinde açıklık ilkesi yer almıştır. Bu ilke kişisel verilere veri sahiplerinin erişim sağlanması hakkını da içermektedir. Verileri elinde tutanlarca yapılan işlemler de açıklık politikası esas alınmalıdır.

-Bireyin katılımı ilkesi: Rehber ilkelerinden 13. maddede düzenlenen bireyin katılımı ilkesi gereği veri sorumlusu verileri erişilebilir hale getirme veya açıklama gibi

---

[237] Şimşek, s. 13; Aksoy, s. 6

[238] Korkmaz, s. 156; Mendos Kuşkonmaz, s. 39; Öztürk, Çalışkan, Seyhan, ss. 45-49; OECD Rehber İlkeleri m.6, .https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (E.T:29/11/2021).

[239]Mendos Kuşkonmaz, ss. 40-41; Şimşek, ss. 12-17; Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:61, Sayı:3, Yıl:2012, ss. 1109-1110.

durumlarda veri sahibinin rızasına ihtiyaç duyması anlamına gelmektedir. Veri sorumluları veri sahiplerini bilgilendirmeli ve bilgi alma hakkının kullanılması engellenirse bu işleme ya da var olan bilgilere veri sahibinin itiraz etme hakkı olduğuna dikkat edilmelidir.

-Hesap verilebilirlik ilkesi: Son olarak 14. maddede veri sorumlularının hesap sorulabilir bir mekanizma oluşturulmalıdır. Veri sorumlularının diğer maddelerde yer alan ilkelere uygun davranmaması halinde veri sorumluları bunun hesabını sorabilmelidir.

Bahsedilen ilkelerin uzun ve yeterince açık olmadığından bahisle birçok eleştiri aldığı görülmektedir[240]. Ancak yine de uluslararası alanda yapılan ilk düzenleme olması ve yalnızca Avrupa Birliği (AB) ülkelerinin değil de daha geniş bir hitap kitlesi olması bu ilkeleri özel kılmaktadır. Özellikle AB ile ABD arasında ortak bir alan oluşturmuştur. ABD OECD üyesi bir ülke olmasına rağmen Avrupa Konseyi (AK) ve Avrupa Topluluğu (AT) üyesi olmadığı için daha sonra ortaya konulan AK ve AB yönergelerine taraf değildir[241]. Bu ilkelerin küresel manada bir etkisi olduğunu söylemek mümkündür. Kıta Avrupası dışında Avusturya, Kanada ve Yeni Zellanda gibi ülkelere ve Asya Pasifik Birliği'nin kendi veri koruma ilkelerinin belirlenmesinde etkili olduğu görülmüştür. Bygrave göre Asya Pasifik Birliği'nde bu ilkeler daha esnek bir şekilde düzenlenmiştir. Birliğin daha çok tüketici güveni endeksli bir görünüm oluşması amacında olduğu söylenebilecektir[242]. Bu rehber ilklerin 108 sayılı Sözleşme yürürlüğe girene kadarki süreçte önemli ilkleri ortaya koyup bir standart belirlemeye çalışması oldukça önemlidir[243].

1985 tarihli Sınırötesi Veri Transferi Hakkında Bildirge ve 1998 tarihli "Global Ağ Gizliliğinin Korunması Hakkında Bakanlık Bildirgeleri de OECD tarafından hazırlanan diğer belgelerdendir[244].

B. Birleşmiş Milletler Temel Metinlerinde Kişisel Verilerin Korunması

[240] Özdemir, Elektronik, s. 19; Mendos Kuşkonmaz, s. 41; Korkmaz, s. 157.
[241] Mendos Kuşkonmaz, s. 42.
[242] Lee A. Bygrave, "Privacy and Data Protection in an International Perspective", Stockholm Institute for Scandinavian Law, 2010, s. 184 (Privacy) https://www.scandinavianlaw.se/pdf/56-8.pdf (E.T:10/01/2022); Mendos Kuşkonmaz, s. 42.
[243] İkbal Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Turhan Kitabevi, Ankara, 2010, s. 158.
[244] Kılınç, s. 1111.

Birleşmiş Milletler (BM) barış ve güvenliği korumak bunun için gerekli ortak önlemler alınmasını sağlamak, halkların eşitliği ve kendi geleceklerinin belirlemesi ilkesine saygı duyulan dostça ilişkiler geliştirmek, temel hak ve özgürlüklerin geliştirilmesi ve güçlendirilmesi adına uluslararası işbirliği sağlamak gibi amaçlara sahiptir. Bu amaçlarına BM Şartı'nın 1. maddesinde değinilmektedir[245].

BM'nin kişisel veriler konusu ile bağlantılı olarak değerlendirilebilecek düzenlemelerine bakıldığında ilk düzenlemenin 10 Aralık 1948 tarihinde kabul edilen BM İnsan Hakları Evrensel Bildirgesi ile yapıldığı görülmektedir. Bildirge BM'nin temel amaçlarından olan herkesin temel hak ve özgürlüklerine saygı gösterilmesi ve geliştirilmesi amacına hizmet etmekte olup insan hakları konusunda önemli standart ve ilkeleri belirtme adına önemli bir adımdır[246]. Bildirgede doğrudan kişisel veriler konusuna yer verilmemiş olup 12. madde de özel hayatın gizliliği hakkına yer verilmiştir. Özel hayatın korunmasına yönelik bir diğer düzenleme ise BM Medeni ve Siyasal Haklar Sözleşmesinde 17. maddede düzenlenmiştir. BM İnsan Hakları Komitesinin 16. Genel Yorumu ile 17. madde kapsamında kişisel verilerinin korunmasının özel hayatın gizliliğinin etkin bir şekilde korunması yönünden gereklilik olduğunu değerlendirmiştir[247]. Ancak bu yoruma ilişkin genel olması ve belirli amaçla veri işlenmesi ya da dürüstlük kuralı gibi kişisel verilere ilişkin önemli ilkelere yer verilmemiş olması nedeni ile eleştiriler yapılmıştır[248]. BM'nin 17. Madde hakkındaki 16. Genel Yorumu kısaca şu şekildedir[249]: Özel hayatın etkili bir şekilde korunması ancak ilgiye bunların ne şekilde tutulduğuna ve ne kadarının saklandığına ilişkin bilgileri öğrenme imkanı verilmesi ile sağlanır. Bu bilgileri öğrenme hakkının yanında ilgili hukuka aykırı olarak toplanmış ya da eksik ve hatalı bilgilerin kaldırılmasını isteme hakkına da sahiptir.

BM kişisel verilere ilişkin olan Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri 1990 yılında kabul etmiştir. BM Rehber İlkeleri olarak adlandırılan bu ilkeler tavsiye niteliğinde olup üye ülkeleri bu konuda

[245]BM Şartı m.1, https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf (E.T:28/11/2021).
[246] Küzeci, s. 133.
[247] Mendos Kuşkonmaz, s. 43.
[248] Bygrave, Data, s. 253; Küzeci, s. 133; Mendos Kuşkonmaz, s. 44; Korkmaz, s. 159.
[249] Küzeci, s. 134.

düzenleme yapmaya teşvik etmektedir. Bu ilkeler bilgisayara işlenen kişisel veriler için uygulanmaktadır. Ancak bu Rehber İlkeleri içerene düzenlemenin en önemli özelliği *"kişisel verilerin korunması için yetkili ve bağımsız olan verilerin korunması organlarının kurulmasını öngören ilk uluslararası belge"* olmasıdır[250].

BM Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler şunlar olarak sayılmıştır. Bu ilkeler yasal ve dürüst yollarla toplama ve işleme ilkesi, işlenen verilerin doğruluğu ilkesi, amacın belirliliği ilkesi, ilgili kişinin erişimi ilkesi, ayrımcılık yapmama ilkesi, veri güvenliği ilkesi, sınır ötesi veri akışı, denetim ve yaptırım ilkesidir. Denetim ve yaptırım ilkesi, bu alandaki denetimin bağımsız ve tarafsız bir kuruma verilmesi ve de kurumca kurulların uygulanması konusunda gerekli yaptırım ve denetimlerin uygulanması anlamına gelmektedir[251].

BM Rehber İlkeleri de OECD Rehber İlkeleri gibi tavsiye niteliğinde olmasına rağmen OECD Rehber İlkeleri gibi etkiye sahip olamamıştır. Ancak yine de Birleşmiş Milletler tarafından böyle bir düzenlemenin yapılması kişisel verilerin gelişmiş ülkeler nezdinde dikkate alınması gereken bir husus olmaktan çıktığını göstermesi açısından önemlidir[252].

C. Avrupa Konseyi Düzenlemelerinde Kişisel Verilerin Korunması

Avrupa Konseyi II. Dünya Savaşından sonra kurulmuştur. Bu Konsey esasen Avrupa'da insan hakları ve demokrasinin gelişmesine yönelik faaliyetler yapmaktadır[253]. Avrupa Konseyinin Statüsüne Dair Sözleşme 5 Mayıs 1949 tarihinde imzaya açılmış ve 3 Ağustos 1949 tarihinde yürürlüğe girmiştir. Türkiye Cumhuriyeti de Konsey'e davet edilerek kurucu üyeler arasında yer almaktadır. Konseyin kuruluşun başlangıç bölümünde hukukun üstünlüğü, halkların temel hak ve özgürlüklerine vurgu yapılmaktadır[254]. Ayrıca Statünün 3. maddesinde konseyin her üyesinin ülke sınırlarında olan her bireyin bu haklardan yararlanması prensibini benimsediği hususuna yer verilmiştir.

---

[250] Şimşek, s. 16; Mendos Kuşkonmaz, s. 44; Küzeci, s. 136.
[251] Kılınç, s. 1112.
[252] Bygrave, Privacy, s.185; Küzeci, s. 136; Mendos Kuşkonmaz, s. 45; Kılınç, s. 1112.
[253] Şeref Gözbüyük ve Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, Turhan Kitabevi, Ankara 2009, s. 8.
[254] https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020093815001_tur.pdf (E.T:02/12/2021).

Konsey temel hak ve özgürlüklerin korunması ve geliştirilmesi konusunda uluslararası alanda en fazla katkıyı sunan kuruluşlardan olmuştur[255]. Konseyin en önemli katkısı Avrupa İnsan Hakları Sözleşmesini hazırlamış olmasıdır. AİHS dışında Konseyin birçok sözleşmesi ve Avrupa İnsan Hakları Mahkemesi ve birçok denetim mekanizması bulunmaktadır. Öncelikle düzenlemeler özel hayatın gizliliğine yönelik olsa bile kişisel veriler konusu da sözleşmelere ve Avrupa Konseyi Bakanlar Komitesi kararlarına yansımıştır. Kişisel verilerin korunmasına ilişkin Avrupa Konseyi Bakanlar Komitesi'nin internette özel hayatın korunmasına ilişkin, sigorta işlemleri kapsamında toplanan veriler ilişkin, tıbbi ve istatistiki verilere ilişkin olmak üzere birçok konuda tavsiye kararı bulunmaktadır[256].

Kişisel verilerin korunması konusuna verilen önem nedeni ile bu konudaki bilinci arttırmak amacıyla 108 sayılı Sözleşme'nin imza tarihi olan 28 Ocak Konsey tarafından "Veri Koruma Günü" olarak ilan edilmiştir[257].

1. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme (108 sayılı Sözleşme)

Avrupa Konseyi tarafından 108 sayılı Sözleşme 1981 yılında kabul edilmiş ve 1985 yılında yürürlüğe girmiştir. Bu sözleşme kişisel verilerin korunmasına yönelik uluslararası hukukta bağlayıcı nitelikte olan ilk belgedir. Bununla birlikte sözleşmede güçlü bir koruma mekanizmasına yer verilmemiştir[258]. Avrupa Konseyi Avrupa İnsan Hakları Sözleşmesinin kişisel verilerin bilgisayarlara işlenmesi gibi konularda doğrudan kişisel veriler konusunu düzenlememiş ve düzenlemelerin yetersiz durumda olması sebebi ile 108 sayılı sözleşme kabul edilmiştir. Böylece kişisel verilerin korunması hakkı ayrı bir hak olarak sözleşmeye aktarılmıştır[259].

AİHS'te özel hayata ilişkin düzenlemeler olmasına ve AİHM kararları ile kişisel verilerin bu kapsamda değerlendiriliyor olmasına rağmen 108 sayılı sözleşmenin düzenlenmesi kişisel veriler konusunda düzenlemeye ihtiyaç

[255] Şimşek, s. 19.
[256] Ayrıntılı bilgi için bkz. Yılmaz, ss. 128-129.
[257] Küzeci, 2021, s. 143.
[258] Atak, AB, s. 90.
[259] Henkoğlu, ss.53, 54.

olmasından kaynaklanmıştır. Çünkü kişisel verilerin korunması alanı için bu düzenlemeler yetersiz kalmıştır. Değişen teknolojik gelişmeler ve kişisel verilerin özel bilişim sistemlerde neredeyse alan sınırlamasına tabi olmadan tutulabilir hale gelmesi, uluslararası alanda veri aktarımlarının yapılıyor olması böyle bir düzenlemeye zemin hazırlamış hatta düzenlemeyi zorunlu kılmıştır[260].

Sözleşmeye Türkiye de taraftır. Sözleşmenin 1. maddesine göre gerçek kişinin uyruğuna, vatandaşlığına ya da bulunduğu ülkeye bakılmaksızın temel hak ve özgürlüklerinin ve kişisel verilerinin otomatik işleme tabi tutulması halinde özel hayatına saygı hakkı bu sözleşme ile güvence altına alınması amaçlanmaktadır. Düzenleme de özellikle otomatik işleme tabi olan kişisel verilerin esas alınması ve bu verilerin uluslararası akışına önem verildiği görülmektedir. Sözleşmeye göre otomatik işleme tabi olacak verilerin niteliği 5. maddede şu şekilde açıklanmıştır: Bu verileri adil biçimde yasal yoldan elde edilmeli ve işlenmelidir. Veriler ancak belirli meşru amaçlar içinde işlenebilir ve ancak bu amaçlarla kullanılabilir. Verilerin kaydedilmesi amaçlarına uygun olarak olur ve aşırı veri kaydedilmez. Kaydedilen veriler doğru olmalıdır ve güncellenmelidir. Kaydedilen veriler süreye bağlı olmalıdır. Bu süre verinin kaydedilme amacına göre olmalıdır. Amaç gerçekleşene kadar ilgili veriler bu sürelerde kişinin kimliği belirlenebilecek şekilde uygun şekilde saklanmalıdır[261].

Sözleşmenin temel özelliklerinden biri 108 Sayılı Sözleşme m. 23 göre Avrupa Konseyi üyesi olmayan ülkelerin de imzasına açık olmasıdır. Bu sebeple sadece üye devletler değil de daha geniş bir alanda uygulaması olabilecek bir sözleşmedir. Bir diğer önemli özelliği ise uluslararası alan da kişisel veriler konusunu içeren ve bağlayıcı olan belge olma niteliğini korumaktadır[262].

Sözleşme ile gerçek kişilerin kişisel verilerinin korunması amaçlanmıştır. Sözleşmenin güvence altına aldığı veriler elle işlenen veriler değil de otomatik olarak işlenen veriler olmuştur. Otomatik veri işleme faaliyetini yapan hem kamu hem de özel sektörden olabilir. Her iki halde de ülke tarafından imza edilmiş bu sözleşmeyi uygulamakla yükümlü olacaklardır. Sözleşmenin 10 maddesinde taraf ülkelerin içi

[260] Düşünceler için bkz. Şimşek, 22; Küzeci, s. 143; Mendos Kuşkonmaz, s. 48.
[261] Bakanlar kurulu onay kararı ve Sözleşmenin Türkçe metni için bkz. 2016/8576 Sayılı Resmi Gazete https://resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf (E.T:02/12/2021).
[262] Küzeci, s. 143.

hukuk düzenlemeleri ile sözleşmeye işlerlik kazandırması gerektiği düzenlenmiştir. Taraf ülkeler uygun şekilde başvuru yolları ve yaptırımlar getirmekle yükümlüdür. Sözleşmeye uygun şekilde iç hukukta yürürlüğe koyulacak yasal düzenlemelerle kişisel verilerin işlenmesi konusunda ortak ülkelerce temel güvenceler sağlanmış olacaktır. Ancak Sözleşme ülkelere yaptıkları iç hukuk düzenlemelerinin uygulanmasını izlemeye yönelik bir kontrol makamı oluşturma zorunluluğu getirmemiştir. Bu hususta eksiklik ek protokol ile giderilmiştir. Bağımsız kontrol makamları getirilecek ve bu makamlar hukuki hak arama yollarına dahil edilerek kişilerin kişisel verilere yönelik şikayetleri inceleme yetkisine sahip olacaktır[263].

Sözleşmenin 11. maddesinde getirilecek düzenlemelerin sözleşmede öngörülenden daha fazla önlem içermesinin sözleşmeye aykırılık olarak yorumlanamayacağı hükmüne yer verilmiştir. Konuya ilişkin farklı değerlendirmeler bulunmaktadır. Atak'a göre özellikle 11. madde hükmü gereği ülkeler düzenlemelerinde otomatik veriler dışında diğer veri işleme faaliyetlerini de güvencelere dahil edebilecek ve bu durum sözleşmeye aykırılık oluşturmayacaktır[264]. Ancak tekrar belirtmek gerekir ki sözleşmenin açıkça düzenlediği hususun otomatik veri işleme faaliyeti olduğu görülmektedir.

2. AİHS 8. Maddesi Kapsamındaki Koruma

Avrupa İnsan Hakları Sözleşmesi (AİHS) kişisel veriler ve temel insan hakları konusunda büyük öneme sahiptir. Daha önce bahsettiğimiz üzere kişisel verilerin korunması hakkı bu sözleşmede doğrudan düzenlenmemiştir. Sözleşme 1950 yılında Roma da imzalanmış ve on devletin onaylama sürecinin tamamlanması sonucunda 1953 yılında yürürlüğe girmiştir. Sözleşmenin 19. maddesi gereğince sözleşmenin ve protokollerinin yorumu ve uygulanması, temel hak ve özgürlüklerin korunması konusunda etkin koruma sağlamak ve uluslararası alanda bu hususlara ilişkin yargısal denetim yapma amacıyla Avrupa İnsan Hakları Mahkemesi kurulmuştur[265].

[263] Atak, AB, ss. 99, 120.
[264] Atak AB, s. 95.
[265] Avrupa İnsan Hakları Sözleşmesi Metni için bkz.

AİHS ülkemiz tarafından 1954 yılında imzalanmış olmasına rağmen Türkiye için önem kazanması 1987 yılında Avrupa İnsan Hakları Komisyonuna ve 1990 yılında Avrupa İnsan Hakları Divanına başvuru hakkı getirilmesi ile olmuştur[266].

AİHS'nin m.8'de özel ve aile yaşamına saygı hakkı yer almaktadır. Bu madde içeriğinde temelde dört koruma alanı yer almaktadır: Birincisi özel yaşam, ikincisi aile yaşamı, üçüncüsü kişinin evi ve dördüncüsü kişinin haberleşmesidir[267]. AİHM'nin de yorumlarıyla 8. maddenin kapsamının genişlediği söylenebilir. Özellikle kişisel verilerin korunması hakkına da doğrudan yer verilmiş olmadığını tekrar belirtmek gerekir. Ancak mahkemece maddedeki hakların güvence altına alınması için kişisel verilerin korunması gerektiği yönünde yorum yapılmaktadır. Bireysel özerklik ve bireylerin kendi bilgilerinin geleceğini belirleme hakkını 8. maddenin yorumunda temel ilkelerden görmektedir[268].

AİHM içtihatlarında özel hayata saygının yalnızca gizli bilgilerin korunması ile sağlanamayacağını bireylerin kendi kişiliğini geliştirmesinin tamamlamasının ve diğer insanlarla ilişkilerini de içerecek şekilde kişilik haklarının da bu koruma kapsamına alındığı kabul edilmektedir. AİHM "kişisel otonomi" yani kişisel gelişimin de m. 8 güvencesi kapsamında olduğunu genişletilmiş yorumla kabul etmektedir[269].

AİHM'in m. 8 kapsamında değerlendirdiği hususlar şunlardır[270]:

- Bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi (Amann vs İsviçre, Başvuru No: 27798/95; Rotaru vs Romanya, Başvuru No: 28341/95)
- Telefon görüşmelerine ilişkin kayıtları izleme (Malone vs Birleşik Krallık, Başvuru No: 8691/79; P.G. ve J.H. vs Birleşik Krallığı, Başvuru No: 44787/98)
- Toplanan verilerin toplanma amacı dışında kullanılması (Leander vs İsviçre, Başvuru No: 9248/81)

---

https://www.anayasa.gov.tr/media/3542/aihs_tr.pdf (E.T:03/12/2021); Mendos Kuşkonmaz, s. 53.

[266] Şeref Gözübüyük ve Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, Turhan Kitabevi, Ankara, 2009, s. 11.

[267] Gözübüyük ve Gölcüklü, s. 333.

[268] Küzeci, s. 149.

[269] Yılmaz, a. 137.

[270] Küzeci, s. 154.

- Sağlık verilerinin gizliliği (Z. vs Finlandiya, Başvuru No: 22009/93; M.S. vs İsveç, Başvuru No: 20837/92)
- Emniyet güçleri tarafından parmak izi ve fotoğrafların alınması (Murray vs Birleşik Krallık, Başvuru No: 14310/88)
- Kişisel verilere erişim hakkı (Gaskin vs Birleşik Krallık, Başvuru No: 10454/83)[271]
- Kişisel verilerin gerektiğinden uzun süre tutulması (S. ve Marper vs Birleşik Krallık, Başvuru No: 30562/04, 30566/04)
- Kimlik hakkı (Wisse vs Fransa, Başvuru No: 71611/01, Ciubotary vs Moldovya, Başvuru No: 27138/04)
- Kişilik ve bireysel özerklik ilkelerini içeren kişisel gelişim hakkı (Christine Goodwin vs Birleşik Krallık, Başvuru No: 28957/95; Evans, Birleşik Krallık, Başvuru No: 6339/05; (Sidabras ve Džiautas vs Litvanya, Başvuru No: 55480/00, 59330/00; K.A. ve A.D. vs Belçika, Başvuru No: 42758/98, 45558/99; Pretty vs Birleşik Krallık, Başvuru No: 2346/02)

Türkiye tarafından da imzalandığını belirttiğimiz AİHS Anayasamızın m. 90/5 hükmüne göre temel hak ve özgürlükleri içerdiği için yasalarla arasında bir uyuşmazlık olması halinde bu sözleşme hükümlerinin esas alınması gerecektir. Sonuç olarak AİHS ve AİHM'nin sözleşmeyi uygulamaya ve yorumlamaya ilişkin kararları oldukça önemlidir. AİHM de kişisel verilerin korunması hususunu açıkça 8. madde kapsamında değerlendirmektedir. Bu da sözleşmeye taraf olan ülkemizce dikkate alınması gereken bir husustur. Ancak AİHM yorumlarının ve kararlarının da çok kapsamlı olmadığı ve sınırlı kaldığı unutulmamalıdır. Örneğin AİHS'nin güvencesi devlet tarafından gerçekleştirilen temel hak ve özgürlüklere yönelik ihlalleri kapsamaktadır. Ancak kişisel verilerin ihlali konusunda bunu gerçekleştiren tarafın devlet mi olabileceği, devletin pozitif yükümlülükleri kapsamında özel sektör

[271] Atak, AB, ss. 106-107; Mendos Kuşkonmaz, s. 58; Güray Dağ, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, Doktora Tezi, İstanbul 2011, s.32-33; *"Gaskin/Birleşik Krallık Kararında AİHM, başvurucunun kendi çocukluğuna ilişkin bilgilere ulaşabilmesinde yaşamsal bir menfaatinin olduğunu kabul etmiştir. Mahkemeye göre, raporları hazırlayan kişilere ulaşılamaması ya da bu kişilerin açıkça itiraz etmemesi durumunda, bu raporlara ulaşmak isteyen bireyin menfaatleri güvence altına alınmalıdır. Şayet raporları hazırlayanlar, bu raporların açıklanmasına rıza göstermiyor yahut cevap vermiyorsa bu durumda raporların açıklanmasına ilişkin nihai kararı bağımsız bir otoritenin vermesi sağlanmalıdır. Dava konusu olayda bu sağlanmamıştır. Bu nedenle, Sözleşmenin 8.maddesinin ihlal edildiği sonucuna ulaşmıştır."*

tarafından gerçekleştirilen veri işleme faaliyetlerini nedeni ile sorumluluk ortaya çıkıp çıkmayacağı yani hangi durumlarda AİHS korumasından yararlanılabileceğinin muğlak olduğu görülmektedir[272].

AİHM m.8 kapsamında ihlal olup olmadığını incelerken kişisel verilerle ilgili tanımlamalarda ve sınırlarını belirlemede 108 sayılı Sözleşmeyi, ülkelerin içi hukuklarındaki yasal düzenlemelerini dikkate almaktadır. Mahkemece *"kişisel verilerin kaydedilme koşulları, kayıtlı kaldıkları süreler, verilerin kullanım şekilleri ve kimlere erişim hakkı tanındığı"* gibi hususlar değerlendirilmektedir[273].

AİHM 8. maddeyi incelerken 2 aşamalı bir değerlendirmede bulunmaktadır: İlki ilgili başvurunun 8. maddede yer alan haklara ilişkin olup olmadığının incelemek ve bu hakların kapsamında olduğuna karar verirse devletin bu hakka saygı gösterme konusunda pozitif yükümlülüğünün olup olmadığı ve varsa buna uygun davranıp davranmadığını belirlemektir. Bahsettiğimiz bu husus maddenin 1. fıkrasına ilişkindir. İkincisi ise maddenin 2. fıkrasına bakılarak 8. maddede yer alan hakka müdahale edilip edilmediği ve eğer müdahale edilmişse bu müdahale yasalara uygun, meşru amaç taşıyan ve demokratik toplum için gerekli olan bir müdahale olup olmadığı konusunda karar vermeyi içermektedir[274].

AİHS m.8/2'de hakka ilişkin sınırlama sebeplerine yer verilmektedir. Buna göre kamu makamlarının müdahalesi için aşağıda yer alan koşullar oluşmalıdır: Yapılan müdahalenin yasa ile öngörülmüş olması gereklidir ayrıca demokratik toplum için gerekli ve öngörülen amaç ile orantılı olması ve de sınırlama sebeplerinden birini ya da birkaçını içermelidir[275].

AİHS m. 8 de yer alan sınırlama sebeplerinin geniş ve muğlak olduğu görülmektedir. Ancak Sözleşmenin metninde yer alan ölçütler ve AİHM tarafından

---

[272] Gözübüyük ve Gölcüklü, s. 332; Küzeci, s.150; X ve Y vs Hollanda Başvuru No:8978/80, Karar: 26/03/1985, par.23; "*sadece devleti ... müdahale etmekten kaçınmaya zorlamaz: bu aslen negatif taahhüdün yanı sıra, özel hayata ve aile hayatına etkin biçimde saygı gösterilmesinin doğasında olan pozitif yükümlülükler de olabilir... Bu yükümlülükler, bireylerin kendi aralarındaki ilişkiler alanında bile, özel hayata saygı gösterilmesini sağlayacak önlemler almayı içerebilir."* Ursula Kilkelly, "Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı (Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi'nin uygulanmasına ilişkin kılavuz)", **Avrupa Konseyi**, Almanya, 2001, ss. 35-36.

[273] Yılmaz, s. 138.

[274] Kilkelly, s. 14

[275] Sınırlama sebepleri şunlardır: Ulusal güvenliğin korunması; kamu emniyetinin korunması; ülkenin ekonomik refahının korunması; düzenin korunması, suçun önlenmesi; genel ahlakın ve sağlığın korunması; üçüncü şahısların özgürlüklerinin ve hakların korunması.

oluşturulan içtihatlar çerçevesinde bu sınırlamalar kayıt altına alınmıştır. Klass ve diğerleri kararı "ilke karar" olması ayrıca somut olayda fiilen bir ihlal gerçekleşmemesine rağmen AİHM tarafından soyut norm denetimi yapılmış olması kararı önemli kılmaktadır. AİHM Klass ve diğerleri kararında sınırlama yapılırken *"Mahkeme... dar yorumlanması zorunlu birkaç istisna ile sınırlanan ifade özgürlüğü ilkesi ile karşı karşıyadır"* denilmek suretiyle sınırlama nedenlerinin dar yoruma tabi olduğunu açıklamıştır[276]. Mahkeme organize suçlulukla mücadele konusunda ulusal güvenlik sebebi ile ülkelerin iç hukuklarında yapılan düzenlemelere daha ılımlı bakmaktadır. Ayrıca Klass ve diğerleri kararı kişisel veriler konusunda ilk kararlardan olma özelliği taşımaktadır. Özellikle kişisel verilerin toplanması konusuna ilişkin önemli tespitleri barındırmaktadır. Söz konusu kararda doğrudan kişisel veri kavramı kullanılmamasına rağmen kişilere ait bilgilerin gizli izleme yöntemleri ile elde edilmesi konusuna değinilmiştir. Klass ve diğerlerin kararında Mahkemeye göre yasal bir dayanak olmaksızın kişinin telefonlarının gizlice dinlenmesi 8. maddenin ve de özel hayatın gizliliği korunması hakkının ihlalidir. Mahkemeye göre, yasal dayanağı olan ve yasaya uygun olarak gerçekleştirilen izleme yöntemleri özel hayatın gizliğine müdahaledir. Böyle bir yasal düzenlemenin yapılmış olması yasanın uygulanması durumunda uygulanan her kişi için temel hak ve özgürlüğüne yönelik bir tehdittir. Sonuç olarak bu tehdit, posta ve telekomünikasyon hizmetlerini haberleşme amacı ile kullanan kişilerin özgürlüklerini etkilemektedir. Kararda devletlerin bu tarz tehditlerle mücadele yasal düzenlemelerle gizli izleme yöntemlerinin kullanılmasını demokratik toplumlarda gerekli olduğunu ve düzenlemeyi kabul edilebilir bulmuştur. Ancak bu yorumu yapmakla birlikte gizli izleme yöntemlerinin kullanılması durumunda bunların kötüye kullanılmasını ihtimalinde gerekli tedbir ve güvenceler var olmalıdır. Mahkeme sınırsız bir yetkiyi kabul etmemektedir[277].

Anayasa Mahkemesi bir kararında; AİHM'in kararlarında 8. madde de yer alan haklardan yararlanılabilmesi için etkili güvencelerin sağlanması gerektiğine dikkat çekmiştir. Diğer bir ifade ile *"müdahaleyi doğuran karar alma sürecinin bu*

[276] Murat Volkan Dülger, "Avrupa İnsan Hakları Mahkemesi Kararlarında Organize Suçla Mücadelede Özel Koruma Tedbirleri", Yıldızhan Yayla'ya Armağan, **Galatasaray Üniversitesi Yayınları**, İstanbul, 2003, (AİHM) ss. 279-280.
[277] Mendos Kuşkonmaz, ss. 54-56; Küzeci, ss. 155-157.

maddeyle korunan hak ve özgürlüklere gerekli saygıyı sağlayacak nitelikte ve adil olması gerek"lidir. AİHM kararlarında etkili güvencelerin sağlanmasındaki temel amacın bu haklara keyfi müdahalede bulunulmasını önlemek, müdahalenin gerekçelendirilmesini sağlamaktır. Mahkeme hem negatif yükümlülüklerde hem de pozitif yükümlülüklerde usule ilişkin etkili güvencelerin oluşturulması gerektiği düşüncesindedir[278].

AİHM m. 8 kapsamında yaptığı değerlendirmelerde öncelikle konunun 1. Fıkra kapsamına girdiği değerlendirmesi yapıp sonrasında 2. fıkrada yer alan sınırlama sebepleri nedeni ile meşruluk kazanması halinde ihlal kararı vermeyecektir. Bu sebeple sınırlama sebeplerine göre yapılan davranışlar ihlal kararı verilmemesine sebep olacaktır. Yukarıda sınırlı olarak sayımı yapılan sınırlama sebeplerinde belirtilmiş amaçlardan bir ya da birkaçına yönelik olması haricinde sınırlamanın da sınırları[279] olan iki ölçüt olan birincisi yasada öngörülen ikincisi ise demokratik toplum için gerekli olan ve de öngörülen amaç ile orantılı olan müdahale meşru olarak değerlendirilmektedir[280].

Sınırlamaların yasal düzenleme ile yapılmış olması önemli bir konudur. Bu şart ile hem resmi makamların keyfiliğinin önüne geçilmeye çalışılmış hem de aleniyet olması sağlanmıştır. AİHM Malone vs Birleşik Krallık kararında düzenlemenin doğrudan kanun olmasını aramadığını belirtmektedir. Karara esas olan başvuruda malın çalıntı olduğu iddia edilmektedir. Başvurucu da aynı zamanda antikacıdır. Mahkemece esas alınan şey ise iç hukukta bu düzenlemelerin ulaşılabilir ve öngörülebilir hukuki dayanağın olmasıdır. Sunday Times vs Birleşik Krallık kararında Mahkeme kişilerin temel hak ve özgürlük konusunda yetki veren düzenlemeye ulaşabilir olması yani vatandaşların bu hukuk kuralının varlığı konusunda bilgi sahibi olabilmeleri ve bu kuralın vatandaşların uymasına sebep olacak kesinlik içerir olması yani öngörülebilir olması gerektiğini ifade etmiştir. Bazı düzenlemelerin biraz soyut, karmaşık ya da uygulayıcıya takdir alanı bırakıyor olması kanun koyucunun takdiridir. Önemli olan bu soyut ya da karmaşık görünen kısımların da basit bir hukuki yardımla öğrenilebilir ve anlaşılabilir olmasıdır. Ayrıca

[278] AYM Ayla Demir İşat [GK], Başvuru No: 2018/24245, 8/10/2020, §72; Ciubotaru vs Moldova, B. No: 27138/04, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/24245 (E.T:22/01/2022).
[279] Gözübüyük ve Gölcüklü, ss. 294, 295.
[280] Küzeci, s. 155.

kanun koyucunun da uygulayıcının takdirine bıraktığı alanlara da belli sınır ve kesinlik sağlamış olması halinde öngörülebilir olma şartı sağlanmış olacaktır[281].

Rotaru vs Romanya Kararında AİHM iç hukuktaki kanuni düzenlemelerde şu noktalara dikkat çekmiştir: Mahkeme ulusal güvenliği etkileyen konularda hangi bilgilerin hangi kişilerce toplanıp kaydedilebileceğine yer verilmediğinden bahsetmektedir. Ne tür verilerin kaydedilebileceği, veri toplama faaliyeti yapılabilmesi için gereken durumlar ve de izlenecek prosedürlerin neler olduğu ayrıca bu verilerin ne kadar süre ile saklanabileceği gibi hususlar düzenlenmemiştir[282]. Mahkeme benzer bir şekilde Huvig vs Fransa Kararında da iletişimin denetlenmesi hususunda sözleşmeci devletlerin vatandaşlarına bazı güvenceleri sağlaması gerektiğini belirtmiştir. Örneğin telefonların dinlenmesinin hangi suç kategorileri için mümkün olduğu, tedbirin hangi sürelerle uygulanabileceği, kayıtların silinmesi gereken hallerin neler olduğu, kamu görevlilerine bu hususta verilen yetki alanının net sınırları gibi[283].

AİHM sınırlamaların demokratik toplumda gerekli olup olmadığı konusunu da incelemektedir. Mahkeme bu koşulu da aramakla birlikte çok fazla değerlendirmesi olmamıştır. Hatta devletlerin de demokratik toplum düzeninin gerekleri ölçütünü temel hak ve özgürlükler konusundaki düzenlemelerinde esas almadığı görülmektedir. Mahkemenin de müdahalenin yasal temeli olması ve sınırlama sebeplerine dayanması koşulları konusuna daha ağırlık verdiği görülmektedir[284]. Demokratik toplum düzeninde gerekli olma konusu irdelenirken gereklilik kavramı zorunluluk oluşturan bir halden ziyade birey hakları ile kamu yararı arasındaki orantı olarak anlaşılmalıdır. Olsson vs İsveç Kararında da Mahkemece davaya bütün olarak bakmakta devletin ilgili ve yeterli nedenlere sahip olup olmadığının incelemektedir[285].

D. Avrupa Birliği Dahilinde Kişisel Verilerin Korunması

[281] Yılmaz, ss. 139-140.
[282] Rotaru vs Romanya Kararı, Başvuru No: 22009/93; Kilkelly, s. 49; Yılmaz, s. 144.
[283] Dağ, s. 30.
[284] Küzeci, s. 158.
[285] Kilkelly, ss. 53-55; Başka kararlar için bkz. Yılmaz, ss. 147-148.

Avrupa Birliği (AB) oluşumu ikinci dünya savaşı sonrasında öncelikle Avrupa Kömür ve Çelik Topluluğu kurulması ile başlamıştır. Daha sonra 1957 yılında Roma Anlaşması ile Avrupa Ekonomik Topluluğu ve Avrupa Atom Enerjisi Topluluğu oluşturulmuş. Nihayetinde bu üç toplulukta Maastricht Anlaşması yani Avrupa Birliği Anlaşması ile bu birlik altıda bir araya gelmiştir[286]. AB'nin kurulması Avrupa'nın ekonomik, sosyal, siyasal ve temel haklar konularında bütünlemesine yönelik önemli bir sürecin sonucu olmuştur. Bu teşkilat kendine özgü birlik mevzuatı oluşturmuş ve vatandaşları lehine birtakım haklar ihdas etmiştir[287]. Birlik siyasal ve ekonomik bir ortaklık oluşturma amacıyla hareket etmektedir. Bu kapsamda mal hizmet ve vatandaşların serbest dolaşımını esas almış ve ortak pazar geliştirmeye çalışmıştır. Böyle bir ortamın oluşturulabilmesi için devletlerarası veri akışı ve buna ilişkin düzenlemeleri gerektiren bir ortam oluşmuştur. AB'de veri akışı için ortak pazarın gerektirdiği koşullara uygun düzenlemeler ortaya koymuştur[288].

Birlik içinde uygulamaya yönelik kararlar veren Avrupa Birliği Adalet Divanın (ABAD) Google-İspanya Kararı çalışmamızda ilkeler kısmında değindiğimiz önemli kararlardandır. Divana başvuru iki şekilde olmaktadır. İlki üye devletlere karşı dava açılması ikincisi ise Birlik düzenlemesine ile ilgili Divanın yorumuna başvurulmasıdır[289].

1. Avrupa Birliği Temel Haklar Şartı

AB Temel Haklar Şartı (ABTHŞ) 7 Aralık 2000 tarihinde imzalanmış ve Avrupa Birliği tarihinde ilk kez AB sınırları içinde yaşayan kişilerin bireysel, siyasal ve ekonomik haklarını tek bir metinde toplanmıştır. Metinde yer alan düzenlemeler 2004 yılında AB Anayasasına dahil edilmiştir. Ancak AB Anayasası onaylanmadığı için metnin önem kazanması Temel Haklar Şartına atıf yapan Lizbon Antlaşmasının kabul edilmesi ile olmuştur. ABTHŞ altı bölümden oluşmuştur. İkinci bölümden yer alan özgürlükler başlığı altında özel hayata ilişkin AİHS hükmüne benzer şekilde bir düzenlemeye yer verilmiştir. Temel şartın 7. maddesinde özel hayata ve aile

[286] https://ab.gov.tr/_105.html (E.T:07/12/2021).
[287] Küzeci, s. 167.
[288] Mendos Kuşkonmaz, s. 66.
[289] Korkmaz, s. 207.

yaşamına, iletişimine herkes saygı gösterilmesini isteme hakkına sahiptir denilmektedir. Maddede haberleşme ifadesi yerine iletişim ifadesinin kullanılmış olması Temel Haklar Şartının AİHS m. 8'e göre gelişime ve yoruma açık bir şekilde düzenleme yapılmaya çalışıldığı şeklinde yorumlanmıştır. Temel Haklar Şartının asıl önemi ise bu metinin kişisel verilerin korunması hakkında ilk metinlerden olmasıdır. Şartların 8. maddesinde kenar başlığı "kişisel verilerin korunması" şeklinde olmuştur. Maddede herkesin kişisel verisinin korunması hakkına sahip olduğu ve bu verilerin dürüst bir şekilde, belli amaçlarla işlenmesi gerektiği ifade edilmektedir. Ayrıca veriler işlenirken rıza, yasa ile öngörülme ya da meşru amaç aranmalıdır. İne maddede kişisel veriler konusunda bilgi edinme hakkı, verilere erişme ve düzeltme hakkına; bağımsız denetim makamına yer verilmektedir[290].

Kişisel verilere ilişkin bu düzenlemenin özel hayatın gizliliği konusundan ayrı şekilde düzenlenmiş olması yeni anayasa çalışmalarında kişisel veriler korunması hususunun ayrıca düzenlenmesine örnek teşkil edecektir. Metinde yer alan herkes ifadesi gerçek kişilere yöneliktir[291]. Ayrıca maddede verilerin işlenmesinin dürüstlük kuralına uygun şekilde ve belli amaçlarla olabileceğine yer verilmiştir. Veri işleme faaliyeti rızayla ya da meşru kılacak sebeplerle olabilecektir. Bunun yanında kişisel verilere erişim hakkı, düzelttirme hakkı ve de kurallara uyulması konusunda bağımsız denetim makamına da yer verilmiştir. Aslında bu düzenleme ile kişisel veriler konusunda AİHM'nin içtihatlarında yer alan konuları düzenlemiştir[292].

2. Avrupa Birliği Veri Koruma Direktifi (95/46/AT)

Ulusal kişisel verilerin korunması mercilerinin AB'ye baskıları sonucunda bu direktif[293] düzenlenmiştir. Öncesinde 1970'li yıllara kadar Avrupa Parlamentosunun

[290] Küzeci, s. 174; Küzeci'ye göre AB ile İlişkiler Genel Müdürlüğü tarafından yapılan Türkçe çevirisinde 8. Maddede çeviri hataları yapılmıştır. Bu hatalar basit görünse de anlamsal farklılıklara yol açmaktadır.

[291] AB Temel Haklar Şartının hazırlanmasına dayanak olarak 95/46/AT sayılı Direktif gösterilmektedir. Bu direktifte yer alan düzenlemelerde gerçek kişiler esas alınmıştır. Bu sebeple Temel Haklar Şartında da herkes tabirinin yalnızca gerçek kişilere yönelik olduğu yorumu yapılmaktadır; Şimşek, s. 73.

[292] Küzeci, ss. 175-176.

[293] Direktifler AB hukuku bakımından kanun yapma araçları arasında yer almaktadır ancak doğrudan bağlayıcı olmayan düzenlemelerdir. Üye devletlerin direktiflerde yer alan temel ilkelere uygun şekilde yasalarını düzenlemeleri beklenir. Bkz. Akıncı, s. 7.

ilke kararları ile veri mahremiyeti konusunda açıklamalar yapılmıştır. Ancak 1980'li yıllarda yeni teknolojik gelişmeler veri mahremiyeti konusunda endişelere sebep olmuştur. AB vatandaşlarının verilerinin korunması ve AB ülkeleri arasında kanuni düzenlemelerde ortaya çıkan farklılıkların giderilmesi için bu direktifin hazırlanması talep edilmiştir. Avrupa Komisyonu tarafından taslak metin hazırlanmış ve Bakanlar Konseyince 1995 yılında kabul edilmiştir. 95/46/AT sayılı bu direktif yine bu yılda onaylanmış ve üç yıl sonra da yürürlüğe girmiştir. Bu veri direktifi, AB Genel Veri Koruma Tüzüğünün (GDPR) 14 Nisan 2016'da onaylanması ve 25 Mayıs 2018'de yürürlüğe girmesi ile yürürlükten kalkmıştır. Tüzük üye devletler için bağlayıcı nitelikte olup devletlere de GDPR'yi iç hukuklarına dahil etmeleri için 2 yıllık süre tanınmıştır[294]. Direktif yürürlükten kaldırılmış olsa da hem AB metinleri arasında hem de KVKK mevzuatımızın hazırlanmasında dikkate alınmış olması açısından önemli bir yere sahiptir[295]. Direktif genel çerçeve belirlemektedir. Direktifin yorumu için yapılmış olan başvuruya ilişkin Avrupa Birliği Adalet Divanın 06/11/2003 tarihli Bodil Linqvist- İsveç Kararında direktifin temel amacının ülkelerinin yasalarının uyumlaştırılması için genel çerçeve çizmek olduğu açıklamaktadır[296].

Düzenlemede yer alan birkaç önemli hususdan bahsetmek gerekir: Direktif sadece gerçek kişilere ilişkin verilerin işlenmesinde uygulanacaktır. Direktifin 1. maddesinde düzenleme bu şekilde olsa da ülkelerin iç hukuklarında tüzel kişileri de bu korumaya dahil edebilmesi mümkün olan haller de olabilir. Örneğin tüzel kişi aracılığı ile gerçek kişilerin verilerine ulaşma durumu olabilir. Yönergede temel alınan sekiz ilkenin olduğu söylenebilir. Bunlar sınırlı amaç ilkesi, kalite prensibi, veri güvenliği ilkesi, hassas verilerin özel korumaya sahip olması[297], şeffaflık ilkesi, veri transfer ilkesi, bağımsız çözüm ilkesi, bireysel çözüm ilkesidir[298].

---

[294] Yılmaz, s. 151.

[295] Mendos Kuşkonmaz, ss. 70-71; Yılmaz, ss. 153-154.

[296] Avrupa Birliği Adalet Divanı Bodil Lindqvist Kararında direktifin üye devletlere yüksek korumayı göstermekle birlikte bazı durumlarda da takdir yetkisi tanımakta olduğu belirtilmiştir. Ancak sonuç olarak üye devletlerin *"kişisel verilerin serbestçe dolaşımı ile özel hayatın gizliliği arasında denge sağladığından"* emin olmasını sağlayıcı düzenlemeler yapmış olması gerekir. https://kisiselveriihlali.com/Anasayfa/wp-content/uploads/2021/10/Bodil-Linsqvits-Isvec-Karar-Cevirisi-23.10.2021.pdf (E.T:07/12/2021).

[297] *"Hassas veriler yönergenin 8. maddesine göre şu hallerde işlenebilir: Veri sahibinin açık muvafakatı, çalışma hukuku alanındaki yükümlülüklere uyma, veri sahibinin yaşamsal çıkarları, özel hukuk tüzel kişilerinin faaliyetleri, verilerin kamuya açıklanmış olması, hukuki iddiaları tesis etme, uygulama ve savunma, sağlık açısından gereklilik, suçlar, mahkûmiyetler ve güvenlik tedbirleridir."*

Linqvist-İsveç kararına esas olan olay kişisel veriler ve internet konusunda önemli bir örnektir. Adalet Divanına aslında direktifin internet ortamında nasıl uygulanabileceği konusunda açıklama yapma olanağı sunmuştur. Bir kilisede çalışan Bayan Lindqvist, internet sitesinde cemaat ve kilise görevlerine ve törenlere yönelik bilgilendirme yapmaktadır. Ancak yapılan işlem katılımcıların rızaları olmadan yapılmaktadır. İnternet sitesinde kişilerin isimleri, telefon bilgileri gibi kişisel bilgileri yer almıştır. Ayrıca bunların yanında hassas veri niteliğinde olan bilgilere de yer vermiştir. Adalet Divanı internet ortamında direktifin uygulanıp uygulanmayacağını ve de internette paylaşılan verilerin üçüncü ülkelere veri aktarma anlamına gelip gelmediği gibi iki hususu açıklığa kavuşturmaya çalışmıştır. Söz konusu kararda Divan üçüncü ülkeye aktarma ile yayınlamanın aynı anlamda olmadığını açıklamıştır. Çünkü bir internet sitesine veri yüklemekle üçüncü ülkeye veri aktarımının aynı anlama geleceğinin kabul edilmesi önemli bir denetimi gerektirecektir. Veri koruma konusunda yeterli korumaya sahip olmayan ve de internet erişimine sahip olan tek bir ülkenin olması halinde transfer yasağı söz konusu olacaktır [299]. Divana göre Yönerge kar amacı gütmeyen durumlarda da uygulanacaktır. Divan, internet sitelerinde yapılan paylaşımları verilerin otomatik yolla işlenmesi olarak kabul etmektedir. Söz konusu işlemde ekonomik bir amaca yönelmiş olunmasa da yönergenin m.3/2 hükmünde yer alan istisnalara, bireyin özel veya aile yaşamına da girmemektedir. Veriler internet ortamında yayınlanarak "belirsiz sayıda kişimin erişimine açık" hale gelmiştir[300].

Bu yönerge de elektronik ortamlarda tutulan verilerin toplanması ve silinmesi süreçlerinde kişinin tanınmasını sağlayan her türlü işlem kişisel verilerin işlenmesi olarak değerlendirilmiştir. Yönergenin 29. maddesi ile kurulan ve tavsiye kararları

Bu haller hukuka uygunluk sebebi olarak değerlendirilebilir. Ancak veriler beli amaçlarla belli kurumlarla paylaşıldığında bu verilerin başkaları ile paylaşılabilmesi için yine veri sahibinin rızası gerekir. Veri sahihi hassas verisini kamuya açıklarsa veri işlenebilir hale gelmektedir. "*AIDS hastası olan bir kişinin televizyon programında HIV virüsü taşıyıcısı olduğunu söylemesi konuya örnek olarak verilebilir.*" Bkz. Kılınç, ss. 1121.

[298] Kılınç, ss. 1121-1123.

[299] Mendos Kuşkonmaz, ss. 76-77.

[300] Küzeci s. 184.

veren 29. Maddede Veri Koruma Grubu "*site yöneticilerinin rutin olarak depoladıkları ziyaretçi IP numaraları"*nı kişisel veri olarak tanımlamaktadır[301].

Önemli hususlardan biri çerez yani cookie'ler konusudur. "*Sosyal medya sitelerinde kullanıcının internet kullanımı sırasında tıklama yoluyla ziyaret ettiği web sayfalarının sunucuları tarafından işlemcisine yerleştirilen 'cookie'ler sayesinde sanal dünyada kullanıcının bir profili çıkarılmaktadır."* Çerez programlar aslında kullanıcıların tanınmasını ve kullanıcıya özel teklifler sunabilmek için özelleştirilme yapılmasıdır. Veri sahibi olan kullanıcının alışkanlıklarının ve de ilgi alanların bu sayede depolanmaktadır. Depolanan verilerin kişisel veri niteliğinde olduğu açıktır. Bu husus kişisel verilerin korunmasına konusunda gözden kaçırılan önemli tehdittir. Yönergenin 4. maddesine göre bu yönergenin uygulama alanı sitede herhangi bir işlem üzerinde kontrol sahibi olan gerçek veya tüzel kişinin işletmesinin olduğu yerleri de kapsamaktadır. İşletme sınırları AB'de olanlar için zaten yönerge uygulama alanı bulmakta iken ayrıca da çerezleri denetleyen bir sistemin AB sınırları içinde olması ihtimalinde yönergenin uygulanması gerektirecektir. 29. Madde Veri Koruma Grubu çerez programları konusunda 2002 yılında vermiş olduğu tavsiye kararında sitenin işletmesinin AB dışında olması halinde bu çerez programları ile AB vatandaşının kişisel bilgilerinin işlenmesine imkan sağlıyorsa böyle bir durumda kişisel verilerin korunması bakımından AB vatandaşının bilgisayarının bulunduğu yer hukuku uygulanması gerektiği kanaatine varmıştır. Örneğin sosyal medya sitelerinde kullanıcılar bizzat kendileri hakkındaki formları gönüllü olarak doldurmaktadır. Bu formlarda kişisel bilgilerini açıklaması halinde elde edilen veriler bir çerez programı aracılığı ile kullanıcıların kimliği belirleyebilecektir. Sonuç bahsettiğimiz çeşitli ihtimallerde de site yöneticileri AB mevzuatına uymakla yükümlü olacaklardır[302].

3. Özel Yaşamın ve Elektronik İletişimin Korunması Yönergesi (2002/58/AT)

[301] Kemal Atasoy, "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması Ve Veri Sahibinin Rızası" **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cevdet Yavuza Armağan, Cilt:22, Sayı:3, 2016, s. 279.
[302] Atasoy, ss. 280-281.

Elektronik iletişim konusundaki eksik düzenlemeler olması nedeni ile 25 Haziran 2002 tarihinde bu yönerge kabul edilmiştir. Yönergenin faklı yönlerinden biri de tüzel kişileri de koruma kapsamına almasıdır. Ayrıca yönergenin 3. maddesinde bu yönergenin kamusal olarak ulaşılabilir elektronik iletişim araçlarınca işlenen veriler için uygulanacağını düzenlemiştir. Bu yönerge de yer alan konular kısaca şu şekildedir[303]: Güvenlik, iletişimin gizliliği, veri işlemenin sınırlanması, istenmeyen iletiler yani spam[304], çerezlerin ve casus yazılımların kullanımları, yer bilgileri, verilerin saklanması[305] konularıdır.

Yönerge spam adı verilen istenmeyen iletiler için düzenlemeler getirmiştir. Kullanıcılar e-mailleri haberleşme vasıtası olarak kullansa da e-mailler siteler tarafından reklam yayma aracı olarak da kullanılmaktadır. Ayrıca kullanıcıların e-mail adresleri kişiler internette gezindiklerinde kullanıcıların kimlerle görüştükleri ya da hangi sitelere bağlandıkları gibi verileri barındırmaktadır Kişilerin e mailleri yoluyla elde edilen genel profil bilgilerinin pazarlama gibi amaçlarla satılması da mümkündür. Bu sebeple yönergeye göre kişilerin mai hesaplarına ticari içerikli mesajların gönderilmesi için önceden kullanıcının rızasının alınması şartını getirmiştir. Benzer şekilde kullanıcıların cep telefonlarına ticari amaçlı mesajların gönderilmesi de önceden kullanıcının rızasının alınması şartına bağlıdır. Kuralın istisnası; önceden bilgilendirme yapılması ve bununla birlikte kullanıcıya ücretsiz bir şekilde rahatlıkla reddetme imkanının tanınmış olmasıdır[306].

Yönerge yani kısaca E-Gizlilik Direktifi 2009 yılında değişikliğe uğramıştır. 2009/136/AT direktifinin getirilmesinin sebebi çerezlerin indirilmesi ile ilgilidir. Daha önce de bahsettiğimiz üzere çerez ya da cookies olarak adlandırdığımız şeyler indirildiğinde kişisel verilerimize ulaşılmasını sağlayan ve kullanıcının işlemcisine indirilen küçük bir veri topluluğudur. Son düzenleme ile indirilebilmesi için rıza

---

[303] Küzeci, s. 202

[304] Atasoy, ss. 288-290; "*Sosyal medyada kişisel verilerin işlenmesine verilen rıza konusunun önemli bir noktasını da opt- in rıza ve opt-out rıza türleri oluşturmaktadır. Opt-in ve opt-out rıza arasındaki en büyük fark, kişisel veri sahibinin veri toplama, işleme, saklama gibi faaliyetlere vereceği rıza beyanını aktif mi, yoksa pasif bir davranışla mı karşı tarafa sunacağının belirlenmesindedir.*"

[305] Verilerin Saklanması konusundaki hükümler 2006/24/ AT sayılı İletişim Trafik Verilerinin Saklanması Yönergesi dikkate alınacaktır. Söz konusu düzenlemede verilerin saklanması "ciddi suç" terimine dayandırılmış olduğu için tartışmalara sebep olmuştur. Verilerin tutulma süreleri altı ile yirmi dört ay şeklinde geniş bir zaman aralığı olarak belirlenmiştir. Bkz. Küzeci, ss. 206-207.

[306] Korkmaz, ss. 227-228.

alınması ön şartı getirilmiştir[307]. Yönergenin 25 numaralı gerekçesinde çerezlerin yerleştirilmesine engel olma olanağının sağlanması gerektiği belirtilmektedir. Ayrıca çerezler vasıtası ile elde edilene verilerin amacı kullanıcıya daha iyi bir hizmet sunulmasının sağlanmasıdır. Bu amaç doğrultusunda elde edilen veriler kişisel verilerin korunması hukukuna uygun olarak tutulmalı ve de amacın ortadan kalkmış olması ya da gerek kalmaması gibi durumlarda silinmelidir[308].

4. 29. Madde Veri Koruma Grubunun 5/2009 Sayılı Çevrimiçi Sosyal Ağlar Konusundaki Tavsiye Raporu[309]:

Sosyal medya birinci bölümde ayrıntılı olarak açıkladığımız üzere kullanıcıların birbiri ile iletişim halinde olmalarını, tercih ve yaşamları hakkında yazılı veya görsel-işitsel paylaşım yapmalarını sağlayan bir platformdur. Bu platformda paylaşılan her bir kişisel veri pazarlama amacı ile hareket eden şirketler için oldukça yararlı bir alan oluşturmaktadır. Sosyal medya; reklam verme ve hedef gruplara ulaşma amacıyla yaygın bir biçimde kullanılmaktadır.

AB düzenlemelerinde de bu husus dikkate alınmaktadır. Düzenlemelere göre veri denetçisi kişisel verilerin toplanması, işlenmesi, saklanması ve silinmesi gibi hususlardan sorumludur. Söz konusu alan sosyal medya olduğunda ise veri denetçisi sosyal medya sitelerinin yöneticileri/sağlayıcılarıdır. Örneğin site içinde bir hesabın açılması ya da kapatılması işlemini bir hizmet aracıdır. Bunun gibi hizmet araçlarını sağlayan ve kullanıcılara temel hizmetleri sunan kişiler hizmet sağlayıcılardır. AB mevzuatında sosyal medya sorumluluğu olan site yöneticilerinden başka veri denetçisi olarak sorumluluğu olan başka bir grup vardır. Bunlar ise uygulama sağlayıcılar/yöneticileridir. Yani akıllı telefonlarda sosyal medyaya ulaşımı sağlayan uygulama sağlayıcılardır. Sosyal medyadaki kullanıcıların da veri denetçisi olduğu durumlar vardır. Örneğin *"Başka bir kullanıcının verilerini başka bir veri denetçisi veya üçüncü bir kişiye ifşa etmesi"* gibi bir durumda ifşa eden kullanıcı veri denetçisinin sorumluluklarına sahip olacaktır. Ancak veri denetçisinin sorumluluğu

[307] Atasoy ss. 281-282.
[308] Korkmaz, s. 229.
[309] Bu başlık altında yer alan bilgiler belirtilen kaynağın özeti niteliğindedir: Atasoy, ss. 282-284.

konusunda getirilen “ailevi istisna” yani kişisel verilerin sadece kişisel veya ailevi amaçlarla sosyal medya sitelerinde işlenmiş olması halinde veri denetçisi sayılmanın sorumluluğunu gerektiren durumlar oluşmayacaktır.

Söz konusu ailevi istisnanın uygulanmayacağı durumlar bulunmaktadır: Veri Koruma Grubuna göre bunlardan ilki kullanıcının bir şirket ya da işletme adına hareket etmesi ya da sosyal medyayı ticari ya da politik amaçlarla veya bağış toplama amacıyla kullanıyorsa kullanıcı ailevi istisnaya dahil edilmez. İkincisi ise sosyal medya kullanıcısının, sadece arkadaşlar gibi bir sınırlama kullanmadan güvenlik ayarlarını herkesin verilerini görebileceği şekilde ayarlamış olması halidir ki bu durumda kullanıcı ailevi istisnaya dahil edilmeden veri denetçisi sorumluluğuna tabi olacaktır. Üçüncü durum ailevi nitelikte bir paylaşım olmasına rağmen paylaşımda üçüncü bir kişinin kişisel verisinin (Özellikle hassas verisi) işleniyor olması ki bu durumda veri işleyen kullanıcı açısından hem medeni hem de ceza hukuku yönünden sorumluluk doğması mümkündür. Bu duruma örnek olarak bir kişinin gittiği bir partide çektiği fotoğrafları kişilik haklarına saldırı oluşturabilecek ve de hakaret niteliğinde olan yorumlarla paylaşması hali verilebilir. Olayda paylaşım yapan kullanıcının kişilik haklarına aykırı davranışı hem medeni hukuk hem de suç niteliğindeki paylaşımı nedeni ile ceza hukuku açısından sorumluluğunun doğmasına sebep olacaktır. Ailevi istisnanın uygulanmadığı son durum kişisel verilerin basın ve ifade özgürlüğünün söz konusu olduğu durumlar veya sanatsal amaçlarla işlendiği durumlardır. Ancak bu hallerde ailevi istisna söz konusu olmasa bile kullanıcıya veri denetçisinin sorumluluğu yüklenmeyecektir. Veri Koruma Grubuna göre son durum için ifade özgürlüğü ve özel hayatın gizliliği konusu söz konusu olup bu iki hak arasında dengenin sağlanması gereklidir.

Hassas veriler konusunda Veri Koruma Grubunun ayrıca açıklamaları bulunmaktadır. Hassas veriler kişinin ırkı, dini ya da sağlığı ile ilgili verilerdir. Sosyal medyada paylaşılan fotoğraflar ya da ziyaret edilen sayfalar bu hassas verilere ilişkin önemli ipuçları sağlamaktadır. AB ülkeleri genellikle veri sahibi tarafından paylaşılan fotoğrafları hassas veri olarak kabul etmektedir. Ancak Veri Koruma Grubu, hassas veri ifşa edilme amacıyla bir fotoğraf paylaşılırsa ancak bu durumda fotoğrafın hassas veri olarak kabul edilmesi gerektiği düşüncesindedir. Veri denetçileri hassas verilerin işlemesi gereken durumlarda bu işlemi gerçekleştirmeden

önce kullanıcının açık rızası elde edilmelidir. Veri Koruma Grubu şirketlerin kullanıcıların hassas verilerini pazarlama amacı ile kullanmaması gerektiğini savunmaktadır.

5. Avrupa Birliği Veri Koruma Regülasyonu (2019/679-GDPR Avrupa Birliği Genel Veri Koruma Tüzüğü)

Kişisel veriler konusunda en son düzenleme GDPR olmuştur. Avrupa Parlamentosu bu tüzüğü 14/04/2016 tarihinde onaylanmıştır. Tüzük 25/05/2018 tarihinde yürürlüğe girmiştir. Tüzüğün yürürlüğe girmesi ile 95/46/AT sayılı yönerge yürürlükten kalkmıştır. Tüzük bağlayıcıdır ve ayrıca niteliği gereği yönergeden farklı olarak başka herhangi bir karara ihtiyaç duyulmadan doğrudan AB üyesi olan devletlerin iç hukukuna dahil olmuştur. Yönergenin kabul edildiği tarihler henüz internet konusunda yeni yeni gelişmelerin olduğu dönemler iken tüzüğün düzenlendiği dönemde daha yüksek bir korumaya ihtiyaç olduğu açıkça anlaşılmaktadır[310].

65/46/AT sayılı yönergenin gelişen teknoloji bakımından yetersiz kalması, kişisel verilerin işlenme alanlarının artması, sosyal medya, bulut gibi depolama sistemleri ve de elektronik ticaretin yaygınlaşması gibi faktörler yeni bir düzenlemeyi zorunlu kılmıştır. Tüzük aracılığı ile AB genelinde yeknesak bir uygulama ve düzen oluşturulmaya yönelik bir adım atılmıştır[311]. AB sisteminde Tüzükler üye devletlerin hukukuna herhangi bir işleme gerek kalmadan doğrudan dahil olmaktadır. GDPR özellikle verilerin taşınması ve unutulma hakkı gibi yeni haklar getirmiş olan hakları güçlendirmiş ve yaptırımların da ağırlaştırmıştır[312].

Veri Koruma Tüzüğü 173 paragraftan oluşan giriş bölümünden ve 99 maddeden oluşmaktadır. Önemli yenilikler getiren kapsamlı bir belge olarak düzenlenmiştir. Tüzükte kişisel verilere ilişkin daha etkin korunma sağlanması, veri işleyenlerin ve kontrolörlerinin sorumluluklarının artırılması, uygulanma alanının

[310] Yılmaz, s. 167.
[311] Nilgün Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", **Marmara Üniversitesi Hukuk Araştırmaları Dergisi**, Cilt:21, Sayı:1, 2015, ss.78-85.
[312] Küzeci, 2021, s. 222.

genişletilmesi gibi konularda önemli düzenlemeler yapılmıştır[313]. GDPR sadece AB vatandaşlarını kapsamaz. AB sınırları içinde yaşayan ancak AB vatandaşı olmayan göçmenler, çalışma ve turist vizesi sahibi olanlar ve de AB sınırları içinde oturma izni sahibi olan kişiler tüzük kapsamına girmektedir. Ayrıca verinin AB sınırları içinde olması o kişisel verinin GDPR kapsamında korunmasını gerekli kılmaktadır. Tüzük hükümlerinin uygulanması için veri işleyen kişinin AB sınırları içinde olması yeterlidir[314]. Özellikle AB merkezli olmayan şirketler açısından esas alınacak şey AB üyesi ülkelerde veri işleme faaliyeti gerçekleştirip gerçekleştirmedikleri olacaktır[315].

Tüzükte yer alan temel düzenlemelere ilk bölümde ilkeler kısmında ve de 6698 sayılı kanun ile karşılaştırmalar yaptığımız kısımda yer verdiğimiz için tekrara düşmemek adına değinmeyeceğiz.

II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN TEMEL ULUSAL DÜZENLEMELER

A. ANAYASA' DA KİŞİSEL VERİLERİN KORUNMASI

Kişisel veriler konusunda 1982 Anayasa'sında yapılan ilk düzenleme 2010 Anayasa değişikliği ile olmuştur. Anayasanın özel hayatın gizliliği başlıklı 20. maddesine 3. fıkra eklenmiştir. Eklenen düzenlemede kişisel verilerin korunmasını isteme hakkına herkesin sahip olduğuna; ilgilinin verileri ile ne yapıldığını öğrenme, verilerine erişme, verilerinin silinmesini ve düzeltilmesini isteme gibi haklarına yer verilmiştir. Ayrıca kişisel verilerin işlenmesi için "açık rıza" ya da "kanunda açıkça öngörülen hal" olması gerektiği belirtilmiştir[316].

Anayasa değişikliği sonucunda eklenen fıkra ile kişisel verilerin korunması hakkı konusunda doğrudan bir anayasal düzenleme olmuştur. Üst başlık olan özel

[313] Akıncı, s. 14.
[314] Öztürk, Altınok Çalışkan, Seyhan, s. 47.
[315] Küzeci, 2021, s. 224.
[316] https://mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5 (E.T:09/12/2021).

hayatın ve gizliliğin korunması başlığı altında dolaylı olarak kişisel verilerin korunması hakkını destekleyen düzenlemeler de yer almaktadır[317].

Kişisel verilerin korunması hakkına ilişkin hususlar Anayasa'da da belirtildiği gibi kanunla düzenlenecektir. Ay. m. 104'te yer alan düzenlemeye göre kişisel verilerin korunması hakkı konusunda cumhurbaşkanlığı kararnamesi ile düzenleme yapılamayacaktır. Çünkü kişisel verilerin korunması hakkına ilişkin düzenleme Anayasanın ikinci kısmında ve kişinin hakları ve ödevleri başlıklı ikinci bölümünde yer almaktadır[318].

Anayasa değişikliği öncesinde Anayasa Mahkemesi de AİHM gibi kişisel verilerin korunması hakkını 20. madde de yer alan özel hayatın gizliliği ve de ifade özgürlüğü çerçevesinde değerlendirmiştir. Anayasa Mahkemesi 2006/167 Esas, 2008/86 Karar sayılı 20/03/2008 tarihli kararında kendilerinden veri talep edilen gerçek ve tüzel kişilerin, kurum yetkililerinin bilgi vermekle yükümlü olduklarına ve bilgi vermedikleri takdirde para cezasının uygulanacağına ilişkin hükmün iptaline karar vermiştir[319].

B. KİŞİSEL VERİLERİN KORUNMASI KANUNU

Kişisel verilerin korunması ile ilgili olan 6698 sayılı Kişisel Verilerin Korunması Kanunu 07/04/2016 tarihinde yürürlüğe girmiştir. Bu kanun hukukumuzda kişisel verilerle ilgili temel kanun olmuştur. Kişisel verilerin korunması konusunda daha önceden doğrudan bir yasal düzenlememiz olmadığı için bu konuda önemli bir boşluk mevcuttu. Ancak teknolojik gelişmeler, ülkeler arası veri transferinde uygulama çıkan sorunlar, AİHM ihlal kararları, AB ülkelerindeki düzenlemeler ve de AB uyum süreci gibi sebeplerle yasal düzenleme yapılması ihtiyacını artmıştır. Kanunun kabulünden birkaç ay önce de 1981 yılında imzalanan ama yürürlüğe konulmamış olan 108 sayılı sözleşme onaylanmış ve yürürlüğe girmiştir[320].

[317] Öztürk, Altınok Çalışkan, Seyhan, s. 48.
[318] Yılmaz, ss. 198-199.
[319] Küzeci, s. 294.
[320] Yılmaz, ss. 201-202.

Kanun 95/46/AT sayılı yönerge esas alınarak düzenlenmiştir. Ancak kanunun kabulü sonrasında Avrupa Parlamentosu tarafından GDPR kabul edilmiştir. Dolayısı ile bazı yönlerden son düzenleme olan ve 95/46/AT sayılı yönergeyi yürürlükten kaldıran GDPR ile bazı farklılıklar oluşmuştur. GDPR(Tüzük) ile temel farklılıklar şu şekildedir[321]:

- 6698 sayılı kanun da doğrudan unutulma hakkı düzenlenmemişken tüzükte silinme hakkı olarak açıkça unutulma hakkını düzenlemiştir. Kanunda 11. maddelerde belli koşullarda kişisel verileri silinmesi ve yok edilmesi hakkından bahsedilmiştir. Ancak yasada açıkça unutulma hakkı adıyla yer almasa da Anayasa Mahkemesi kararlarında AİHM kararlarına atıflar yapılarak unutulma hakkı açıkça kullanılmaktadır. Örneğin N.B.B. başvurusunda bu konuya açıkça yer vermiştir. Mahkeme unutulma hakkının doğrudan anayasa ya da kanunda düzenlenmediğini ancak Anayasanın 5, 17, 20. maddelerinde yer alan düzenlemelerin ve de internetin ortaya çıkardığı riskler sebebi ile doğal bir sonuç olduğunun tespitini yapmıştır. Mahkemeye göre günümüzde internette birkaç kelime yazarak *"bireylerin geçmişte yaptıkları ve hatırlamak ve/veya hatırlanılmasını istemedikleri hatalarını"* öğrenmek mümkündür. Mahkeme ABAD'nin Google Spain Kararını dayanak göstererek ifade özgürlüğü ile bu haklar arasında adil bir denge kurulması gerektiğine de değinmiştir[322].

- Tüzük kişisel verilerin işlenmesinde alınan rıza konusunda ayrıntılı düzenlemelere sahiptir. Özellikle verilen rızanın her zaman geri alınması konusu 6698 sayılı Kanunda açıkça yer almayan bir konudur. Çocukların rızaları konusunda kanunda bir düzenleme yapılmamışken tüzükte on altı yaşından küçük çocuklar için ebeveynlerinin rızası ile "bilgi toplumu hizmetleri"nden yararlanabilecekleri hükmüne yer verilmiştir.

---

[321] Yılmaz, ss. 220-246.

[322] AYM Genel Kurul Kararı N.B.B. Başvuru No: 2013/5653, 03/03/2016, § 45,46,47.
Genel Kurul kararında unutulma hakkı Ay, m. 17 ve m. 20/3 bağlamında bir değerlendirilmeye tabi tutulmuştur. *"...devletin bireye geçmişte yaşadıklarının başkaları tarafından öğrenilmesi engellenerek "yeni bir sayfa açma" olanağı verme hususunda bir sorumluluğu olduğu açıktır… İnternet vasıtasıyla kolayca ulaşılabilir ve uzun süre muhafaza edilebilir kişisel veriler nedeniyle başkaları tarafından kişiler hakkında ön yargı oluşturabilmesi nedeniyle manevi varlığının geliştirilmesi için gerekli onurlu bir yaşam sürdürmesine ve manevi bağımsızlığına müdahaleyi sürekli kılmaktadır."* https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653 (E.T:01/01/2022).

- Kanunda düzenlenen idari para cezaları tüzükte yer alan idari para cezalarıyla karşılaştırıldığında oldukça azdır. Tüzükte idari para cezaları 20 milyon Euro veya kurumun gelirine göre gelirinin yüzde 4'üne ulaşabilecek idari para cezası miktarları öngörülmüşken 6698 sayılı kanunda idari para cezası için belirlenen en üst rakam 1 milyon Türk Lirası olarak belirlenmiştir.

- Tüzükte kişisel verilerin işlenmesi sebebi ile zarara uğrayanların tazminat talebinde bulunabileceği düzenlenmemiştir. Ancak 6698 sayılı kanunda 11. maddede sadece kanuna aykırı olarak kişisel verilerin işlenmesi hali için tazminat öngörülmüştür.

- Tüzük ile kanunda öngörülen veri sorumlusu kişiler ve sorumlulukları biraz farklıdır. Tüzükte veri kontrolörü ve veri işleyicisi vardır. Özellikle veri kontrolörünün görev tanımın, kişisel verinin işlenmesindeki amacı ve yöntemi belirleyen olması olarak açıklanması önemlidir. Tüzüğe göre her ikisi de kişisel veri ihlallerinde sorumludur. Kanunda ise veri sorumlusu için idari para cezaları öngörülürken veri işleyenler için idari para cezası öngörülmemiştir.

- Tüzüğe göre kişilerin rızası olsa dahi verinin transfer edileceği ülkenin yeterli teminatlar sağlamadığı durumda verinin AB dışına çıkarılması yasaktır.

- Tüzüğe göre veri kontrolörü veri ihlali meydana geldiğinde ihlal sebebi ile bildirim yapmakla yükümlüdür. Önlemlerin alınabilmesi için veri kontrolörü veri koruma otoritesine ve veri sahibine 72 saat içinde bildirim yapacaktır. Kanunda ise m. 12/5'te veri sorumlusuna bildirim yükümlülüğüne yer verilmiş ancak süre konusu düzenlenmemiştir. (Daha önce belirttiğimiz üzere Kişisel Verileri Koruma Kurumu 2019/10 Sayılı Kararı uyarınca bildirme süresi ihlali öğrenmeden itibaren 72 saat olarak kabul edilmiştir.)

- Tüzükte hassas veya önemli miktarda büyük veriler tutan kurumların veri koruma görevlisinin bulunmasını zorunlu kılınmaktadır. Veri koruma etki değerlendirmesi yapma zorunluluğu, gerçek kişilerin verilerinin korunmasında başlangıçtan itibaren veri koruması ve tasarımdan itibaren veri koruması gibi ilkelere yer verilmesi gibi hususlara tüzükte yer verilmiş ancak kanunda yer almamaktadır. Veri taşınabilirliği hakkı yani verinin bir kontrolörden başka kontrolöre taşınması hakkı veri sahibine tanınmış bir hak olarak tüzükte düzenlenmiştir. Kanunda böyle bir hususa yer verilmemiştir.

Kanun kapsamındaki birçok maddeye ve hususa temel ilkeler kısmında yer verdiğimiz için ayrıca ayrıntılı açıklama yapmayarak çalışmamıza devam ediyoruz.

C. İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCADELE EDİLMESİ HAKKINDA KANUN (5651 SAYILI KANUN)

5651 Sayılı Kanun[323] özellikle 2020 yılında yapılan değişikliklerle sosyal medya kanunu adıyla da anılmaktadır. Kanun kapsamında sosyal medya süjeleri ve yükümlülüklerini kısaca açıklayacağız. Kanun internetteki yayınlarda oluşan kişilik hakları ihlallerini esas almaktadır. Kişilik hakkı ihlal edilen kişiler erişimin engellenmesi gibi birçok tedbir talep edebilmektedir. Ayrıca bu yasa ile unutulma hakkı konusunda yasal düzenleme yapılmasına yasal dayanak oluşmuştur. Türkiye'den günlük erişimi 1 milyondan fazla olan yurtdışı kaynaklı sosyal medya sağlayıcılarına Türkiye'de temsilci bulundurma zorunluluğu getirilmiştir. Ayrıca sosyal ağ sağlayıcılarına, Bilgi ve Teknolojileri ve İletişim Kurumuna (BTK) başvuru yolları ve usulleri düzenlenmiştir[324]. Sosyal medya sağlayıcıların merkezleri genellikle yurtdışındadır. Bu durum resmi kurumların taleplerinin ulaştırılması ve yargısal kararların yerine getirilmesi açısından önemli sorunlara yol açmaktaydı. Bu soruna son değişikliklerle çözüm getirilmeye çalışılmıştır. Sosyal medya sağlayıcılarına getirilen yükümlülüklerine uyulması ve taleplerin merkeze ulaştırılması konusunda muhatap oluşturma amaçlanmıştır.

1. Sosyal Medya Ağ (Site) Sahipliği Ve Yükümlülükleri

Sosyal medya (ağ) site sahiplikleri genel olarak sosyal etkileşim amacıyla kullanıcılar tarafından oluşturulan, paylaşılan ve/veya sair yollarla sağlanan dijital içeriğe, bunlar üzerinde herhangi bir editör faaliyetinde bulunmaksızın yer veren; bunları değiştirmeksizin bireysel ve/veya toplu iletişime açan ve kullanıcılara bu

[323] https://mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf (E.T:22/01/2022).
[324] Öztürk, Altınok Çalışkan, Seyhan, ss. 49-50.

şekilde sağladığı sosyal etkileşim imkanını internet üzerinden gerçekleştiren ticari amaçlı internet süjeleridir[325].

Akkurt sosyal medya ağ sahipleri şeklinde ifade etmiştir ancak sosyal medya, sosyal ağları da içine alan daha geniş bir kavramdır. *"Çevrimiçi sosyal ağlar kavramı sosyal medya ile aynı anlama gelmemektedir. Facebook ve Twitter gibi sosyal ağlar sosyal medyanın sadece bir parçasını oluşturmaktadır. Sosyal medya, sosyal ağlara ek olarak blogları, fotoğraf ve video platformlarını, forum ve derecelendirme platformlarını ve açık kaynak platformlarını da içermektedir[326]."* Çalışmamız kapsamında sosyal ağ ya da sosyal medya tabiri ayrım yapılmadan instagram, twitter ve facebook için kullanılacaktır.

Hukuki ve idari anlamda internet konusundaki temel düzenlemelerin 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[327] ile yapıldığı görülmektedir. Özellikle bu kanunda 7253 sayılı kanunla[328] yapılan 29/07/2020 tarihli değişiklikle sosyal medya site sahipleri hakkında hukuki bir tanım yapılmış ve site sahiplerine bazı idari yükümlülükler ve sorumluluklar getirilmiştir.

Sosyal medya ağları sahipleri genellikle tüzel kişiliğe sahip şirketlerdir. Bu platformlarda işlenen suçlarda suçun faili olan gerçek kişiler cezalandırılsa bile tek başına sosyal medya platformundaki suç unsurlarını ortadan kaldırmamaktadır. Bu suç konusu içerik ve unsurların kaldırılması konusunda sosyal medya ağları ile onların yasal yükümlülükleri konusunda kanuni düzenlemeler yapılması gerekmiştir. Uygulamada mahkeme kararlarının dahi merkezleri yurtdışında olan sosyal medya platformlarında muhatap ortaya konulamadığı ve kararların uygulanmasında sorunlar

---

[325] Akkurt, s. 132-133.

[326] Bülent Kent, "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu", **Bilişim Hukuk Dergisi**, Cilt:2, Sayı:1, 2020, s. 5.

[327] https://mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf (E.T:18/09/2021)

[328] Söz konusu kanun değişikliğine ilişkin yasa medyada yeni sosyal medya kanunu olarak ifade edilmiştir. Bu kanun değişikliğinde Alman Ağ Yaptırım Yasası (NetzDG) model alınmıştır. Akkurt, s. 179-180;https://detr.abcdef.wiki/wiki/Netzwerkdurchsetzungsgesetz#Soziale_Netzwerke (E.T:18/09/2021); Almanya da sosyal medya aracılığı ile nefret söylemleri içeren suçların işlendiği oldukça yaygın görülmektedir. *"Nefret söylemleri içeren verileri ve diğer sair suçlara ilişkin içeriklerden Youtube %90'ını, Facebook %39'unu, Twitter ise sadece %1'ini sildiği bilgisi ile yola çıkıldığında ne kadar çok korumasız bir yapılanmanın olduğu görülür";* Murat Volkan Dülger, Mustafa Temmuz Oğlakçıoğlu, "Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanuna İlişkin Değerlendirme", **Ceza Hukuku Dergisi**, Sayı:37, Ağustos 2018, s.88; İlgili Kanunun Çevirisine ulaşım için bkz. Sena Kontoğlu, "Alman Sosyal Ağ Kanunu," **Türkiye Adalet Akademisi Küresel Bakış Çeviri Hukuk Dergisi**, Cilt: 8, Sayı:24 Haziran 2018, ss. 143-150.

çıktığı görülmektedir ve kullanıcıların geri dönülemez şekilde haklarının ihlal edilmektedir. 5651 sayılı kanunla birtakım düzenlemeler yapılmış olsa dahi özellikle sosyal medya olarak adlandırdığımız mecrada daha ayrıntılı düzenlemelerin olması gerektiği için 7253 sayılı kanunla sosyal ağ sahipliği kavramının tanımlanması ve özellikle ek m. 4 ile idari yaptırım ve tedbirler düzenlenmiştir. Devletlerin temel hak ve özgürlükleri korumadaki pozitif yükümlülüğünü yerine getirmesi gerekirken sosyal ağ platformları kişilik hakları ve özel hayatın gizliliği korunması zorlaşmaktadır[329].

Öncelikle 5651 sayılı kanunun özel ceza kanunu değildir. Ancak bu kanunla düzenlenen tedbirler bazı suç tipleri ile ilgilidir. Ayrıca da bu kanunda yapılan tanımlar ve açıklamalar ceza sorumluluğunun belirlenmesi gibi hususlarda yardımcı kaynak niteliğinde kabul edilebilir. Kısaca söz konusu 5651 sayılı kanuna "internet kabahatleri yasası" denilebilir[330].

Kanunun 2. maddesi s fıkrasında sosyal ağ sağlayıcıları *"Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişiler"* olarak tanımlanmaktadır.

Yargıtay sosyal ağ sağlayıcılar ile yapılan işlemin internet üzerinden bir yayın olduğunun tespitini yapmaktadır. Facebook üzerinden yapılan kişilik ihlaline yönelik erişimin engellenmesi talebinin sulh ceza hakimliğince reddi üzerine kanun yararına bozma talebi ile Yargıtay'ın önüne gelen olayda Yargıtay şu açıklamaları yapmıştır: Sosyal ağlarda kullanıcılar tarafından yapılan paylaşımlara somut olayda erişim sağlayan sayısının belirsiz sayıda kişi olarak kabulü gerekir. Bu sebeple internet kullanıcılarının ve de sosyal medya kullanıcılarının bu hesapları üzerinden yaptıkları paylaşımlar "internet üzerinden yapılan yayın" olarak kabul edilmelidir[331].

Söz konusu tanımlar sosyal medya konusunda önemli tanımlardır. Ancak konumuz kapsamına çok çıkmadan kısaca açıklanması gereken hususlardır. Paylaşılan içeriklerde hakları ihlal edilen kişilerin muhataplarını belirlenmesi, cezai

---

[329] https://www2.tbmm.gov.tr/d27/2/2-3050.pdf (E.T:19/09/2021).
[330] Kayıhan İçel ve Yener Ünver, **Kitle İletişim Hukuku (Basın-Radyo-Televizyon-Sinema-Video-İnternet)**, Yeniden İncelenmiş 9. Baskı, Beta Yayıncılık, İstanbul 2012, s.447.
[331] Yargıtay 9. CD 2020/6817 E. 2021/1704 K. 17/01/2021 T.
https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:16/01/2021).

ve hukuki sorumlukların kapsamını tespit edebilmesi adına gereklidir. Bu sebeple hukuki ve idari boyutuna ilişkin açıklamalara yer vereceğiz.

a. Sosyal Medya (Ağ) Site Sahipliği Hukuki Niteliği

Sosyal medya kullanıcıların olduğu kadar sosyal medya ağ sahiplerinin de içerik ürettiği bir platformdur. Bu durumda sosyal medya ağ sahiplerinin bizzat kendisinin içerik ürettiği durumdaki sorumluluğu ile kullanıcının içerik ürettiği durumdaki sorumluluğu ve yükümlülüğü faklı olacaktır. Sosyal medya ağ sahiplikleri kullanıcı tarafından oluşturulan içerikler bakımından yer sağlayıcı olarak kabul edilecekken bizzat oluşturdukları içeriklerde içerik sağlayıcı olarak değerlendirilecektir[332]. 7253 sayılı kanun öncesi hukuki durum bu şekilde değerlendirilmekteydi. Ancak yeni düzenleme ile bu sorumluluk ve yükümlülüklere ek olarak sosyal ağ sağlayıcısı sıfatı ile yapılan düzenlemeye de tabi olduğu ek m. 4/9 da açıkça ifade edilmiştir.

Kanunun 2. maddesi f ve m fıkrasında içerik sağlayıcı internette bilgi ve içerik üreten, değiştiren ya da sağlayan; yer sağlayıcı ise bu içeriklerin yer aldığı sistemleri sağlayan ya da işletenler olarak tanımlanmaktadır. Hem içerik sağlayıcı hem de yer sağlayıcı gerçek ya da tüzel kişi olabilecektir.

Kanuna göre web sitelerini kendi sunucularında barındıran yer sağlayıcıların ticari faaliyet gütmeseler dahi Faaliyet Belgesi almak zorundadırlar. Kamu kurumları ve üniversitelerin de yer sağlayıcı olduğu kabul edilmektedir[333].

Sosyal medya içerikleri kullanıcılar tarafından oluşturulmaktadır. İnternet içerikleri barındıran sistemleri sağlayan ve/veya işletenler internet yer sağlayıcısıdır. Daha ayrıntılı açıklamak gerekirse içerikleri kendisinin ya da başkasının bilgisayarında, bulut bilişim sistemlerinde[334] ya da veri tabanlarında depolayan ancak çoğunlukla kendisinin işlettiği sair yazılım ara yüz ve/veya internet siteleri

[332] Akkurt, s. 133.
[333] Kaya, s. 224.
[334] Bulut Bilişim (Cloud Computing): 2000'li yıllarda gündeme gelen özellikle kurumsal çözümler için kullanılan büyük veri ve bilgi teknolojisidir. Çeşitli bilişim kaynakları ile ortak havuza erişim sağlayabilmektedir. Birçok kurum modeli bulunmaktadır; Turan, s. 288.

marifetiyle yayınlayan internet süjeleridir[335]. Sosyal medya mecralarının bu yer sağlayıcı kapsamında değerlendirilemeyeceği yönünde görüşler olsa da hukukumuzda Yargıtay Kararları[336] dikkate alındığında sosyal medya platformlarının yer sağlayıcı olarak değerlendirilmesi gerektiği görülmektedir[337].

Kanunda içerik sağlayıcının yükümlülükleri 4. maddede düzenlemiştir. Düzenlemede içerik sağlayıcıların internet kullanımına sunduğu her içerikten sorumlu olduğu ancak bağlantı sağladığı başkasına ait bir içerik söz konusu olduğunda sorumluluğunun gerçekten içeriğin benimsenip benimsenmediğinin tespiti yapılarak değerlendirilme gerekir. Bu noktada içerik sağlayıcının veriyi paylaşırken onu açıkça benimsediği ve benimsemiş olduğu için yaymaya çalıştığının görülür olması halinde sorumluluk doğacaktır. İçerik sağlayıcının sorumluluğu bu durumda genel hükümlere göre olacaktır. İçel ve Ünver'e göre buradaki başkasına ait içerikten sorumluluk husus yasal karine amacıyla düzenlenmemiştir. Yalnızca yardımcı norm niteliğine sahiptir. Cezai sorumluluğu gerektiren durumlarda hakim iştirak hükümlerine göre ayrı bir değerlendirme yapabilmesine engel değildir. Yer sağlayıcı konusunda kanundaki düzenleme yer sağlayıcıların yer sağladığı içerikleri kontrol etme veya hukuka aykırı içerikleri tespit etme gibi bir yükümlülüğe sahip olamadıkları şeklindedir. Yer sağlayıcılar bu şekilde doğrudan ceza hukukuna ilişkin sorumlulukla karşı karşıya kalmayacaktır. Bu düzenlemeye rağmen özellikle içerik sağlayıcı ile yer sağlayıcısının iştirak halinde olduğu anlaşılması halinde cezai sorumluluklarının doğması mümkündür. Ayrıca 5. maddenin 2. fıkrasında yer sağlayıcının hukuka aykırı içerikten haberdar edilmesi hali için yer sağlayıcıya yayını çıkarmak şeklinde bir yükümlülük yüklemiştir. Bu yükümlülük haberdar

---

[335] Yetim, s. 65; Kaya, s. 224.

[336] Yargıtay 12. CD. 2014/2502 E. 2014/17838 K. 15/09/2014; *"...Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğünün İnternet Ortamında işlenen Suçlarda Uluslararası Ceza İstinabe İşlemlerine ilişkin yazısına göre, google, yahoo, facebook, skype, hotmail, twitter, youtube gibi internet ortamında yaygın olarak kullanılan yer sağlayıcı firmaların merkezinin Amerika Birleşik Devletleri'nde bulunduğu.."* Yargıtay 19.CD. 2015/12260 E. 2017/7086 K. 20/09/2017; *"Dolayısıyla sanık, 5651 sayılı Kanun'un 2/m maddesi bağlamında "yer sağlayıcı"; sitede içerik paylaşımı yapan üçüncü kişiler ise aynı Kanun'un 2/f maddesi uyarınca "içerik sağlayıcı" konumundadırlar…"* https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T: 16/01/2022).

[337] Söz konusu değerlendirmeler sosyal medya platformlarının tanımdan farklı olarak sistem (hosting hizmeti verenler) değil de yazılım oldukları ve yazılımların yer sağlayıcı olarak kabul edilemeyeceğinden hareket etmektedir. Ancak sosyal medya yazılımlarının da kullanıcılar tarafından içerik üretilen ve değiştirilen, bu içerikleri barındıran bir sistem kabul edilmektedir. Ayrıntılı bilgi için bkz. Akkurt, ss. 136-138.

edilmenin 8. ve 9. madde hükümlerine göre olması durumunda söz konusudur. Bu yükümlülüğe uymama halinde yer sağlayıcılar 5651 sayılı kanun kapsamında idari para cezaları ile karşı karşıya kalacaktır[338].

Erişim sağlayıcılar başkalarına ait içeriklere ulaşılmasını sağlayan aracılardır. Bu sebeple kendilerinin doğrudan cezai sorumluluğa sahip olmaması internet özgürlüğü açısından gerekli bir durumdur. Erişim sağlayıcıların aracı olması ile ifade edilmek istenen bir köprü olmasıdır ki köprüden geçen her bilgi ve verinin suç içerip içermediğinin erişim sağlayıcı tarafından kontrol edilmesi olanaklı değildir[339].

5651 sayılı kanun kapsamında da erişim sağlayıcılarına hukuka uygunluk kontörlü yapma şeklinde doğrudan bir yükümlülük yüklenmemiştir. Ancak erişim sağlayıcıya hukuka aykırı içeriklerle ilgili erişimi engelleme kararlarını uygulama yükümlüğü getirilmiştir. Ayrıca erişim sağlayıcıları cezai sorumluluklarının oluşması pek muhtemel olmadığı için 5651 sayılı kanunla idari tedbirler ve idari para cezaları getirilmiştir. Bunların fazla ağır olması halinde erişim sağlayıcıların internet aracıları olduğu ve internetin gelişimi için kendilerine ihtiyaç olduğu unutulmamalıdır[340].

b. Sosyal Medya Ağ Site Sahipliği Hukuki Niteliği Yer Sağlayıcı Sıfatıyla Tabi Olduğu Özel Yükümlülükler

İlk yükümlülük hukuka uygunluk ön denetimidir. (Sosyal medya) Yer sağlayıcılarının hukuka uygunluk denetimi yapma gibi bir yükümlülükleri yoktur. Pratikte de sitelerin içerikleri tek tek bir ön denetimden geçirerek sisteme yüklemeleri mümkün değildir. Yargıtay kararlarında da yer sağlayıcıların hukuka uygunluk ön denetimi yapma gibi bir yükümlülüklerinin kural olarak olmadığı görüşündendir[341].

İlgili kararda Yargıtay ilk derece mahkemesinin gerekçesini uygun bulmuş ve kararı onamıştır[342]. İlk derece mahkemesi, somut olayda davalının işlettiği sitenin

[338] İçel ve Ünver, s. 448.
[339] Hasan Sınar, "İnternetin Ortaya Çıkardığı Sorunlara Bir Ceza Hukuku Yaklaşımı" **MHB**, Yılmaz Altuğ'a Armağan, Cilt:17, Sayı:1-2, (İnternet), s. 366.
[340] İçel ve Ünver, ss. 448-449.
[341] Akkurt, s. 140.
[342] Yargıtay 11. HD. 2014/6453 E. 2014/12510 K. 30/06/2014 T. https://kararara ma.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:05/10/2021).

video paylaşımını, izlenmesini sağlayan bir site olduğunu ve site içeriklerinin kullanıcılar tarafından oluşturulduğunu belirtmektedir. Ayrıca mahkemeye göre siteye binlerce kullanıcı aynı anda video yüklemesi yapabilmektedir ki böyle bir durumda davalının kullanıcılar tarafından yüklenen her içeriğin kontrolünü yapması mümkün değildir.

5156 sayılı Kanun m.5/1'de de açıkça yer sağlayıcının içerikleri kontrol etme yükümlülüğünün olmadığı belirtilmektedir.

İkinci yükümlülük içeriğin yer sağlayıcı tarafından yayından çıkarılması yükümlülüğüdür ki buna uyarı yöntemi adı verilmektedir. İçeriğin yer sağlayıcı tarafından yayından çıkarılması yükümlülüğü m. 2/1-r bendi uyarınca bulunmaktadır. Bu işlem uyarı yöntemi ile gerçekleşir. Bahsedildiği üzere yer sağlayıcısının hukuka uygunluk ön denetimi yapma yükümlülüğü yoktur ancak bir kişilik hakkı ihlali gerçekleştirildiğinde bunun uyarı yöntemi ile kendisine bildirilmesi halinde içeriği çıkartma yükümlülüğü doğacaktır. Madde metninde uyarı yöntemi kişilerin haklarının ihlal edildiğini düşündüklerinde içeriğin kaldırılması için önce içerik sağlayıcısına daha sonra yer sağlayıcısına başvurmalarını içeren bildirim olarak açıklanmaktadır.

Üçüncü yükümlülük içeriğin kamu otoritelerince/erişime engellenmesine katlanma ve gereğini yerine getirme yükümlülüğüdür. Yer sağlayıcıların içeriğin kamu otoritelerince/erişime engellenmesine katlanma ve gereğini yerine getirme yükümlülüğü vardır. Kanunun m.8, 9 ve 9/A maddelerinde bu konuda özel düzenlemeler yapılmıştır.

Dördüncü yükümlülük ise kamuoyuna bildirme (aleniyet) yükümlülüğüdür. Kamuoyuna bildirme (aleniyet) yükümlülüğü kanunun 3. maddesinde belirtilmektedir. Maddenin 1. fıkrasında her üç sağlayıcı için de kullanıcıların kendilerine ulaşması için internet sayfalarında gerekli iletişim bilgileri bulundurması zorunluluğu vardır. Bu bilgilerin doğru ve güncel olması gerekir.

Beşinci yükümlülük trafik bilgilerini saklama ve gizlilik yükümlülüğüdür. Trafik bilgilerini saklama ve gizlilik yükümlülüğü özellikle cezai soruşturmalarda kritik nitelik taşıyan delil ve kişilere ulaşmada önem göstermektedir. Kanunun m.2/1-j bendinde trafik bilgisi *"Taraflara ilişkin IP adresi, port bilgisi, verilen*

hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini" olarak tanımlanmaktadır.

Altıncısı ise Anayasa Mahkemesince iptal edilen kamu otoritelerince istenilen bilgileri sağlama ve tedbir alma yükümlülüğüdür. Kamu kurumlarınca istenilen bilgileri sağlama ve tedbir alma yükümlülüğü kanunun 5. maddesi 5. fıkrasında yer almaktaydı. Ancak Anayasa Mahkemesi'nin 2014/87 E. 2015/112 K. ve 08/12/2021 tarihli kararı ile yer sağlayıcının bu yükümlülüğüne ilişkin 5. fıkra iptal edilmiştir. Bu yükümlülüğün fıkranın düzenlenmiş biçimi açısından haberleşmenin ve özel hayatın gizliliğini ihlal edebilecek şekilde olduğu konusunda eleştiriler mevcuttu[343].

c. Sosyal Medya Ağ Site Sahipliği Hukuki Niteliği ve 7253 Sayılı Kanun İle "Sosyal Ağ Sağlayıcı" Sıfatıyla Tabi Olduğu (Ek) Özel Yükümlülükler

İlk yükümlülük Türkiye'de yetkili temsilci belirleme ve kuruma bildirme yükümlülüğüdür**.** Yeni yasal düzenleme ile benzerlik gösteren (model düzenleme olarak gösterilen) Alman Sosyal Ağ Kanunu toplam 6 maddeden oluşmaktadır. Kanunun 5. maddesinde iki ayrı yetkili atanması hususu düzenlenmiştir. İlk atanacak temsilci "yetkili alıcı"dır. Bu temsilci adli ve idari kurum ve makamlarda sosyal ağ sağlayıcının resmi temsilcisi olacak kişidir. Kendisine şikayetler ve yazışmalar tebliğ edilecek, kendisi kullanıcı taleplerine cevap verecek, mahkeme ve resmi kurumlarda tam yetkili olarak muhatap alınacak kişi olacaktır. İkincisi ise adli makamların soruşturmalarında ve kolluk kuvvetlerinin bu soruşturmalara yönelik taleplerinde istenen bilgileri sağlamakla görevli "irtibat kişisi"dir[344]. Söz konusu düzenlemeler ile sosyal ağ sağlayıcılarının ülkede bir "posta kutusu" oluşturmasını amaçlanmıştır[345].

7253 sayılı kanunla 5651 sayılı kanun ek m. 4'te "Türkiye'den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcı" için bazı yükümlülükler getirmektedir. Bunların başında Türkiye'de bir temsilci atamak gelmektedir. Bu temsilciler, özellikle yurtdışı merkezli olan sosyal medya

[343] Kaya, ss. 219-220, 229; Akkurt, ss. 171-176.
[344] Kent, 12; Akkurt, ss. 189-190.
[345] Kent, s. 39.

şirketlerine ulaşılması ve yapılacak tebligatlar konusunda muhatap sağlanması açısından büyük öneme sahiptir. Söz konusu temsilcinin atanması için Alman Sosyal Ağ Kanunundan farklı olarak günlük erişimi[346] bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcı ifadesine yer verilmiştir. Sonuç olarak yurt dışı kaynaklı olsa bile günlük erişimi bir milyondan az olan ve yurt içi kaynaklı sosyal ağ sağlayıcılar için Türkiye de temsilci atanması zorunluluğu konulmamıştır. Ayrıca atanan temsilcilerin Kuruma bildirilmesi ve sitelerinde bu temsilcilerin bilgilerine yer verilmesi gereklidir.

Çalışmamızın hazırlanması sürecinde Facebook, Twitter, Google ve Youtube gibi büyük platformların temsilci ataması yaptığı görülmüştür. Ayrıca TBMM Dijital Mecralar Komisyonu tarafından Facebook (Meta) ve Youtube platformlarının temsilcileri ile görüşmeler yapılmıştır. Söz konusu görüşmelerin yer aldığı komisyon tutanaklarında temsilcilere milletvekillerince sosyal medya platformlarında yer alan kişisel verilerin korunması konusu başta olmak üzere güncel sorunlar hakkında sorular yöneltildiği görülmektedir[347].

İkinci yükümlülük kişilik hakkını ihlal eden taleplere cevap verme yükümlülüğüdür. Ek madde 4'ün üçüncü fıkrasına göre sosyal ağ sağlayıcıya, Kanunun 9. ve 9/A maddelerinde yer alan konularda yapılacak başvuru en geç 48 saat içinde cevaplandırılmalıdır. İlgili başvurulara olumlu ya da olumsuz bir cevap verilmelidir. Cevabın olumsuz olması durumunda ise gerekçeli şekilde cevap sunulmalıdır. Kanunun 9. maddesinde kişilik hakkı ihlalinde uyarı yöntemi ile önce içerik sağlayıcısına ondan cevap alınamaması veya ulaşılamaması halinde ise yer sağlayıcısına başvurulabileceği bu şekilde içeriğin yayından çıkarılmasını sağlanabileceği düzenlenmiştir. Ayrıca buna alternatif olarak kişilerin doğrudan sulh ceza hakimliklerine başvurup içeriğin çıkartılmasını/engellenmesini isteyebileceği düzenlenmiştir. Kanunun 9/A maddesinde ise özel hayatın gizliliği sebebi ile içeriğe

[346] Günlük Erişim sayısının tespitine ilişkin açıklamalar için bkz. Akkurt s. 191.

[347] 02/12/2021 Tarihli TBMM Dijital Mecralar Komisyonu Tutanağı: Söz konusu toplantıya Google ve Youtube Türkiye temsilcileri katılmıştır.
https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=2890
(E.T:23/12/2021).
04/11/2021 Tarihli TBMM Dijital Mecralar Komisyonu Tutanağı: Söz konusu toplantıya yeni adı ile Meta (Facebook, İnstagram ve WhatsApp) Türkiye temsilcisi katılmıştır. https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=2849
(E.T:23/12/2021).

erişimin engellenmesi düzenlenmiştir. Bu durumda kişiler doğrudan Bilgi Teknolojileri ve İletişim Kurumuna (BTK) başvurarak erişimin engellenmesini talep etmektedir. Kurum başkanı kendisine gelen talebi Erişim Sağlayıcıları Birliğine bildirir. Yapılan istekte özellikle URL yani yayının tam adresi verilmesi temel hak ve özgürlükler açısından önem arz etmektedir.

Getirilen üçüncü yükümlülük içeriğin çıkarılmasına veya erişimin engellenmesine ilişkin başvurular ve ilgili kararın uygulanması hakkında rapor verme yükümlülüğüdür. Rapor yükümlülüğü ek m. 4'ün 4. fıkrasında düzenlenmiştir. Sosyal ağ sağlayıcıları altı aylık dönemlerle kendilerine yapılan başvurularla ilgili raporlar hazırlayarak BTK'ye bildirecektir. Maddenin üçüncü fıkrası kapsamındaki başvurular konusunda düzenlenen raporlar BTK'ye gönderildiği gibi ayrıca kişisel verileri içermeyecek şekilde sosyal ağ sağlayıcısının internet sitesinde yayınlayacaktır.

Model alınan düzenleme olarak bahsettiğimiz Alman Sosyal Ağ Kanunda bizdeki BTK'ya bildirmek şeklinde olan yükümlülük bu raporların "Federal Gazete"de yayımlanması olarak düzenlenmiştir. Kanunumuzda yer alan düzenleme bu yönüyle eleştirilmektedir. Yalnızca 3. fıkra kapsamındaki başvurulara ilişkin raporlar sosyal ağ sağlayıcı tarafından halka açıklanacak olması bunun denetimini sağlayacak olan mekanizmanın olmaması önemli bir boşluk oluşturmaktadır. Kamuoyu tarafından idareye sunulan raporlar ile sosyal ağ sağlayıcısı tarafından sitesinde açıklanan veriler arasındaki farklılıklar tespit edilemeyecektir[348]. Ayrıca Alman Federal Gazetesinde yayınladıktan sonra en geç bir ay içinde sosyal ağ sağlayıcıları kendi ana sayfasında raporu hazırlamakla ve yayınlamakla yükümlüdür. Kanuna göre bu rapor kolaylıkla tanınabilir olmalı, hemen ve her zaman erişilebilir olmalıdır. Alman Sosyal Ağ Kanundaki düzenleme de raporların içeriği konusunu da ayrıntılı bir şekilde düzenlenmiştir. Bu kanunun 2. maddesinde raporda asgari olarak ele alınması gereken konular açıklanmıştır. Raporlama ile amaçlanan yasadışı içeriklerin daha çok hangi yöntemlerle kaldırıldığı, daha çok hangi tür şikayetlerin yapıldığı ve bunların nasıl sonuçlandırıldığının açıklanarak daha şeffaf bir sonuç elde etmektir[349].

[348] Akkurt, s. 119.
[349] Dülger ve Oğlakcıoğlu, s. 102.

İnstagram, Ocak 2022 tarihli "5651 sayılı Kanun Kapsamındaki Kullanıcı Taleplerine İlişkin Şeffaflık Raporu'nda 1 Temmuz ile 31 Aralık arasında 3695 adet raporlama olduğunu bildirmektedir. Şeffaflık Raporunda bu başvurulardan 2334'ünün tekrar raporlama olduğundan geriye kalan 1361 başvurunun incelendiğini ve bu başvurulardan 854'ünün de sadece instagram profilinin tamamını bildirmek şeklinde olduğunu ifade edilmektedir. İncelemeler sonucunda başvurular arasından 252'sinde ihlal olduğu tespit edilmiştir[350].

Dördüncü yükümlülük Türkiye'deki kullanıcılarının verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alma yükümlülüğüdür. Ek madde 4'ün 5. fıkrasında sosyal ağ sağlayıcılarını Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri almakla yükümlü kılınmıştır. Ancak kanunda yukarıda sayılan tedbirlerin yerine getirilememesi halinde yaptırımları sayılmışken bu fıkra uyarınca gerekli yükümlülük yerine getirilmediğinde hangi yaptırımın uygulanacağı düzenlenmemiştir. Bu fıkranın gerekçesi de ortaya konulmamıştır. Büyük sosyal medya şirketlerinin merkezleri yurtdışında olduğu için kullanıcı verilerini de yurt dışındaki sunucularında tuttukları bilinmektedir. Metinde de Türkiye'de barındırılması gerektiği değil de barındırılması yönünde gerekli tedbirlerin alınması şeklinde ifade kullanılmıştır. Alman Sosyal Ağ Kanununda benzer şekilde düzenleme bulunmamaktadır[351].

Son yükümlülük ise hukuka aykırılığı mahkeme kararıyla tespit edilen içeriğin çıkarılması veya erişime engellenmesi yükümlülüğüdür. Kanunda ek m.4/8'de hukuka aykırı olduğu mahkeme kararı ile tespit edilen içeriklerin sosyal ağ sağlayıcısına bildirilmesi ile doğan yükümlülüğünden bahsedilmektedir. Maddeye göre sosyal ağ sağlayıcısı, hukuka aykırılığı bir yargısal makam tarafından tespit edilmiş içeriği çıkarmak ya da içeriğe erişimi engellenmekle yükümlüdür. Bu kararları uygulamak verilen süre ise kendisine yapılan bildirimden itibaren 24 saattir. Kararının uygulanması halinde doğan zararlardan sosyal ağ sağlayıcısı sorumlu olacaktır.

[350] İnstagram sayfasında 2021 yılına ait Mart-Haziran 2021, Haziran 2021, ve Temmuz-Aralık 2021 olmak üzere üç adet şeffaflık raporuna Türkçe ve İngilizce olarak yer verilmektedir. Bkz. https://help.instagram.com/842275446492500/?helpref=related_articles (E.T:19/01/2022).
[351] Akkurt, ss. 200-201.

Hukuka aykırı ifadesi Alman Sosyal Ağlar Kanunda Alman Ceza Kanununa atıf yapılarak belli suç tipleri ile ilişkilendirilmiştir. Ancak bizim kanun metnimizde bir açıklık bulunmamaktadır. Bu sebeple mahkemeler tarafından özellikle suç veya kişilik hakkı ihlali olarak tespit edilen içerikler hukuka aykırı içerikler olacaktır. Örneğin m.8, m.8/A, m.9, m.9/A içeriklerinde sayılan suç kategorilerine bakıldığında ek m.4'te bahsedilen hukuka aykırılıklar da bu suç tipleri ile ilgili içerikler olduğu düşünülmelidir. Fıkranın son cümlesiyle sosyal ağ sağlayıcısının sorumluluğuna gitmeden önce belli bir usul getirilmemiş hatta doğrudan sosyal ağ sağlayıcısına başvuru için bir şart aranmadığı hükmü getirilmiştir. Bununla anlaşılması gereken sosyal ağ sağlayıcısının sorumluluğunun kusursuz sorumluluk olduğudur[352].

Yaman Akdeniz ve diğerleri kararında AYM tarafından twitter.com adlı sosyal medya sitesine erişimin tamamen engellenmesi hali için ihlal kararı verilmiştir. Somut olayda belli URL adreslerine yönelik erişimin engellenmesi kararı mahkemece alınmışken sosyal medya sitesi bütünüyle erişime kapatılmıştır. AYM ilgili kararda bu şekilde erişimi engellemenin kanunda yasal dayanağının olmadığını, sosyal medya sitesini kullanan tüm kullanıcıların ifade özgürlüğünü kısıtlayıcı nitelikte olduğunu belirtmiştir. [353].

Hukuka aykırı bir içerik söz konusu olduğuna erişim sağlayıcı, yer sağlayıcı ya da içerik sağlayıcının yurtdışı merkezli olması onlara ulaşılmasını oldukça zorlaştırmaktadır. AYM kararlarına esas olan twitter, youtube ve wikipedia erişimi engelleme gerçekleştiği tarihlerde URL engellemenin zor olduğu söylenebilir. Büyük sosyal medya şirketlerinin Türkiye'de temsilci bulundurmaması ve ulaşım zorluğu bu durumun ortaya çıkmasında önemli bir etken olmuştur. AYM bu kararlarında demokratik toplum düzeninin gereği kriterini dikkate almıştır[354].

Erişimin engellenmesi kararının sitenin bütününe yönelik alınması için gerçekten zorunluluk arz eden bir durumun oluşması gerekmektedir. Yani gerçekleşen bir ihlalin önüne başka türlü geçme olanağının olmaması gerekmektedir.

---

[352] Akkurt, s. 202.

[353] Yaman Akdeniz ve diğerleri, Bireysel Başvuru No: 2014/3986, 02/04/2014; https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/3986?KelimeAra%5B%5D=yaman+akdeniz&BasvuruAdi=YAMAN+AKDEN%C4%B0Z+VE+D%C4%B0%C4%9EERLER%C4%B0 (E.T:05/10/2021).

[354]Hayrettin Kurt, "Erişim Engellemeden Demokratik Toplum Ya Da Kamu Düzenine Eleştirel Bir Bakış", **Adalet Dergisi**, Sayı: 67, 2021/2, s. 158.

Bu şekilde sitenin bütününe yönelik bir erişimin engellenmesi kararının verilmesi durumda mahkemelerce başka bir olanak bulunmadığı hususunu gerekçelendirmesi zorunludur. Hakim, URL adresi belirtilerek içeriğe erişimin engellenmesi ile ihlalin engellenemeyeceği şeklinde bir düşünce olabilir. Bu durumda gerekçesini de belirterek internet sitesinin tümüne yönelik erişimin engellenmesine karar vermesi de mümkündür. 5651 sayılı kanunun 9. maddesindeki hüküm, temel hak ve özgürlüklerin sınırlandırılmasındaki temel argümanımız olan ölçülülük ilkesinin sonucudur[355].

2.Sosyal Medya Kullanıcısı ve Yükümlülükleri

a. Sosyal Medya Kullanıcısının Hukuki Niteliği: İçerik Sağlayıcı Kavramı

Sosyal medya kullanıcısının içerik sağlayıcı konumunda olduğu durumlar vardır. Bu durum aslında tez konumuzun da temeldir. İçerik kavramının neyi ifade ettiğinin tespiti için 5651 sayılı kanunda bulunan tanımlara bakmamız gerekir.

Veri ile bilgi aynı anlama sahip değildir. Veri aslında bir hammaddedir yani bilgi için bir kaynaktır. Bilgi ise toplanan, anlamlı bir şekilde işlenen verilerdir[356]. Uygulamada eş anlamlı gibi kullanıldığı çokça görülmektedir. "*İçerik sağlayıcı, kendisine ait olsun olmasın her türlü bilgiyi ve veriyi üreterek, mevcut olanları değiştirerek veya analog olanları elverişli hale getirerek (sayısallaştırarak-dijitalleştirerek) internet üzerinden başkalarının erişimine sunan(sağlayan) gerçek veya tüzel kişiler olarak tanımlanabilir[357].*"

Sosyal medya kullanıcıların hukuki ve teknik anlamada bir içeriği üretmesi ya da değiştirmesi bu içerikleri sağlayan kişi konumunda olmalarından dolayı kendileri mevzuat kapsamında içerik sağlayıcı olarak kabulünü gerektirmektedir. Yargıtay'ın görüşünün de bu yönde olduğu söylenebilecektir. Yargıtay bu kararlarında siteye

[355]Aka, ss. 261-262.
[356] Turan, ss. 279-280.
[357] Akkurt, ss. 233-234.

içerik yükleyen kullanıcıları 5651 sayılı kanun m. 2/1-f uyarınca içerik sağlayıcı olduğunu ifade etmektedir. [358].

İçerik sağlayıcı olan sosyal medya kullanıcısının kendi fotoğrafının paylaşması ya da başka paylaşımların altına özgün yorum yapması kendisinin veri üretmesi anlamına gelecektir. İçerikteki bir fotoğrafın etiketlenmesi ya da yeni bir yorum eklenmesi yani ana veriyi tadil etmesi halinde buna da bilginin değiştirilmesi denilmektedir. Ayrıca bilginin yani verinin sağlanması durumu vardır. Bu da kullanıcının kendisi tarafından üretilmeyen bir veriyi başkaları ile paylaşmasıdır. Örneğin bir alıntının fotoğrafını ya da bağlantısını doğrudan ya da bir paylaşımla birlikte diğer kullanıcılara sunması şeklinde olabilecektir. Facebook, twitter ve instagram kullanıcıları sosyal medyada gerçekleştirdikleri faaliyetler açısından içerik sağlayıcı olarak kabul edilecektir[359].

İçerik sağlayıcının meydana getirebileceği olası ihlalleri şu konulardadır:

- Şeref ve Haysiyete İlişkin İhlaller,
- Özel Hayatı Gizliliğine İlişkin İhlaller,
- Ad, Resim, Haberleşmenin Gizliliğine İlişkin İhlaller,
- Sosyal Medya Kullanmayan Üçüncü Kişilerin Kişilik Haklarının İçerik Sağlayıcı Tarafından İhlali,
- Sosyal Medyada Anne ve Babalar Tarafından Çocuklarının Kişilik Haklarının İhlali,
- Sosyal Medya Hesabı Sahibinin Ölümünden Sonraki Akıbeti ve Bu Çerçevede Gerçekleşebilecek İhlaller.

Bahsettiğimiz kişilik hakkı ihlallerinin ceza hukuk açısından da değerlendirilmesi gerekir. Her ihlalin ceza hukuku açısından oluşturabileceği suç tipleri üzerinde son kısımda durulacaktır.

b. İçerik Sağlayıcının Özel Yükümlülükleri

[358] Yargıtay 19 CD. 2015/12260 E. 2017/7086 K. 20/09/2017 T. Yargıtay 4. HD. 2016/6124 E. 2017/8370 K. 18/12/2017 T. *"5651 sayılı Kanunda belirtilen şekilde Facebook sosyal paylaşım sitesinde "facebook.com/..." isimli sayfanın içerik sağlayıcısının kim olduğu tespit edilerek varılacak sonuca göre bir karar verilmesi."*https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T 15/06/2022).

[359] Akkurt, s. 237; Kaya, s. 235.

İlk yükümlülük hukuka uygunluk denetimidir. Kanunda açıkça içerik sağlayıcının internete sunduğu her türlü içerikten sorumlu olacağına işaret etmiştir. Metinde açıkça hukuka uygunluk denetiminden bahsedilmese de içerik sağlayıcının yani sosyal medya özelinde kullanıcının hukuka aykırılık olması durumunda sorumlu olacağı da anlaşılmaktadır. Bu durumda sosyal medya kullanıcısının paylaştığı içerikleri henüz paylaşmadan bir öz denetime ve filtrelemeye tabi tutması gerektir. Ayrıca bazı yazarların görüşlerine[360] göre bu denetimi sadece paylaşım yapılmadan önceye aittir demek de hatalı olacaktır. İçeriği paylaştıktan sonra da bu denetim devam etmelidir. İçerik sağlayıcı için 5651 sayılı Kanunun m. 4/2 düzenlemesinde bağlantı paylaşılması konusunda açıklama yapılmaktadır. Düzenlemede içerik sağlayıcı olarak bağlantı sağlanılması halinde başkasına ait içerikten sorumlu olunmayacağı ancak, daha önce de bahsettiğimiz üzere sunuş biçimi değerlendirilerek içerik sağlayıcının açıkça benimsediği görülmesi halinde sorumluluğu genel hükümlere göre olacaktır. Kanunun bu anlatımından kişinin sosyal medyada başka bir kullanıcıya ait içeriği bağlantıyı kendisinin de onayladığını belirtecek şekilde bir yorumla paylaşması halinde kullanıcının genel hükümlere göre sorumluluğunun doğacağı anlaşılmaktadır. Genel hükümlere göre sorumluluk ifadesinden suç teşkil eden içerikler için TCK, kişilik hakkı ihlalleri için TMK, haksız fiil olması durumunda TBK hükümlerinin uygulanacağı düşünülmektedir[361].

İkinci yükümlülük içeriğin içerik sağlayıcı tarafından yayından çıkarılması yükümlülüğüdür. 5651 sayılı kanunun 9. maddesinin başlığı 06/02/2014 tarihli 6518 sayılı kanunla yapılan son düzenlemeye göre içeriğin yayından çıkarılması ve erişimin engellenmesidir. Ancak daha önce düzelteme ve cevap hakkını içeren bir anlayışla içeriğin yayından çıkarılması ve cevap hakkı başlığı değiştirilerek son düzenleme ile cevap hakkının göz ardı edildiği düşünülmektedir. Maddede içerik sağlayıcısına sonra yer sağlayıcısına ve/veya sulh ceza hakimliğine başvuru seçenekleri ve usulü anlatılmıştır. İçeriğin yayından çıkarılması her birinden de istenebilecekken erişimin engellenmesi sulh ceza hakiminden istenebilecektir. Bu

[360] Akkurt, s. 240.
[361] Akkurt, s. 241.

seçenekler yerinde doğrudan genel hükümler dairesindeki mekanizmaların işletilmesi de mümkündür.

Üçüncü yükümlülük ise içeriğin kamu otoritelerince çıkarılmasına/erişime engellenmesine katlanma ve gereğini yerine getirme yükümlülüğüdür. 5651 sayılı kanunun kapsamında verilen hakim, mahkeme kararları ve başkan tarafından verilen kararlar içerik sağlayıcısı tarafından uygulanmak zorundadır. İçerik sağlayıcısı m.8/A kapsamında verilen kararı derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirmesi gerekmektedir. Söz konusu zorunluluk icrai yani aktif bir yönü bulunmaktadır. Ancak bunun ihlali halinde doğacak cezai bir sorumluluğuna ilişkin hüküm de bulunmamaktadır. Yargıtay 19. Ceza Dairesinin bu konuda verdiği bir kararında suçta ve ceza da kanunilik ilkesinin altı çizilerek içerik sağlayıcının beraatine karar vermiştir[362].

Dördüncü olarak sayacağımız yükümlülük kamuoyuna bildirme (aleniyet) yükümlülüğüdür. 5651 sayılı kanunun 3. maddesinde bilgilendirme yükümlülüğü düzenlenmiştir. Kanun koyucu her üç sağlayıcıyı da kendilerini tanıtan ve iletişim için gereken bilgilerini bizzat kendilerine ait internet sitesinde tutmakla yükümlü kılmıştır. Bu bilgiler doğru ve güncel olmalı, kullanıcıların ulaşabileceği şekilde tutulmalıdır. Yükümlülüğü yerine getirmeyen sağlayıcılar açısında idari para cezası öngörülmüştür. Söz konusu yükümlülüğün ticari amaç gütmeden sosyal medyayı kullanan kullanıcıları kapsayacağını düşünmek çok mümkün değildir. Herhangi bir sosyal medya kullanıcısının adres ve telefon numarası gibi kişisel bilgilerinin alenen ifşa etmesi mümkün değildir. Kanun maddesinin amacının da bu kullanıcılar için olmadığı sonucuna ulaşılmaktadır[363].

Kamuoyunu bilgilendirme yükümlülüğüne ilişkin 3. madde de yönetmelikle belirlenen usul ve esaslar çerçevesinde tanıtıcı bilgilerin düzenleneceğini ifade etmektedir. İlgili madde İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğinin tanıtıcı bilgiler hakkında açıklama

---

[362] Yargıtay 19. CD 2016/117 E. 2017/6570 K. 11/09/2017; *"..erişimin engellenmesine dair bir mahkeme kararının gereğini yerine getirmekle yükümlü kılınmayan ve "sorumlu kişi" tanımında bulunmayan "içerik sağlayıcısı" sanığın eyleminden artık sorumlu tutulamayacağı, dolayısıyla suçun faili olamayacağı sabit olup, bu nedenlerle sanığın beraatine.."*; Yargıtay 19. CD 2016/2978 E. 2017/8878 K. 30/10/2017; https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:15/01/2022).

[363] Akkurt, s 247.

yapan 5. maddesinde ticari ve ekonomik amaçlı içerik sağlayıcılarının iletişim adı altında vermesi gereken bilgiler görülmektedir. Bu yönetmelik ile kanun maddesi birlikte değerlendirildiğinde herhangi bir sosyal medya kullanıcısının bilgilendirme yükümlülüğüne tabi olmadığı düşünülmektedir[364].

En sonda ise kamu otoritelerince istenilen bilgileri sağlama ve tedbir alma yükümlülüğünü sayabiliriz. Bu yükümlülük tartışmalara sebep olan ve kişilere ait verilerin idare tarafından mahkeme kararı olmadan temin edilmesinin temel hak ve hürriyetler karşısında sakıncalar barındıran bir düzenlemeydi. 5651 sayılı kanun m.4/3 hükmünde yer alan içerik sağlayıcının kuruma talep edilen evrakların verilmesi gerektiği ile ilgili düzenleme Anayasa Mahkemesinin 8/12/2015 tarihli ve 2014/87 Esas, 2015/112 Karar numaralı kararı ile iptal edilmiştir.

3. Erişim Sağlayıcı ve Toplu Kullanım Sağlayıcılar: İnternet Erişimi Sağlayanlar

a. Erişim Sağlayıcı Kavramı ve Yükümlülükleri

Erişim sağlayıcı sosyal medyanın pasif süjelerindendir. Bu kavramın tanımı 5651 sayılı kanunun 2. maddesinin 1 fıkrasının e bendinde yapılmıştır. Tanıma göre internete erişim olanağı sağlayan yani kullanıcıların internete ulaşmasına aracılık eden kişilerdir. Gerçek veya tüzel kişiler erişim sağlayıcı olarak nitelendirilmektedir. İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliğin 3. maddesi 1. fıkrası ç bendinde de benzer bir tanım yapılmış "internet toplu kullanım sağlayıcılarına ve abone olan kullanıcılara" erişim sağlama ifadesine yer verilmiştir. Erişim sağlayıcı olan kişilerin tacir olma zorunluluğu olup olmadığı konusunda tartışmalar mevcuttur. Tartışmaların temelini oluşturan düzenleme Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik m.4'te bulunan "…erişim sağlayıcı olmak isteyen sermaye şirketlerinin…" şeklindeki ibaredir. Ancak diğer mevzuat hükümlerinde bu konuda açık düzenleme bulunmamaktadır. Bu sebeple erişim sağlayıcı kişilerin tacir

[364] Kaya, s. 237, Dülger, s. 776, Akkurt, s. 247.

olması gibi bir zorunluluğu var denilemeyecektir. Erişim sağlayıcılara örnek verecek olursak TTNet, Turkcell, KabloNet bunlara örnektir[365]. Ayrıca 5651 sayılı kanun gereği özel hukuk tüzel kişiline haiz Erişim Sağlayıcıları Birliği (ESB) kurulmuştur. Kurumun tüzüğünde ayrıntılı düzenlemeler bulunmaktadır. Birlik, erişimin engellenmesi kararlarının uygulanmasını sağlamakla görevlidir[366]. 5651 sayılı kanunun 8 maddesi ESB görevi dışındadır. Bu madde uyarınca verilen hakimliklerin erişimin engellenmesi kararların ESB'ye gönderilmesi durumunda bu kararlar kanunen muhatabı olması gereken BTK'ye gönderilmektedir. Sosyal medyada gerçekleşen ihlallerle ilgili ESB sitesinde sıkça sorulan sorular kısmında URL adresi ile erişimin engellenmesi mümkün olsa bile bazen bunun yapılmadığı durumlar olduğu belirtilmektedir. Özellikle hesap oluşturularak kullanılan örneğin 'facebook.com', 'youtube.com', 'twitter.com' sosyal medya sitelerinde 'https' protokolünü kullanılmamakta ve sebeple erişimin engellenmesinde zorluk yaşanmaktadır. ESB'ye bu şekilde gelen erişimin engellenmesi kararlarının uygulanmasının mümkün olmadığı kararı veren yargı makamlarına bildirilmektedir[367].

Erişim sağlayıcıların temel olarak iki yükümlülüğe sahip olduğu söylenebilir. İlki erişim sağlayıcının hukuka aykırı içeriği çıkartma yükümlülüğü ki bu yükümlülük 5651 sayılı kanunun 8/A maddesinde BTK Başkanı tarafından alınan karar sebebiyledir. İkinci yükümlülük ise adli makamlar ve kamu otoritelerince kendisine gönderilen erişimi engellenmesi kararlarını yerine getirmektir.

b. Toplu Kullanım Sağlayıcı Kavramı ve Yükümlülükleri

Toplu kullanım sağlayıcı kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan olarak 5651 sayılı kanun m. 2/1-i de tanımlanmıştır. Toplu kullanım sağlayıcı olabilmek için sağlayıcıların 5651 sayılı kanun kapsamında bir abonelik ya da bağlantı sağlayan kişi konumunda olması gerekir. Kanun metnindeki tanımın yeterli olmadığı noktalar olabilir. Örneğin bir

[365] Akkurt, ss. 306-307: Kaya, ss. 206-207.
[366] https://www.esb.org.tr/wp-content/uploads/2021/03/Esb-Tuzugu-2016.pdf (E.T:30/09/2021).
[367] https://www.esb.org.tr/s-s-s/ (E.T:30/09/2021).

evde bireysel internet üyeliğini diğer aile fertleri ile paylaşan kişilerin erişim sağlayıcı olarak kabul edilebilmesi mümkün müdür? Bu hususta kanun metninden bu gibi durumların kastedilmediği anlaşılabilmektedir. Ancak rıza konusunun açıklanmış olması gerektiğine ilişkin düşünceler mevcuttur. Toplu kullanım sağlayıcıların bağlantı şifrelerinin rızaları dışında ele geçirilmesi durumunda sorumluluklarının doğup doğmayacağı hususu açık değildir.

Toplu kullanım sağlayıcının nihai olarak şu şekilde tanımlanması mümkündür: Kendisine erişim sağlayıcı tarafından sağlanan toplu kullandırma yetkisine istinaden, internet aboneliği ya da bağlantısını, özellikle kamuya açık yerlerde, aile üyeleri ile aynı evde yaşayanlar ve benzeri kimseler hariç birden fazla kişinin rastgele bireysel erişimine toplu halde olanak sağlayacak şekilde ve iradi olarak paylaşan gerçek veya tüzel kişilerdir[368].

Yukarıdaki tanım ticari amaç güden ya da gütmeyen herhangi bir kimseyi ayrıca değerlendirmeden yapılmış bir tanımdır. Ancak ticari amaç güdenler açısından İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik[369] m.3/1-l'de herkese açık bir şekilde ve ücret karşılığında toplu internet hizmeti sağlayan kişiler olarak tanım yapılmıştır.

D. Ceza Hukuku Kapsamında Kişisel Verilerin Korunması

1. Ceza Hukuku Kapsamında Değerlendirilecek Sosyal Medyada Paylaşılan Veriler

İnternetin özellikle de sosyal medyanın yaygınlaşması ile özel hayat ihlalleri gün geçtikçe daha da artmaktadır. Bazı sosyal medya ağlarının birçok ülke nüfusundan fazla kullanıcıya sahip olması da bu konuda önemli bir etkendir[370]. Çalışmamızda da özellikle facebook, instagram ve twitter üzerinden yapılan paylaşımlara yer vermeye dikkat ettik. Sosyal ağlar oldukça geniş ve farklı

[368] Akkurt, s. 314.
[369] https://resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm (E.T:30/09/2021).
[370]Doğan Kılınç, "Anayasa Mahkemesinin Özel Hayatın Korunmasına İlişkin 2013/1614 Sayılı Kararı Üzerine Değerlendirmeler", **Internatıonal Journal of Legal Progress**, Cilt: 1 Sayı: 2, 2015, (Özel Hayat), ss.184-185.

özelliklere sahip olduğu için bu üç sosyal ağın birbiri ile benzer yönlerinin olması değerlendirme kolaylığı sağlamaktadır. İlk bölümde de değindiğimiz üzere facebook ve instagram sosyal ağlarının sahibi Facebook yeni adıyla Meta şirketidir. Her iki sosyal ağ da özellikle bu sebeple bazı farklılıkları olsa da büyük oranda benzer hale getirilmiştir. Twitter ise genel sosyal ağ özelliği olarak görsel ve işitsel paylaşımlardan ziyade düşünce ve yazıların paylaşıldığı bir sosyal ağdır. Her üç sosyal medya platformu hem görsel-işitsel hem de düşünce yazılarının paylaşılmasına izin vermektedir. Sadece uygulama özellikleri bazı alanların daha fazla kullanılmasını sağlamaktadır. Sonuç olarak kişisel verilere ilişkin ihlallerin yapılması her üç sosyal medya platformunda da oldukça yaygın olarak görülmektedir.

Yapılan bir çalışmada sosyal medyada gerçekleşen hak ihlalleri ve sosyal medya aracılığı ile gerçekleşen suçlar oldukça çeşitli olduğu görülmektedir. Mayıs 2020 de erişime açık Yargıtay kararları incelendiğinde 2016-2019 yılları arasında 1.172 dosyada facebook, twitter ve instagram isminin geçtiği görülmüştür. Bu dosyaların 953 tanesinin doğrudan bu sosyal medya platformları aracılığı ile işlenen suçlar olduğu tespit edilmiştir. Suç tiplerinde bakıldığında bu dosyalarda 1.139 adet suç olduğu görülmüştür. En çok facebook aracılığı ile suç işlenmiştir. Suçlardan 996 adedinin facebook, 122'sinin twitter ve kalan 21 adedinin de instagram yoluyla işlendiği tespit edilmiştir. Facebook konusunda birçok karar bulunmakta iken twitter ve instagram konusunda çok az kararın olması dikkat edilmesi gereken bir husustur. Facebook ve twitterın 2007'li yıllardan beri kullanıldığı ancak bu süreçte facebook kullanıcı sayısının daha fazla olduğu ve de instagramın 2011'li yıllardan sonra kullanılmaya başladığı görülmektedir. Yargıtay kararlarındaki yansıyan bu durum yerel mahkemelerde de mevcuttur. Kararların az olmasının temel sebebinin özellikle instagram sosyal medya platformlarının facebooktan ve de twitterdan çok daha sonra kişilerin yaşamına dahil olması yani nispeten daha yeni olması sebebiyle olduğu söylenebilir[371].

[371] Murat Cihan ve Sıtkı Yıldız, "Sosyal Medya Aracılığı İle İşlenen Suçlar", **Kırıkkale Üniversitesi Sosyal Bilimler Dergisi**, Cilt:11, Sayı:1, Ocak 2021, ss. 141-142.

Cihan ve Yıldız'ın çalışmasında üç sosyal medya platformunda işlenen suç tiplerine dair oluşturduğu tablo şu şekildedir[372]:

1.	Hakaret	283	24,8
2.	Özel hayatın gizliliği	159	14,0
3.	Verileri hukuka aykırı olarak verme ve ele geçirme	134	11,7
4.	Nitelikli Dolandırıcılık	116	10,2
5.	Tehdit	104	9,1
6.	Şantaj	53	4,7
7.	Cumhurbaşkanına hakaret	45	4,0
8.	Bilişim sistemindeki verileri bozma yok etme	42	3,7
…			…
	Toplam	**1.139**	**100**

Tablo 3: Facebook, Twitter, İnstagram aracılığı ile işlenen suçlardan 2016-2019 yılları arasında Yargıtay tarafından karara bağlanan suçlar**.**

Çalışmada her üç sosyal medya platformu aracılığı ile işlenen 28 farklı suç tipi olduğu tespit edilmiştir. Tabloda görüleceği üzere ilk sırada hakaret suçu yer almakta ikinci sırada özel hayatın gizliliğini ihlal üçüncü sırada ise verileri hukuka aykırı olarak verme ve ele geçirilmesi suç tipleri yer almaktadır. Ayrıca en çok kararın olduğu facebook özelinde de ilk üçte de aynı sıralama vardır. Twitter da ilk sırada hakaret varken ikinci sırada kişilik haklarına saldırı üçüncü sırada özel hayatın gizliliğini ihlal sekizinci sırada ise kişisel verileri hukuka aykırı olarak verme veya ele geçirme on birinci sırada ise haberleşmenin gizliliğini ihlal suçu yer almıştır. Yargıtay kararlarında instagram aracılığı ile işlenen suç tiplerinde ise yapılan sıralamada ilk sırada nitelikli dolandırıcılık ikinci sırada kişisel verileri hukuka aykırı olarak verme ve ele geçirme üçüncü sırada ise özel hayatın gizliliğini ihlal suçu yer almaktadır[373].

[372] Cihan ve Yıldız, ss. 144-145.

[373] Cihan ve Yıldız, ss. 141-144; Birden fazla suç tipini ilgilendiren kararlar bulunmaktadır. Bu sebeple dosya sayısı ve suç tipi sayısı farklı göründüğü durumlar olmaktadır.

2. TCK m. 135 ve m. 136 Açısından Sosyal Medya Paylaşımlarının Değerlendirilmesi

Çalışmamızda ceza hukuku açısından yapılacak değerlendirmede özellikle sosyal medyada kişilerin kendi rızaları herkese açık hesaplarından paylaştıkları kişisel verilere değinmek istiyoruz. Rıza dışı paylaşımlar ve de korumalı hesaptan yapılan paylaşımlar oldukça geniş bir alanı ve farklı suç tiplerini ilgilendirmektedir.

Kişisel verilerin korunması konusu medeni hukuktaki temel kavramlardan olan kişilik hakkı ile doğrudan bağlantılıdır. Verilerin işlenmesi, saklanması ve transferi gibi işlemler veri sahibinin rıza göstermesinin aranması aslında kişilik hakkının niteliğinin doğal bir sonucudur. Kişilik hakkı, devredilemez ve kişiye sıkı sıkıya bağlı olan bir haktır. Bu sebeple kişinin rızası kişilik hakkına dolayısıyla da kişisel verileri konusundaki hukuka uygunluk sebebi olarak düzenlenmiştir. Rızanın verilmesi hukuka ve ahlaka aykırı bir amaçla olmaması gerekir. Rıza verilen durumlarda verilen rızanın da ayırt etme gücüne sahip kişilerce verilmiş olması gerekir. Küçük veya kısıtlılar söz konusu olduğunda bu kişiler verecekleri rızanın tüm sonuçlarını öngörebilecek durumda olmalı aksi takdirde yasal temsilcilerinin de onayı gerekecektir. Ayrıca rıza alınırken kişilerin bu konuda doğru bir şekilde bilgilenmesi ve aydınlatılmış olması gerekir. Kişi rızasını serbest bir iradesi ile kişilik haklarına saldırı sayılabilecek durumdan oluşmadan önce ya da en geç o anda açıklayabilmelidir[374].

Sosyal medyada profil oluşturan kişiler hayatlarına dair paylaşımlar yapmaktadır. Burada mahremiyet algısı önem arz etmektedir. Günümüzde mahremiyet algısının kişiden kişiye değiştiği görülmektedir. Bu sebeple mahremiyetin bireylerin kendilerine özel olan ve diğerlerince öğrenildiğinde herhangi bir zarar içermeyen, bireylerin bizzat kendilerinin açıklayıp açıklamama hususunda karar verdiği bir konu olduğu söylenebilecektir. Kişiler hayatlarından hangi kesitleri ve durumları kimlerle paylaşacaklarına kendileri karar verdiği için mahremiyetin tanımını da ölçüsünü de kendileri belirlemektedir. Sosyal medya

[374] Atasoy, s. 286; Serap, Helvacı, **Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar**, Beta Yayınları, İstanbul, 2001, s. 105; Aydın Zevkliler, Mehmet Beşir Acabey, K. Emre Gökyayla, **Medeni Hukuk- Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku**, 6. Baskı, Seçkin Yayınları, Ankara, 2000, ss. 489-490.

Bauman tarafından "mahremiyetin yok oluşu" olarak değerlendirilen sanal dünyaya dahildir. Bauman'a göre bu sanal dünya ve internet her şeyi gören veya görüntüleyen ancak görünmez olan bir alandır. Veriler bu alanda sayısız sunucu tarafından tamamen silinemeyecek bir şekilde ulaşılabilir halde var olmaktadır. Sosyal medyanın kişilerin hayatlarındaki konumlarından dolayı sosyal medya odaklı bir yaşam gelişmiş ve kişilerin yalnızca sosyal medyada paylaşma amacıyla fotoğraf çekildiği bir durum oluşmuştur. Kişilerin yalnızca dijital albümler kullanması bu fotoğraflardan genellikle gerçek albümler oluşturulmadığı görülmektedir. Sosyal medyada konum belirtilerek yapılan paylaşımlar da bulunmaktadır. Humphreys tarafından yapılan bir araştırmada konum bilgisine yönelik sosyal paylaşım ağlarını kullanıp paylaşım yapan kullanıcıların gizlilik kaygısı gütmediği görülmüştür. Ayrıca bu kullanıcılar kendilerini paylaştıkları bilgilerin kontrolünün kendilerinde olduğunu ya da bu konuda yeterince deneyimli bireyler olduğunu düşünmektedirler[375].

KVKK 5.ve 8. maddede kişisel verinin işlenmesi ve transferi konusunda açık rızanın arandığı hükmü düzenlenmiştir. Örneğin kişilik haklarına yapılan herhangi bir saldırıda kişilerin zımni ya da açık bir rıza olması hukuka uygunluk için yeterli iken söz konusu verilerin doğrudan kişisel veriler olması halinde veri sahibinin açık rızasını içeren beyanı gereklidir. 6698 sayılı kanunun 5. maddesinin 2. fıkrasının d bendinde açık rızaya gerek duyulmayan hallerden biri olarak veri sahibi tarafından verinin alenileştirilmesi hususunu düzenlenmiştir. Sosyal medyada birçok kişisel veri paylaşılmaktadır. Bu verilerin bir kısmı kişinin hassas verileri olarak kategorilendirebileceğimiz verilerdir. Hassas veriler konusundaki 6. maddenin 2. fıkrasında ise hassas verilerin açık rıza dışında işlenmesinin yasak olduğu hükmü yer almaktadır. Ayrıca maddenin 4. fıkrasında da hassas verilerin işlenebilmesi için Kişisel Verileri Koruma Kurulu tarafından belirlenen tedbirlerin uygulanması gerektiği belirtilmektedir. Hassas verilerin kişilerin bizzat kendisi tarafından sosyal medyada alenileştirilmesi durumunda "yeterli önlemlerin alınması" şartı ile bu verilerin işlenmesi hukuka uygun olabilecektir. Ancak Atasoy'un da önemle belirttiği şey madde m. 6/4 metninde yer alan yeterli önlemlerin alınması ibaresinin muğlak olmasıdır. Bu yeterli önlemlerin niteliği ya da genel özellikleri açıklanmamıştır[376].

[375] Çetin, s. 781.
[376] Atasoy, s. 287.

Hassas verileri kişiler için yaşamsal önem taşıyan haklar olarak değerlendirilmelidir. Kişiler bu verileri bizzat kendileri alenileştirilmiş olsa dahi bu veriler hala öncelikli korumaya sahiptir[377]. Bulut'a göre hassas veriler hakkında KVKK m. 5/2'de açık rıza dışında işlenebilecek hallerin uygulanabileceğine ilişkin açık bir hüküm yoktur. Buna rağmen KVKK m. 5/2 hükümleri de hassas verilerin işlenmesinde kullanılmaktadır[378].

Sosyal medyada kişilerin hassas veri niteliğinde olan etnik kökenine, cinsel hayatına ya da genetik verilerine ilişkin paylaşımlar yaptığı görülmektedir. Örneğin son yıllarda kişinin genetik kökenine ilişkin tespitler yapan programlar sonucunda çıkan analizler sosyal medya kullanıcıları tarafından sık sık paylaşım konusu yapılmaktadır. Kullanıcıların hastalıklarını belirterek yardım toplaması, yaşadığı bir olayı anlatırken cinsel tercihlerini ya da dini inançlarını açıkladığı paylaşımları da hassas verilerini açıkladığı başka örneklerdir. Budak tarafından yapılan bir çalışmada kişilerin yüzde 67,5'i dini görüşleri mahrem olarak görmemektedir. Dini görüşleri mahrem olarak görenlerin ise yüzde 48,3'ünün bu görüşlerini sosyal medya da hiçbir zaman paylaşmayacaklarını ifade ettiği görülmüştür. Cinsel tercihler konusunda kişilerin büyük çoğunluğunun bunların mahrem nitelikte olduğunu ve bu tercihlerini sosyal medyada hiçbir zaman paylaşmayacaklarını ifade ettikleri görülmüştür. Ancak cinsel tercihleri mahrem olarak görmeyenlerin yüzde 68,2'sinin ve mahrem olup olmadığı konusunda kararsız olanları yüzde 75'inin de bu tercihlerini hiçbir zaman sosyal medyada paylaşmayacaklarını ifade ettikleri görülmüştür[379]. Yapılan başka bir çalışmada belirlenen kişilerin sosyal medya hesaplarında hangi verileri paylaştıklarının tespitine ilişkindir. Sorunun muhatabı olan kullanıcılara kişisel bilgilerini paylaşıp paylaşmadıkları sorulduğunda yüzde 71,2'sinin kişisel bilgilerine ilişkin bilgileri paylaştıklarını ifade ettikleri görülmektedir. Sosyal medyada fotoğraf paylaşma konusunda ise yüzde 52,4 oranında fotoğraf içeren paylaşımları çok

[377] Bulut, s. 123; Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, 1. Baskı, Yetkin Yayınları, Ankara, 2004, (Kişisel) s. 45; Henkoğlu, s. 29

[378] Hassas verilerin işlenmesi hususundaki hukuka uygunluk sebepleri GDPR'da ayrıca düzenlenmiştir. Hassas verilerin, normal kişisel veriler hakkındaki hukuka uygunluk sebeplerinin dışında tutulması ve hassas veriler için ayrı hukuka uygunluk sebeplerinin oluşturulması daha doğru bir yaklaşım olacaktır. Bulut, s. 142.

[379] Budak, ss. 164-165.

yaptıklarını ifade etmişlerdir[380]. Tüm bu çalışmalar dikkate alındığında kullanıcıların hassas verilerin paylaşılmaması gerektiğinin farkında olduğu tespiti yapılabilmektedir. Ancak mahremiyet algısının da kişiden kişiye değiştiği de görülmektedir. Hassas veriler paylaşılsın ya da paylaşılmasın herhalde ve durumda hassas verileri "hassas veri niteliğini" kaybetmemektedir. Hassas veriler, KVKK m. 6 uyarınca düzenlenen özel hükümlere ve de TCK m. 135/2'de yer alan cezayı ağırlaştırıcı sebebe ilişkin hükümlere tabi olacaktır.

Kişinin kendi resmini paylaşması durumu sosyal medyada oldukça yaygın olan hatta karşımıza en çok çıkan durumdur. Bu durumda kişinin bu paylaşımının kopyalanmasına ya da başka kullanıcılar tarafından paylaşılmasına rızasının olup olmadığı sorunu ortaya çıkmaktadır. Bu sorunun cevabı somut olaya göre değişebilecektir. Kullanıcılar paylaşımlarını kendi rızası ile yaptığı bu paylaşımlara kimlerin erişebileceğini belirleyebilmektedir. Kullanıcının sınırlı sayıda kişinin görebileceği şekilde yaptığı paylaşım yani korumalı bir hesap kullanması gibi durumlarda bu paylaşımını üçüncü kişilerin görmesini istemediği anlamına gelmektedir. Ya da paylaşımın türüne göre değerlendirmeler de yapılabilir. Örneğin hikaye diye adlandırılan ve kullanıcının süreli paylaşımı olan bir paylaşım türü bulunmaktadır. Hikayeler paylaşıldığı andan itibaren 24 saat ve de kişinin görebilmesini istediği kullanıcılarca görülebilmektedir. Süreli ya da korumalı hesaplardan yapılan farklı paylaşım türlerinin doğal olarak herkesin görmesini ya da kaydetmesini istemediği anlaşılabilmektedir. Bizce üçüncü kişilerin kullanıcının bu paylaşımlarının kopyalamasına veya paylaşmasına rıza göstermediği kabul edilmelidir. Bir diğer ihtimal kullanıcının herkese açık bir hesap kullanarak sınırlama yapmadan paylaşım yapıyor olmasıdır. Bu durumda paylaşım yapan kişinin kendi resimlerini üçüncü kişilerce ticari amaçlı kullanılmasını ya da resimleri üzerinde birtakım düzenlemeler yaparak paylaşmasına rıza vermediğinin kabulü gerekecektir. Aslında değerlendirdiğimiz tüm hususlar bizi tek bir sonuca ulaştırmaktadır: Kullanıcının kişisel verisini paylaşmasının ardında olan amaç. Kullanıcının rıza göstermesi durumunda rızanın neye yönelik olduğu ya da alenileştirme durumunda alenileştirme amacının neye yönelik olduğunun tespiti gerekmektedir.

[380]Serkan Gönen, Halil İbrahim Ulus, Ercan Nurcan Yılmaz, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", **Bilişim Teknolojileri Dergisi**, Cilt. 9, Sayı: 3, 2016, s. 235.

Rıza teşkil eden hususlar konusunda Yargıtay Hukuk Genel Kurulunun bir kararında daha önce resmin bizzat kişinin kendisi tarafından internet sitesine verildiği yani rızanın verilmiş olması sebebi ile kişilik hakkının zedelenmediğini düşünen yerel mahkemeden farklı düşünmüştür. HGK'ye göre olayda resmin kullanılması konusunda verilen rıza yalnızca kültürel ve tanıtım faaliyetlerine yönelik sitede paylaşım yapılması şeklindedir. Yani rızayla resmin verilmesi ile kişi resim üzerindeki tüm tasarruf hakkını kaybetmiştir denilemez. Rızanın verildiği konu dışında davalının resmi ticari amaçlarla kullanmış olması davacının kişilik haklarını zedelemiştir[381]. Söz konusu karar ceza hukukunda hukuka uygunluk sebebi olan rızaya ilişkin olmasa da ayrıca doğrudan sosyal medyada kullanıcı tarafından yapılan bir paylaşım olduğu görülmese de çalışmamız kapsamında önemli açıklamalar yapmaktadır. Ayrıca rızanın ve alenileştirmenin "amacı" konusuna da dikkat çekmektedir. Sosyal medyanın yeni bir alan olması ve değişkenliği sebebi ile her konuda bir görüş, değerlendirme ya da yargısal karar elde etmek mümkün değildir. Bu durum sosyal medya konusunda her kaynağı ve değerlendirmeyi inceleyip bir süzgeçten geçirme ihtiyacını doğurmaktadır.

Kişisel verilerin korunması konusunda ceza hukukunda en temel düzenlemeler TCK m. 135'e yer alan kişisel verilerin kaydedilmesi suçu ve de TCK m. 136'da yer alan kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçlarıdır. Her iki suç tipinde de kanun koyucu bu işlemlerin hukuka aykırı olarak yapılması halinde söz konusu suçların oluşacağını öngörmektedir. Fiilin hukuka aykırı olmasının ne anlama geldiğine dair tanımlama yapılacak olursa bu husus kısaca "hukuk düzeni tarafından izin verilmeyen fiilin yasal düzenlemedeki tanıma uygun olması" şeklinde ifade edilebilecektir. Sonuç olarak hukuka aykırı olarak gerçekleştirilen fiil hukuk düzeninin tamamı açsından bir çatışma oluşturacak nitelik taşımaktadır[382]. Ancak şunu da belirtmek gerekir ki ilgili suç tiplerine ilişkin düzenlemelerde hukuka aykırılık ibaresi yer almasa bile fiilin kanuni tanımdaki tipe uygun olması halinde onun hukuka aykırı olduğuna karine teşkil edecektir. Karine olduğunun kabulü halinde de hukuka aykırılık ve tipe uygunluk her somut olayda

[381] Aka, s. 244.
[382] Hasan Sınar, "Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK md. 136)", **Kişisel Verileri Koruma Dergisi**, Cilt:2, Sayı:1, s. 53.

değerlendirilmelidir. Çünkü bazı durumlarda tipe uygunluk olmasına rağmen hukuka aykırılık oluşmamış olabilecektir[383]. Bu sebeple rıza konusunu da ayrıntılı açıklayacağımız konu olan hukuka aykırılık nasıl oluşabilir, bu suç tiplerinde yer alan eylemlerden olan veriler nasıl kaydedilir, verilir ya da ele geçirilir kavramlarına değinmek gereklidir.

Kişisel verilerin korunması konusunda düzenlenen suç tiplerinin ortak özellikleri şu şekilde açıklanabilir. Bu suçlar sırf hareket suçu, soyut tehlike suçudur. Bu suçlar kasten işlenebilen bir suçlardır. Suçların faili ya da mağduru gerçek kişiler olabilecektir. Suçun konusu ise gerçek kişilere ait kişisel verilerdir. TCK m. 135 ve m. 136'da yer alan suçlar icrai hareketle işlenebilen suçlardır. Bu suçların soruşturulması ve kovuşturulması şikayete bağlı değildir. Kişisel verilerin korunması hakkı Anayasa'da özel hayatın gizliliği kapsamında ancak ayrı bir hak olarak kabul edilmektedir. Bu suç tipleri ile korunan hukuki değer doğrudan kişisel verilerin korunması hakkıdır[384].

a. Kişisel Verilerin Kaydedilmesi, Kişisel Verileri Verme, Yayma ve Ele Geçirme Suçlarının Maddi Unsuru

TCK m. 135'te kişisel verilerin kaydedilmesi konusunda yapılan açıklamalara bakıldığında suçun maddi konusu kişisel veriler olsa da kanunda kişisel verilerin niteliği gereği sınırlı sayım yapılamamıştır. Bu konuda kişisel verilerin korunması hukukunda incelenen kişisel veriler esas alınacaktır. Tartışmalar olsa da bu durum kanunilik ilkesine aykırılık oluşturmamaktadır[385]. Konuya ilişkin TCK m. 136'nın Anayasanın 38. maddesine aykırı olduğu iddiası ile iptali istenen olaya ilişkin AYM

---

[383] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, **Türk Ceza Hukuku Genel Hükümler**, 11. Baskı, Seçkin Yayıncılık, Ankara, 2020, (Genel) ss. 276-278; Maddi ve biçimsel hukuka aykırılık ayrımı konusunda Özbek, Doğan ve Bacaksız farklı bir düşünceye sahiptir. Yazarlarca biçimsel ve maddi hukuka aykırılık şeklinde bir ayrımın yerinde olmadığı düşünülmektedir. Özellikle maddi hukuka aykırılık konusunda yapılan menfaatin gerçekten ihlal edilip edilmediği incelemesi yalnızca cezanın şahsileştirilmesinde araç olarak kullanılabilir.

[384]Mahmut Koca ve İlhan Üzülmez, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m.135)", **DEÜ Hukuk Fakültesi Dergisi,** Durmuş Tezcan'a Armağan, Cilt:21, 2019, ss. 74-75.

[385] Korkmaz, s. 387; Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, **Yorumlu Uygulamalı Türk Ceza Kanunu**, Adalet Yayınevi, Ankara 2010, s. 4116; Suçta ve cezada kanunilik ilkesi gereği kişisel verinin yasada düzenlemesi gerektiği görüşü için bkz. Durmuş Tezcan, "Özel Hayatın Gizliliğini İhlal Ve Kişisel Verilerin Kaydedilmesi Suçu İle İlgili Bazı Gözlemler", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: 71, Sayı:1, 2013, s. 1162.

kararında AYM, ceza kanununda doğrudan kişisel verinin tanımı yapılmamış olsa da kişisel verinin tanımının hem ulusal hem de taraf olunan uluslararası mevzuatta açıkça yapıldığını bu sebeple TCK m. 136 hükmünde belirsizlik olduğunun kabul edilemeyeceğini ifade etmiştir. Sonuç olarak Mahkeme kişisel veri ifadesinin suçta ve cezada kanunilik ilkesine aykırılık oluşturmadığına hükmetmiştir[386].

Önceki kısımlarda belirttiğimiz gibi kişisel verilerin neler olduğuna dair KVKK'de sınırlı sayım yapılmamıştır. KVKK'den daha önce yürürlüğe girmiş olan Türk Ceza Kanunu'nda da kişisel verilere ilişkin tanımlama yapılmamış yalnızca hassas verilere ilişkin bir açıklama yapılmıştır. Kişisel verilerin tanımı konusuna önceki açıklamalarımızı dikkate alarak tekrara düşmemek adına ayrıca "kişisel veri nedir?" şeklinde ayrıntılı açıklamalara yer vermeden yalnızca kısaca değineceğiz. İlgili verilerin bir gerçek kişiye ilişkin olması ve o kişiyi belirlenebilir kılması bu suçun konusudur.

Suçun isimlendirmesi gereği verilerin kişisel veri niteliğinde olan ve kişilerin tek başına üzerinde tasarruf hakkı olabilen verileri esas alınacaktır. Anayasa Mahkemesinin 2016 tarihli Bülent Kaya Kararında TCK m. 135 ve 136'da korunan verilerin "*herkesin ulaşabileceği bir ortamda paylaşılmamış"* olan veriler olması gerektiği ifade edilmiştir. Kişisel verinin herkesle paylaşılarak özel hayat alanından genel hayat alanına geçirilmiş olması halinde TCK m. 135 ve 136 hükümlerine göre bir korumaya ihtiyaç duymadığı anlamına gelmektedir[387]. Bazı Yargıtay Kararlarında kişisel verilerin kişinin üçüncü kişilerin bilgisine sunmadığı yalnızca kendisi istediğinde sınırlı çevresi ile paylaştığı bilgiler olarak anlaşılması gerektiği ifade edilmiştir[388]. Herkesçe ulaşılabilir ortamda paylaşılmamış ve üçüncü kişilerin bilgisine sunmadığı şeklindeki açıklamaya katılmamakla birlikte Yargıtay kararında sayılan verilerin kişisel veri niteliğinde olduğu kabul edilecektir

Doktrinde farklılıklar olduğu gibi Yargıtay bazı kararlarında da farklılıklar bulunmaktadır. Yargıtay bir kararında herkesçe bilinen ve ulaşılması için fazla çaba gerektirmeyen bilgilerin kişisel veri kabul edilmeyeceğini düşünmektedir. Yine başka bir kararında kişiyi belirlenebilir kılan ve onu diğer kişilerden ayırmayı

[386]AYM, 2015/32 E. 2015/102 K. 12/11/2015 T. https://www.resmigazete.gov.tr/eskiler/2015/12/20151202-16.pdf (E.T:13/12/2021).
[387] Özbek, Doğan, Bacaksız, ss. 587-589; Korkmaz, s. 387.
[388]Sınar, ss. 38-39.

sağlayan niteliklerini içeren verilerin kişisel veri olduğunu düşünmekle birlikte bu verilerin kişinin sınırlı çevresi ile paylaştığı ve herkes tarafından bilinmeyen veriler olduğunu söylemektedir. Yargıtay bu açıklamaları yaptıktan sonra bazı kararlarında kişinin özel hayatına ilişkin fotoğrafları kişisel veri olarak kabul etmemektedir. Bu tarz fotoğrafların yayınlanmasının söz konusu olduğu bir olayda yalnızca TCK m. 134/2'nin uygulanması gerektiğine hükmetmiştir[389].

Yargıtay Ceza Genel Kurulunun bir kararında ise 135 ve 136. maddelerde korunan hukuki değerin sadece sır niteliğindeki bilgiler olması gerektiğine ilişkin bir hükmün bulunmadığı belirtilmiştir. Kararda TCK m.135'in gerekçesine değinilmiştir. Gerekçede gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğinin belirtildiği bu sebeple her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesinin, yayılmasının 136. maddedeki suçu oluşturacağı ifade edilmiştir. Somut olayın içeriği sebebi ile ayrıca hakaret suçundan da hüküm kuran Genel Kurul TCK m. 125 ile m. 136 hükümlerinde farklı neviden fikri içtima uygulanarak en ağır olandan TCK m. 136 hükmünden ceza verilmesi gerektiğine karar vermiştir. Genel Kurul Kararına katılmayan bazı üyelere göre *"ilgili kişi tarafından alenileştirilmemiş, üçüncü kişilerle paylaşılmamış, bilinmesinin kişinin yaşam şekline, ekonomik ve finansal ve bilişim alanına zarar verme ihtimali bulunan bilgiler olması halinde"* kişisel veri suçun konusu olabilecektir. Bu hususlar haricindeki durumlarda verilerin kullanılış amacına göre farklı suç tipleri oluşabilecektir. Örneğin hakaret, dolandırıcılık gibi suçların konusu olabilecektir. Somut olaydaki fotoğraf açısından m. 136 hükmü ve kişisel verilerin korunması hükümleri uygulanmamalıdır. Çünkü fotoğraf kişinin belirlenmesi mümkün olmayacak şekilde paylaşılmıştır. İsmi ya kendisini belirleyebilecek başka bir bilgiye yer verilmemiştir[390]. Koca ve Üzülmez'e göre YCGK'nin fotoğrafı kişisel veri niteliğinde kabul etmesi şeklindeki tespiti isabetli olmakla birlikte kişi bunu kendisi alenileştirdiği için başka kişilerce kaydedilmesi ya da yayılması sebebi ile TCK m. 135 ya da m. 136'da yer alan suç tipleri oluşmamıştır[391].

[389] Yaşar, Gökcan, Artuç, ss. 4435-4442.
[390] YCGK, 2012/1510 E. 2012/331 K. 17/06/2014 T. https://kararara ma.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:30/12/2021).
[391] Koca ve Üzülmez, s. 92.

Yargıtay Ceza Genel Kurulunun kararında karşı oy kullanan üyelerin kendi ifadeleri ile *"ilgili kişisinin, her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim (TCK'nın 6/1-9) okyanusuna bıraktığı bir kişisel verisinin hangi okyanus, deniz, göl, gölet ve bataklığa gireceğine artık engel olamaz."* demek bizce mümkün değildir. Kişinin rızayla paylaştığı ya da alenileştirdiği fotoğrafı ya da başka kişisel verisi kaydedildiğinde bir hukuka uygunluk sebebi oluşabilecekken TCK m. 136 açısından hukuka uygunluk sebebi de vardır denilemez. TCK m. 136 açısından özellikle rızayla paylaşılmış olan ve aleni hale getirilen verinin farklı amaçlarla kullanımına rıza verilmiş olup olmadığı önemlidir. Milyonlarca verinin olduğu sosyal medya platformlarında örneğin kişinin kendini tanıtma amacıyla kullandığı profil fotoğrafının alınıp farklı şekillerde kullanılmasını cezai yaptırıma bağlayan bir yasal düzenleme olmalıdır. Kişini resmi bizzat kendisini tanıyan kitle için kişiyi belirli kılmaktadır. Yukarıda bahsettiğimiz kararda köşe yazarı olan mağdurun yazı yazdığı gazetede işi sebebiyle yer alan fotoğrafının sanıklar tarafından kişinin onurunu ve şerefini zedeleyecek şekilde sosyal medyada cinsel amaçlarla kullandığı görülmektedir. YCGK'de hakaret suçu oluştuğu kabul edilmiştir. Bu fotoğrafın yalnızca farklı bir suç tipi oluşturulacak şekilde kullanılmış olması halinde cezalandırılması elbette bir zorunluluktur. Ancak bunun dışında kişilerin yüzleri dahil fiziksel özelliklerinin kişisel veri olduğunun kabulü ve TCK m. 136 hükümlerince bu verileri yayan, veren ya da hukuka uygun olarak kaydetme olmadan ele geçiren failin cezalandırılması gerektiğinin kabulü gerekir. YCGK'nin hakaret suçu dışında ayrıca da TCK m. 136 açısından da mahkumiyet hükmü vermiş olması bizce doğrudur.

Koca ve Üzülmez'e göre örneğin rızayla paylaşılan ya da alenileştirilen veriler kişisel verilerin hukuka aykırı kaydedilmesi suçunun konusu olabilir. Ancak suç tipine ilişkin hukuka aykırılık incelemesinde suçun oluşmadığı kanaatine varılabilir. Herhalde hukuka uygun olarak kabul edilebilmesine kadar bu verilerin suçun konusu olduğu kabul edilmelidir[392]. Doktrinde kişilerin kendi rızaları ile sundukları ve alenileştirdikleri verilerin artık TCK m. 135-136 kapsamında suçun konusu olarak değerlendirilemeyeceği görüşünde olan yazarlar bulunmaktadır.

[392] Koca ve Üzülmez, s. 77.

Kişinin gizli tutma amacı olmadan alenileştirdiği kişisel verilerin suçun konusu olarak kabul edilemeyeceğini kabul eden görüşler vardır[393].

Suçun faili herkes olabilecektir. TCK m. 135 ve m. 136 özelinde düşündüğümüzde kişisel veriyi hukuka aykırı olarak kaydeden, veren, yayan ya da ele geçiren kişiler bu iki suç tipinin faili olabilecektir Suçun mağduru da herkes olabilecektir[394]. Çalışmamız kapsamında değerlendirdiğimizde suçun failinin sosyal medya kullanıcısı bir kişi olabileceği gibi sosyal medya kullanıcısı olmayan ama herkese açık bir hesaba erişebilecek bir internet kullanıcısı olabileceğini düşünebiliriz. Suçun mağduru ise sosyal medyada çeşitli şekillerde herkese açık hesabından verisini paylaşan sosyal medya kullanıcısı olan kişi olacaktır. Suçun faili ve mağdurunun gerçek kişi olması durumunda TCK m. 135 ve m. 136 hükmünün uygulanmasında tartışmalı bir husus yoktur. Ancak "Sosyal medya kullanıcısının bir tüzel kişi olduğu durumlarda tüzel kişilerin sosyal medyadaki verileri bu kapsamda korunur mu?" sorusu akıllara gelecektir. Ancak bizce TCK ve Kişisel Verilerin Korunması Kanunu ile kişisel veriler konusundaki tanımlamaları değerlendirildiğinde doğrudan gerçek kişiye esas alındığı görülmektedir. Tüzel kişiler suçun mağduru ya da faili olarak kabul edilmemektedir. Doktrinde de genel olarak kabul gören görüş tüzel kişilerin suçun mağduru değil de ancak suçtan zarar gören olarak değerlendirilebileceğidir Yargıtay kararlarında da benzer düşünce hakimdir. Yargıtay bazı kararlarında şirketlerin finansal verilerinin kişisel veri olarak kabul edilmeyeceği ve de kişisel verilerin yalnızca gerçek kişilere ait bilgiler olduğuna ilişkin kararları mevcuttur[395]. Doktrinde başka bir görüşe göre bu suçun mağdurunun tüzel kişiler olamaz aynı zamanda suçtan zarar gören olarak da kabul edilemez. Tüzel kişilere ait veriler söz konusu olduğunda TCK m. 239'da yer alan suç tip uygulama alanı bulabilecektir[396]. Suçun failini tüzel kişi olup olamayacağı noktasında ise ceza sorumluluğunun şahsiliği ilkesi sebebi ile suçun failinin tüzel kişi olamayacağı düşünülmektedir[397].

---

[393] Aydın, s. 130.
[394] Özbek, Doğan, Bacaksız, ss. 581, 591.
[395] Sınar ss. 40-41; İtişgen, s. 190; İzzet Özgenç, **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayıncılık, Ankara, 2011, s. 198.
[396] Koca ve Üzülmez, s. 75.
[397] İtişgen, s. 190.

Kişisel veriler hakkında suç oluşturan eylemin tüzel kişinin faaliyetleri kapsamında gerçekleştirilmesi halinde TCK m. 140 hükmü gereğince tüzel kişilere özgü güvenlik tedbirleri uygulanabilecektir[398]. Ceza hukuku açısından suç ve cezaların şahsiliği ilkesi gereği tüzel kişilerin doğrudan cezai sorumluluğu bulunmamaktadır. Özel hukuk açısından tüzel kişilere özgü bazı hak ve borçlara sahip olmaları kabul edilmekle birlikte bu durum ceza hukuku açısından kabul edilmemiştir. Bu sebeple tüzel kişinin organlarının eyleminden dolayı tüzel kişiye ceza verilemeyecektir. Tüzel kişilere özgü güvenlik tedbirleri ise TCK m. 60'ta sayılmıştır[399]. Bu hükümler dışında önceki kısımlarda bahsettiğimiz üzere sosyal medya süjeleri olan tüzel kişiler için özellikle KVKK ve de 5651 sayılı Kanunu'nda yer verilen kabahatler ve idari yaptırımlar bulunmaktadır. Bu sebeple tüzel kişiler yönünden o kısımda yer alan tedbirler ve yaptırımlar da uygulanabilecektir.

TCK m. 135'te yer verilen ilk hareket kaydetmedir:

Kaydetmek: Kaydetme ile ifade edilmek istenen verinin bir araç kullanılarak ya da kullanılmayarak tekrar ulaşmayı mümkün kılacak bir şekilde saklanmasıdır. Kanunda bu kaydetmenin nasıl olacağına ilişkin bilinçli bir şekilde açıklama yapılmamıştır. Kanun gerekçesinde de bu husus belirtilmiştir. Çünkü hangi durumlarda kaydedilme fiilinin suç oluşturup oluşmayacağına ilişkin sınırlı bir sayıma gidilmesi halinde suçun kapsamı daraltılmış olacaktır. Bu sebeple kaydetme fiili gerçekleştiğinde suç oluşup oluşmadığını tespitinin yapılabilmesi için aranması gereken şey hukuka uygunluk sebebinin olup olmadığıdır[400]. Bu eylemin nasıl gerçekleştirildiği önem arz etmemektedir. Ancak kaydetme eyleminin hafıza da tutma ya da ezberleme gibi şekillerde olmasının kabul edilmesi pek mümkün değildir. Özbek, Doğan ve Bacaksız'a göre kaydetmedeki amacın hasıl olabilmesi için bunun kullanılabilir ve saklanabilirliği olan bir araçla yapılması gerekir. Bunlarında sağlanabilmesi için kaydetme işleminin bir CD, kaset ya da şifreli bir alanda kaydedilmelidir. Verinin hukuka aykırı şekilde kaydedilmesi ile suç tamamlanacaktır[401]. Ketizmen'e göre ise suçun oluşması için verinin herhangi bir

[398] Sınar, s. 40.
[399] M. Yasin, Aslan, "Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu", **Ankara Barosu Dergisi**, Cilt.:68, Sayı:2, 2010, ss. 243-245.
[400] Korkmaz, s. 392.
[401] Özbek, Doğan, Bacaksız, s. 581.

şekilde kaydedilmesi yeterli olacaktır. Suç tipinin düzenlenmesine ilişkin bilişim ve teknolojik gelişmelerin etkili olduğu görülse de maddede bu şekilde bir ayrım yapılmamıştır. Yani hukuki olarak bu suç tipinde bir bilişim sistemine kaydetme ya da bir kağıda kaydetme arasında bir farklılık yoktur[402]. Benzer görüşte olan yazarlar da kağıda yazılma ile kayıt işlemi gerçekleşmiştir demektedir. Çünkü kağıda yazılma sureti ile istenen amaç hasıl olmuş ve tekrar kullanılması mümkün hale gelmiştir[403].

Sosyal medyada rızayla herkese açık bir şekilde paylaşılan bir verinin başka bir kullanıcı tarafından ekran görüntüsü alınarak kaydedilmesi halinde kullanıcının rızasının neye yönelik olduğuna göre hukuka uygunluk sebebi aranacaktır. Örneğin İnstagram uygulaması kişilerinin gönderilerini "koleksiyona kaydet" şeklinde bir özellik sunmaktadır. Kaydetme eylemi bu özellik kullanılarak uygulamaya özgü bir şekilde yapılabilecektir[404]. Her kullanıcı bu özelliği kullanarak gönderiyi paylaşan kullanıcı bu gönderisini profilinde tutulduğu müddetçe instagram uygulamasında koleksiyonunun içinde görebilecektir. Kullanıcıların herkese açık bir hesaptan yaptığı bir paylaşımın ya da belli kişilerin görebileceği şekilde yaptığı paylaşımın başka bir kullanıcı tarafından kaydet seçeneği kullanılarak instagram uygulamasında kaydedilmesi kanımızca suç oluşturmayacaktır. Kullanıcıların instagram tarafından sunulan bu özelliği bildiği ve de paylaşımlarını görmesine izin verdiği kullanıcıların bu gönderileri kaydet seçeneği ile kaydetmesini öngördüğü ayrıca da buna izin verdiği kabul edilebilecektir. Ayrıca sosyal medyada veri paylaşımı ile kişinin verilerini kendisinin alenileştirdiği kabul edilecek olursa da bu durumda da verilerin kaydedilmesinin suç oluşturmayacağı düşünülebilecektir. Hukuka aykırılık konusunda değineceğimiz üzere aleniyetin bizzat ilgili kişi tarafından sağlanması halinde KVKK hükümlerine göre verilerin işlenmesinde açık rıza aranmamaktadır. Şunu da belirtmek gerekir ki KVKK'de yer alan hukuka uygunluk sebeplerini suç tiplerine uygulamak istediğimizde KVKK'de yer alan ilkeler de dikkate alınmalıdır. Sonuç olarak KVKK sistematiğinde hukuka uygunluk hali sayılabilecek haller kişisel

---

[402] Ketizmen, s. 233; TCK Madde Gerekçeleri, s. 220, Suçun yasal tanımında kayda alınmanın yöntemi belirtilmemektedir. Bu sebeple aracın teknolojik alet olup olmaması önemli değildir. https://docplayer.biz.tr/1257504-Turk-ceza-kanunu-madde-gerekceleri.html (E.T:05/01/2022).

[403] Korkmaz, s. 393; Koca ve Üzülmez, s. 78; Uğur Orhan, "Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:70, Sayı:4, 2021, s. 1371.

[404] https://shiftdelete.net/instagramdan-koleksiyonlar-ozelligi-81208 (E.T:13/12/2021).

veriler konusunda bahsettiğimiz temel ilkelerle uyumlu sonuçlar sağlamaya yöneliktir. Örneğin KVKK m. 4'te yer alan genel ilkelerden olan verilerin dürüstlük kuralına uygun olarak işlenmesi, veri işleme amacına bağlı olarak ölçülü bir şekilde verilerin işlenmesi gerekir. Bu genel ilkeler TCK m. 135 açısından KVKK m. 5'te yer alan hukuka uygunluk sebeplerinin uygulanmasında bizce dikkate alınması gereken hususlardır. Ayrıca KVKK hükümlerinin hukuka uygunluk sebebi sayılıp sayılamayacağı ya da şikayete tabi olmama sebebi ile rızanın hukuka uygunluk sebebi olup olmadığına yönelik tartışmalar bulunmaktadır. Bu hususu ilişkin açıklamaları ilgili kısımda yapacağız.

TCK m. 136 açısından verilerin hukuka uygun ya da hukuka aykırı olarak kaydedilmiş olması önem arz etmemektedir. Önemli olan aşağıda açıklayacağımız verme, yayma ya da ele geçirme fiillerinin hukuka uygunluk sebebi olmadan gerçekleştirilmesidir.

Vermek[405]: *"Kişisel verilerin bir başkasına sunulması, aktarılmasıdır."* Suçun tamamlanması için kişisel verinin bir başkası tarafından öğrenilebilir kılınması yeterlidir. Yapılacak aktarma işleminin yöntemi hakkında bir sınırlama yapılmamaktadır. Kişisel verileri başkasına verme birçok şekilde yapılabilir. Bu işlem elimizde bulunan teknolojik araçlarla, basit bir yazılı evrakla, sosyal medya araçlarından yapılabilecek paylaşım, mesajlarla ya da bulut bilişim sitemine yapılacak depolamalarla ve aktarmalarla mümkündür[406]. Yargıtay 12. Ceza Dairesinin 09/11/2016 tarihli bir kararında verme, yayma eyleminin gerçekleşebilmesi için bir verinin kaydedilmiş olmasını ya da ele geçirilmiş olmasını aramaktadır. Verinin defalarca kullanılabilmesini sağlayan işlemler kaydetme işlemi olarak kabul edilebilir.

Yaymak[407]: "*Verilerin içeriğinin birçok kişinin öğrenebileceği bir araç vasıtası ile başkalarının bilgisine sunulmasıdır."* Yaymak eylemi birçok şekilde gerçekleşebilir. Kişiler internet ve basın aracılığıyla, cep telefonu, mail gibi farklı yöntemlerle bu yayma eylemini gerçekleştirebilir. Yayma eylemi ile vermek eylemi arasındaki ayrım kişisel verileri ulaştırdıkları kişi sayısına bakılarak yapılmaktadır.

---

[405] Handan Yokuş Sevük, **Türk Ceza Hukuku Özel Hükümler**, Güncellenmiş 2. Baskı, Adalet Yayınevi, Ankara, 2019, s. 279.
[406] Sınar, 42.
[407] Yokuş Sevük, s. 279.

Verme eyleminde genellikle bir kişiye ulaştırılma söz konusu olabilecekken yayma eylemi birden çok kişiye ulaştırmayı hedeflemek söz konusudur[408]. Örneğin bir kişisel verinin mail ortamında başka birisine aktarılması verme ancak bu sosyal medyada paylaşılması yayma fiili olarak kabul edilebilir[409]. Vermek ve yaymak seçimlik hareketlerinin her ikisi de olmuşsa tek suç oluşmuş sayılmalıdır. Ayrıca yaymanın vermeyi de kapsadığı durumlar olabilecektir. Özbek, Koray ve Bacaksız'a göre vermek ile yaymak konusunda dikkat edilecek iki önemli husus vardır. İlk husus verinin yayma niteliği taşımayacak şekilde başkasına aktarılmasının verme kabul edileceğidir. İkincisi ise bu seçimlik hareketlerin bir araç ile yapılması gerektiğidir. Araç kullanılmadığı takdirde örneğin kulaktan kulağa aktarma eyleminin bu madde kapsamında verme ya da yayma eylemi olarak kabulü mümkün değildir[410].

Kişisel verilere ilişkin sözlü paylaşımlar TCK m. 135 kapsamında veri kaydetme ya da Kişisel Verilerin Korunması Kanunu kapsamındaki veri işleme olarak kabul edilmemektedir. Sözlü paylaşımların TCK m. 136 kapsamında değerlendirilmemesi halinde bu eylemlerin cezasız kalması ihtimali söz konusu olduğunu düşünülmektedir. Bu hususa örnek olarak bir kişinin patronu hakkındaki kişisel veriyi sözlü olarak bir arkadaşına aktarması halinde bu hareket duyu organları nedeni ile olduğu için TCK m. 136 kapsamında değerlendirilmeyecektir. Ancak aynı kişi bu aktarmayı yazılı olarak bir mesaj ya da sosyal medya uygulamasında herkese açık olamayacak şekilde yine aynı arkadaşı ile paylaşacak olsa TCK m. 136'nın oluştuğu söylenebilecektir[411]. Kanaatimizce bu görüşe katılmak mümkün değildir. KVKK mevzuatı, TCK m. 135 ve 136 esasen dijital bir sistemlerde olan ya da fiziki olarak yazılı işlemler sonucu ihtiyaç duyulan yasal düzenlemeler olmuştur. Söz konusu yasal düzenlemelerin ortaya çıkışı internet ve sosyal medya ile olmuştur. Basit bir sözlü aktarımı korumak için özel hayata ilişkin ve tazminat hukukuna ilişkin diğer düzenlemeler yeterli cezai ve hukuki sonuçların ortaya çıkmasını sağlamaktadır. Bu sebeple kanımızca de kulaktan kulağa aktarılan bir kişisel verinin TCK m. 136 kapsamında değerlendirilmemesi gerekir. Yargıtay'ın bir kararında da

[408] Yokuş Sevük, s. 279; İtişgen, s. 188.
[409] İtişgen s. 188.
[410] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, **Türk Ceza Hukuku Özel Hükümler**, 16. Baskı, Seçkin Yayıncılık, Ankara, 2021, (Özel Hükümler), s. 592.
[411] Eşref Barış Börekçi, **Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu**, (Yayınlanmamış Yüksek Lisans Tezi) Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019, s. 61.

bu yönde bir değerlendirme yapılmaktadır. Kararlara göre kişilerin, duyu organları ile öğrendiği bilgi ve verileri aklında tutup bir başkasına bunları açıklaması halinde TCK m. 135 ve m. 136 değil de TCK m. 134/1'de bulunan suç tipi dikkate alınmalıdır. Görüldüğü üzere Yargıtay böyle durumlarda özel hayatın gizliliğine ilişkin TCK m. 134 hükümlerine gitme eğilimindedir[412].

Ele geçirmek: Kişisel verilerin ele geçirilmesi mağdura ait kişisel verilerin failin kendi egemenlik alanına dahil edilmesi ya da bu verilerin faile aktarılmasıdır. Ele geçirmek verme ya da yayma eylemlerinden farklı olarak üçüncü bir kişiye veri aktarımı sağlama işlemi değildir. Ele geçirmek, kişilerin tasarruf yetkilerinin olmadığı bir kişisel veriyi üzerinde tasarruf edebilecek şekilde elde etmesidir.

Kişisel verilerin kaydedilmesi TCK m. 135'teki suç tipi ile kişisel verilerin hukuka aykırı olarak verilmesi ve ele geçirilmesine ilişkin suç tipinin her ikisinin de söz konusu olabileceği durumlar olabilir. Fail önce kişiye ilişkin kişisel bilgiyi kaydeder daha sonra yayabilir. Bu durum için öğretide farklı görüşler bulunmaktadır. Bir görüşe göre kişisel verilerin kaydedilmesi zaten TCK m. 136'da yer alan kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu için gereken bir durumdur. Kaydedilme suçu oluşmadan diğer suç tipi oluşmayacağından TCK m. 135 bu durumda geçit suç niteliğindedir[413]. TCK açısından kişisel verileri verme ya da ele geçirmeye konu olacak verinin hukuka uygun ya da hukuka aykırı olarak ulaşılmış olması hususu değerlendirmemiştir. Bu sebeple TCK m. 136'nın oluştuğu bir durumunda kişisel verinin hukuka uygun olarak kaydedilmesi halinde TCK m. 135'in oluşacağını söylemek çok mümkün değildir[414]. Başka bir görüşe göre her iki suçtan da ceza verilmesi gereklidir[415]. Bir diğer görüş ise ele geçirme fiiline odaklanmaktadır. Ele geçirme eylemi kaydetme ile gerçekleşirse yalnızca TCK m. 135 uygulanacak ile kaydetme dışındaki ele geçirme eylemi için ise TCK m. 136 uygulanacaktır[416]. Örneğin hukuka aykırı bir şekilde elde edilen yani ele geçirilen bir

---

[412] Yargıtay, 12. CD, 2017/3928 E. 2018/3190 K. 21/03/2018 T.; Yargıtay. 12. CD, 2016/2168 E. 2016/5860 K. 06/04/2016 T; Yargıtay 12. CD 2015/9893 E. 2016/12504 K. 09/11/2016 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:19/12/2021).

[413] Murat Volkan Dülger, **Bilişim Suçları**, Seçkin Yayıncılık, Ankara, 2004. s. 280 (Bilişim Suçları); Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, Yetkin Yayıncılık, Ankara 2010, s. 348.

[414] Yaşar, Gökcan, Artuç, s. 4126; İsmail Malkoç, **Açıklamalı Türk Ceza Kanunu**, Cilt II, Malkoç Kitabevi, 2013, s. 2201; İtişgen, s. 197.

[415] Soyaslan, s. 346.

[416] Özbek, Doğan, Bacaksız, s. 592.

veri henüz kaydedilmemişse yalnızca TCK m. 136'da yer alan ele geçirme fiili gerçekleştirildiği için yalnızca TCK m. 136 hükmü uygulama alanı bulacaktır[417].

Yargıtay kararına konu olan bir olayda sanık, eşiyle ve eşinin bir iş arkadaşının birlikte günlük kıyafetlerle çekildikleri ve sosyal medyada kendi hesaplarında paylaştıkları bu fotoğrafları aralarında duygusal bir ilişki varmış gibi gösterecek şekilde slaytlar hazırlayarak youtube gibi mecralarda yayınlamıştır. Yargıtay ilk derece mahkemesi tarafından özel hayatın gizliliğine ilişkin yapılan değerlendirmeyi uygun bulmamıştır. Yargıtay'a göre katılanlar kendileri internet ortamında bu resimleri yayınlamıştır. Resimler kamuya açık alanlarda günlük kıyafetleriyle poz verilmiş şekilde çektirilmiştir. Yani mahrem olan özel yaşam alanları olan görüntüler değildir. Ancak sanık tarafından bu resimler katılanların hesaplarından elde edilmiştir. Bu resimlerin ele geçirilip youtube da farklı içerikler oluşturularak paylaşılması söz konusudur. Bu sebeple Yargıtay, resimlerin sanık tarafından sosyal medya hesaplarında hukuka aykırı bir şekilde paylaşıldığı konusunda tartışmanın olmadığı ve bu sebeple TCK m. 136/1'in oluşmuş olduğu tespitini yapmıştır[418].

Ele geçirme konusunda örnek verilebilecek durumlardan biri de kişilerin sosyal medya hesaplarının çalınmasıdır. Phishing saldırıları (Sazan Avlama) adı verilen ve kişilerin mail hesaplarına atılan mailler ya da sosyal medya hesaplarına atılan mesajlardaki linkler yoluyla kişilerin bu hesaplarının ya da kişisel verilerinin çalınmasıdır. Bu saldırılarda kurumsal hesaplardan gelmiş gibi görünen mesajlar atılmakta ve kişiler gönderilen linke tıkladıklarında hesapları çalınmış olmaktadır. Phishing saldırıları hem en eski hem de hala en etkili yöntemlerdendir[419]. Phishing ile mağdur aldatılarak verileri ele geçirilmektedir. Bu sebeple TCK m.243'te yer alan bilişim sistemine girme suçu olarak değerlendirilmez[420]. Kanımızca bu yöntemle sosyal medya hesaplarını ele geçirilmesi TCK m. 136 kapsamında değerlendirilmelidir. Kullanıcıya gönderilen linkler kişinin rızası dışında bir işlem

[417] Özbek, Doğan, Bacaksız, s. 581.
[418] Yargıtay 12. CD. 2015/11703 E. 2017/870 K. 08/02/2017 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:01/02/2022).
[419] Akbulut, Bilişim Alanında Suçlar, s. 86.
[420] Akbulut, Bilişim Alanında Suçlar, s. 131.

oluşturarak verilerinin ve hesabının ele geçirilmesine yol açmaktadır. Kullanıcının rızası dışında hukuka aykırı olarak verilerinin ele geçirildiği kabul edilebilir.

Yargıtay, bir gazetecinin *"kamu yararı bulunmadığı ve hiç gerekmediği halde"* mağdurun kimlik bilgilerini ve adresi gibi kişisel verilerini içeren savcılığa sunulan şikayet dilekçesini twitter hesabında paylaşması üzerine TCK m. 136/1'de yer alan suçun işlenmiş olduğuna hükmetmiş ve ilk derece tarafından verilen beraat kararını bozmuştur[421].

b. Kişisel Verilerin Kaydedilmesi, Kişisel Verileri Verme, Yayma ve Ele Geçirme Suçlarının Manevi Unsuru

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu kasten işlenebilen bir suçtur. Fail kaydettiği verilerin başkasında ait olduğunu biliyor olmalıdır. Daha doğrusu kişisel verileri konu alan bu suç tipinde yer alan gerçek kişiye ait olan ve kişinin şahsı bakımından önem arz eden bir veri olduğu bilmesi gerekir. Yoksa doğrudan hukuken kişisel veri niteliğinde kabul edildiğini tespit etmiş olması beklenmez. Madde metninde dikkat çeken önemli husus açıkça hukuka aykırılık ifadesinin olmasıdır. Doktrinde bir görüşe göre hukuka aykırı olarak kişisel verilerin kaydedilmesi ibaresinde hukuka aykırılık manevi unsurla ilgili değildir. Yani bu ifade, kasıt ve manevi unsur konusu ile değil de kusurluluk konusunun işlendiği hukuka aykırılık unsuru ile değerlendirilecektir. Esasen bu ibare hakimler için uyarı fonksiyonu göstermektedir[422].

TCK m. 136'da yer alan kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu da kasten işlenebilen bir suçtur. Fail mağdura ait verileri yaydığını, verdiğini ya da ele geçirdiğini biliyorsa suçun oluşması için yeterli olacaktır. Ayrıca özel bir saik ya da amaç aranmaz. Ancak öğretide doğrudan kast haricinde bu suçun olası kastla da işlenebileceğine dair görüşler bulunmaktadır[423].

[421]Yargıtay 12. Ceza Dairesi 2018/8139 E. 2019/4827 K. 10/04/2019 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:09/01/2022).
[422] Koca ve Üzülmez s. 81.
[423] Sınar, s. 52.

Özbek, Doğan ve Bacaksız'a göre bu suç kasten işlenebilen bir suç olduğu için olası kastla da işlenebilecektir[424].

Yargıtay bazı kararlarında failin kastını değerlendirmeye çalışmaktadır. 2015 tarihli bir Yargıtay kararında hukuka uygunluğa ilişkin sebeplerinin sadece ceza hukukunda değil hukukun tümünde aranması gerektiğinin ve somut olayda sanığın hukuka aykırı davrandığının bilincinde olmadığının tespitini yapmıştır. İlgili karara esas olan olay sanık tarafından katılana ait olan whatsapp profil fotoğrafının kaydedilmesi ve sonrasında da bu fotoğrafın katılana gönderilmesi üzerine verilmiştir. Söz konusu fotoğraf kişinin whatsapp profilinde yer alan katılanın oğlunun fotoğrafıdır. Sanık, katılan ile eniştesinin birlikte olduğunu ve bu fotoğrafı teyzesinin boşanma davasında kullanmak için kaydettiğini belirtmektedir. Yargıtay tarafından yapılan incelemede TCK m. 136 açısından somut olayda failin kast ya da taksirinin bulunmadığı tespit edilmiştir[425]. Yargıtay, kişinin numarasını kaydedenlerin whatsapp özelliği olarak kişilerin profil fotoğrafını da rahatlıkla görebildiğinin tespitini yapmaktadır. Karar tarihi itibari ile hukuka uygunluk sebebi olan alenileştirmeye ilişkin KVKK düzenlemesi henüz yapılmamıştır. Doktrinde Yargıtay'ın bu kararındaki değerlendirmesinin aslında kasta yönelik değil de henüz yasal bir düzenlemesi yapılmamış olan alenileştirme hukuka uygunluk sebebine yönelik olduğunu düşünenler vardır[426].

c. Kişisel Verilerin Kaydedilmesi, Kişisel Verileri Verme, Yayma ve Ele Geçirme Suçlarının Hukuka Aykırılık Unsuru

Anayasa m. 20/3'ün üçüncü cümlesinde kişisel verilerin işlenmesi için *"ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla"* ifadesi kullanılmıştır. TCK m. 135 kişisel verilerin kaydedilmesi açısından da ancak bu iki halin hukuka uygunluk sebebi olduğu söylenebilecektir[427]. Öncelikle TCK genel hükümlerinde düzenlenmiş olan hukuka uygunluk sebepleri uygulama alanı

[424] Özbek, Doğan, Bacaksız, ss. 589, 594.
[425] Yargıtay 12. CD, 2015/3247 E. 2015/16760 K. 04/11/2015 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:09/01/2022).
[426] Börekçi, s. 72.
[427] Koca ve Üzülmez, s. 81.

bulacaktır. Kişisel verilere ilişkin düzenlemeler içeren diğer kanun olan Kişisel Verilerin Korunması Kanununda öngörülen hukuka uygunluk sebepleri uygulama alanı bulacaktır. Daha önce açıkladığımız üzere bizce KVKK'de yer alan hukuka uygunluk sebepleri uygulanırken KVKK m. 4'te yer alan genel ilkeler de dikkate alınmalıdır. Aksi takdirde KVKK'nin uygulanması gereken her durumda dikkate alınması gereken bu genel ilkeler göz ardı edilmiş olacak ve hukuka uygunluk sebepleri de amacına aykırı bir şekilde uygulanmış olacaktır.

TCK m. 135 ve m. 136 açısından TCK m. 24/1 hükmü gereği kanunun öngördüğü haller hukuka uygunluk sebeplerinin başında gelmektedir.

Sınar'a göre kişisel verilerin hukuka aykırı olarak kaydedilmesi, kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçlarında, TCK'da yer alan hukuka uygunluk nedenleri ile birlikte KVKK m. 5'te yer alan hukuka uygunluk nedenleri de uygulama alanı bulabilecektir. KVKK, TCK'dan sonra yürürlüğe gitmiştir. KVKK hükümleri ile kişisel verilerin korunması konusunda TCK genel hükümlerindeki hukuka uygunluk sebeplerine ek bazı koşulların ve sebeplerin öngörüldüğü belirlenebilir. Mevcut durumda TCK ile KVKK arasındaki ilişkiyi genel norm ve özel norm olarak değerlendiren görüşler bulunmaktadır[428].

TCK m. 24/1'e düzenlemesinde kanun hükmünü yerine getiren kişiye ceza verilmeyeceği hükmü yer almaktadır. Kanun hükmünün yerine getirilmesi kişisel verilerin kaydedilmesinde ya da başkasına verilmesinde yayılmasında veya ele geçirilmesinde bu fiiller için hukuka uygunluk sebebi sayılabilecektir. KVKK m. 5/1'de kişisel verilerin işlenmesi için açık rıza olması gerekirken m. 5/2'de açık rıza aranmayan hal düzenlenmiştir. Açık rıza kanunlarda açıkça öngörülen hallerde aranmayacaktır. Ayrıca özel nitelikli verilerin işlenmesine ilişkin düzenlemeyi içeren 6. maddenin 3. fıkrasında özel nitelikte veriler de açık rıza olmaksızın işlenebilir hale getirilmiştir. Madde de sağlık ve cinsel hayata ilişkin özel veriler ise bunun dışında tutulmuştur. Bir diğer önemli hüküm ise kişisel verilerin aktarılmasına ilişkin Kanunun 8. maddedir. Verilerin aktarılması da açık rızaya tabi olmakla birlikte m. 8/2'de açık rızaya gerek olmayan haller konusunda m. 5 ve m. 6/3'e gönderme yapmaktadır. Konumuz açsından sosyal medyada verilerin paylaşılması durumunda

[428] Sınar, s. 54.

hassas verileri içeren bir paylaşım olması sadece rıza ile paylaşılması değil ayrıca hassas veriler konusunda yeterli önlemlerin alınması halinde veri işleme hukuka uygun olacaktır. KVKK'de hem özel nitelikte verilerin işlenmesini düzenleyen m.6/4'te hem de özel nitelikte kişisel verilerin aktarılmasında açık rızaya gerek olmayan hallere değinen m.8/2-b'de "yeterli önlemlerin" alınması ifadesi kullanılmıştır. Bu ifade belirsiz olmakla birlikte hassas veriler söz konusu olduğunda ek önlemlerin alınması gerektiğini ifade eden bir düzenlemedir[429].

KVKK m. 5'te TCK hükümlerinde karşılığı doğrudan karşılığı olmayan ama TCK m. 135 ve m. 136 açısından uygulanabilirliği değerlendirilebilecek iki kavram bulunmaktadır. Bu kavramlardan ilki alenileştirme ikincisi ise meşru menfaattir[430].

Koca ve Üzülmez'e göre KVKK m.5/2-d bendinde yer alan aleniyet kavramı kişisel verilerin kaydedilmesine dair kişinin rızası olmasa bile hukuka uygunluk sebebi teşkil eder. Şöyle ki kişinin bizzat kendisinin aleni hale getirdiği veriler varsa artık bu verilerin kaydedilmesine dair rızası aranmamalıdır ve TCK m. 135'teki suç tipi oluşmamaktadır. Kişiler kendilerine ait kişisel verilerini dijital mecralarda ve sosyal medya platformlarında yayınlamışsa artık bu verilerinin başkaları tarafından kaydedilmesi, açıklanması ya da elde edilmesi gibi hallerde TCK m. 135 veya m. 136 hükümlerinde yer alan suç tipleri oluşmayacaktır. Bu durumlarda kişinin kendisine ilişkin mahremiyetini bizzat kendisinin kaldırdığı ve de hukuki ve cezai korumalardan vazgeçtiği düşünülmektedir. KVKK mevzuatında da bu görüş neticesinde m.28/2-b bendi uyarınca ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi konusunda Kanunun 10, 11 ve 16. maddelerinin uygulanmayacağı hükmüne yer verilmiştir[431]. Açıkçası doktrindeki görüşler kişisel verilerin kendisi aleni hale getirenlerin tüm haklarından vazgeçmiş gibi bir tablo çizilmektedir. İlgili kanunun 10. maddesi aydınlatma yükümlülüğüne 11. maddesi ise kişinin haklarına ilişkindir. Madde metninde açıkça "zararın giderilmesini talep etme hakkı hariç" tutulduğu belirtilmiştir. Kişinin tazminat hakkı saklı tutulduğu bir durumda cezai korumalardan vazgeçtiğini söylemek kanımızca mümkün değildir. Kişinin maddi ve manevi zararlarla kaşı karşıya kalması mümkünken bunun cezai bir

[429] Atasoy, ss. 287-288.
[430] Sınar, ss. 54-56.
[431] Koca ve Üzülmez, s. 83.

karşılığının olmayacak olması hakkaniyetli bir durum olarak görünmemektedir. Ayrıca mağdur tarafından kişisel verilerin alenileştirilmesinde ya da açık rıza vermesinde belli bir amaç bulunmaktadır. KVKK genel ilkelerinde yer alan amaca bağlılık ilkesi gereği verisini alenileştiren ya da işlenmesine açık rıza gösteren ilgilinin amacının tespit edilmesi gerekir.

Sosyal medya konusunda kanunda öngörülen hallerden en önemlisi aleniyet olarak kabul edilebilir[432]. Ceza hukuku açısından net bir tanımı yapılmayan aleniyet genellikle herkesin vakıf olabileceği şekilde kamuya açık olma anlamına gelmektedir. TCK'da aleni ifadesini suç tipinde ya da nitelikli halinde içeren birçok suç bulunmaktadır. Örneğin bir sosyal medya paylaşım sitesinde yapılan intihara yönlendiren mesajlar içeren bir paylaşımın intihara alenen teşvik bu suç tipini oluşturacağı düşünülmektedir. Hakaret suçunun alenen işlenmesi de TCK'da yer alan başka bir düzenleme örneğidir. Sosyal medyada çocukların da girip ulaşabileceği şekilde müstehcen görüntülerin paylaşılması halinde de m. 226/1-b fıkrasında yer alan aleniyetin sağlandığı kabul edilmektedir. Söz konusu suç tipleri için yapılan değerlendirmelerde aleniyet hususu ile kastedilenin *"belirsiz ve çok sayıda kişi tarafından hakaretin öğrenilmesinin mümkün kılınacak şekilde*" yapılmış olunmasıdır. İnternet ortamı dikkate alındığında bu ortamda özel bir kullanıcı adı ya da şifre gerektirmeyen ve herkesçe ulaşılabilen bir platform söz konusu ise aleniyetin gerçekleşmiş olacağı kabul edilebilecektir[433]. Bu düşünceden yola çıkıldığında sosyal medyanın bir kullanıcı adı ve şifre ile profil oluşturularak girilen bir platform olduğu görülmekle birlikte herkese açık paylaşım yapan kişilerin paylaşımlarının kullanıcı olamayan kişilerce de görülebildiği, ekran görüntüsü ya da fotoğrafı alınarak kaydedilebildiği bir ortam olduğunu söylemek mümkün olacaktır. Bu sebeple kişilerin bizzat kendi rızaları ile herkese açık şekilde paylaştıkları verileri bizzat kendileri tarafından alenileştirdiklerinin kabulü gerekebilir. Ancak verileri üzerinde yapılabilecek her türlü işleme rıza gösterdikleri söylenemeyecektir.

Yargıtay 12. Ceza Dairesinin bir kararında normalde profili herkese açık olmayan bir sosyal medya kullanıcısının herkes tarafından görülebilen tek

[432] Börekçi, s. 92; Korkmaz, s. 407.
[433] Fehmi Şener Gülseren, "Ceza Hukukunda Aleniyet Kavramı" **LAÜ Sosyal Bilimler Dergisi**, Haziran 2014, ss. 33, 36, 38, 41.

fotoğrafının profil fotoğrafı olduğu bir olayı incelemiştir. Katılan beyanında özellikle arkadaşları haricindeki kimseler için korumalı bir hesap kullandığını belirtmektedir. Daire söz konusu olayda kişisel verilerin kaydedilmesi değil de kişisel verileri verme veya ele geçirme suçunun değerlendirilmesi gerektiğini ancak herkese açık profil bu fotoğrafın kaydedilip başka bir facebook hesabında kullanılması olayında suç oluşmadığı ve TCK m. 136 açısından beraat kararının onaylandığı görülmüştür. Kararda, kişinin fotoğrafının kimlik bilgileri ile paylaşılmadığı müddetçe TCK açısından bu fiilin suç olarak kabul edilmeyeceği ancak istenirse hukuki sorumluluğa ilişkin hükümlere başvurulabileceği düşüncesine yer verilmiştir[434]. İlgili karara muhalefet şerhi koyan üye ise bu eylemin TCK m. 136'da yer alan suç tipine uygun olduğunu ve mahkumiyet kararı verilmesi gerektiğini ifade etmiştir. Üye gerekçesinde kişinin fotoğraflarının kişisel veri olduğunu hususunda bir tartışma bulunmadığını ve fotoğrafların *"kişi hakkında bir sayfada yapılacak anlatımı ve tarifi tek bir karede ifade edebilme özelliğine"* sahip olduğunu belirtmiştir. Somut olayda sanığın eyleminin hukuka aykırı olarak yayma olduğu görülmektedir. TCK m. 136 kişisel verinin yayılması durumunda kişisel verinin nasıl elde edildiği ile ilgilenmemektedir. Sonuç olarak sanığın sahte bir hesaptan mağdurun fotoğrafını paylaşması haklı ve hukuka uygun değildir[435]. Sanığın aleni hale getirdiği fotoğrafı sosyal medya da kendisine ulaşmak isteyenlerin kendisini tanımasına yöneliktir. Profil fotoğraflarının niteliği ve amacı da budur. Yani ilgilinin ceza hukuku açısından mağdurun verisini alenileştirme amacı bellidir. Verilerinin bir başkası tarafından yayılması alenileştirme amacına aykırıdır.

Kişisel verilerin korunması hukuku açısından alenileştirilen verilerin işlenmesinde alenileştirme amacı dikkate alınmaktadır. Örneğin kişi iletişim bilgilerini araç satmak ya da bir ürünün kendisine ulaştırılmasını sağlamak amacıyla alenileştirdiğinde bu iletişim bilgilerinin başka amaçlarla kullanılması halinde alenileştirilmiş olsa bile verilerin işlenmesini hukuka aykırı hale getirmektedir[436].

---

[434] *"...sadece başka bir facebook profilinde yayınlanması eyleminin suç olarak kabul edilemeyeceği, bu eylemlerin yalnızca özel hukuk yaptırımlarına konu olabileceği göz önüne alındığında mahkemece sanık hakkında beraat kararı verilmesinde bir isabetsizlik görülmemiş…"* Ali Fuat Özbakır, **Sosyal Medyada ve İnternette Hukuki Sorumluluk**, Adalet Yayınevi, Ankara, 2019, ss. 242-243.

[435] Yargıtay 12. Ceza Dairesi, 2015/4349 E. 2016/5349 K. 30/03/2016 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:22/01/2022).

[436] Öztürk, Altınok Çalışkan, Seyhan, s. 67.

Açıklanan sebeplerle TCK açısından hukuka uygunluk sebebi olarak alenileştirmenin kullanılması halinde "alenileştirme amacı" dikkate alınması bir gerekliliktir. Özellikle sosyal medyada herkese açık bir şekilde fotoğraf paylaşılması bu fotoğrafın kaydedilmesi özellikle yukarıda belirttiğimiz şekillerdeki gibi uygulama içi özelliklerle yapıldığında hukuka uygunluk sebebi olabilecektir. Aynı zamanda kullanıcıların fotoğraflarında üzerinde taşıdığı bir kıyafetin reklamını yaptığı açıkça anlaşılır şekilde olması durumunda alenileştirme amacının bu yönde olduğu görülebilmektedir. Alenileştirilen verilerin alenileştirilmesi amacı dışında işlenmesi ya da aktarılması hukuka uygunluk sebebi olmayacak TCK m. 135 ve m. 136'da düzenlenmiş olan suç tiplerini oluşturabilecektir. Kanımızca ancak bahsettiğimiz hususlar dikkate alınarak hukuka uygunluk sebebi olarak KVKK m.5/2 gereğince TCK m. 135 hususunda ve de KVKK m. 8/2'nin yönlendirmesi sayesinde m. 5/2 gereğince yine TCK m. 136 da uygulama alanı bulabilecektir.

TCK m. 139 hükmü gereğince özel hayata ve hayatın gizli alanına karşı suçlar başlığı altında yer alan suç tipleri şikayete bağlı iken kişisel verilerine ilişkin olan hükümler şikayete bağlı değildir. Söz konusu suç tiplerinin şikayete bağlı olmaması rızanın hukuka uygunluk sebebi sayılıp sayılamayacağı konusunda tartışmaları beraberinde getirmiştir. Çünkü Özbek, Doğan ve Bacaksız'a göre rıza hukuka uygunluk sebebi olarak kabul edebilmemiz için kişinin iradesine bağlı durumlar olmalıdır. Şikayete bağlı olduğu kabul edilmeyen suç tiplerinde de kamu menfaati ağır bastığı için rıza ile eylemin hukuka uygun hale gelmediği düşünülmektedir. TCK m. 26 hükmünde yer alan ilgilinin rızası hukuka uygunluk sebebi değil de kanun hükmünün uygulanması hukuka uygunluk sebebi hükmü dikkate alınacaktır. Yargıtay kararları ve öğretide kişisel verileri konusunda rızanın hukuka uygunluk sebebi olduğu düşünülmektedir. Aksi halde Anayasa m. 20 ve Kişisel Verilerin Korunması Kanunu m. 5/1 hükmü ile çelişkili bir durum oluşmaktadır[437]. Bu konuda Koca ve Üzülmez suç tipinin şikayete tabi olmamasının TCK m. 26 "ilgilinin rızası" hukuka uygunluk sebebinin uygulanmasına engel olmadığını düşünmektedir. Hatta yazarlara göre Anayasa'da m. 20 kişilerin kişisel verileri üzerinde nasıl tasarrufta bulunabileceği konusunda düzenleme yer almasa

[437] Özbek, Doğan, Bacaksız, Özel Hükümler, ss. 589, 594.

veya bu hakların mutlak surette tasarruf edilebilir haklardan olduğu belirtilmemiş olsa bile rıza bu suç tipinde hukuka uygunluk hali oluşturacaktır[438].

TCK m. 135'te yer alan kaydetme fillinin hukuka aykırılık tespit edilirken daha önce bahsettiğimiz şekilde Kişisel Verilerin Korunması Kanunun 5. maddesinde olan veri işlemeye ilişkin hükümlere dikkat edilecektir[439]. Maddenin gerekçesinde, ilgilinin rızası sonucunda yapılmış bir kaydetme işleminin suç teşkil etmeyeceği belirtilmektedir[440]. İlgilinin rızası bu suç tipi açısından hukuka uygunluk sebebi kabul edilirse TCK m. 26/2 hükmünün yanında Anayasa m. 20/3'te ve de KVKK m. 5/1'de ilgilinin rızasının nasıl olması gerektiğine ilişkin hükümler dikkate alınacaktır. Bu hükümlere göre ilgilinin açık rızası ile kişisel veriler kaydedilir. Açık rızanın KVKK m. 3/1-a'da, rızanın alınacağı konunun belli olması, ilgilinin bu konu hakkında bilgilendirilmesi ve bunun sonucunda ilgilinin herhangi bir etki altında olmadan rızasını açıklaması olarak tanımlanmıştır. Açık rızaya dayılı kişisel verilerin kaydedilmesi işlemi hukuka aykırı olmayacaktır. Açık rıza değil de zımni rızayı yeterli görülmesi gibi bir ihtimalde TCK m. 30/1-3 düzenlemesi kapsamında hukuka uygunluk sebeplerinin maddi şartlarında hata hükümleri değerlendirilmelidir[441].

Hata konusu bu suç tipleri için önem arz etmektedir. Suç tipinin yeni olmasından dolayı vatandaşların gerçekleştirdiklerin suç oluşturup oluşturmadığı konusunda hataya düşmeleri ihtimali vardır. Kişisel veriler konusunun yeni yeni Yargıtay Ceza Genel Kurulu'nun önüne geldiği ve YCGK'nin bu konuda verdiği ilk kararlardan olması dolayısıyla da hukuka aykırılık konusu ve hata konusunda önemli açıklamalara yer verilmiştir. Failin işlediği fiilin haksızlık oluşturduğu konusunda kaçınılmaz bir hataya düşmesi gerekir. Failin cezalandırılmaması için gerçekten eyleminin bir hukuka aykırılığa meydan vermediğini, yaşamı algısı ve şartlarının da faili bu şekilde düşünmeye sevk ettiğini düşündürmelidir. Açıkçası fail eyleminin hukuka uygun olduğu hususunda kaçınılmaz bir şekilde yanılgıya düşmelidir. Yargıtay kararına esas olan somut olayda şikayette bulunmak ve muhtemel idari bir soruşturma için şikayet dilekçelerinin ekinde sunmak amacıyla özel bir hastaneden

[438] Koca ve Üzülmez, ss. 85-86; Orhan, s. 1375.
[439]Yokuş Sevük, ss. 273-274.
[440] Türk Ceza Kanunu Madde Gerekçeleri, s. 220, https://docplayer.biz.tr/1257504-Turk-ceza-kanunu-madde-gerekceleri.html (E.T:05/01/2022)
[441] Koca ve Üzülmez, s. 86.

doğum belgesi temin edilmiştir. Sanıklar temin işlemi sırasında özel hastanenin kendilerine belgeyi normal bir şekilde temin ettiğini herhangi bir kimlik bilgisi dahi istemediği, kendilerinin de belgeyi yalnızca idari soruşturma için idareye teslim ettiklerini başka herhangi bir amaçla kullanmadıklarını ve yaymadıklarını ifade etmişlerdir. Genel Kurul, sanıklardan birinin memur diğerinin de sağlık çalışanı olması sebebi ile sanıkların doğum belgesinin kişisel veri niteliğini ve eylemlerinin hukuka aykırı olduğunu bilebilecek durumda olmalarını dayanak göstererek hata hükümlerini uygulamamıştır. Ancak Genel Kurul Kararına katılmayan bir üye sanıkların eylemlerinin haksızlık oluşturduğunun farkında olmadıklarını üstelik Genel Kurulun önüne dahi kişisel veriler konusunda bir olayın Türk Hukuk Tarihinde ilk defa geldiğini ve öğretide bu suç tiplerine ilişkin hususta fikir birliğinin de olmadığını belirterek sanıklar hakkında TCK m. 30/4 hata hükümlerinin uygulanmasının gerektiği yönünde karşı oy gerekçesi sunmuştur[442].

Kanımızca TCK m. 136 açısından rıza konusu biraz farklıdır. Fail tarafından verilmiş ya da yayılmış olan kişisel verilerin failin elinde nasıl bulunduğu önem arz etmemektedir. Daha önce de bahsettiğimiz üzere buraya kadarki kısımda olan hukuka aykırılık ya da uygunluk TCK m. 136 açısından araştırılmaz. Hukuka aykırılık verme, yayma ya da ele geçirme fiillerinde aranacaktır. Örneğin sosyal medyada herkese açık şekilde paylaşılan bir fotoğrafın kaydedilmesi ve izin verilen kişilerce görülmesi mümkündür. Ancak paylaşım yapılması bu fotoğrafın başkaları tarafından da yayılması ve paylaşılmasına verilen bir rıza değildir. Bir Yargıtay kararında kişinin daha önce sosyal medya hesabında paylaştığı resimlerin fail tarafından aynı kişi adına sahte bir hesap açılarak bu hesaptan paylaşılması TCK m. 136 kapsamında değerlendirilmektedir. Yargıtay somut olayda sanığın kendi sosyal medya hesabından mağdurun rızası ile paylaştığı fotoğrafları daha sonra mağdurla olan tartıştıktan sonra sahte bir hesapta paylaşmasını üzerine TCK m. 136'nın oluştuğuna hükmetmiştir. Katılanın sanıkla olan fotoğrafları kişisel veridir ve bu fotoğrafların daha önce yayınlanmış olması onların kişisel veri niteliğini kaybetmesine sebep olmayacaktır. Sanık kendisi daha önce katılanın rızası ile bu

[442] Yargıtay Ceza Genel Kurulu 2012/1514 E. 2014/312 K. 10/06/2014 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:30/12/2021).

fotoğrafları paylaşmış olsa dahi daha sonra rıza almadan aynı fotoğrafları yayamaz[443].

Başka bir Yargıtay Kararında da twitter üzerinden mağdur tarafından paylaşılan fotoğrafın sanık tarafından da paylaşılması durumunda ilk derece mahkemesince özel hayatın gizliliğinin ihlali hususu incelenmiş ancak mağdurun kendi rızası ile bu resmi yayınladığından bahisle beraat kararı vermiştir. Yargıtay ilk derece mahkemesinin kararının şu gerekçesini *"...katılanın bahse konu fotoğrafının herkese açık şekilde sosyal paylaşım sitesindeki sayfasında paylaştığı, katılanın herhangi bir kısıtlama yapmaması nedeniyle bu şekilde paylaştığı fotoğrafının başkaları tarafından görülmesinden ve paylaşılmasından rahatsızlık duymadığı, bu nedenle bahse konu fotoğrafın alınmasının ve yorum yapılmasının yüklenen suçu oluşturmayacağı..."* yanlış bulmuştur. Yargıtay Ceza Dairesine göre bu fotoğrafın özel yaşama ilişkin olmadığı söylenebilse de kişisel veri olmayacağı söylenemez. Kişisel veri nitelindeki fotoğrafın sanık tarafından yayınlanma biçiminin hukuka aykırı olduğu açıktır[444].

Kullanıcının herkese açık hesabında kişisel verileri olan ismini, resmini, kimlik bilgilerini ya da cep telefonu bilgilerini paylaşmış olması durumunda bunların kaydedilmesi TCK m. 135'te yer alan suç tipini oluşturmayacaktır. Ancak verilen rıza bu kişisel bilgilerin yayılmasını kapsamamaktadır. Böyle bir durumda sosyal medya da herkese açık bir şekilde paylaşılan verilerin kaydedilmesi bir suç değilken bu verilerin yayılmaya çalışılması durumunda bunun TCK m. 136'nın oluşmasına sebebiyet verebileceği değerlendirilmelidir[445].

Rızaya konusunda Yargıtay, önceden verilen rızanın sonradan kalkması halinde verilerin paylaşılmaya devam edilmesinin hukuka aykırılık oluşturduğunu belirtmektedir. Somut olayda günlük kıyafetlerle birbirlerine sarılarak fotoğraf çekilmiş olan sanık ve katılanın önce bu fotoğrafları sanığın sosyal medya hesabından paylaştıkları görülmektedir. Ancak daha sonra ilişkileri sonlanmış ve katılanın rızası dahilinde paylaşılmış olan fotoğrafların sanık tarafından sosyal

[443] Sınar, s. 46; Yargıtay 12. CD. 2017/2960 E. 2018/1541 K. 14/02/2018 T.
[444] Yargıtay 12. Ceza Dairesi 2020/2426 E. 2021/6589 K. 06/10/2021 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:03/01/2022).
[445] Gürkan Özocak, "Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti", s. 9, http://ozocak.com/Dosyalar/a104b3.pdf (E.T:13/01/2022).

medya hesabından kaldırılması istenmiştir. Yargıtay, özel yaşamın gizliliğine ilişkin olmayan fotoğrafların sanık tarafından mağdurun rızasına aykırı olarak yayınlanmaya devam edilmesinin TCK m. 136/1 hükmü gereği kişisel verileri hukuka aykırı olarak yayma suçundan ceza verilmesi gerektirdiğine hükmetmiştir[446].

Bir diğer hukuka uygunluk sebebi olan basının haber verme hakkı TCK m. 26/1 düzenlemesi kapsamında değerlendirilebilir. Kişisel verileri ele geçirme, verme ve yaymanın basının haber verme hakkı kapsamında hukuka uygunluk sebebi sayılabilmesi mümkündür. Ancak şu hususlara uygun şekilde haber verme hakkının kullanılması gerekir. Bir kişiye ait kişisel verileri yayabilmesi için ilgili haber gerçek, güncel olmalı, haberin yayınlanmasında kamu yararı bulunmalı, konu ile ifade arasında düşünsel bağlılık olmalıdır. Haberin bu özellikleri taşımaması halinde bir kişinin resmi, görüntüsü, sağlık durumu gibi kişisel verilerini basın yayın araçları ile deşifre edilirse yapılan fiil hukuka aykırı olacaktır. Örneğin AIDS hastası olan birinin tek başına bu sağlık bilgisinin açıklanmasında kamu yararı bulunmamaktadır. Ama başkalarının sağlığının tehlikeye düşüren belli bir durum nedeniyle ve uyarı amacıyla kişinin sağlık bilgisinin açıklanmasında kamu yararı bulunabilir. Tanınmış olan kişilere ait bilgilerin kamu yararı olması halinde açıklanması da hukuka uygunluk sebebi arz edebilecektir. Kişinin konumu ve tanınmışlığı gibi özellikleri de haberde kamu yararının olması konusunda yapılacak tespitte önemlidir[447].

Kişisel Verileri Koruma Kanunun 28. maddesinde bazı istisnalara yer verilmiştir. Bu haller olduğu zaman KVKK hükümleri uygulanmayacaktır. Ancak 28. maddede sayılan istisnalar ceza hukuku açısından doğrudan hukuka uygunluk sebebi olarak kabul edilmemelidir. Özel hukuk uyuşmazlıklarına ilişkin yargılamalarda da mahkemelerin 28. maddeyi dar yorumla uyguladıkları görülmektedir[448].

Daha önce bahsettiğimiz üzere instagramda yer alan koleksiyona kaydet özelliği ile kullanıcıların gönderileri instagram bünyesinde kaydetmeleri kanımızca hukuka uygunluk sebebi oluşturmaktadır. Çünkü kullanıcılar instagram özelliklerini kabul ederek bu sosyal medya uygulamasını kullanmaktadırlar. Dolayısıyla bu

[446] 12. Ceza Dairesi 2017/150 E. 2017/6231 K. 13/09/2017 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:09/01/2022).
[447] İtişgen, s. 104.
[448] Ayrıntılı bilgi için bkz. Börekçi, ss. 96-98.

hususa da rıza verdikleri kabul edilmelidir. Ancak bu özelliği kullanılmadan kullanıcı bir ekran görüntüsü alarak ya da doğrudan fotoğrafını çekerek gönderiyi kendisine ait telefon veya bilgisayar gibi elektronik araçlarının dijital hafızasına kaydederse TCK m. 135 açısında fail olacak mıdır? Fail olsa da diğer kullanıcının bu gönderiyi herkese açık bir şekilde rızayla paylaşması herkesin bu veriyi bu şekilde kaydetmesine ilişkin bir rıza mıdır? Özellikle TCK m. 135 açısından sosyal medyada paylaşılan verilerin bu şekilde kaydedilmesinin suç oluşturup oluşturmayacağına ilişkin tarafımızca ulaşılabilen net yargısal bir karar ya da görüş bulunmamaktadır. Ancak genel tavrın herkese açık bir şekilde paylaşılan ve aleni hale getirilen kişisel verilerin verme ya da yayma eylemi olmadan sadece kaydedilmesi halinde TCK m. 135 açısından hukuka uygunluk sebebi sayılması yönünde olduğu görülmektedir. Söz konusu TCK m. 135 hükmü m. 139 sebebi ile şikayete tabi olmayan bir suç tipi olarak düzenlenmiş olsa dahi bu hususta şikayet olmadan ya da TCK m. 136 hükmü gereğince yapılan bir verme ya da yayma eylemi olmadan tespiti zor bir hususdur. Bu konuda açıkça söylemek gerekir ki kullanıcıların, diğer kullanıcıların kişisel verilerini içeren gönderilerini beğendiklerinde ekran görüntüsü almaları oldukça yaygındır. Bazen kişisel veri içeren bir fotoğrafta bir kıyafetinin bazen yalnızca kişinin görüntüsünün beğenilmesi bazen de kişinin gittiği mekana ait konum bilgisinin ya da bir eşyasının unutulmamak istenmesi nedeni ile kişisel verileri içeren gönderilerin ekran görüntüsü ya da fotoğraf çekilmesi yoluyla kaydedildiği görülmektedir. Bu durumda kanımızca failin kastı da önem arz etmektedir.

Budak'ın yaptığı bir anket çalışmasında kişilere bir grup halinde çekilen fotoğrafları sosyal medyada yayınlarken fotoğrafta bulunan diğer kişilerden izin alıp almadıkları ve bu fotoğrafların mahrem nitelik taşıyıp taşımadığı sorulmuştur. Anket çalışması sonunda bu fotoğrafları mahrem nitelikte gören kişilerin yüzde 49,4'ünün fotoğrafları izin almadan paylaştıklarını ifade ettikleri görülmüştür[449]. Grup halinde olan fotoğraflarda fotoğrafta bulunan kişilerin rızaları dışında bu fotoğrafların paylaşılması oldukça yaygın bir durumdur. Kişinin yüzü ve görüntüsünün kişisel veri olduğunu açıktır. Kullanıcılar tarafından rızası dışı paylaşılması hukuka aykırılık

[449] Budak, ss. 162-163.

oluşturacaktır. Ayrıca rıza dışı paylaşılan bu fotoğraflarda kişiler etiketlenmiş olabilir.

Etiketleme sosyal medya konusunda açıklamalara yer verdiğimiz bir husustur. Kullanıcı bir gönderi paylaşırken yanında bulunan ya da kendisini de o paylaşımda yer almasını sağlamak amacıyla kullanıcının adını gönderiye dahil etmektedir. Kısaca kullanıcı bir başka kullanıcıyla çekildiği bir fotoğrafı kendi profilinde paylaşacağında fotoğrafta bulunan diğer kullanıcının profiline ulaşılmasını sağlayan bir nevi link koymaktadır. Diğer kullanıcılar bunun aracılığı ile fotoğrafta yer alan kullanıcının kim olduğuna ulaşabileceklerdir. Öncelikle herkese açık bir hesaptan paylaşım yapan kullanıcının diğer kullanıcıyı gönderisinde etiketlemesi için rızasının alınmış olması gerektiği kabul edilmelidir. Kullanıcının diğer kullanıcı ile olan fotoğrafını etiketleyerek ya da etiketlemeyerek herhangi bir şekilde paylaşabilmesi için rıza almış olması gerekir. Çünkü bizce rıza dışı bu şekilde yapılan paylaşım TCK m. 136 hüküm gereğince kişisel verilerin hukuka aykırı olarak verme ya da yayma faaliyeti kapsamında değerlendirilebilecektir. Ancak şunu da belirtmek gerekir ki etiketlemenin kullanıcıyı belirli hale getirilmesi yanında kullanıcının kendisinin bir paylaşımda yer aldığından bir bildirimle haberdar olmasını sağlama işlevi de vardır. Kullanıcının kendisi etiketlenmeden paylaşılan bir fotoğrafından haberdar olması çok zordur. Ancak kendisini tanıyan başka bir kullanıcının ilgili paylaşımı görmesi ve kendisine haber vermesi ile öğrenebilecektir. Bu sebeple etiketlemenin hukuka aykırı eylemden haberdar olunması ve örneğin 5651 sayılı kanunda yer alan tedbirlere başvurulması açsından önemli olduğunu da belirtmek gerekir.

3. TCK m. 135 ve 136 Açısından İçtima

TCK m. 135 ve 136 her biri zincirleme suç şeklinde işlenebilir[450].

Kişisel verileri hukuka aykırı olarak verme, yayma, ele geçirme fiillerinin bir suç işleme kararının icrası kapsamında olacak şekilde değişik zamanlarda aynı mağdura karşı işlenmesi halinde TCK m. 43/1 zincirleme suç hükümleri uygulama

[450] Özbek, Doğan, Bacaksız, ss. 590, 595.

alanı bulabilecektir. Yargıtay bir kararında mağdura ait fotoğrafların internette, gazetede ve dergide ayrı ayrı yayınlanmasına ilişkin somut olayda TCK m. 136 açısında zincirleme suç hükümlerinin uygulanması gerektiğini ayrıca TCK m. 135'in de oluştuğunu belirtmiştir. Failin sosyal medya hesabında mağdura ait fotoğrafı paylaştıktan sonra mağdurun kimlik bilgilerini paylaştığı bir olayda zincirleme suç hükümlerini uygulanabilir bu durumda ceza artırım yapılarak verilir yani tek ceza uygulanır. Bu kişisel verilerin paylaşılması ile internet sitede kaldığı süre boyunca suç işlenmeye devam etmektedir. Bu yüzden kesintisiz suçun var olduğu düşünülmektedir[451]. Suçun, kesintisiz suç niteliğinde olduğu bu durumlarda kesintinin meydana gelmesi ile suç işlenmiş sayılacaktır[452].

TCK m. 135 kişisel verilerin kaydedilmesinin birden çok mağdura yönelik olması halinde TCK m. 43/2'de yer alan aynı neviden fikri içtima hükümlerinin gündeme gelmesi ihtimali fazladır. Örneğin kişisel verilerin kaydedilmesinin tek fiille birden fazla mağdurun bilgilerini içerecek şekilde olması mümkündür. Özellikle dijital ortamda tutulan verilerde tek fiille birden fazla kişiye ait veriye ulaşma ve onları kaydetme oldukça kolaydır. Mağdurun birden fazla olduğu bu durumlarda TCK m. 43/2 hükmü nedeni ile yine TCK m. 43/1 uygulanacaktır. Tek fiile birden fazla kişinin kişisel verisinin kaydedilmesi durumunda tek ceza verilecek ancak cezada artırım yapılacaktır. Ancak doktrinde mağdur sayısınca suç oluştuğu şeklinde düşünceler de bulunmaktadır[453].

TCK m. 136'daki seçimlik hareketlerden herhangi birinin gerçekleştirilmesi suçun oluşması için yeterlidir. Ancak bu seçimlik hareketlerden birden fazlası gerçekleştirilmişse TCK m. 61 kapsamında ceza belirlenirken bu durum alt sınırdan uzaklaşmak konusunda hakim tarafından kullanılabilecektir[454].

Her iki suç tipinin birlikte var olduğu durumlarda içtima hükümlerinin uygulanıp uygulanmayacağı hususuna ele geçirme ve kaydetme fiillerini açıklarken kısaca giriş yapmıştık. Temelde TCK m. 135 için TCK m. 136 açısından bir geçit suçu niteliğinin olduğu şeklinde görüşler olmakla birlikte tarafımızın da katıldığı

[451] İtişgen, s. 196; Korkmaz, s. 476; Sınar, s. 58.
[452] Dülger, Bilişim Suçları, s. 280.
[453] Korkmaz, s. 427.
[454] Korkmaz, s. 477.

görüş göre "geçit suç" niteliğinde olmadığı yönündedir[455]. TCK m. 136 açısından suç konusu verinin her zaman hukuka aykırı olarak kaydedilmiş olması gerekmez yani hukuka uygun bir şekilde kaydedilmiş bir veri hukuka aykırı olacak şekilde ele geçirilmiş olabilir. Esasen TCK m. 136 açısından verinin yayılması, verilmesi ya da ele geçirilmesi eyleminin hukuka aykırı olması önemlidir. Kişisel verilerin kaydedilmesi ile birlikte başkasına verme ya da yayma fiilinin aynı anda gerçekleştiği durumlarda en ağır cezanın verilmesini öngören TCK m. 44 fikri içtima kuralları uygulanabilecektir. Örneğin bir kişinin internetteki bir sitesine kişisel veriyi niteliğinde olan kaydetmesi ve bu internet sitesinin herkesçe ulaşılabilir olması durumunda TCK m. 135 ve m. 136'nın birlikte gerçekleştiği söylenebilecektir. Bu durumda kaydetmenin haksızlık içeriğinin diğer suç tipi içinde eridiğinden bahisle en ağır olan suçtan ceza verilmesi daha uygun olacaktır[456].

TCK m. 243'te yer alan bilişim sistemine girme suçu ile TCK m. 136 arasında da geçit suç ilişkisi bulunmamaktadır. Eğer bilişim sistemine girerek kişisel veriler elde edilmişse burada TCK m. 44'te yer alan farklı neviden fikri içtima kuralları uygulanabilecektir. Fail tek hareketle hem bilişim sistemine hukuka aykırı olarak girmiş hem de yine hukuka aykırı olarak kişisel verileri ele geçirmiştir. Tek fiille her iki suçla korunan hukuki değer ihlal edildiği durumda TCK m. 44 uyarınca en ağır cezayı gerektiren suç olan TCK m. 243 hükmünden ceza verilecektir[457]. Başka bir görüşe göre burada gerçek içtima kuralları uygulanmalıdır. Çünkü bilişim sistemine girme ile verileri ele geçirme arasında zamansal açıdan bu iki fiilin birbirinden bağımsız olarak gerçekleştirilmektedir[458].

TCK m. 244/2 hükmünde yer alan seçimlik hareketlerden bilişim sisteminde olan verinin başka yer gönderilmesi eyleminin gerçekleşmesi halinde ise bu suçla TCK m. 136 arasında fikri içtima hükümleri uygulanabilir[459]. Yargıtay kararına esas olan bir olayda fail tanımadığı bir kişinin mail adresinin, facebook ve twitter hesaplarının şifresini ele geçirmiş ve erişilemez kılmıştır. Daha sonra da mağdurun

[455] Yaşar, Gökcan, Artuç, s. 4126; Ayrıntılı bilgi için bkz. İtişgen s. 196; Geçit suç söz konusu olduğunda bir zorunluluk ilişkisi var olmalıdır. Daha hafif nitelikte olan suçun da aynı hukuki değeri korumaya yönelik olması ve ağır suçun gerçekleşebilmesi için hafif suçun da işlemiş olması aranır.
[456] Özbek Doğan Bacaksız s. 590.
[457] İtişgen, s. 197.
[458] Sınar, s. 60.
[459] İtişgen, s. 197.

telefon numarasını da elde ederek gizli numaradan mağduru aramış ve mağdura kişisel bilgilerinin kendisinde olduğunu söylemiştir. Mahkemece sanık hakkında TCK m. 136/1 kişisel verileri hukuka aykırı olarak ele geçirmek ve m. 244/2 bilişim sistemindeki verileri erişilemez kılmak suçlarından verilen mahkumiyet kararı Yargıtay tarafından onanmıştır[460].

TCK m. 245'te kişinin kendisine ait olmayan bir banka kartını ele geçirmesi şeklinde bir harekete yer verilmiştir. Bu suç tipinde ele geçirme fiili söz konusu olduğunda ve kişisel verilerin ele geçirilmesine teşebbüs edilmesi halinde Yargıtay TCK m. 136'ya teşebbüsten de ceza verilmesi gerektiğine hükmetmiştir. Yargıtay, ATM'ye kredi kartı bilgilerini kopyalamaya çalışan faillerin daha kimsenin kredi kartı bilgilerini çalmadan yakalanmalarına ilişkin olayda TCK m. 136 ve m. 135 hükümlerinin uygulanması gerektiğine hükmetmiştir[461]. TCK m. 245'te yer alan suç tipi oluştuğunda bu suçla TCK m. 135 ya da 136 arasında gerçek içtima hükümlerinin uygulanması gerektiği düşünülmektedir[462].

TCK m. 245/2 ile TCK m. 136 suç tiplerinin birlikte oluştuğu görüldüğü durumlarda TCK m. 42 hükmü gereği birleşik suç hükümleri uygulanması yönünde Yargıtay kararları vardır. Kişilerin kredi kartlarının kopyalanıp kişisel verilerin hukuka aykırı olarak geçirilip bunların mağdurların hesaplar ile ilişkilendirilip sahte kartlar üretilmesi halinde TCK'nin 245. maddesinin 2. fıkrasındaki suç tipi oluşmaktadır. Ancak kişisel veri niteliğinde olan kredi kartı bilgilerinin elde edilmesi ya da kopyalanmasının suçun zorunlu bir unsuru olduğu görülmektedir. Böyle bir durumda için bir bileşik suç niteliği sebebi ile TCK m. 136'dan dolayı ayrıca ceza verilmez[463].

TCK m. 136'nın hakaret suçu ile birlikte işlenmesi ihtimali de bulunmaktadır. Bu halde de fikri içtima hükümleri uygulanabilecektir[464]. Örneğin daha önce

---

[460] Yargıtay 12. Ceza Dairesi, 2014/17556 E. 2015/1675 K. 02/02/2015 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:09/01/2022).

[461] Dülger, s. 419; Dülger'e göre sanıkların bu sistemi kurmaları ama herhangi bir veriyi ele geçirmeden yakalanmış olmaları bu fiillerini m.245 açısından sadece hazırlık hareketi şeklinde kabulünü gerektirmektedir; Yargıtay 8. Ceza Dairesi, 2012/31924 E. 2014/1479 K. 23/01/2014 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T 06/01/2022).

[462] Dülger, s. 472; İlgili kısımda TCK m. 245/A hükmünün yürürlüğe girmesi öncesinde verilmiş Yargıtay kararları olduğu belirtilmektedir.

[463] Sınar, s. 58.

[464] Özbek, Doğan, Bacaksız, s. 595.

bahsettiğimiz üzere kişinin telefon numarasının sosyal medyada cinsel amaçla iletişim sağlanması yönünde paylaşılması hem kişisel verinin hukuka aykırı olarak yayılmasına hem de kişinin onur ve şerefine yönelik bir eylemdir.

TCK m. 134/1 fıkrasında yer alan özel hayatın gizliliğinin ihlal edilmesi durumunda kişisel verilerin kaydedilmesi ihtimalinde TCK m. 135 ile arasında içtima hükümlerinin uygulanıp uygulanamayacağı da önemli bir husustur. Doktrindeki bir görüşe göre özel hayatın gizliliğinin ihlali sırasında kişisel veri kaydedilirse TCK m. 134/1 oluşacaktır. Başka bir görüşe göre ise kaydedilen veri sadece özel hayata ilişkin değil de aynı zamanda kişisel veri niteliğine sahipse bu durumda TCK m. 134 ile m. 135 arasında farklı neviden fikri içtima hükümleri uygulanacaktır[465]. Koca ve Üzülmez'e göre kişiye ait görüntülerin ve seslerin kişisel veri niteliğinde olduğu bir gerçektir. Görüntü ve seslerin kişisel veri olduğu net olmakla birlikte bunlar her zaman özel hayat alanına ilişkin olmayabilir. Bu sebeple şöyle bir ayrım yapılmalıdır: Kaydedilen kişisel veriler özel hayata ilişkinse TCK m. 134/1'de yer alan suç oluşmuştur özel hayata ilişkin değilse TCK m. 135 oluşmuştur. Yani TCK m. 135 genel olarak kişisel verilerin kaydedilmesini düzenlerken TCK m. 134/1 kaydedilen içerikler özel hayata ilişkin görüntüleri konu almaktadır. Her iki yasal düzenleme arasında genel ve özel norm ilişkisi oluşmuştur. Sonuç olarak TCK m. 134/1'de yer alan düzenlemenin daha özel bir düzenleme olduğunun kabulü gerekir. Yargıtay'ın kararlarının benzer yorum doğrultusunda olduğu görülmektedir[466]. Benzer şekilde görüntülerin kişisel veri olduğunun kabulü ile birlikte TCK m. 134/2 ile m. 136 her ikisinin uygulama olanı olan durumlarda Yargıtay TCK m. 134/2'yi uygulamaktadır[467]. Kişisel verilerin hukuka aykırı olarak elde edilmesi, bir başkasına verilmesi ya da yayılmasının özel hayatın gizliliğine yönelik bir ihlali de oluşturduğunu söylemek mümkündür. Ancak doktrinde başka bir görüşe göre kişisel verilere ilişkin TCK' m. 136 hükmü TCK m. 134 hükmüne göre özel norm olarak

[465] Korkmaz, s. 429.
[466] Koca ve Üzülmez, ss. 90-91; Yargıtay 12. CD. 2014/11530 E. 2015/584 K. 19/01/2015 T. *"…mağdurun internet ortamından rızası ile gönderdiği çıplak fotoğrafların flash diske kaydedilip babasına verilmesi şeklinde gerçekleşen olayda, mağdurun cinsel ve fiziksel mahremiyetine ilişkin çıplak görüntülerinin kişisel veri kapsamında değerlendirilemeyeceği, fiilin kişisel verilerin kaydedilmesi suçunu değil, özel hayatın gizliliğini ihlal suçunu oluşturacağına karar verilmiştir."*
[467] Dülger, s. 532.

kabul edilmelidir[468]. Başka bir görüşe göre ise kişisel veri niteliği taşımayan bilgiler veya TCK m. 134/2 ses görüntü kayıtları söz konusu olduğunda genel norm olarak TCK m. 134 uygulama alanı bulacaktır[469].

Haberleşmenin gizliliğini ihlal sureti ile kişisel verilerin ele geçirilmesi halinde TCK m. 132 ile m. 136 arasında özel ve genel norm ilişkisi olduğu yönünde görüşler bulunmaktadır. Ancak bu iki suç arasında özel genel norm ilişkisi olduğunu söylemek çok doğru olmayacaktır. Tek fiille her iki suçun da işlenmiş olması halinde fikri içtima hükümleri uygulanıp fail en ağır cezayı içeren suçtan cezalandırılacaktır[470].

4. TCK m. 135 ve m. 136 Açısından Çocukları Konu Alan ya da Çocuklar Tarafından Yapılan Sosyal Medya Paylaşımlarının Değerlendirilmesi

Önceki açıklamalarımızda kişisel verilerin korunmasına ilişkin ceza hukukunda yer alan iki önemli suç tipine dair maddi, manevi ve hukuka aykırılık unsuru açıklamıştık. Bu kısımda ebeveynlerin paylaşımları ve çocukların rızası konusu başta olmak üzere çocuklara özgü durumlara değineceğiz.

Yetişkinlerin rızası konusu kadar çocukların rızası konusu da önemlidir. KVKK'de çocukların rızalarına ilişkin doğrudan bir düzenleme yer almamaktadır. Günümüzde çocuklarını sosyal medyada paylaşan ebeveynler oldukça yaygındır. Çocukların sosyal medyada paylaşılması çeşitli sebeplerle olabilmektedir. Ebeveyn bazen çocuğunun hastalığı sebebi ile başlattığı bağış kampanyası nedeni ile bazen bilinçsiz bir şekilde çocuğunun her halini paylaşmakta bazen de reklam ve ürün satışı için çocuğunu ile yaptığı çekimleri paylaşması gibi sebeplerle paylaşım yapmaktadır. Bu paylaşımlar ebeveynlerin kendi hesaplarından ya da çocukları adına açtıkları ve kendileri tarafından kontrol edilen hesaplardan yapılmaktadır. Bu hesaplar herkese açık veya yalnızca kendi kişilerinin görebileceği şekilde korumalı olabilmektedir. Birçok ebeveyn çocuklarını paylaşırken olumsuz sonuçları göz önünde

[468] İtişgen, ss. 197-198.
[469] Sınar, s. 59.
[470] İtişgen, ss. 197-198

bulundurmamaktadır. Çocuklara ait görüntülere ulaşan pedofili kişilerin bu fotoğraflar üzerlerinde yapılan değişikliklerle bu amaçlarla kullanması, sitelere yüklemesi ve yayması gibi durumlarla karşılaşılmaktadır[471].

Paylaşılan çocuk fotoğraflarının çocuk istismarcıları tarafından ya da istismar amacı olmadan da farklı amaçlarla kullanılmaktadır. Örneğin ABD'de yaşayan bir anne facebookta 4 yaşındaki kızını paylaşmaktadır. Ancak bu gönderilerinin bir başka kullanıcı tarafından da kaydedilerek paylaşıldığını New York'ta yaşayan bu kullanıcının paylaşımlarında kızını kendi kızı gibi gösterdiğini görmüştür. Bunun üzerine facebook üzerinden şikayette bulunulmuş ancak söz konusu içerikler topluluk kurallarına aykırı görülmediği için kullanıcının hesabı kapatılmamıştır[472]. Facebookta küçük yaşta bir çocuğunun fotoğrafını profil fotoğrafı olarak kullanan bu şekilde kendisini çocuk olarak tanıtan ancak çocukları istismar etmeye yönelik eylemler gerçekleştiren birçok kullanıcı bulunmaktadır. Kendi yaşında ve algısında olduğu düşünerek çocukların böyle kullanıcılara karşı korumasız durumda olduğu görülmektedir[473].

Ebeveynlerin sosyal medyada çocuklarını paylaştıkları oldukça sık görülen bir durumdur. Burada velayet hakkına kısaca değinmek gerekir. Türk Medeni Kanunu m. 339'da velayet hakkının getirdiği hak ve yükümlülüklere yer verilmiştir. Bu hak anne ve babanın çocuğa karşı olduğu kadar çocuğun da anne ve babaya karşı olan hak ve yükümlülüklerini içermektedir. Çocuğun yararı velayet hakkı kapsamında korunmaya çalışılan en temel konudur[474]. Velayet hakkı üzerinde kamu denetimi bulunmamaktadır. Ancak yine de gerekli durumlar hakime bazı müdahalelerde bulunma imkanı sağlanmıştır[475]. Ebeveynler çocukların henüz fiziksel ve zihinsel gelişimini tamamlayamadığı bir yaşta iken çocuğun hayat alanına yine

---

[471] Kaya, s. 189; Canan Erdoğan, "Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında)", **DEÜ. Hukuk Fakültesi Dergisi**, Sayı:21 (Özel Sayı), 2019, ss. 2447-2448.

[472] Ömer Ali Girgin ve Seray Gönal, "Çocuğun Kişisel Verilerinin Sosyal Medyada Ebeveyn Tarafından Paylaşılmasının Hukuki Sonuçları" **TAAD**, Yıl: 11, Sayı: 44 Ekim 2020, s. 107.

[473] Uluç ve Süslü, s. 346.

[474] Murat Akdi. "Ana- Babanın Çocuğun Fotoğraf ve Görüntülerinin Sosyal Medyada Yayınlamasından Doğan Sorumluluğu" **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:22, Sayı:3, 2016, ss. 125.

[475] Mustafa Dural, Tufan Öğüz, Mustafa Alper Gümüş. **Türk Özel Hukuku Cilt 3 Aile Hukuku**, Filiz Kitabevi, İstanbul 2016, s. 351; TMK m. 346 hükmüne göre anne babanın çocuğun menfaatini koruyamadığı durumlarda hakim tarafından çocuğun korunması amacıyla önlemler alınabilir.

çocuğun yararı doğrultusunda müdahale edebilir[476]. Örneğin kişilerin resim hakları üzerindeki yetkisi benzer şekilde çocuklar için de geçerlidir. Ayırt etme gücüne sahip bir çocuğun kendi fotoğrafının ailesi tarafından sosyal medyada yayınlanmamasını istemesi halinde çocuğun iradesine aykırı davranılması kişilik hakkı ihlali olacaktır. Şunu açıkça söylemek gerekir ki: Çocukların kişilik hakları yetişkin herhangi bir bireyin haklarından farklı değildir. Çocuklar ebeveynlere bırakılan cansız nesneler değildir[477].

2014 yılında Mott Çocuk Hastanesi'nde 0-4 yaş arasında çocuğu olan 569 anne-baba örnekleminde Michigan Üniversitesi tarafından bir çalışma yapılmıştır. Yapılan çalışmada annelerin yüzde elli altısının, babaların yüzde otuz dördünün sosyal medyada anne babalık deneyimlerine ilişkin paylaşımlar yaptığını ifade etmiştir. Çalışmada yapılan paylaşımların 5 kategoriden oluştuğu tespit edilmiştir. Paylaşımların yüzde yirmi sekizi çocukları uyutma, yüzde yirmi altısı beslenme ve yeme ile ilgili ipuçlarına, yüzde on dokuzu ise çocukları disipline etmeye, yüzde on yedisi çocukların günlük bakımına ve yüzde on yedisi ise çocuklarının davranışlarına ilişkin paylaşımlar yapmaktadır. Çalışmada anne babalar yapılan paylaşımlardan dolayı başka bir ailenin çocuğunun ileride utanabileceğini düşündüklerini söylemişlerdir. Bu şekilde düşünen anne baba sayısı çalışmaya katılanların yüzde yetmişinden fazlasını oluşturmaktadır. Çalışmada yer alan önemli bir diğer sonuç ise çocuklarını içeren paylaşımlar yapan anne ve babaların %56'sının aslında çocuklarının ilerde utanmasına sebep olacak paylaşımlar yapıyor olmasıdır. Ayrıca yapılan paylaşımların %51'i de çocuklarının konumları hakkında bilgi veren paylaşımlardır. Anne ve babaların %27'sinin çocuklarının uygunsuz fotoğraflarını paylaştığı görülmüştür[478].

---

[476]Sera Reyhani Yüksel, **Velayet Hakkının Anayasal Sınırları**, Legal Yayıncılık, İstanbul, 2016, s. 128.

[477] Akdi, s. 132-133, Hülya İmamoğlu, "Çocuğun Kişiliğinin Ana Babaya Karşı Korunması", **AÜHFD**, Cilt:54, Sayı:2, 2005, ss. 191, 193, 213, *"Ayırt etme gücüne sahip çocuk, kişilik hakkının ana babanın hukuka aykırı müdahalesi ile ihlal edilmesi veya ihlal tehlikesine maruz kalması halinde TMK 24 ve 25 hükümleri uyarınca hakimden korunmasını isteyebilir."*

[478] Canan Erdoğan, s. 2450; Rabia Merve Erişir ve Deniz Erişir. "Yeni Medya ve Çocuk: Instagram Özelinde Sharenting (Paylaşanababalık) Örneği" **Yeni Medya**, Sayı: 4-5, s. 51; Meltem Ertuğrul, "Çocuğun Kişisel Verilerinin Velisi Tarafından Sosyal Medyada Kullanılmasının Kişilik Hakkı İhlali Bakımından Değerlendirilmesi", **YBHD**, Yıl:6, Sayı:2, 2021, s. 517.

Çocuklarının verilerini ve görüntülerini paylaşan ebeveynlerin farklı bir tabirle aslında çocuklarının kendi dijital ayak izini oluşturma hakkını ellerinden aldıkları söylenebilir[479]. Çocuklar aileleri tarafından yapılan bu gibi paylaşımlar nedeni kişisel verileri ihlal edilen ve özel hayatlarına müdahale edilen çocuklar ailelerine karşı dava açmak zorunda kalabilmektedir. İtalya'da bir çocuğun kendisinin fotoğraflarını sosyal medyada paylaşan annesine dava açması örneğinde de görüldüğü üzere çocuklarının ebeveynlerine karşı açtıkları davalar çoğalacaktır[480]. Kişinin sahip olduğu değerlerin kitlelerin izlenmesini sağlayacak şekilde sunulması kısaca mahremiyet ihlalidir. Yetişkinler kendi mahremiyet sınırları konusunda karar verebilir. Ancak çocuklar söz konusu olduğunda bazen bilgi eksikliği bazen özensiz davranılmış olması gibi sebeplerle çocukların mahremiyetine dikkat edilmediği görülmektedir[481]. Çocukların oldukça küçük yaşlarda kendisinin fotoğraflarının paylaşılmasına pek anlam verememektedir. Ancak ergenlik döneminde çocukların farkındalıkları artmakta ve arkadaş çevrelerinin görmesini istemediği fotoğraflarının ailesi tarafından rızası dışında paylaşılmış olması çeşitli psikolojik sorunları beraberinde getirmektedir. Çocuğun birey olma yolculuğunda ailesine karşı öfke duymasına veya mahrem alanlarının açığa çıkarılmasını nedeni ile psikolojik sorunlar yaşamasına sebep olabilecektir. Aileler çocuklarının fotoğraflarını onların rızası dışında paylaşmamalıdır. Aileler çocuklarının özellikle mahrem görüntülerini içeren fotoğrafları paylaşırken şu soruyu kendilerine ciddi bir şekilde sormalıdır: Çocuğumun bu fotoğrafını hangi amaçla paylaşıyorum? Çocuğum ilerde bu fotoğrafı gördüğünde nasıl bir tepki verir? Bu soruları sormak ve sosyal medya hesaplarının gizlilik ayarlarını kullanmak ebeveynler açısından önemli bir sorumluluktur[482]. Son dönemde reklam işbirlikleri amacıyla ebeveynler tarafından yapılan paylaşımlar

---

[479] Ertuğrul, s. 517.

[480] Yargılama sonucunda anneye fotoğraflarını paylaşması konusunda verilen mahkeme kararına uymaması ya da çocuğunun rızasına aykırı davranmaya devam etmesi durumunda tazminat ödemesi gerektiğine hükmedilmiştir; Ertuğrul, s. 518; Murat Uçak, Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası" **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:1, ss. 46-47;
The Independent, "Woman faces £9,000 fine if she posts pictures of her son on Facebook", 12.7.2018, https://www.independent.co.uk/news/world/europe/facebook-fines-woman-son-photos-post-social-media-court-italy-rome-a8155361.html (E.T: 16/10/2021).

[481] Serap Duygulu, "Sosyal Medyada Çocuk Fotoğrafı Paylaşımlarının Mahremiyet İhlali ve Çocuk İstismarı Açısından Değerlendirilmesi,"**, TRT akademi**, Cilt:4, Sayı:8, Temmuz 2019, s. 437.

[482] Şengül Hablemitoğlu, "Çocuk Hakları İhlali ve Çocukların İstismar Alanı Olarak 'Sosyal Medya' (Bölüm II.)", 11/07/2016 https://www.linkedin.com/pulse/%C3%A7ocuk-haklar%C4%B1-ihlali-ve-%C3%A7ocuklar%C4%B1n-istismar-alan%C4%B1-ii-hablemito%C4%9Flu (E.T:30/06/2021).

oldukça yaygın olarak görülmektedir. Bu paylaşımlarla taraflardan biri çocukların sempatikliği ve de saflığı kullanılarak ticari kazanç sağlarken diğeri ise çocuğunun görünürlüğünü kullanarak hem kazanç hem de popülerlik sağlamaktadır. Sonuç olarak ebeveynler çocuklarını bilinçli ya da bilinçsiz bir şekilde istismar ederek onların psiko-sosyal gelişimlerinin olumsuz etkilemektedir[483].

Ailelerin çocuklarını sosyal medyada paylaşması durumu haricinde çocukların bizzat kendilerinin sosyal medyayı kullanıyor oldukları da görülmektedir. İngiltere de yapılan bir araştırmada çocukların %59'u henüz 10 yaşına ulaşmadan sosyal medyayı kullandığını ifade etmiştir. Ayrıca Facebook kullanma yasal sınırı 13 olmasına rağmen 8-16 yaş aralığındaki çocukların %52'si bu resmi yaş sınırını dikkate almayarak sosyal medya kullandıklarını ifade etmektedir[484].

TÜİK tarafından 22/12/2021 tarihinde "Çocuklarda Bilişim Teknolojileri Kullanım Araştırması" sonuçlarını açıklamıştır. Araştırmaya göre 6-15 yaş grubundaki çocukların internet kullanım oranı %82,7 olarak tespit edilmiştir. Bu yaş aralığındaki çocukların %90,1'i hemen hemen her gün internet kullandığını ifade ederken, %8,5'i haftada en az bir defa ve %1,4'ü ise haftada bir defadan az internet kullandığını ifade etmiştir. Söz konusu açıklamalar doğrultusunda düzenli internet kullananların, internet kullananların %98,6'sını oluşturduğu görülmüştür. Araştırmada çalışmamız açısından dikkat çeken bir diğer husus ise düzenli internet kullanan bu çocukların %31,3'ünün sosyal medya kullandığını beyan etmesidir. *"Sosyal medyayı kullanan 6-15 yaş grubundaki çocukların %77,7'sinin hemen her gün, %16,5'inin haftada en az bir defa, %5,8'inin ise haftada bir defadan az sosyal medya kullandığı görüldü. Düzenli İnternet kullanıp hemen her gün veya haftada en az bir defa olmak üzere düzenli sosyal medya kullandığını beyan eden çocukların oranı %94,2 oldu. Bu oran, 6-10 yaş grubundaki çocuklarda %84,6 iken 11-15 yaş grubundaki çocuklarda %95,9 oldu [485]."* Araştırma sonucunda ortaya konulan en önemli şey 6-15 yaş aralığındaki çocukların sosyal medyada var oldukları gerçeğidir. Düzenli olarak sosyal medyayı kullanan çocukların hafta içi ve hafta sonu günlük 2

[483] Girgin ve Gönal, s. 108.
[484] https://dijitalmedyavecocuk.bilgi.edu.tr/2017/04/06/sosyal-medya-ve-cocuklar/ (E.T:23/12/2021).
[485] Söz konusu araştırma 29 Mart-21 Mayıs 2021 tarihleri arasında yapılmış ve Hanehalkı Bilişim Teknolojileri Kullanım Araştırması kapsamında 6-15 yaş aralığındaki çocuklara uygulanmıştır. https://data.tuik.gov.tr/Bulten/Index?p=Cocuklarda-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2021-41132 (E.T:22/12/2021).

saati aşan hatta 3 saat civarında sosyal medyayı kullanıyor oldukları hususu da dikkati çekmektedir. Kanımızca 16-18 yaş aralığı haricinde 6-15 yaş aralığında olan çocuklar tarafından sosyal medyanın yaygın bir şekilde kullanıldığı ortaya konulmuştur. Çocukların sosyal medya kullanıcısı olmaları halinde eylemlerinin hukuki ve cezai sorumluluğu ayrıca düzenlenmesi gereken bir konudur. Araştırma konusu çocukların yaş aralığı ceza hukuku açısından sorumluluğun tam olmadığı bir yaş aralığıdır.

Facebook hizmet koşullarında yer alan "3. Facebook'a ve Topluluğumuza Verdiğiniz Taahhütler" başlığı altında ve de İnstagram koşullarında, aşağıda belirtilen durumlarda kişinin Facebook kullanamayacağı düzenlenmiştir. Bu taahhütlere göre 13 asgari yaş sınırının altında olanlar, cinsel suçlardan mahkum olmuş olanlar ve mevzuat gereği şirketin ürünlerini kullanmaktan yasaklanmış olanlar bu sosyal medya platformunu kullanamayacaktır[486]. Bu koşullara göre Facebook ya da Meta topluluğuna dahil olan instagram söz konusu olduğunda hesap açılıp kaydolurken kullanıcı bu koşullara uygunluğunu onaylamaktadır. Ayrıca kullanıcı olabilmek için kişi hizmet koşulları haricinde veri ilkesi ve çerez ilkelerini de onaylamak zorunludur. Sonuç olarak kullanıcı olurken hem taahhütler hem de izinler verilmektedir. Konumuz kapsamında verilen taahhütlerden örneğin kişinin cinsel suçtan hüküm giymemiş olmadığını ya da 13 yaşının altında olmadığını taahhüt etse de bunun denetimini sağlayacak bir makam bulunmamaktadır. Bu platformlarda kullanıcıların önemli bir kısmının gerçek kimlik bilgilerini kullanmadığına dikkat edildiğinde yaş sınırının da facebook tarafından tespit edilmesi de mümkün değildir.

Doğum tarihi, yaş ve cinsiyet gibi verileri kişisel veri olmakla birlikte kişinin kimlik bilgilerini doğru verme zorunluluğu belli durumlarda düzenlenmiştir. Örneğin kamusal makamlara kişilerin kimlik bilgilerini doğru vermeleri gerekirken özel bir şirket olan sosyal medya platformu sahibi şirketlere kimliğe ilişkin doğru bilgilerin verilmesi zorunluluğu olup olmadığı da önemli bir konudur. İnstagram kullanım koşullarında kullanıcıların izinsiz olarak başka kişilerin kimliğini kullanamayacağı

[486] https://tr-tr.facebook.com/legal/terms/update (E.T:23/12/2021); benzer şekilde İnstagram kullanım koşullarında da aynı düzenleme vardır. *"Instagram Hizmeti, size Facebook, Inc. tarafından sunulan Facebook Ürünlerinden biridir. Bu Kullanım Koşulları, sizinle Facebook, Inc. arasında bir sözleşme teşkil eder."* https://help.instagram.com/581066165581870 (E.T:23/12/2021).

ve yanlış bilgiler veremeyeceği düzenlenmiştir. Kullanıcının gerçek kimlik bilgilerini sunma zorunluluğunun olmadığı belirtilmekle birlikte iletişim bilgilerinin hesapların güvenliğini sağlama açsından gerekli olduğunun altı çizilmiştir. Sosyal medya platformları ile kullanıcı arasındaki sözleşmenin bir özel hukuk sözleşmesi olarak kabul ettiğimizde kişinin gerçek bilgilerini vermesini zorunlu tutmamaktadır. Sözleşmesel ilişkiye aykırı olacak hareket kişinin verdiği bilgilerin doğru olmaması ya da başkasının kimliğini kullanmasıdır. Topluluk kuralları ve koşullara aykırı davranıldığının tespiti halinde yaptırımlar öngörülmüştür. İnstagram bu koşullara aykırı davranılması halinde aykırılığın durumuna ve devamlılığına göre instagram içerikleri silebilecek, kaldırabilecek, hizmet sunmayı kısmen ya da tamamen durdurabilecektir[487].

Kişiler facebook sosyal medya uygulamasının bir özelliği olan ülke ve yaş kısıtlaması seçeneğini kullanabilir. Facebook tarafından özellikle kullanıcının sayfasının konusunun alkol veya cinsel ürünler içermesi durumunda yaş kısıtlamaları kullanılması önerilmektedir[488]. Sosyal medya neredeyse yaş sınırına tabi olmadan çocukların da kolayca ulaşabildiği kamuya açık bir ortam haline gelmiştir. Bu sebeple hem kullanıcıların bu konuda bilinçli davranması hem de sosyal medya şirketlerinin özellikle müstehcenlik suçu açısından bir filtreleme yöntemi geliştirmesi gerektiği görülmektedir. Aksi takdirde çocuklara ulaşan bu tarz verilerin ruhsal ve zihinsel gelişimlerine olumsuz etkileyeceğini öngörmek zor değildir.

Kişisel verilerin korunmasında çocukların özellikli bir durumunun olmasının nedeni kısaca şu şekilde ifade edilmektedir: Bu durumun iki temel nedeni bulunur ilki statik açıdan çocuğun yeterli olgunluğa ulaşamamış olması nedeni ile korunmaya muhtaç olmasıdır. Diğeri ise dinamik açıdan gelişim sürecinde olan çocuğun bu süreci daha iyi şekilde tamamlayabilmesi için daha özel bir muameleye gerek duymasıdır. Çocuklar bu süreçte yasal temsilciye ihtiyaç duyarlar. Çocukların verileri işlenirken yasal temsilcilerin onayı ya da rızası aranır ancak bu hal yasal temsilcilerin iradesinin çocukların iradesinden üstün olduğunu göstermemektedir.

[487] https://help.instagram.com/581066165581870 (E.T:23/12/2021).

[488] Facebook, "Ülke veya yaş kısıtlamalarını Facebook Sayfama nasıl eklerim ve bunları nasıl düzenlerim?" **Facebook Yardım Merkezi**, https://tr-tr.facebook.com/help/778445532225441?helpref=search&query=ya%C5%9F%20k%C4%B1s%C4%B1tlamas%C4%B1%20kullan%C4%B1lmas%C4%B1%20%C3%B6enri&search_session_id=e892e6f5b4fe0223abe2841a506a4b13&sr=0 (E.T:23/12/2021).

Çocuk söz konusu olduğunda kişisel verilerin korunması hakkı yine çocuğa ait bir haktır. İnternete erişim hakkının kullanılmasında 29. Veri Koruma Grubuna göre çocuğun veli ya da vasisinin rızası aranmamalıdır. Ancak verilerin doğrudan pazarlama amaçlı olarak işlenmesi durumunda yasal temsilcinin rızası aranmalıdır. Çocuğun olgunluk düzeyinin belirlenmesi rıza konusunda dikkate alınan bir diğer hususdur. Son olarak danışılma hakkı olarak ifade edilen husus bulunmaktadır. Buna göre örneğin çocuğun görüntüsünün kullanılması durumunda uyulması zorunlu olmasa da çocuğa danışılıp görüşünün alınması gerektiği düşünülmektedir[489].

Bu hususa ilişkin GDPR'de düzenleme yapılmıştır. Daha önce de bahsettiğimiz üzere Tüzük, sosyal medyada kullanıcı oluşturma ya da pazarlama faaliyetleri söz konusu olduğunda bu işlemlerin çocuğun özellikle koruma altına alınması gereken işlemlerden olduğunu belirtmektedir[490]. Çocuğun verilerinin işlenmesinde çocuğun özel yararı esas alınmalıdır. Tüzükte yer alan 8. madde çocuğun rızası konusunu ayrıca düzenlenmektedir. Madde de çocuğun doğrudan rızasının alınabilmesi için en az 16 yaşında olması aranmıştır. Yani rıza yaşı en az 16 olarak belirlenmiş ancak üye devletlere bu yaş sınırını 13 yaştan küçük olmamak kaydıyla daha da düşürebilmeleri konusunda seçenek tanımıştır. Belirlenen yaştan küçük olan çocuklar için velayet hakkı olan kişiden rıza ya da onay alınacaktır[491].

AİHM Reklos ve Davourlis kararında anne ve babanın izni olmadan, yeni doğmuş olan çocuğun fotoğrafının (herkesin giremeyeceği steril ortama bir fotoğrafçının girmesi sağlanarak) çekilmesi konusunda ailenin şikayetini incelemiştir. Aile tarafından bu duruma onay verilmemiş ve çekilen fotoğrafların negatifleri talep edilmiştir. AİHM olayda kişilerin görüntülerinin etkili şekilde korunması gerektiğinin altını çizmiş ve kişilerin görüntüleri üzerindeki denetimi kaybetmemeleri için en geç fotoğrafın çekilme anında rıza alınmış olması gerektiğini belirtmiştir. Mahkeme, kişisel veri olan görüntülerin koruma hakkının kullanımının çocuklar söz konusu olduğunda ailelerince denetleneceğini bu sebeple onların fotoğraf çekilmeden önce onların rızalarının alınması gerektiğini olayda ise buna

[489] Küzeci, 2021, ss. 272-274.
[490] Uçak, s. 46; Küzeci, 2021, s. 274.
[491] https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf (E.T:08/01/2022).

aykırı davranılması sonucunda AİHS m. 8'in ihlal edildiği şeklinde karar vermiştir[492].

Sosyal medya siteleri aslında çocuklar için tasarlanmamış mecralardır. Bu mecrada olan yaş sınırlarına riayet edilmemekte ve topluluk kuralları da yeterli olmamaktadır. Böylelikle doğrudan ya da dolaylı olarak hedef kitle çocuklar olmasa bile çocukların kişisel verileri bir şekilde kaydedilmektedir. Özellikle ailelerin çocukların bu hususlarda gözetim yükümlülüğünü ihmal ettiği durumlarda çocukların mahremiyetinin olmayacağı, kendi geleceklerinin belirleme hakkı, ayrımcılığa tabi olmama gibi haklarının olumsuz etkileneceği ve ihlallere açık hale geleceği görülmektedir. Çocukların bu hakları üzerindeki etkileri tespit etmek, değerlendirmek ve çözümler sunmak amacıyla için "Çocuk Hakları Etki Analizi (ÇHEA)" başlığı altında çalışmalar yapılmaktadır. Uluslararası hukukta sözleşmelerle kabul edilen çocuk haklarının internet ortamında da geçerli olduğu bir gerçektir. Özellikle dünyada her üç çocuktan birinin internet kullandığı dikkate alındığında çocuk hakları açısından bu konunun önemi daha da artmaktadır. Bu durumda çocukların korunmasına hizmet eden çocuk haklarına internet ve yapay zeka sebebi ile yeni nesil haklar ilave edilip edilmeyeceği sorusu da gündeme gelmektedir. Yapay zeka konusunu sebebi ile değişime uğrayacak mevcut çocuk haklarını kısaca şöyle sayabiliriz: Kendi geleceğini belirleme hakkı, verilerinin korunması ve mahremiyet hakkı, kişisel bütünlük hakkı, oyun oynama hakkı, ayrımcılığa ve kötü muameleye maruz kalmama hakkı, kendini ifade edebilme hakkı, elektronik ortamı güvenle kullanabilme hakkı, kendi iradesiyle kararlar alabilme hakkı. Bu haklar dışında çocuk haklarının daha güvenle ve etkin bir şekilde kullanılabilmesi *"Çocuğun yapay zeka sistemlerinin yaşam döngüsüne katılım hakkı, çocu*ğun *yapay zeka sistemlerinin yaşam döngüsünü gözetim hakkı, çocuğun kendi iradesiyle, kendi kararlarını alma hakkı, yapay zeka sistemlerine ilişkin 'açıklanabilirlik' ilkesi uyarınca, basit, açık, yalın bir dille bilgi edinme hakkı, çocuk merkezli yapay zeka sistemleri geliştirilmesini talep etme hakkı"* şeklinde yeni nesil haklar belirlenip yasal düzenlemeler yapılmalıdır. Ayrıca çocukların kişisel verilerinin çocuğun üstün yararı gözetilerek bu verilerin hassas veri olarak

[492] Küzeci, 2021, s. 275.

adlandırılması sosyal medya mecralarının ve devletlerin bu hususa daha fazla önem göstermelerini sağlayabilecektir[493].

Berber ve Atabey'in makalesinde de değindiği bir çalışma olan farklı ülkelerden ve kültürlerden 9 ve 22 yaş arası 709 çocuk ve gençle yapılan çalışmada dijital ortamdaki temel problemleri ve yorumları sorulmuştur. Çocukların ve gençlerin internete erişimden mahremiyete dair birçok konuda düşünceleri alınmıştır. Çocukların dijital dünya sayesinde birçok suçun işlendiğinin farkında olduğu kendilerini güvensiz hissettiklerini, özellikle konum bilgisi paylaşma konusunda çekindiklerini belirtikleri görülmektedir. Ayrıca sosyal medyada kendilerine fiziksel şiddetten daha da zarar veren eylemlerle karşılaştıklarını ifade etmektedirler. Örneğin şiddet içerikli paylaşımlar ve cinsel içerikli paylaşımlara maruz kaldıklarından bahsetmektedirler. Çalışmanın sonunda çocukların hepsinin de yaşlarına uygun, mahremiyetlerine riayet edilen, şiddete ve uygunsuz içeriklere maruz kalmamalarını sağlayacak düzenlemelerin yapılmasını istedikleri sonucuna ulaşılmıştır. Çocuklar ve gençler bu olumsuzlukların giderilerek dijital mecraları kullanmak istediklerini belirtmektedirler[494].

Çocuğun bizzat kendisinin rıza verebilmesi için belli bir olgunluğa ulaşmış olması gerekir. Örneğin İskoçya'da bu yaş 12, Avusturya'da ise 14 yaş sınır olarak kabul edilmiştir. Bu yaş sınırında olan çocuklar aksi kanıtlanmadıkça kişisel verilerinin korunması konusunda rıza verebilir kabul edilmektedir. Kişisel Verileri Koruma Kurulunun 11/08/2020 Tarihli 2020/622 Sayılı Kararına konu olan bir olayda gerçeğe aykırı düzenlenmiş olan ve çocuğunun E Nabız sisteminde yer alan raporun velisi tarafından kaldırılmasını istenmiştir. Ancak veri sorumlusunca kaldırılmaması üzerine veli, Kişisel Verileri Korunma Kuruluna şikayette bulunulmuştur. Kurul, ayırt etme gücüne sahip çocukların kendisi ile ilgili olan kişisel verilerinin korunması hususunda velileri ile iradelerin çatışmadığı sürece velileri tarafından da şikayet haklarının kullanılabileceğini ifade etmiştir. Dülger'e göre iradelerin çatışmaması ifadesinin kullanılması ile çatışma halinde ne olacağı

[493] Leyla Keser Berber ve Ayça Atabey, "Yapay Zeka Sistemlerinin Çocuk Haklarına Etkilerinin Değerlendirilme Yöntemi: Çocuk Hakları Etki Analizi" **Adalet Dergisi**, Cilt:66, Sayı:1, 2021, ss. 58, 59, 61, 63, 64.

[494] Our Rights in a Digital World (A snapshot of children's views from around the world) https://5rightsfoundation.com/uploads/Our%20Rights%20in%20a%20Digital%20World.pdf (E.T:15/01/2022).

sorunu gündeme gelmektedir. Ayrıca ayırt etme gücüne sahip çocukların kimler olduğunun cevabı da önemlidir. Mevzuatımızda bu hususa ilişkin düzenleme bulunmamaktadır. Ancak çocuğun iradesine öncelik verilmelidir. Örneğin çocuğun kişisel verisi olan fotoğrafının çocuk tarafından açıkça sosyal medyada paylaşılmaması istenirse ebeveyn tarafından bu fotoğraf yayınlanmamalıdır. Hatta yayınlandıysa kaldırılmalıdır. Gelecekte bu fotoğrafın muhatabının yine çocuğun kendisinin olacağı unutulmamalıdır. Sosyal medya kullanıcısının çocuk olduğu durumda aydınlatma yükümlülüğünün nasıl yerine getirilebileceği ve muhatabının kim olması gerektiği de bir diğer önemli sorundur. Dülger bu durum için şu soruları sormaktadır. Çocuklar söz konusu olduğunda aydınlatma yükümlülüğü kime karşı yerine getirilecek, nasıl bir üslup kullanılacak, KVKK'de yer alan haklar kim tarafından kullanılacak ve çocukların yaşlarında bir sınıflandırmaya gidilecek mi? Bu soruların cevabı aslında mevcut hukuk boşluğunu dolduracaktır[495].

GDPR, KVKK düzenlemeleri ve sosyal medya şirketlerinin aldığı önlemleri kısaca belirttikten sonra ceza hukuku kapsamında bu korumanın nasıl sağlandığına ilişkin örneklere değinmek gerekir. Çocuklar söz konusu olduğunda müstehcenlik suçu ile özel hayatın gizliliğinin ihlali ve kişisel verilerin hukuka aykırı olarak kaydedilmesi suçu arasındaki ilişkiye kısaca değerlendirilmelidir. Yargıtay kararlarında çocukların görüntülerin rızayla ya da rıza dışında kaydedilmesi durumunda müstehcenlik suçu ile özel hayatın gizliliğini ihlal suçu arasında içtima ilişkisi kurmaktadır. Bilindiği üzere müstehcenlik suçu daha ağır cezalar içermektedir. Yargıtay da bu sebeple fikri içtima hükümleri doğrultusunda failin ağır olan müstehcenlik suçunun cezası ile cezalandırılması gerektiği yönünde kararlar vermektedir. YGK, 15 yaşından küçük bir çocuğun cinsel içerikli görüntülerini kayda alan sanığın TCK m. 226/3 ve özel hayatın gizliliğini ihlali suçlarının işlendiği ancak TCK m. 44 gereği en ağır cezası olan müstehcenlik suçundan ceza verilmesine oy çoğunluğu ile karar verilmiştir. Alınana kararda karşı oy kullanan on dört üye müstehcenlik suçunun değil de yalnızca özel hayatın gizliliğinin ihlali suçunun

[495] Dülger, Murat Volkan. "Gdpr Ve Kvkk Bakımından Çocukların Kişisel Verilerinin Korunması Ve Konuya İlişkin Kurul Kararının Değerlendirilmesi" https://www.hukukihaber.net/gdpr-ve-kvkk-bakimindan-cocuklarin-kisisel-verilerinin-korunmasi-ve-konuya-iliskin-kurul-kararinin-degerlendirilmesi-makale,8753.html (E.T:16/10/2021).

işlendiğini düşünmektedir[496]. Yargıtay 12. Ceza Dairesi bir kararda müstehcenlik ve kişisel veriler konusunda TCK m. 135 ve m. 136 değerlendirmesi yapılmıştır. Somut olayda fail 13 yaşındaki mağduru ikna ederek onun cinsel içerikli görüntülerini kaydetmektedir. Daireye göre bu fiil TCK m. 226/3 kapsamında suç oluşturmaktadır. Yerel mahkemenin TCK m. 135/1 hükmü gereğince mahkumiyete karar vermesi hatalı görülmüştür. Failin daha sonra bu görüntüleri facebook üzerinden paylaşması ise Daireye göre TCK m. 226/5 hükmünün uygulanmasını gerektirmektedir. Ancak yerel mahkeme bu konuda da TCK m. 136/1 hükmünü uygulayarak mahkumiyet kararı vermiştir. Sonuç olarak Daire, TCK m. 135/1 ve m. 136/1 hükümlerine göre verilen mahkumiyet hükmünün hatalı olduğuna, bu hükümlerin değil de TCK m. 226/3-1 ve m.226/5'te yer alan müstehcenlik suçunun ilgili fıkralarının uygulanması gerektiğine hükmetmiştir[497].

2019 yılında getirilen TCK m. 136/2 hükmü şu şekildedir[498]: **"***Suçun konusunun, Ceza Muhakemesi Kanununun 236'ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır." denilmektedir.* CMK hükmünde yer alan 5. fıkrada cinsel istismar suçunun mağduru olan çocukların soruşturma ve kovuşturma aşamasında beyanları alınırken görüntülerinin kaydedilmesi düzenlemesi yer almaktadır. Örneğin adli makamlarca saklanan bu beyan ve görüntülerin ele geçirilmesi ya da sosyal medya da yayınlanması söz konusu olduğunda TCK m. 136/2 uyarınca verilen ceza arttırılacaktır. Bu düzenleme çocuklara ilişkin kişisel veriler üzerinde gösterilmesi gereken hassasiyet neticesinde gerçekleştirilmiştir. Cinsel istismar suçunun mağduru olan çocukların böyle bir durumda beyan verirken kaydedilen görüntüleri ve açıklamaları kanımızca hassas veri niteliğindedir. Çocukların verilerinin korunması noktasında ceza hukukunda daha çok düzenlemeye ihtiyaç duyulmaktadır. Cezasız kalacağı ve kendilerini savunamayacakları düşüncesi ile faillerin çocuklara ait veriler üzerinde daha fazla temel hak ihlalleri gerçekleştirildiği görülmektedir.

---

[496] Yargıtay Ceza Genel Kurulu 2014/603 E. 2015/66 K. 24/03/2015 T. Ayrıca benzer değerlendirme içeren karar için bkz. 12. Ceza Dairesi 2017/6505 E. 2018/3606 K. 28/03/2018 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:28/12/2021).

[497] 12. Ceza Dairesi 2019/3839 E. 2020/5418 K. 21/10/2020 T. https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ (E.T:28/12/2021).

[498] TCK m. 136/2 hükmü değişiklik **(Ek:17/10/2019-7188/17 md.)** https://mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5 (E.T:22/01/2022).

SONUÇ

Çalışmamızda yer verdiğimiz terimler sürekli değişmekte ve yerlerine yeniler eklenmektedir. Bu değişimin ve gelişimin ortasında sosyal medya konusundan bahsetmenin olumlu yönleri olduğu kadar olumsuz yönleri de bulunmaktadır. Değişen terim ve tabilerin hukuki yansımalarını bulmak ve de bunları belli bir kalıba koymaya çalışmak çalışmamızın olumsuz ya da zor olarak adlandırabileceğimiz tarafıdır. Olumlu tarafı da yorumlanmamış şeyleri yorumlamaktır ki özellikle ceza hukuku yönüyle sosyal medyanın birçok yönünün değerlendirilmediği görülmektedir.

Dijital dünya da başta unutulma hakkı olmak üzere kişisel verilerin korunmasına ilişkin birçok ilke ve yasal düzenleme bulunmaktadır. Özellikle devletlerin ve ticari şirketlerin, veri işleme ve veri aktarma ihtiyacı günümüzde ulusal ve uluslararası düzenlemelerle belli bir sistematiğe kavuşmuştur. Ancak ülkemiz açısından Kişisel Verilerin Korunması Kanunu 2016 yılından beri uygulanmaya başlayan yeni bir düzenlemedir. Kişisel verilerin korunması konusunda önemli yasal düzenlemeler getiren KVKK uluslararası düzenlemelerde yer alan temel ilkeleri ve hukuka uygunluk sebeplerini barındıran bir kanun olmuştur. Ancak kanunun yeni olması beraberinde uygulama sorunlarını getirmiş ve ceza hukukumuzda ayrıntılı düzenlemeye sahip olmayan kişisel verilerin korunması meselesine çözüm olamamıştır. Benzer şekilde 5651 sayılı Kanununda da 2020 yılında değişiklikler yapılmış; sosyal ağlar tanımlanmış, çeşitli başvuru yolları düzenlenmiş, sosyal medya platformlarına kişisel verileri Türkiye'de tutması ve Türkiye temsilcisi ataması gibi yükümlülükler yüklenmiştir. Ancak bu kanunla da cezai hükümler getirmemiştir. Her iki yasal düzenleme interneti ilgilendirse de kişisel verilerin ceza hükümleri anlamında korunmasını sağlayacak ve sosyal medyada gerçek kişiler tarafından gerçekleştirilen fiilleri tanımlayacak nitelikte değildir. Sosyal medya kişilere birçok yönüyle internetten daha farklı bir ortam sağlamaktadır. Sonuç olarak mevcut ulusal düzenlemelerimiz internet üzerinden yapılacak birçok işlemi ya da eylemi öngörebilecek biçimde düzenlenmiş olsa da aynı şeyi sosyal medyada gerçekleştirilen eylemler için söylemek mümkün değildir.

Kullanıcılar sosyal medya kullanırken, profil oluştururken, diğer kullanıcılar hakkında yorum yaparken, bir arkadaşının da olduğu fotoğrafı arkadaşının rızasını almadan paylaşırken, herkese açık şekilde paylaşım yapan bir kullanıcının fotoğrafını kendisi gibi paylaşırken ya da konumlarını ve hassas verilerini paylaşırken eylemlerinin hukuki ve cezai sonuçlarından haberdar değildir. Çoğu zaman kullanıcılar, kişisel veriyi kaydettiklerini ya da paylaşımları ile başkasının kişisel verilerini yaydıklarının farkında olmamaktadırlar. Sosyal medyada paylaşılan verilerin ceza hukuk yoluyla korunması konusunda kanımızca üç temel sorun vardır. İlki hukuka uygunluk sebepleri ki bunlardan en önemlisi kişisel verilerin aleni hale getirilmesidir. İkincisi ise kişisel verilerin korunmasına ilişkin TCK m. 135-136 ile özel hayatın gizliliğinin ihlali konusunu düzenleyen TCK m. 134 arasındaki ilişkidir. Üçüncüsü ise çocukların ailelerinin ve kendilerinin sosyal medya kullanımlarında onların kişisel verilerinin nasıl korunacağıdır.

Sosyal medyada gerçekleştirilen kişisel veri ihlalleri özellikle herkese açık hesaplardan yapılan paylaşımlarda kendini daha çok göstermektedir. Korumalı ya da gizli hesaplardan yapılan paylaşımlarda rıza unsurunun olmadığı çoğu kullanıcı tarafından anlaşılır şekildedir. Bu hususların yanında kişisel verilerin korunmasına yönelik olan TCK m. 135 ve m. 136 hükümlerinin şikayete bağlı olmaması, KVKK'deki hukuka uygunluk sebeplerinin TCK açısından ve sosyal medyadaki eylemler açısından değerlendirilirken kavram kargaşasının oluşması gibi hususlar net çözümler sunulmasını zorlaştırmaktadır. İncelediğimiz yargı kararları, birçok konuda net ve ortak içtihatlar koyamamaktadır. Özellikle KVKK'de yer alan hukuka uygunluk sebeplerinin TCK açısından doğrudan hukuka uygunluk sebebi sayılmasının sakıncaları olduğu görülmektedir. KVKK sistematiği milyonlarca kişinin görebileceği bir ortamda veri işleme ya da veri aktarımı yapılmasına yönelik bir düzenleme değildir. Ayrıca KVKK kapsamında yapılacak işlemler için genel ilkeler belirlenmiştir. Hukuka uygunluk sebepleri bu ilkeler bağlamında değerlendirilmelidir. Örneğin alenileştirmenin ceza hukuku açısından hukuka uygunluk sebebi kabul edilebilmesi için KVKK genel ilkelerden olan amaca bağlılık ilkesi dikkate alınmalıdır. Kanunun sistematiğinde veriler üzerinde tasarrufta bulunan kişiler ne kadar çok olsa da sayılabilir ve belirlenebilir gerçek ya da tüzel kişilerdir.

Ancak sosyal medyada alenen paylaşılan veriler başka bir kullanıcı tarafından kaydedilebilir yani işlenebilir hale gelmektedir.

Yargıtay tarafından doğrudan KVKK hukuka uygunluk sebeplerine atıf yapılarak alenileştirmenin hukuka uygunluk sebebi olarak açıklandığı bir karara tarafımızca rastlanmamıştır. Rıza söz konusu olduğunda nasıl ki rızanın neye verildiğine ilişkin incelemeler yapılması gerekiyorsa, alenileştirme hukuka uygunluk sebebi olarak uygulanması halinde de alenileştirme amacının incelenmesi gerekir. Aksi takdirde sosyal medyada aleni olarak paylaşılan her veri üzerinde kaydetme, yayma ya da yayma eylemi şekillinde yapılan tasarruf hukuka uygun kabul edilecektir. TCK m. 135 açısından alenileştirilmenin hukuka uygunluk sebebi sayılması nispeten daha anlaşılır olsa da TCK m. 136 açısından bu pek söylenemez. Çünkü alenileştirilen bir kişisel verinin kaydedilmesi yani işlenmesi belki hukuka aykırı olarak nitelendirilmese de bu verinin verilmesi ya da yayılmasının hukuka uygun olduğunu söylemek zordur. Özellikle verinin işlenmesi ile kaydedilmesi yakın anlamlı olsa da verinin aktarılması verme ve yayma eylemlerini tam olarak karşılamamaktadır.

Öncelikle sosyal medyada kullanıcıların neden hesaplarını herkese açık olacak şekilde kullandığının tespiti gerekir. Kullanıcıların birçoğu takipçi sayısını arttırma ve popülarite kazanma amacıyla korumalı hesap kullanmamaktadır. Herkese açık hesap kullanarak şahsi ya da ticari sebeplerle daha görülür hale gelmeye çalışmaktadır. Sonuç olarak alenileştirmenin amacı, kişisel verisi olan fotoğraflarının sayısız sayıda kişi tarafından farklı amaçlarla kaydedilmesine ya da yayılmasına yönelik değil de sosyal medyada görülür hale gelmedir. Sosyal medya platformunun özellikleri doğrultusunda koleksiyona kaydet gibi seçeneklerle kaydedilmesi veya kullanıcının adı bildirilerek, etiketlenerek paylaşılması yani yayılması halinde alenileştirilen veri alenileştirme amacına uygun olarak kullanılmış olacaktır. Alenileştirme amacı kesinlikle irdelenmesi gereken bir konudur. Sosyal medya platformları söz konusu olduğunda şikayete bağlı olup olmama, suç tipinin cezasının ağırlığı, sosyal medyada paylaşım yapan kişilerin gerçek iradelerinin tespiti ve hangi hallerin hukuka uygunluk sebebi sayılabileceği konusunda TCK'da özel bir düzenleme yapılması bir gerekliliktir. Kişisel verilerin korunması hakkının özel hayata dair bir hak olmasından kaynaklı olarak TCK'da yer alan özel hayatın

korunmasına dair hükümlerle TCK m. 135 ve m. 136 arasından nasıl bir ilişki kurulacağı yargısal kararlarda sık sık tartışılan bir konu olmuştur. Örneğin kişilerin görüntülerinin hem özel hayatın gizliliğini ihlal suçunun hem de kişisel verilerin kaydedilmesi suçunun konusu olduğundan hangi durumlarda hangi madde açısından değerlendirilmesi gerektiği hususu açıklamaya muhtaç bir konudur. Bazı Yargıtay kararlarında olduğu gibi özel hayata dair mahremiyet içeren bir görüntünün TCK m. 135 yerine TCK m. 134 hükmü gereğince değerlendirilmesi ve TCK m. 134'ten ceza verilmesi suçun şikayete bağlı olmasına sebep olacaktır.

Çocuklara ait kişisel verilerin korunması konusu da yasal düzenlemeye muhtaç bir konudur. Çalışmamızda ebeveynleri tarafından çocuklarına ait görsellerin ticari amaçlarla kullanılması ya da çocukların çok küçük yaşlarda denetimsiz olarak sosyal medya kullanıyor olması gibi hususlar da değerlendirmeye çalıştığımız sorunlardandır. Avrupa Birliği Genel Veri Koruma Tüzüğünde bilgi toplumu hizmetlerinin çocuklar tarafından kullanılmasında bir yaş sınırının belirlenmiş olması çocuklara yönelik bir düzenleme gerekliliğinin uluslararası alanda ilk işaretlerini vermektedir. Sosyal medya platformları belli kurallar dahilinde hizmet verdiklerini belirtse de topluluk kuralları ya da veri ilkeleri etkin şekilde uygulanan kurallar değildir. Bilgi toplumları hizmetleri konusunda Tüzük ve ülkelerin kendi tercihleri doğrultusunda çocukların 13 yaşından itibaren sosyal medya platformlarını kullanması yasal olarak mümkün kılınmıştır. Ancak 13 yaşından küçüklerin sosyal medyaya erişimini uygun görmeyen söz konusu kuralın bir denetim mekanizması mevcut değildir. Kullanıcıların gerçek kimliklerini açıklama zorunluluğunun olmadığı bir mecrada kullanıcıların yaşlarının tespitinin mümkün olduğu söylenemeyecektir. Ancak sosyal medya platformlarının bu konuda bazı çalışmaları var olmakla birlikte teknolojinin, yapay zekanın getirdiği imkanlar kullanılarak ve kullanıcıların yalnızca bu husus için gereken verileri toplanarak yaşa ilişkin doğrulamaların yapılması gerekir. Cezai sorumlulukları açısından yetişkinlerden farklı değerlendirmelere tabi tutulması gereken çocukların eylemlerinin sosyal medya ortamında kandırılmaya ve suiistimal edilmeye daha açık olduğu görülmektedir. Dijital ortamın getirdiği ulaşılabilirlik ve rahatlık hissi kötü niyetli kişilerle karşılaşan çocukların hayatlarında geri dönülemez psikolojik zararlara yol açtığı çok sık görülür hale gelmiştir.

KAYNAKÇA

Aka, Beyza. "Sosyal Medyada Kişilik Hakkı İhlalleri ve Hukukî Korunma Yolları", **İzmir Barosu Dergisi**, Mayıs 2017, ss.231-287.

Akar, Erkan. **Sosyal Medya Pazarlaması- Sosyal Webde Pazarlama Stratejileri**, Efil Yayınevi, Ankara, 2011.

Akbulut, Berin. **Bilişim Alanında Suçlar**, 2. Baskı, Adalet Yayınları, Ankara, 2017.

Akdağ, Hale. **Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması**, (Yayınlanmamış Yüksek Lisans Tezi) Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010.

Akdi, Murat. "Ana- Babanın Çocuğun Fotoğraf ve Görüntülerinin Sosyal Medyada Yayınlamasından Doğan Sorumluluğu" **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt: 22, Sayı: 3, 2016, ss.123-144.

Akgül, Aydın. **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığından Kişisel Verilerin Korunması,** 2. Baskı, Beta Yayıncılık, İstanbul, 2016.

Akgül, Aydın, "Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' ve Ab Adalet Divanı'nın 'Google Kararı' ", **Türkiye Barolar Birliği Dergisi**, Sayı: 116, 2016, ss.11-38. (Google)

Akıncı, Ayşe Nur. "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler Ve Türk Hukuku Bakımından Değerlendirilmesi", **Çalışma Raporu, T.C. Kalkınma Bakanlığı Yayınları**, 2017.

Akkurt, Sinan Sami. **Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması**, Seçkin Yayıncılık, 2. Baskı, Ankara, Ekim 2020.

Akkurt, Sinan Sami. “Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlâli Hâlinde Ortaya Çıkacak Cezaî Sorumluluğa Medenî Hukuk Bağlamında Bir Bakış” **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:25, Sayı:2, 2017, ss.329-373.

Aksoy, Hüseyin Can. **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010.

Aktaş, Batuhan. **Özel Hayatın Gizliliğini İhlal Suçu**, Der Yayınları, İstanbul, 2017.

Andreas M. Kaplan ve Michael Haenlein, “Users of the World, Unite! The Challenges and Opportunities of Social Media”, **Business Horizons**, Cilt:53, Sayı:1, 2010, ss.59- 68.

Arslan Öncü, Gülay. **Özel Yaşama ve Aile Yaşamına Saygı Hakkı Anayasa Mahkemesi Bireysel Başvuru El Kitabı-8**, Avrupa Konseyi, Epamat Basım, Ankara, 2019.

Aslan, M. Yasin, “Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu”, **Ankara Barosu Dergisi**, Cilt: 68, Sayı: 2, 2010, ss.30-37.

Atak, Songül, “Avrupa Konseyi’nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler”, **Türkiye Barolar Birliği Dergisi**, Sayı: 87, 2010, ss.90-120. (AB)

Atak, Songül. “Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri”, **Kazancı Hakemli Hukuk Dergisi**, Sayı: 57-60, 2009, ss.200-222.

Atasoy, Kemal. “Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması Ve Veri Sahibinin Rızası” **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt:22, Sayı:3, ss.269-301.

Aydın, Sedat Erdem. **AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu**, İstanbul, Aralık 2015.

Ayözer, A. Çiğdem. **Kişisel Verilerin Korunması- Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil**, Beta Yayınları, İstanbul, 2016.

Başalp, Nilgün. "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt: 21, Sayı: 1, 2015, ss.77-105.

Başalp, Nilgün. **Kişisel Verilerin Korunması ve Saklanması**, 1. Baskı, Yetkin Yayınları, Ankara, 2004. (Kişisel).

Börekçi, Eşref Barış. **Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu**, (Yayımlanmamış Yüksek Lisans Tezi) Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019.

Bozdoğan Akbulut, Berrin. "Bilişim Suçları" **Selçuk Üniversitesi Hukuk Fakültesi Dergisi,** Milenyum Armağanı, Cilt:8, Sayı:1-2, 2000, ss.546-547.

Budak, Hatice. "Sosyal Medya İletişiminde Mahremiyetin Serüveni" **İnsan ve Toplum Bilimleri Araştırmaları Dergisi,** Cilt:7, Sayı:1, 2018, ss.146-170.

Bulut, Metin. "Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler", **Ankara Barosu Dergisi**, Yıl:78, Sayı:3, 2020, ss.110-150.

Büyükarslan Ali, Murat Kırık, **Sosyalleşen Birey, Sosyal Medya**, Çizgi Kitapevi, Konya, 2014.

Bygrave, Lee A. "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", **International Journal of Law and Information Technology**, Cilt: 6, 1998, ss.247-284, (Data)

https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf (E.T:10/01/2022).

Bygrave, Lee A. "Privacy and Data Protection in an International Perspective", **Stockholm Institute for Scandinavian Law**, 2010, ss.166-198, (Privacy) https://www.scandinavianlaw.se/pdf/56-8.pdf (E.T:10/01/2022).

Castells, Manuel. **İsyan ve Umut Ağları**, çev. Ebru Kılıç, Koç Üniversitesi Yayınları, İstanbul, 2013.

Cihan, Murat ve Sıtkı Yıldız. "Sosyal Medya Aracılığı ile İşlenen Suçlar: Facebook, Twitter ve Instagram Örnekleri" **Kırıkkale Üniversitesi Sosyal Bilimler Dergisi**, Cilt:11, Sayı:1, Ocak 2021, ss.135-150.

Çetin, Ebru "Sosyal Paylaşım Ağlarında Fotoğraf, Yer/Mekan Bildirimi Paylaşımları ve Mahremiyet: Facebook Örneği" **Uluslararası Sosyal Araştırmalar Dergisi**, Cilt:8 Sayı:41, 2015, ss.779-788.

Dağ, Güray. **Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması**, (Yayınlanmamış Doktora Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011.

Deniz, İlknur. **Çocuklara Ait Kişisel Verilerin Türk Medeni Kanunu ve Kişisel Verilerin Korunması Kanunu Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2021.

Develioğlu, Hüseyin Murat. **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayınları, İstanbul, 2017.

Durak, Yasemin. "İnternet Yoluyla Kişilik Haklarına Saldırı ve Hukuki Koruma" **Selçuk Hukuk Fakültesi Dergisi**, Yıl:2014, Cilt:22, Sayı:1, ss.101-125.

Dural, Mustafa ve Tufan Öğüz. **Türk Özel Hukuku Cilt II Kişiler Hukuku,** 14. Baskı, Filiz Kitabevi, İstanbul, 2013.

Dural, Mustafa, Tufan Öğüz, Mustafa. Alper Gümüş. **Türk Özel Hukuku Cilt 3 Aile Hukuku**, Filiz Kitabevi, İstanbul, 2016.

Duygulu, Serap. "Sosyal Medyada Çocuk Fotoğrafı Paylaşımlarının Mahremiyet İhlali ve Çocuk İstismarı Açısından Değerlendirilmesi,"**, TRT akademi**, Cilt:4, Sayı:8, Temmuz 2019, ss.428–487.

Dülger, Murat Volkan. **Bilişim Suçları**, Seçkin Yayıncılık, Ankara, 2004. (Bilişim Suçları)

Dülger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku**, 5. Baskı, Seçkin Yayınları, Ankara, 2020.

Dülger, Murat Volkan. "Avrupa İnsan Hakları Mahkemesi Kararlarında Organize Suçla Mücadelede Özel Koruma Tedbirleri", Yıldızhan Yayla'ya Armağan, **Galatasaray Üniversitesi Yayınları**, İstanbul 2003, ss.275-283. (AİHM)

Dülger, Murat Volkan, Mustafa Temmuz Oğlakcıoğlu "Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanuna İlişkin Değerlendirme". **CHD**. Ağustos 2018.

Erdem, Mustafa Ruhan, Durmuş Tezcan, Oğuz Sancakdar ve Rifat Murat Önok, **İnsan Hakları El Kitabı**, 8. Baskı, Seçkin Yayınevi, Ankara, 2019.

Erdoğan, Canan. "Çocukların Kişisel Verilerinin Korunması (Sosyal Medya Örneği Kapsamında)" **D.E.Ü. Hukuk Fakültesi Dergisi**, Sayı:21 (Özel Sayı), 2019, ss.2445-2467.

Erdoğan, Yavuz. "Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi (MADDE 135, 136, 137, 138)" **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:8, Sayı:2, Aralık 2013.

Erişir, Rabia Merve ve Deniz Erişir. "Yeni Medya ve Çocuk: Instagram Özelinde Sharenting (Paylaşanababalık) Örneği" **Yeni Medya**, Sayı: 4-5, 2018 Bahar-Güz ss.50-64.

Elmalıca, Hasan. "Bilişim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, 2016, ss.1603-1636.

Ertuğrul Meltem. "Çocuğun Kişisel Verilerinin Velisi Tarafından Sosyal Medyada Kullanılmasının Kişilik Hakkı İhlali Bakımından Değerlendirilmesi", **YBHD**, Yıl:6, Sayı:2, 2021, ss.513-564.

Girgin, Ömer Ali ve Seray Gönal. "Çocuğun Kişisel Verilerinin Sosyal Medyada Ebeveyn Tarafından Paylaşılmasının Hukuki Sonuçları" **TAAD,** Cilt:11, Sayı: 44, Ekim 2020.

Güzel, Cansel. "Sosyal Medyanın Neliği, Gelişimi ve Kullanım Alanları Üzerine Kuramsal Bir İnceleme", **Sosyolojik Düşün**, Cilt:5, Sayı:2, Aralık 2020.

Gönen, Doruk. **Tüzel Kişilerde Kişilik Hakkı ve Korunması**, On İki Levha Yayıncılık, İstanbul, 2011.

Gönen, Serkan, Halil İbrahim Ulus, Ercan Nurcan Yılmaz. "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", **Bilişim Teknolojileri Dergisi**, Cilt: 9, Sayı: 3, 2016, ss.229-236.

Gözübüyük, Şeref, Feyyaz Gölcüklü. **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması**, Turhan Kitabevi, Ankara, 2009.

Gür, İkbal. **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Turhan Kitabevi, Ankara, 2010.

Helvacı, Serap, **Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar**, Beta Yayınları, İstanbul, 2001.

Henkoğlu, Türkay. **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, 1. Baskı, Yetkin Yayınları, Ankara, 2015.

İçel, Kayıhan, Yener Ünver. **Kitle İletişim Hukuku (Basın-Radyo-Televizyon-Sinema-Video-İnternet)**, Yeniden İncelenmiş 9. Baskı, Beta Yayıncılık, İstanbul, 2012.

İmamoğlu, Hülya. "Çocuğun Kişiliğinin Ana Babaya Karşı Korunması", **AÜHFD**, Cilt:54, Sayı:2, 2005, ss.183-218.

İşgüzar, Hasan. "Kişilik Hakkının İhlali Nedeniyle Manevi Tazminat Davasının Şartları", **Ankara Barosu Dergisi,** Sayı:6, 1990, ss.855- 876.

İtişgen, Rezzan. "Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu", **Türkiye Adalet Akademisi Dergisi**, Yıl: 6, Sayı:23, Ankara, Ekim 2015, ss.179-202.

Karakaş, Muhammed Emin. "Dijital Geçmişin İnternet Erişiminden Kaldırılması 'Unutulma Hakkı' ve Türk Hukukunda Görünümü", **Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 3 Sayı: 2 Yıl: 2020, ss.262-289.

Kaya, Mine. **Elektronik Ortamda (Elektronik Haberleşme- İnternet- Sosyal Medya) Kişilik Hakkının Korunması**, Seçkin Yayınları, Ankara, Eylül 2015.

Keser Berber, Leyla, Ayça Atabey. "Yapay Zeka Sistemlerinin Çocuk Haklarına Etkilerinin Değerlendirilme Yöntemi: Çocuk Hakları Etki Analizi" **Adalet Dergisi**, Cilt:66, Sayı:1, 2021, ss.55-85.

Ketizmen Muammer, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008.

Kent Bülent, "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu", **Bilişim Hukuku Dergisi**, Cilt :2, Sayı:1, 2020, ss.1-46.

Kerim Kılıç, "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135**)", Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:25, Sayı:1 Haziran 2021, ss.1-45.

Kılınç, Doğan. "Anayasa Mahkemesinin Özel Hayatın Korunmasına İlişkin 2013/1614 Sayılı Kararı Üzerine Değerlendirmeler", **International Journal Of Legal Progress**, Cilt:1, Sayı: 2, 2015, ss.177-204. (Özel Hayat)

Kılınç, Doğan. "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:61, Sayı:3, Yıl:2012, ss.1089-1169.

Kietzmann, Jan H. Kristopher Hermkens, Jan P. Mccarty, Bruno S. Silvestre. "Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media" **Busines Horizons**, Cilt: 54, Sayı: 3, 2011, ss.241-251. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.687.4642&rep=rep1&type=pdf (E.T:15/01/2022).

Kilkelly, Ursula. "Özel Hayata Ve Aile Hayatına Saygı Gösterilmesi Hakkı (Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Klavuz)", **İnsan Hakları El Kitapları No. 1**, Strasbourg, 2011.

Kişisel Verileri Koruma Kurumu, "Çocukların Kişisel Verilerinin Korunması-Ürün ve Hizmet Geliştirenler Bakımından Dikkat Edilmesi Gerekenler", **KVKK Yayınları**, Ankara, 2020.

Koca, Mahmut ve İlhan Üzülmez. "Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)" **D.E.Ü. Hukuk Fakültesi Dergisi,** Prof. Dr. Durmuş TEZCAN'a Armağan, Cilt:21, Özel Sayı, 2019, ss.69-93.

Koçak, N. Gizem. **Bireylerin Sosyal Medya Kullanım Durumlarının ve Motivasyonlarının Kullanımlar ve Doyumlar Yaklaşımları Bağlamında İncelenmesi: Eskişehir'de Bir Uygulama**, (Yayınlanmamış Doktora Tezi), Anadolu Üniversitesi, Eskişehir, 2012.

Kontoğlu, Sena. "Alman Sosyal Ağ Kanunu," **Türkiye Adalet Akademisi Küresel Bakış Çeviri Hukuk Dergisi**, Cilt: 8, Sayı:24, Haziran 2018, ss.143-150.

Korkmaz, Ali. "İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması", **KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi**, Sayı: 16 (Özel Sayı I), 2014. (Ali Korkmaz)

Korkmaz, İbrahim. **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayıncılık, 2. Baskı, Ankara, 2019.

Köksal, Yüksel, Şuayb Özdemir. "Bir İletişim Aracı Olarak Sosyal Medya'nın Tutundurma Karması İçerisindeki Yeri Üzerine Bir İnceleme", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt:18, Sayı:1, 2013, ss.323-337.

Köse Aysun, Melike. **Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)**, Seçkin Yayıncılık, Ankara, 2018.

Kuruoğlu, Kübra. “Dijital Ortamda Panoptisizm.” **Akademik Sosyal Araştırmalar Dergisi**, Sayı:31, Ekim 2016, ss.254-267.

Kurt, Hayrettin. “Erişim Engellemeden Demokratik Toplum ya da Kamu Düzenine Eleştirel Bir Bakış”, **Adalet Dergisi**, Cilt: 67, Sayı:2, 2021, ss.151-162.

Küzeci, Elif. **Kişisel Verilerin Korunması**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010.

Küzeci, Elif. **Kişisel Verilerin Korunması**, On İki Levha Yayıncılık, 4. Baskı, İstanbul, 2021.(2021)

Laçin, İrem. “Unutulma Hakkı”, **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, Doç. Dr. Melike Batur Yamaner’in Anısına Armağan, Cilt: 1, 2014, ss.391-419.

Malkoç, İsmail. **Açıklamalı Türk Ceza Kanunu**, Cilt II, Malkoç Kitabevi, 2013.

Mendos Kuşkonmaz, Elif. Kişisel Verilerin **Türk Ceza Kanunu Kapsamında Korunması**, (Yayımlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013.

Metin, Yüksel. “Temel Hakların Sınırlandırılması ve Ölçülülük: Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?”, **SDÜHFD,** Cilt: 7, Sayı 1, 2017, ss.1-74.

Nair, Güney ve Emine Balta. “Bilgi İletişim Teknolojileri Kullanımında Sınırları Aşan Bir Sosyal Sorun Alanı Olarak Unutulma Hakkı” **CÜ Sosyal Bilimler Dergisi**, Cilt: 41, Sayı: 2, Aralık 2017, ss.113-126.

Nalbantoğlu, Seray. “Bir Temel Hak Olarak Unutulma Hakkı”, **Türkiye Adalet Akademisi Dergisi**, Yıl:9, Sayı: 35, 2018, ss.583-605.

Oğuzman, Kemal, Özer Seçili, Saibe Oktay Özdemir**, Kişiler Hukuku (Gerçek ve Tüzel Kişiler),** 12. Baskı, Filiz Kitabevi, İstanbul, 2012.

Orhan, Uğur. "Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:70, Sayı:4, 2021, ss.1359-1384.

Önok, Murat. "Kişisel Verilerin Korunması Bağlamında 'Unutulma Hakkı' Ve Türkiye Açısından Değerlendirmeler", **İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:16, Sayı:1, 2017, ss.155-188.

Özbakır, Ali Fuat. **Sosyal Medyada ve İnternette Hukuki Sorumluluk**, Adalet Yayınevi, Ankara, 2019.

Özbek, Veli Özer, Koray Doğan. Pınar Bacaksız. **Türk Ceza Hukuku Genel Hükümler**, 11.Baskı, Seçkin Yayıncılık, Ankara, 2020.(Genel)

Özbek, Veli Özer, Koray Doğan. Pınar Bacaksız. **Türk Ceza Hukuku Özel Hükümler,** 16.Baskı, Seçkin Yayıncılık, Ankara, 2021.

Özdemir, Hayrünnisa. "Haberleşmenin Gizliliği ve Kişisel Veriler", **Erzincan Hukuk Fakültesi Dergisi**, Cilt:13 Sayı:1-2, 2009.

Özdemir, Hayrünnisa. **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayınları, Ankara 2009. (Elektronik)

Özgenç, İzzet. **Türk Ceza Hukuku Genel Hükümler**, Seçkin Yayıncılık, Ankara, 2011.

Öztürk, Bahri, Elif Altınok Çalışkan, Serkan Seyhan. **Kişisel Verilerin Korunması Hukuku Teorik Ve Pratik Çalışma Kitab**ı, Seçkin Yayıncılık, Ankara, 2021.

Özocak, Gürkan. "Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti", ss.1-18, http://ozocak.com/Dosyalar/a104b3.pdf (E.T:13/01/2022).

Reyhani Yüksel, Sera. **Velayet Hakkının Anayasal Sınırları**, Legal Yayıncılık, İstanbul, 2016.

Salihpaşaoğlu, Yaşar. "Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme", **Gazi Üniversitesi Hukuk Fakültesi Dergisi** Cilt: 17, Sayı: 3, 2013, ss.227-266.

Sert, Şeyma. **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Seçkin Yayınları, Ankara, 2019.

Sınar, Hasan. "Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma Veya Ele Geçirme Suçu (TCK md. 136)", **Kişisel Verileri Koruma Dergisi**, Cilt:2 Sayı:1, ss.33-62.

Sınar, Hasan. "İnternetin Ortaya Çıkardığı Sorunlara Bir Ceza Hukuku Yaklaşımı" **MHB**, Yılmaz Altuğ'a Armağan, Cilt:17, Sayı:1-2, 2020, ss.355-372. (İnternet)

Solove, Daniel J. "The New Vulnerability: Data Security and Personal Information" **GW Law Faculty Publications**, 2008; https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2090&context=faculty_publications (E.T:25/01/2022).

Soyaslan, Doğan. **Ceza Hukuku Özel Hükümler**, Yetkin Yayıncılık, Ankara, 2010.

Soykan, Cavidan. "Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı" **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt:56, Sayı:2, 2007, ss.63-74.

Şen, Ersan. "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", **İstanbul Barosu Dergisi**, Cilt: 83, Sayı:3, 2009, ss.1197-1214.

Şen Ersan ve Yasemin Yurttaş. "Bilgisayar Programları Karşısında Özel Hayatın Korunması" **Terazi Hukuk Dergisi**, Cilt:5, Sayı:42, 2010, ss.29-44.

Şener Gülseren, Fehimi. "Ceza Hukukunda Aleniyet Kavramı" **LAÜ Sosyal Bilimler Dergisi**, Haziran 2014, ss.32-59.

Şimşek, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta Basım, İstanbul, 2008.

Tezcan, Durmuş. "Özel Hayatın Gizliliğini İhlal Ve Kişisel Verilerin Kaydedilmesi Suçu İle İlgili Bazı Gözlemler", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: 71, Sayı:1, 2013, ss.1159-1164.

Turan, Metin. **Bilişim Hukuku**, 5. Baskı, Seçkin Yayıncılık, Ankara, 2021.

Tüfekçi, Zeynep. "Can you see me now? Audience and Disclosure Regulation in Online Social Network Sites". **Bulletin of Science, Technology & Society**, Cilt: 28, Sayı:1, 2008, ss.20-36.

Uçak, Murat. Kişisel Verilerin Hukuka Uygun İşlenmesinde Çocuğun Rızası" **Kişisel Verileri Koruma Dergisi**, Cilt:3, Sayı:1, ss.41-60.

Uluç, Güliz ve Bilal Süslü, "Örnek Yargıtay Kararlarıyla Sosyal Medya Hukuku", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi** Cilt:8 Sayı:17, Aralık 2016, ss.337-351.

Yaşar, Osman, Hasan Tahsin Gökcan, Mustafa Artuç. **Yorumlu Uygulamalı Türk Ceza Kanunu (madde 86-146)**, Adalet Yayınevi, Ankara, 2010.

Yetim, Servet. **Ceza Muhakemesi Hukuku Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (Facebook Örneği)**, Seçkin Yayıncılık, Ankara, 2016.

Yılmaz, Berrak. **Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, (Yayınlanmamış Doktora Tezi) Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2019.

Yokuş Sevük, Handan. **Türk Ceza Hukuku Özel Hükümler**, Güncellenmiş 2. Baskı, Adalet Yayınevi, Ankara, 2019.

Zevkliler, Aydın, Mehmet Beşir Acabey, K. Emre Gökyayla. **Medeni Hukuk- Giriş, Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku**, 6. Baskı, Seçkin Yayınları, Ankara, 2000.

İNTERNET KAYNAKLARI

02/12/2021 Tarihli TBMM Dijital Mecralar Komisyonu Tutanağı, https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=2890, (E.T:23/12/2021).

04/11/2021 Tarihli TBMM Dijital Mecralar Komisyonu Tutanağı, https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=2849, (E.T:23/12/2021).

108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Sırasında/Karşısında Gerçek Kişilerin Korunmasına İlişkin Sözleşme, https://resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf, (E.T:02/12/021).

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, https://mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf, (E.T:22/01/2022).

AB Anlaşması, https://ab.gov.tr/_105.html, (E.T:07/12/2021).

AB Genel Veri Koruma Tüzüğü, https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf, (E.T:26/11/2021).

AB Gizlilik Gereği İçerik Kaldırma Başlıklı Google Formu, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637202230061146146-20083139&rd=1, (E.T:26/11/2021).

ADAB Bodil Lindqvist Kararı, https://kisiselveriihlali.com/Anasayfa/wp-content/uploads/2021/10/Bodil-Linsqvits-Isvec-Karar-Cevirisi-23.10.2021.pdf, (E.T:07/12/2021).

AİHS, https://www.anayasa.gov.tr/media/3542/aihs_tr.pdf, (E.T:03/12/2021).

AYM Karar Arama, https://kararlarbilgibankasi.anayasa.gov.tr/Ara?BasvuruNoYil=2018&BasvuruNoSayi=24439, (E.T:27/11/2021).

Anayasa Mahkemesi Kararı, E.2010/40, K.2012/8, 19/01/2012, https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2012/8?EsasNo=2010%2F40, (E.T:12/11/2021).

Anayasa Mahkemesi Kararı, Youtube Llc Corporatıon Servıce Company ve diğerleri [GK], Bireysel Başvuru No: 2014/4705,

https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/4705?BasvuruNoYil=2014&BasvuruNoSayi=4705, (E.T:27/09/2021).

Anayasa Mahkemesi Kararı, Ayla Demir İşat [GK], Bireysel Başvuru No: 2018/24245, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/24245, (E.T:22/01/2022).

Anayasa Mahkemesi Kararı, N.B.B. [GK], Bireysel Başvuru No: 2013/5653, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653 (E.T:01/01/2022).

Anayasa Mahkemesi Kararı, Yaman Akdeniz ve diğerleri, Bireysel Başvuru No: 2014/3986, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/3986?KelimeAra%5B%5D=yaman+akdeniz&BasvuruAdi=YAMAN+AKDEN%C4%B0Z+VE+D%C4%B0%C4%9EERLER%C4%B0, (E.T05/10/2021).

Anayasa Mahkemesi Kararı, 2015/32 E. 2015/102 K. 12/11/2015 T., https://www.resmigazete.gov.tr/eskiler/2015/12/20151202-16.pdf, (E.T:13/12/2021).

Alman Ağ Yaptırım Yasası (NetzDG), https://detr.abcdef.wiki/wiki/Netzwerkdurchsetzungsgesetz#Soziale_Netzwerke, (E.T:18/09/2021).

Avrupa Konseyi, https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020093815001_tur.pdf, (E.T:02/12/2021).

BBC, “5 soruda Facebook verilerini 'usulsüz kullanmakla' suçlanan Cambridge Analytica”, **BBC Dünya Haberleri,** https://www.bbc.com/turkce/haberler-dunya-43469094, (E.T:17/01/2021).

Dülger, Murat Volkan. “Gdpr Ve Kvkk Bakımından Çocukların Kişisel Verilerinin Korunması Ve Konuya İlişkin Kurul Kararının Değerlendirilmesi” **HukukiHaber.net**, https://www.hukukihaber.net/gdpr-ve-kvkk-bakimindan-cocuklarin-kisisel-verilerinin-korunmasi-ve-konuya-iliskin-kurul-kararinin-degerlendirilmesi-makale,8753.html (E.T:16/10/2021).

Erişim Sağlayıcıları Birliği Tüzüğü, https://www.esb.org.tr/wp-content/uploads/2021/03/Esb-Tuzugu-2016.pdf, (E.T:30/09/2021).

Erişim Sağlayıcıları Birliği Sıkça Sorulan Sorular, https://www.esb.org.tr/s-s-s/, (E.T:30/09/2021).

Gerçek Gündem. “Kişisel bilgiler çalınmıştı! Yemek Sepeti krizinde kafa karıştıran sorular.”, **Gerçek Gündem**, 18/04/2021, https://www.gercekgundem.com/ekonomi/267745/kisisel-bilgiler-calinmisti-yemek-sepeti-krizinde-kafa-karistiran-sorular, (E.T:25/11/2021).

Griffin, Andrew. “Sosyal Medyada Henüz Yazmadıklarımız Bile Gizli Değil”, (Çev. Demrikol, Elvide) **İndependent Türkiye**, 22/01/2019, https://www.indyturk.com/node/10186/haber/sosyal-medyada-hen%C3%BCz-yazmad%C4%B1klar%C4%B1n%C4%B1z-bile-gizli-de%C4%9Fil, (ET:14/06/2021).

Hablemitoğlu, Şengül. “Çocuk Hakları İhlali ve Çocukların İstismar Alanı Olarak Sosyal Medya”, 2016, https://www.linkedin.com/pulse/%C3%A7ocuk-haklar%C4%B1-ihlali-ve-%C3%A7ocuklar%C4%B1n-istismar-alan%C4%B1-ii-hablemito%C4%9Flu, (E.T:30/06/2021).

İnanç Sönmez, Bade. “Türkiye'de Kaç Kişinin, Ne Kadar ve Hangi Amaçla İnternet Kullandığı Açıklandı.”, **Webtekno Teknoloji Haberleri,** https://www.webtekno.com/turkiye-de-kac-kisinin-ne-kadar-ve-hangi-amacla-internet-kullandigi-aciklandi-h107112.html, (E.T:03/08/2021).

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik, https://resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm, (E.T:30/09/2021).

Kılınç, Şahin. "Mark Zuckerberg'den Veri Skandalı Açıklaması: Hata Yaptık, Ayrıca Bunlar Buz Dağının Görünen Kısmı", **Webtekno,** https://www.webtekno.com/mark-zuckerberg-den-veri-skandali-aciklamasi-hata-yaptik-ayrica-bunlar-buz-daginin-gorunen-kismi-h42795.html, (E.T:12/09/2021).

Kılınç, Ümit. "Instagram'daki Gizli Profilleri Gösteren Bir Web Sitesi Ortaya Çıktı", **Webtekno,** https://www.webtekno.com/instagram-gizli-profilleri-gosteren-web-sitesi-ortaya-cikti-h98955.html, (E.T:12/09/2021).

Kişisel Verilerin Korunması Kanunu, https://mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, (E.T:10/10/2021).

Kişisel Verileri Koruma Kurulu Kararı Özel Nitelikli Veriler, https://kvkk.gov.tr/Icerik/5408/Ozel-Nitelikli-Kisisel-Verilerin-Kanuna-Aykiri-Sekilde-Internet-ve-Sosyal-Medya-Mecralarinda-Paylasilmasi, (E.T:14/11/2021).

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, https://resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, (E.T:27/11/2021).

Medya kelimesinin anlamı, kökeni ve tarihçesi, 24/08/2019, https://www.kokeni.com/medya-kelimesinin-anlami-kokeni-ve-tarihcesi/, (E.T:27/09/2021).

Mayfield, Anthony. "What is Social Media", http://www.icrossing.co.uk/fileadmin/uploads/eBooks/What_is_ Social _ Media_iCrossing_ebook.pdf (E.T: 10/08/2021).

Our Rights in a Digital World (A snapshot of children's views from around the world), https://5rightsfoundation.com/uploads/Our%20Rights%20in%20a%20Digital%20World.pdf, (E.T:15/01/2022).

Şekercioğlu, İlker. "İnstagram Yine Kopyaladı" **ShiftDelete.net**, https://shiftdelete.net/instagramdan-koleksiyonlar-ozelligi-81208, (E.T:13/12/2021).

Teknik Düzenlemelerin Bildirimi ve Bilgi Toplumu Hizmetlerine İlişkin Kurallar Hakkında Bir Usul Belirlenmesine Yönelik 2015/1535 Sayılı Direktif, https://ugdgm.ticaret.gov.tr/data/5f450c3f13b8761320144cdc/Avrupa%20Birli%C4%9Fi%20D%C3%BCzenlenmemi%C5%9F%20Alan%20Yasal%20%C3%87er%C3%A7eve.pdf, (E.T:23/12/2021).

TÜİK. "Hanehalkı BT Kullanım Araştırması" **TÜİK,** https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679, (E.T:27/09/2021).

TÜİK. "Hanehalkı BT Kullanım Araştırması 2021 Yılı", **TÜİK**, https://data.tuik.gov.tr/Bulten/Index?p=Cocuklarda-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2021-41132, (E.T:22/12/2021).

Türkiye Cumhuriyeti Anayasası, https://mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5, (E.T: 06/01/2021, 30/09/2021).

Türk Ceza Kanunu, https://mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5, (E.T:10/10/2021).

Türk Ceza Kanunu Madde Gerekçeleri, https://docplayer.biz.tr/1257504-Turk-ceza-kanunu-madde-gerekceleri.html, (E.T:05/01/2022).

Türk Dil Kurumu, https://sozluk.gov.tr/, (E.T:21/11/2021, 07/09/2021).

The Independent, "Woman faces £9,000 fine if she posts pictures of her son on Facebook", **The Independent**, 12/07/2018, https://www.independent.co.uk/news/world/europe/facebook-fines-woman-son-photos-post-social-media-court-italy-rome-a8155361.html (E.T: 16/10/2021).

Ulus, Ç. "Blogger" anneye çocuk istismarı suçlaması!" **Gazetevatan**, http://www.gazetevatan.com/-blogger-anneye-cocuk-istismari-suclamasi--1080670-gundem/ (E.T:16/10/2021).

Yargıtay Karar Arama, https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/, (E.T:12/09/2021-25/01/2022).

Yemek Sepeti Kamuoyu Duyurusu KVKK, https://kvkk.gov.tr/Icerik/6936/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Yemek-Sepeti-Elektronik-Iletisim-Perakende-Gida-Lojistik-AS, (E.T:25/11/2021).

Yemek Sepeti Veri İhlal Bildirimi KVKK, https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi, (E.T:29/11/2021).

Yıldız, Rıdvan. "Sosyal Medyada Konusu Suç Teşkil Eden İçeriğin Paylaşılması", https://www.bartin.info/sosyal-medyada-konusu-suc-teskil-eden-icerigin-paylasilmasi-makale,1772.html, (14/11/2021).

Webhakim, "Instagram Gizli (Kapalı) Hesap Görme Uygulaması 2022", **Webhakim**, https://webhakim.com/instagram-gizli-hesap-gorme-uygulamasi.html, (E.T:12/09/2022).

FACEBOOK, İNSTAGRAM, TWİTTER TANIM, İLKE VE KOŞULLARI

Facebook. “Veri İlkesi”, https://www.facebook.com/policy.php?locale=tr_TR, (E.T:12/09/2021-25/01/2022).

Facebook. “Ülke veya yaş kısıtlamalarını Facebook Sayfama nasıl eklerim ve bunları nasıl düzenlerim?” **Facebook Yardım Merkezi**, https://tr-tr.facebook.com/help/778445532225441?helpref=search&query=ya%C5%9F%20k%C4%B1s%C4%B1tlamas%C4%B1%20kullan%C4%B1lmas%C4%B1%20%C3%B6enri&search_session_id=e892e6f5b4fe0223abe2841a506a4b13&sr=0, (E.T:23/12/2021).

Facebook. “Zaman Tüneli.” **Facebook Yardım Merkezi,** https://tr-tr.facebook.com/help/search?query=zaman%20t%C3%BCneli, (E.T:17/09/2021).

Facebook. “Bir Sorunu Düzeltin.” **Facebook Yardım Merkezi,** https://tr-tr.facebook.com/help/1719980288275077/?helpref=hc_fnav, (E.T:14/09/2021).

İnstagram. “Kullanım Koşulları” **İnstagram Yardım Merkezi**, https://help.instagram.com/581066165581870, (E.T:23/12/2021).

İnstagram. “5651 sayılı Kanun uyarınca hazırlanan Facebook Şeffaflık Raporu'nu nerede bulabilirim?”, **İnstagram Yardım Merkezi**, İnstagram 2021 yılına ait Mart-Haziran 2021, Haziran 2021, ve Temmuz-Aralık 2021 Şeffaflık Raporu, https://help.instagram.com/842275446492500/?helpref=related_articles, (E.T:19/01/2022).

İnstagram. “İnstagram Veri İlkesi”, **İnstagram Yardım Merkezi,** https://help.instagram.com/519522125107875, (E.T:18/01/2022).

İnstagram. “Instagram'da verilerime nasıl erişirim veya verilerimi nasıl gözden geçiririm?” **İnstagram Yardım Merkezi**, https://help.instagram.com/181231772500920, (E.T:22/01/2022).

İnstagram. “Birinin instagram fotoğraf ve videolarıma yorum yapmasını nasıl engellerim veya engelini nasıl kaldırırım?” **İnstagram Yardım Merkezi,** https://help.instagram.com/234506470408555/?helpref=related_articles, (E.T:22/01/2022).

İnstagram. “Birisinin gönderilerime yorum yapmasını geçici olarak sınırlayabilir miyim?” **İnstagram Yardım Merkezi,** https://help.instagram.com/4106887762741654/?helpref=search&query=yorum%20kapat&search_session_id=ae3cff9c95bd55542431b695948f40e5&sr=19, (E.T:22/01/2022).

İnstagram. “İnstagram Direct’i Nasıl Kullanırım?” **İnstagram Yardım Merkezi**, https://tr-tr.facebook.com/help/instagram/684926628219030/?helpref=search, (E.T:17/09/2021).

Twitter. “Twitter Privacy Policy”, https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-aug-19th-2021/Twitter_Privacy_Policy_EN.pdf, (E.T:12/09/2021).

Twitter. “Tweettleme” **Twitter Yardım Merkezi**, https://help.twitter.com/tr/using-twitter/how-to-tweet, (E.T:14/09/2021).