T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI

ELEKTRONİK ORTAMDA SAKLANAN KİŞİSEL VERİLERİN ELDE EDİLMESİ / DEĞİŞTİRİLMESİ SURETİYLE İŞLENEN SUÇLARIN CEZA HUKUKU AÇISINDAN DEĞERLENDİRİLMESİ

DOKTORA TEZİ

Alaattin BÜK

Danışmanlar
Prof. Dr. Remzi FINDIKLI
Prof. Dr. Hasan Hüseyin BALIK

Ankara - 2015

T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ VE YÖNETİMİ ANABİLİM DALI

ELEKTRONİK ORTAMDA SAKLANAN KİŞİSEL VERİLERİN ELDE EDİLMESİ / DEĞİŞTİRİLMESİ SURETİYLE İŞLENEN SUÇLARIN CEZA HUKUKU AÇISINDAN DEĞERLENDİRİLMESİ

DOKTORA TEZİ

Alaattin BÜK

Danışmanlar
Prof. Dr. Remzi FINDIKLI
Prof. Dr. Hasan Hüseyin BALIK

Ankara - 2015

ONAY

Alaattin BÜK tarafından hazırlanan "Elektronik Ortamda Saklanan Kişisel Verilerin Elde Edilmesi/Değiştirilmesi Yoluyla İşlenen Suçların Ceza Hukuku Açısından Değerlendirilmesi" başlıklı bu çalışma, 25/12/2015 tarihinde yapılan savunma sınavı sonucunda (~~oybirliği~~ / oyçokluğu) ile başarılı bulunarak jürimiz tarafından Güvenlik Stratejileri ve Yönetimi Anabilim dalında Doktora tezi olarak kabul edilmiştir.

.....

Prof. Dr. Remzi FINDIKLI (Başkan-Danışman)

.....

Prof. Dr. Hasan Hüseyin BALIK

.....

Prof. Dr. Doğan SOYARSLAN

.....

Yrd. Doç. Dr. Oğuz ATA

.....

Yrd. Doç. Dr. Mustafa YAYLA

TELİF HAKLARI BEYANNAMESİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Doktora tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde yollama yaparak yararlandığımı belirtir; bunu şerefimle beyan ederim.

Enstitü veya başka herhangi bir mercii tarafından belli bir zamana bağlı kalmaksızın, tezimle ilgili bu beyana aykırı bir durumun tespit edilmesi durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

25./12./2015

Alaattin BÜK

ÖNSÖZ

Bu çalışmayı yapma konusunda bana fikir veren ve yol gösteren danışman hocam Prof. Dr. Remzi FINDIKLI, Prof. Dr. Hasan Hüseyin BALIK ile katkılarından dolayı Prof. Dr. Kemal BAŞLAR, Prof. Dr. Cengiz BAŞAK, Yrd. Doç. Dr. Mustafa YAYLA ve Prof. Dr. James Jim DRYLIE'ye teşekkür ederim.

ÖZET

T.C.
Polis Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Stratejileri ve Yönetimi Anabilim Dalı
Elektronik Ortamda Saklanan Kişisel Verilerin
Elde Edilmesi / Değiştirilmesi Suretiyle İşlenen Suçların
Ceza Hukuku Açısından Değerlendirilmesi
Alaattin BÜK
Doktora Tezi
Tez Danışmanları: Prof. Dr. Remzi FINDIKLI
Prof. Dr. Hasan Hüseyin BALIK
2015 – 277 Sayfa

Belirli bir kişiye ilişkin olan veya belirli bir kişiyle irtibatlandırılabilen bütün bilgiler olarak tanımlanabilen kişisel verilerin işlenmesi günümüzde fizik alandan çıkarak bilişim alanına kaymıştır. Gelişen teknoloji ile birlikte kişisel verilerimiz sadece kamu kurumları tarafından değil, özel tüzel kişilikler ve kişiler tarafından da işlenmektedir. Temelinde korunan hukuki yarar olarak özel hayatın gizliliğinin korunması amaçlanan kişisel verilerin; toplanması, elde edilmesi, kaydedilmesi, düzenlenmesi, depolanması, uyarlanması, değiştirilmesi, değerlendirilmesi, kullanılması, açıklanması, aktarılması, ayrılması, birleştirilmesi, dondurulması, silinmesi veya yok edilmesi gibi işlemlerin belirlenen ilkeler doğrultusunda yerine getirilmesi amaçlanmaktadır. Bununla birlikte kişisel verileri koruma altına alınan kişiler yönünden ise; kendisine ait bilgiler ile ilgili olarak, kanunların getirdiği koruma önlemlerinin ihlal edilmesi halinde, bu ihlali yapan kurum veya kişiler aleyhine tazminat veya ceza davası açmak hakkı da bu korunmanın kapsamındadır.

Mevzuatımızda kişisel verilerin korunmasına ilişkin olarak 5237 sayılı TCK'nin 135, 136 ve 138. maddelerinde düzenleme bulunmakta olup, inceleme konusunun bilişim alanında bulunan kişisel veriler olması nedeni ile yine aynı

yasanın 243 ve 244. maddelerinin birlikte incelenmesi gerekir. Fizik nitelik kazanmış kişisel veriler ile bilişim alanına dahil olmakla birlikte ayrı bir inceleme konusu olan TCK'nin 245. maddesinde düzenlenen banka ve kredi kartlarının kötüye kullanılması bu suçun suçu kapsama dahilinde değildir. Henüz tasarı halinde olan Kişisel Verilerin Korunması Hakkındaki Kanunun 16. maddesinde ki cürümlere ilişkin madde TCK'nin 135. ve 136. maddelerine atıf yaparken, 17. maddesinde tasarıdaki kabahatlere ilişkin düzenlemeler bulunmaktadır. Kişisel verilerin korunmasının uluslararası boyutu ile karşılaştırmalı hukuk açısından özellikle ABD'nin hukuki düzenlemeleri önem arz etmekte olup, bizim sistemimiz daha çok Fransız sistemi ile benzeştiği için Avrupa hukuku da incelenmiştir. Özellikle CMK, PVSK gibi bazı yasalarımızda da kişisel veriler ile ilgili özel hükümler içeren hükümler bulunmaktadır. Bir bakıma bir sentez olan bu konu, yargısal faaliyet açısından da yeni bir alan olduğundan dolayı içtihatlar ve bilimsel veriler birlikte değerlendirilmiştir.

Bilişim alanının yapısı gereği klasik suçlarında kişisel verilerek kullanılarak işlenmesinin mümkün kıldığı gözetilerek, doğrudan bilişim alanında bulunan kişisel verilerin korunmasına yönelik bir düzenlemenin olmayışı, tüzel kişilerin fail ve mağdur sıfatı, ölen kişilerin kişisel verilerinin korunması, yer bakımından yetki, suçun işlendiği zaman sorunu, suçun önemine rağmen müeyyidelerin caydırıcılıktan uzak oluşu, bu suç tipiyle ilgilenen özel adli birimlerin olmaması gibi sorunlar halen çözüm beklemektedir.

Kişisel verilerin korunmasına yönelik etkin bir yasa oluşturulması acil bir ihtiyaçtır. Ancak bu yasa yapılıncaya kadar elimizde bulunan uluslararası sözleşmeler, Türk Ceza Kanunu ve özel yasalardaki ceza düzenlemeleri ile yasal boşluk bulunan konularda içtihatlar da kullanılarak kişisel veriler korunmaya çalışılmalıdır.

Anahtar Kelimeler: Kişisel Veri**,** Kişisel Verilerin Korunması, Bilişim Suçları, Siber Suçlar, Bilişim Alanındaki Kişisel Verilerin Korunması, Türk Ceza Hukukunda Kişisel Verin Korunması ve Bilişim Suçları

ABSTRACT

Police Academy
Institute of Security Sciences
Department of Security Strategies and Management

Evaluation of the Crimes Committed by Acquisition or Replacement of Personal Data Stored Electronically in The Light of The Criminal Law

Alaattin BÜK
Ph. D. Dissertation
Supervisors: Prof. Dr. Remzi FINDIKLI
Prof. Dr. Hasan Hüseyin BALIK
2015 – 277 Page

Today, personal data described as all information relating or being related to specific individual has shifted from the material realm to the electronic discourse. With the development of technology, our personal data is processed not only by the official but also private sector. In order to protect personal privacy, the activities like personal data collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, disclosure by transmission, dissemination, alignment or combination, blocking, erasure or destruction should be carried out in accordance with determined principles. In addition to this, from the point of those whose data is under the protection of law, in case of any violation relating to the protection of personal data, protection also includes right to bring a civil or criminal action against violators.

The articles 135, 136 and 138 of the Turkish Penal Code concern the general protection of personal data therefore they should be evaluated with the articles 243 and 244 of the Turkish Penal Code containing provisions relating to automatic processing of personal data. Personal data in a psyhical forms and, though it concerns automatic processing of personal data, the article 245 of Turkish Penal Code relating

to improper use of bank or credit cards are not applied to this crime. While the article 16 of the Turkish Draft Law on Protection of Personal Data concerning the felony refers to the articles 135 and 136 of Turkish Penal Code, the article 17 of the same draft contains provisions on the misdemenaur. It is very important to take into consideration of the international dimension of the personal data protection and especially USA legal perspective, in addition to this as our legal system is more similar with the French Legal System it is also necassary to investigate European Law. Especially, Turkish Penal Procedure Code and The Law on the Powers and Duties of Police also contain some special provisions relating to personal data. As the topic is relatively new from the judicial perspectives the scientific data and the case-law considered together.

Given the nature of the information field it is possible that classic crimes can be comitted by using personal data. Problems like the lack of direct codification concerning personal data, the corporate entity's victim and perpetrators status, the competence of the criminal court, the protection of the deceased persons'personal data, the problem of the time of commission of the crime, the unsifficient sanctions for the crime, the lack of special judicial unit responsible for that type of crime still wait solution. The necessity to create an efficient law on the protection of personal data is very clear. However, until the law concerned is enacted, the personal data will be protected with existing international conventions, Turkish Penal Code, the other related domestic law and case laws.

Key Words: Personal Data**,** The Protection of The Personal Data, Cybercrime, The Protection of The Personal Data on İnformation Service, The Protection of Personal Data and Cybercrime in Turkish Criminal Law.

ELEKTRONİK ORTAMDA SAKLANAN KİŞİSEL VERİLERİN ELDE EDİLMESİ / DEĞİŞTİRİLMESİ SURETİYLE İŞLENEN SUÇLARIN CEZA HUKUKU AÇISINDAN DEĞERLENDİRİLMESİ

İÇİNDEKİLER

Sayfa

TEZ ONAY SAYFASI II

TELİF HAKLARI BEYANNAMESİ III

ÖNSÖZ IV

ÖZET V

ABSTRACT VII

İÇİNDEKİLER IX

KISALTMALAR XIV

GİRİŞ 1

BİRİNCİ BÖLÜM

ELEKTRONİK ORTAMDA SAKLANAN KİŞİSEL VERİLERİN ELDE EDİLMESİ VE KULLANILMASI YOLU İLE İŞLENEN SUÇLARIN ORTAK ÖZELLİKLERİ

1.1. KORUNAN HUKUKİ YARAR (HUKUKİ DEĞER) 8

1.1.1. Kişisel Verilerin Korunmasına İlişkin Suçların Hukuki Konusu Olarak Özel Hayatın Gizliliği 11

1.1.2. Kişisel Verilerin Korunmasına İlişkin Genel Bilgiler 15

1.1.2.1. Kişisel Veri **20**

1.1.2.1.1. Hassas Kişisel Veriler **24**

1.1.2.1.2. Anonim Kişisel Veri **27**

1.1.2.2. Kişisel Verinin İşlenmesi **28**

1.1.2.3. Kişisel Verilerin Korunması **31**

1.1.3. Bilişim Suçlarının Konusu Hakkında Genel Bilgiler **34**

1.1.3.1. Bilişim Konusunda Temel Bilgiler **35**

1.1.3.1.1. Bilişim 36

1.1.3.1.2. Bilişim Alanı 37

1.1.3.1.3. Bilişim Sistemi 38

1.1.3.1.4. Veri 39

1.1.3.2. Bilişim Suçu Kavramı Hakkında Genel Bilgiler **40**

1.1.3.2.1. Siber Cinayet 42

1.1.3.2.2. Siber Tehdit ve Şantaj 42

1.1.3.2.3. Siber Dolandırıcılık 42

1.1.3.2.4. Siber Hırsızlık 43

1.1.3.2.5. Siber Terörizm 43

1.1.3.3. Bilişim Suçları Alanındaki Hukuki Düzenlemeler **44**

1.1.3.4. İnternet Üzerinden İşlenen Suçlarda Kişilik Haklarının İhlali ve Korunması **46**

1.1.4. Sonuç Olarak Korunan Hukuki Yarar **48**

1.2. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK HUKUKİ DÜZENLEMELER **52**

1.2.1. Uluslararası Düzenlemeler **54**

1.2.2. Ulusal Düzenlemeler **63**

1.2.2.1. Anayasa **64**

1.2.2.2. Avrupa Birliği Komisyonu İlerleme Raporları, Katılım Ortaklığı Belgesi ve Türkiye Ulusal Programında Kişisel Verilerin Korunması **65**

1.2.2.3. Özel Hukuk 68

1.2.2.4. Ceza Hukuku 71

1.2.2.5. Ceza Muhakemesi Kanunu 75

1.2.2.6. Kişisel Verilerin Korunması Kanunu Tasarısı 76

1.2.2.7. Kişisel Verilerin Korunması Kanun Tasarısı'nda Yer Alan Cezai Tedbirler 81

1.3. 5237 SAYILI TÜRK CEZA KANUNUNDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN SUÇ TİPLERİ 83

1.3.1. Kişisel verilerin kaydedilmesi suçu (m.135) 86

1.3.2. Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu (m.136) ve Nitelikli Haller (m.137) 87

1.3.3. Verilerin Yok Edilmemesi Suçu (m.138) 88

1.3.4. Kişisel Verilerin Korunması Hakkındaki Düzenlemelere İlişkin Ortak Bir değerlendirme 89

1.3.5. Bilişim Sistemleri Aracılığıyla Kişisel Veriler Aleyhine İşlenebilecek Suçlara Örnekler 91

1.4. 5237 SAYILI TÜRK CEZA KANUNUNDA BİLİŞİM SUÇLARINA İLİŞKİN SUÇ TİPLERİ 96

1.4.1. Hukuka Aykırı Olarak Bilişim Sistemine Girme veya Sistemde Kalma Suçu (m.243) 97

1.4.2. BilişimSisteminin İşleyişinin Engellenmesi, Bozulması, Verilerin Yok Edilmesi veya Değiştirilmesi Suçu (m. 244/1-2-3) 103

1.4.3. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu (m. 244/4) 105

1.4.4. Madde Koruması Altına Alınan Fiilerin Doğuracağı Sonuçlara Göre İncelenmesi 106

1.4.4.1. Verileri Bozma……107

1.4.4.2. Verileri Yok Etme……..….107
1.4.4.3. Verileri Değiştirme…….108
1.4.4.4. Verileri Erişilmez Kılma…….108
1.4.4.5. Veri Yerleştirme……..108
1.4.4.6. Verileri Başka Bir Yere Gönderme……...109
1.4.5. Bilişim Alanında Suçlar Bölümünde Düzenlenen Suç Tiplerinin Diğer Suç Tipleriyle Olan İlişkisinin İncelenmesi..... 108

İKİNCİ BÖLÜM

SUÇUN UNSURLARININ İNCELENMESİ

2.1. SUÇUN MADDİ UNSURLARI 116
2.1.1. Pozitif Unsurlar 118
2.1.1.1. Hareket **118**
2.1.1.2. Netice **135**
2.1.1.3. Nedensellik Bağı **143**
2.1.2. Negatif Unsurlar 146
2.1.2.1. Hukuka Aykırılık Unsuru **146**
2.1.2.2. Hukuka Uygunluk Nedenleri **150**
2.1.2.2.1. Hakkın Kullanılması **153**
2.1.2.2.2. Meşru Müdafaa **155**
2.1.2.2.3. Kanun Hükmünün Yerine Getirilmesi **156**
2.1.2.2.4. İlgilinin Rızası **160**
2.2. SUÇUN MANEVİ UNSURU 163
2.3. SUÇUN SÜJELERİ 167
2.3.1. Suçun Süjesi Olarak Tüzel Kişilerin Sorumluluğunun İncelenmesi .. 168
2.3.1.1. Tüzel Kişi Kavramı **168**

2.3.1.2. Tüzel Kişilerin Ceza Sorumluluğu 169

2.3.2. Suçun Faili 170

2.3.2.1. Veri İşleyenin Sorumluluk ve Yükümlülükleri 172

2.3.2.2. Bilişim Alanında Saklanan Kişisel Verilere Yönelik Suçlar Yönünden Fail 178

2.3.2.3. Fail Yönünden Eylemin Nitelikli Hali 182

2.3.2.4. Failin İnternet Yönünden İncelenmesi 186

2.3.2.5. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna (5651 sayılı İnternet Kanunu) göre İnternet Süjelerinin Sorumluluğu 188

2.3.3. Suçun Mağduru 192

2.4. YER BAKIMINDAN YETKİ 198

2.4.1. Sınır Ötesi Veri Aktarımı 208

2.5. SUÇUN İŞLENDİĞİ ZAMAN SORUNU 210

2.6. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ 212

2.6.1. Teşebbüs 212

2.6.2. Suçların İçtiması 220

2.6.2.1. Zincirleme Suç……...221

2.6.2.2. Fikri İçtima 225

2.6.3. İştirak 230

2.7. GÖREVLİ MAHKEME VE KOVUŞTURMA 232

2.8. ZAMANAŞIMI 235

2.9. MÜEYYİDE……..……..…..……..……..238

SONUÇ 242

KAYNAKLAR 246

ÖZGEÇMİŞ 275

KISALTMALAR

AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
AİHM : Avrupa İnsan Hakları Mahkemesi
AİHS : Avrupa İnsan Hakları Sözleşmesi
ATM : Automatic Teller Machine (Bankaların Otomatik Vezneleri)
AÜHFD : Ankara Üniversitesi Hukuk Fakültesi Dergisi
AY : Anayasa
Bkz : Bakınız
BM : Birleşmiş Milletler
CD. : Ceza Dairesi (Yargıtay)
CGK. : Ceza Genel Kurulu (Yargıtay)
DARPA : Defense Advanced Research Projects Agency
(Savunma Konulu İleri Araştırma Projeleri Dairesi)
EÜHFD : Erzincan Atatürk Üniversitesi Hukuk Fakültesi Dergisi
EGM : Emniyet Genel Müdürlüğü
EULA : End User License Agreement
(Son Kullanıcı Lisans Sözleşmesi)
f. : fıkra
FBI : Federal Bureau of Investigation
(Federal Soruşturma Bürosu; ABD)
GBT : Genel Bilgi Toplama
GÜHFD : Gazi Üniversitesi Hukuk Fakültesi Dergisi
HFD : Hukuk Fakültesi Dergisi
HD. : Hukuk Dairesi (Yargıtay)
IC3 : Internet Crime Complaint Center
(İnternet Dolandırıcılığı Şikayet Merkezi, ABD)
İBD : İstanbul Barosu Dergisi
İHEB **:** İnsan Hakları Evrensel Beyannamesi
İÜHFD : İstanbul Üniversitesi Hukuk Fakültesi Dergisi
KHK : Kanun Hükmünde Kararname

m.	: madde
NSA	: National Security Agency (Ulusal Güvenlik Dairesi, ABD)
NW3C	:National White Collar Crime Center
	(ABD, Ulusal Beyaz Yaka Suç Merkezi)
OECD	: Ekonomik İşbirliği ve Kalkınma Teşkilatı
PC	: Personal Computer (Kişisel Bilgisayar)
PVSK	: Polis Vazife ve Salahiyet Kanunu
s.	: sayılı (Metin içi), sayfa (Atıf bölümü)
SGK	: Sosyal Güvenlik Kurumu
SÜHFD	: Selçuk Üniversitesi Hukuk Fakültesi Dergisi
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: 5237 sayılı Türk Ceza Kanunu
TTK	: Türk Ticaret Kanunu
vb.	: ve bunun gibi

GİRİŞ

Özel yaşam alanımızın gizliliği hakkında, insan hakları ile ilgili uluslararası belgelerde ve demokratik anayasalarda düzenlemeler bulunmaktadır. Kişisel verilerin korunması kapsamında; kişisel veri olarak niteleyebileceğimiz; fiziksel özellikler, kişisel düşünce, görüş ve inançlar, öğrenim, iş hayatı, sağlık ile ilgili bilgiler ve bireysel hayatı veya ailesi ile olan ilişkileri, haberleşmeleri kişinin rızası olmadan herhangi bir şekil veya durumda kulanılmaması, başkalarına açıklanamaması, eğer kendisi tarafından aleni hale getirilmiş bilgiler varsa yanlızca açıklandığı amaç ve kapsamla sınırlı olarak kullanılabilmesi bulunmaktadır. Son yıllarda elektronik bilgi işlem yöntemleri ile kişisel verilerin derlenmesi, sınıflandırılması, saklanması ve istenildiğinde istenen form ve biçimde kullanılabilmesi olanağı ortaya çıkmıştır. Fakat bunun doğal sonucu özel yaşama ait bu bilgilerin (kişisel verilerin) rıza dışı ve hukuka aykırı olarak kullanılması riski oldukça artmıştır. Kısaca, rıza dışı olarak verilerin kişi veya kamuya duyurulması ve bilginin süratli bir şekilde ilgisi bulunan ya da bulunmayan herhangi bir yere aktarılmasına imkan sağlamıştır.

Teknoloji ve kitle iletişim araçlarındaki gelişmeler de özel hayatın gizliliği hakkına müdahale yöntemlerindeki çeşitliliği önemli derecede artırmaktadır. Örneğin, önceden kişisel verilere ulaşma aracı olarak kullanılan parmak izinin alındığı kişi sayısı çok az iken, günümüzde sadece işlenen suçlardan sonra parmak izi alınanlardan başka, silah ruhsatı, sürücü belgesi ve pasaport gibi evrakların temini için yapılan başvurulardan çalışılan işyerlerine, oradan alışveriş yapılan özel firmalara kadar artık sayılamayacak kadar pekçok alanda herhangi bir nedenle parmak izi alınmayan kişi neredeyse yok gibidir. Hatta sadece parmak izi de değil, göz retinasından ses tanımaya kadar birçok farklı alanda biyometrik tespitlerle yapılmaktadır. Artık kişilerin hayatlarının neredeyse tüm kesimleri herhangi bir şekilde kayıt altına alınmakta, bir çeşit elektronik gözetim sağlanmakta ve sonuç

olarak kişisel verilerin korunması faaliyetlerinin büyük bir tehlike altında bulunduğu görülmektedir[1].

Bilgi ve iletişim teknolojileri sayesinde, kişisel verilerin derlenmesi, bir sistematik dahilinde sınıflandırılması, çok büyük kapasiteli bilgi işlem cihazları içerisinde saklanması ve istenildiği zaman işleme tabi tutularak kolayca ulaşılabilmesi kolaylaşmış olduğu için sonuç olarak özel yaşamla ilgili kişisel verilerin haksız olarak kullanılması yoluyla işlenebilecek suç sayısı da oldukça artmıştır. Bu haliyle, bilişim teknolojisindeki akıl almaz gelişmeler karşısında sınırlı bir alan dışında, pek çok klâsik suçun bilişim yoluyla işlenebileceğini söylemek hayal değildir. Elektronik ortamda saklanan kişisel verilerin elde edilmesi ve kullanılması ile işlenebilecek suç tipine, suçun işleniş şekli, kullanılan vasıtalar ve suçun niteliği itibarı ile sınırsız sayıda örnek vermek mümkündür. Bu örnekler, hırsızlık, dolandırıcılıktan başlayarak en uç noktada adam öldürmeye sebep olmaya kadar varacaktır. Yine bu yöntemle işlenen suçların sonuçları, klâsik suçlara oranla çok büyük ve tahrip edicidir. Örneğin, sanal ortam kullanılarak bilişim cihazları ile entegre edilmiş tıbbi cihazlara manuel olarak ya da internet aracılığıyla müdahale edip, tedaviye ilişkin veriler değiştirilmek suretiyle cinayetler dahi işlenebilmektedir. Artık her bilgisayara bağlı bilgisayar kameraları (webcam) ile kişilerin en mahrem görüntüleri çekilmekte ve bu yolla elde edilen görüntüler şantaj yapmakta kullanılmakta, bu yolla evlilikler bozulup aileler dağılabilmektedir. Devletin resmî güvenlik birimlerinin dışında birçok resmi ya da özel kurum ve kuruluş da bireyler hakkında çok önemli bilgiler toplayarak özel hayatı ihlal etme imkânına sahip hâle gelebilmektedir[2].

Türk hukukunda diğer hukuk sistemlerinin aksine, elektronik ortamdaki kişisel verilerin korunmasına ilişkin özel bir kanunî düzenleme henüz kabul

---

[1] Bozlak, Ayhan, *Avrupa İnsan Hakları Mahkemesi Kararları Çerçevesinde Türk Ceza Hukukunda Özel Hayatın Korunması*, Yayımlanmamış Doktora Tezi, Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2013, s. 2

[2] Cerrah, İbrahim, "Bilişim Teknolojileri ve Etik: Bilişim Teknolojilerinin Güvenlik Hizmetlerinde Kullanımının 'Etik Boyutu' ve 'Sosyal' Sonuçları", *Polis Bilimleri Dergisi*. Ankara: 2002, Cilt: 4, Sayı: 1-2, s. 137-155

edilmemiştir[3]. Bu sebeple, kişisel verilerin herhangi bir şekilde hukuka aykırı olarak tecavüze uğraması halinde Türk Medenî Kanunu ve Borçlar Kanunu'nun kişilik haklarının korunmasına ilişkin hükümleri uygulanmaktadır[4]. Burada tartışılabilecek konulardan en önemlisi ise, klâsik suçu düzenleyen kanunların, bilişim vasıta kılınarak işlenmesi halinde uygulamanın nasıl olacağıdır. Örneğin, bilişim vasıta kılınarak işlenen hakaret suçunda 5237 sayılı Türk Ceza Kanununun (TCK) 125. maddesi uygulanabilecektir. İlgili maddenin 2. fıkrasında "Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.", 4. fıkrasında ise "Ceza, hakaretin alenen işlenmesi hâlinde, altıda biri; basın ve yayın yoluyla işlenmesi hâlinde, üçte biri oranında artırılır." düzenlemeleri getirilerek elektronik ortamda işlenebilecek suçlarda kapsam içine alınmaya çalışılmıştır. Ancak, ceza kanunlarında bilişim suçları düşünülmeden düzenlenen klasik suçlar, bilişim vasıtasıyla işlendiğinde de, yalnızca klasik suça öngörülen sınırlar içerisinde ceza tayin edilebilecektir. Oysa suçun bilişim vasıtasıyla işlenmesi, klâsik fiillere göre, oldukça geniş etki ve sonuçlara neden olabilecektir. İnternet yoluyla işlenen bir hakaret suçunun etki alanı, dünya çapındadır. Böylesi durumlarda, klâsik suç fiilinin cezasını vermek yeterli değildir. Burada, kanunda cezanın alt sınırından uzaklaşılarak ceza verilerek sorun çözümlenir denilebilir. Ancak bu yaklaşım da her zaman adaleti sağlayamayabilir. Açıkçası, bilişim yoluyla

---

[3] Her ne kadar TC. Adalet Bakanlığının hazırladığı ilk "Kişisel Verilerin Korunması Kanun Tasarısı" Bakanlar Kurulu tarafından TBMM'ye sevkedilmis ise de, Tasarı uzun süre komisyonda bekledikten sonra hükümsüz hale gelmiştir. Bkz. TBMM, "Tasarı ve Teklifler", http://www.tbmm.gov.tr /develop/owa/tasari_teklif_gd.sorgu_yonlendirme, (Erişim: 27.11.2014). Bu ilk tasarı ile ilgili elestiriler yönünden ayrıntılı bilgi için bkz. Beyli, Ceylin; *Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Elestiriler*, Türkiye Bilisim Surası Hukuk Çalısma Grubu Kişisel Veriler Raporuna ait Görüsler, http://www.ihop.org.tr/dosya/izleme/tbs_kisisel_veri_ceylin_beyli_gorus1. pdf, s. 3-8, (Erişim: 27.11.2014); Ersoy, Eren; "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", http://www.ab. org. tr /ab06/bildiri/6.doc, (Erişim: 08.07.2010)

Bu konudaki ikinci çalışma 26.12.2014 tarihinde TBMM başkanlığına sunulan metindir. Henüz genel kurul önüne çıkmayan bu taslak adalet komisyonunda incelenmek üzere beklemektedir. Adalet Bakanlığı Kanunlar Genel Müdürlüğü, "Tasarılar", http://www.kgm.adalet.gov.tr/ Tasariasamalari/Tbmmkms/Tbmmkom/kişiselveriler.pdf, (Erişim: 24.05.2015)

[4] Başpınar, Veysel, "Elektronik Tapu Sicili Düzenlenirken, Tapu Sicilinin Aleniyeti ve Diğer Alanlarla İlgili Alınması Gereken Tedbirler", *Ankara Üniversitesi Hukuk Fakültesi Dergisi (AÜHFD)*, 2008, Cilt. 52, Sayı: 3 (97-132), Sayı: 116.

işlenen klâsik suçların, çok daha geniş etki ve sonuçları gözetilerek kanuni düzenlemelerin yapılması gerekmektedir[5].

Uluslararası alanda düzenlenen bilişim alanında bulunan kişisel verilerin korunmasına dair birçok düzenleme bulunmasına ve bu düzenlemelerin zaman içerisende geliştirilerek günün ihtiyacına karşılık verebilecek durumda olmasına karşın Türkiye yeterince bu gelişmeleri takip edememiştir. Belirtilen alandaki koruma TCK'nin sınırlı sayıdaki maddesine havale edilerek uygulayıcıların yorumuna bırakılmış durumdadır. İşte Kanunumuzdaki bu boşluk bu çalışmanın yapılmasında ki ana amaç olmuştur. Klasik yöntemlerle fiziki ortamda kişisel veri biriktirilmesi çok azalmış, genel uygulama bilişim sisteminde depolama olarak uygulanmaktadır. Bilişim sistemleri artık cebe girecek kadar küçülerek inanılmaz derecede yaygınlaştığı için kişisel verilerin elde edilmesi ve kullanılarak suç işlenmesi çok kolaylaşmaktadır. Kaldı ki bilginin paylaşımını kolaylaştıran internetin varlığı da düşünülürse, bilişim sistemlerinde saklanan kişisel verilerin korunması ile ilgili alanın boşluk kabul etmeyeceği ve bu konuda acil düzenlemeler yapılması gerektiği açıktır. Fakat henüz bu alanda bir çalışma yapılmamış olması gözetilerek mevcut kanunlarda ve kanun gücünde kabul edilen uluslararası sözleşmelerde bulunan kişisel verilerin korunmasına ilişkin ceza hükümleri yorumlanarak ilgililerine bir yol haritası çizilmeye çalışılmıştır.

Çok hızlı değişen ve gelişen bir alan olan bilişim karşısında, bu gelişmeye paralel kişisel verileri koruyan hukuki düzenlemeler bulunmadığından kişisel veriler daha korunmasız hale gelmektedir. Bu nedenle araştırmanın kapsamını, sınırlarını ve izlenecek yöntemi belirlemek konusu önemli olduğu için ilk önce bilişim suçları alanında yazılmış kaynaklar taranmıştır. Bilişim suçlarının kaynakları, gelişimi ve bu konudaki hukuki çalışmalar doğrultusunda oluşan fikir kapsamında kişisel verilerin korunmasına yönelik eserler incelenmiştir. Konu ile ilgili olarak internet taranmış, makaleler ve haberler incelenmiştir. Uygulamanın bu konudaki yön vericiliği

[5] Karagülmez, Ali, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, Ankara: Seçkin Yayınevi, 2005, s. 126

incelememiz için önem arzettiğinden yine AİHM ve Yargıtay'ın bu konudaki kararları da incelenmiş, alanında uzman hukukçular ile mülakat yapılmıştır.

Tezin sınırlılıkları yönünden ise, çok geniş bir inceleme alanı olan bilişim alanının da saklanan kişisel verilerin korunmasına ilişkin hukuki alanın her bölümü ile ilgilenilmesi mükün olmadığı gibi araştırmanın amacını da aşacaktır. Bu nedenle inceleme konusu, bilişim sistemi içerisinde kayıtlı olarak tutulan dijital veriler ile sınırlı tutulmuştur. İçerisinde kişisel veri barındıran ve artık bir fizik özellik kazanmış olan banka kartları ve kredi kartlarının çalınması ve kullanılması yolu ile işlenen suçlar hakkında inceleme yapılmamıştır. Kaldı ki bu konuda TCK'nin 245. maddesinde özel bir düzenleme bulunması da bu konunun ayrı olarak incelenmesi gerekliliğini ortaya koyar. Haliyle kişisel verilerin korunmasına ilişkin incelemenin alanı bilişim sistemleri ile çerçevelendiği için fizik ortamda tutulan kişisel veriler ile ilgili bir çalışma yapılması da söz konusu olmamıştır.

Tezin kuramsal çerçevesine gelince, öncelikle bilişim ve kişisel veriler ile ilgili genel açıklamalarda bulunulmuş, arkasından ceza hukuku açısından iç hukukta yapılan düzenlemeler ve özellikle TCK'nin ilgili maddeleri incelenmiş ve bir sentez mahiyetinde olan konu hakkında yorum yöntemi ile sonuca varılmaya çalışılmıştır. Yukarıda açıklanan amaç doğrultusunda birinci bölümde öncelikle uluslarası alanda bu konuda yapılmış ve yürürlükte olan anlaşmalar incelenmiştir. Bunlardan özellikle Türkiye'nin taraf olduğu ve iç hukuk düzenlemesi haline gelen daha çok Avrupa Konseyi'nin 108 sayılı Sözleşmesi olarak anılan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması'na" dair sözleşme ile Birleşmiş Milletler Genel Kurulu'nun 1990 yılında "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" adı ile yayınladığı sözleşmenin önemli olduğu için üzerinde durulmuştur. Birinci bölümde ayrıca, inceleme konusunun asıl çerçevesini iç hukukta uygulanan ceza hükmü içeren düzenlemeler oluşturduğundan 5237 sayılı TCK'nin ilgili maddeleri ile kişisel verilerle ilgili ceza hükmü içeren özel ve kamu hukukuna ilişkin kanunlardan kısaca bilgi verilmiştir. Yine birinci bölüm içerisinde korunan hukuki yarar başlığı altında, konunun anlaşılabilirliğini sağlamak bakımından kişisel veri ve bilişim hakkında kapsamı geniş olmamak kaydıyla açıklamalarda bulunulmuştur. Ancak çalışmanın konusu olan kişisel verilerin

korunması bilişim suçlarının işlendiği saha olduğundan, bu alanın belirlenmesi, hangi eylemin bilişim vasıtasıyla işlenen kişisel verilerin ihlali suçu olduğunun kısmen tespiti anlamına gelecektir. Bu bakış açısıyla bilişim alanının ve kişisel verilerin hangi unsurlardan oluştuğu teker teker sayılacak, tanımlamaları yapılacak, kavramların anlaşılabilmesini sağlayacak kadar ayrıntıya girilecek, ancak, tüm bunlar yapılırken örneğin "donanım, kişilik" gibi kavramlar münhasıran teknik bir terim olarak irdelenmeyecek, bilişim alanının bir unsuru olma yönüyle, daha da ötesinde bilişim suçunun açıklamasına zemin teşkil edecek ölçüde genel amaç doğrultusunda incelenecektir. Dinamik bir saha olan bilişim teknolojilerinin teknik olarak tüm yönleriyle ortaya konulması tek bir çalışmanın kapsamı açısından oldukça büyük bir çalışma olacaktır. Ayrıca teknik açıklamalar çalışmanın amacını aşacağından çalışmanın kapsamı yukarıda belirtildiği şekilde sınırlandırılmıştır. Asıl olarak konuya ilgi duyanların ve özellikle bu konu üzerinde çalışan hukukçuların bilişim ve kişisel verilerin korunması sahasını tanımaları ve bu konudaki ulusal ve uluslararası çalışmaları kavramaları hedeflenmiştir.

İkinci bölümde ise tez ile asıl incelenmesi amaçlanan TCK'de düzenlenen suç tiplerinin ceza hukukunun kurumları açısından incelenmesine geçilmiştir. Bu kapsamda; suçun maddi ve manevi unsurları ile hangi fiillerin suçu oluşturacağı, kasıt ya da kusur aranıp aranmayacağı araştırılmıştır. Yine suçun işlenme yeri ve zamanı belirlenerek yetki ve zaman aşımı gibi uygulamada çok tereddüt yaratan sorunlarının nasıl halledileceği konusu açıklığa kavuşturulmaya çalışılmıştır. Konunun anlaşılabilmesi için öncelikli olarak her bölüm başlığı altında genel bilgiler verilmiş daha sonra TCK'deki maddelerin tek tek incelenmesine geçilmiş ve sonuçta konu hakkında genel bir değerlendirme yapılmıştır.

BİRİNCİ BÖLÜM

ELEKTRONİK ORTAMDA SAKLANAN KİŞİSEL VERİLERİN ELDE EDİLMESİ VE KULLANILMASI YOLU İLE İŞLENEN SUÇLARIN ORTAK ÖZELLİKLERİ

Kişisel verilerin bilişim sistemleri ve ağırlıklı olarak bilgisayarlarla işlenmesi, işlenme hızındaki ve miktarındaki artış, bu nitelikteki verilerin işlenmesine ilişkin usul ve esasların belirlenmesine yol açmıştır. Yukarıda da belirtildiği üzere, kişisel verilerin işlenmesine ilişkin düzenlemelerin yapılmasında ana neden, kişisel verilerin yani veri/enformasyon mahremiyetinin ve dolayısıyla özel hayatın gizliliğinin korunması isteğidir[6]. Kişisel verilerin bilişim sistemde yayılması ile başlayan risk 1960'lı yıllarda, ilk bilgisayarların kullanılmasına ve kişisel bilgileri içeren veri tabanlarının oluşturulmasıyla dikkatleri çekmiştir[7]. Bu tarihlerde bilgisayarlar vasıtasıyla hem kamusal alanda faaliyet gösteren kurum ve kuruluşlar, hem de büyük ticari işletmeler, kendileri faaliyet alanları ile ilgili kişisel bilgileri derlemek, işlemek, ilişkilendirmek ve saklamak suretiyle büyük ilerlemeler kaydetmişlerdir. Bu uygulamaların kurum ve kuruluşların etkinlik ve verimlilikleri yönünden büyük avantajlar sağlarken, diğer yönden de gerek kamu ve gerek özel sektör kuruluşlarını kişiler karşısında dengesiz oranda güçlü kılacak bilgilerin toplanması şeklinde bir gelişme ile kişi hak ve özgürlüklerinin ihlali açısından endişe oluşturacak sorunlara yol açılmıştır. Bu gelişmeler üzerine kişisel veriler ile ilgilenen insan hakları savunucularının yazdığı yazılar, yapılan toplantılar sonucu kamuoyu oluşturulmuş ve bu faaliyetler neticesinde alakalı makamların ilgisi çekilebilmiş, bu çalışmalar sonucunda ulusal ve uluslararası düzeyde belgeler oluşturulmuştur. Özellikle ulusal düzeyde kişisel verilerin korunması ile ilgili ceza kanunlarında düzenlemeler yapılmıştır.

---

[6] Ketizmen, Muammer, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara: Adalet Yayınevi, 2008, s. 215

[7] Değirmenci, Olgun, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", http://www.caginpolisi.com.tr/37/59-60-61-62-63-64.htm, (Erişim: 28.7.2011), s. 2.

Günümüz toplumunda değerlendirilmesi gereken en önemli sorunlardan birisi de, bilgilerin depolanması ve tasniflenmesi suretiyle bireylerin gözetimidir. Sadece devlet tarafından değil, özel bir takım kişi ve kuruluşlarca da yapılan gözetimin temeli kişisel verilerin işlenmesine dayanmaktadır. Örneğin bankalar arasındaki ortak bilgi paylaşımının bir sonucu olarak, herhangi bir banka bir bireyin diğer bankalarda ne kadar mevduatı, onlara ne kadar borcu olduğunu öğrenebilmektedir. Bu uygulama, bireylerin ekonomik faaliyetlerinin bir bölümünün ve aktif-pasif dengesinin bir tür denetimidir. Bu sayededir ki, artık bireyler T.C. Kimlik Numarasının yer aldığı tek bir telefon mesajıyla kredi başvurusu yapılabilmektedirler. Bunun dışında büyük hipermarketler müşterilerine verdikleri indirim kartları sayesinde müşterilerinin harcama alışkanlıklarını takip etme olanağına sahip olmaktadırlar. Nitekim her alış-verişten önce indirim ve puan kazanma amacıyla kart barkottan geçirilmekte ve böylelikle müşterilerin alışveriş alışkanlıkları kayıt altında tutulabilmekte ve böylece kişilerin kişisel bilgilerinden haberi bile olmadan yararlanarak pazarlama teknikleri geliştirilmektedir[8].

1.1. KORUNAN HUKUKİ YARAR (HUKUKİ DEĞER)

Anayasamızla güvence altına alınan ve kişilere ait olan özel bilgilerin korunmasının gerekliliği tartışmasızdır. Ancak bu kişisel bilgilerin neler olduğu mevcut kanunlarımızda net olarak belirtmemiştir. Örneğin kredi kartı alışkanlıklarımız kişisel veri kabul edilecekmidir. Her gün telefonlarımıza SMS mesajı olarak gelen ya da emailimize gönderilen reklamlarla ilgili olarak, günümüzde gündelik hayatın olmazsa olmazları arasına giren kredi kartı harcamalarından alışveriş alışkanlıklarımız kayıt altına alınmakta; daha sonra bunlar büyük firmalara satılarak haksız kazanç elde edilmektedir[9]. Yine hukukumuza göre telefon görüşmeleri hakim kararıyla kanuni olarak dinlenebilmekte ve görüşme esnasındaki veriler delil olarak kabul edilmektedir. Telefon görüşmelerinin bu riskinden kaçmak isteyen suçlular,

[8] Karakehya, Hakan, "Gözetim ve Suçla Mücadele", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2009, Cilt: 58, Sayı: 2, s.323

[9] Şen, Bilal, "Elektronik Gözetim", http://hkmcengiz.tr.gg/ELKTRNK-GZTIM.htm, (Erişim: 10.07.2015)

internet üzerinden haberleşmektedirler. Bu durumda telefon konuşmalarının kişisel veri kapsamına girip girmeyeceği hususunun incelenmesi bizi korunan hukuki yarar konusuna götürmektir.

Öncelikle hukuki değer konusunun açıklanmasında yarar bulunmaktadır. Hukuki değer bir suça ilişkin kanuni tanımın yorumunda başvurulan en önemli araçtır. Hukuki değerler, hukuk toplumundaki sosyal düzenin devamı için geçerliliği zorunlu olan ideal, manevi değerlerdir. Bu değerler, sosyal düzen açısından korunması gereken soyut değerlerdir[10]. Hukuki değerlerin kaynağı, davranış normlarıdır. Bu değerleri korumaya yönelik davranış normlarından kaynaklanan yükümlülüklere aykırı davranışlar, hukuka aykırılık teşkil etmektedir. Bu itibarla, hukuki değer kavramıyla yükümlülük kavramı arasında sıkı bir ilişki mevcuttur, ancak aynı şeyler değildirler[11]. Suç teşkil eden her fiil, aynı zamanda bir hukuki değerin ihlali niteliği arzetmektedir[12]. Ceza hukuku bakımından önemli olan tipe uygun ve hukuka aykırı bir fiilin varlığıdır. Tipe uygun ve hukuka aykırı bir fiilin varlığı (haksızlık) belirlendikten sonra, failin bu haksızlıktan kişisel olarak sorumlu tutulup tutulmayacağının araştırılmasına (kusur) geçilmektedir. Haksızlığın belirlenmesinde failin kişisel özellikleri dikkate alınmayacaktır[13]. Bir fiilin kanunda suç olarak tanımlanmasıyla bir veya birden çok hukuki değer koruma altına alınmış olabilir[14]. Örneğin konumuza ilişkin olarak bilişim sitemi içerisindeki bir kişisel verinin ele geçirilerek menfaat amaçlı kullanılması ile hem özel hayatın gizliliğine hem de bilişim alanına karşı suç işlenmiş olmaktadır. Hukuki değerler, kendi aralarında bir derecelendirmeye tabi tutulduğu için suçların tasnifinde başvurulan yegane ölçüt olma özelliğini taşımaktadır. Hukuki değerlerin aralarındaki bu derece farklılıkları zorunluluk halinin uygulanması bakımından büyük bir önem taşımaktadır. Zorunluluk halinde, bir hukuki değerin ilişkin olduğu konu, örneğin kişisel veriler tehlikeyle karşı karşıya ise bu konunun korunması uğruna daha az

[10] Ünver, Yener, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, Ankara: Seçkin Yayınevi, 2003, s. 149
[11] Özgenç, İzzet, *Türk Ceza Hukuk, Genel Hükümler*, 7. Bası, Seçkin Yayanevi, Ankara: 2006, s. 156
[12] Önder, Ayhan, *Ceza Hukuk Genel Hükümleri*, Cilt: II-III, İstanbul: Filiz Kitapevi, 1992, s. 93
[13] Koca, Mahmut ve Üzülmez, İlhan: *Türk Ceza Hukuku Genel Hükümler*, Ankara: Seçkin Yayınevi, 2011, s. 78
[14] Ünver, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, s. 494

derecedeki bir hukuki değerin ilişkin olduğu konu, örneğin haberleşme özgürlüğü kısıtlanmakta yani ihlal edilmektedir[15].

Ağırlıklı olarak bilgisayar teknolojisi merkezinde gelişen bilişim teknolojisinin sağladığı depolama, işleme ve eşleştirme gibi işlevlerin, bir kişinin bilinmesini ya da bilinebilmesini sağlayan her türlü veri olarak tanımlanan kişisel verilerin toplanması ve işlenmesi için kullanılması, kişisel verilerin korunmasına ilişkin düzenlemelerin yapılmasına yol açmıştır. Bu düzenlemelerin ana nedeni, kişisel veri niteliğindeki bilgilerin bilişim sistemleri kullanılarak işlenmesi karşısında temel hak ve hürriyetlerin ve özellikle özel yaşamın gizliliğinin korunmasıdır. Bilişim alanındaki suçları düzenleyen maddelerdeki suçun konusu bilişim sisteminin bütünü veya bir kısmı olarak görünse de suçun konusu ile suç vasıtasıyla korunan hukuki değer her zaman aynı olmayabilir. İnceleme konusu suçlarda da suçun konusu bilişim sistemi olmasına rağmen, korunan hukuki değer kişisel verilerin korunmasıdır[16]. Bilişim sistemine girilerek elde edilen kişisel verilerin suç işlenmesinde kullanılması durumunda korunan hukuki yarar karma nitelik taşımaktadır. Bir taraftan Anayasanın 20. maddesinde düzenlenen özel yaşamın korunması, sırların masuniyeti, haberleşme özgürlüğü kavramlarının, bilişim sistemleri kullanılarak ihlal edilmesinin önüne geçilmesi, bir taraftan da, işlenmesi amaçlanan suçun koruduğu hak korunmaya çalışılmaktadır. Bilişim sistemine girme, daha sonra işlenmesi olası (verileri bozma, yok etme, değiştirme, dolandırıcılık vs. gibi) suçların işlenmesine uygun bir ortam hazırlamanın ilk adımıdır.

Bilişim sistemlerinin kullanımının ceza hukukuna etkisi açısından incelendiğinde, TCK'de yer alan kişisel verilerin korunmasına ilişkin suçlar, söz konusu etkinin en belirgin olarak ortaya çıktığı konulardan biridir. Bu nedenle, her ne kadar ikinci bölümde incelenen suçlardan bağımsız bir gelişim göstermiş olmasına rağmen, bilişim sistemlerinin kullanımının ceza hukukuna etkisi bakımından kişisel verilerin korunması "bilişim alanında suçlar" başlığı altında

---

[15] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 207

[16] Kurt, Levent, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, Ankara: Seçkin Yayınevi, 2005, s. 170

incelenen suçlar yanında ikinci ana konuyu oluşturmaktadır. Kişisel verilerin korunmasına ilişkin suçlar, genelde, kişisel verilerin hukuka aykırı olarak bilişim sistemi aracılığıyla işlenmesi ya da bilişim sistemine yerleştirilmesinin cezalandırılması şeklinde ortaya çıkmaktadır[17]. Bu açıdan özel hayatın gizliliğinin korunması söz konusu maddelerde düzenlenen suçların hukuki konusunu oluşturmaktadır[18]. Açıklanan nedenle öncelikle kişisel verilerin korunmasına hakim olan ilkelerin incelenmesinde yarar vardır.

1.1.1. Kişisel Verilerin Korunmasına İlişkin Suçların Hukuki Konusu Olarak Özel Hayatın Gizliliği

Devlet kavramının ortaya çıktığı zamanlardan itibaren devlet güvenliğinin korunması ile bireylerin özel yaşamını koruma arasındaki hassas denge her zaman gündemde yer işgal etmiştir. Özel hayatın gizliliği hakkı kişinin özel hayatını devlete karşı koruduğu gibi bireylerin birbirlerinin özel hayatına müdahale etmesini de önler[19]. Bilginin elektronik ortamda saklanabilmesi ve değişimi hükümetlere ve özel sektöre, ilgili bireylerin bilgi ve rızası olmadan bile, yurttaşlara ait bireysel verilere sahip olma, bunları işleme, denetleme, kullanma ve değiş tokuş yapma konusunda eskisinden daha çok imkân sağlamaktadır[20]. Gittikçe artan miktarda hassas bireysel, tıbbi ve ticari veriler gibi kişisel veriler toplanmakta, işlenmekte ve ulusal sınırları aşan şebekeler yoluyla el değiştirmektedir. Özellikle teknolojinin devlete, bireyler hakkındaki özel bilgilere eskisinden daha fazla erişme imkânını sağlaması nedeniyle bu konunun gündeme taşımasını gerektirmiştir.

Bilgisayar teknolojisi ile başlayıp yazılım kullanan iletişim araçlarında ki hızlı ilerleme sonucu gelişen bilişim teknolojisinin sağladığı depolama, işleme ve

---

[17] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 207

[18] Tosun, Öztekin, "Özel Hayatın Gizliliğini İhlal Suçları", *Değişen Toplum ve Ceza Hukuku Karşısında TCK'nin 50. Yılı ve Geleceği Sempozyumu*, İstanbul:22-26 Mart 1976, İstanbul Üniversitesi Hukuk Fakültesi Yayınları, No: 2270, 1977, s. 379-380

[19] Aras, Ümit Yaşar, *İnsan Hakları Temelinde Özel Hayat Hakkının Ulusal ve Uluslararası Alanda Uygulamaları,* Yayımlanmamış Yüksek Lisans Tezi İstanbul: Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 49

[20] Ersoy, Uğur, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2009, s.18

eşleştirme gibi işlevlerin, kişisel verilerin toplanması ve işlenmesi için kullanılması, kişisel verilerin korunmasına ilişkin düzenlemelerin yapılmasını gerekli kılmıştır. Bu düzenlemelerin ana nedeni, bilişim sistemleri kullanılarak kişisel verilerin işlenmesi karşısında temel hak ve hürriyetlerin ve özellikle özel yaşamın gizliliğinin korunmasıdır[21]. Son zamanlarda resmi ya da gayri resmi şekilde insanların özeline olan ilginin artması ve teknolojinin gelişmesi ve bireyin özel hayatına müdahale edebilecek araçların hızla yayılması özel hayatın gizliliği hakkının korunmasının iki temel sebebini oluşturmaktadır[22]. Açıklanan nedenlerle kişinin sosyal, siyasal, dini, kültürel yahut ekonomik alanına yapılacak olası tecavüzlerin önüne geçilebilmesi amacıyla özel hayatın gizliliği hakkı başlıca bir insan hakkı olarak korumaya tabi tutulmaktadır[23].

Kişisel verilerin korunmasının temelini oluşturan özel hayatın gizliliğinin korunması konusunun incelenmesi ise ayrı bir öneme haizdir. Kişisel verilerin koruması hukukunun ortaya çıkıp hızla gelişmesinin bir sebebi de özellikle batı kültüründeki bireyin toplum karşısındaki öne çıkışı ve ferdiyetçiliğin giderek etkisini artırmasıdır[24]. 1948 tarihli "İnsan Haklan Evrensel Bildirgesini" izleyen dönemde batılı çoğulcu demokrasilerden oluşan Avrupa Konseyi bünyesinde hazırlanıp yürürlüğe konulan "Avrupa İnsan Hakları ve Ana Hürriyetleri Sözleşmesiyle (AİHS)" İnsan hakları uluslararası güvenceye kavuşturulmaya çalışılmıştır[25]. Özel hayatın gizliliğini, birbiriyle ilişkili dört başlık altında incelemek mümkündür. Bu açıdan, özel hayatın gizliliği;

I- Kişinin eşyasının, özel kâğıtlarının ve üstünün dokunulmazlığı, konut dokunulmazlığı gibi hususları içeren "bölgesel mahremiyet";

II- Kişinin telefon görüşmelerinin, mektuplarının, diğer vasıtalar kullanarak

---

[21] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 189
[22] Üzeltürk, Sultan, *Özel Hayatın Gizliliği Hakkı*, İstanbul:Beta Yayınları, 2004, s. 6
[23] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.15
[24] Tanrıkulu, Cengiz, *Bilişim Hukuku ile İlgili Alman Federal Yüksek Mahkemesinden Örnek Kararlar*, s.11.
[25] Robinson, Neil; Graux, Hans; Botterman, Maarten ve Valeri, Lorenzo "*Review of the European Data Protection Directive*", Published by the Rand Corporation, United Kingdom, 2009, s.6

yaptığı yazışmaların, elektronik posta ve diğer iletişim olanaklarını içeren "haberleşmenin gizliliği";

III- Kişinin vücut bütünlüğüne yönelik genetik testi, uyuşturucu testi, kızlık zarı testi gibi müdahaleleri içeren "vücut bütünlüğüne ilişkin mahremiyet",

IV- Kişisel verilerin toplanması ve kullanılması ve genel olarak işlenmesi sürecini kapsayan "veri mahremiyeti" başlıkları altında toplanabilir[26].

Hubmann, hayat alanının üç kısımdan oluştuğunu belirtmektedir. Bunlar kişinin güven duyduğu kimselerle paylaştığı, bunun dışındaki kişilere kapalı olmasını istediği "giz alanı", kişinin gizli hayatı olarak kabul edilmeyecek fakat ailesi, akrabaları, yakın çevresi ve arkadaşları gibi sıkı ilişkiler içinde olduğu sınırlı sayıda kişilerle paylaşmak istediği "özel alanı" ve kişinin başkalarının bilmesinden rahatsız olmadığı kamuya açık "ortak alanı"[27]. İşte burada mahremiyet kavramı ile özel yaşamın gizliliği arasındaki ayırım daha belirgin olarak ortaya çıkmaktadır. Mahremiyet kişinin giz ve özel alanını kapsamakta iken, özel yaşam mahremiyeti de içine alan bir üst kavramı ifade etmektedir ve özel yaşamın gizliliği hakkı kişinin mahrem alanının dışındaki kamuya açık alanını da koruma altına almaktadır[28]. Örneğin meslek gereği bir sırrın öğrenilmesi o sırrı giz alanı kapsamından çıkartmaz[29]

Özel hayatın gizliliğinin bozulması ya da özel hayatın gizliliğine müdahale olarak gözetim, Westin'e göre, "fiziksel gözetim", "psikolojik gözetim" ve "veri gözetimi" şeklinde üç başlık altında toplanabilir. Yazar *"fiziksel gözetimi"* kişinin

---

[26] Benneth, J. Colin, *Regulating Privacy: Data Protection And Public Policy In Europe And United States*, London: Cornell University Press, 1992, s.511; *Privacy And Human Rights 2002*; "An International Survey of Privacy Laws and Developments", http.privacyinternatonal.org/survey /phr2002/phr2002-part1.pdf, s. 8 (Erişim: 25.7.2012); Prisella, M Regan, *Legislating Privacy. Technology, Social Vaules, And Public Polity*, The University Of North Carolina Press, 1995, s 69-70.

[27] Helvacı, Serap*, Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar*, İstanbul: Beta Yayınları, 2001, s.62

[28] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s.194

[29] Ergül, Ozan, "Özel Yaşamın Gizliliği Hakkı ve Korunması", Yayımlanmamış Yüksek Lisans Tezi, Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 1998, s. 28

özel yazışmalarının, hareketlerinin, konuşmalarının ya da bulunduğu yerin kişinin bilgisi veya rızası dışında optik ya da akustik araçlarla gözetlenmesi; *"psikolojik gözetimi "* yazılı ya da sözlü testlerin ya da bu iş için kullanılan elektronik veya manuel araçların veya meteryallerin kullanılması suretiyle kişiden istemi ile vermediği bilgileri elde etme veya kişinin farkında olmadan kendisinin özel hayatı ve kişiliği bakımından önemli olabilecek hususların açığa çıkartılması; "*veri gözetimi"* ise veri işlemeye yarayan otomatik veya otomatik olmayan araçlar kullanılarak kişi veya gruplar hakkında bilgi ya da enformasyon toplanması, değiştirilmesi veya kullanılması olarak tanımlamaktadır[30].

Miller, bilişim sistemlerinin kullanılarak yapılan veri gözetimindeki artışın, özel hayatın gizliliğinin korunmasını iki açıdan zayıflattığını belirtmektedir. Bunlardan ilki, kişisel verilerin bilişim sistemleri aracılığıyla işlenmesi bilişim sistemlerinin erişime açık olması niteliğinden dolayı, kişisel verisinin kişinin rıza gösterdiğinden çok daha fazla kişiye ulaşması sonucu kişinin kendisine ait kişisel verilerine kimlerin erişebileceğini kontrol imkânının ortadan kalkmasıdır. Diğeri ise, kişisel verinin işlenmesi sürecinde (toplama, depolama, kullanım, iletim) ortaya çıkan ve verinin içeriğinin doğruluğunun ortadan kalkması gibi durumları netice veren hatalar sonucu kişinin kendisine ait kişisel verinin doğrulunu kontrol edememesidir[31].

Özel hayatın korunma alanı da sınırsız değildir. Bu sınırlılıklardan ilki devletin hizmet götürme sorumluluklarından kaynaklanan sınırlılıklardır. Örneğin, vatandaşa kamu hizmeti sunulabilmesi için belirli bilgilerin kamu kurumlarınca tutulması gerekliliği böyle bir durumu anlatmaktadır. İkincisi, belli kurumların ve mesleki oluşumların meslek üyelerini düzenlemek ve hizmet alanların haklarını korumak amacıyla tuttukları kayıtlardır. Üçüncüsü, ifade özgürlüğüne kamu yararı nedeni ile bir takım sınır oluşturulmasıdır[32]. Çünkü özel hayatın gizliliği ile ifade

---

[30] Westin, Alan F, *Privacy and Freedom*, London, Bodley Head, 1970, s.52.
[31] Miller, Atthur B, *The Assault on Privacy: Computers, Data Banks and Dossiers*, The University of Michigan Pres, 2. Edition, 1971, s. 138
[32] Üzeltürk, *Özel Hayatın Gizliliği Hakkı*, s. 10

özgürlüğü birbiriyle çelişkiye girebilen hak ve özgürlük alanlarını teşkil etmektedir[33]. Bunun gibi, bilgi edinme hakkı ile özel hayatın gizliliği hakkı arasında da ince bir çizgi bulunmaktadır. Bu nedenle hukuksal düzenlemeler bu kavramlar üzerinde çeşitli sınırlamalar getirmek suretiyle insan haklarının sağlanmasında denge kurulmasını amaçlamaktadır[34].

Kişisel verilerin işlenmesine ilişkin düzenlemelerle korunmak istenen veri/enformasyon mahremiyeti ve dolayısıyla özel hayatın gizliliği, TCK'de kişisel verilerin kaydedilmesi, ele geçirilmesi, verilmesi, yayılması ve yok etme yükümlülüğünün yerine getirilmemesi esas alınarak koruma altına alınmıştır. Bu açıdan özel hayatın gizliliğinin korunması söz konusu maddelerde düzenlenen suçların hukuki konusunu oluşturmaktadır. Bu kapsamda kişisel verilerin korunması kavramı üzerinde durularak, kişisel veri, kişisel verilerin işlenmesi, korunması ve bu konuda yapılan hukuki düzenlemeler üzerinde durulması gerekecektir.

1.1.2. Kişisel Verilerin Korunmasına İlişkin Genel Bilgiler

Kişisel verilerin kayıt altına alınması, temel hak ve hürriyetlerin, özelliklede özel hayatın korunması 1970'li yıllardan itibaren gündeme gelmiş ve sonucunda kişisel verilerin işlenmesi ve korunmasına yönelik düzenlemeler yapılmaya başlanmıştır[35]. Kişisel veri tanımına kadar olan süreci anlayabilmek için kişisel verilerin korunmasına ilişkin düzenlemelerin incelenmesinden önce temel terimlerin incelenmesinde yarar bulunmaktadır. Ancak bu kısımda sadece temel kavramlar üzerinde durulması daha uygun olup, bu konu ile ilgili detaylı bilgi verilmesi araştırmanın amacını aşacağından araştırmacılar için atıfta bulunulan kaynaklara havale edilmesi daha yerinde olacaktır.

---

[33] Soykan, Cavidan, *Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı: Özel Hayatın Gizliliği ve İfade Özgürlüğü*, Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi İnsan Hakları Merkezi Çalışma Metinleri, 2006, s.4

[34] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunma*, s.15

[35] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 189

Kişi kavramı ile ilgili olarak; Hukuk dilinde, kişi, hak sahibi olan varlık anlamını taşımaktadır. Hukuk düzeninin haklara ve borçlara sahip olma konusunda kişiler yönünden belirleme yapması bu kavramı hukuki hale getirmiştir[36]. Kişiyi, "hak ehliyetine sahip olan varlık" biçiminde tanımlamak daha uygundur. Şu halde hukuki anlamda kişi, "hak sahibi olabilen ve borç altına girebilen varlık demektir[37]. Ancak, "Kişi" ve "kişilik" kavramlarının karıştırılmaması gerekir. Zira, kişi, hukuk düzeni tarafından haklara ve borçlara ehil sayılan (hak ve borç sahibi olabileceği kabul edilen) varlıkları ifade eder. Başka bir ifade ile kişi, hukuk nazarında hak ehliyetine sahip varlıklardır[38].

Kişilerin, "gerçek kişiler" ve "tüzel kişiler" şeklinde iki çeşidi vardır. Gerçek kişiyi, fiziki varlığının yanında bilinci olan bir varlık olarak nitelendirmek doğru olacaktır[39]. Gerçek kişiler insanlardır. Tarihin bazı dönemlerinde bazı insan sınıfları kişi sayılmamışken bugün artık, çağdaş hukuk sitemlerinin hepsinde insanlar hukuken kişidirler. Tüzel kişiler ise, kendilerine kişilik tanınmış bir kısım kişi toplulukları ile mal topluluklarıdır. Bunlar, tabi oldukları kurallardan hareketle kamu hukuk tüzel kişileri ve özel hukuk tüzel kişileri şeklinde iki guruba ayrılabilir. Özel hukuk tüzel kişilerinin ideal amaç taşıyanları dernek veya vakıf, ekonomik amaç taşıyanları da ticaret şirketi adını alır[40].

Kişilik kavramına bakacak olursak; Kisi, yukarıda da belirttiğimiz üzere hak ve yükümlülüklere sahip olan hak süjesidir. Kişilik kavramı ise, kişiye bağlı ve hukukça korunan bedeni, manevi, hukuki nitelikteki varlıkların tümünü ifade eder[41]. Geniş anlamda kişi kavramına, kişilik hakkının konusunu oluşturan kişisel değerlerin bütünü de girer[42]. Kişilik kavramı statik ve durağan bir kavramı ifade etmekten çok dinamik ve hayatın ve mekanın değişimine paralel olarak değişen ve dönüşen bir kavramı ifade etmektedir[43]. Kişilik hakları parayla ölçülemeyen, iktisadi değer taşımayan varlık ve değerleri koruduğu için kişilik hakkı, şahıs varlığı haklarına

---

[36] Akipek Öcal, Şebnem, *Medeni Hukuk-I-,* Eskişehir: Anadolu Üniversitesi Yayınları, 2011, s. 36
[37] Arpacı, Abdülkadir, *Kişiler Hukuku (Gerçek Kişiler)*, İstanbul: Beta Yayınları, 2000, s. 1
[38] Dural, Mustafa ve Öğüz, Tufan, *Türk Özel Hukuku*, *Kişiler Hukuku*, Cilt: 2, 8. Bası, İstanbul: Filiz Kitapevi, 2006, s. 5
[39] Fındıklı, Remzi ve Bilgiç, Veysel, *İdare Hukuku,* Ankara: Anadolu Yayıncılık, 2006, s. 43
[40] Ayan, Mehmet ve Ayan, Nurşen, *Kişiler Hukuku*, 3. Baskı, Konya: Mimoza Yayınevi, 2011, s.4.

girmektedir[44]. Kişilik bir değerler toplamıdır. Bu toplamın içinde, hak ve borçlara sahip olabilme yanında, hak ve borçlara sahip olabilmek için hukuki işlemler yapabilme ehliyeti, kişilik alanına giren ve hukukça korunan tüm değerler ile kişisel durumlar yer alır[45]. Görülüyor ki, kişilik terimi ile kişinin kişi olması dolayısı ile içinde bulunduğu hukuki durumun ifadesine çalışılmaktadır[46].

Kişilik kavramının genel sonucu gereği kişilik hakkı kavramının incelenmesini gerektirir. Kişilik hakkının konusunu kişilik hakkı altında korunmaya değer bulunan kişiye ait unsurlar oluşturur. Türk-İsviçre Hukuku sisteminde kişilik hakkı varlığı açıkça kabul edilmiş ancak kişiliğin kavramını oluşturan unsurlar tek tek sayılmamış[47], genel bir kişilik hakkı kabul edilerek bu şekilde korunma yoluna gidilmiştir. Kişilik hakkı kişiliğe bağlı olan değerlerin sınırlı sayıda olmaması ve sürekli gelişmesi nedeniyle farklı şekillerde tanımlanmaktadır. Bir tanıma göre kişilik hakkı, kişiyi var eden, kişiliğini serbestçe geliştirmesini sağlayan, diğer kişilerden farklılığını temin eden bütün değerler üzerindeki bir haktır[48]. Kişilik hakkı, kişisel varlıklar üzerinde söz konusu olan şahsa bağlı bir mutlak haktır[49]. Yargıtay'ın bir kararında kişilik hakkı *"kişinin özgür ve başkasına bağlı olmadan varlığını sürdürmesi, kendine özgü yaşam biçimini sağlamasını amaçlar. Bu haklar insanın doğumu ile kazanılan ve kişiliğe bağlı olan haklardır."* şeklinde tarif edilmiştir[50].

Kişilik hakkının maddi ve manevi değerler şeklinde iki çeşit olarak karşımıza çıktığını görürüz. Bunlardan kişiye bağlı maddi kişisel değerler; Kişinin sağlıklı ve

---

[41] Öztan, Bilge, (2000), *Medeni Hukukun Temel Kavramları,* Ankara: Turhan Kitabevi, s.209
[42] Arpacı, *Kişiler Hukuku (Gerçek Kişiler)*, s.2
[43] Özel, Sibel; *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, 1. Baskı, Ankara: Seçkin Yayınevi, 2004, s.36
[44] Öztan, Bilge *Şahsın Hukuku Hakiki Şahıslar*, Ankara: 2001, s.116
[45] Zevkliler, Aydın; Acabey, M. Beşir ve Gökyayla, Emre, *Medeni Hukuk*, 6. Baskı, Ankara: 1999, s. 211
[46] Arpacı, *Kişiler Hukuk (Gerçek Kişiler),* s. 2
[47] Sırabaşı, Volkan; *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz*, Ankara: Adalet Yayınevi, 2003, s.27; Öztan, *Medeni Hukukun Temel Kavramları*, s.118, Arpacı, *Kişiler Hukuku (Gerçek Kişiler)*, s. 107.
[48] Özel, *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, s.27
[49] Kılıçoğlu, Ahmet, *Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk*, Ankara: Ankara Üniversitesi Basımevi, 1993, s.4
[50] Yargıtay 4. HD., 15.02.2001, 2000/10596 E., 2001/1501 K., Yargıtay Kararları Dergisi, Cilt: 27, sayı:8, s.1170.

tam bir bedensel yapıya sahip olmasını ve bunun sürdürülmesini ve insan haklarının ilk ve vazgeçilmez değerlerini ifade eden haklardır. Anayasımızın 17. maddesi "Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir" diyerek kişinin maddi kişisel değerleri olan yaşam hakkı, vücut tamlığı ve hareket özgürlüğünü garanti altına almıştır. Kişinin maddi değerleri üzerinde yapılan müdahaleler hukuka uygunluk şartları içinde yapılmışsa örneğin, tıbbi müdahale nedeniyle yapılmışsa meşru kabul edilecektir[51].

Kişiye bağlı manevi kişisel değerler yönünden ise*;* Kişilik hakkı denildiği zaman daha çok akla gelen kişinin manevi değerleri olan şeref ve haysiyeti, itibarı, adı, özel hayatı, resmi ve sesi gibi unsurlar üzerindeki hakları kişinin manevi kişisel değerlerini oluşturmaktadır. Bu değerler şöyle gruplandırılabilir:

Kişinin Şeref ve Haysiyeti; Şeref ve haysiyet kavramı kişiye toplum tarafından verilen manevi değerlerin tümünü ifade etmektedir[52]. Şeref ve haysiyet kavramı da somut duruma göre değişebilen çok yönlü bir kavramdır. Şeref ve haysiyetin zedelenip zedelenmediği objektif değer yargılarına göre belirlenir. Bu manada şeref ve haysiyetin zedelenmesi için kişinin itibarının azalması söz konusu olmalıdır[53]. Şeref ve haysiyet ihlali gerçek kişiler için olduğu kadar tüzel kişiler için de söz konusu olabilir[54].

Kişinin Özel Hayatı; Kişinin hayat alanı kamuya açık alan, özel alan ve mahremiyet alanı olarak üçe ayrılmaktadır[55]. Kişi yaşamının doğal sonucu olarak herkesin bildiği ve kamuya açık yerlerde meydana gelen olaylar kişinin kamusal

---

[51] Soysal, Tamer, "Elektronik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk", *Ankara Barosu Dergisi*, Cilt: Kış 2007, Sayı. 1 s. 144-167, http://www.ankarabarosudergisi.com/arsiv.html.

[52] Öztan, *Medeni Hukukun Temel Kavramları,* s.128, Kılıçoğlu. *Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk*, s.61

[53] Özel, *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, s.36

[54] Sırabaşı, *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz*, s.29.

[55] Öztan, *Medeni Hukukun Temel Kavramları*, s.133; Kılıçoğlu, *Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk*, s.83.

alanını oluşturmaktadır ve kural olarak hukuksal koruma altında değildir[56]. Kişinin özel alanı da kişinin yakın çevresi ile paylaştığı ve kişinin mahremiyet alanından daha geniş bir alanı ifade etmektedir[57]. Kişinin mahremiyet alanı veya giz alanı diye de bilinen alan ise kişinin kendisinde saklı tutmak istediği, diğer kişilerce bilinmesini arzu etmediği olay ve hareketlerinden oluşur[58]. Bu bağlamda kişiye ait e-posta şifresi ve adresinin ele geçirilerek kişiye ait mesajların okunması kişinin mahremiyet alanına aykırılık teşkil edecektir.

Kişiye Ait Ad, Resim ve Ses; Öztan İsmi, "Bir kimseyi ferdileştirmeye ve diğer kişilerden ayırt etmeye yarayan kişisel değerlerdir"[59] şeklinde tanımlamaktadır. Kişinin korunmaya değer isim kavramına kişiyi ve ailesini toplum içinde tanıtmaya yarayan unvan, takma isim, müstear isim, arma, rozetler ve simgeler de girer[60]. Bu bağlamda teknolojinin gelişimi ile birlikte kişinin hayatının vazgeçilmez öğelerinden biri haline gelen kişiye ait elektronik posta adresleri de kişinin adı üzerindeki korumadan yararlanacaktır. İsimler, toplum nazarında ayırt ediciliği sağlarken, hukuki güvenliği sağlamada da büyük önem taşımaktadır. Kişiye ait resim ve ses de kişiye ait manevi değerlerdendir. Hiç kimse hukuka aykırı şekilde bir başka kişinin resmini çekemez, yapamaz; sesini veya görüntüsünü kaydedemez ve yayınlayamaz, teşhir edemez, kullanamaz[61].

Tüzel kişiler ad ve soyadı kullanmazlar, ama onların da ayırt edici bir özellik olarak mutlaka bir isme sahip olmaları gerekir[62]. Türk Ticaret Kanunu (TTK) ticaret unvanını, tacirin, ticari işletmesine ilişkin işlemleri yaparken ve bu işlemlerle ilgili hukuki işlemlerde bulunurken kullandığı ad olarak belirtmektedir (TTK. m.39).

---

[56] Kılıçoğlu, *Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk*, s.83; Öztan, *Medeni Hukukun Temel Kavramları*, s.134.

[57] Arpacı, *Kişiler Hukuku (Gerçek Kişiler),* s. 82. Şimşek, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması,* İstanbul:Bata Yayınları, 2008, s. 141

[58] Kılıçoğlu*, Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk*, s.84. Öztan, *Medeni Hukukun Temel Kavramları*, s.134; Arpacı, *Kişiler Hukuku (Gerçek Kişiler)*, s. 141;

[59] Öztan, *Medeni Hukukun Temel Kavramları*, s. 270

[60] Arpacı, *Kişiler Hukuku (Gerçek Kişiler)*, s.179, Öztan, *Medeni Hukukun Temel Kavramları, Şahsın Hukuku*, s.168; Arpacı, *Kişiler Hukuku (Gerçek Kişiler)*, s.179

[61] Sırabaşı, *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz*, s.30.

[62] Öztan, *Medeni Hukukun Temel Kavramları*, s.293

TTK'nin 52. maddesi ticaret unvanı ve işletme adlarının korunmasını düzenler. Ancak, ticaret unvanı ve işletme adı aynı zamanda Türk Medeni Kanunu (TMK) anlamında birer isim olduklarından TMK'nin 26. maddesinde düzenlenen adın korunması ile ilgili hüküm kapsamına sadece kişi adları değil, ticaret unvanı ve işletme adı da girecektir.

Kişiye Bağlı Mesleki ve Ticari Kişisel Değerler; Toplum kişiyi mesleki olarak biriktirdiği bu değerlerle bütünleştirmekte ve kişinin saygınlığı ve itibarı bu değerlerle belirlenmektedir. Kişinin mesleki ve ticari değerleri diğer değerlerden farklı olarak parasal sonuçlar doğurmaya en elverişli olanlardır. Kişinin yürüttüğü mesleğe bağlı olarak kişinin mesleki şeref ve haysiyeti ile mesleki gizlilik alanı oluşacaktır. Ticari öneme haiz bu kişisel verilerin kullanılarak bir takım menfaatler elde edilmesi de firmanın tüzel kişiliğinin ihlali anlamında olacaktır[63].

1.1.2.1. Kişisel Veri

Kişisel verilerin korunması hakkını anlayabilmek için öncelikle "kişisel veri" (personal data) kavramını tanımlamak gereklidir. Kişisel veri kavramının tanımlanmasında uluslararası belgelerin hemen hemen tümünde mutabakata varılmış tanım; kişisel verinin doğrudan doğruya ya da dolaylı olarak bir gerçek kişi ile ilintili olabilecek ve onu belirlenebilir kılacak her türlü bilgi olduğudur[64]. Kişisel veri kavramı, Kişisel Verilerin Korunması Kanun Tasarısının 3. maddesinde "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak ifade edilmektedir. Kişisel veri kapsamındaki bilgiler, bir kimsenin kimliğine, fiziksel özelliklerine veya sağlığına, etnik kökenine, öğrenim ve istihdam durumuna ilişkin olabileceği gibi, bir kişinin bireysel, sosyal ve aile içi yaşantısına ilişkin bilgiler ve başkaları ile gerçekleştirdiği haberleşmeler olabilir. Benzer şekilde, bir kimsenin ikamet, emniyet ve kredi kartı bilgileri ile kişisel düşünce ve inançları ve hatta

---

[63] Taşkın, Alim **"**Tüzel Kişilerin Kişilik Haklarının Korunması**"**, *AÜHFD*, Cilt:42, 1991-1992, s. 144-167.

[64] Millard, Christopher, Hon, W. Kuan, "Defining Personal Data in E-Social Science", London, *Information, Communication & Society Journal*, Volume: 15, Issue: 1, February 2012, s. 66-84; Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.16.

alışveriş alışkanlıklarına ilişkin bilgiler de kişisel veri kapsamında yer almaktadır[65].

Nilgün Başalp ise kişisel veriyi; "bir kişinin belirlenebilir kılınması, verilerin doğrudan ya da dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişinin tanımlanabilmesi, yani şahsın o şahıs olduğunu ortaya çıkarılabilmesi özelliği olarak tanımlamıştır"[66]. Örneğin verilerin bir kimlik numarasıyla ilişkilendirilmesi ya da kişinin psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal kimliğini ifade eden, etnik, dini, siyasi, ailevi sağlık ve genetik bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi kişisel veriyi göstermektedir. Başka bir ifade ile kimlik numarası, vergi numarası, pasaport numarası, telefon numarası, motorlu taşıt plakası, ad, soyad, özgeçmiş, fotoğraf, ses, parmak izleri, genetik bilgiler gibi kişiye özel bir içerik taşıyan veriler ile dolaylı olarak kişiyi belirlenebilir kılan kriterlerin kombinasyonu (yaş, meslek, medeni durum, adres vb.) olan veriler kişisel veri kapsamında ele alınabilir[67]. *"Kişi hakkında kişinin bilinmesini ya da bilinebilmesini sağlayan her türlü bilgi ve enformasyonu içeren veriler"* olarak tanımlayan Ketizmen kişisel verileri, kişinin kendisi ve yaşantısı hakkında bilgi veya enformasyon içermesi ya da bunları elde etme aracı olarak kullanılması nedeniyle özel hayat ile yakından ilişkili olduğunu ve özel hayat kapsamında kaldığını belirtmektedir[68]. Kişisel verilerin korunmasına ilişkin düzenlemeler ise, gelişen bilişim teknolojileri sonucunda kişilere ait verilerin işlenme olanaklarının ve yoğunluğunun artmasına daha genel bir ifade ile *"veri gözetimine"* bir tepki olarak, temel hak ve hürriyetleri ve özellikle özel hayatın gizliliğini koruma amacını taşımaktadır[69].

OECD tarafından yayınlanan 108 sayılı Sözleşmenin 2/(a). maddesinde ise kişisel veri, *"kim olduğu belirli olan ya da kim olduğu tespit edilebilen bireylerle*

---

[65] Aksoy, Hüseyin Can, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, 1. Baskı, Ankara: Seçkin Yayınevi, 2010, s.1

[66] Başalp, Nilgün, *Kişisel verilerin Korunması ve Saklanması,* Ankara: Yetkin Yayınevi, 2004, s. 16

[67] Uygun, Murat, *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi ışığında kişisel verilerin korunması,* Yayımlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 43

[68] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 192

[69] Benneth, *Regulating Privacy: Data Protection And Public Policy In Europe And United States*, s. 332

ilgili enformasyon" olarak tanımlanmaktadır. Yine sözleşmenin uygulanmasına yönelik Yönergenin 2/(a). maddesinde ise kişisel veri, *"kim olduğu belirli olan ya da kim olduğu tespit edilebilen gerçek kişilerle ilgili enformasyon"* şeklinde tanımlanmıştır. Maddenin devamında kim olduğu tespit edilebilen kişi, *"özellikle bir ID numarasına referans yapılmak suretiyle veya belirli fiziksel, psikolojik, ruhsal (zihinsel) ekonomik, kültürel ya da sosyal kimliği ile ilgili bir ya da birden fazla faktörlere bağlı olarak doğrudan ya da dolaylı olarak tespit edilen veya edilebilen kişi"* şeklinde tanımlanmıştır. Kişisel verilerin bu şekilde geniş tanımlanarak, kişi hakkında herhangi bir bilgi ve enformasyon yanında, kişiyle ilgili ses ve görüntüler de kapsama alınmaktadır[70]. 1992 tarihli İsviçre Kişisel Verilerin Korunması Hakkında Federal Kanunu'nun 3/a maddesinde kişisel veriyi yukarıda açıklandığı gibi belirli veya belirlenebilir bir kişiyle ilgili bütün bilgiler olarak tanımlamıştır[71].

Son dönemlerde ülkemizde telekomünikasyon alanında kişisel verilerin korunmasına yönelik yürürlükte bulunan Yönetmeliğin[72] tanımlar kısmında da, kişisel veriler, "tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi" şeklinde tanımlanmıştır[73]. Kişisel verilerin korunması kanun tasarısının 3/1-ç. maddesinde kişisel veri, "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır. Tanımın sınırlarının bu şekilde sınırlandırılmayarak korunması hedeflenen "kişisel veri" kavramının kapsamı geniş tutulmuştur. Bu düzenlemeye göre, doğrudan bireye ait olan, bireyi tanımlayan, birey

---

[70] Korff, Douwe**,** Ec Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49): *Comparative Summary of National,* Humen Right Centre, Colchester (UK): University of Essex, s.15 vd.

[71] Döner, Ayhan*, Kişisel Verilerin Korunması Hakkında Federal Kanun*, *Erzincan Atatürk Üniversitesi Hukuk Fakültesi Dergisi (EÜHFD)***,** Cilt: X, Sayı: 1-2, 2006, s.1-16, http://www.erzincan.edu.tr/birim/HukukDergi/makale/2006_X_18.pdf, (Erişim:28.01.2014)

[72] Bilgi Teknolojileri ve İletişim Kurumu tarafından çıkarılan ve halen yürürlükte bulunan "Telekomünikasyon Sektöründe Kişisel Verilerin ve Gizliliğin Korunması yönetmeliği" (KT.06.02.2004, RG. N. 25365).

[73] Özdemir, Hayrunnisa, "Haberleşmenin Gizliliği ve Kişisel Veriler", *EÜHFD*, Cilt: XIII, Sayı 1-2 http://www.erzincan.edu.tr/birim/HukukDergi/makale/2009%20XIII_1-11.pdf, (Erişim:28.01.2014)

tarafından kullanılan veriler olabileceği gibi bireye işaret eden, vücut bütünlüğü de dahil herşey "kişisel veri" sayılmıştır. Bu kapsamda; bireyin göz ve ten rengi, vücut ölçüleri gibi fiziksel özellikleri, kan gurubu, kan tahlili sonuçları gibi sağlık verileri, kullanılan telefon numaraları, iş ve ev adresleri gibi sosyal pozisyon bilgileri, ve sosyal faaliyetlere ilişkin mensubu olunan dernek ve vakıflar da dahil olmak üzere kişi hakkında bilgi veren tüm unsurlar "kişisel veri" olarak dahil edilmiştir[74]. Ancak 2008 tarihli Tasarıda tüzel kişiler de koruma altına alınmışken yeni tasarı kapsam dışında tutarak tüzel kişilerin kişilik varlıklarının korunmasını diğer kanunlara bırakmıştır.

TCK'nin 135 vd. maddelerinde düzenlenen suçlar bakımından kişisel veri tanımı yapılmamıştır[75]. Madde gerekçesi incelendiğinde, kişiyle ilgili kayda geçirilmiş bilgi ve enformasyonun kişisel veri kapsamında değerlendirildiği, kişiyle ilgili ses ve görüntülerin kişisel veri kapsamında değerlendirilmediği sonucuna varılır[76]. Bu nedenle doğrudan kişiye ait olan ve kişinin üzerinde tek başına tasarrufta bulunabileceği veriler olarak anlaşılmalıdır. Gerçekten, bir anonim şirketin ticari sırları gibi bazı bilgiler veri niteliğinde olmakla birlikte kişisel olmaktan çok kurumsal olabilir. Bu yönde, kişiyle ilgili ses ve görüntüleri içeren veri ya da biyometrik veri gibi kişinin tanınabilmesi ya da bilinebilmesini sağlayan diğer her türlü veri, kişisel veri kapsamındadır[77].

TCK'nin 239. maddesi[78] ile ticari sır, bankacılık sırrı veya müşteri sırrı ile fenni keşif ve buluşlar veya sınai uygulamaya ilişkin bilgiler ayrı bir hükümde

---

[74] Şen, Ersan, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", *İstanbul Barosu Dergisi*, Cilt: 2009/3, Sayı: Mayıs-Haziran, Cilt:83, Sayfa:1197.

[75] Güney, Niyazi; Özdemir, Kenan ve Balo, Yusuf Solmaz, *Yeni Türk Ceza Kanunu,* Ankara: Adil Yayınevi, 2004, s. 415

[76] Soyaslan, Doğan. *Ceza Hukuk Özel Hükümler*, 3. Bası, Ankara: Yetkin Yayınları, 2005, s. 273

[77] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları,* s. 230.

[78] *"Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması*
Madde 239- (1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi halinde de bu fıkraya göre cezaya hükmolunur."

koruma altına alınmış olduğundan, 135. madde ve devamındaki hükümlerde yer alan suçların konusunu oluşturmaz. Söz konusu veriler bakımından öne çıkan değer özel hayatın gizliliğinden çok toplumun korunması ile ekonomi, sanayi ve ticaret alanındaki güvenlik olduğundan kanun koyucu 239. maddeyi "Topluma Karşı Suçlar kısmında", *Ekonomi, Sanayi ve Ticarete İlişkin Suçlar* bölüm başlığı altında ayrıca düzenlemeyi tercih etmiştir[79].

Kişisel verileri etki alanlarına göre "Hassas" ve "Anonim" kişisel veri olarak iki guruba ayırabiliriz. Buna göre;

1.1.2.1.1. Hassas Kişisel Veriler

Hassas kişisel verileri, kişilerin ırki kökenlerine, felsefî düşüncelerine, siyasî görüşlerine, dini inançları, mezhep ayrılıkları veya bunun dışında kalan inançları; sendika, dernek ve vakıf üyeliği, sağlığına veya vücuduna ilişkin özellikleri ve özel hayat ve hür türlü mahkûmiyetleri vb. şeyler ile ilgili kişisel veriler "özel niteliği olan" ya da "hassas" kişisel veriler olarak adlandırılmakta olup, genel kabul gören yaklaşıma göre bu verilerin kural olarak işlenmesi yasaktır[80]. Ancak istisnai olarak, kamu yararının gerektirmesi, kişinin rızasının alınması vb. bazı hallerde bu verilerin işlenmesine izin verilebilmektedir. Örneğin İsviçre Kişisel Verilerin Korunması Hakkında Federal Kanunu'nun 3/c maddesinde dini, ideolojik, siyasi veya sendikayla ilgili görüş ve faaliyetleri, sağlık, özel (cinsel) hayat, ırki aidiyet, sosyal yardım uygulamaları, idari veya cezai yaptırımlara ilişkin uygulamalar özel olarak korunmaya değer kişisel veriler olarak belirlenmiştir[81].

TCK'nin 135. maddesinde yer verilmiş olan hassas kişisel verilere biraz daha yakından bakılacak olursa bunlar;

---

[79] Özbek, Veli Özer, *TCK İzmir Şerhi*, Seçkin Yayınevi, 2005, Ankara: s.73

[80] Kaya, Cemil, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", *İstanbul Üniversitesi Hukuk Fakültesi Dergisi (İÜHFD),* 2011, Cilt: 69, Sayı: 1-2, s.317-334.

[81] Döner, *Kişisel Verilerin Korunması Hakkında Federal Kanun*, s. 1-16

Siyasi Görüş; kişilerin, devletin etkinliklerinin amaç, yöntem ve içerik açısından hangi esaslara göre düzenlenmesi ve gerçekleştirilmesi gerektiğine ilişkin düşüncelerini ifade etmektedir[82].

Felsefi ve Dini Görüş; Türk mevzuatı açısından bu kavramlar bir arada düşünülmelidir. Dini görüş kişinin Tanrıya, tabiatüstü güçlere, çeşitli kutsal varlıklara inanma ve tapınma sistemidir[83]. Bu maddede yer alan felsefi görüşün ise, kişinin inceleme amacı taşıyan düşünce etkinliği sonucu ulaştığı tüm görüşler[84] şeklinde tanımlanan, felsefi görüşün genel tanımı olarak kabul edilmemesi amaca daha uygun olacaktır. Hassas verileri tanımlayan ve TCK'deki düzenlemelere kaynaklık eden Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin ilgili maddesinde "dini ya da diğer inanç", Bireylerin Kişisel Verilerinin İşlenmesi ve Bu Verilerin Serbest Dolaşımı ile İlgili Olarak Korunması Hakkındaki 95/46/EC sayı ve 24.10.1995 tarihli Avrupa Birliği Konseyi Ve Avrupa Parlamentosu Direktifi'nin aynı verileri düzenleyen maddesinde ise "dini veya felsefi inanç" ifadeleri kullanılmıştır. Avrupa İnsan Hakları Mahkemesi de *Campbell ve Cosans – İngiltere* davasında verdiği kararın 36. paragrafında felsefi inancı, demokratik bir toplumda saygı görmeye değer olan ve insan onuru ile bağdaşmaz bir nitelik taşımayan fikirler olarak tanımlamıştır[85].

Irki Köken; kişilerin, kalıtımsal olarak, ortak fiziksel ve fizyolojik özellikler taşıyan insan topluluklarından hangisine dahil olduğu bilgisidir[86].

Ahlaki Eğilim; kişilerin toplum içinde yaşamaları dolayısıyla uymaları gereken kurallara yaklaşımları olarak tanımlanabilir[87]. Bu veri kategorisine

---

[82] Türk Dil Kurumu Sözlüğü, "Politika Nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=politika&ayn=tam. (Erişim: 30.01.2014)

[83] Türk Dil Kurumu Sözlüğü, "Din Nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=din&ayn=tam. (Erişim: 30.01.2014)

[84] Türk Dil Kurumu Sözlüğü, "Felsefe nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=felsefe&ayn=tam. (Erişim: 30.01.2014)

[85] Singleton, Susan, *Data Protection,* The New Law, Jordans, Bristol, 1998, s.10.

[86] Türk Dil Kurumu Sözlüğü, "Irk Nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=Irk&ayn=tam. (Erişim: 30.01.2014)

uluslararası mevzuatta hassas veri olarak yer verilmemektedir, bu durum bizim mevzuatımıza özgüdür[88]. Kişinin ahlaki eğiliminden kastın, TCK'nun *"Genel Ahlaka Karşı Suçlar"* Bölümünde yer alan suçlar da göz önüne alınarak, toplumun genelince hoş görülmeyen ve özellikle cinsellikle bağlantılı davranışlara ilişkin eğilim olduğu söylenebilir.

Cinsel Yaşam; kişinin cinsel eğilimlerini ve seks hayatını kapsayan bir kavramdır. Özellikle toplumun geneli tarafından normalin dışında kabul edilen eşcinsellik, biseksüellik, sadizm, mazoşizm gibi eğilimlere sahip bireyler açısından, bu tür bilgiler gerçekten de ayrımcılığa maruz kalınma riski yaratan ve hassas bir nitelik taşımaktadır. Doğal olmayan cinsel davranışların ne olduğu konusunda Türkiye'de henüz resmi bir çalışma yapılmamıştır. TCK'de, ölü kişiyle ve hayvanlarla yapılan cinsel eylemler ile şiddet içeren cinsel davranışlara ilişkin resim ve görüntüleri açıkça yasaklamıştır. Ayrıca, bunlarla beraber sadece "doğal olmayan cinsel davranışlar"dan bahsetmiş, açıklayıcı bir tanım yapmamıştır[89].

Sağlık Durumu; kişinin sağlığı ile ilgili her türlü bilgiyi kapsayan, çok geniş bir kategoridir. Kişinin sadece mevcut durumu değil, sağlık geçmişi de bu kavramın parçasıdır.

Sendikal Bağlantı; kişilerin, işçi veya işverenlerin kendi aralarında kurdukları birliklerden hangisine üye olduğunu veya hangisi ile beraber çalıştığını gösterir[90].

---

[87] Türk Dil Kurumu Sözlüğü, "Ahlak Nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=ahlak&ayn=tam. (Erişim:30.01.2014)

[88] Küzeci, Elif, *Kişisel Verilerin Korunması*, Ankara: Turhan Kitabevi, 2010, s. 373.

[89] Ahi, M. Gökhan**, "**Doğal olmayan yoldan yapılan cinsel davranışlar ne demektir?", http://www.bilisimhukuk.com/2009/08/"dogal-olmayan-yoldan-yapilan-cinsel-davranislar"-ne-demektir/2/, (Erişim: 16.01.2010), s.1

[90] Akdağ, Hale, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 25 vd.

1.1.2.1.2. Anonim kişisel veri

Kişisel veri tanımının tersinden yola çıkarak verinin bir kişi ile irtibatlandırılamayan veya bu veriden yola çıkarak bir kişiye ulaşılamayan veya kaynağının belirlenememesi veya belirlenenmez hale gelmesi veya getirilmesi neticesinde oluşan bilgiye "anonim veri" adı verilmektedir[91]. Karşımıza istatistik, araştırma, planlama vb. amaçlarla tutulan ve herhangi bir kişiyi belirtmekten ziyade kitlesel bilgi yığını olarak çıkan bu tür veriler, ilgili kişilerle ilişkilendirilmeleri mümkün olmadığından kişisel veri sayılmamaktadır. Zira verinin sahibi ile veri arasındaki illiyet bağı kopmuş olduğundan, bu tür veriler üzerinde yapılan herhangi bir işlem kişi hak ve hürriyetlerinin ihlali sonucunu da doğurmayacaktır[92].

Özet olarak, korunması gereken kişisel bilgileri; tasarıda tanımlandığı gibi belirli bir kişiye ilişkin olan veya belirli bir kişiyle irtibatlandırılabilen bütün bilgiler olarak gözterebiliriz. Buradaki bütün bilgilerden kasıt, kişinin özel veya resmi pozisyonu, kişisel, ailevi ve toplumsal yaşamı, inançları, görüşleri, eserleri, öğrenimi ve iş hayatı, görevi, geliri, borçları, mal varlığı, düşünceleri vb. kapsamı genişletilebilecek tüm bilgileri içermektedir. Bu bilgilerden özel nitelikli dolayısıyla duyarlı bilgiler olarak nitelendirebileceğimiz, kişinin dini, inancı, etnik kökeni, siyasal görüşleri, sağlığı ve cinsel yaşamı daha katı koruma önlemlerine tabi tutulur. Hatta bu veriler doğrudan insan hakkı çerçevesinde değerlendirildiğinden çoğu ülkede bu koruma yalnız ülkenin yurttaşlarına değil yurttaş olmayan kişiler için de geçerli kabul edilmektedir. Bu bilgilerin en önemli özelliklerinden biri kişiyle beraber geçerliliklerini devam ettirmeleridir, yani bu bilgilere sağlanan koruma kişinin hayatta olduğu süre ile kısıtlıdır ve kişinin yaşamdan ayrılması ile birlikte bu bilgilerle ilgili koruma önlemleri de belli ölçülerde kalkar[93]. Diğer taraftan artık saklanmasına ihtiyaç duyulmayan kişisel verilerin, kişisel verileri bulunduran veya işleme tâbi tutan kişi veya kuruluşlar tarafından koşulları oluştuğunda, silinmesi veya

[91] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.20
[92] Başalp, *Kişisel Verilerin Korunması ve Saklanması* s. 16, Ersoy*, Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.20
[93] Boz, Ahmet, *Kişisel Verilerin Korunması; Türkiye, ABD ve AB Örnekleri*, Yayımlanmamış Yüksek Lisans Tezi, Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü, 2014, s. 7-10

tümüyle yok edilmesi koruma kapsamındadır[94]. Koruma önlemlerini uygulamak öncelikle kişisel verilerle ilgili koruma kararlarını almakla görevli makamlar ile kişisel veri tabanlarını kaydeden, bulunduran ve kişi ve kuruluşların görev ve yetkisindedir. Ancak üçüncü kişiler yönünden de bazı görev veya sorumluluklar vardır. Kişisel verilerin korunmasının kapsamı; söz konusu bilgilerin toplanması, elde edilmesi, kaydedilmesi, düzenlenmesi, depolanması, uyarlanması, değiştirilmesi, değerlendirilmesi, kullanılması, açıklanması, aktarılması, ayrılması, birleştirilmesi, dondurulması, silinmesi veya yok edilmesi gibi işlemlerin belirlenen ilkeler doğrultusunda yerine getirilmesi anlamını taşımaktadır. Bu korumanın kişiye bakan yönü ise kişinin kendisine ait bilgiler ile ilgili olan ve kanunların getirdiği koruma önlemlerinin ihlal edilmesi halinde ilgili kişiye bu ihlali yapan kurum veya kişiler aleyhine tazminat veya ceza davası da açmak hakkını da içermektedir[95].

Ölülere ilişkin kişisel veriler hakkında bir değerlendirme yapmadan konunun tam olmayacağı açıktır. Kişisel verilerin korunması hakkındaki kanun tasarısında ölü kişilere ait kişisel veriler koruma kapsamında değildir. Ancak ölen kişinin kişisel verileri tamamıyla korumasız da değildir. Öyle ki kişisel verilerin korunması temel haklardandır. Bu sebeple kişiler ölseler de bu değerler koruma altındadırlar. Ölen kişilere ait kişisel verilerin ihlalinde Türk-İsviçre Hukukunda, ölenin mirasçılarının kişilik hakları zarar göreceğinden TMK'nin 25. maddesinde belirtilen haklara, ilgili mirasçılar da sahiptir. Kişisel veriler, Anayasa'da yer alan haberleşme özgürlüğünün kapsamına da dâhildirler. Öyle ki kişilerin gerçekleştirdikleri haberleşmelerde yer alan kişisel verileri anayasal anlamda korunmaktadırlar[96].

1.1.2.2. Kişisel Verinin İşlenmesi

Kişisel verilerin toplanması, elde edilmesi, kaydedilmesi, organize edilmesi, saklanması, değiştirilmesi, uyarlanması, birleştirilmesi, düzenlenmesi, okunması, sorulması, kullanılması, açıklanması, erişilebilir hale getirilmesi, transfer yoluyla

---

[94] Kılınç, Doğan, *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, AÜHFD*, Cilt: 61, Sayı.3, 2012, s. 1125

[95] Küzeci, *Kişisel Verilerin Korunması*, s.259 vd.

[96] Özdemir, *Haberleşmenin Gizliliği ve Kişisel veriler,* s. 5

başkalarına verilmesi, yayılması ya da hazır bulundurulması için yapılan işlemlerin yanı sıra verilerin kombinasyonu ya da ilişkilendirilmesi ve hatta bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü işlem ya da işlemler bütünü kişisel verilerin işlenmesi tanımı kapsamında değerlendirilebilir[97]. İşlem, elektronik bir ortamda gerçekleştirilebileceği gibi elektronik olmayan kağıt vb. gibi bir vasıta ile geçekleştirilen kişisel verilerle ilintili olabilecek her türlü süreci de içerebilir[98]. Kişisel veri ile ilgili otomatik işlemeden kasıt, verilerin otomasyon sistemlerinin kullanıldığı yöntemlerle, örneğin bilgisayar eliyle işlenmesidir. Bu sayede verilerin toplanmasından başlayarak geçtiği tüm aşamaları kapsayan bütün işlem türleri koruma altına alınmaktadır[99].

Kişisel verilerin işlenmesi kapsamında değerlendirilemeyecek kayıtlar arasında kişinin kendisi için tuttuğu özel kayıtlar da vardır. Örneğin kişinin kişisel bilgisayarında kayıtlı fotoğrafları, adresleri, telefon kayıtları vb. kişisel ya da sosyal nitelikteki ilişkiler sonucu tutulan kayıtlar bu kapsamda ele alınamayacaktır. Bunun aksine mesleki ve ticari faaliyetlere ilişkin olarak işlenen kişisel veriler ise özel kayıt kapsamında düşünülmemekle beraber, bu tür verilerin kişinin iradi olarak herkesin erişimine açık tutması hali hariç olmak üzere kişisel veri olarak sayılması gerekir[100].

Kişisel verilerin işlenmesine ilişkin düzenlemelerin kapsam ve içeriğini oluşturan ilkeler genel olarak[101];

1. Kişisel verilerin dürüstlük kuralı çerçevesinde ve hukuka uygun bir şekilde toplanması ve işlenmesi *(dürüst toplama ilkesi - dürüst ve hukuka uygun toplama ve işleme);*

---

[97] Başalp, *Kişisel verilerin Korunması ve Saklanması,* s. 16
[98] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.20
[99] age, s.18
[100] Başalp, *Kişisel verilerin Korunması ve Saklanması,* s. 16, Dülger, Murat Volkan; "Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti", *Hukuk Günlüğü,* http://www.hukukgunlugu.org/saglik-hukukunda-kisisel-verilerin-korunmasi-ve-hasta-mahremiyeti/, (Erişim: 21.06.2015)
[101] Küzeci, *Kişisel Verilerin Korunması*, s.195 vd, Özdemir, *Haberleşmenin Gizliliği ve Kişisel Veriler,* s. 135 vd.

2. Kişisel verilerin, toplanma amacına uygun ve gerekli olduğu miktarla sınırlı olarak toplanması *(asgarilik ilkesi);*
3. Kişisel verilerin hukuka uygun ve önceden belirlenmiş objektif amaçlarla toplanması, işlenmesi *(amaçla bağlılık ilkesi);*
4. Veri sahibinin rızasının veya kanuni bir yetkinin varlığının bulunması durumunda belirlenen amaçlar dışında bir amaç için kişisel verilerin kullanımına izin verilmemesi *(kullanımın sınırlandırılması ilkesi);*
5. Kişisel verilerin doğru, tam ve işlenme amaçları ile ilgili olması (*amaca uygunluk ilkesi)*;
6. Kişisel verilerin rıza dışı ya da yetkili olmayan kişiler tarafından yayılması, veriye zarar vermeden, yok edilmeden veya değiştirilmeden korumak için gerekli güvenlik önlemlerinin alınması *(koruma / güvenlik ilkesi);*
7. Veri sahiplerinin, kendisine ait ve veri işleyen kişi ve kurumlarca elde tutulan verileri hakkında bilgilendirilmesi, bunlara erişimlerinin sağlanması ve yanlış veya yanıltıcı olması durumunda düzeltme olanağının bulunması *(bireysel katılım ilkesi);*
8. Veri işleme sorumlularının, yukarıda belirlenen hususlara uyma yönünde sorumluluklarının bulunması *(sorumluluk ilkesi)* olarak sekiz başlık altında toplamak mümkündür[102].

Kişisel Verilerin Korunması Kanun Tasarısının 4. maddesinde konuyla ilgili olarak kişisel verilerin işlenmesine ilişkin genel ilkeler sayılmıştır. Buna göre kişisel veriler:

- Hukuka ve dürüstlük kurallarına uygun olmak.

[102] Wacks, Reymond, *Personal Information: Privacy and Law,* Clarendon Pres, Oxford, 1989. s.210, Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 216, İlkiz, Fikret, "Kişisel Veriler ve Gizliliği"*, BİA Haber Merkezi*, http://www.bianet.org/bianet/hukuk/154921-kisisel-veriler-ve-gizliliği, (Erişim: 23.07.2014), Kılıç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", s. 1111.

- Doğru ve gerektiğinde güncel olmak.
- Belirli, açık ve meşru amaçlar işlenmek.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmak.
- İşlenme gayesine uygun süre kadar saklamak.

Belirtilen bu ilkeler, genel ilkeler olup, veri işlenmesi ile ilgili tüm işlemelerde, hatta ilgili kişinin veri işlenmesine rızasının bulunduğu veya kişisel verilerin kamunun yararlanmasına açık olduğu hallerde dahi geçerli olacaktır. Bu ilkeler kapsamında değerlendirme yapacak olursak, veri kütüğü sahibi, veri işleme amacını önceden açık ve kesin olarak belirlemelidir. Ancak bu amacın meşru olması ve ilgili kişiler tarafından biliniyor olması da gerekir. Ayrıca veri kütüğü sahipleri, veri işleme amaçlarını işlem yapmadan önce açıkça belirteceklerdir. Belirttikleri bu amaçlar dışında başka amaçlarla veri işleyen üçüncü kişilere açıklayan veri kütüğü sahipleri ise bu fiillerinden dolayı sorumlu olacaklardır. Diğer taraftan, işlenen kişisel verilerin belirlenen amaçların gerçekleştirilmesi için yeterli olması, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılması gerekmektedir[103].

1.1.2.3. Kişisel Verilerin Korunması

Bilişim sistemlerindeki gelişmeler sonucu kişiler, kurumlar ve işletmelerin sahip oldukları veriler, bilgisayar kullanılarak yapılan sahtekarlıklar, bilgisayar korsanlıkları, bilgi hırsızlığı, ilgili kuruluşların kendi çalışanlarınca oluşturulabilecek potansiyel iç saldırılar, bilgi sızdırma ve elektronik saldırılar gibi çok çeşitli kaynaklardan gelen tehdit ve tehlikelerle karşı karşıyadır. Kötü niyetle bilgisayarları ağ üzerinden ele geçirerek bilgisayarlara zarar veren kişilerin kullandığı yöntemler, kişisel ve tüzel kişilere ait verilerin rıza dışı elde edilmesi, kaydedilmesi, kullanılması veya değiştirilmesi gibi tehditler sürekli artmakta olup, kişiler ve kuruluşlar belirtilen tehlikeler karşısında her geçen gün biraz daha risk altına

[103] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.104

girmektedirler. Özellikle kurumsal hizmetlerin internet ortamında sunulması eğiliminin artması, açık ve özel ağlar arasındaki geçişler, bilgilerin halka açık sistemlerle paylaşılması gibi uygulamaların artması sonucu bilgilere erişimin denetlenmesi güçleşmekte ve güvenlik zayıflıklarına neden olmaktadır[104].

Enformasyon teknolojisinin hızlı gelişimi, kişilere ait birçok veriyi elektronik ortamda kolaylıkla tutulabilir ve başkalarına aktarılabilir hale getirmiş ve kişisel verilerin işlenmesi ihtiyacını kaçınılmaz bir olgu olarak karşımıza çıkarmıştır. Özellikle veri transfer yollarının çeşitlenmesiyle zamanla yarışır hızda gerçekleştirilen transferler, kişisel verilerin hem ulusal hem de uluslararası alanda değiş-tokuşunu tehlikeli boyutlarda artırmıştır[105]. Sadece, sahibini ilgilendiren ve onun özel hayatının bir parçasını oluşturan söz konusu verilerin işlenmesinde ruh ve beden bütünlüğünün dokunulmazlığını, kişinin temel hak ve özgürlükleri ile maddi ve manevi varlığını korumak amacıyla yeterli derecede koruma önlemleri alınması "kişisel verilerin korunması" kavramını ortaya çıkarmamıştır. Bunun yanında kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usullerin belirlenmesi, bireyi merkez kabul eden siyasal görüş ve modern hukuk düzeninin bir amacı olarak kişisel verilerin korunmasının hukuki bir zemine oturtulması isteği de bu kavramı popüler hale getirmiştir[106].

Kişisel verilerin korunmasının özel hayatın gizliliği kapsamında değerlendirilmesi, kişisel verilerin işlenmesine ilişkin usul ve esasların genel olarak özel hayatın gizliliğinin sınırlandırılması kapsamında ele alınmasını gerektirmektedir. Kişisel verilerin işlenmesine izin ya da yetki veren normlar özel hayatın gizliliğinin meşru olarak sınırlandırılması anlamına gelmektedir[107]. Özel hayatın gizliliğinin korunmasının bir yönü olarak karşımıza çıkan kişisel verilerin korunması ise, özel hayatın gizliliğinin korunması kapsamında *"veri mahremiyeti"* ya

---

[104] Karaarslan, Enis; Koç, Serhat ve Akın Gökhan, "Vatandaşlık Numarası Bazlı E-devlet Sistemlerinde Kişisel Veri Mahremiyeti Durum Saptaması", http://web.itu.edu.tr/akingok/ubhk10/E-devlet_Sistemlerinde_Veri_Guvenligi.pdf, (Erişim: 25.06.2015) s. 1,

[105] Başalp, *Kişisel Verilerin Korunması ve Saklanması,* s. 4

[106] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.19

[107] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s.207

da diğer bir ifade ile *"enformasyon mahremiyetine"* karşılık gelmektedir[108]. Veri mahremiyeti, bu süreç içerisinde kişi hakkındaki bilgi ya da enformasyonun toplanması, kullanılması ve iletilmesi anlamında genel olarak bilgisayarlar aracılığıyla işlenme sürecini kapsayan ve "*veri gözetim"*olarak adlandırılan duruma tepki olarak karşımıza çıkmaktadır[109].

Bilişim teknolojilerinin internet vasıtasıyla iletişim teknolojileriyle birleşmesi sonucunda meydana gelen gelişmeler, kişisel verilerin korunması hakkının alanını genişletmiş ve önemini çok artırmıştır[110]. Genel olarak kişisel verilerin işlenmesi usul ve esaslarının gösterildiği, kişisel verilerin korunması başlığı altında toplanabilecek kanunlar birçok ülkenin mevzuatına girmiş bulunmaktadır. Kişisel verilerin korunmasına ilişkin suçlar incelendiğinde, genel olarak kişisel verilerin işlenmesine ilişkin usul ve esaslara aykırı fiillerin çeşitli yönleriyle ele alındığı görülmektedir. Bu açıdan kişisel verilerin korunmasına ilişkin suçlar, kişisel verilerin işlenme usul ve esaslarına aykırı kimi fiiller esas alınarak düzenlenmiştir[111]. Nitekim İtalya ve Almanya'da kişisel verilerin korunmasına ilişkin usul ve esasların yer aldığı kanunlarda aynı zamanda kişisel verilerin korunmasına ilişkin suçlara da yer verilmiştir. Buna karşın Fransa'da kişisel verilerin korunmasına ilişkin suçlar, kişisel verilerin korunmasına ilişkin kanun yerine Fransız Ceza Kanunu'nda düzenlenmiştir[112]. Ülkemizde ise, halen kişisel verilerin korunmasına yönelik olarak kişisel verilerin işlenmesine ilişkin usul ve esasların yer aldığı özel bir düzenleme olmamakla birlikte, kişisel verilerin korunmasına yönelik suçlara TCK'nin 135 vd. maddelerinde yer verilmiştir ve düzenlenmede, Fransız Ceza Kanunu'nda takip edilen yöntemin tercih edildiği görülmektedir[113].

Kişisel verileri koruyan kanuni düzenlemeler özel hayatın gizliliği alanında etkin bir rol üstlenmelidir. Bu etkinlik kanunun kapsamının dikkatli belirlenerek,

---

[108] Westin, *Privacy and Freedom*, s. 68 vd.
[109] Miller, Atthur B,*The Assault on Privacy: Computers, Data Banks and Dossiers*, The University of Michigan Pres, 2. Edition, 1971, s. 38
[110] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.22
[111] Kesmez, *Kişisel Verilerin Korunması Üzerine,* s.332.
[112] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 218.
[113] Kesmez, *Kişisel Verilerin Korunması Üzerine,* s.332.

keyfiliğe yol açacak sınırlamalar ve istisnalar getirilmeden düzenleme yapılması yanında teknolojik gelişmelere paralel gelişen ve çeşitlenen sorunlara çözüm getiren nitelikte olması gerekir. Yine hiçbir kural yaptırımsız anlam ifade etmeyeceğinden kişisel verilerle ilgili olarak kanunların getirdiği koruma önlemlerinin ihlal edilmesi halinde bu ihlali yapan kurum veya kişiler aleyhine ceza davası açma veya tazminat isteme hakkını da içermelidir[114].

Kişisel verilerin korunmasının kapsamı konusunda bir değerlendirme yapacak olursak; öncelikle tüzel kişiler hakkında tutulan verilerin kişisel verilerin korunması kapsamında değerlendirilip değerlendirilmeyeceği hususu üzerinde durmak gerekir. Genel olarak bu verilerle bir gerçek kişiye ulaşmak olanaklı ise doğal olarak bu verilerin kişisel veri olarak değerlendirilmesi gerekir. Ancak doğrudan doğruya tüzel kişiler hakkında tutulan kayıtlar konusunda genellikle tüzel kişiler hakkında tutulan bilgilerin de bu kapsama dahil edilmesi gerektiği yönünde bir uygulama söz konusudur[115]. Tüzel kişilere ilişkin olarak incelenmesi gereken bir konuda veri işleyen olarak kamu ve özel hukuk tüzel kişilerinin sorumluluğu konusudur. Artık özel sektör elindeki kişisel veri kamu alanına göre hayli artmış olduğundan genellikle ulusal düzenlemelerde işleyenin kimliğinden bağımsız olarak herkes için veri koruması düşüncesi hakim olmuş, kamu sektörü-özel sektör şeklindeki yerleşik ayrımdan uzaklaşılarak her iki sektör de düzenlemelere dahil edilmiştir.

1.1.3. Bilişim Suçlarının Konusu Hakkında Genel Bilgiler

Bilgisayar teknolojisindeki gelişmeler ve buna bağlı olarak bilgisayar yazılımlarının güncel eşyalarda dahi kullanılması, mobil iletişim araçlarının yaygınlık kazanması elektronik dünyayı hayatımızın ayrılmaz bir parçası haline getirmiştir. Özellikle İnternet kullanımının hızla yaygınlaşarak artması, kişiler ve kurumların işlerini artık çok büyük oranda elektronik ortamda gerçekleştirmesi sonucunda e-devlet, e-imza, e-ticaret, e-posta gibi yöntemler hızla klasik çalışma biçimlerinin yerini

[114] Doğan, Mehmet, "Kişisel Verilerin Korunmasında AB Standartları ve Türkiye'nin Durumu", *EGM Asayiş Dairesi Başkanlığı,* http://www.egm.gov.tr/egitim/dergi/eskisayi/35sayi/yeni/web/makaleler/ mehmet doganhtm, (Erişim: 05.10.2009)

[115] Başalp, *Kişisel Verilerin Korunması ve Saklanması,* s. 18

almaktadır[116]. Daha önce bizzat yüz yüze yapılan bir çok işlem artık sanal alemde gerçekleştirilmektedir. Örnek olarak bankacılık işlemleri bankaya, devlet dairelerindeki bir takım işlemler ilgili kurumlara gitmeden evimizdeki, iş yerimizdeki kişisel bilgisayarlarımızla veya cep telefonlarımızla yapabilmekteyiz. Bu gelişme beraberinde bilişim suçlarını doğurmuş ve yaygınlaşmasını sağlamıştır. Öyleki kimi zaman sırf merak saiki ile dahi suç işlenebilmektedir.

Bilişim suçlarında meydana gelen artışın temel nedenlerinden birisi de bilişim sistemlerinin bünyelerinde suç yaratıcı unsurları barındırması olarak görülmektedir. Bilişim sistemlerinin suç yaratıcı özelliklerini giderme yönünde bir gayret sarf edilmediği gibi, bilişim sistemleri ile ilgili suçların yine bu sistemler tarafından önlenebileceği yönünde yaygın bir inanç vardır[117]. Bilgisayarlarla birlikte, önceki yüzyılın son çeyreğinde çok hızlı bir gelişim gösteren iletişim araçlarındaki gelişmeler de, klasik suçlardan farklılık arz eden, işleniş şekli ve faillerinin profilleri yönünden yeni suç tiplerinin ortaya çıkmasına neden olmuş, güncel kullanım şekliyle ayrı bir başlık altında incelenen bilişim suçlarını doğurmuştur. Klasik suç tiplerine göre düzenlemeler getiren ceza kanunlarının bu yeni gelişen suç tipleri açısından yeterli güncellemeye sahip oluğunu söylemek ise pek mümkün değildir. Bilişim suçlarının belirlenmesi ve bunlarla mücadele yöntemlerinin geliştirilmesi çok geniş bir incelemeyi gerektirir. Ancak bundan da önemlisi bu konunun kavaranabilmesi için öncelikle bu konuyla ilgili kavram ve tanım sorunlarının belirlenmesi ve bunların açıklanmasını gerekir[118].

1.1.3.1. Bilişim Konusunda Temel Bilgiler

Bilişim alanında işlenen suçların anlaşılabilmesi için öncelikle bilişime ait temel bilgilerin öğrenilmesine ihtiyaç bulunmaktadır. Bilişim ile ilgili ilk icatların

---

[116] Karaarslan ve diğerleri, "Vatandaşlık Numarası Bazlı E-devlet Sistemlerinde Kişisel Veri Mahremiyeti Durum Saptaması", s. 1

[117] Değirmenci, Olgun, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", http://www.caginpolisi.com.tr/37/59-60-61-62-63-64.htm, (Erişim: 28.7.2011)

[118] Dülger, *Bilişim Suçları İle Mücadele,* 2. Polis Bilişim Sempozyumunda Sunulan Bildiri, (14-15.04.2005), Ankara: Sheraton

yapılmaya başlanmasından bu güne kadar olan gelişmeler ilk başta kullanılan teknoloji ile bugün erişilen teknoloji arasında çok büyük bir fark olduğunu göstermektedir. Bu farklılık daha da büyüyerek devam etmekte ve sayısal yapıdan, dijital yapıya oradan belki daha farklı bir sisteme doğru değişim göstermektedir. Bu bölümde kanunlarda geçen kavramların öğrenilmesi ve bilişim suçlarının daha anlaşılabilir hale getirilmesi amaçlanmış olup, ayrıntıya girmekten kaçınılmıştır.

1.1.3.1.1. Bilişim

Türk Dil Kurumunun "Güncel Sözlük" adlı eserinde bilişimi, "İnsan oğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığı ile düzenli ve akla uygun bir biçimde işlenmesi bilimi" olarak tanımlamaktadır[119]. Bilgi vermek kökeninden gelen "informatiqe" sözcüğü başlangıçta kullanılsa da daha sonra terk edilerek Türkçe karşılığı olarak bilgi kökeninden gelen "bilişim" sözcüğü kullanılmaya başlanmıştır[120]. Bilişimin, genel olarak bilgisayarın gelişimi ile aynı dönemlerde ortaya çıkan bir terim olması, bilişimin kendisinin bilgisayar ile birlikte anılması ve birbirine bağlantılı olarak tanımlanması sonucunu doğurmuştur[121]. Bilgisayar teknolojisi ise başlangıçta bilişim alanına müdahil olamayacak bir konumda iken 1990'lı yıllardan sonra günümüze kadar çok hızlı bir şekilde evrimini sürdürmüş, hacim olarak küçük, hız, bellek ve teknik özellikleri bakımından sürekli gelişerek bilişim alanının ayrılmaz bir parçası olmuştur[122].

Öğretide bilişim sözcüğünün birçok tanımı yapılmıştır. Birkaç örnek verecek olursak; Yazıcıoğlu bilişimi; *"Bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve*

---

[119] Türk Dil Kurumu Sözlüğü; http//www. tdk. gov.tr. (Erişim: 21.03.2011)
[120] Kızıltan, Mehmet Burak, *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, Yayımlanmamış Yüksek Lisans Tezi, İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s.20
[121] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, 2008: s.13
[122] Balık, Hasan Hüseyin (Ed.), *Temel Bilgisayar Teknolojileri Kullanımı*, Elazığ: Fırat Üniversitesi Basım Evi, 2003, s. 3

mesleki disipline verilen ad" olarak tanımlamıştır[123]. Değirmenci-Yenidünya'ya göre ise bilişim; *"Teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır"*[124]. Taşdemir bilişimi, *"Bilginin otomasyona tabi tutulması sonucunda işlenmesinin yani verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılması anlamlarını içermektedir"* şeklinde tanımlamıştır[125]. Kızıltan ise doktirindeki görüşleri toparlayarak bilişimi; *"İnsanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin temeli olan bilginin elektronik araçlarla özellikle bilgisayarlar aracılığıyla düzenli ve akılcı biçimde işlenip, organize edilmesi, değerlendirilmesi ve ses, görüntü, veri taşıyan iletişim hatları aracılığıyla aktarılması ile ilgili bilim dalı"* olarak tanımlamaktadır[126]. Buraya kadar yapılan açıklamalardan anlaşılacağı üzere, bilişim terimi, bilgisayara göre, daha geniş bir alanı kapsayan bir üst kavram olup, bilginin, bilişim vasıtası olarak adlandırılabilecek cihazlar aracılığı ile toplanması, işlenmesi, depolanması ve aktarılmasıdır şeklinde özetlenebilir.

1.1.3.1.2. Bilişim Alanı

Bir eylemin bilişim suçu olup olmadığının tespiti açısından hangi alanda işlendiğinin tespiti çok önemlidir. İnceleme konusu faaliyetin bilgisayar sistemini temel alarak mı yapıldığı, yoksa bilgisayarın o faaliyetin gerçekleşmesinde yardımcı bir unsur olarak mı kullanıldığının tespiti gereklidir. Örnek göstermek gerekirse bankaların ATM[127] cihazları bir bilgisayar sistemi olduğu için bu faaliyetin

---

[123] Yazıcıoğlu, *Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile,* İstanbul: Alfa Basım Yayım Dağıtım, 2004, s.131

[124] Yenidünya, Caner ve Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, İstanbul: Legal Yayıncılık, 2003, s.27

[125] Taşdemir, Kubilay, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, Ankara: Turhan Kitapevi, 2009, s. 243

[126] Kızıltan, *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, s. 22

[127] ATM, "Automatic Teller Machine" kelimelerinin baş harflerinden oluşan bir kısaltmadır. Banka kartı ya da kredi kartı ile bankadan para çekme veya banka işlemi yapmaya yarayan makinelere verilen isimdir. Kaynak: nedir.com, "Atm Nedir" http://atm.nedir.com/#ixzz2zTJKIneY, (Erişim: 21.04.2014)

bilişim alanı içinde cereyan ettiği yani bir bilişim faaliyeti olduğu söylenebilecektir. Çünkü bu bilgisayar sistem çöktüğünde cihaz görevini asla icra edemeyecektir[128]. Ancak, bilgisayar sistemleri bir kısım faaliyetlerde veya sistemin tamamında değil bir kısım aşamalarında etkin ve faaliyet bilişim sistemini temel almıyor ise, mesela radyo ve televizyon yayıncılığı gibi iletişim temelliyse bu saha bilişim alanı olarak kabul edilmeyecek ve bu alanda icra edilen bir ihlalde bilişim suçu olarak kabul edilemeyecektir[129]. Özetle, bilgisayarı da kapsayan ve özellikle bilgisayar ve bu özellikli aygıtların içinde bulunduğu bir alan olarak tanımlanabilecek olan bilişim alanında toplanması amaçlanan veriler yerleştirildikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler olduğudur[130]. Bilişim alanını unsurları hakkında şimdi veya daha sonra sınırlayıcı bir açıklama yapmak mümkün değildir. Sürekli gelişen teknolojinin getirdiği yenilikler bilişim alanının çerçevesini halen genişletmeye devam etmektedir. Bu kapsamda günümüz itibarı ile bilişim alanın unsurları konusunda fikir verecek açıklamalarda bulunulması daha doğru olacaktır.

1.1.3.1.3. Bilişim Sistemi

Bilişim sistemi en basit ifadeyle elektronik makinelerdir. Bu makineler veri veya bilgilerin kaydedildiği ve bu verileri işleme tabi tutabilen, sonuçları ya da verileri çıktı şeklinde verebilen cihazlardır. Bu sistemin bileşenleri, başlangıçtan itibaren sırasıyla; "girdi", "bilgi işlemleri" ve "çıktı" şeklinde üçe ayırabilir. Girdi, bilgisayar dilinde, belli özelliği olan öğelerin oluşturduğu bir kümeyi; bilgi işlemleri, girdi ile başlayan programın amaca uygun olarak işlendiği bölümü; çıktı ise, bir önceki bölümde işlenen bilgilerin okunabilir, anlamlı kümesidir[131]. Burada bilişim sistemi olarak sadece yalnızca bilgisayarlardan söz edildiğinin kabulü yanıltıcı olacaktır. Örneğin verilerin depolanması, işleme tabi tutulması veya nakledilmesindeki

---

[128] Şeker, Güven, "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum", www.insanbilimleri.com/makaleler/kamu-yönetimi/bilişim-suçlarinin.htm, (Erişim: 25.06.2010)
[129] Kurt, *Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* s. 18
[130] Yazıcıoğlu, *Bilgisayar Suçları,* s.133
[131] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri,* s.126

modem, ATM cihazları, benzeri işlem makineleri gibi pek çok yazılım kullanan cihaza yönelik fiiller bilişim alanında suç sayılamayacaktır[132]. TCK'nin konu başlığı "Bilişim Suçları" olup, zaten doğrudan bilgisayarı değil, daha üst kavram olan bilişim sistemini işaret etmektedir. 243 ve 244. madde metinleri incelendiğinde suçun işlendiği ana temanın bilişim sitemi olduğu açıkça belirtilmiş olduğundan bu konuda zaten tereddüde mahal yoktur.

1.1.3.1.4. Veri

Bilişim sisteminin temel yapı taşı veridir. Bilişim sistemlerinin amacı veriyi saklamak, işlemek ve sonuç çıkartmaktır. Veri bilgilerin belirli bir formata dönüşmüş halidir[133]. Bir bilişim sisteminde saklanan, yazı, resim, program v.b gibi her şey veridir[134]. TCK'nin 243. maddesinin gerekçesinde sistem içindeki bütün soyut unsurların veri teriminin kapsamı içerisinde yer aldığı belirtilmiştir. Avrupa Siber Suç Sözleşmesinin "tanımlar" başlıklı 1. maddesinde veri "Belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünüdür." şeklinde tanımlanmıştır[135].

Bu noktada ayrıştırılması gereken bir konu ise veri ile bilginin aynı şey olmadığıdır. Bilgi, öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat[136] olarak ifade edilebilecek iken, bu malumatın bilgisayarın anlayıp işleyebileceği haline de veri denilmektedir. Veri ve bilgi özde aynı olup sadece şekil farklılığı vardır. Rakamsal, alfabetik ve simgesel nitelik taşıyan veriler anlam olarak insanlar için hiçbir şey ifade etmese de, bilişim sisteminin anlayabildiği bilgi

---

[132] Yazıcıoğlu, *Bilgisayar Suçları*, s.224
[133] Yenidünya ve Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, s.48
[134] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 37
[135] İnternet Medya ve Bilişim Federasyonu, "Avrupa Siber Suç sözleşmesi", www.imef.org.tr/uluslararasi-ıliskiler/257-avrupa-konseyi-siber-suclar-sozlesmesi-.html. (Erişim: 22.08.2011)
[136] Türk Dil Kurumu, "Veri ve Bilgi Nedir" http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5425839dc592e5.35646613, (Erişim: 26.09.2013)

formatıdır[137]. Bilgi – işlem (enformasyon) teknolojisi, bilginin içeriğiyle değil, biçimiyle (veri olarak alınması, işlenmesi, saklanması, erişilmesi ve iletilmesi vb.) ilgilenir[138].

1.4.3.2. Bilişim Suçu Kavramı Hakkında Genel Bilgiler

Genel olarak bilişim suçunun ülkemizde kavramının tanımı yapılmış değildir. Doktrinde bu konuda yapılan birçok tanım bulunmakla birlikte üzerinde uzlaşılan bir tanım yoktur. Kısaca bilişim suçu, bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suçtur denilebilir[139]. Bu tanımı, bilişim suçları, bilişim alanındaki gelişmelere paralel artış gösteren ve teknolojinin yardımı ile genellikle sanal ortamda kişi veya kurumlara karşı maddi veya manevi zarar verecek davranışlarda bulunmaktır şeklinde genişletmemiz mümkündür[140]. Bu konuda çalışma yapan Yenidünya ve Değirmenci, "Bir bilgisayarda ya da bilgisayar olarak nitelendirilmemesine rağmen veri iletişimi sağladığı için bilişim alanının unsurlarından olduğu kabul edilmesi gereken diğer elektronik, manyetik, mekanik araçlar üzerinde (örneğin, cep telefonu, üzerindeki web paneli sayesinde ağa bağlanıp bilgi aktarımı yapabilen elektronik ev aletleri, üzerinde yüklü programlar aracılığı ile şifreli yayınları alan, bunları işleyen ve bunlardan sonuç çıkartan dekoderler) veya bunları veri-işletimi için birbirine irtibatlayan soyut veya somut bir ağ üzerinde gerçekleştirilebilir eylemleri" bilişim suçu olarak kabul ettiklerini belirtmektedirler[141]. Yine aynı konu üzerinde çalışmaları olan Akbulut bilişim suçunu; "verilerle veya veri işleme konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sitemlerine karşı işlenen suçlar" şeklinde tanımlanmaktadır[142]. Dülger ise bilişim suçunu, "verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sitemleri aracılığı ile işlenen suçlar" şeklinde tanımlamaktadır[143]. Bilişim

---

[137] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s.39
[138] Yazıcıoğlu, *Bilgisayar Suçları*, s.30
[139] Karargülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 40
[140] Tavukçuoğlu, Cengiz, *Bilişim Terimleri Sözlüğü*, Asil Yayın Dağıtım, Ankara: 2004, s.27
[141] Yenidünya ve Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, s.31
[142] Akbulut, Berrin Bozdoğan, "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi (SÜHFD)*, Cilt:8, Yıl. 2000, Sayı.1-2, s.551
[143] Dülger, *Bilişim Suçları*, s.67

alanında işlenen suçlar ile ilgili çok sayıda terim üretilmiş olsada (Computer Crimes, Cyber Crimes, IT Crimes (Information Technologies – Bilgi Teknolojileri), Crime of Networks vb.) en çok tarcih edilen ve amaca hizmet eden "Bilişim Suçları" olarak kullanılması daha uygun olacaktır[144].

Bilişim suçları kapsamına giren suçların tanımlanması ve sınıflandırılmasının yapılması daha sonra yapılacak çalışmalara hazırlık teşkil edecek ve her bir suç tipi daha rahat anlaşılmış olacaktır. Burada suç tipleri arasındaki farkı oluşturan esas etken "suçun işlenmesindeki amaç" olmalıdır. Bilişim suçlarının işlendiği yöntemden daha çok, hizmet ettiği amacı tespit etmek önemlidir. Örneğin; bilişim sistemine girmek için birçok yöntem bulunmaktadır; virüs, trojan programları kullanılarak veya arka kapı denilen sistem açıkları zorlanarak giriş yapılabilir. Amacın burada "sisteme girme" fiili olduğuna dikkat etmek lazımdır. Eylem sırasında kullanılan yöntemler ancak suçun ağırlaştırıcı nedenlerini oluşturabilir. Mesela bir bilişim sistemine girmek için başka sistemlere de giriş yapılmış olması bu duruma örnek gösterilebilir. Bu suç tipine ilişkin AB, Avrupa Konseyi ve diğer Avrupa ülkelerince yapılan tanımlamaların ülkemize uyarlanması sonucu aşağıda verilen suç tanımları oluşturulmuştur. Bu tanımlamalarda benzer mahiyette İngilizce tabirleri ile (örneğin; Unauthorized Acces, Computer Sabotage, Computer Fraud gibi) karşılaşmak da mümkündür. Bilişim suçları tek hareketli veya tek vasıta ile işlenebilen suçlar olmadığından anlaşılabilmesi için bir tasnife tabi tutarak incelemek çalışmayı kolaylaştıracaktır.

Siber suç kavramı genel olarak bilgisayar ağlarında işlenen suçlara (crimes related to computer networks) siber suçlar (Cyber Crime) tabiri kullanılmaktadır. Siber suç; bilgisayar aleyhine veya bilgisayar aracılığı ile işlenen suçlar olarak tanımlanabilir[145]. Siber suç kavramıyla aslında bilişim suçları ifade edilmektedir. Ancak, bilişim suçlarının tek bir bilişim sisteminde işlenen şekli değil, bilişim sistem

---

[144] Dokurer, Semih, 'Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri', *Polis Dergisi*, Sayı: 37, 2003, s. 56.

[145] Çeken, Hüseyin, "ABD'de İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğunun Hukuki Esası", http://archiv.jura.uni-saarland.de/turkish/HCeken1.html (Erişim: 25.2.2015)

ağları vasıtasıyla, özellikle internetle işlenen suçlar kastedilmektedir[146]. Özetle siber suçları, bilişim sistemleri ve bilişim teknolojileri kullanılarak bu sistemlerde ve bilişim ağlarında işlenen suçlar şeklinde tanımlamak mümkündür[147].

Bu kapsamda geniş anlamda siber suçlar incelenecek olursa, bilişim sistemlerinde işlenmesi mümkün olan suçlara şu şekilde birkaç örnek verilebilir;

1.1.3.2.1. Siber Cinayet

Kaliforniya örneğinde olduğu gibi hastanenin kayıtlarına girerek hastaların reçetelerinin sanal ortamda değiştirilmesi sonucu yanlış tedavi ile ölen hastalar yönünden bu değişikliği yapan ve kişisel veriyi değiştiren kişi her ne kadar doğrudan bedene yönelik bir icraatta bulunmasa dahi cinayet işlemiş olacaktır[148].

1.1.3.2.2. Siber Tehdit ve Şantaj

Kişilerin kişisel verilerinin, özellikle cinsel hayatlarına, mali durumlarına ilişkin elde edilecek verilerin kullanılması suretiyle tehdit ve şantaj yapılabilmektedir. Sohbet odalarında (chat programları) karşısındakinin soyunma görüntülerini kaydeden ve bunu şantaj için kullanan İstanbul ve Nevşehir polisinin ortak eylemi sonucu yakalanan 17 yaşındaki şantajcının eylemi buna örnek verilebilir[149].

1.1.3.2.3. Siber Dolandırıcılık

Bilişim sitemleri kullanılarak kişisel verilerin elde edilmesi suretiyle dolandırıcılık mümkündür. Bilişim sistemlerinde yer alan programların veya verilerin değiştirilmesi, sahte veya değiştirilmiş veriler girilmesi, mevcut verilerde oynamalar yapılması, hileli bir takım hareketlerle bilişim sistemlerinin işleyişinin değiştirilmesi

---

[146] Yenidünya ve Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, s.33
[147] Ergün, İsmail, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, 2008, Turhan Kitapevi, Ankara: s.37.
[148] http://www.milliyet.com.tr/1997/06/16/ekonomi/turkfir.html. (Erişim:08.05.2014)
[149] Pekel, Ahmet, "Siber Tehditler ve Bilgi Güvenliği", www.slideshare.net/mobile/AhmetPekel/siber-tehditler-ve-bilgi-gvenlii. Ankara: Nisan 2011, (Erişim: 12.03.2015)

mümkün olabilir. Bir bankanın web sitesinin bir kopyasının yapılıp buradan kişinin yanıltılarak alınacak kişisel verilerinin kullanılması yoluyla dolandırıcılık yapılması örnek verilebilir[150].

1.1.3.2.4. Siber Hırsızlık

Bilişim sistemlerinin kullanılması yolu ile hırsızlık suçunun da işlenmesi mümkündür. Örneğin, trojen programları vasıtası ile ele geçirilen kişisel veri niteliğindeki hesap numaraları ve şifrelerin kullanılması suretiyle hesaplardaki paraların kendi veya bir başkasının hesabına aktarılması siber hırsızlık olarak nitelendirilebilir. Klasik hırsızlık suçunun oluşabilmesi için gerekli olan koşullar siber hırsızlık suçunun gerçekleşmesi ve ceza sorumluluğunu doğurabilmesi açısından da uygulanabilir niteliktedir[151].

1.1.3.2.5. Siber Terörizm

Sanal alemde işlenebilecek suç çeşitlerinden biri de siber terörizmdir. "Terörizm belirli bir siyasal ve sosyal amaca ulaşabilmek için bireylere, mallara ve toplumsal yaşayış düzenine zarar verilerek, toplumu ve yöneticileri yıldırma, baskı altında tutma çalışmaları olarak tanımlanırsa, siber terörizmde benzer faaliyetin bilişim sistemi kullanılarak gerçekleştirilmesidir denilebilir"[152]. Özellikle internetten yararlanarak örgütlenme, eğitim ve destek almak suretiyle yapılan terörist saldırı sonucu 11.09.2001'de New York'ta "İkiz Kuleler" olarak anılan Dünya Ticaret Merkezi yıkılmıştır[153].

Genel olarak bilgisayar odaklı veya bilgisayar destekli, fakat internet

---

[150] Tulum, İsmail, *Bilişim Suçları ile Mücadele,* Yayımlanmamış Yüksek Lisans Tezi, Isparta: Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 27

[151] Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, s.37

[152] Özcan, Mehmet, (2004), "Siber Terörizm ve Ulusal Güvenlik", *İnternet ve Hukuk*, Derleyen: Yeşim M. Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayını, s. 308.

[153] Tanyol, Tuğrul, (2002), "Anarşizm ve İnternet", *Cogito İnternet: Üçüncü Devrim*, Yapı Kredi Yayınları Sayı: 30, Yıl: Kış 2002, s. 207

ağlarının kullanıldığı suçlar siber suç olarak tanımlanmaktadır[154]. Bu suç tipinde bilgisayarın etkin rol oynaması gerekmez. Bu suçu işleyenin özel bilgisayar becerilerinin de bulunması gerekmez. Kısacası bu suç tipinde bilgisayarın suçu işlemede bir araç olduğu görülmektedir. Örneğin, bir şüpheli ve mağdur Web tabanlı sohbet odaları, Microsoft Ağı Messenger (MSN) ya da e-posta yoluyla iletişim kurabilir ve suç bu şekilde işlenebilir. Bilgisayar suçlarında ise genellikle suçluların kurbanlarına karşı başarıyla bu suçları işlemek için bilgisayar işletim becerilerinin temel seviyesinden daha fazla olmasını gerektirir. Örneğin, heckerler tarafından üretilen virüs vb. gibi zararlı yazılımlar yolu ile diğer bilgisayarlara zarar verilmesi bilgisayar suçunu oluşturur[155]. Teknoloji sürekli geliştiği için, şu anda geleneksel (klasik) suçlarla paralel ya da birlikte değerlendirilen bilişim suçları, gelecekte suçlu davranışlarının bütün türlerini ihtiva eden bir yapıya bürünecektir. Gelecekte bilişim suçları; uyuşturucu ticareti, insan kaçakçılığı, terörizm ve karapara aklama suçlarını da içerisine alacaktır[156].

1.1.3.3. Bilişim Suçları Alanındaki Hukuki Düzenlemeler

Oldukça önemli bireysel ve toplumsal sonuçları bulunan bilişim suçları bugün kanıksanmış bir gerçeklik olarak önümüzde durmaktadır[157]. Hal böyle olunca bu suç tipleriyle yürütülecek mücadelenin de çok geniş düşünülmesi gerekir. Bilişim suçlarıyla mücadelenin, ceza hukuku normlarıyla sağlanmaya çalışılması yalnızca bir boyutudur. Esasen daha önem arzeden boyutu, kişi, kurum ve hatta devletlerin bilişim sistemi kullanmaktan kaynaklanan sorunların çözümüne yardımcı olacak

---

[154] Casey, E ile Thomas, D ve Loader, B bu konuda tanımlar vermektedir:
Casey siber suçu, bilgisayarların yoğun kullanmadığı suçlar da dahil olmak üzere bilgisayar ve ağları içeren herhangi bir suç olarak tanımlar. Casey, James E., *Digital Evidence and Computer Crime,* London: Academic Press, 2000, s. 8
Thomas ve Loader ise, siber suçun, yasa dışı veya kaçak olarak belirli kişiler tarafından, küresel elektronik ağlar üzerinden yapılan ve bilgisayarın aracılık ettiği faaliyetler olduğuna dikkat çekmektedirler. Thomas, Douglas and Loader, Brain D., *Introduction – Cyber crime: Law Enforcement, Security and Surveillance in the Information age*. in B. & B. Loader (Eds.), London: Routledge, 2000, s. 3

[155] Kyung-shick, Choi, "Computer Crime Victimization and Integrated Theory: An Empirical Assessment", http://www.cybercrimejournal.com/Choiijccjan2008.htm, (Erişim: 23.01.2014)

[156] Etter, Barbara, *Leadership İn The Hi-Tech Crime Environment, Australasian Centre For Policing Research,* To 2/2002 Pelp At The Aipm Sydney, s.11

[157] Özdilek, Ali Osman, "Bilgisayar Suçları Ne Kadar Ciddi?", http://www.hukukrehberi.net/Details.aspx?id=88, (Erişim: 20.02.2014) s. 4

önlemlerin alınması ile özellikle ceza hukuku dışında, tazminat ve sorumluluk hukuku alanında yapılması gereken düzenlemelerin yapılması daha ön plana çıkmaktadır[158].

Bilişim suçlarıyla mücadele açısından alınması gereken önlemler sanal alanın, daha da özelde bu gün vazgeçilmez hale gelen ve yaygınlaşan internetin düzenlenmesidir. Sanal alanın düzenlemesi konusunda temel olarak dört türlü faaliyet birbiriyle yarışmaktadır. Bu yöntemler; ulusal alanda, uluslararası anlaşmalarla, uluslararası kuruluşlar oluşturularak ve kendi kendine yapılan düzenlemedir. Bunlardan dördüncü seçenek sanal alan kullanıcılarının etik davranışlarıyla ilgili bir düzenlemedir.[159]. Kendi kendine yapılan düzenleme yeni bir kavram olup, örnek olarak "işbirliğine dayalı düzenleme" (co-regulation) ve "öz-düzenleme" (self-regulation) yöntemleri gösterilebilir[160]. Anılan düzenleme modelinde; kullanıcılar bilişim sitemini kullanırken, uygulamaya özgü ve kendiliğinden meydana gelen kurallar bulunmaktadır. Bu kuralların hepsi sanal alana uygulanamayacağı için içinden seçim yapılması, filtrelenmesi, sanal alanı kullanacakların ve sistem yöneticilerinin seçilmesi vb. düzenlemeler kendi kendine yapılacaktır[161]. Sanal alanda kendiliğinden oluşturulan ve yine sanal alan için uygulanacak bu düzenlemeler için kısaca "netiket" denilmektedir[162].

Düzenlenen suç tipleri ve düzenleme usulleri farklı olmakla birlikte bilişim suçlarına ilişkin düzenlemelerin birkaç istisna dışında tüm ülkelerin hukuk sistemlerine dahil edildiği görülmektedir. Ülkeler bu düzenlemeleri yaparken temel

---

[158] Özdemir, Muammer, "Suç ve Ceza", *PC Magazine Türkiye*, Sayı: Mayıs 2000, s. 20, Dülger, *Bilişim Suçları*, s. 320

[159] Çeken, Hüseyin, *Council of Europe's Convention 2001 on Cybercrimes and Turkey,* Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi, Avrupa Topluluğu Enstitüsü, 2003, s.10

[160] Akdeniz, Yaman, (2003), "Internet Governance: Towards the Modernization of Policy Making Process in Turkey", *İstanbul, Ankara, İzmir, Adana, TBV Series:1*, Papatya Publication Education, s.51-57; Akdeniz, Yaman, "Çağdaş İnternet Yönetimi", *Güncel Hukuk Dergisi*, İstanbul: Sayı: Haziran 2004, s.24

[161] Johnson, David R. ve Post, David G., "And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law", *Coordinating the Internet*, MIT Press, Massachusetts, USA, s. 62-91

[162] Memiş, Tekin, (2001), "İki Uluslararası Sempozyum ve Bir Özet", Erzincan: EÜHFD, Cilt:V, s. 2001

olarak iki ayrı sistemden birini benimsemekte ve düzenlemelerini bu çerçevede gerçekleştirmektedirler. Bazı ülkeler bilişim suçlarına ilişkin cezai hükümleri ayrı bir kanunla hayata geçirmektedirler[163]. Bilişim suçlarını önlemek ve bu alandaki hukuka aykırı eylemleri cezalandırmak için ayrı bir kanunun varlığını gerekli görmeyen, suç politikaları gereğince suçları tek bir ceza kanunu içinde bulundurmak isteyen kimi ülkeler ise, bu alandaki cezai hükümleri ceza kanunlarında yaptıkları değişiklikler ile düzenlemektedir. TCK'de bu yöntemi benimsemiştir. Bir diğer sistemi benimseyen ülkeler ise mevzuatlarında yer alan hükümleri bilişim sistemleri kullanılarak işlenen suçları da kapsamına alacak şekilde genişletmekte ve ilave maddeler eklemektedir. Bu ülkelerde, bilişim sistemleri kullanımı ile gerçekleştirilen hukuka aykırı eylem hangi hukuki menfaati ihlal ediyorsa, suça o hukuki menfaati koruyan bölümde yer verilmektedir[164].

1.1.3.4. İnternet Üzerinden İşlenen Suçlarda Kişilik Haklarının İhlali ve Korunması

Kişisel değerlerin konusunu oluşturduğu kişisel verilerin devletten ve diğer kişilerden gelecek saldırılara karşı hukuk düzenince korunması bir zorunluluktur. Kişilik hakkı, kişinin hayatı, vücut tamlığı, sağlığı, özel hayatı ve sırları, ismi, resmi, hürriyeti, şeref ve haysiyeti kısaca tüm kişisel değerleri üzerinde söz konusu olan mutlak bir haktır[165]. Sanal ortamda kurulan bilgi bankalarında kişisel veri niteliğinde ve gizli kalması gereken bilgiler kaydedilmekte ve depolanmakta fakat devlet ve büyük işletmeler açısından büyük kolaylıklar sağlayan bu bilgi bankaları kişisel verilerin korunmasında yarattığı zaafiyet bakımından büyük tehlike arzetmektedir. Çünkü bu yolla, rıza dışı olarak kişinin özel hayatına ilişkin bilgileri üçüncü kişilerin eline geçebilme hatta yayılabilme tehlikesi ile karşı karşıyadır. Özellikle internet bu ihlalleri artıran ve hızlandıran bir etkiye sahiptir. İnternet yolu ile kişilik haklarının

---

[163] Kanun metinleri için bkz. Schjolberg, www.mossbyrett.of.no/info/legal.html, (Erişim:15.01.2013)

[164] Akbulut, Berrin, *Bilişim Suçlarının Tanımı, Tasnifi, Avrupa Hukukundaki Yeri*, Bilişim Suçları ile Mücadele Semineri (09.05.2003), Ankara: Jandarma Okullar Komutanlığı, s.4-5; Yazıcıoğlu, *Bilgisayar Suçları*, s.172.

[165] Tandoğan, Haluk, "Şahsiyetin Akit Dışı İhlallere Karşı Korunmasının İşleyiş Tarzı ve Basın Yoluyla Olan İhlallere Karşı Özel Hayatın Korunması", *AÜHFD*. Yıl. 1963, Cilt: XX, sayı.1-4, s.1-36.

ihlallerinin en başında elektronik posta (e-posta/e-mail) gönderme ve internetteki bir web sitesinde yapılan yayın yoluyla gerçekleştirilenler gelmektedir. Bunlardan başka, kişisel bilgilerin, alışkanlıkların, eğilimlerin kaydedilerek başkalarına sunulması (Cookie) ile bir kimsenin alan isminin (Domain Name) rıza dışı kullanılması da şahsiyet hakkına yönelik ihlaller arasında sayılabilir.

Bu tür suçlar mukayeseli hukukta da karşımıza çıkmaktadır. Örneğin, İngiltere'de bilişim suçları ayrı bir düzenleme ile ihdas edilmiştir. "Bilgisayarın Kötüye Kullanılması Kanunu" bu konudaki özel kanundur[166]. Alman Hukuku'nda ise, bilişim suçları ayrı bir kanunla değil, "Alman Ceza Kanunu/Strafgesetzbuch (StGB)" içerisinde düzenlenmiştir[167]. Fransız Ceza Kanunu ile bilişim suçları düzenleme altına alınmış ve yeni suç tipleri oluşturulmuştur[168]. Amerikada ise FBI bünyesinde kurulan IC3 (Internet Crime Complaint Center) bulunmaktadır. IC3, Federal Soruşturma Bürosu (FBI-Federal Bureau of Investigation) ve Ulusal Beyaz Yaka Suç Merkezi (NW3C - National White Collar Crime Center) arasında bir ortaklık olarak kurulmuştur. İnternet ile ilgili suç duyurularını almak ve araştırmak, geliştirmek ve suç duyurusu bakımıdan bir araç olarak hizmet etmek için federal, eyalet, yerel ya da uygun göreceği herhangi bir soruşturma için uluslararası kolluk ve / veya düzenleyici bir kurumdur. IC3'nin kurulmasıyla amaçlanan Internet suçlarıyla mücadeledir. Bu kurumda çalışan siber suç görevlileri; eyelet, federal devlet, yerel ve uluslararası kuruluşlar dahil geniş bir kesime kolluk hizmeti vermeye devam etmektedir[169].

Türk Hukukunda bu konuya ilişkin özel bir kanun olmadığı için, Türk Medeni Kanununun 24 ve 25. maddelerine dayanan şahsiyet hakkının korunması

---

[166] Eralp, Özgür, "Bilişim Suçları" http://www.ozgureralp.av.tr/ makaleler/bilisimsuclari sistemi engelleme 244.html, (Erişim: 16.03.2012)

[167] Mahmutoğlu, F. Selami, "Türk Ceza Kanununda Yer Alana Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", http://fsmahmutoglu.av.tr/pdf/aec4ba0684aa8f46aec75249e66d910173a2f8f47818077253.pdf, (Erişim: 21.9.2013), s. 1

[168] Schjolberg, Stein, http://www.mosstingrett.no/info/legal.html, (Erişim: 31.08.2006); Aktaran: Demircan, Tunc, *Bilişim Alanında Suçlar***,** Yayımlanmamış Yüksek Lisans Tezi, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s.38.

[169] IC3 hakkında daha geniş bilgi almak için bkz. http://www.ic3.gov/about/default.aspx, (Erişim:15.01.2014)

çerçevesinde kişisel veriler korunmaya çalışılmaktadır. Bu anlamda, internet kullanıcılarının rıza dışı her türlü kişisel bilgilerinin kaydedilmesi ve kullanımı hukuka aykırı sayılmalıdır. Özetle amaca uygunluk olarak yukarıda açıkladığımız ilke uyarınca bir hizmetten yararlanmak için verilmiş bilgilerin, ancak o hizmetin amacı çerçevesinde kalan kullanımları hukuka uygun kabul edilebilir.

1.1.4. Sonuç Olarak Korunan Hukuki Yarar

TCK'nin 135. ve 136. maddesinde düzenlenen suçla korunan hukuki yarar, Avrupa İnsan Hakları Sözleşmesinin 8. ve Anayasanın 20. maddelerinde güvence altına alınan kişilerin özel hayatının gizliliği ve korunması hakkı olduğu ortaya çıkmaktadır[170]. Bilişim alanında düzenlenen suçlar yönünden korunan hukuki yararı ise TCK'nin 243 ve 244. maddeleri ile ele almak gerekecektir. TCK'nin 243. maddesinde ki düzenlemede, bir bilişim sistemine yetkisiz erişim tek başına suç değildir; yetkisiz erişimden sonra erişilen sistemde kalmak fiiliyle suç gerçekleşmektedir. Bu tespit, maddeyle korunan hukuki yararın belirlenmesinde etkilidir. Çünkü 243. madde, yalnızca anlık yetkisiz erişimleri suç saymamakta, bir başka anlatımla anlık yetkisiz erişimlerde korunmaya değer hukuki bir yarar görmemektedir. Bu açıdan bu maddede korunan hukuki yarar karma nitelik taşımaktadır. Öncelikle kanun maddesinin düzenleniş amacında korunan temel yararın güvenilirlik olduğu sonucu çıkarılabilir. Bir bilişim sisteminin yalnızca güvenlik sistemlerinin kırılarak girilmesi orada kalınması sonucunda bile, o sistemin güvenilirliği konusundaki genel kanı yok edilmektedir[171]. Fakat bir yönüyle madde düzenlemesinde yalnızca yetkisiz erişim suç sayılmayıp, kalma fiilininde işlenmesi arandığına göre suçla korunan hukukî yarar, bilişim sisteminin güvenliğidir düşüncesi tartışmalı hâle gelmektedir. Bir başka ifadeyle, 243. maddenin (1) numaralı fıkrasında bilişim sisteminin güvenliği koruduğu ancak, kalmaya devam etme niteliğini taşıyan yetkisiz erişimlerden sonra düşünülebilir. Bu durum ise, 243/1 maddesinin işlenebilmesini ya da uygulanabilmesini oldukça güçleştirmektedir[172].

---

[170] Parlar ve diğerleri, *Türk Ceza Kanunu Yorumu*, s. 1037
[171] Dülger, *Bilişim Suçları,* s. 213-214
[172] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s.256

243. maddenin (2) numaralı fıkrasındaki *"Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir"* hükmü ise, bilişim sistemi güvenliğinin korunan temel hukukî yarar olduğu düşüncesini zayıflatmaktadır.

Bunun yanında bilişim sistemine hukuka aykırı erişimin engellenmesiyle, sistemi kullananların birden çok sayıda ve farklı menfaatleri korunmaktadır. Bu çıkarların başlıcaları; verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı veya kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukukî yararlardır. Görüldüğü üzere bilişim sistemine hukuka aykırı girme fiiller engellenmesi ile artık sadece özel hayatın gizliliğine müdahale edilmesi değil, hem ekonomik, hem de sosyal bir değer taşıyan sistemin güvenliğinin de korunması temel ilke teşkil etmektedir[173]. Bu suçun cezalandırılması, daha sonra işlenebilecek suçları engelleyici yönüyle bir tedbir özelliğide göstermektedir.

TCK'nin 244. maddesinin (1) ve (2) numaralı fıkralarında düzenlenen suçlara ilişkin korunan hukukî yarar hakkında ki görüşler üzerinde uzlaşılmış değildir. Yazarlar tarafından bu konuda çeşitli görüşler ileri sürülmüştür. Bu görüşlerin incelenmesinde konunun anlaşılabilirliği açısından yarar bulunmaktadır. Dülger'e göre, bu maddelerde ki korunan hukukî yarar, karma özellik taşır ve bilişim sistemi ile bilişim sistemi içerisinde yer alan verileri tasarruf edebilme yetkisi bulunan kişi veya kurumların, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi ve benzeri değerleri haksız müdahalelerden korumaktır[174]. Kurt tarafından ileri sürülen farklı bir görüş ise, genellikle 244. maddede bilişim sistemi ile birlikte bu sistem içerisindeki verilerin dokunulmazlığı korunan hukukî yararı oluşturmaktadır. Suçun konusu ise, bilişim sisteminin soyut ve somut bileşenleri ile sistem içinde yer alan verilerdir. Maddenin (1) numaralı fıkrasında, bilişim sistemi sahibinin mülkiyet hakkı korunurken aynı sistemin zilyedinin ise iletişim kurma, teknolojik gelişim özgürlüğü ve bilişim sisteminin dokunulmazlığı korunmaktadır. (2) numaralı fıkrada

[173] Yazıcıoğlu, *Bilgisayar Suçları*, s.19
[174] Dülger, *Bilişim Suçları,* s. 231

ise, bazen mülkiyet hakkı, bazen de verilerin içeriğine göre, fikri mülkiyet hakkı, özel hayatın gizliliği, ticari sırlar da korunmaktadır[175]. Yazıcıoğlu ise, 244. madde kapsamındaki bir suç, kimi zaman hırsızlığa veya dolandırıcılığa ya da güveni kötüye kullanmaya, hatta zimmet suçuna çok benzemekte olduğunu, fakat bu suçlardan, hırsızlığın mal üzerinde işlenmesi zorunlu iken, verinin mal olmaması; aynı şekilde dolandırıcılıkta da hile ile mağdurun kandırılması gerekirken, bilişim sistemlerinin ise kandırılmasının söz konusu olamaması sebebiyle klâsik hırsızlık ve dolandırıcılık suçlarının o zaman gerçekleşemeyeceği görüşündedir[176].

Avrupa Konseyi Siber Suç Sözleşmesi'nin 4. ve 5. maddelerinin dayanak raporları 244. maddenin (1) ve (2) numaralı fıkralarıyla paralellik taşımaktadır. Sözleşmenin 4. maddesinde korunan hukukî yarar, bilgisayar verilerine veya programlarına zarar verilmesini, veri ve programların bozulmasını, zarar görmesini engellemek, böylece bunların doğru ve işlevsel olarak çalışmalarını sağlamak olarak ifade edilmekledir. 5. maddede korunan hukukî yarar ise, temel olarak bilgisayar sabotajıyla ilgilidir ve bilişim sistemlerinin sağlıklı şekilde kullanımını sağlamak ve buna yönelecek haksız davranışlara engel olmaktır[177]. Burada korunmaya çalışılan, bilişim sistemi kullanıcılarının ve operatörlerinin, fonksiyonlarına uygun şekilde bu sistemlerini kullanma haklarıdır. Sistemlerin sağlıklı çalışabilmesi, bilişim sistemlerinin sağlıklı çalışmalarının korunabilmesine bağlı olduğu için özel korumadan yararlanmaktadır[178].

Sonuç olarak bilişim alanında saklanan kişisel verilerin elde edilmesi ya da kullanılması suretiyle işlenen suçlarda öncelikle bilişim sistemine girilmesi gerektiğinden TCK'nin 243 ve 244. maddelerindeki eylem ile başlanan fiilde bilişim sadece bir araç olarak kullanılacağı asıl olanın kişisel veriye müdahale edilmesi sonucu 135 ve 136. maddelerin düzenlediği alanın ihlal edildiğidir. Bu durumda

---

[175] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s.168
[176] Yazıcıoğlu, *Bilgisayar Suçları*, s.144
[177] Ankara Barosu, "Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı", http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/a/sibersuclar.pdf. (Erişim:19.02.2014)
[178] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 187

burada korunan hukuki yararın, kişisel verisi kullanılan kişinin özel hayatı veya kişi kendi kişisel verisini suistimal ediyorsa ilgili kişi ya da kurumun suça konu hakkının ihlal ediliyor olmasıdır[179]. Korunan hukuki yararda eylemin durumuna göre değişiklik gösterecektir. Örneğin bir kişinin özel görüntülerine ulaşılarak yapılan şantajda özel hayatın gizliliği ve ekonomik bütünlüğü, hastane kayıtlarına ulaşılarak kişinin ölümüne neden olunması durumunda hayat hakkı, kendi kişisel verilerini değiştirerek erken emeklilik hakkı elde etmesinde ise kamu hukuku ihlal edilmiş olacaktır. Fakat suçun teşebbüs aşamasında kalması halinde aynı zamanda bilişim sistemi ile ilgili tamamlanmış bir suç bulunacağından bilişim suçlarına ilişkin korunan hukuki yararında işlenmesi gerekmiş ve konuya yukarıda değinilmiştir.

[179] Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, s.77

1.2. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK HUKUKİ DÜZENLEMELER

Teknolojinin hızla ilerlemesi, kitle iletişim araçlarının yaygınlaşması ve yaygınlaşan bu araçlar sayesinde kişilerle ilgili bilgilere erişiminin çok kolaylaşması, bu verilerin hukuka aykırı olarak yetkisiz ve çoğu zaman kötü niyetli kişilerin eline geçmesine neden olmaya başlamıştır. Kişisel verilerin üzerindeki hakimiyet konusunda o kadar çok hassasiyet ve korku ortaya çıkmıştır ki, bu korku romanlarına dahi konu olmuştur. George Orwell 1949 yılında yayınlanan 1984 isimli romanında gelişen bilgi teknolojileri sayesinde Büyük Abi'nin (Big Brother) herkesi gözetlediği ve kişiler hakkında her türlü bilgileri toplayarak bu kişiler üzerinde hâkimiyet kurduğu teması işlenmiş ve özel hayatın gizliliği gibi temel hakların ihlali karşısında toplumu bilinçlendirme yolunda yayınlar yapılamaya başlanmıştır[180]. Bu endişeye paralel olarak aynı zamanda bilişim güvenliği konusu da gündeme gelmiş ve kişisel bilgilerin korunması bağlamında gerek teknik, gerekse hukuksal gelişmeler yaşanmıştır.

Kişisel verilerin korunmasına yönelik ilk temel düzenlemeler özel hayatın gizliliğine ilişkin düzenlemelerle olmuştur. İnsan Hakları Evrensel Beyannamesi'nin 12. maddesinde[181], Avrupa İnsan Hakları Sözleşmesi'nin "Özel hayatın ve aile hayatının korunması" başlıklı 8. maddesinde[182], Avrupa Birliği Temel Haklar Şartı'nın "Özel hayata ve aile hayatına saygı" başlıklı 7. maddesinde, özel hayatın

---

[180] Başalp, *Kişisel verilerin Korunması ve Saklanması,* s. 21.

[181] İHEB 12. madde; "Hiç kimsenin özel yaşamına, ailesine konut dokunulmazlığına ya da yazışma özgürlüğüne keyfi olarak karışılamaz; Kimsenin onur ve ününe karşı kötü davranışlarda bulunulamaz. Herkesin bu karışma ve kötü davranışlara karşı kanunlarla korunma hakkı vardır." Ankara Barosu, "Avrupa İnsan Hakları Evrensel Bildirisi", http://www.ankarabarosu.org.tr/siteler/abihm.org/iheb.htm. (Erişim: 17.02.2014)

[182] AİHS 8. madde; "Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir." Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü İnsan Hakları Daire Başkanlığı, "Avrupa İnsan Hakları Sözleşmesi", http://www.inhak.adalet.gov.tr/temel/aihs.pdf. (Erişim: 17.02.2014)

gizliliğine ilişkin düzenlemeler getirilmiştir[183]. Fakat bu genel çalışmaların yanında kişisel verilerin korunmasına dair duyulan ihtiyaca paralel olarak daha özel çalışmalar da yapılmaya başlanmıştır. Kişisel verilerdeki bu özel çalışmalar tarih itibarı ile ilk uluslararası düzenlemelerde ortaya çıktığından öncelikle uluslararası alanda bu konuda yapılan çalışmaların akabinde Türkiye'de bu konuda yapılan ulusal düzeydeki çalışmaların incelenmesi daha uygun olacaktır. Bu konuda çalışmanın ana çerçevesini ceza hukuku oluşturduğu için ceza yaptırımı içeren düzenlemeler ve özellikle henüz kanunlaşmayan "Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı" üzerinde ayrıntılı durulması yararlı olacaktır.

Amerika Birleşik Devletleri (ABD), bilgisayarın icat edildiği ilk ülke olarak bilişim alanındaki suçlarla ilk önce tanışan ülke konumundadır. Bu durumda doğal olarak hem akademik, hem mevzuat, hem de uygulamada ABD merkez alınabilecek bir ülke pozisyonundadır[184]. Bu kapsamda kayıtlı olarak karşımıza çıkan ilk bilişim suçu, 18.10.1966 tarihli Minneapolis Tribune gazetesinde yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" isimli haber ile gündeme girmiştir[185]. Aslında bu ilk bilişim suçu olarak anılsada bilişim suçu niteliği taşıyan fiiler, 1960'lı yılların başında yine Amerika'da telefon şirketlerini zarar uğratan "phreaker, elektronik korsanlar" olarak nam salmış bir gurup insanın yaptığı uzun mesafeli telefon görüşmeleriyle karşımıza çıkmaktadır[186]. İlk bilişim suçu kıpırtılarının bulunduğu bu yılları takip eden 1970'li yılların ilk yarısı ulusal ve uluslararası boyutta bilişim suçlarıyla ilgilenilmeye başlanan ve ilk bu konuda ceza normlarının düzenlendiği dönem olmuştur. Bilişim suçlarına yöneliki ilk kapsamlı kanun teklifi Amerikan Kongresi'ne 1977 yılında sunulmuştur. Bu kanun teklifinin

---

[183] Ersoy, Uğur, (2009), *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü, s. 49

[184] "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları hakkında Kanun Tasarısı" gerekçesinden alıntı, Türkiye Bilişim derneği, http://www.tbd.org.tr/index.php?dummy=1&sayfa=raporlar&vkid=194&t= 1300665963&jfr=true&keepThis=true&TB_iframe=true&height=500&width=800, (Erişim: 12.05.2013)

[185] Aydın, Emin**,** *Bilişim Suçları ve Hukukuna Giriş*, Ankara: Doruk yayınları, 1992, s.25.

[186] Mungo, Paul ve Clough, Bryan, *Sıfıra Doğru Veri Suçları ve Bilgisayar Yeraltı Dünyası* (Çev. Emel Kurma), İstanbul: İletişim Yayınları, 1999, s.20.

önemi Kongre tarafından kabul edilmemesine karşın, bilişim suçlarının dünya çapında tanınmasını sağlamıştır[187].

1.2.1. Uluslararası Düzenlemeler

Uluslararası antlaşmaların onaylanması halinde iç hukukta da kanun gücünde olması nedeniyle burada inceleme konusu yapılması uygun görülmüştür. Uluslararası sözleşmelerin iç hukuka etkisi bakımından; Kişisel verilerin korunmasına ilişkin olarak Anayasanın 16. maddesinde yabancılar yönünden uluslararası hukuka yollama yapılmıştır. Yine Anayasa'nın 90. maddesinde de uluslararası antlaşmaların onaylanması düzenlenmiştir. Bu iki madde birlikte göze alındığında, iç hukukta, kanunla benimsenen insan haklarına ilişkin uluslararası sözleşmeler, iç hukuk kuralı olarak Türk hukuk düzeninde en üstte yer almaktadır[188]. Kaldı ki Anayasa'nın 90/5. maddesin de "Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır'' şeklinde yapılmış bulunan düzenleme ile Türk iç hukuku açısından uluslararası sözleşmelerin kanundan daha üstün olduğu ve uygulayıcı tarafından evveliyatla uygulamada tercih edilmesi gerektiği söylenebilir[189]. Bir başka yönüyle ise iletişim teknolojisindeki gelişmelere paralel olarak ülkeler arası ilişkilerin de gelişmesiyle, ulusal düzenlemelerin yetersiz olması ülkeleri uluslararası işbirliğine ve ulusal düzenlemeleri uluslararası standartlara uyarlamaları gereksinimini kaçınılmaz kılmıştır[190].

Kişisel verilerin korunması hakkının ayrı bir alan olarak doğrudan doğruya ele alınması ve bu konuda uluslararası kriterler belirlenmesine dair ilk çalışma Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 1980 yılında kabul

---

[187] Schjolberg, Stein, "The Legal Framework – Unauthorized Access to Computer Systems", *Penal Legislation in 44 Countries*, www.mossbyrett.of.no/info/legal.html, (Erişim: 15.01.2013)

[188] Selçuk, Sami (1999), "Avrupa İnsan Hakları Sözleşmesi ve Türk Uygulaması", *Türkiye Günlüğü Dergisi,* Cilt: Ocak-Şubat 1999, Sayı: 54, s. 15 vd.

[189] Başlar, Kemal, *Türk Mahkeme Kararlarında Avrupa İnsan Hakları Sözleşmesi*, Ankara: Şen Matbaası, 2008, s. 17 ve 18

[190] Kaya, Cemil, *Assessing the Transfer of Personal Data in the European Union,* 1. Baskı, İstanbul: On İki Levha Yayıncılık, 2011, s. 1.

edilmiş olan "Gizliliğin Korunması ve Sınır Ötesi Kişisel Veri Akışları Hakkında Rehber İlkeler" (Guidelines on The Protection of Privacy and Transborder Flows of Personal Data) adını taşıyan belgedir[191]. Belge düzenleme açısından daha çok rehber ilkelere sahip olup, bu Rehber İlkeler, 23.09.1980 tarihinde kişisel verilerle ilgili olarak, bu verilerin toplanması, kaydedilmesi ve koruma altına alınması ile ülke sınırını aşan bilgi akışı ihtiyacının karşılanmasında asgari düzeyde uluslararası uzlaşının sağlanması ve ana ilkelerin tespiti gayesiyle çeşitli hükümetler, sivil toplum örgütleri, iş dünyası ve tüketici temsilcilerinin iştirakiyle yapılan bir çalışma sonucu kabul edilmiştir. Bu çalışma, kişisel verilerin korunması amacıyla yapılan düzenleme ve uygulamalarda uluslararası uyumun sağlanması, gizliliğin korunmasının etkinliği ile veri transferindeki sınırlar arasında bir denge sağlanması, ayrıca devletlerin gerek kamu gerekse de özel sektör bazında uygulama ve düzenlemelerini kontrol altına almanın temini amacıyla ülkesel bazda düzenlemeler yapmasının teşvik edilmesi ve bu konuda bir fikir vermek amacıyla yapılmıştır[192].

Belirlenen Rehber İlkeler bağlayıcılığı olmayan tavsiye niteliğinde bir belge olduğundan dolayı, konu uluslararası antlaşma niteliğini haiz bir belge ile kuvvetlendirilmek istenmiş[193] ve telekomünikasyon sistemlerinde meydana gelen gelişmeler ve veri iletişim hızlarının ülkelerarası çok yüksek hızlarda yapılması karşısında elektronik veri bankalarında saklanan, kişilerin özel hayatlarına ilişkin verileri koruma konusunda Avrupa Konseyi üyesi ülkelerin mevzuatlarının yetersiz kalmasından dolayı, konuyu uluslararası boyutta ele almak ve uluslararası bir sözleşme ile düzenlemek gerekmiş; bu amaçla 1981 yılında "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" hazırlanmıştır. 28.01.1981 tarihinde Avrupa Konseyi üyesi ülkelerle birlikte Türkiye

---

[191] OECD, "Guidelines on The Protection of Privacy and Transborder Flows of Personal Data" http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborder flowsofpersonaldata.htm, (Erişim: 17.02.2014)

[192] OECD, "Guidelines on The Protection of Privacy and Transborder Flows of Personal Data" http://www.oecd.org/document/18/0,2340, en 2649 34255 1815186 111 1,00.html, (Erişim: 03.05.2012)

[193] Wong, Rebecca. (2007). "Data Protection Online: Alternative Approaches to Sensitive Data", *Journal of International Commercial Law and Journal of International Commercial Law and Technology,* Vol. 2, Issue 1, Law Department, University of Sheffield, s.2

tarafından da imzalanmış, fakat Türkiye bu belgeyi onaylamamıştır[194]. Avrupa Birliğinde bu belgenin yürürlüğe girmesi 1985 yılında mümkün olabilmiştir. Belge ile ilgili olarak günümüze kadar değişik zamanlarda farklı tavsiye kararları alınmış, 1999 yılında ise Belge'de bir takım değişiklikler yapılmıştır. Ancak Belge Avrupa ülkelerinin yanında bütün dünyada kabul görmüş ve konu hakkında düzenleme yapmak isteyen tüm ülkelerin ulusal mevzuatının hazırlanmasında rehber olmuştur[195]. Sözleşmenin amacı; üye devletlerin hâkimiyet alanında kişisel alanın korunması sağlanırken, kişisel verilerin korunması ile ilgili yeknesak bir hukuk düzeni ortaya koymak olmuştur[196].

İncelenmesi önem arzeden uluslararası belgelerden bir diğeri de "Sanal Ortamda İşlenen Suçlar Sözleşmesi'dir". Sözleşme, suç sorunlarına dair Avrupa Komitesi'nin (CDPC- European Committee on Crime Problems) 1996'da, Avrupa Konseyi'ne siber suçlara ilişkin bir uzman komitesi kurmasını tavsiye etmesine üzerine oluşturulmuştur[197]. 01.07.2004'de yürürlüğe giren "Sanal Ortamda İşlenen Suçlar Sözleşmesi", bu alandaki ilk uluslararası antlaşmadır[198]. Öte yandan "Sanal Ortamda İşlenen Suçlar Sözleşmesine Ek Protokol[199]" ise, bilgisayar sistemleri aracılığıyla işlenen, ırkçı ve yabancı düşmanlığı güden nitelikli eylemlerin cezalandırılmasını düzenlemektedir[200]. Bazı devletlerin ifade özgürlüğünün kısıtlanmasına dönük endişeleri sebebiyle, ırkçılık ve yabancı düşmanlığının bilişim sistemleri aracılığıyla işlenmesinin cezalandırılması konusunda uzlaşı sağlanamamış

---

[194] Değirmenci, Olgun, *Bilişim Suçları*, Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2002, s.40.

[195] Kesmez, Necdet "Kişisel Verilerin Korunması Üzerine", *Bilişim Şurası*, http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0044/01KIŞISELVERILERINKORUNMASI.doc, (Erişim:14.02.2014), s. 2-3

[196] Tansuğ, Avniye, "AB'nin Yeni Ekonomik Silahı: Veri Saklama Hukuku", s.56

[197] İçel, Kayıhan, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", *İÜHFD*, Cilt: 59, Sayı: 1-2, 2001, s. 4-5.

[198] Türkiye bu sözleşmeyi 10.11.2010 tarihinde imzalamış, 22.04.2014 tarihinde onaylanmıştır (Kanun No: 6533).
Önok, Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede uluslararasi İşbirliği", http://dosya.marmara.edu.tr/huk/fak%C3%BCltedergisi/nurcentel/murat onok.pdf. (Erişim: 31.03.2014), s. 1241

[199] 28.01.2003 tarihinde Strazburg'da kabul edilmiştir.

[200] Helvacıoğlu, Aslı Deniz, "Avrupa Konseyi Siber Suç Sözleşmesi – Temel Hükümlerin İncelenmesi", *İnternet ve Hukuk Dergisi* (derleyen Yeşim, M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul: 2004, s. 279

ve bu konu Sözleşmede "Ek 1. Protokol" olarak girmiştir[201]. "Budapeşte Sözleşmesi" olarak anılan bu sözleşmede üç amaç olduğu söylenebilir.

1) Siber suçlar konusunda terim birliği dolayısı ile de mevzuat uyumunun sağlanması,
2) Uluslar arası yetki kurallarını belirleyerek soruşturmanın ve kovuşturmanın sağlıklı yürütülmesini sağlamak,
3) Uluslararası işbirliği yöntemlerini belirleyerek, yürürlüğünü sağlamak[202].

Sözleşme'nin 3. kısmı, sınır tanımayan niteliğe sahip, bir çok devlet üzerinde aynı anda işlenebilen ve soruşturulması ile kovuşturulması çok teknik ve zorunlu bir süreç gerektiren, delillerin heran yok olabildiği bir suç türüyle mücadelede, etkin ve çok hızlı uluslararası işbirliği sağlaması yönüyle en önemli kısmı olmaktadır. Sözleşme, sadece siber suç olarak tanımlanan fiilleri değil; "elektronik şekilde" delil toplanmasını gerektiren tüm suçları, yani bilişim sistemi aracılığıya işlenmiş klasik suç tiplerini, kapsamaktadır[203]. İnternetin icadı ve hızla yaygınlaşmasının bir sonucu olarak vicdanları yaralayan[204] bilişim sistemleri vasıta kılınarak çocukların pornografik içerikli görseller kullanılarak veri üretilmesi, yayılması ve saklanması eylemlerinin belirtilen sözleşme ile açık ve ayrıntılı olarak tanımlanması ve söz konusu eylemlerin sanal ortamda da olsa gerçekleştirilme şekli farketmeksizin suç olarak düzenlenmesi bu sözleşmenin dikkat çeken en önemli yararlarında birisidir[205]. Sözleşmede birtakım verilere el konulmasına ya da bunların muhafazına ya da bunların açıklanmasına yönelik hükümler mevcuttur. Ancak bu düzenlemelerin aşırı müdahaleci bir elektronik denetleme sistemi getirdiğini söylemek doğru

---

[201] 01.03.2006'da yürürlüğe giren bu Protokol, Türkiye tarafından henüz imzalanmış değildir.

[202] Sözleşme metni için bkz. TBMM, "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)", http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf. (Erişim: 29.11.2014)

[203] Koca, Mahmut, "*Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku"*, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, Ankara: Beta Yayınları, Cilt: 3, 2003, s. 791.

[204] Raman, Jari, "Computer Crime", ENLIST, Nov. 7, 2000, http://itlaw.law.strath.ac.uk/ENLIST/subjects/is/commentary/ (Erişim: 06.05.2012), s.6

[205] Dülger, Murat Volkan, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", *Kazancı Hukuk, İşletme ve Maliye Bilimleri Dergisi*, İstanbul: Sayı:5, Ocak 2005, s. 114

olmayacaktır. Çünkü resmi bir ceza soruşturması olmadıkça, gerek servis sağlayıcı gerekse polis tarafından, kişisel iletişimin denetlenmesine yer verilmemiştir[206].

Kişisel verilerin korunmasına dair uluslararası çalışmalardan biri de Birleşmiş Milletler (BM) tarafından sergilenmiştir. 14.12.1990 tarihinde Birleşmiş Milletler Genel Kurulu'nun 45/95 sayılı Kararı ile "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Rehber İlkeler (Guidelines for the Regulation of Computerized Personal Data Files)" adını taşıyan belgede, bilgisayar ortamında işlenen kişisel verilerin korunmasıyla ilgili olarak devletlerin ulusal mevzuatlarında asgari düzeyde düzenlemesi gereken bir takım ilkelere yer verilmiştir[207]. Bu alanda, BM tarafından yapılan "Uluslararası Kişisel ve Siyasal Haklar Sözleşmesi" temel amacı olmamakla birlikte özel hayatın korunmasına yönelik olarak yapılan düzenlemelerden biri sayılabilir. Birleşmiş Milletler İnsan Hakları Komitesi bu Sözleşmenin özel hayatı düzenleyen 17. maddesinde, hem kamusal hem de özel sektör alanında kişisel verilerin korunmasına dair düzenlemelerin yapılmasının zorunlu olduğu belirtilmektedir. Komite, kamu ve özel sektörler bakımından kişisel verilerin korunmasının garanti altına alınmasına ilişkin olarak ortaya koyduğu görüşünde; kişisel veriler hakkındaki düzenleme aracının kanun olması ve koruma için etkili önlemlerin kanunla alınması gerektiğini, bireylerin kişisel verilerinin saklanma amacının kolayca tespit haklarının bulunduğunu, kendilerine ilişkin verileri hangi kurum ya da kurumların kontrol ettiğini bilebilmesi ve aksi bir davranış karşısında bireyin kişisel veriyi yok etmeyi talep etme hakkına sahip olması gerektiğini belirtmektedir[208].

Avrupa Birliği (AB) tarafından yapılan düzenlemelerin bu çalışmada göz ardı edilemez bir yeri vardır. Birliğin oluşturulma sürecinde özellikle AB antlaşmasının

---

[206] Önok, *Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede uluslararasi İşbirliği*, s. 1245

[207] Kesmez, *Kişisel Verilerin Korunması Üzerine*, s. 3

[208] General Comment 1, UNDo Cilt: Hrı\Gen\1\Rev.1 At 21 (1994) http://www1.umn.edu/humanrts /gencomm/hrcom16.htm, (Erişim: 14.02.2014), Lee, A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Right Treaties", *International Journal of Law and Information Technology*, Vol.6, No.3, s.247-284, http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf, (Erişim: 14.02.2014)

6/2. maddesinde[209] Avrupa Birliğine üye devletlerin anayasal geleneklerinde bulunan ortak değerlerin bir sonucu olan ve topluluk hukukunun genel prensiplerinden kaynaklanan temel haklara saygı özel bir yere sahiptir. Bu bakış açısıyla Avrupa İnsan Hakları Sözleşmesinin (AİHS) 8. maddesi "özel ve aile hayatını" daha özenli olarak koruma altına almıştır[210]. Avrupa İnsan Hakları Mahkemesi'de (AHİM) bu prensiplerden kaynaklanan bir haraketle kararlarının bir kısmında, kişisel verilerle ilgili kararlarında verilerin gizliliği, özel hayatın korunması kavramlarına önem vermiş, hatta bu konuda mevzuat düzenlemesi konusunda öncü olmuştur. Özellikle *"özel hayat"* kavramı kapsamında ve 8. maddeyle güvenceye bağlanan en mühim konulardan biri de kişisel verilerdir. AHİM birçok kararında "özel hayat" ile ilgili olarak bu kavramın geniş yorumlanması gerekliliği üzerinde durmuştur. Buna göre kişilere ait özel hayatın kapsamında kalan verilerin toplanması, kaydedilmesi, saklanması ve kullanılması Sözleşmenin 8. maddesi kapsamında değerlendirilerek kararlar verilmektedir[211]. Bu konuda yapılan en hayati eleştirilerden birisi ise; "kişisel verilerin, özel hayatın gizliliğinin geleneksel yaklaşımlar ve yine bu alanda benimsenen bir takım ilkelerle korunmaya çalışılmasının, teknolojik alanda yaşanan gelişmeler karşısında yetersiz kalması, kendine özgü bazı gereklilikleri nedeniyle ayrı bir alan olarak ele alınması gerektiği konusundadır"[212]. AİHM'nin "kişisel veri" hakkındaki görüşü, bu konuda yapılan başvurular üzerine verdiği birçok kararında, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme'ye*"* atıfta bulunmasından ötürü, bu Sözleşmedeki "kişisel veri" tanımını benimsediği olarak yorumlanabilir.

---

[209] Başbakanlık Avrupa Birliği Genel sekreterliği, "Avrupa Birliği Antlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma", http://www.ab.gov.tr/files/pub/antlasmalar.pdf. (Erişim:07.06.2015)

[210] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 200

[211] Bkz. Leander v. Sweden kararı. "*Leander* kararında Mahkeme, başvurucu hakkında güvenlik soruşturması yapılması ve elde edilen bilgilerin doğruluğuna karşı başvurucuya itiraz hakkı verilmemesinin özel yaşama saygı hakkına müdahale oluşturduğuna belirtmiştir. Ancak kararın devamında ise Mahkeme, iç hukukta kanuna dayanan bu müdahalenin ulusal güvenliği koruma amacını taşıdığına, müdahale devletin takdir alanı içinde kaldığından ve gizli soruşturmanın istismarına karşı yeterli ve etkili güvenceler getirildiğinden demokratik bir toplumda gerekli olan müdahale nedeniyle özel yaşama saygı hakkının ihlal edilmediğine karar vermiştir." Tezcan, Durmuş; Erdem, M. Ruhan ve Sancakdar, Oguz, *Avrupa İnsan Haklan Sözleşmesi Işığında Türkiye'nin İnsan Haklan Sorunu*, Ankara: Seçkin Yayınevi, 2004, s. 387.

[212] Küzeci, *Kişisel Verilerin Korunması*, s.70.

Yukarıda anılan Sözleşmenin "özellikli veri kategorileri" başlığını taşıyan 6. maddesi; *"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."*[213] şeklindedir. Bu maddenin yorumundan, söz konusu Sözleşmeye göre bir kişinin kimliğini belirten ya da belirtmeye elverişli verilerin "özellikli veriler", bunun dışında kalan veriler ise "diğer veriler" olarak ikiye ayrılarak uygulandığı söylenebilir. Kaldi ki kişisel verilerin hakkında madde metni açıklayıcı bir şekilde tespit yaptığından bu konuda her hangi bir sorun kalmamıştır. Ancak ilgilenilmesi gereken asıl sorun; bu madde kapsamında bulunmayan, fakat kişinin kimliğine işaret eden ya da belirlemeye uygun diğer verilerin belirlenmesine ilişkindir. Açıkçası bu sorunun çözümü için en önemli başvuru kaynağı Avrupa İnsan Hakları Mahkemesi içtihatları olacaktır. Belirtilen türden şikayetler ile yapılan başvurular nedeniyle verilen kararlara bakıldığında; bir kişinin görüntüsü, fotoğrafları, parmak izi, gen profili, tıbbi verileri ve örnekleri, ev ve iş adresi, ekonomik durumunun detaylarının "kişisel veri" kapsamında değerlendirildiği görülmektedir. Tabii ki kaçınılmaz sonuç olarak, bu konudaki gelişmelere paralel olarak, sınırlandırılamayacak bu listenin kapsamının sürekli genişlemesi doğaldır.

Sözleşmenin 8.maddesinde koruma altına alınan "özel hayat" hakkının ihlali suçu verinin toplanması, saklanması ve kullanılması eylemlerinin birlikte gerçekleştirilmesi şekilinde olabileceği kadar her bir eylemlede bu hak ihlal edilebilir. Bununla birlikte Mahkeme, kararlarını verirken toplanan, saklanan veya kullanılan verilerin özelliklerini, kullanım durumunu ve sonuçta elde edilebilecek çıktıları da dikkate almaktadır. Mahkeme bu konuda Sözleşmenin 8. maddesinin 1.

---

[213] Avrupa Konseyi, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme" http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm, (Erişim: 26.01.2013), s.1

fıkrası ile 2. fıkrası arasında "adil bir dengenin" kurulup kurulmadığı ölçütüne dikkat etmektedir[214].

AB'de kişisel verilerin korunması konusunda ilk tasarılar doksanlı yıllarda ortaya çıkmaya başlamıştır. Avrupa Parlamentosu ve Avrupa Konseyi 24.10.1995 tarihinde "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesini" 95/46/EC Direktifi olarak kabul etmiştir[215]. Bu Yönergenin yürürlüğe girmesi oldukça gecikmiş ve ancak 1998 yılında yürürlüğe girebilmiştir. Avrupa Parlamentosu ve Bakanlar Konseyi 1997 yılında bu Direktifi desteklemek ve eksik kalan alanları tamamlamak maksadıyla "Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesini" yapmış ve yürürlüğe koymuştur. Bu yönerge ise 97/66/EG nolu yönerge ismini almıştır[216]. Bunu müteakip AB bu Yönergeyi tamamlayan ve ileri teknolojik ortamlardaki ilişkileri de kapsayacak şekilde yeni bir veri saklama hukuku olarak ortaya koyduğu 2002/58/EC Sayılı "Özel Hayatın Korunması ve Elektronik İletişim Yönergesini"[217] çıkartmış, daha sonra 2006/24/AB sayılı ve 15.03.2006 tarihli Direktif, 2002/58/AT sayılı Direktifin yerini almıştır[218]. Bu düzenlemelerin Türk Kişisel Verilerin Korunması Kanun Tasarısının oluşumunda önemli etkileri olmuştur. Bununla beraber bağlayıcı tek uluslararası arası antlaşma olma niteliğini hala koruyan Avrupa Konseyi tarafından kabul edilmiş olan "Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkında Sözleşme'dir"[219]. Avrupa Konseyinin kabul ettiği Sözleşmeleri, konusuna göre bir tasnife tabi tuttuğumuzda, Avrupa'da standart kurallar oluşturulmasına katkı sağlayacak anlaşmalar ve üye ülkeler arasında

---

[214] Salihpaşaoğlu, Yaşar, "Özel Hayatın Kapsamı, Avrupa İnsan Hakları Mahkmesi İçtihatları Kapsamında Bir Değerlendirme", *Gazi Üniversitesi Hukuk Fakültesi Dergisi (GÜHFD)*, Cilt:17, Sayı:3 2013, s. 244,

[215] Tansuğ, "AB'nin Yeni Ekonomik Silahı: Veri Saklama Hukuku", 55.

[216] Başalp, Nilgün, "Kişisel Verilerin Korunması ve İnternet", *İnternet ve Hukuk Dergisi,* Derleyen Yeşim M. Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004, s.27.

[217] Tansuğ, "AB'nin Yeni Ekonomik Silahı: Veri Saklama Hukuku", s.55

[218] Korff, EC Study on Implementation of Data Protection Directive*,* s. 1-210

[219] Kesmez, "Kişisel Verilerin Korunması Üzerine", s.3

işbirliğine katkı sağlayacak anlaşmalar şeklinde iki gurup olduğu görülecektir. 108 Sayılı Sözleşme standart kuralları belirleyen birinci kategoride yer almaktadır[220].

ABD'de ise "Siber Bilgi Paylaşım ve Koruma Kanunu (Cyber Intelligence Sharing And Protection Act - CISPA)" bulunmaktadır. 11.11.2011 tarihinde Beyaz Saraya sunulan kanun tasarısının amacı internet üzerinden yapılan veri akışına ilişkin bilgilerin ABD hükümeti ve ilgili teknoloji şirketleri arasında paylaşımını sağlamaktır. Böylece tasarının kanunlaşması ile ABD hükümetine siber tehditleri araştırmada yardımcı olmaya ve ağın siber tehditlere karşı güvenli olması sağlamaya çalışılmaktadır [221]. Kanun içerik olarak aslında siber güvenliği tehdit etme potansiyeli bulunan durumlarda kişisel verilerin ABD hükümetiyle paylaşılmasını öngörmektedir[222]. ABD'de çıkan bu kanun ile ABD vatandaşı olmayan ancak ABD şirketlerinden hizmet alan kişiler açısından da önem taşımaktadır. Bahsi geçen ABD şirketleriyle paylaşılan tüm veriler, hiçbir mahkeme kararı ya da kullanıcı rızası olmadan ABD hükümeti ve dolayısıyla bir başka ABD şirketiyle paylaşılabilecektir. Bir başka deyişle e-postalar, bulutta depolanan doküman ve dosyalar, sosyal medyadaki özel paylaşımlar ABD hükümeti tarafından izlenebilecektir.

Konuyla ilgili olarak ABD'de ilk defa 1984 yılında "*Counterfeit Access Device and Computer Fraud and Abuse Act (Erişim Aygıtlarını Taklit Etme, Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu)*" ile "*Credit Card Fraud Act (Kredi Kartı Sahteciliği Kanunu)*" yürürlüğe girmiştir. Aynı Kanunda 1986 yılında "*Computer Fraud and Abuse Act (Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Kanunu)"* ile değişiklikler yapılmıştır. Bunlarla birlikte bilişim suçlarında mücadelede;

---

[220] Benoit, Rohmer Florance ve Klebes, Heinrich, *Avrupa Konseyi Hukuku Pan-Avrupa Hukuk Alanına Doğru,* Ankara: Avrupa Konseyi Yayını. 2006, s. 110, http://www.dispolitika.org.tr/dosyalar/kitap_akh.pdf, (Erişim: 17.06.2015)

[221] Wikipedia, "Cyber Intelligence Sharing and Protection Act", http://tr.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act, (Erişim:23.01.2014)

[222] BThaber.com, "CISPA: İnsan Hakları İhlalinin Yasal Yolu (Mu?)", http://www.bthaber.com/cispa-insan-haklari-ihlalinin-yasal-yolu-mu/, (Erişim:23.01.2014)

- 18. U.S.C. 1029 sayılı Erişim Aygıtlarıyla İlgili Sahtecilik ve Bağlı Eylemler,
- 18. U.S.C. 1030 sayılı Bilgisayarlarla İlgili Sahtecilik ve Bağlı Eylemler,
- 18. U.S.C. 2511 sayılı Telli, Telsiz ve Elektronik İletişime Müdahale ve İletişimin Açıklanmasının Yasaklanması,
- 18. U.S.C. 2701 sayılı Depolanmış İletişime Yetkisiz Erişim,
- 18. U.S.C. 2702 İçeriğin Açıklanması,
- 18. U.S.C. 2703 Kanuni Erişim İçin Gerekli Şartlar isimli kanunlar da kullanılmaktadır.

Ayrıca ABD'nin bilişim hukuku alanı mevzuatında "Elektronik Haberleşme Gizlilik Kanunu (1986), Bilgi ve Teknoloji Kanunu, Ulusal Bilgi Altyapısı Kanunu (1992), Çocukların On-line Yayınlardan Korunması Kanunu (1998), İnternette Kumarın Önlenmesi Kanunu (1997), Anti-Terörizm Kanunu (2001), İletişim Ahlâk Kanunu (1996)" bulunmaktadır[223]. Pek yakında, internet hızının milisaniyelerle ölçülecek bir hıza erişmesi ve elektronik iletişimin olağanüstü artmasına paralel kişisel verilerin büyük bir hızla kurumlar arası hatta ülkeler arası aktarılmaya başlanmasıyla, korunması gereken alanların daha da genişleyeceği ve buna nisbetle kişisel verilerin korunmasının da oldukça güçleşeceği apaçık ortadadır. Bu nedenle bu hakkı koruma altına alan kanunlar ve diğer düzenlemelerin ile benzer belgelerde belirlenen ilke ve kuralların uygulanması ile ilgili sistemlerin yeniden gözden geçirilme gerekliliği ortaya çıkacaktır.

1.2.2. Ulusal Düzenlemeler

Türk hukuk sistemi içerisinde kişisel verilerin korunması hukuku yakın zamanlarda giderek artan bir şekilde yerini almaktadır. Anayasamızda çeşitli uluslararası ve uluslarüstü metinlerde ayrı bir hak olarak düzenlenen kişisel verilerin korunmasına

[223] Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları hakkında Kanun Tasarısı gerekçesinden alıntı, http://www.tbd.org.tr/index.php?dummy=1&sayfa=raporlar&vkid=194&t=1300665963&jfr =true &keepThis=true&TB_iframe=true&height=500&width=800, (Erişim: 12.05.2013)

paralel çerçeve niteliğinde maddeler halinde sıralanan hükümlerle yetinilmiş, kişisel verilerin korunmasına dair doğrudan hükümler genel ve özel kanunlara bırakılmıştır. Türk Medeni Kanunu kişilerin özel hayatını Medeni Hukuk açısından 24 ila 27. maddeleri arasında koruma altına almıştır. TCK'de ise 135 vd. maddelerde kişisel verilerin korunmasına ilişkin düzenlemeler yer almıştır. Bunun dışında İş Kanunu vb. gibi özel hukuk alanında yer alan kanunlarda da düzenlemeler bulunmaktadır. "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Korunması Hakkında Yönetmelik" kişisel verilere özgü tek ve en önemli düzenleme olarak karşımıza çıkmaktadır. Ayrıca Türkiye'nin gerek imzalamış olduğu 108 sayılı Avrupa Konseyi Sözleşmesi'ne uyum sağlamak, gerekse de AB'ye giriş sürecinde genelde AB mevzuatına, özelde de 95/46 sayılı Direktif ile iç mevzuatı uyumlaştırmak amacıyla kişisel verileri koruma kanunu olarak çıkartılması düşünülen[224] ve ülke gündemini oldukça meşgul eden bu konu hakkında asıl düzenleme Adalet Bakanlığı tarafından hazırlanan "Kişisel Verilerin Korunması Hakkında Kanun Tasarısıdır". Bu tasarı AB tarafından yapılan tavsiyeler dikkate alınarak değişik zamanlarda oluşturulan komisyonlarca hazırlanmış ve bu tasarılardan ilki 09.11.2005 tarihinde Adalet Bakanlığınca tasarıya son şekli verilerek Başbakanlığa, Türkiye Büyük Millet Meclisine (TBMM) sevki için gönderilmiş, tasarı daha sonra kadük hale gelmiştir[225]. İkincisi ise 22.04.2008 tarihinde TBMM'ye sunulmuş, fakat bu tasarıda kanunlaşmayarak kadük olmuştur. En son tasarı 26.12.2014 tarihinde Adalet bakanlığınca Başbakanlığa, TBMM'ye gönderilmek üzere sevkedilmiş ve halen kanunlaşmamıştır.

1.2.2.1. Anayasa

Bir üst norm olan Anayasada elektronik ortamda işlenen kişisel veriler ile ilgili özel bir hüküm bulunmamaktadır. Zaten Anayasanın ruhuna aykırı olacak bu durum kanunlara havale edilmiş olup, kanunlarda uyulması gereken kuralların çerçevesi belirlenmiştir. Kişisel verilerin korunmasıyla ilgili olan 20. madde, "Özel Hayatın

---

[224] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 88

[225] Tasarını son haline ulaşmak için bkz. Adalet Bakanlığı Kanunlar Genel Müdürlüğü, "Tasarılar" http://www.kgm.adalet.gov.tr/kişiselveriler.htm, (Erişim: 25.05.2015)

Gizliliği ve Korunması" kenar başlığını taşır. Kişisel verilerin korunması ilk kez anayasaya 2010 yılında yapılan değişiklikle girmiş[226] ve bu maddeyle kişisel verilerin korunması hakkı anayasal koruma kazanmıştır. Düzenleme kapsamında, kişilerin kendilerine ait veya ilgilendiren kişisel veriler yönünden hangi hak ve yetkilere sahip oldukları ile kişisel verilerin işlenilebilme halleri düzenlemiştir. Konun ayrıntılarını düzenleme yetkisi ise kanuna bırakılmıştır. 22. madde ile de bir nevi kişisel veri olma özelliği taşıyan elektronik ortamda e posta gibi vasıtalarla haberleşmede kullanılan veriler kişisel veri korunması kapsamında değerlendirilmekte ve güvence altına alınmaktadır[227]. Aşağıda gösterilen anayasal güvenceler ise, kişisel verilerin korunması hakkına dolaylı bir şekilde güvence getirmektedir;

Anayasa Başlangıcı (6'ncı paragraf),
Madde 2: Hukuk devleti ilkesi,
Madde 17: Bireyin maddi ve manevi varlığını geliştirme hakkı,
Madde 21: Konut dokunulmazlığı,
Madde 22: Haberleşmenin gizliliği,
Madde 24: Dini ve vicdani kanaatleri açıklamaya zorlanamama,
Madde 25: Düşünce ve kanaatleri açıklamaya zorlanamama.

1.2.2.2. Avrupa Birliği Komisyonu İlerleme Raporları, Katılım Ortaklığı Belgesi ve Türkiye Ulusal Programında Kişisel Verilerin Korunması

Kişisel verilerin korunması ile ilgili düzenlemeler Avrupa Birliği Komisyonu İlerleme Raporlarında, Ulusal Program ile Katılım Ortaklığı Belgelerinde de yer almaktadır. İlerleme Raporları, AB'ye aday ülkelerin, katılım için geçen bu süreçde Kopenhag Kriterlerine uyum göstermek için kaydettikleri gelişmeleri takip eden ve değerlendiren, 1998 yılından bu yana Avrupa Birliği Komisyonu tarafından yıllık

[226] Resmi gazete, http://www.resmigazete.gov.tr/eskiler/2010/05/20100513.htm, (Erişim: 05.05.2011)
[227] Civelek, Dilek Yüksel, *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi,* Yayımlanmamış Uzmanlık Tezi, Ankara: Devlet Planlama Teşkilatı, 2011, s.141

olarak hazırlanan raporlardır[228]. Türkiye hakkında 2001 yılından itibaren ilerleme raporları hazırlanmaya başlamıştır. İlerleme raporlarının inceleme konusuna bakan yönüyle, kişisel verilerin korunması alanında mevzuat eksikliğimizin bulunduğu sonucuna varılarak, özellikle bu konu üzerinde durularak, bu eksikliğin giderilmesi tavsiye edilmektedir[229].

Ulusal programlar ise, AB'ne aday ülkelerin hazırladıkları ve Avrupa Birliği Komisyonuna sunularak, Katılım Ortaklığı Belgesinde yer alan ve öncelikle yerine getirilmesi istenilenlerin nasıl yapılacağına dair rapor mahiyetinde belgedir. Ulusal Programlarda genellikle, aday ülkelerin mevzuatlarında AB müktesebatı ile uyum sağlamak için yapacakları düzenlemeler, uyum sürecinde ihtiyaç hissedilen mali ve beşeri kaynaklar, AB müktesebatının yürütülebilmesi için uyumlulaştırılması lüzumlu yönetsel yapı ve sonuç olarak bütün bu konulara ilişkin kısa ve orta vadeli öncelikli yapılacak işler takvimi belirlenmektedir[230]. 2001, 2003 ve 2008 yıllarına ilişkin ulusal programlarda kişisel verilerin korunması konusunda yasal düzenlemeler yapılacağı taahhütü yer almaktadır[231]. Katılım Ortaklığı Belgesi ise; Avrupa Birliği Komisyonu tarafından hazırlanan ve Avrupa Birliği Konseyi tarafından kabul edilen, AB'ye aday ülkelerin, herbirinin AB'ye katılımının sağlanması yönünde kaydedeceği gelişmeler için öngörülen öncelikli alanların değerlendirildiği bir belgedir[232]. Bu belgede, Kopenhag Kriterlerine uyum sağlanması yükümlülükleri kapsamında, aday ülkelerin kısa ve orta vadeli önceliklerine ilişkin bir takvim de bulunmaktadır.

Şimdiye kadar 2001, 2003, 2006, 2008 ve 2014 yıllarında Katılım Ortaklığı Belgeleri kabul edilmiştir. Bunlardan 2001 tarihli Katılım Ortaklığı Belgesinde aday ülkeler için; veri koruma alanında AB müktesebatının, Schengen Bilgi Sistemi ve

---

[228] Raporlara ulaşmak için bkz; Avrupa Birliği Bakanlığı, "İlerleme Raporları" http://www.ab.gov.tr/index.php?p=46224 (Erişim: 20.05.2011)

[229] Raporlara ulaşmak için bkz; Avrupa Birliği Bakanlığı, "İlerleme Raporları" http://www.abgs.gov.tr /index.php?p=123&l=1 (Erişim:20.05.2011)

[230] Başbakanlık Dış Ticaret Müsteşarlığı Avrupa Birliği Genel Müdürlüğü, *Avrupa Birliği ve Türkiye*, Ankara: Doğuş Matbaacılık, 2002, s. 464.

[231] Avrupa Birliği Bakanlığı, "İlerleme Raporları", http://www.abgs.gov.tr/index.php?p=123&l=1 (Erişim:20.05.2011)

[232] Başbakanlık Dış Ticaret Müsteşarlığı Avrupa Birliği Genel Müdürlüğü, *Avrupa Birliği ve Türkiye,* s. 459.

Europol'a katılabilmek için benimsenmesi gerekliliği belirtmiştir[233]. 2003 tarihli Belgede; aday ülke mevzuatının kişisel verilerin korunmasına ilişkin birlik müktesebatına uyum sağlanmasından bahsedilmiştir[234]. 2006 tarihli Belgede; AB müktesebatı doğrultusunda, kişisel verilerin korunması alanında bir kanun kabul edilmesi ve bu kanundan doğan uygulamaları takip edebilecek bağımsız bir denetim mekanizması kurulmasının önemi vurgulanmıştır. 2008 tarihli Belgede; AB'nin kişisel verilerin korunması hakkındaki müktesebatı ile aday ülkenin bu konuda çıkarttığı ilgili mevzuatın uyumlaştırılması ve bağımsız bir veri koruma denetleme idaresinin kurulmasına yönelik çabaların artırılması tavsiyesinde bulunulmuştur[235].

Buna karşın Avrupa Komisyonu tarafından 1998 yılından 2014 yılına kadar her yıl "Düzenli İlerleme Raporları" hazırlanmıştır. Bu raporlardan özellikle 2014 tarihli olanında kişisel verilerin ihlaline dair çok endişe verici düzenlemelerin bulunduğu belirtilerek, kişisel verilerin korunmasına dair genel ve kapsamlı bir kanunun yürürlüğe girmesi ve hükümetlerden bağımsız bir veri koruma ve denetim biriminin kurulması gerekliliği üzerinde durulmuştur. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun'da yapılan değişikliklerin, Milli İstihbarat Teşkilatı (MİT) ve Telekomünikasyon İletişim Başkanlığının (TİB) yetkilerini istisnai biçimde genişlettiği, bu durumun, kişisel verilerin korunmasına ilişkin bir mevzuatın ve bağımsız bir denetleme organının olmaması ile birlikte, Türkiye'de kişisel verilerin yeterli düzeyde korunmadığı yönündeki endişeleri arttırdığını rapor etmiştir[236].

---

[233] Avrupa Birliği Bakanlığı, "2003 tarihli katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2003.pdf (Erişim:20.05.2011)

[234] Avrupa Birliği Bakanlığı, "2006 tarihli katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2006.pdf (Erişim:20.05.2011)

[235] Avrupa Birliği Bakanlığı, "2007 tarihli katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2007.pdf. (Erişim:20.05.2011)

[236] Avrupa Birliği Bakanlığı, "2014 tarihli katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/ilerlemeRaporlariTR/2014_ilerleme_raporu_tr.pdf. (Erişim: 29.11.2014)

1.2.2.3. Özel Hukuk

Şüphesiz, kişisel verilerin devlet veya gerçek ve özel hukuk tüzel kişileri tarafından kaydedilmesi ve işlenmesi doğrudan kişinin özel hayatına yapılan bir müdahale olduğu içindir ki, bu hak ve hürriyetlerden kişisel verilerin korunması alanını en çok ilgilendireni özel hayatın gizliliği hakkıdır[237]. Bu hak kişiliğe bağlı, dokunulmaz, devredilmez ve vazgeçilmez temel haklardandır. Bu nedenle, kişi kural olarak kişisel verilerini işleyen herkese karşı kişiliğinin korunmasını isteyebilecektir. Yine bu haktan kaynaklanan hangi kişisel verilerinin kim tarafından kimin için hangi amaçla elde edildiğini öğrenebilme yetkisine sahiptir. Sonuç olarak kişi hangi kişisel verilerinin kime veya kimlere iletileceğini kontrol edebilme hakkına da sahip olacaktır.

Kişisel verilerin korunmasına ilişkin özel hukukta doğrudan doğruya bir düzenleme bulunmamakla birlikte, bu konuda genel olarak "kişilik haklarının korunması" kavramına ilişkin genel düzenlemeler kapsamında bir korumanın sağlanabileceği söylenebilir. Özel hukukta kişilik hakkı genel anlamda Türk Medeni Kanununun 23, 24 ve 25. maddeleri ile Türk Borçlar Kanununun 58. maddesi çerçevesinde korunmaktadır. Özel bir hüküm öngörülmediği sürece, kişilik hakkının korunması genel olarak bu hükümlere tabi kılınacaktır[238]. Türkiye'de kişilik haklarına yönelik saldırıların önlenmesinde ve kişisel verilerin korunmasında Türk Medeni Kanunun ve Borçlar Kanununun hükümleri kanuni dayanak oluşturmaktadır. Ancak, genel hükümlerle kişisel verileri etkin bir şekilde korumak, bu alanın kendine özgü niteliği gereği yeterli olmamaktadır. "213 sayılı Vergi Usul Kanunu[239]", "4857 sayılı İş Kanunu[240]", "5490 Sayılı Nüfus Hizmetleri Kanunu[241]", "4982 sayılı Bilgi Edinme

---

[237] Üzeltürk, *Özel Hayatın Gizliliği Hakkı*, s.99 -100.

[238] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s.228

[239] Örnek: madde 148; "Kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek ve tüzel kişiler, Maliye Bakanlığının veya vergi incelemesi yapmaya yetkili olanların isteyecekleri bilgileri vermeye mecburdurlar. Bilgiler yazı veya sözle istenilir."

[240] Kanun bu düzenlemesi ile işverene, işçileri hakkında işçi-işveren ilişkisi nedeniyle sahip olduğu bilgileri dürüstlük kurallarına ve hukuka uygun olarak kullanma ile gizli kalmasında işçinin haklı yararı bulunan kişisel verileri açıklamama ödevi getirmiştir.

[241] 1. maddede Kanunun amacının "Kişinin doğumundan ölümüne kadar kişisel ve medeni durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukuki olayların belirlenip

Kanunu[242]", "5809 Sayılı Elektronik Haberleşme Kanunu[243]", "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[244]", "5070 sayılı Elektronik İmza Kanunu[245]", "Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik[246]", "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik[247]", "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve

---

saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamak" olduğu düzenlenmiştir

[242] Kanunun 2. maddesi düzenlemesine göre; "bilgi edinme, kurum ve kuruluşların kaydettikleri verilere kanunun belirlediği çerçevede ulaşma hakkı" olarak tanımlanabilir.

[243] Kanunun 12/2-d. maddesi işletmecilerin, kişisel verilerin gizliliğini sağlaması açık bir yükümlülük olarak hak ve yükümlülükleri arasında sayılmıştır. Yine aynı maddenin 2-g fıkrasında, işletmecilerden bir huhuka uygunluk nedeni olan kanun emrini yerine getirme kapsamında kanunlarla yetkili kılınan kurumlarca yasal dinleme ve iletişimin denetlenmesine teknik olanak sağlanmasını sağlamak bir yükümlülük olarak yer almıştır. Kanunun 55. maddesine göre, "Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz." Kanunun 56. maddesine göre ise, "Abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz, kendisine veya başkasına yarar sağlamak maksadıyla kullanılamaz."

[244]Kanunda, İnternet ortamında işlenen bazı suçlarla mücadele etmek temel amaç olarak gösterilmiştir. 5651 sayılı Kanunda ayrıca, "erişim sağlayıcı, yer sağlayıcı, içerik sağlayıcı, İnternet toplu kullanım sağlayıcı ve ticari amaçla İnternet toplu kullanım sağlayıcıları" düzenlenmiştir.

[245]Kanunun12. maddesi kişisel verilerin korunmasıyla ilgilidir. Buna göre "Elektronik sertifika hizmet sağlayıcısı; elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez. Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz. Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz."

[246]Yönetmelikte konuyla ilgili olarak; "fizik kimliğin tespiti için gerekli olan kayıt ve bilgilerin neler olduğu ve bunları almaya yetkili mercilerin kimler olduğu, verilerin imhası ve verilerin muhafazasına" ilişkin hükümler bulunmaktadır. Bu tür muayene ve incelemeler sonucu elde edilen bilgiler ve tespitler kişilerle ilgili olduğundan, kişisel verilerin korunması kapsamında değerlendirilmesi gerekir.

[247]Bu kanun, "Ceza Muhakemesi Kanununda da düzenlemesi bulunan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izleme tedbirlerine ilişkin talepte bulunulması, kararların alınması ve uygulanmasında uyulacak usul ve esasları" belirlemektir.

Bu konuda ayrıntılı bir çalışma için bkz. Yardımcı, Murat, *Türk Hukukunda İletişimin Denetlenmesi*, Seçkin Yayınevi, Ankara: 2009.

Gizliliğin Korunması Hakkında Yönetmelik[248]" gibi kanunlarda konuya ilişkin dolaylı da olsa düzenlemeler bulunmaktadır.

Kişisel verilerin en çok depolanabileceği ve bu konuda da suistimale açıklığı bakımından polis uygulamaları dikkat çekicidir. Bu konu ile ilgili düzenlemeler getiren "Polis Vazife ve Salahiyet Kanunu'nun" (PVSK) Ek 7. maddesi kişisel verilerden olan haberleşme hürriyetiyle doğrudan bağlantılı iletişimin tespiti konusunda önemli yetkiler içermektedir. Yine kanunda ki önemli düzenlemelerden biride parmak izi ve fotoğrafların kayda alınmasına ilişkin PVSK'nin 5. maddesidir. Maddeye göre, maddede düzenlemesi bulunan kişilerin alınan parmak izlerinin, sisteme kaydedilen bilgiler, kimlik tespiti gibi kişisel verilerin mahkemeler, hâkimlikler, cumhuriyet savcılıkları ve kolluk güçleri tarafından kullanılabilir olması veri toplayanın sorumluluğu çerçevesinde değerlendirilmelidir.

Son olarak, idare tarafından bilgi edinmenin hukuk çerçevesinde yürütülmesi için oluşturulan "Bilgi Edinme Değerlendirme Kurulu" hakkında bilgi vermek gerekir. Kurul kişisel verilerin elde edilmesiyle ilgili alanda faaliyet gösteren bir kurumdur. Kurulun; kamu görevlileri için düzenlenen özlük dosyaları, sicil raporları ve benzeri kişisel veri içeren bilgi ve belgelerin ilgilisi tarafından görülebileceğine dair çeşitli tarihlerde verdiği kararlar bulunmaktadır. Kurul kararlarının ortaya çıkarttığı en önemli sonuç; ilgilisinin kendisiyle ilgili bilgi ve belgelere erişim hakkının bilgi edinme hakkı kapsamında kaldığının belirlenmesi olmuştur[249].

---

[248]Yönetmelik; telekomünikasyon sektöründe, özel hayatın gizliliği ile kişisel verilerin korunmasına ilişkin temel hak ve yetkilerin etkin bir biçimde korunması amacına yönelik 2002/58 numaralı AB Direktifini esas alınarak hazırlanmıştır. Yönetmelikte ana hedef kullanıcıların telekomünikasyon hizmetlerinden yararlanırken gizlilik haklarına sahip olmaları ve bu hakkın korunmasıdır. Yönetmeliğin amacı ise, telekomünikasyon sektöründe kişisel bilgilerin kaydedilmesi, işlenmesi ve gizliliğinin korunmasının güvence altına alınması olarak belirlenmiştir. Yönetmeliğin hedef kitlesi ise, telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişilerdir. Bkz. Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 88

[249] Kaya, Cemil, *İdare Hukukunda Bilgi Edinme Hakkı*, Ankara: Seçkin Yayınevi, 2005, s. 106.

1.2.2.4. Ceza Hukuku

Bilişim alanında suçlar ülkemizde ilk olarak, 765 sayılı TCK'ye 1991 yılında yapılan eklemelerle yaptırım altına alınmıştır. Bu düzenlemeler yapılırken Fransız hukukunun bu konudaki düzenlemelerinden etkilenmiştir. Ancak 2005 yılında 765 sayılı yasayı mevzuatımızdan kaldırarak yürürlüğe giren 5237 sayılı yeni TCK'de bilişim alanında suçlar, ülkemizde olduğu kadar tüm dünyü hukukunda meydana gelen gelişmeler ve yaşanan olgular gözetilerek yeni bir anlayışla yeniden düzenlenmiştir[250]. Bilişim alanında suçlar başlığı altında, 243. maddede iki, 244. maddede üç ve nihayet 245. maddede üç suç tipi olmak üzere, aslında toplamda sekiz ayrı suç tipi, üç hüküm içerisinde yaptırıma bağlanmıştır. Kişisel verilerin korunması ile ilgili olarak 765 sayılı mülga TCK'de yeterli düzenleme bulunmamakta olduğundan, bu verilerin izinsiz olarak işlenmesi ve başkalarına açıklanması gibi eylemlerle ceza hukuku kapsamında yeterli mücadele olanağı bulunmamakta, bu konudaki uyuşmazlıklar genellikle tazminat davalarına konu olmakta iken[251], 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı TCK ile birlikte, özel hayatın korunmasına dair söz konusu eksiklikler büyük ölçüde giderilip, yaptırıma bağlanarak ceza davası açma olanağı getirilmiş ve böylelikle de gerek Anayasamızın 20-22. maddelerine, gerekse de konuya ilişkin uluslararası belgelere uyum sağlanmıştır[252].

5237 sayılı TCK'nin 132 ila 140. maddeleri "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölüm başlığında aşağıdaki maddelerde düzenlenmiştir:

Madde 132: Haberleşmenin gizliliğini ihlal,
Madde 133: Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması,
Madde 134: Özel hayatın gizliliğini ihlal,
Madde 135: Kişisel verilerin kaydedilmesi,

---

[250] Erdağ, Ali İhsan, "Bilişim Alananda Suçlar (Türk ve Alman Ceza Hukukunda)", *GÜHFD*, Cilt. 14, Sayı. 2, 2010, s. 300
[251] Ülkü, Muhammet Murat, "5237 Sayılı TCK. 132-140. maddelerinde Yer Alan Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", Ankara: Adalet Bakanlığı Yayınişleri Dairesi Başkanlığı, s.3. http://www.ceza-bb.adalet.gov.tr/makale/150.pdf, (Erişim: 05.10.2009)
[252] Küzeci, *Kişisel Verilerin Korunması*, s. 286 vd.

Madde 136: Verileri hukuka aykırı olarak verme veya ele geçirme,

Madde 137: Nitelikli haller,

Madde 138: Verileri yok etmeme,

Madde 139: Şikayet,

Madde 140: Tüzel kişiler hakkında güvenlik tedbiri uygulanması.

TCK'de doğrudan doğruya kişisel verilerin korunmasına yönelik hükümler 135 ile 140. maddeler arasında düzenlenmiştir. "Kişisel verilerin kaydedilmesi" başlıklı 135. madde gerekçesinde, çağımızda hastaneler, sigorta şirketleri, bankalar, mağazalar gibi çeşitli kurum ve kuruluşlar tarafından kişilerle ilgili kayıtların bilgisayar ortamında tutulduğu, bu bilgilerin kaydedilme gayeleri başka bir amaçla kullanılmasından veya yasal ya da yasal olmayan bir şekilde kayıt maliki haricinde bir kişinin ele geçirmek suretiyle hukuka aykırı bir şekilde faydalanmasından dolayı hakkında bilgi toplanan kişiler aleyhine büyük zararlar oluşabileceği, bu nedenle kişisel verilerin hukuka aykırı olarak kaydedilmesinin suç olarak tanımlandığı ve bu kapsamda "kişisel veri" kavramının da "gerçek kişiyle ilgili her türlü bilgi" olarak tanımlandığı görülmektedir[253]. Verilerin kaydedildiği yerin bilgisayar ortamı veya kağıt üzerinde olması arasında bir ayırım gözetilmediği, bu şekilde 108 sayılı Avrupa Konseyi Sözleşmesine uyum sağlandığı, kişinin rızasına bağlı olarak, kendisiyle ilgili bilgilerin kaydedilmesinin suç oluşturmayacağı, ancak belirlenebilir özellikteki kişisel verilerin kanuna uygun olarak kaydedilmesi ve buna bağlı olarak kamu kurumlarının sağladığı kamu hizmetinin gereklerine göre kişilerle ilgili bazı bilgiler ilgili kanun hükümlerine istinaden kaydedilmesinin suç teşkil etmeyeceğinden bahsedilmektedir[254].

TCK 135/2. fıkrada sayılan veriler arasında da bir ayrım yapmış, "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgileri" "mutlak dokunulmaz" veriler olarak kabul ederken; "ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri "nisbi dokunulmaz" veriler olarak kabul etmiştir. Diğer bir deyişle ilk grupta yer alan veriler hiçbir

[253] Özbek, Veli Özer, *TCK İzmir Şerhi,* Ankara: Seçkin Yayınevi, 2005, s. 946
[254] Ülkü, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", s.14

şekilde kaydedilemez (işlenemez) ve bunun mümkün kılan bir hukuk kuralı yaratılamaz. Buna karşılık ikinci grup verilerin kaydedilmesi mümkündür. Ancak bunun için mevzuattaki kurallarda yer alan koşullara uygun hareket edilmelidir. Belirtilen sonuca hükümde yer alan "hukuka aykırı olarak" ibaresinden ulaşılmaktadır[255]. İkinci fıkrada düzenlenen ve "Hassas" veya "özel nitelikli" olarak değerlendirilebilecek bu veriler birinci fıkradan ayrı olarak tek tek sayılmasına karşılık bunların kaydedilmesine yönelik ağırlaştırıcı bir hüküm getirilmemiş olması bir eksikliktir. Kanunun gerekçesinde; bu verilerden kişilerin ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kaydedilmesinin özellikle suçluluğun önlenmesi ve suçlularla mücadele ile suç ve suçluların tespitini sağlamak gayesiyle, sınırları belirlenmek şartıyla izin verilebileceği, bu durumun doğal sonucu olarak söz konusu suçun oluşmayacağı ifade edilmektedir. Ancak açıklanan konuda bir düzenleme bulunmadığından söz konusu madde ile sağlanmak istenilen amaca aykırı biçimde ihlallerin doğabileceği ihtimali gözden kaçırılmamalıdır[256].

Hemen belirtelim ki TCK'nin 135/2. maddesinin yazımına da eleştiriler yöneltilmiştir. Özbek, maddedeki " ... *bilgileri kişisel veri olarak kaydeden"* ibaresine yer verilmesinin sanki bu verilerin kişisel veri olmadığı gibi bir anlam ortaya koyduğunu, halbuki bu verilerin de kişisel veri olduğunu, hatta diğer verilere göre daha özel bir nitelik taşıdığı için daha ağır cezayı gerektiren suçun nitelikli halleri arasında sayılmasının daha doğru olacağını belirtmekte olduğuna dayandırmaktadır[257]. Nitekim hem "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" hem de "Kişisel Verilerin Korunması Kanunu Tasarısı" söz konusu verilere *özellikli veri* niteliği tanımıştır. Sözleşmenin 6. maddesine göre "*İç hukukta uygun güvenceler sağlanmadıkça, ırk menşeini, politik düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkumiyetleri, otomatik bilgi işlemine tabi tutulamazlar."* Yine

---

[255] Özbek, *TCK İzmir Şerhi,* s. 949
[256] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 94
[257] Özbek, *TCK İzmir Şerhi,* s. 949

Tasarının 7/1. maddesinde "*Kişilerin ırk, siyası düşünce, felsefi inanç, din, mezhep veya diğer inançları; dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkumiyetleri ile ilgili kişisel veriler işlenemez.*"[258] düzenlemesi getirilmiştir. Yukarıda açıklanan verilerin işlenmesinin özel hayatın ve aile hayatının gizliliğinin ihlalini önleyecek yeterli tedbirlerin alınması şartıyla belli koşullar altında imkan bulunduğu açıkça ifade etmiştir. Bu yönüyle TCK'nin 135 maddesine paralel bir düzenleme getiren Tasarının 50. maddesinin de gözden geçirilmesi gerekmektedir.

Kanunun 137. maddesine göre bu suçun, "kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi halinde verilecek ceza yarı oranında artırılacaktır. Buna göre, örneğin bir devlet memuru tarafından hakkında tahkikat yaptığı herhangi bir şahsın söz gelimi politik düşünceleri ya da felsefi inancına dair bilgileri hukuka aykırı biçimde tutulmuş ise burada ceza yarı oranında artırılacaktır[259]. Diğer taraftan, TCK'nin 140. maddesi uyarınca bu suçun işlenmesi durumunda, tüzel kişilere özgü olarak TCK'nin 60. maddesinde düzenlenen güvenlik tedbirlerine hükmolunacaktır. Bireyler hakkındaki kişisel verilerin hukuka uygun (örneğin bir kanun hükmü gereği, bir mahkeme kararı gereği ya da kişinin rızası ile) ya da hukuka aykırı olarak kayda alınmış olması 135. madde kapsamında değerlendirilecek iken, bu aşamadan sonra söz konusu verileri hukuka aykırı olarak başkasına veren ya da bunları hukuka aykırı olarak ele geçiren kimse 136. madde kapsamında cezalandırılacaktır[260].

Hukuka uygun olarak kaydedilmiş olan kişisel verilerin kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi, "Verileri yok etmeme" başlıklı 138. madde ile bağımsız bir suç olarak tanımlanmıştır. Örneğin Adli Sicil Kanunu'nun 12. maddesi, arşiv bilgilerinin ilgilinin ölümü üzerine ve her halde kaydın girildiği tarihten itibaren seksen yılın geçmesiyle tamamen silineceğini

---

[258] Avrupa Konseyi, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme", s.1
[259] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.95
[260] Ülkü, , "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", s.15

belirtmektedir. Eğer bu süre geçmesine rağmen kişinin adli sicil arşiv kaydı silinmemiş ise, silmekle görevli olan kişi bağımsız bir suç olarak düzenlenen 138. madde uyarınca cezalandırılacaktır. Yine bu suçun işlenmesi dolayısıyla da 140. madde hükmüne göre tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacaktır[261]. TCK'de kişisel veri tanımının yapılmamış ve kişisel verilerin korunmasına dair ayrıntılı düzenlemeye gidilmeyip sadece genel hüküm ve yaptırımlarla yetinilmiş olunması, bu konuya dair özel bir kanunun çıkarılması ihtiyacını daha da artırmaktadır. Bu amaçla hazırlanan Kişisel Verileri Koruma Kanun Tasarısı'nın en kısa zamanda kabul edilerek yürürlüğe sokulması, gerek hukukukumuzdaki kişisel hak ve özgürlüklerin güvence altına alınması ile ilgili boşluğun doldurulmasına yardımcı olacak, gerekse de başka ülkelerden aktarılması istenilen kişisel verilerin elde edilmesinde yaşanan zorlukların giderilmesinde önemli bir imkan sağlayacaktır.

1.2.2.5. Ceza Muhakemesi Kanunu

Ceza Muhakemesi Kanununun (CMK) 75 vd. maddelerinde kişisel verilerin işlenmesi düzenlenmiştir. Soy bağının tespiti veya suç mahallinde elde edilen delillerin, suç ile ilgili şüpheli veya sanığa ya da mağdura ait olup olmadığının araştırılması, zorunluluk halinde moleküler genetik incelemeler yapılması, şüpheli, sanık veya diğer kişilerin beden muayenesi ve vücudundan numune alınması, konuya ilişkin örnekler olarak gösterilebilir. Fiziki kimliğin tespitine yönelik olarak, şüpheli veya sanığın, kimliğinin teşhisine yönelik araştırmalarda, Cumhuriyet savcısının emriyle fotoğrafı, parmak ve avuç içi izi, beden ölçüleri, bedeninde bulunan ve teşhisine yardımcı olacak diğer özellikleri ile ses ve görüntülerin kaydedilmesine izin verilmektedir[262]. CMK'nin 75., 76. ve 78. madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonucu elde edilen bulgular CMK'nin 80. maddesi kapsamında kişisel veri niteliğinde olup, alınma amacı dışında başka bir amaçla

---

[261] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 98

[262] Öztürk, Bahri; Tezcan, Durmuş; Erdem, Mustafa Ruhan; Sırma, Özge; Saygılar, Yasemin F. ve Alan, Esra, *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, Ankara: Seçkin Yayınevi, 2010, s. 92 vd.

kullanılamaz, dosya içeriğini öğrenme yetkisi bulunanlarca açıklanamaz, yayınlanamaz ve bir başkasına verilemez[263].

CMK'nin 134 vd. maddelerinde ise; bilgisayar ortamında verilerin kopyalanması, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izlemeyle ilgili önlemler ve bu önlemlerin denetlenmesine ilişkin hükümler düzenlenmektedir. Buna göre; 134. maddede "*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma",* işlemlerine ilişkin düzenlemeler getirilmiştir. 135. maddeye göre ise; "*Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir*." Görüldüğü üzere, kişinin iletişimine müdahale edilebilmesinin tek yolu ancak yargı kararıyla mümkündür[264]. Yine 140. maddede sayılan belli suçların işlendiğine dair güçlü şüphe bulunması ve başka bir şekilde delil elde edilmesinin mümkün olmaması hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki eylemleri ile işyeri izlemeye uygun araçlarla izlenebilir, sesli ve görüntülü kaydı yapılabilir. Günümüzde, telekomünikasyon vasıtasıyla yapılan iletişimin son derece yaygınlaşması ve hayatın vazgeçilemez bir parçası haline gelmesi karşısında bu maddenin değerinin daha da arttığı söylenebilir.

1.2.2.6. Kişisel Verilerin Korunması Kanunu Tasarısı

Mevzuatımızdaki kişisel verilerin korunmasına yönelik doğrudan hükümler bulunmaması ve bu hükümlerin, doğrudan kişisel verilerin korunması amacına yönelik değil, ancak her bir hükmün ilgili olduğu alanda ve zamanının ihtiyaçlarına cevap vermesi amacı ile düzenlemiştir. Bu nedenle bu hükümler kişisel verilerin

---

[263] Hakeri, Hakan ve Ünver, Yener, *Ceza Muhakemesi Hukuku*, Ankara: Adalet Yayınevi, 2008, s. 131
[264] Özbek, Veli Özer; Kanbur, Mehmet Nihat; Doğan, Koray; Bacaksız, Pınar ve Tepe, İlker, *Ceza Muhakemesi Hukuku*, Ankara: Seçkin Yayınevi, 2008, s. 234 vd.

korunmasına özgü felsefeden yoksun bulunduğundan, konuya ilişkin artan ihtiyaca cevap verilmesi amacıyla, kişisel verilerin korunmasına yönelik bir kanunun hazırlanması düşünülmüştür. Zaten 108 sayılı Avrupa Konseyi Sözleşmesi ile 95/46 sayılı AB Direktifi de ülkelerin söz konusu metni iç hukuklarıyla uyumlaştırılması amacıyla Kişisel Verilerin Korunması Kanunu çıkarmaları gerektiğini vurgulamıştır[265]. Zira Türkiye'de söz konusu uluslarüstü metinlerle uyumlu bir kanunun bulunmaması, AB üyesi devletler ile ülkemiz arasındaki bilgi akışını da olumsuz yönde etkilemektedir[266]. Bu güne kadar 2005, 2008 ve 2014 tarihli üç tasarı yapılmıştır. Tasarıların hepside 108 sayılı Avrupa Konseyi Sözleşmesi ile 95/46 sayılı AB Direktifinden ve OECD'nin 23.09.1980 tarihli "Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafiğinin Korunmasına İlişkin Rehber İlkeler" ile ilgili uluslararası belgelerinden büyük ölçüde esinlenmiştir[267].

Kişisel Verilerin Korunması Hakkında Kanun Tasarısı; kişisel verilerin kanuna uygun ve dürüst bir şekilde kaydedilmesi ve işlenmesi, güncelleştirilmelerin önceden belirlenmiş ve meşru amaçlar için yapılması ve saklanması, saklama süresinin kullanım amacına uygun olması, verilerin toplanma amacına aykırı olarak paylaşılmaması, veri sahibinin kendisine ilişkin verileri öğrenme, değiştirme ve gerekirse yok etme haklarını düzenlemektedir[268]. Tasarının hazırlanmasındaki maksat, kişisel verilerin toplanması ve başkalarının kullanımına verilmesi değil, kişisel verilerin işlenmesinde, maddi ve manevi varlığı ile temel hak ve özgürlüklerinin korunması ve kişi dokunulmazlığının sağlanmasıdır. Kişisel verileri işleyen gerçek ve tüzel kişiler, bu bilgilerin toplanmasında tamamen serbest olmayıp diledikleri gibi bilgi toplayamayacaklar, kendileri veya üçüncü şahıslar lehine istedikleri zaman bu bilgileri kullanamayacak ve kullandıramayacaklardır. Tasarıda Kanunun amacı; "Kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen

---

[265] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 97

[266] Başalp, Nilgün ve Keser Berber, Leyla, "Kişisel Verilerin Korunması Projesi", http://www.bilgiedinmehakki.org/tr/index.php?option=comcontent&task=view&id=83&Itemid=24, (Erişim:16.02.2014)

[267] Üzeltürk, *Özel Hayatın Gizliliği Hakkı,* s.103.

[268] Kılınç, *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, s. 1156,

gerçek ve tüzel kişilerin uyacakları usul ve esasları düzenlemek" olarak ifade edilmiştir[269]. Böylelikle tasarı kişisel verilerin korunması hakkını insan hakları kavramının ayrılmaz bir ilkesi olarak hukuk sistemimize sokmaktadır[270]. Ancak Tasarı, sorunları çözecek net bir dil kullanmamış, muğlak ifadeler yoluyla kişi hak ve hürriyetine müdahale noktasında belirli ve kesin bir çizgi çizememiştir. Kişisel verilerin toplanması ile kullanılması ve kullandırılmasında sakınca doğuracak kadar serbesti tanımış, en önemlisi de amaçlananın kişi hak ve hürriyetlerinin korunması olduğu fikrini gözardı edip, somut koruyucu kurallar getirmemiştir.

Kişisel verilerin işlenmesine ilişkin tanımada yer veren tasarı, verilerin toplanmasından başlayarak tüm işlem türleri tanım kapsamı altına alınmıştır. Bu kapsamda kişisel verilerin bilgisayar vb. otomasyon sistemlerinin kullanıldığı yöntemlerle işlenmesi gibi otomatik sistemler kullanılmadan manuel olarak işlenmesi hali de kişisel verilerin işlenmesi kapsamında ele alınacaktır. 2005 tarihli tasarıdan farklı olarak 2008 ve 2014 tarihli tasarıda kişisel verinin bir kişiyle ilişkilendirilemeyecek hale getirilmesini tanımlayan "Anonim hale getirme" işlevine yer verilmiştir. Ayrıca yine tanımlar bölümünden Veri kütüğü sistemi, Veri kütüğü sistemi sahibi, Kurum, Başkanlık, Başkan, Sicil, İlgili Bakan tanımlarınada yer verilmeyerek bir önceki sistem terk edilerek yeni bir idari birim oluşturulması öngörülmüştür. Yeni tasarıda koruma kurulu yüksek kurul olmaktan çıkartılmış, sadece kurul olarak belirtilmiş, genel sekreterlik oluşturlmuş, veri kütüğü sisteminden vazgeçilmiş ve yerine veri sorumlusu sitemi getirilmiştir. Veri kayıt sisteminin bilişim alanı düşünülerek kurgulandığı anlaşılmaktadır.

Özel niteliği olan kişisel verilerin işlenmesi ise Tasarının 6. maddesinde sayma yöntemiyle belirlenmiş olup, "Kişilerin ırkı, etnik kökeni, siyasî düşüncesi, felsefî inancı, dini, mezhebi veya diğer inançları; dernek, vakıf ve sendika üyeliği, sağlığı veya cinsel hayatıyla ilgili verileri ilgili kişisel veriler" özel nitelikli kişisel veriler olarak tanımlanmış ve kural olarak bu verilerin işlenemeyeceği hüküm altına alınmıştır. Ancak bu fıkranın istisnası da hemen 2. fıkrada düzenlenmiş, yeterli

[269] Adalet Bakanlığı Kanunlar Genel Müdürlüğü, "Tasarılar", s.1
[270] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması,* s. 100

önlemlerin alınması şartıyla, istisnai hallerde bu verilerin işlenmesine cevaz verilmiştir. Tasarıda, kişisel verilerin korunmasından ziyade, toplanması ve sonrasında da istenildiğinde kamu otoritesi tarafından kullanılabilmesine imkan sağlama düşüncesinin baskın olduğu görülmektedir. Önemli olan, kişisel verilerin mümkün olduğu kadar elde edilmesinin, saklanmasının, bir yerde toplanmasının ve kullanıma açılmasının önüne geçmektir[271]. Oysa Tasarı, banka ve kredi kurumları, sigorta şirketleri, sağlık kuruluşları gibi çeşitli kişi, kurum ve kuruluşlar tarafından elde bulundurulmakta ve saklanmakta olan tüm kişisel verilerin Kanun uyarınca oluşturulacak bir kurul tarafından denetlenmesi, bu Kurula her türlü bilgiye erişim imkanı sağlanması, bu yolla temel hak ve özgürlüklerin sınırlandırılmasının önünü açmaktadır.

Tasarıda kişisel verinin aktarılmasını düzenleyen 8. madde 2008 tarihli tasarıya oranla konuyu daha ayrıntılı düzenleyerek daha güvenceli hale getirmiştir. Tasarının dikkat çeken bölümlerinden biride "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 9. maddesidir. Bu madde "Pasif Bilgi Edinme Hakkını" düzenlemiştir. Buna göre; veri sorumlusu, kişisel verilerin kaydedilmesi sürecinde ilgili kişilere; veri kütüğü sahibi ile varsa temsilcisinin kimliği, kişisel verilerin işlenme amacı, kişisel verilerin aktarılabileceği kişiler, veri toplamanın yöntemi, hukukî sebepleri ve muhtemel sonuçları, kişisel verileri öğrenme hakkı ile düzeltme hakkı konusunda bilgi vermekle yükümlüdür[272]. Pasif bilgi edinme hakkının muadili olarak Tasarının "İlgili kişinin hakları" başlıklı 10. maddesi ile "Aktif Bilgi Edinme Hakkı" düzenlemiştir. Düzenlemeye göre, herkes veri kütüğü sahibinden kendisiyle ilgili; işlenen bir kişisel veri olup olmadığını öğrenmek, işlenmişse buna ilişkin bilgi istemek, kişisel veriler noksan veya hatalı ise bunların düzeltilmesini istemek, hukuka aykırı bir kayıt yada işleme varsa yok edilmesini, bunların sonucunda yapılan işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini istemek hakkına sahiptirler. 2005 tarihli tasarının 11. maddesinde belirttiği istisnalar 2008 ve 2014 tarihli tasarılarda yer almamıştır. Buna göre; önceki tasarıdaki hukuka uygunluk

[271] Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, s.75
[272] Kılınç, *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, s. 1166

nedenleri, aydınlatma yükümlülüğü, veri kütüğü sicili, sicile kayıt ve ön inceleme konularıyla ilgili maddeler milli güvenlik, kamu düzeni, suçun önlenmesi, devletin ekonomik çıkarları için gerekli görülürse uygulanmayacaktı[273] yeni tasarıdan bu madde çıkartılarak kişisel verilerin yasal korumasını kaldıran sebeplerde tasarıdan çıkartılmış oldu.

Tasarının en sakıncalı maddesi ise "İstisnalar" başlığını taşıyan 24. maddesidir. Bu maddede sayılan hallerde kanun hükümlerinin uygulanmayacağı belirtilmiş ve sayma yöntemi kullanılarak istisna halleri gösterilmiştir. Maddenin 1. fıkrasının "ç" bendinde düzenlenen ve Polis, Jandarma ve Milli İstihbarat Teşkilatının istihbarat faaliyetlerine ilişkin veri toplamaları istisna gösterilmiştir. Günümüzde gelinen nokta itibarı ile bu kamu kuruluşlarına verilen yetkinin, yetkiyi kullanan kişilerce suiistimal edilerek kötüye kullanılabileceği düşünüldüğünde getirilen istisna oldukça sakıncalıdır. Yine Tasarının 24/1-d bendinde Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ile Terörizmin Finansmanın Önlenmesi Hakkında Kanun çerçevesinde yapılacak veri işlemelerin yasa kapsamı dışında bırakılması aynı endişelerle sakıncalıdır. Burada dikkat çeken en önemli husus bu meddeler kapsamında yapılacak veri işlemesinin yargı denetiminde olmadan yapılıyor olmasıdır. Fişleme sonucunu doğurabilecek bu açıkların tasarıya alınması, korunmak istenen hakkın özü ile uyuşmamamaktadır. Tasarının 24. maddesinin 2. fıkrasında düzenlenen istisna ise yasanın getirdiği güvenceleri tamamen ortadan kaldırmaktadır. Madde uyarınca, veri sorumlusunun aydınlatma yükümlülüğünü düenleyen 9. madde ile sicile kayıt yükümlülüğünü düzenleyen 15. maddelerinin hükümlerinin sayılan nedenlerle uygulanmayacağı düzenlenmiştir. Yukarıda sayılan gerekçelerle bu düzenlemede kendi içerisinde Tasarının ruhuyla uyuşmamaktadır.

Söz konusu tasarının yukarıda belirtilen sakıncaları giderildikten sonra bir an önce kanunlaştırılarak Türk hukuk sitemi içerisinde yerini alması, gerek ulusal gerekse de uluslararası veri akışını kolaylaştırmanın yanı sıra, özel hayatın

[273] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.127

gizliliğinin sağlanması açısından da bireylerin garanti altına alınmasını sağlayacaktır. Zira konuya ilişkin genel hükümler yetersiz kalmakta, kamu kurumları açısından özel kanunlardaki hükümler ile özel sektörün kendi kendilerine belirledikleri etik ilkeler kişisel verilerin korunmasıyla ilgili ülke çapında standart normların oluşturulmasında dağınıklık sergilemektedir[274].

1.2.2.7. Kişisel Verilerin Korunması Kanun Tasarısı'nda Yer Alan Cezai Tedbirler

Kişisel verilerin hukuka aykırı işlenmesi, silinmemesi ve açıklanması durumlarında fiilleri gerçekleştirenlerin cezai sorumlulukları söz konusu olur[275]. Bu tür fiillere karşı cezaî tedbirlerin uygulanmasına tasarının beşinci bölümünde 16 ve 17. maddelerde yer verilmiştir. 2005 ve 2008 tarihli düzenlemelerden tamamen farklı bir düzenleme getiren bu maddeler daha ayrıntılı olarak cezai tedbirleri hüküm altına almıştır. Yine bir diğer farklılık kişisel verilere ilişkin suçları kabahatler ve suçlar olarak ayırarak düzenlemesidir. Tasarının 16. maddesi suçlar ile ilgili hükümleri düzenlemiş ve burada TCK'de ki kişisel verilere ilişkin suçlara atıf yapılmıştır. Buna göre, *"Bu kanun hükümlerine aykırı olarak; kişisel verileri ele geçiren, kaydeden, bir başkasına veren veya yayanlar ya da yok etmeyenler 26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun ilgili hükümlerine göre cezalandırılır "* (m. 16/1). Tasarı TCK ile paralel bir düzenleme getirerek uygulamada yeknasaklığı sağlamak istemiştir. 16. maddenin 2. fıkrası 135. ve 136. maddelerindeki suçu işleyenler için getirilen ceza hükümlerine tabi kılınmıştır. TCK'nin 135. vd. maddelerinde düzenlenen suçların hukuki konusunu özel hayatın gizliliğinin ihlali oluşturmaktadır[276]. Görüleceği üzere TCK'nin 135. ve 136. maddeleri tasarının 16/2. maddesinde birleştirilerek kişisel verilerin hukuka aykırı kaydedilmesi, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, elde edilebilir hale getirilmesi, sınıflandırıması ya da kullanılmasının engellenmesi veya üçüncü kişilere aktarılması şeklinde düzenlenmiş ve sadece 135. madde de yazan cezayla

---

[274] Küzeci, *Kişisel Verilerin Korunması*, s.351

[275] Dinç, Engin, *Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu,* Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır, Dicle Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 75 vd.

[276] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s.207

cezalandırılacağı belirtilmiştir. TCK'nin 138. maddesinde düzenlenen kişisel verilerin silinmemesini ise tasarının 16/3. maddesi karşılamaktadır. Tüzel kişilere yönelik cezai tedbirler ise tasarıda 16/4. maddede yer alırken bu maddenin muadili TCK'nin 140. maddesinde kendisine yer bulmuştur. Kişisel Verileri Koruma Kanun Tasarısının TCK'nin 136. maddesine atıf yapan 34/3. maddesi ise tasarının 16/2. maddesinde erimiştir. 2005 tarihli Kişisel Verileri Koruma Kanun Tasarısının 34/4. maddesinde yer alan, *"Yukarıdaki fıkralarda belirtilen fiillerin Türk Ceza Kanununun 137. maddesinde belirtilen şekilde işlenmesi halinde ceza, aynı maddeye göre tayin edilir"* hükmü 2014 tarihli tasarıda yer almamıştır. Tasarı genel olarak TCK'ye atıf yaptığından TCK'nin ilgili 137. maddesinin zaten ihtiyacı karşılayabileceği düşünülebilir. TCK'nin 137. maddesinde ise *"yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenmesi hâlinde, verilecek ceza yarı oranında artırılır"* hükmü bulunmaktadır.

Tasarının 17. maddesinde düzenlenen kabahatler, 9, 11, 14 ve 15. maddelere atıf yaparak düzenlemiştir. Tasarının 9. maddesinde "Veri sorumlusunun aydınlatma yükümlülüğü", 11. maddede "Veri güvenliğine ilişkin yükümlülükler", 14. madde de kurula yapılan şikayetin incelenmesi usulü ve nihayet 15. madde de veri sorumluluarı siciline ilişkin düzenlemeler bulunmaktadır. Tasarının 17. maddesi uyarınca belirtilen maddelere aykırı davranılması kabahet olarak düzenlenmiş ve bu maddeleri ihlal eden fiiller para cezası ile cezalandırılmıştır. Burada 11. madde üzerinde durmakta yarar bulunmaktadı. Veri sorumlusu 3. maddede yapılan tanıma göre "Birim, kurum veya kuruluşlarda veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi" ifade etmektedir. Veri sorumlusu kavramına bazı yazarlarda "Veri Koruma Görevlisi" olarak rastlamaktayız. Kavramsal bu farklılığa rağmen sonuç itibarı ile verilerin düzenli tutulmasından ve korunmasında sorumlu olan kişiyi ifade etmektedir[277]. Kişisel

[277] Keser Berber, Leyla; Ülgü, Mahir M ve Er, Cüneyd, *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*, 1. Baskı, İstanbul: Karakter Color AŞ, 2009, s. 122

veriyi işleyenin hukuk dışı eylemi 16. madde uyarınca TCK'nin 135. maddesinde düzenlenen hapis cezasını gerektiriken, veri işleyenin fiilerinden sorumlu olan veri sorumlusunun para cezasını gereketiren 17. madde kapsamında değerlendirilmesi bir eksiklik gibi görünsede, burada düzenlemenin veri sorumlusunun veri işleyenin denetim ve gözetim görevinden kaynaklı sorumluluğuna yönelik olduğunu kabul etmek gerekir. Veri sorumlusunun, veri işleyenin hukuk dışı eylemine iştirak sayılabilecek fiilerini 17. madde değil, 16. madde kapsamında değerlendirmelidir.

Kabahatlere ilişkin 17. madde kapsamında kalan eylemlerle ilgili atıf yapılan maddelerde tüzel kişileri ilgilendiren bölümler bulunmasının doğal sonucu olarak 2. fıkra uyarınca kabahatlere ilişkin eylemlerden sadece gerçek kişileri değil, tüzel kişileride sorumlu tutmuştur. Kabahati oluşturan eylemi kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarında çalışanların işlenmesi halinde ilgil kurum çalışanlar hakkındaki disiplin hükümlerine göre işlem yapılacağı düzenlenmiştir. Bu maddedeki düzenleme TCK'nin 137. maddesinde düzenlenen ağırlaştırıcı sebep ile benzerlik göstermektedir.

1.3. 5237 SAYILI TÜRK CEZA KANUNUNDA KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN SUÇ TİPLERİ

Ceza hukukuna etkisi açısından bilişim sistemleri kullanılarak işlenen suçlar arasında, kişisel verilerin korunmasına ilişkin suçlar, bilişim teknolojilerindeki gelişmeye paralel biçimde en çok etkilenen suçlar olarak karşımıza çıkmaktadır. Bu nedenle her ne kadar ikinci bölümde incelenen suçlardan bağımsız bir gelişim göstermiş olmasına rağmen, bilişim sistemlerinin kullanımının ceza hukukuna etkisi bakımından kişisel verilerin korunması "Bilişim Alanında Suçlar" başlığı altında incelenen suçlar yanında ikinci ana konuyu oluşturmaktadır[278]. Kişisel verilerin korunmasının genel anlamda bilişim sistemlerinin kullanımının bir etkisi olarak özel hayatın gizliliğinin ihlali olarak ortaya çıkması, kişisel verilerin korunmasına ilişkin düzenlemelerin otomatik işlem olarak da adlandırılabilecek olan özellikle bilişim

[278] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları,* s. 191

sistemleri aracılığıyla işlenmesine odaklanmasına neden olmuştur[279]. TCK'de düzenlenen kişisel verilerin korunmasına yönelik hükümler eksik norm niteliğinde olup özellikle hukuka aykırılığın hangi hallerde oluştuğuna ilişkin olarak basvurulabilecek olan kişisel verilerin korunmasına ilişkin düzenlemenin yapılması gerekir[280]. Kişisel verilerin korunmasına ilişkin suçları, genel olarak, hukuka aykırı olarak kişisel verilerin bilişim sistemine yerleştirilmesi, bilişim sistemi aracılığıyla işlenmesi ya da kaldırılmamasının cezalandırılması şeklinde ortaya çıkmaktadır. TCK'de ise, bu hususlar suçun unsurları arasından genel olarak çıkartılmıştır.

Kişisel verilere ilişkin suçların anlaşılabilmesi bakımından kişisel verilerin işlenmesine dair ilkeler olarak da adlandırılan kişisel verilerin işlenmesine ilişkin usul ve esasların bilinmesi gereklidir[281]. Bunun için de öncelikle "*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*" Bölümünde Düzenlenen Suç Tiplerini incelemekte yarar bulunmaktadır. TCK'de hem özel hayatın gizliliği genel olarak, hem de özel hayatın gizliliğinin çeşitli yönleri ayrıntılı olarak düzenlenmiştir. Bunlar; "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde 132. vd. maddelerinde düzenlenmiştir. Kanunun 132. maddesinde "haberleşmenin gizliliğini ihlal", 133. maddesinde "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması", 134. maddesinde "özel hayatın gizliliğini ihlal", suçlarına yer verilmiştir[282]. Gerek doktrinde özel hayatın gizliliği kapsamında değerlendirilen ve gerekse Anayasanın 20. vd maddelerinde özel hayatın gizliliği kapsamında düzenlenen konut dokunulmazlığını ihlal suçu ise TCK'de "Hürriyete Karşı Suçlar" başlığını taşıyan yedinci bölümde, 116. maddede düzenlenmiştir. Düzenleme açısından, 765 sayılı TCK'nin özel hayatın gizliliğinin korunmasına ilişkin suçlara daha az yer verdiği görülmektedir[283].

---

[279] Başalp, *Kişisel verilerin Korunması ve Saklanması*, s. 32 – 33.
[280] Türkiye Bilişim Derneği, Kamu Bilişimi Platformu 2. Çalışma Grubu Nihai Raporu, *Kişisel Verilerin Korunması,* Ankara: TBD/Kamu-BDB/2008-CG2, 2008, s. 34
[281] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları,* s. 206
[282] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 91
[283] Danışman**,** Ahmet, *Ceza Hukuku Açısından Özel Hayatın Korunması***,** 1. Baskı, Konya, Selçuk Üniversitesi Yayınları, 1991, s.136

Kişisel verilere ilişkin düzenlemelerin bulunduğu TCK'nin 135 vd. maddelerindeki suçlar incelendiğinde, genel olarak kişisel verilerin işlenmesine ilişkin ilkeler olarak ifade edilen, hem ulusal hem de uluslararası düzenlemelerde çeşitli şekillerde yer verilen usul ve esasların esas alındığı görülmektedir. Aşağıda inceleneceği üzere, "veri işleyenin sorumluluk ve yükümlülükleri" başlığı altında değerlendirilen kişisel verilerin korunmasına ilişkin ilkelerin çeşitli görünümleri suç olarak düzenlenmiştir. Bu açıdan TCK'nin 135 vd. maddelerinde, dürüst ve hukuka uygun toplama ve işleme, amaçla bağlılık ilkeleri başlığı altında incelenen kişisel verilerin işlenmesine ilişkin usul ve esasların belirli yönleriyle konu edinildiği görülmektedir. Nitekim 135. maddede suçun maddi unsuru olarak kişisel verinin kaydedilmesi, 136. maddede düzenlenen suçun seçimlik hareketlerini oluşturan, kişisel verinin ele geçirilmesi, verinin başkasına verilmesi ve yayılması, dürüst ve hukuka uygun toplama ve işleme ayrıca amaçla bağlılık ilkesinin bir görünümü olarak karşımıza çıkmaktadır. 138. maddede düzenlenen verinin yok edilmemesi ise özellikle amaçla bağlılık ilkesi ile ilişkisi bulunmaktadır. 138. maddede düzenlenen verinin yok edilmemesi suçunda ise verilerin sistem içerisinde yok edilmesi hükmüne yer verilmiştir. Bu haliyle 138. maddede düzenlenen kişisel verilerin yok edilmesi bakımından suçun konusunun sistem içerisindeki veri olarak kabul edilmesi sonucunda bu suçun kapsamının daraltıldığını söylemek mümkündür[284]. Kişisel verilerin korunmasına ilişkin suçlar açısından 137. maddeye göre, kişisel verilerin korunmasına ilişkin 135 ve 136. maddelerde düzenlenen suçların *"kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle"* ve *"Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle"* işlenmesi halinde verilecek cezanın yarı oranında arttırılacağı öngörülmüştür[285].

[284] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 205
[285] age, s.203

1.3.1. Kişisel verilerin kaydedilmesi suçu (m.135)

TCK'nin 135. maddesi iki fıkra halinda düzenlenmiştir[286]. Genel bir ifade kullanılarak kişisel verilerin hukuka aykırı olarak kaydedilmesi eylemi maddenin 1. fıkrasıyla düzenlenmiştir. Aynı maddenin 2. fıkrasında ise her ne şekilde olursa olsun kişilerin siyasi, felsefi ve dini görüşlerinin, hukuka aykırı olarak da ırksal kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak kaydedilmesi suç olarak düzenlenmiştir[287]. Kişilerin rızaları dışında kişisel verilerinin bilişim sistemlerine kaydedilmesi aynı zamanda kişilik haklarına bir saldırı niteliği de taşır ve bu suç gelişen bilişim teknolojisiyle birlikte ülkemizde ve dünyada çok sık karşılaşılan bir fiil olarak karşımıza çıkmaktadır. Artık kamu ve özel kurumların tamamı kişisel veri işlemektedir. Özellikle sağlık kuruluşlarının hastalarıyla ilgili, banka ve diğer finansman şirketleri ile sigorta şirketlerinin müşterilerinin kredi kullanabilme imkanı ve ödeme güçleriyle ilgili, ticari şirketlerin ise pazarlama amaçlı faaliyetler ve reklamasyon için yukarıda sayılan kişisel verileri toplayıp kullanmaktadırlar. Bu suç tipinin ortaya çıkmasında bu gelişmeler sonucu bu tür bilgilerin ilgilisinin izninin alınmaksızın sanal ortama veri olarak aktarılmas etkili olmuştur. Bu düzenlemeler Türkiye'nin de onaylayarak taraf olduğu Avrupa Konseyi'nin hazırladığı belgelerden olan "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" ile paralellik sağlamış ve bu sözleşmedeki ilgili düzenlemeler iç hukukumuz açısından geçerlilik alanı bulmuştur[288].

Temel hak ve özgürlüklerin korunmasının önemi bir yana kamusal ve özel faaliyetlerin sürdürülebilmesi açısından kişisel verilere ihtiyaç vardır. Bu kapsamda kamu ve özel sektörde kişisel verilerin işlenmesine izin verilmesi kaçınılmaz

---

[286] **Madde 135: "**(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.
(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."

[287] Özel, *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, s.865; Değirmenci, *Bilişim Suçları*, s.156-157; Dülger, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", s.117

[288] Dülger, Murat Volkan, (2004), *Bilişim Suçları*, 1. Baskı, Ankara: Seçkin Yayınevi, s.267; Dülger, *Bilişim Suçları ve Yeni Türk Ceza Kanunu*, s.117

olmaktadır. Kişisel verilerin işlenmesine izin verildiğinde en doğal beklenti bu bilgileri işleyen ve saklayan kurumun, özellikle de devletin bu tür verilerin güvenliğini sağlaması yolundadır. Bununla birlikte internetin yaygınlaşması sayesinde kişilerle ilgili bilgilere erişimin çok kolaylaşması bu verilerin hukuka aykırı olarak yetkisiz ve çoğu durumda kötü niyetli kişilerin eline geçmesine neden olmuştur. İnternet yolu ile yapılan kişilik hakları ihlalleri arasında en geniş kapsamlı olanı, kişisel veriler bağlamında karşımıza çıkmaktadır. Esasen bankacılık başta olmak üzere pek çok alanda işlemleri hızlandırmak ve güvenilir kılmak amacıyla kişisel verilerin toplanması ve ilgililerin yararlanmasına sunulması bir zorunluluktur. Ancak bu zorunluluk bir başka zorunluluğu da beraberinde getirir ki, toplanan verilerin korunması, bu verilerden yararlanılarak kişilerin özel hayat alanına tecavüzün önlenmesi ve kişilik hakları ihlallerinin engellenmesini zorunlu kılar[289].

1.3.2. Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu (m.136) ve Nitelikli Haller (m.137)

Kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi eylemleri TCK'nin 136. maddesiyle[290] bağımsız bir suç tipi olarak düzenlenmektedir. Bu düzenlemeyle güdülen amaç çok sık karşılaşılan ve en çok işlenen kişisel veri suçu olan kimlik hırsızlığı eylemlerini yaptırım bağlamak amacıyla düzenlenmiştir. İnternet günümüzde kimlik bilgilerimiz de dahil kişisel verilerimizin depolandığı bir alan haline gelmiştir. Dolandırıcılık, hırsızlıktan başlayarak terör suçlarına kadar kimlik hırsızlığı yapılarak suç işlenebildiği düşünüldüğünde bu suç tipinin ceza yasamızda yer alması yerinde bir düzenleme olmuştur[291]. Bu suçun nitelikli halleri Kanunun 137. maddedesinde[292], düzenlenerek, suçun bir kamu görevlisi ya da meslek sahibinin konumlarından kaynaklanan

---

[289] Tiftikçi, Mehmet, "Özel Hukuk ve İnternet", http://inet-tr.org/inetconf/tammetin/hukuk.html (Erişim: 27.10.2010)

[290] **"Madde 136. -** (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır."

[291] Dülger, *Bilişim Suçları,* s.276; Dülger, *Bilişim Suçları ve Yeni Türk Ceza Kanunu,* s.115

[292] **"Madde 137 -** (1) Yukarıdaki maddelerde tanımlanan suçların;
a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,
b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,
İşlenmesi hâlinde, verilecek ceza yarı oranında artırılır."

avantajlardan yararlanarak bu suçu işlemeleri halini arttırıcı neden olarak görmüştür. Güven duygusuna bağlı olarak kişisel bilgilerin verildiği, kanunda belirtilen kişilerin daha ağır ceza ile cezalandırılması önleyicilik olarak olumlu bir düzenlemedir.

1.3.3. Verilerin Yok Edilmemesi Suçu (m.138)

Kişisel verilerin yok edilmeleri, kişisel verilerin korunması açısından en az kaydedilmesi ve depolanması kadar önem arzetmektedir. Kaydedilme amacı sona eren veya kanunen saklanması için öngörülen süre dolan kişisel verilerin kayıtlı oldukları yerden silinmesi vezifesi verilen görevlilerin bu görevlerini yerine getirmemeleri halinde uygulanacak yaptırımlar TCK'nin 138. maddesiyle[293] düzenlenmiştir[294]. Yasa koyucu bu suça ilişkin düzenlemeyle amaç olarak, kişisel verilerin her ne kadar hukuka uygun olarak kaydedilse dahi sürekli olarak kayıtlı kalmalarının, örneğin bilişim sistemi içerisinde bulunmasının ve böylece her zaman ulaşılabilir olmasının önüne geçilmesi hedeflenirken, aynı zamanda verileri sistemden silmeyerek bu konudaki görevlerini ihmal edenlere yaptırım öngörülmektedir. Verilerin yok edilmesi şüphesiz ki, kaydedilmesinde gösterilen titizlik kadar önem arz eder. Gerçekten de verilerin yok edilmesi hem birey hem de devlet için önemlidir. Özellkle demokratik görünümlü bir devlet yönünden vatandaşlarını sürekli gözetleyen bir nevi fişleyen bir devlet görüntüsü, diğer demokratik devletler nazarında demokratik, özgürlükçü ve çoğulcu bir devlet olarak görülmeyeceği gibi, böyle bir devletin vatandaşları da çağdaş ilkelere bağlı bir toplum haline gelemeyecektir. İlk kez 5237 sayılı TCK ile düzenlenen[295] söz konusu suç tipiyle bunun önüne geçilmek istenmektedir[296].

138. maddede düzenlenen verilerin yok edilmemesi suçu fail yönünden özellik gösterir. Bu suçun failleri sadece verileri yok etme yükümlülüğü olan kişiler

---

[293] **"Madde 138 -** (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir."

[294] Özel, Cevat, (Eylül 2001), "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İstanbul: İstanbul Barosu Dergisi, Cilt. 75, Sayı: 3, s.865; Değirmenci, *Bilişim Suçlar*, s.157; Dülger, *Bilişim Suçları ve Yeni Türk Ceza Kanunu*, s.118

[295] Dülger, *Bilişim Suçları ve Yeni Türk Ceza Kanunu*, s.117-118

[296] Dülger, *Bilişim Suçları*, s.281

olabilirler. Bu açıdan 138. madde düzenlenen verileri yok etmeme suçu mahsus suç olarak düzenlenmiştir. 138. madde düzenlenen suçun başka bir yönden farklılığı ise 135 ve 136. maddede yer alan suçların maddi unsurlarını oluşturan hareketlerin icrai bir nitelik taşımasına karşın 138. maddede ise ihmali bir hareketin esas alınmasıdır.

1.3.4. Kişisel Verilerin Korunması Hakkındaki Düzenlemelere İlişkin Ortak Bir Değerlendirme

Konu kapsamındaki bilişim alanındaki kişisel verilerin elde edilmesi yolu ile işlenen suçlar bakımından korunan hukuki değer temelinde veri olduğu için TCK'nin 135. ve 136. maddelerinin ortak değerlendirilmesi yerinde olacaktır. Her iki maddede düzenlenen suçun hukuki konusu kişisel verilerdir[297]. Kişisel verinin ne olduğu ya da bundan ne anlaşılması gerektiği konusunda düzenlemede bir açıklık bulunmamaktadır. Fakat bu bir kanun boşluğu değilidir[298]. Çünkü genel uygulama olarak kanun koyucu kazuistik kanun yapma yönteminden ayrılmak için bazen kanunda yer alan bazı terimlerin anlamını öğreti veya diğer düzenlemelere bırakır. Nitekim Ülkemizin de taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin" 2/a maddesi bu konuda düzenleme yapmıştır. Buna göre kişisel nitelikteki veriler, kimliği belirtilen veya belirlenebilen gerçek kişiyle ilgili tüm bilgileri ifade eder[299]. Kişisel Verilerin Korunması Kanunu Tasarısı da benzer bir tanım getirmiştir (m.3). Ceza Muhakemeleri Kanununun (CMK) özellikle yeni hükümleri kişisel veri konusunda zengindir. Örneğin CMK 81/1. maddeye göre kaydedilen ''kişinin fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri", 78-80. maddeye göre "moleküler genetik inceleme sonucu", 75-76. maddeye göre "beden muayenesi ve/veya vücuttan örnek alınması suretiyle elde edilen" veriler ve 135. maddeye göre kayda alınan

---

[297] Parlar, Ali ve Hatipoğlu, Muzaffer, *Türk Ceza Kanunu Yorumu*, Seçkin Yayınevi, Ankara: 2010, s. 1036

[298] Özbek, Veli Özer; Kanbur, Mehmet Nihat; Doğan, Koray; Bacaksız, Pınar ve Tepe, İlker, *Türk Ceza Hukuku Genel Hükümler*, Ankara: Seçkin Yayınevi, 2010, s. 517

[299] Kesmez, "Kişisel Verilerin Korunması Üzerine", s. 2

"telekomünikasyon yoluyla iletişimi" gibi maddelerde kişisel veriler ile ilgili düzenlemeler bulunmaktadır[300].

Bu konuda getirilebilecek eleştirilerden biride, TCK'nin 135/2. maddesindeki "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır" şeklindeki düzenlemedir. Zira bu hüküm söz konusu "...bilgileri kişisel veri olarak kaydeden" ibaresine yer vermek suretiyle sanki bu verilerin kişisel veri olmadığı gibi bir anlam ortaya koymaktadır. Halbuki yukarıda yer alan tanımdan da anlaşılacağı üzere bu veriler de kişisel veridir. Hatta diğer verilere göre daha özel bir nitelik taşıdığı için daha ağır cezayı gerektiren suçun nitelikli halleri arasında sayılması daha doğrudur[301]. Nitekim hem "Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" hem de "Kişisel Verilerin Korunması Kanun Tasarısı" söz konusu verilere özellikli veri niteliği tanımıştır. Sözleşmenin 6. maddesi "İç hukukta uygun güvenceler sağlanmadıkça, ırk menşeini, politik düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkumiyetleri, otomatik bilgi işlemine tâbi tutulamazlar." düzenlemesi getirerek söz konusu verilerin işlenmesinin özel hayatın ve aile hayatının gizliliğinin korunmasını sağlayacak yeterli önlemlerin alınması şartıyla belli koşullar altında mümkün olabileceğini açıkça ifade etmiştir.

Düzenlemede ortaya çıkan bir diğer özellik ise TCK'nin 135/2 fıkrada sayılan veriler hakkında da bir ayırım yapılmış olmasıdır. Düzenleme "*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine*" ilişkin bilgileri mutlak dokunulmaz veri kabul ederken, "*ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına*" ilişkin bilgileri nisbi dokunulmaz veriler olarak kabul etmiştir. Diğer bir deyişle ilk gurupta yer alan veriler hiçbir şekilde kaydedilemez ve

---

[300] Öztürk ve diğerleri, *Ceza Muhakemesi Hukuku,* s. 132
[301] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 517

bunu mümkün kılan bir hukuk kuralı yaratılamaz. Buna karşılık ikinci gurup verilerin kaydedilmesi mümkündür. Ancak bunun için mevzuattaki kurallarda yer alan koşullara uygun hareket edilmelidir. Hükümde yer alan ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına düzenlemesinin hukuka aykırı olarak ibaresinden sonra gelmesinden anlaşılmaktadır[302]. Bu düzenlemenin bir özelliği de sadece gerçek kişilere ait kişisel verileri koruma altına almasıdır. Bazı bilgiler veri niteliğinde olmakla birlikte kişisel olmaktan çok kurumsal olabilir. Örneğin, anonim şirketin ticari sırları gibi veriler TCK'nin 239. maddesinde düzenlediği için bu verilere karşı işlenen suçlar TCK 135. maddenin kapsamında olmaz[303].

1.3.5. Bilişim Sistemleri Aracılığıyla Kişisel Veriler Aleyhine İşlenebilecek Suçlara Örnekler

Bilgisayar, internet, akıllı telefonlar, androit yazılımlı tablet bilgisayarlar ve uydu teknolojisi sayesinde artık yapılabilecekler yalnızca insanların hayalleri ile sınırlı bir hal almıştır. Bu güne kadar suç kabul edilmediği için bu eylemleri yapanların suçlu kabul edildiği binlerce insan, artık bilişim teknolojilerindeki gelişmeler nedeniyle bilerek ya da bilmeyerek suç işler hale gelmiştir, çünkü hayatı kolaylaştıran teknoloji suç işlemeyi de kolaylaştırmaktadır. Aşağıdaki örnekler henüz bilişim suçlarının basit sayılabilecek adımlarıdır. Bilişim sistemleri kullanılarak neler yapabileceğine verilecek örnekler ile konunun anlaşılabilirliğini sağlamak daha anlamlı olacaktır.

Bilgisayar teknolojileri sayesinde bir hastanenin bilgisayarlarına giren teröristler çok kullanılan birkaç ilacın dozajını insan yaşamına son verecek veya ciddi rahatsız edecek şekilde değiştirebilirler veya cinayet işlenebilir. Bilişim uzmanı James Clay'in anlattığına göre ABD'nin Kaliforniya eyaletinde bilgisayarla bir cinayet işlenmiş. Kurban, bir hastanede tedavi gören bir hastadır. Katil, bilgisayar yoluyla hastanenin sistemine girmiş ve kurbana verilen ilaçların listesini saptayıp,

---

[302] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 94
[303] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 517

listeyi değiştirerek kurbanı öldürecek ilaçları ve dozajları sisteme kaydetmiş, sonuçta hasta ölmüş ve cinayeti işleyenden ortada ne bir isim ne de bir iz kalmıştır[304].

ABD'nin Scotland Yard şehrinde bir hacker yetkisiz olarak telefon ağına girip 620.000 sterlin değerinde uluslararası telefon görüşmesi yapmıştır[305]. Siber saldırılar sonucu devletlerin ekonomik bütünlüğüne verilen zararlar hayal sınırlarını zorlayacak boyuttadır. Aynı şekilde Türk Telekom'a ait internet sitesine yapılacak bir saldırı ile tüm telefon faturaları üzerinde değişiklik yapabilir. Yine telefon veya internet abonelerinin ücretlerini azaltabileceği gibi artırabilir veya ödenmemiş borçları ödendi şeklinde gösterebilir. Nihayet olarak fatura bilgileride kişisel veri niteliğinde olduğu için kişilerin mali durumları bundan etkilenecek ve dahası böyle bir saldırıya maruz kalan bir devlet kurumunun içine düşeceği karmaşanın yarattığı toplumsal huzursuzluk sonuçları itibarı ile ciddi boyutlarda olacaktır.

Dijital teknolojideki gelişmeler kalpazanlık, dolandırıcılık ve sahtecilik gibi konularda da organize suç örgütlerine kolaylıkar sunmaktadır. Sahte kimlik, para, pasaport vb. belge düzenleme artık çok kolaylaştığı gibi kaliteside artmıştır. Kişisel bilgilerin sanal ortamda yoğun bir şekilde dolaşımda olduğu bir dönemde olduğumuzdan hiç haberiniz olmadan kişisel bilgileriniz kullanılarak suç işlenmesi her an olasıdır. Bu konuda dünyadan verilebilecek somut örnekler bulunmaktadır. 18 yaşındaki Maxus takma adını kullanan bir hacker, Amerikda online müzik hizmeti sunan bir şirket olan *CD Universe*'nin internet sitesine abone olan üç yüz bin kişinin kredi kartının numaraları kopyalanmış ve bu şirketten bu numaraları açıklamama karşılığında yüz bin Amerikan Doları haraç istemişlerdir. Şirket bu bedeli ödemeyi kabul etmeyince Maxus kurduğu internette bu kart bilgilerini yayınlamıştır. Bu durumdan haberi olan kartların sahipleri kredi kartlarını iptal etmişler veya *CD Universe*'den yaptıkları alışverişlere ait hesap özetlerini kontrol etmişlerdir. Ancak bu kredi kartlarının bazıları ile internet üzerinden başka alışverişler yapıldığı

---

[304] Güngör, Zehra, "Türk Şirketlerin Bilgisayar Güvenlik Planları Yok", Milliyet, http://www.milliyet.com.tr/1997/06/16/ekonomi/turkfir.html. (Erişim:08.05.2014)

[305] Özcan Mehmet, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu", http://adlibilirkisi.org/index.php?sayfa=makaleoku&kategori=5&id=18 (Erişim: 12.11.2014) s. 1

açıklanmıştır. Çeşitli güvenlik birimleri, suçluların peşine düşmüş ama önemli bir başarı elde edememiştir[306].

Aşağıdaki örnek her gün onlarca kez yaşanan bilişim suçlarının mali boyutlarının ulaşabileceği seviyeler konusunda yeterli olacaktır: Amerika'da, federal kanunlarına göre, kredi kartı kullanan tüketicilerin, sadece kendi hesapları üzerinde yapılan hileli alışverişlerin ilk 50 doları için kredi kartı sağlayan kurum sorumludur ve birçok kredi kartı şirketleri bu miktarı bile güvence altına almamaktadır. Yine, Federal Ticaret Komisyonu'na göre banka kartı alımları otomatik dolandırıcılığı koruma almadığı için kimlik hırsızlığı kurbanları genellikle, kredi derecelendirmeleri düştüğü için bunun telafisi için harcanan miktarın 1.000 dolardan fazla olduğunu bildirmektedir. Danışmanlık firması Boston Celent Communications'a göre 2000 yılında kimlik hırsızlığının finansal kurumlara doğrudan zararlarının maliyeti 2.4 milyar doları bulmakta[307] iken İntel Security firmasının yaptığı araştırmaya göre günümüzde siber suçların küresel düzeydeki maliyetinin 445 milyar doları bulduğu rapor edilmektedir[308].

Sanal alemin sunduğu kolaylıklardan yararlanılarak, özellikle telif hakları sahipleri büyük mali kayıplara uğratılmaktadır. Teknolojideki gelişmeler telif hakkının konusu oluşturan her türlü materyalin izinsiz olarak çoğaltılabilmesine ve izinsiz dolaşımına imkan tanımaktadır. Bu şekilde her geen yıl telif hakkı ihlal edilen eserlerin sahiplerin sadece youtube'de yayınlanan eserlerinden dolayı yaklaşık 36 milyon dolar mali kayıpları olduğu tahmin edilmektedir[309]. Daha ileri giden bir uygulama olarak bilgisayar ve internet konusunda uzman olan bir kısım suçlular yine interneti kullanarak bazı firmaların bilgisayar sistemlerini çökertmekle tehdit ederek haraç toplamaktadırlar. Bu tür bir tehdite maruz kalan firmalar karşı karşıya

---

[306] NTVMSNBC, "2000 Hacker'lerin Yılı Oldu", http://arsiv.ntvmsnbc.com/news/51092.asp, (Erişim: 08.05.2014)

[307] Hansen, Brian, "Cyber Crime, Should penalties be tougher?" *Kean University*, http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2002041200&type=query&num=cyber+crime&#.UtlbJ9JRbIU, (Erişim: 23.01.2014)

[308] Son Dakika, "Siber Suçların Maliyeti 445 Milyar Dolar", *Haberler*, http://www.sondakika.com/haber/haber-siber-suclarin-maliyeti-445-milyar-dolar-7001053/, (Erişim: 07.06.2015)

[309] Aktif Haber, "Muzik Videoları Youtube'dan Kaldırılıyor", http://www.aktifhaber.com/muzik-videolari-youtubedan-kaldiriliyor-923286h.htm (Erişim:26.03.2014)

kaldıkları tehdidin büyüklüğü karşısında bazen haraç ödemek zorunda kalmaktadırlar. Örneğin 1993-1995 yılları arasından İngiltere ve ABD'de bu gruplara haraç olarak 42,5 milyon sterlin ödendiği çeşitli medya organlarında yer almıştır[310].

Amerikada California State Üniversitesinde San Marcos Öğrenci Konseyi başkanlığı seçimlerine katılan 22 yaşındki Matthev Weaver isimli kişi okul öğrencilerinden 750 kişinin kimlik bilgilerini key logger denilen cihazı kullanarak çaldığı ve bunları oy kullanmak için kullandığı ortaya çıktı. Mart 2012 seçimleriyle ilgili olarak ağ yöneticileri kampüste tek bir bilgisayar ile bağlantılı olağandışı oylama etkinliğini fark ettiler ve son saatte usulsüzlüğü yakaladılar. Bir polis memuru Weaver'ın bilgisayarını araştırmak için gönderildi ve onun çalıntı kimlikleri kullanarak kendisi için 600'den fazla oy kullandığı anlaşıldı. Eğer Weaver başarılı olsa idi 300.000 dolarlık bir bütçeyi yönetecekti[311].

Konumuz ile ilgili olarak Türkiye'de de bu konuda verilebilecek somut örnekler bulunmaktadır. Adapazarı'nda 600 öğrencinin eğitim gördüğü bir lisede, son iki yıldır ilk beşe giren 17 yaşındaki T.A.E.'nin, okul müdür yardımcısı olan babasının e-okul şifresi ile okul kayıtlarına girerek notlarında düzeltme yaptığı, kendi notunu yükseltirken, 300'e yakın öğrencinin notlarını ise düşürdüğü ortaya çıktı. Milli Eğitim Bakanlığı'nın ihbar hattı 147'ye gelen ihbar üzerine soruşturma başlatan İl Milli Eğitim Müdürlüğü müfettişlerinin araştırmasıyla ortaya çıkan skandalın ardından liseli genç başka okula gönderildi[312].

Milli Eğitim Bakanlığı'nın MEBSİS kapsamında uygulamaya koyduğu ve eğitim alanındaki birçok hizmetin sanal ortama taşınmasını sağlayan İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi'ndeki (İLSİS) tüm verilerin; ünlü paylaşım sitesi Rapidshare'de paylaşıma açıldığı ortaya çıktı. SQL veritabanında yayımlanan verilerde, 687 bin öğretmenin TC kimlik numaraları, isimleri, çalıştıkları

---

[310] Özcan "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu", s. 1

[311] Federal Bureau of İnvestigation, "Election Hack, Stealing Votes the Cyber Way", https://www.fbi.gov/news/stories/2013/august/election-hack-stealing-votes-the-cyber-way/election-hack-stealing-votes-the-cyber-way, (Erişim:15.01.2014), s.1

[312] Mynet, "Lisede Şifre Skandalı, 300 Ögrenci Mağdur", http://www.mynet.com/haber/guncel/lisede-sifre-skandali-300-ogrenci-magdur-653206-1, (Erişim: 11.02.2014)

okullar gibi sadece il ve ilçe milli eğitim müdürlüklerinde yer alması gereken bilgiler yer aldığı tespit edildi[313].

En ilgi çekici kişisel veri hırsızlığı ise üçü kadın onbeş kişinin gözaltına alınması ile sonuçlanan ve tüm Türk vatandaşlarını kapsayacak şekilde yapılan veri hırsızlığıydı. 70 milyon Türk vatandaşına ait adres, telefon ve kimlik bilgilerini çalan çetenin bu bilgileri hukuk bürolarına paket programlar halinde sattığı belirlendi. Paketler arasında Telefon Sorgu Programı, Plaka Sorgu Programı gibi başlıklar var. Çete bu bilgileri resmi kurumların wep sitelerinden çalıp, paket program haline getirdikten sonra yaklaşık 1.500,00 – 2.000,00 TL karşılığı özellikle avukatlık bürolarına satıyor, avukatlık bürolarıda bunları icra takibi gibi işler için kullanıyordu. Tahminen 1500 hukuk bürosuna satılan bu verilerin kullanılmasıyla hukuk dışı bir işlemin yine hukuk için kullanılması gibi bir durum ortaya çıkması oldukça ilgi çekicidir[314].

Mali sonuçları açısından en vahim kişisel veri hırsızlıklarından biri Ankara'da ortaya çıktı. Medyaya yansıyan kadarıyla Ankara'daki 1 milyon 568 bin kişiye ait tapu bilgilerinin çalındığı tespit edildi. Tapu verilerini ele geçirenlerin, bu bilgileri ise 500,00 lira karşılığında sattığı belirlendi. Tapu bilgilerinin başta emlakçılar ile bazı banka, kredi kuruluşlarına satıldığı öğrenildi[315]. Yukarıda bahsedilen olaylar, medyaya yansıyan binlerce olaydan (çok büyük bölümü yansımıyor) neler yapılabildiğine ilişkin fikir vermesi açısından seçtiğimiz çok küçük bir kısmıdır.

---

[313] Hürriyet, "687 Bin Öğretmenin Kimlik Numaraları Çalındı" http://www.hurriyet.com.tr/gundem /10988928.asp, (Erişim: 11.02.2014)

[314] Türk Hukuk Sitesi, "70 Milyon Kişinin Kimlik Bilgileri Çalındı", http://www.turkhukuksitesi. com/showthread.php?t=52705, (Erişim: 11.02.2014)

[315] Hürriyet, "Ankara'da Vatandaşların Tapu Bilgileri Çalındı", http://www.hurriyet.com.tr/gundem/ 27662013.asp, (Erişim: 30.11.2014)

1.4. 5237 SAYILI TÜRK CEZA KANUNUNDA BİLİŞİM SUÇLARINA İLİŞKİN SUÇ TİPLERİ

Yukarıda TCK'deki kişisel verileri düzenleyen maddeler üzerinde durulmuştu. Fakat kişisel verileri düzenleyen maddeler sadece bilişim ortamında bulunmazlar, fizik ortamda kayıt altına alınan kişisel verilerde bulunmaktadır. Ancak araştırma konusu bilişim sistemi içerisinde kayıtlı olan kişisel veriler olduğu için ceza kanununda düzenlenen ilgili bilişim suçlarına yönelik düzenlemelerinde incelenmesi gerekecektir. Çünkü kişisel verilerin bilişim sistemine kaydedilmesi, işlenmesi, saklanması, kullanılması ve silinmesine ilişkin hareketlerin bilişim vasıtaları ile yapılması gerekecektir. Buda ilk eylemin bilişim alanında gerçekleşmesi dolayısıyla bilişim suçlarının da incelenmesini zorunlu hale getirmektedir. Ceza kanunumuz bilişim ile ilgili suçları üçüncü kısımda düzenlenen "Topluma karşı suçlar" içerisinde onuncu bölüm altında dört madde halinde düzenlemiştir. Aşağıda tek tek incelenecek olan maddelerden ilki 243. madde, "Bilişim Sistemine Girme", diğeri 244. madde; "Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirmeyi" düzenlemektedir. İnceleme konusu bilişim siteminde kayıtlı veriler ile sınırlandırıldığı için fizik meteryallerin bulunmasını zorunlu kılan yani banka ve kredi kartları ile bilişim siteminin kullanılarak işlenen suçları düzenleyen 245. madde inceleme konusu yapılması kapsamı aşacağı için burada incelenmeyecektir. Kaldı ki zaten 244. maddenin 2. fıkrasında bilişim suçunun banka veya kredi kurumuna karşı işlenmesi hali düzenlenerek inceleme konusunu bu yönden açık bırakmamaktadır. İlgili bölümde en son düzenleme maddesi olan tüzel kişiler hakkında güvenlik tedbirlerinin uygulanması ise ilgili olduğu bölümlerde incelenecektir. Esas olarak 243. madde kişisel verilere erişmeksizin bilişim sistemine müdahaleyi düzenlediği için asıl incelenecek madde 244. madde olacaktır.

1.4.1. Hukuka Aykırı Olarak bilişim Sistemine Girme veya Sistemde Kalma Suçu (m.243)

TCK'nin bilişim suçlarına ilişkin olarak ayırdığı bölümün ilk düzenlemesi karşımıza 243. maddede[316] "hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu" olarak çıkmaktadır. TCK'de bu madde "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme veya orada kalmaya devam etme" şeklinde düzenlenerek bilişim sistemine girme eylemini suç haline getirmiştir[317]. Avrupa Siber Suç Sözleşmesinin 2. maddesinde düzenlenen "hukuka aykırı erişim" suçu ile 243. maddede düzenlenen suç tipi arasında paralellik bulunmaktadır[318]. Bu maddede düzenlenen suç tipiyle, verilere yönelik bir suç işlenmeksizin, sadece bilişim sistemine ve dolayısı ile de verilere yetkisiz erişim fiileri suç tipi haline getirilmiştir[319]. Diğer bir deyişle bu suç tipinde cezalandırma için, bilişim sistemine girilmesi yeterli olmakta verilerin ele geçirilmesi, bozulması veya yok edilmesi şartı aranmamakta, kısacası bilişim sisteminin güvenliğinin ihlal edilmesi suç tipi haline gelmektedir[320]. Bu suç düzenlemesi ile özellikle bilişim suçlularının eylemlerinin önlenmesine yönelik bir tür önleyici tedbir mahiyetinde norm getirilmiş olup, yerinde bir düzenlemedir[321]. Bunun inceleme konusu suç açısından önemi verileri ele geçirmeye gerek olmadan bilişim sistemine yapılacak bir müdahale ile kişisel verilerin kullanılmasının önlenerek bir zarar veya menfaat elde edilmeye çalışılması halidir.

---

[316] "**Madde 243**; (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.
(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.
(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."

[317] Dülger, *Bilişim Suçları* 2004, s.212

[318] Yazıcıoğlu, *Bilgisayar Suçları*, s.177; *Dülger, Bilişim Suçları ve Yeni Türk Ceza Kanunu*, s.115

[319] Dülger, *Bilişim Suçları*, s.213.

[320] Akbulut, Berrin Bozdoğan, *Türk Ceza Hukukunda Bilişim Suçları*, Yayımlanmamış Doktora Tezi, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 1999, s.78; Değirmenci *Bilişim Suçları*, s.153; Yazıcıoğlu, *Bilgisayar Suçları*, s.177; Dülger, *Bilişim Suçları*, s.115

[321] Dülger, Murat Volkan, "Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi", Türk Ceza Kanunu Tasarısı, İstanbul Barosu- Türk Ceza Hukuku Derneği Toplantısı, 10.09.2004, Kurumsal Raporlar-Toplantılara Sunulan Raporlar-Bilimsel Raporlar, İstanbul: İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayını, 2004, s.111; Dülger, *Bilişim Suçları*, s.115

Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve orada kalmaya devam etme fiili TCK'de ilk kez düzenlenen bir suç tipidir. TCK'de verilerin ele geçirilmesi hatta elde edilen verilerin kullanılmaları ile ilgili doğrudan düzenleme bulunmadığı için bazı durumlarda bu eylemler yaptırımsız kalmaktadır. Bununla beraber, ele geçirilen veriler kişisel nitelikte ise, kişisel verilerin hukuka aykırı olarak ele geçirilmesini yaptırım altına alan aynı Kanunun 136. maddesi, veriler sistemden kaldırılarak ele geçirilecek olursa, bu defa 244/2. maddesi gündeme gelebilecektir[322].

Hukuka aykırı olarak bilişim sistemine girme suçu önleyeci tedbir mahiyetinde bir düzenlemedir. Çünkü bilişim suçları ancak bilişim sistemine girilmek suretiyle mümkündür. Bilişim sistemlerine hukuka aykırı olarak girme, sonrasında sistem ve verilerin güvenliğine, gizliliğine, bütünlüğüne yönelik eylemleri beraberinde getirmektedir[323]. Sisteme girme ve orada kalmaya devam etmenin yöntemi ve amacı önemli değildir. Madde gerekçesinde bu husus "hukuka aykırı olarak sisteme girilmesi ve orada kalmaya devam edilmesi fiillerinin doğal, haksız ve kasten gerçekleştirilmiş olması yeterlidir" denilerek açıklanmıştır[324]. Bütününe veya bir kısmına girilecek bilişim sistemi ile sistemin yazılımı (Softwere) kastedilmektedir. Sistemin hardwere (donanımsal yanına) girme eylemleri bu hükmün kapsamı dışındadır[325]. Ancak bu hükümler sisteme e-posta ya da dosya gönderilmesini kapsamaz[326].

ABD'de yetkisiz erişim bizde düzenlenen suçtan farklı olarak değerlendirilmektedir. Yetkisiz erişim suçunun oluşabilmesi için zararın meydana gelmesi ve bu zararı belirli bir miktardan aşağı olmaması gerekmektedir. Bu düzenleme bir anlamda TCK'nin 243/3. maddesindeki düzenlemeye paralel gibidir. TCK'deki düzenlemeden farkı oluşan zararın belirli bir miktardan aşağı olmaması ve

---

[322] Yazıcıoğlu, *Bilgisayar Suçları*, s.177 vd.
[323] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 254
[324] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması,* s. 155
[325] Dülger, *Bilişim Suçları,* s.218
[326] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması,* s. 155

kamu sağlığı ve güvenliğinin tehdit edilmiş bulunmasıdır. Bizdeki halihazır düzenleme ile "port tarayıcı[327]" kullanımı suç olarak değerlendirilmelidir[328]. Bu konuyla ilgili olarak, Federal Ceza Kanununun 18 USC SeC. 1030 (a) (5) (B) maddesi bir davada "port tarayıcı" kullanımına uygulanmıştır. Bu maddeye göre soruşturma yapılabilmesi için temel olarak altı unsurun kanıtlanması gerekmektedir. Bu altı unsura göre; sanık, korumalı bir bilgisayara kasten erişmiş olmalı, sanığın erişimi yetkisiz olmalı, erişimin neticesi olarak verilerin, sistemin veya bir programın bütünlüğüne veya kullanılabilirliğine zarar verilmiş olmalı, zarar en az 5.000,00 Amerikan Dolarlık ekonomik kayba sebep olmalı veya kamu sağlığını veya güvenliğini tehdit etmelidir[329].

Bu suçun maddi unsuru hangi yöntemle olursa olsun, hukuka aykırı olarak bilişim sisteminin bütününe veya bir kısmına girme ve sistemde kalmaya devam edilmesi fiilidir. Maddenin düzenleniş şekline getirilebilecek bir eleştiride sisteme girildikten sonra sistemde kalınması gereklililiğinin de aranmasıdır. Düzenleme bu haliyle bilgisayar sisteminin güvenilirliği ve bütünlüğünün korunmasına ters düşmektedir[330]. Bu durum Avrupa Siber Suç Sözleşmesinin 2. maddesinde öngörülen amaç ilede çelişir. Zira sözleşmenin anılan maddesinde bilişim sistemine hukuka aykırı erişim suçun oluşması için yeterli sayılmış, failin ayrıca burada kalmaya devam etmesi aranmamıştır[331]. Diğer taraftan failin girdiği sistemde kalmasını aramak, birçok soruyu da beraberinde getirmektedir. Örneğin; bilişim sistemine hukuka uygun olarak giren failin, izni sona erdikten sonra hukuka aykırı olarak kalmaya devam etmesi durumunda ne olacağı açıklığa kavuşturulmamıştır. Kanunun gösterdiği birinci hareket yapılmadığı için suç oluşup oluşmayacağı sorusunu yanıtlamak gerekir. Kanun, hukuka aykırı olarak girme ve orada kalmaya devam

---

[327] Port, internet ile bilgisayar arasındaki bağlantıyı kuran kapılardır. Örneğin sık kullanılan http protokolü, 80 nolu portu kullanır. Port tarayıcılar ise bu portlardan hangisinin açık olduğunu tarayarak bilgisayarlara sızmayı sağlarlar.

[328] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 177

[329] ABD Federal Mahkemesi'nin Kasım 2001 tarihli Scott Moulton kararı port tarayıcı ile ilgili örnek bir karardır. Bu konuda bakınız Özdilek, Ali Osman, "Port Tarayıcı Kullanımı Hukuka Aykırımıdır-2", http://www.turk-internet.com/portal/yaziyaz.php?yaziid=7068, (Erişim: 23.03.2014)

[330] Yazıcıoğlu, *Bilgisayar Suçları*, s. 83

[331] Dülger, *Bilişim Suçları ve Yeni Türk Ceza Kanunu,* s. 114

etmeyi açıkça aradığına göre, hukuka uygun girdikten sonra hukuka aykırı olarak orada kalmaya devam edilecek olursa, bu hükmü uygulamak "suçta ve cezada kanunilik ilkesi" aykırı düşeceği düşünülebilir[332].

TCK'nin 243. maddesinin metninde bulunan "giren ve orada kalmaya devam eden" ibaresi, kanun hazırlandığında bulunmamakta olup TBMM Genel Kurulunda bu biçimini almıştır[333]. Genel Kurul görüşmeleri de incelendiğinde, kanun koyucunun, madde metnine "veya" yerine "ve" ibaresini koyması bilinçsiz bir tercihten ibaret değildir. Biraz, suçun maddi öğesi ile manevi öğesi karıştırılmış ve manevi öğenin gerçekleşmemesi hali suçsuzluk sayılması yerine, maddi öge değiştirilerek, tesadüfen bilişim sistemine girilmesi hususu çözümlenmeye çalışılmış ise de, Kanun koyucu bu tercihi bilinçli olarak yaptığından ve bilerek ve isteyerek madde metnine "ve" ibaresi konulduğundan, bu bağlacın "veya" olarak anlaşılması mümkün olmayacağı, aksi bir yorumun kanun koyucunun amacını aşacağı görüşü daha öne çıkmıştır[334].

Genel olarak zarar suçu, suçun meydana gelmesi için zarar oluşmasının arandığı suçlardır. Buna karşılık sadece zarar tehlikesinin doğmasıyla yetinilen suçlara ise tehlike suçu denilmektedir. Zarar suçlarında zarar, korunan hukuki yarar da meydana gelen eksilmedir. Tehlike suçlarında ise korunan hukuki yarar açısından bir zarar oluşmamakta, sadece tehlike doğmaktadır[335]. Bilişim sistemine girme bir tehlike suçu olarak düzenlenmiştir. Ayrıca girme ve orada kalma eylemiyle verilerin güvenliğinin tehlikeye düşüp düşmediği araştırılamaz. Ancak maddenin üçüncü fıkrasındaki suçun oluşması için, failin bilişim sistemine girmeyi ve orada kalmayı istemesi, ancak verilerin yok olmasını ya da değiştirilmesini öngörmesine karşın istememiş olması gerekir. Fail, verilerin yok olması veya değişmesini de ister ise, bu durumda, TCK'nin 243/3. maddesindeki suç değil, aynı kanun'un 244/2. maddedeki

---

[332] Yaycı, Esra, *Bilişim Suçlar,* Yayımlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s. 78

[333] Güney ve diğerleri, *Yeni Türk Ceza Kanunu,* s. 1547

[334] Yaşar, Osman; Gökçen, Hasan Tahsin ve Artuç, Mustafa, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, Ankara: Adalet Yayınevi, 2010, s.6742

[335] Centel, Nur ve Zafer, Hamide, *Ceza Muhakemesi Hukuku*, İstanbul: Beta Yayınları, 2011, s. 197

suç oluşur[336]. Ayrıca bu maddedeki suçun oluşması için, failin hukuka aykın olarak bilişim sistemine girmesi ve orada kalması ile verilerin yok olması veya değişmesi arasında uygun illiyet bağının olması zorunludur[337].

Kanun koyucu, suçun oluşması için "girmek" ve "sistemde kalmaya devam etmek" eylemlerini birlikte aradığından, suç birleşik hareketlidir. "girmek" ve "kalmaya devam etmek (çıkmamak)" şeklinde biri icrai, diğeri ihmali nitelikte iki hareket birleşmekte ve bu suça vücut vermektedir. "kalmaya devam etmek" gerçekleştiği anda suç tamamlanır, ancak bitmez, bu andan itibaren gerçekleşen fiilin icrası devam eder. Fiilin icrasının devam ettiği bu tür suçlara mütemadi suç denilir[338]. Bu durumda bilişim sistemine giren ve orada kalmaya devam eden kimsenin sistem içinde kalması ne kadar olmalıdır? Çoğunlukla kalma eylemi zaman mefhumu olmaksızın girmekle birlikte başlamış olmaktadır; çünkü suç zorunlu olarak bir mütemadi suçtur. Ayrıca sistemde bir milisaniye dahi kalmakla verileri ele geçirme imkanı bulunduğu için, sonuç olarak kalma da gerçekleşmiş olacaktır. Girmekle zaten suçla korunan hukuki yarar, yani verilerin ve sistemin gizliliği ihlal edilmiş olacaktır[339]. Bu suç ile sistem sahibinin özel alanının dokunulmazlığı, huzur ve sükûn, verilerin gizliliği korunmak istendiğine göre, korunan bu değerlere müdahale edebilebilmesinin mümkün oldacağı süre kadar bilişim sistemi içinde kalmış olmak, suçun oluşumu için yeterli kabul edilecektir. Bu süre ise somut olayın koşullarına göre belirlenmelidir[340]. Suçun tamamlanması bir kişinin, bilişim sistemine girdiğini farketmesine rağmen sistemi terk etmemesi ile olur[341].

---

[336] Yazıcıoğlu, Yılmaz, "Hukukumuzda TCK'nin 243. Maddesi Kapsamında Bilişim Sistemine Girme Eylemi", *Bilişim Hukuku Konferansı Kitabı,* Ankara: Yargıtay Başkanlığı, (09-10.10.2008), s. 84**;** Taşdemir**,** *Bilişim-Banka veya Kredi Kartlannın Kötüye Kullanılması-Dolandıncılık Suçları*, s. 260

[337] Malkoç, İsmail*, Açıklamalı-İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu*, Ankara: Malkoç Kitapevi, 2007, Cilt: II, s. 1671

[338] Artuk, Mehmet Emin; Gökçen, Ahmet ve Yenidünya, Ahmet Caner, *5237 Sayılı Kanuna Göre Hazırlanmış Ceza Hukuku Özel Hükümler,* Ankara: Turhan Kitapevi, 2007, s. 658

[339] Yazıcıoğlu, *Bilgisayar Suçları*, s. 22

[340] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması,* s. 154

[341] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 259

TCK'nin 243. maddesinin üçüncü fıkrasına göre, failin bilişim sisteminin bütününe veya bir kısmına, hukuka aykın olarak girilmesi ve orada kalmaya devam etmesi nedeniyle sistemin içerdiği veriler yok olur veya değişirse, fail daha ağır bir ceza ile cezalandırılır. Üçüncü fıkra ile birinci fıkrada düzenlenen suçun, neticesi sebebiyle ağırlaşmış hali hüküm altına alınmıştır[342]. Yokedilen veya değiştirilen verilerin hukuka aykırı olarak girilen bilişim sistemindeki veriler olması gerekir. Kişinin bilişim sistemine girmede kullandığı bilgisayar veya benzeri cihazındaki verilerin zarar görmesi bu suçu oluşturmaz. Bir diğer husus ise verinin tamamının değil, kısmi değişim ya da zarar görmesininde yeterli olacağıdır[343]. Yokolan veya değişen verinin öneminin bir ehemmiyeti yoktur. Çünkü kanun koyucu düzenlemede böyle bir ayırıma gitmemiştir[344]. Hukuk dışı erişim ile bilişim sistemlerine giren kişilerin, girme eylemi için bilgisayarın yazılımına müdahale etmek durumunda oldukları gerçeği karşısında her hukuksuz erişimin sonucunda 3. fıkradaki ağırlaştırıcı halinde gerçekleştiğini söylemekte sakınca bulunmamaktadır.

Maddenin 2. fıkrasında hafifletici neden düzenlenmiştir. TCK'nin 243/2. maddesine göre, hukuka aykın olarak bilişim sistemine girme ve kalmaya devam etme eyleminin, bedeli karşılığında yararlanılabilen sistemler hakkında işlenmesi halinde, faile verilen cezadan indirim yapılır. Bedeli karşılığı yararlanılan sistemlere, internet cafelerde olduğu gibi bir ücret karşılığı kiralanmış sistemleri, ücret karşılığı internet üzerinden hizmet veren web sitelerini, bedel karşılığı internet bağlantı servisinin sağlandığı sistemleri ve bir kuruluş tarafından bir hizmetin sunulduğu bilişim sistemini dahil etmek mümkündür. Ancak bu örnekleri artırmak da olanaklıdır[345]. Bu fıkrada kanun koyucu bilişim sisteminden çok mal varlığını korumaya yönelik bir düzenleme getirdiğinden indirim öngörülmüştür[346]. Bu kapsamda bedeli karşılığında özel televizyon yayınlarının izlenmesine imkan tanıyan

[342] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 6748
[343] Yazıcıoğlu, *Bilgisayar Suçları*, s. 85
[344] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 6749
[345] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 109
[346] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler,* s. 4650

cihazlar birer bilişim sistemi olduğu halde bu suç için TCK'nin 163/2. maddesinde özel düzenleme bulunduğu için 243/2 kapsamına girmeyecektir[347].

1.4.2. Bilişim Sisteminin İşleyişinin Engellenmesi, Bozulması, Verilerin Yok Edilmesi veya Değiştirilmesi Suçu (m. 244/1-2-3)

Bilişim sistemleri ile bu sistemlerde kayıtlı verilere her türlü zarar verici eylem TCK'nin 244. maddesinin 1. ve 2. fıkralarında[348] suç tipi olarak düzenlenmiştir. Düzenlemenin 1. fıkrasında "bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması", 2. fıkrasında ise "bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi" eylemleri suç tipi haline getirilmiştir[349]. Avrupa Siber Suç Sözleşmesinin 4. maddesinde düzenlenen "verileri etkileme" 244/1. fıkra, 5. maddesinde öngörülen "sisteme etki" 244/2. fıkradaki düzenleme ile uyumluluk sağlanması için yapılmış düzenlemelerdir[350]. Bu düzenlemede getirilen suç tipi ile bilişim sisteminin bozulması veya her ne şekilde olursa olsun çalışmasının engellenmesi ya da sisteme kayıtlı verilerin kullanılamaz hale getirilmesi cezalandırılmak istenmektedir. Maddenin gerekçesi de, maddenin düzenleniş amacının yukarıda açıklandığı gibi bilişim sistemlerine yönelik zararlandırıcı eylemlerin ayrı bir suç haline getirilmesinin amaçlandığını belirtilmektedir. Madde düzenlenirken özellikle mala zarar verme eylemi ile karıştırılmaması, yani bilişim

---

[347] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 6750

[348] "Madde 244; (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.
(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.
(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır."

[349] Dülger, *Bilişim Suçları*, s.230.

[350] Yazıcıoğlu, *Bilgisayar Suçları*, s.179

sisteminin Hardwere (Donanım) kısmına zarar verme eyeminden ayırmak için yerinde olarak "zarar verme" tabiri kullanılmamış, kapsam dışı tutulmuştur[351].

Maddenin 1. fıkrasında, "engelleme"' "bozma" gibi iki seçimlik hareket düzenlenmiştir. Suçun oluşması için bu iki seçimlik hareketten birisinin gerçekleşmesi yeterlidir. İkisi birlikte gerçekleşmesi halinde de tek suç vardır. Bu takdirde yargıcın temel cezayı tayin ederken TCK'nin 61. maddesini[352] gözetmesi yerinde olacaktır. Sistemin işleyişinin engellenmesi ile sistemin gerektiği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi anlaşılmalıdır[353]. Böylece sistemin veri işleme hızı, düzenli çalışma yetenekleri olumsuz şekilde etkilenmektedir. Yoksa sistem bozulmamakta, ancak sağlıklı çalışamamaktadır, örneğin; sistem devamlı e-mail (e-posta) ya da zararlı virüs gönderilmek suretiyle çalışamaz hale getirilmektedir. Kanun koyucu burada bilişim teknolojilerinin ruhuna uygun şekilde, kavramı çok geniş tutmuştur. Buna göre nasıl olduğunu aramaksızın sistemin işleyişini bozmak dışında, sistemin işlemesini engelleyen her türlü eylemi buraya dahil etmek istemiştir. Böylece teknolojinin gelişmesi nedeniyle her gün çeşitlilik kazanan bu tür faaliyetlerin gerisinde kalınmak istenmemiş ve kanun yapma tekniğine uygun davranılmıştır. Engellenme sürekli veya geçici olabilir[354].

Sistemin işleyişini bozmak ile ilgili olarak ise, bilişim sisteminin olağan koşullarda yapması gereken işlevlerinin değişikliğe uğratılmasıdır. Bu eylem, dışarıdan sisteme yapılacak fiziksel bir etki ile olabileceği gibi, sistemdeki veri ve programlara ilişkin eylemlerle de gerçekleştirilebilir[355]. Bozmak eyleminin gerçekleştirilme yöntemi, suçun oluşması bakımından önemli değildir. Böylece

---

[351] Dülger, *Bilişim Suçları* s.230-231; Dülger*, Bilişim Suçları ve Yeni Türk Ceza Kanunu*, s.115. Karşı Görüşte Bkz: Yazıcıoğlu, *Bilgisayar Suçları*, s.179; Özel, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", s.860-865; Değirmenci, *Bilişim Suçları*, s.154

[352] TCK m. 61 – Cezanın belirlenmesi ve bireyselleştirilmesi.

[353] Değirmenci, *Bilişim Suçları*, s. 161

[354] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 269

[355] Yazıcıoğlu, *Bilgisayar Suçları*, s. 263

sistem çökertilmekte, verileri ve işleyiş düzeni bozulmaktadır. Bu tanımlardan da anlaşılacağı üzere "bozmak" engelleme sonucunu da doğuran bir anlama sahiptir. Bir bilişim sisteminin işleyişini bozan bir müdahale, aynı zamanda onun işleyişini de engellemiş olur. Ancak bu durum her iki kavramın aynı anlama geldiğini göstermez. Çünkü engellemek, bozmak demek değildir ve bir bilişim sisteminin işleyişi, bozulmadan da engellenebilir[356]. Bilişim sistemine zarar vermek kastıyla icra hareketlerine başlayan failin fiziki bir saldırısı sonucunda bilgisayarın fizik yapısının zarar görmesi durumunda, aynı zamanda bilişim sisteminin de bozulacağı mutlaktır. Failin tek fiil ile kanunun çeşitli maddelerini ihlâl etmesi halinde, TCK'nin 44. maddesi uyarınca en ağır cezayı gerektiren aynı Kanunun 244/1. maddesi uyarınca cezalandırılması gerekecektir[357].

TCK'nin 244. maddesinin 2. fıkrasında düzenlenen suçun konusunu, bir bilişim sisteminin verilerinin dokunulmazlığı oluşturmaktadır. Bu suç, Avrupa Siber Suç Sözleşmesinin 4. maddesinde düzenlenen "verilere müdahale" eylemini karşılamaktadır.

1.4.3. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu (m. 244/4)

"Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu", TCK'nin 244. maddesinin 4. fıkrasında[358] düzenlenmiştir. Bu suç tipi düzenlenirken maddenin ilk iki fıkrasına atıf yapılmıştır. 244/1 ve 2. fıkralar birleştirilerek 4. fıkraya eklendiğinde suç tipi "Bir bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemin içerdiği verilerin bozulması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi, erişilmez kılınması, değiştirilmesi ve yok edilmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlanmasının başka bir suç oluşturmaması halinde, ... cezasına hükmolunur" şeklinde olacaktır. Bu fıkranın

---

[356] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s.5

[357] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 273

[358] "Madde 244; (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

en dikkat çekici yönü bu suç tipi açısından, "başka bir suç oluşturmaması halinde" ifadesinin kullanılmasıdır. Bu şekilde yasa koyucu failin eyleminin bir başka suç tipinde düzenleniyor olması halinde 244/4. fıkrada ki suçun oluşmayacağını, fiile ilgili madde de düzenlenen suça ilişkin cezanın uygulanacağını hüküm altına alınmıştır. Kanunun gerekçesinde bu düzenleme ile ne anlaşılması gerektiği; "bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir" şeklinde belirtilmiştir[359].

Haksız çıkarın maddi olması gerekmez. Kanun koyucu madde metninde "haksız bir çıkardan" bahsetmektedir. Fail bu fiilleri işlerken başka çıkarlar elde etmeyi murat etmiş olabilir. Fail o an kendisi için belki paradan da önemli olan bir menfaati temin etmek kastı ile eylemi gerçekleştirebilir. Bir öğrencinin, öğretmeninin bilişim sistemine girerek sınav sorularını çalması veya notlarını düzeltmesi ya da kötü olan notlarını yok etmesi hallerinde fail maddi olarak bir şey kazanmamakta, ancak bu fiilleri haksız manevi bir çıkar sağlamak için yerine getirmektedir. Bu fiilleri bir başka arkadaşı içinde yapıyor olması halinde de durum aynıdır[360].

1.4.4. TCK'nin 244. Maddesi Koruması Altına Alınan Fiilerin Doğuracağı Sonuçlara Göre İncelenmesi

244. maddede genel olarak hem sistemi, hemde verileri koruyan hükümler düzenlenmiştir. Maddenin birince fıkrasında sistem korunurken, ikinci fıkrada veriler korumnmaya çalışılmıştır. Verilerin ihlaline ilişkin eylemler çok değişik şekillerde karşımıza çıkmaktadır. İkinci fıkra verileri ihlal eden fiilleri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme şeklinde sayma usulüyle belirlemiştir. Bilişim sistemi teknolojisinin sürekli gelişim içerisindi olduğu düşünüldüğünde bu fiilere yenilerinin eklenebileceğini gözeterek benzer fiileride kapsar bir düzenlemenin yapılması daha

[359] Dülger, *Bilişim Suçları*, s.244; Dülger, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", s.116
[360] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 203

yerinde olacaktır. Bu eylemlerin biraz daha açılarak incelenmesinde yarar bulunduğundan aşağıda tek tek üzerinde durulacaktır.

1.4.4.1. Verileri Bozma

Bozmak, kelime anlamı itibariyle, bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek, bir şeyin veya yerin düzenini karıştırmak, zarar vermek, işleyişini yitirecek şekilde şeklini değiştirmek olup, verilerin sıhhatli halinin ortadan kaldırılması anlamına gelmektedir[361]. Veri içeren bir dosya (ses, müzik, grafik, metin vs. olabilir) bozularak ya tamamıyla faydalanamayacak hale ya da kısmen hasarlı hale gelir. Bilişim sistemine girerek bilfiil veya girmeden zararlı bir program vasıtasıyla verilerin bozulması halinde bu suç oluşacaktır[362]. Bilişim sistemindeki verilere zarar verilmesi bazen sadece veri ile sınırlı kalmaz bilişim sisteminin işleyişini engellemiş veya bozmuş olabilir. Bu durumda ise failin maddenin 1. fıkrasına göre cezalandırılması gerekir. Fail, burada bilişim sistemine zarar vermek istememekte, yalnızca bir kısım verileri kullanılamaz hale getirmeyi amaçlamaktadır.

1.4.4.2. Verileri Yok Etme

Verilerin ortadan kaldırılması anlamına gelmektedir. Bu anlamda yok etme, verilerin silinmesini de kapsamaktadır, Burada önemli olan verinin, mağdurun tasarruf alanından çıkartılmış olması ve normal yollardan ulaşılmasının güçleştirilmesidir. Ortadan kaldırılan veriye, mağdurun kendisinin veya bir uzmanın tekrar ulaşabilme imkanının varlığı suçun oluşmasını engellemeyecektir. Bununla birlikte, örneğin; bir dosyanın geri dönüşüm kutusuna atılması gibi, verinin sistemde tutulmakla birlikte, sırf yerinin değiştirilmesi niteliğindeki hareketler bu suçu oluşturmayacaktır[363].

---

[361] Türk Dil Kurumu Sözlüğü; http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5422feb62e5a01. 76805949

[362] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması,* s.167

[363] Koca**,** Mahmut, (2009), "Hukukumuzda TCK'nin 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", *Bilişim Hukuku Konferansı*, T.C. Yargıtay Başkanlığı, Ankara: Yargıtay Basımevi, (09-10.10.2008), s. 89-99.

1.4.4.3. Verileri Değiştirme

Verilere başka bir görünüm kazandırma, başbir biçime sokmadır[364]. Örneğin; bir bilgi notunun değiştirilmesi, hastahane verilerinin olduğundan az veya çok gösterilmesi gibi müdahaleler veri değiştirmeye girer. Bununla beraber örneğin şifrenin değiştirilerek sisteme ulaşılmasının engellenmesi değiştirme değil aşağıda incelenecek olan verileri erişilmez kılma içinde değerlendirilebilir.

1.4.4.4. Verileri Erişilmez Kılma

Maddi anlamda yok etmemekle birlikte, sahibinin veya kullanıcısının istediği zaman verilere ulaşması için gereken işlem bağı ortadan kaldırılmaktadır. Burada veriler bozulmamakta ve yok edilmemekte sahibinin veya kullanıcısının sisteminde bulunan verilere ulaşması engellenmektedir. Bir kimsenin bilgisayarındaki dosyasına şifre koymak buna örnek verilebilir.

1.4.4.5. Veri Yerleştirme

Sistemin ait olduğu kişinin izni olmaksızın, verilerin sisteme kaydedilmesi, eklenmesi ya da yüklenmesidir[365]. Bu eylemle, sistemde bulunan verilere zarar verilmemekte, onlara ulaşma olanağı ortadan kaldırılmamakla birlikte sisteme bir takım veriler ilave edilmektedir. Sisteme veri yerleştirilmesi izinsiz olabileceği gibi, izinli olarak sisteme girildikten sonra veri girişi yapılması suretiyle de olabilir. İnternet ortamından da sisteme veri yerleştirmek olanaklıdır. Sisteme yerleştirilen veriler, daha sonra oluşturulan bir belgenin içeriğini etkilemişse, fail ayrıca belgede sahtecilikten sorumlu tutulur (TCK m. 212[366])[367].

---

[364] Yazıcıoğlu, *Bilgisayar Suçları*, s. 263
[365] Dülger, *Bilişim Suçları,* s.237
[366] **"TCK madde 212. -** (1) Sahte resmî veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması hâlinde, hem sahtecilik hem de ilgili suçtan dolayı ayrı ayrı cezaya hükmolunur."

1.4.4.6. Verileri Başka Bir Yere Gönderme

Verilerin başka bir bilişim sistemine veya veri taşıma cihazına aktarılması, taşınması ya da kopyalanması anlamına gelmektedir. "var olan verileri başka yere göndermek", mağdura ait verilerin gerek mağdurun bilişim sisteminde farklı bir dosyaya, gerekse de, farklı bir bilişim sistemine gönderilmesi anlamını taşır. Dolayısıyla verilerin, mağdura ait olmayan başka bir bilişim sistemine gönderilmesi şart değildir[368]. Bununla birlikte bu hareket bakımından verilerin erişilmez olup olmadığına bakılmaksızın, bulunduğu bilişim sisteminin dışına transfer edilmesinin yeterli olduğu sonucuna varmak gerekir. Bu suç bakımından seçimlik hareketlerin bazılarının, birbiriyle örtüştüğü görülmektedir[369].

Verilere yönelik işlenen suçlar seçimlik hareketli suçtur. Görüldüğü gibi, maddenin fıkrasında seçimlik hareketler belirtilmiştir. Bu hareketlerden herhangi birisinin gerçekleştirilmesi durumunda maddedeki suç oluşur. Örneğin; verilerin bir kısmının bozulası, bir kısmının silinmesi halinde olduğu gibi belirtilen sonuçlardan birden fazlasının aynı anda oluşması halinde faile bir kez ceza verilecektir.

1.4.5. Bilişim Alanında Suçlar Bölümünde Düzenlenen Suç Tiplerinin Diğer Suç Tipleri İle Olan İlişkisinin İncelenmesi

TCK'nin "Bilişim Alanında Suçlar" bölümünde düzenlenen suç tiplerini oluşturan eylemin işlenmesi ile aynı eylemin sonucu olarak bir başka suç tipinin daha ortaya çıkması muhtemeldir. Örneğin, aynı fiilin sonucu olarak hem bilişim suçu hemde görevi kötüye kullanma, hırsızlık, mala zarar verme ve dolandırıcılık gibi Kanunun diğer bölümlerinde düzenlenen suç tipleri oluşabilir. TCK bilişim suçlarının düzenlenmesi bakımından karma bir yöntem benimsemiş bilişim suçlarını hem "Bilişim Alanında Suçlar" başlığı altında düzenlemiş (m. 243-246), hem de geleneksel suç tipleri içinde bunlara yeni ilaveler yaparak söz konusu suç tipini genişletmiş, suçun bilişim yoluyla düzenlenmesini suçun nitelikli hali olarak kabul

---

[367] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler,* s.713
[368] Dülger, *Bilişim Suçları,* s. 230
[369] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 8

etmiştir. Öte yandan TCK bazı suçlar bakımından bu suçların basın yayın yoluyla işlenmiş olmasını ağırlatıcı neden olarak öngörmüş ve 6/g maddesinde "Basın ve yayın yolu ile deyiminden; her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar" anlaşılır demek suretiyle internet vb. yolla yapılan yayını da bu tanım içine sokmuştur. Bu suretle bilişim yoluyla işlenen suçların kapsamı da genişlemiş olmaktadır[370]. Bunların birbirleriyle olan ilişkilerinin suç tiplerine göre teker teker incelenmesi gerekir.

TCK'nin 243. maddesindeki "Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren ve orada kalmaya devam eden kimse", bir adım daha atarak sistemdeki verileri bozsa veya seçimlik hareketlerden birisini gerçekleştirse, burada geçitli suç konusu olacak, fail daha ağır ceza içeren 244/2. maddedeki suç nedeniyle cezalandırılacaktır[371]. İkinci fıkradaki suç, bazen hırsızlığa, bazen dolandırıcılığa, bazen güveni kullanmaya çok benzemektedir. Sayılan suçların, örneğin; hırsızlığın mal üzerinde işlenmesinin zaruri olması, verinin ise mal olarak kabul edilmesinin mümkün bulunmaması, dolandırıcılıkta ise hile ile bir kişinin kandırılmasının gerekmesi, bilişim sistemlerinin ise kandırılmasının söz konusu olmaması sebebiyle, klasik hırsızlık ve dolandırıcılık suçlarının gerçekleşmeyeceği söylenebilir[372].

244. maddede sayılan eylemlerin güveni kötüye kullanma suçunu oluşturup oluşturmadığının tespiti için yapılan eylemin TCK'nin 155. maddesi[373] ve 244. maddesi ile karşılaştırılarak değerlendirilmesi gerekmektedir. Somut olaya göre, veriler üzerinde değişikliğe neden olan bozan değiştiren, yok eden, başka bir yere taşıyan ve benzeri eylemlerde bulunan kişinin, bu veriler üzerinde sözleşme ile tesis

---

[370] Ergün, İsmail, "Yeni Türk Ceza Kanunu'nda Bilişim Suçları", *2. Polis Bilişim Sempozyumunda Sunulan Bildiri*, 14 – 15.04.2005, Ankara.

[371] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 272

[372] Yazıcıoğlu, *Bilgisayar Suçları,* s.144

[373] **"Güveni kötüye kullanma**

Madde 155. - (1) Başkasına ait olup da, belirli bir şekilde kullanmak üzere zilyedliği kendisine devredilmiş olan mal üzerinde, kendisinin veya başkasının yararına olarak, zilyedliğin devri amacı dışında tasarrufta bulunan veya bu devir olgusunu inkar eden kişi, şikâyet üzerine, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır."

edilen bir zilyetlik yetkisinin olması gerekmektedir. Bu şekilde bir sözleşme ile bu veriler üzerinde zilyet olarak bir takım haklara sahip olan kişi, bu yetkisini aşarak amacı dışında tasarrufta bulunuyor ise güveni kötüye kullanma suçunun oluştuğu söylenebilir[374]. Ancak her somut olayda zilyetliğin devri amacı iyi araştırılmalıdır. Bilişim sisteminde var olan verilerin sözleşme gereğince bir başka kişi tarafından başka bir yere aktarılması istenebilir. Bu durumda aktarmayı yapacak kişi, bu verileri istenilen yerin dışında bir yere aktarır ve bundan da kendisine veya başkasına bir menfaat temin ederse, güveni kötüye kullanma suçunun oluştuğu söylenebilir. Bu durumda 244. madde için aranmayan şikâyet şartının somut olayda mevcut olup olmadığına bakmak gerekir[375]. Son fıkranın uygulanabilmesi için failin eyleminin maddede aranan tipik suçtan farklı bir suçu oluşturmaması koşulu getirilmiştir. Bu bakımdan eylemin, güveni kötüye kullanma, hırsızlık, dolandırıcılık veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne dayanılarak ceza tayin edilemeyecektir. Bunun dışında TCK'de bilişim sistemlerinin kullanılması suretiyle hırsızlık (TCK m. 142/2-e[376]) ve dolandırıcılık (TCK m. 158/1-f[377]) ile 245. maddede banka ve kredi kartlarının kötüye kullanılması suçları ayrıca düzenlenmiştir[378].

Hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle (TCK m. 142/2-e) ve dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi (TCK m. 158/1-f), uygulamada tartışma konusu olmaktadır[379]. Hırsızlık suçu ancak taşınabilen bir mal üzerinde işlenmektedir. Dolayısıyla hırsızlık suçunun hukuki konusu taşınabilir bir maldır.

---

[374] Dülger, *Bilişim Suçları,* s. 230

[375] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 272

[376] **"Nitelikli hırsızlık**
Madde 142. - (1) Hırsızlık suçunun;...
(2) Suçun; ...
e) Bilişim sistemlerinin kullanılması suretiyle, ...
... İşlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur."

[377] **"Nitelikli dolandırıcılık**
MADDE 158. - (1) Dolandırıcılık suçunun; ...
f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle, ...
... İşlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

[378] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 168

[379] Taşkın, Şaban Cankat, *Bilişim Suçları,* Bursa: Beta Yayınları, 2008, s. 116

Oysa verinin "mal" olarak kabul edilmesi olanaklı değildir. Bilişim sisteminin kullanılması halinde, üzerinde icra hareketinin gerçekleştiği her şey "veri"'dir. Bu halde artık TCK m. 142/2-e'de düzenlenen suç değil TCK m. 244. maddede düzenlenen suç oluşacaktır[380].

Dolandırıcılık suçuna gelince; bu suç ile iki hukuki konu korunmaktadır. Birincisi insan iradesinin özgürlüğü, ikincisi, malvarlığına ilişkin varlık ve menfaatlerdir. Dolandırıcılık suçunda, bir şeyin teslimi, hile ile sakatlanmış ve özgür olmayan bir iradeye dayanmaktadır. Bu suçun oluşması için, hileyle kandırılmış olan mağdurun fesada uğratılmış iradesiyle malı teslim etmesi ya da başka bir davranışla kendi malvarlığı zararına bir işlemde bulunması zorunludur. Yararın, bilişim sistemi yanıltılarak elde edilmesi halinde dolandırıcılık suçu oluşmayacaktır. Bununla birlikte çok sınırlı sayıda TCK'nin 142/2-e ve 158/1-f maddelerinin uygulanma alanı bulması da olanaklıdır[381]. Bir örnek verecek olursak; ağ üzerinden rezervasyon imkânı sunan ve aynı sistemle ödemeleri kabul eden bir otelin bilişim sistemine giren fail, hafta sonu için rezervasyon yaptırsa, sonra da otelin bilişim sistemine yapılan rezervasyonun ödemelerinin yapılmış olduğuna dair gerçeğe aykırı veri yerleştirse, akabinde otele gitse, otel yetkilisi kendi ilişim sistemlerine girdiklerinde rezervasyonun ve ayrıca ödemenin yapıldığına ilişkin fail tarafından yerleştirilen verileri görerek aldansa ve failin kalmasına izin verse, bu olayda, bilişim sistemleri vasıta kılınarak dolandırıcılık suçu işlenmiş demektir[382]. Bu olayda, (m. 158/1-f) uygulanacağı için TCK'nin 244/4. maddesi gündeme gelmeyecektir. Zira fıkradaki başka suç oluşturmama koşulu gerçekleşmemiştir[383].

Bu suçun özelliği tali norm niteliğinde olmasıdır. Tali normlar, bu konuda bir boşluk bırakmamak üzere konulan hükümlerdir, bir fiil hakkında asli ve tali norm şeklinde iki hüküm bulunuyorsa, asli norm öncelikle uygulanacaktır. Nitekim madde metninde suçun bu özelliğini ifade etmek üzere, fiilin başka bir suçu oluşturmaması

---

[380] Dülger, *Bilişim Suçları,* s. 289
[381] Soyaslan, *Ceza Hukuk Özel Hükümler*, s. 610
[382] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 171
[383] Taşkın, *Bilişim Suçları,* s. 117 ve 182

gerektiğinden bahsedilmiştir. Bu durumda bilişim sistemleri aracılığıyla haksız çıkar sağlama şeklinde bir olayla karşılaştığında, ilk önce fiilin, örneğin; güveni kötüye kullanma, hırsızlık, dolandırıcılık veya zimmet gibi başka bir suçu oluşturup oluşturmadığı araştırılmalıdır. Şayet olayın gerçekleştiriliş şekli bu suçlardan biri tanımına uygun ise, bu suçlar işlenmiş olacaktır. Gerçekleştirilen bu suçlardan birisinin tanımına uymuyorsa, o zaman 244. madde fıkrası hükmü uygulanabilecektir[384].

TCK'de bilişim vasıtasıyla işlenebilecek suç türleri daha çok bulunmakla birlikte ilgili olan alanlar itibarıyla bir sıralama yapmak daha yararlı olacaktır.

1) *"Haberleşmenin gizliliğini ihlâl suçu" (m. 132),*
2) *"Haberleşmenin engellenmesi suçu" (m. 124),*
3) *"Kişisel verilerin kaydedilmesi suçu" (m. 135),*
4) *"Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu" (m. 136),*
5) *"Verilerin yok edilmemesi suçu" (m. 138),*
6) *"Eğitim ve öğretimin engellenmesi suçu" (m. 112),*
7) *"Kamu kurumu veya kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinin engellenmesi suçu" (m. 113)* gibi dolayısıyla bilişim suçuna yer vermekte olup klâsik suç tiplerinden sadece hırsızlık (TCK m. 142/2-e) ve dolandırıcılık (TCK m. 158/1-f) suçunda bilişim sistemlerinin kullanılmasını özel ağırlatıcı sebep olarak değerlendirme altına almaktadır[385].

Kanun ayrıca, sahtecilik[386] suçu bakımından bilişimin getirilerini dikkate almaktadır. Bunun gibi, kanun hırsızlık (TCK m. 144/1-b), dolandırıcılık (TCK m.

---

[384] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 10
[385] Erdağ, *Bilişim Alananda Suçlar,* s. 279 vd.
[386] Kanun sahtecilik suçlarında bilişim faktörünü öngörmeyerek Avrupa Konseyi Siber Suç Sözleşmesinin 7 inci maddesi ile taraf Devletlerce «bilgisayarla ilişkili sahtecilik eylemlerinin» yaptırım altına alınmasına yönelik düzenlemeyi göz ardı etmiş olmaktadır.

159), yağma (TCK m. 150/1) gibi birçok suçta değerlendirdiği "hukukî bir ilişkiye dayanan alacağın tahsili amaç" kavramına bilişim suçlarında önem atfetmemektedir. Yine haksız olarak girilen sistemdeki verinin kopyalanmasını (765 sayılı TCK'nun 525/a-1 ve 2 inci maddelerinde düzenlenen), iletişime müdahaleyi, bir bilişim sistemine veya programına girme imkânı veren şifrelerin dağıtımını veya hukuk dışı olarak bir bilgisayar sistemi veya programının sunularından istifadeyi sağlayacak cihaz veya programları satmayı veya tedarik etmeyi müeyyide altına alan bir hükmü de ihtiva etmemektedir[387].

Burada en dikkati çeken husus, 5327 sayılı kanunun, 765 sayılı TCK'de olduğu gibi bu tür suçları artık mal aleyhine suçlar içinde değil ve fakat topluma karşı suçlar içinde mütalaa ediyor olmasıdır. Yeni TCK'ye bilişim suçları bakımından genel olarak bakıldığında, bir yandan mukayeseli hukuktaki gelişmelere yeterince paralel olmadığı, bir yandan da Avrupa Konseyi Bakanlar Komitesinin "Avrupa Konseyi Siber Suç Sözleşmesinde" öngörülmekte olan düzenlemelere de tam bir uygunluk arz etmediği gözlenmektedir. Ayrıca bilişim suçları bakımından 5237 s. Kanundaki hükümlerin kendi içinde ciddi çelişkiler içerdiğini ve gerek Siber Suç Sözleşmesinde gerekse Birleşmiş Milletler 10. Suçluların İyileştirilmesi ve Suçların Önlenmesi Hakkındaki Viyana Kongresinde özellikle bilgisayar ağlarının ve burada işlenen suçların önlenmesi için öngörülen bazı düzenlemelerin eksik olduğu da genel olarak söylenebilecek hususlardandır[388].

---

[387] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 61

[388] Yazıcıoğlu, Yılmaz, "Türk Mevzuatında Bilişim Suçları", *AB Uyum Komisyonu Çalısması*, http://www.taa.gov.tr/duyurularana/130606/bilisimsempozyum/sunum/makale.pdf (Erişim: 03.05.2011) s. 17,

İKİNCİ BÖLÜM

SUÇUN UNSURLARININ İNCELENMESİ

Birinci bölümde, inceleme konusu suçun temel özellikleri açıklanmıştır. Genel bir değerlendirme olarak suçun anlaşılabilirliğini kolaylaştıracak kavram ve unsurlar üzerinde durulması önem arz ettiği için hem kişisel verilerin korunması, hem de suçun birlikte işlenmesini gerektiren bilişim sistemleri ile işlenen suçlar açıklanmıştır. Ancak bilişim alanında ki kişisel verilerin korunmasına ilişkin suç tiplerinin ceza hukukunun temel kavramları ile ele alınarak incelenmesi de gerekmektedir. Suçun unsurlarından olan fail, mağdur, yer bakımından yetki, suçun işlendiği zaman gibi konuların detaylı bir şekilde üzerinde durularak ortaya çıkabilecek sorunların da tespiti ancak bu yöntemle yapılabilecektir. Tabi ki bu incelemede de yine TCK'nin kabul ettiği sistematik izlenmiş ve doktirinin bu konudaki görüşlerine yer verildiği kadar uygulamacıların görüş ve önerileride aksettirilmeye çalışılmıştır.

Her bir suçun kanuni tanımında yer alan unsurları, maddi ve manevi olmak üzere, iki ana grupta toplanmaktadır. Bu itibarla, suçun yapısal unsurlarının açıklanmasında bu maddi ve manevi unsurlar ayırımının esas alınması gerekmektedir. Suçun unsurlarından maksat, suçun varlığı için bulunması zorunlu olan şartlardır. Maddi unsurların gerçekleşmiş olması yeterli değildir, manevi unsurun da gerçekleşmesi diğer bir deyişle cezalandırılabilme için maddi unsurun manevi unsur ile desteklenmesi gerekir[389]. Yukarıda açıklanan nedenlerle suçun unsurlarının genel olarak kısaca açıklanması ve akabinde inceleme konusu suç yönünden ayrı ayrı değerlendirmesi yararlı olacaktır.

[389] Tan, Mehmet, *Türk Ceza Kanunu Genel Hükümler*, 1. Baskı, Ankara: Seçkin Yayınevi, 2011, s.455

2.1. SUÇUN MADDİ UNSURLARI

Her bir suçun kanunî tanımında yer alan unsurlar, maddi ve manevi olmak üzere, iki ana grupta toplanmaktadır. Suçun analitik bir biçimde incelenmesi, esas itibariyle, iki teorinin doğmasına neden olmuştur. İkili ayrım adı verilen geleneksel teoriye göre suç "*kusurlu irade ile işlenen bir fiil"*dir, dolayısıyla suçun biri maddi *(objektif)* diğeri manevi *(sübjektif)* olmak üzere iki genel kurucu unsuru vardır[390]. Bu itibarla, suçun yapısal unsurlarının açıklanmasında bu maddi ve manevi unsurlar ayırımı esas alınması daha uygun olacaktır. Fiilin harici görünüm şekli maddi unsurlar tarafından tanımlanır. Suçun kanuni tanımında yer alan objektif unsurları; fail, mağdur, suçun konusu, hareket, hareketin tür ve şekilleri, gerektiği takdirde netice olarak belirlemek mümkündür. Tipikliğin, yazılı olanların yanı sıra neticeli suçlardaki nedensellik bağı gibi, yazılı olmayan unsurları vardır. Suçların herhangi bir unsurunun olayda gerçekleşmemesi faile ceza verilmesine, fiilin suç sayılmasına dolayısı ile ceza davasının açılmasına engel olur. Suç unsurlarının her birinin olayda gerçekleşmesi şarttır[391].

Hukuka aykırılık, tipikliğin bir unsuru değil, suçun genel bir unsurudur. Ancak bazı suçların kanuni tanımında "hukuka aykırı", "hukuka aykırı olarak" ya da "haksız" veya "haksız olarak" şeklinde ifadelere yer verilmektedir. Bir suçun kanuni tarifinde bu tür ifadelerin geçtiği hallerde bir ayırım yapmak gerekir. Şayet bu kavram münferit bir unsurun sıfatı olarak görünüyorsa, gerçek bir tipiklik unsuru söz konusudur. Bu durumda kastın bu hukuka aykırılığı da kapsaması gerekir[392]. Örneğin; TCK'nin 244. maddesinin 4. fıkrasında düzenlenen "bilişim sitemini veya verileri engellemek ya da bozmak suretiyle çıkar sağlama suçunda", failin "kendisinin veya başkasının yararına haksız bir çıkar sağlaması" aranmaktadır. Dolayısıyla bu suç tipinde yer alan "haksız" kelimesi, yalnızca suçun "çıkar sağlama" unsuruna ilişkin bir vasıftır. Bu itibarla failin sağladığı çıkarın haksız

---

[390] Toroslu, Nevzat, *Ceza Hukuku, Genel Kısım*, Ankara: Savaş Yayınevi, 2008, s.76.
[391] Nuhoğlu, Ayşe; Yenisey, Feridun ve Nurullah, Kunter, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, 17. Baskı, İstanbul: Beta Yayınları, s. 50
[392] Özbek, *TCK İzmir Şerhi,* s.68

olduğunu bilmesi de gerekir. Bir başka deyişle, burada tipikliğin unsuru olan hukuka aykırılık kastın kapsamında olmalıdır.

Bilişim sistemindeki kişisel verilerin korunması hususunda, öncelikle bu suçun oluşabilmesi için, ortada vasıta olarak kullanılan bir "bilişim sistemi" bulunmalıdır. Bu nedenle diğer unsurlarda uygulanan usulden bir miktar ayrılarak önce bilişim sisteminin anlaşılabilmesi için gerekli açıklamalar üzerinde durmakta yarar bulunmaktadır. Kişisel verilerin elde edilmesi yolu ile işlenen suçların işlenme şekli ve alanı sınırlandırılmamıştır. Özellikle bilişim alanında kullanılan elektronik cihazlardaki gelişim ve çeşitlenme bu suçun işleniş şekillerini oldukça genişletmiştir. Hareket unsuru suçun işlendiği alanın özelliğine göre değerlendirilmelidir. Bilişim ortamındaki bir verinin elde edilmesi bilgisayar, cep telefonu, oyun konsolu vb gibi yazılım kullanan cihazlar ve internet yardımı ile elde edilebilir ve suç işlenebilir. Bu nedenle öncelikle bilişim alanının tanınmasında yarar bulunmaktadır[393].

5237 sayılı TCK'nin sisteminde esas alınan suç teorisinde ise suçun unsurları üçe ayrılmaktadır. 1- Maddi Unsur, 2- Manevi Unsur, 3- Hukuka Aykırılık Unsuru. Bu sistemde, kusurluluk suçun bir unsuru değildir. Kusurluluk, işlendiği suç dolayısı ile fail hakkında bulunulan bir değerlendirme yargısıdır. Haksızlık ve kusur daima belli bir konuyla ilişkilendirilerek değerlendirmeye tabi tutulmak zorundadır. Ceza hukukunda bu değerlendirmenin konusunu ise, insan davranışları oluşturur[394]. TCK'de düzenlenen şekli ile suçun unsurlarından maddi unsur ise pozitif ve negatif unsurlar olarak ikiye ayrılır. Bunlardan pozitif unsur suçta bulunması gereken, cezalandırabilmek için mutlaka aranan unsurlardan olup bunlar, fiil, nedensellik bağı ve sonuçtur. Negatif unsur ise fiilin cezalandırılabilmesine engel olan, yani suçta bulunmaması gereken unsurlardır. Biz bunlara kısaca hukuka ulgunluk nedenleri de demekteyiz. İleride ayrıntılı olarak ela alınacak olan hukuka uygunluk nedenleri meşru müdafaa, hakkın kullanılması, ilgilinin rızası ve kanun hükmünün yerine getirilmesi olarak görünmektedir. Manevi unsurlar ise, hareketin veya ihmalin

---

[393] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s.268

[394] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s.78

mutlaka bilinçli ve iradi olmasını gerektirir. Bunlar kast ve taksir olarak adlandırılır. Kast ise isteme ve bilme unsurlarından oluşur. Taksir kasttan ayrı olarak cezalandırılmayı gerektiren fiilin istenmeden yapılması, davranış kurallarının ihlali ya da davranış kurallarına uymama şeklinde olacaktır. TCK'de hem bilişim alanındaki suçlar hem de kişisel verilerin korunmasına ilişkin suçlar ile ilgili olarak yapılan düzenlemelerdeki korunan hukuki yararın tek tek ele alınmasında konunun incelenmesi açısından gereklilik bulunmaktadır.

2.1.1. Pozitif Unsurlar

Pozitif unsurlar suçta bulunması gereken, suçun cezalandırılabilir olması içini aranan unsurlardır. Pozitif unsurlardan "Hareket" ve "Netice" mutlaka suçta bulunması gereken unsurlar olduğu halde "Nedensellik Bağı" sadece sonucu bulunan suçlarda aranan bir unsurdur. Bu unsurların inceleme konusu suç bakımından detaylı olarak araştırılması konunun aydınlatılması açısından faydalı olacaktır.

2.1.1.1. Hareket

Hareket, insanın dış dünyada beliren iradi davranışı olarak tanımlanır. Ceza hukukunda hareketin iki değişik görünüş şekli bulunur; yapmak ve yapmamak. İlkinde icrai, ikincisinde ise ihmali bir hareket söz konusudur. Kişinin iç dünyası, bir hareket ile dış dünyaya yansımadığı sürece, ceza hukukunun devreye girmesini sonuç vermez[395]. Hareketin konusunun hareketten etkilenme derecesine göre de suçları bir ayrıma tabi tutmak mümkündür. Bir suçun işlenmesiyle hareketin konusu ya zarara uğratılır ya da tehlikeye maruz bırakılır. İşte hareketin konusu üzerindeki etkinin yoğunluk derecesine göre suçları, zarar suçları ve tehlike suçları şeklinde ikiye ayırmak mümkündür. Suçun kanuni tarifinde fiilin tanımlanışına göre suçlar, tek veya çok hareketli suçlar, serbest hareketli suçlar, bağlı hareketli suçlar, seçimlik hareketli suçlar ve mütemadi suçlar olarak bir ayırıma tabi tutulabilir[396]. Hareketin konusu ile korunan hukuki değeri birbirine karıştırmamak gerekir. Ceza hukuku

[395] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.201
[396] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 163

tarafından koruma, cezalandırılmak suretiyle hukuk normları tarafından yasaklanan fiillerin toplumun bu menfaatlerini tehlikeli bir şekilde ihlal etmeye uygun olması anlamına gelir[397].

Suçun maddi unsuru içerisinde suçun işleniş şekli yönünden hareketin incelenmesi önem arz etmektedir. Suçun oluşabilmesi için ilk adım kişisel verinin ele geçirilmesi ile olacaktır. Ele geçirme ifadesi, CD, USB gibi materyaller dışında sistem yönünden yerinde değildir. Çünkü burada ele geçirme değil, bilişim sistemindeki bilgiye ulaşma ve bilginin öğrenilmiş olması söz konusudur. Bu nedenle, bu suçlar konut dokunulmazlığının elektronik ihlaline de benzetilmektedir[398].

TCK'nin 135. maddesiyle düzenlenen suçun hareket unsuru, "hukuka aykırı olarak kaydetmek" biçiminde olarak gösterilmiştir. Kişisel verilerin hukuka aykırı olarak kayda alınması, bir bilişim sistemine ya da veri taşıma aracına girilmesi şeklinde olabileceği gibi kişisel bilgilerin bir dosya kâğıdına el yazısı ya da daktilo ile geçirilmesi şeklinde de olabilecektir. Hastaneler, sendikalar, finans kurumları ve sigorta şirketleri gibi pek çok kurum kişilerin sağlık durumları, siyasal düşünceleri, DNA örnekleri ve bunun gibi kişisel özelliklerini, özellikle gizli kalması istenilen bilgileri veri halinde kaydetmekte ve saklamaktadırlar[399]. İşte bu düzenleme ile bu veriler gerek sanal ortamda gerekse yazılı ortamda kayda girerken ya da arşivlenirken kurumlar veya bireyler tarafından daha dikkatli olunması gerekecektir. 135. maddede, suçun işlenme şekli ve alanı sınırlandırılmamıştır. Kişisel verilerin hukuka aykırı olarak her türlü kayıt edilmesi fiili bu suçu oluşturmaktadır. Burada önemli olan, kayıta konu verinin olması, bu verinin gerçek kişiye ait olması, kişisel olması ve hukuka aykırı şekilde kayıt edilmesi gerekmektedir. İnceleme konusu

---

[397] Jascheck, Hans Hainrich, *Almanya Federal Cumhuriyeti Ceza hukukuna Giriş* (Çev: Feridun Yenisey; Kayıhan, İçel ve Köksal Bayraktar: Türk Ceza hukukuna İlişkin Açıklamalar), İstanbul: Beta Yayınları, 1989, s. 256.

[398] Önder, *Ceza Hukuk Genel Hükümleri,* s. 507; Değirmenci, *Bilişim Suçları*, s. 127-128; Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 129.

[399] Kişisel sağlık verileri ile ilgili ayrıntılı bilgi için; Gürbüz, Meral, "Özel Hayatın Gizliliği Bağlamında Kişisel Sağlık Verilerinin Korunması", *Legal Hukuk Dergisi,* 2015, Cilt: 13, Sayı: 149, s.69-90.

açısından fiziki metaryeller üzerine kaydedilen kişisel veriler inceleme alanı içerisinde değildir.

Bu suç için öne çıkan özellik hukuka aykırılık unsurudur. Suçun oluşması için, kişisel verilerin hukuka aykırı biçimin de kayda alınması gerekir. Bu kapsamda örneğin, adli sicil kayıtlarının, mahkumiyetlerin kaydedilmesi 5352 sayılı Adli Sicil Kanunu gereğidir. Ayrıca parmak izi ve fotoğrafların kayda alınması hususu da 2559 sayılı Polis Vazife Ve Selahiyetleri Kanununun 5. maddesiyle hüküm altına alınmıştır. Bu Kanunlara uygun olarak mahkûmiyetlerin kaydedilmesi veya parmak izlerinin ve fotoğraflarının arşivlenmesi hukuka aykırı sayılmayacaktır. Ancak, kişisel verinin kaydedilmesinin hukuka uygun sayılabilmesi için, bu konuda yetkili makama kanun tarafından verilmiş açık bir yetkinin olması gerekir. Kanun tarafından verilmiş açık bir yetki olmadan kişisel verileri kaydetmek, TCK'nin 135. maddesinde düzenlenen suçu oluşturacaktır. Bu "kaydetme" bilgisayar ortamına olabileceği gibi, fiziki ortama ilişkin de olabilir. Ancak, veri kaydetmenin gerçekleşmesi için, mutlaka bir yere bilgilerin yazılması, depolanması, saklanması veya şerh düşülmesi gerekir[400]. Bir kimsenin kişisel verileri daha sonra kullanmak üzere ezberlemesi durumu, buradaki kaydetme olarak algılanamaz[401].

Maddenin 2**.** fıkrasında suçun konusu olarak bir kısım hususlar ayrıca belirtilirken; bunlardan bir kısmının hukuka aykırı olarak kaydedilmesi özellikle vurgulanmış, diğer kısmı için böyle bir vurgu yapılmamıştır. Örneğin, kişilerin siyasi, felsefi ve dini görüşlerine, ırki kökenlerine ilişkin bilgileri kişisel veri olarak kaydeden kimsenin cezalandırılacağı vurgulanmış, bunun için eylemin hukuka uygun veya aykırı olması arasında bir fark yokmuş gibi düzenleme yapılmıştır. Böylece bu kişisel verileri hukuka uygun olarak kaydetmenin bile, TCK'nin 135. maddesinde düzenlenen suçu oluşturacağı izlenimi oluşturmuştur[402]. Kaydedilen verilerin kişinin yaşamına, mesleğine, ahlaki eğilimlerine, siyasi, felsefi veya dini görüşlerine, ırki

---

[400] Şen, Ersan, *Türk Ceza Kanunu Yorumu*, Ankara: Vedat Kitapçılık, 2006, s.603.
[401] Malkoç, İsmail, *Açıklamalı-İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu*, Ankara: Malkoç Kitapevi, 2007, Cilt: I, s. 912.
[402] Parlar ve Hatipoğlu, *Türk Ceza Kanunu Yorumu*, s. 1038.

kökenlerine ilişkin olması arasında bir fark yoktur[403]. Kanun koyucu milli güvenlik, milli savunma, kamu düzeni ve kamu güvenliğinin korunması amacıyla bir istihbarat birimine kişilerin siyasi, felsefi veya dini görüşlerine veya ırki kökenlerine ilişkin bilgileri toplama ve depolama görevi verse bile, bu suçun olaşacağını düşünmek gerekir. Bu suçun oluşması için, kişisel verisi kaydedilen kimsenin, herhangi bir zarara uğraması zorunlu değildir[404]. Salt kişisel verinin kaydedilmesiyle bu suç oluşmaktadır. Burada yeri gelmişken belirtilmesi gereken bir hususta kolluk birimleri tarafından önceden hakkında soruşturma yapılan kimselerle ilgili GBT[405] kayıtlarının tutulmasının da, bu kapsamda değerlendirilecek olmasıdır. Bu suçun oluşması için, kişisel verilerin kaydedilmesi yeterlidir. Ayrıca, bu kişisel verilerin kullanılması veya bu verilerden bir fayda sağlanması zorunlu değildir.

TCK'nin 136. maddesiyle düzenlenen suçun hareket unsuru, "hukuka aykırı olarak verme, yayma veya ele geçirme" biçiminde gösterilmiştir. Bu suç, seçimlik hareketli bir suçtur. Verme, yayma veya ele geçirme hareketlerinden birinin yapılması suçun oluşması için yeterlidir[406]. Verme, bir kimsenin elindeki bir şeyi bir diğerine aktarması; yayma, bir kimsenin elindeki bir şeyi birden fazla kimsenin bilgisine sunması, birden fazla kimseye vermesi, ulaştırması; ele geçirme ise, bir kimsenin bir başkasının elinde olan bir materyali onun rızası dışında veya rızasıyla elde etmesi anlamına gelmektedir[407]. Kanun koyucu verme ve yaymayı kişisel veriyi elinde bulunduran yönünden belirlerken, ele geçirmeyi kişisel bilgiyi elinde olmayıp sahip olmak isleyen kişi açısından ele almıştır. Örneğin, dinleme kararı sonucu kanuni yollardan elde edilen bir telefon konuşması bir başkasına ulaştırılırsa, bu

---

[403] Soysal, "Elektronik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk", s. 273.

[404] Arslan, Çetin ve Azizağaoğlu, Bahattin, *Yeni Türk Ceza Kanunu Şerhi*, Ankara: Asil Yayın Dağıtım, 2004, s. 609.

[405] GBT, hakkında yakalama, tutuklama yahut yurt dışına çıkma yasağı kararı çıkartılmış olan veya hakkında böyle bir karar bulunmamakla birlikte askeri bir suçtan dolayı (yoklama, bakaya gibi) askerlik şubesine veya birliğine teslim olması gereken kimseler hakkında tutulan bir fiştir denilebilir. Herhangi bir şekilde, gözaltına alınmış bulunan kimseler ile disiplin cezası almış bulunan kimselerin kayıtları burada yoktur. Kaynak: Forumtr, "GBT nedir", http://www.frmtr.com/hukuk/359142-gbt-nedir.html, (Erişim: 23.04.2014)

[406] Parlar ve Hatipoğlu, *Türk Ceza Kanunu Yorumu*, s. 1041

[407] Türk Dil Kurumu Sözlüğü, "Verme, Yayma ve Ele Geçirme Nedir", http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK (Erişim: 21.03.2014)

husus verme sayılacak; bu polis memuru telefon konuşmalarını gazetelere gönderilirse, bu husus yayma olarak adlandırılacak; telefon konuşması elinde olmayan kimse veri saklama memurundan bunu almak için çabalayıp, alırsa ele geçirme söz konusu olacaktır. Veren veya yayanın bu kişisel verileri hukuka uygun veya hukuka aykırı surette elde etmiş olmasının bir önemi bulunmamaktadır. Ancak, kişisel verileri hukuka aykırı olarak kaydettikten sonra bu verileri başkasına sunan kimse, hem TCK'nin 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunu, hem de aynı kanunun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak verme suçunu işlemiş olacaktır. Burada gerçek içtima hükümleri uygulanacaktır[408].

Madde metninden de anlaşılacağı gibi, bu verme, yayma veya ele geçirme eylemleri hukuka aykırı olarak gerçekleştirilmelidir. Örneğin, 5352 sayılı Adli Sicil Kanununun 7. ve 8. maddelerinde adli sicil bilgilerinin kimlere verilebileceği belirlenmiştir. Bu maddelerde belirlenen kişi veya mercilere bu bilgilerin verilmesi TCK'nin 136. maddesinde düzenlenen suçu oluşturmayacaktır. Ancak, bu bilgiler anılan hükümlerde belirlenen kişi veya mercilerden başkasına verilirse, suçun hukuka aykırılık unsuru gerçekleştiğinden anılan suç oluşacaktır[409].

TCK'nin 243/1. maddesinde düzenlenen bilişim sistemine girme suçunun hareket unsurunu, bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve orada kalmaya devam etme oluşturur. Bu suçun oluşması için icrai nitelikteki girme eyleminin ve ihmali nitelikteki sistemde kalmaya devam etme eyleminin birlikte gerçekleşmesi gerekir. Suça konu yer, bilişim sisteminin donanımı ile ilgili fiziki kısmı değil, yazılımı ile ilgili görünmeyen yeri, sanal alemi oluşturur. O halde büyük bir bilgisayar sisteminin bulunduğu odanın içine girip, orada geceleyen kimsenin eylemi bilgisayara girme kapsamında olmayacağı için bu suç kapsamında değerlendirilmeyecek belki hakkı bulunmayan yere elatma kapsamında düşünülebilecektir[410]. Failin, bilişim sisteminin bütününe veya bir kısmına girmesi ile

---

[408] Malkoç, *Açıklamalı Yeni Türk Ceza Kanunu,* s.607-608
[409] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.4126
[410] Yazıcıoğlu, "Bilişim Sistemine Girme Eylemi", s. 83

bu suç oluşur. Sistem içerisinde girişin sınırlandırıldığı bir kısma, bir bölüme girilmesi ile de anılan suç oluşur. Belirli bir kısma girilmesinin sınırlandırılması, bir bilişim sistemi içerisindeki yetkiler bakımından okuma, yazma ve çalışma yetkileri içerisinde en az okuma yetkisinin de verilmemiş olması anlamına gelir. Burada seçimlik hareketli bir suç değil, birden fazla hareketli bir suç söz konusudur. Failin yalnızca girmesi veya yalnızca orada kalması ile bu suç işlenemeyecektir. Fail bilişim sistemi üzerinde hakkı olan kimsenin rızasıyla veya hukuka uygun sayılan başka bir şekilde sisteme girmesine rağmen, süresi bitmesi veya rızanın başka nedenle kalkması nedeniyle buradan çıkması ile anılan suç oluşmayacaktır[411]. TCK'nin 243. maddesinde düzenlenen suçta seçimlik hareket yoktur. Suçun oluşumu için, bilişim sistemine haksız olarak "girme" yetmez; ayrıca sistemde "kalmaya devam etme" de gerekmektedir.

Kanunun kullandığı terminoloji açısından da sıkıntı bulunmaktadır. "girme" ile "erişim" sözcüklerinin kullanımında, bilişim sisteminin kendine özgü yapısı bakımından farklılıklar bulunmaktadır. "Girme" sözcüğü, fiziki bir yeri, alanı anlatır. Elektronik yapıdaki (sanal alemdeki) bilişim sistemine ise, girme değil, erişim söz konusudur. Özellikle, suç işleyen bakımından bu sisteme yetkisiz erişim gerçekleştirilmektedir. Kanunun girmek kelimesini kullanmıştır ancak burada girmek kelimesi, gerçek anlamda bir yere girmek olmayıp bilişim sisteminin sanal kısmını oluşturan yazılım kısmına (Softwere) tamamen veya bir kısmen erişmek, ulaşmak, veya dahil olmak anlamında kullanılmıştır. Girme eyleminde, mesafenin yakın ve uzak olması ile iletişimin kablolu veya kablosuz olması farketmez. Örneğin bir finans kuruluşunun bilgisayar ortamında tutulan kayıtlarına erişilerek, müşterilerin hesabının hukuka aykırı bir şekilde incelenmesi veya hukuka aykırı olarak bir kamu kurumunun bilişim sistemine dışarıdan erişerek, sistemdeki bazı bilgilerin incelenmesi veya açık halde bulunan kişisel bilgisayarda bir takım pencerelerin açılarak bakılması halinde anılan suçu oluşacaktır. Burada verilere ulaşımın internet vasıtasıyla uzaktan ya da bizzat verinin kayıtlı bulunduğu bilgisayardan yapılması

---

[411] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları,* s. 256; Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları,* s. 107-108

arasında fark bulunmamaktadır[412].

243. maddenin en tartışmalı yönlerinden birisini, suçun unsurlarından olan "kalmaya devam etme" konusu teşkil etmektedir. Sisteme girdikten sonra, "kalmaya devam etme" unsurunun gerçekleşmesi için ne kadar bir süre geçmesi gerektiğinin belirlenmemesi sorun oluşturmaktadır. 243. maddede, "orada kalmaya devam eden" ibaresi, "kalan" sözcüğüne göre, daha geniş bir anlam çağrıştırmaktadır. Maddede, "giren ve kalan" denilmemektedir. "Kalma" sözcüğüne göre, "kalmaya devam etme", daha nitelikli, yani daha uzun süren bir temadiyi gündeme getirmektedir. Önceden, her suç için geçerli bir kalmaya devam etme süresi belirlemek doğru bir yaklaşım olmayacaktır. Kalmaya devam etme unsuru için "yeterli süre", araştırması veya değerlendirmesi her somut olayın özelliğine göre hâkim tarafından yapılmalıdır. Bu konuda bir kıstas olarak; bilişim sistemine erişen fail, bilişim sisteminin tamamına veya bir kısmına dahil olduğunu anladığı sırada, çıkması için gerekli olan makul süre dışında, sistemde kalmış ise anılan suçu işlemiş sayılması uygulanabilir[413]. Fail girer girmez hemen çıkar ise anılan suç oluşmayacağı savunulsa[414] dahi girme eylemi ile verilerin elde edilmesi veya zarar görmesi riski oluştuğu için kalınan sürenin bir öneminin olmadığı söylenebilir. Ancak, sistemde kalmaya devam eden failin, bu aşamada yaptıkları konusunda maddede bir açıklama yer almamaktadır. Failin sistemden hemen çıkmayıp, sistemdeki bilgileri öğrenmesi halinde kalmaya devam etme gerçekleşmiş olacağına ilişkin görüşler de bulunmaktadır[415]. Sistemde kalmaya devam etmeyi, failin sistemdeki bilgileri öğrenmiş olmasına bağlamak, bu suçun işlenme alanını daraltabilir. Failin, sistemde kalmaya devam etmesi önemlidir; yoksa bu sürede sistem bilgilerini öğrenmesi gerekli değildir. Kaldı ki, failin anlık olarak girmesiyle, sistemdeki bilgileri öğrenme de mümkündür. Bu halde de "orada kalmaya devam etme" unsuru süre bakımından gerçekleşmemiş olacaktır. Failin bu

[412] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler,* Cilt:5, s.4631
[413] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler,* s.4632
[414] Meran, Necati, *Sahtecilik-Mal Varlığı-Bilişim Suçları İle Ekonomi ve Ticaret Alanında Suçlar*, Ankara: Yetkin Yayınevi, 2008, s. 565
[415] Dülger, *Bilişim Suçları*, s.218

suçu işlerken hangi amaçla hareket ettiğinin de bir önemi yoktur.[416].

Bu suç, girme ve kalmaya devam etme ile işlendiğinden, kalmaya devam edildiği anda suç tamamlanır. Ancak kalma eylemi sürdüğü sürece anılan suç da oluşmaya devam eder. Başka bir deyişle suçun bu özelliği gereği, anılan suç mütemadi suç niteliğindedir. Suç temadinin sona erdiği anda tamamlanmış sayılacaktır[417]. Ancak failin eylemi sonucu, bu konuda bir kastı olmaksızın bilişim sisteminin içerdiği veriler yok olmuş veya değişmiş ise bu durumda, maddenin birinci fıkrası değil, üçüncü fıkrası hükümleri uygulanacaktır[418]. Kişisel veriler yönünden ise bilişim sistemine girmiş ve orada kalmış olması kişisel verilerin değiştirilmesi, kaydedilmesi gibi suçlar ile bir başka suçun oluşmasına neden olursa TCK'nin ilgili maddesi uygulanacaktır.

TCK'nin 244/1. maddesinde düzenlenen eylemin hareket unsuru bir bilişim sisteminin işleyişini engellemek veya bozmak alarak belirlenmiştir. Bir bilişim sisteminin işleyişini, kendisine yönlendirilen komutlara uygun olarak veri işleme faaliyeti olarak kabul etmek gerekirse, bu faaliyetin; dışarıdan gerçekleştirilen bir müdahale ile kısmen veya tamamen önlenmesi durumu "engellenme", kendisinden beklenen işi yapamayacak şekilde kısmen veya tamamen tahrip edilmesi durumu da "bozma" olarak kabul edilmelidir[419].

Dülger**,** sistemin işleyişinin engellenmesinin sistemin çeşitli yönleriyle sürekli ya da geçici olarak iş görmesinin engellenmesi anlamına geldiği, bu bağlamda sisteme her türlü müdahalenin bu kapsamda değerlendirilmesi gerektiğini dile getirmiştir[420]. Kurt ise; bir bilişim sisteminin işleyişinin engellenmesi halinde sistemin bozulması değil ifa ettiği fonksiyonları yerine getirmesinin engellendiğini kabul etmektedir[421]. Koca'ya göre de bilişim sistemine yapılan müdahalelerle

---

[416] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 170-171
[417] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6744
[418] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s.257
[419] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 856
[420] Dülger, *Bilişim Suçları*, s.234
[421] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması,* s.164

sistemin veri işleme fonksiyonunu yerine getirmemesi halinde bilişim sisteminin engellenmesi; sistemin işlem yapabilmesini sağlayan unsurlarına yapılan müdahalelerle fonksiyonunu tamamen veya kısmen yerine getiremeyecek duruma sokulması halinde ise bozulması söz konusudur[422]. Karagülmez bir bilişim sisteminin bozulmasını sistemin tamamen çalışamaz hale gelmesi, sistemin olağan koşullarda yapması gereken işlevlerin değişikliğe uğratılması, haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılması olarak belirtmektedir[423]. Bu noktada; örneğin bir bilişim sistemine bir yazılım yerleştirilmek suretiyle o bilişim sisteminin işleyişine müdahale ediliyorsa, burada yapılması gereken değerlendirme müdahalenin etkisidir. Eğer sisteme yüklenen yazılım (örneğin bir virüs programı); bilişim sisteminin işleyişini geçici olarak kesintiye uğratmışsa engelleme, bilişim sisteminin işleyişini o an itibariyle kalıcı olarak sonlandırmışsa bozma eylemi gerçeklemiş olur. Hemen ifade etmek gerekir ki bilişim sistemi dışındaki unsurlara yapılan müdahaleler 244. madde anlamında bozma ya da engelleme olarak kabul edilemez. Örneğin, taşınabilir bilgisayarın yere atılarak kırılması, klavyenin tuşlarının parçalanması gibi durumlar mala zarar verme suçu oluşturur. Bunun yanında bilgisayarın şifresinin değiştirilerek bilgisayara girişin engellenmesi, yazılım sisteminin çökertilmesi durumunda 244/1. maddedeki suçun oluştuğu söylenebilir[424].

Ele geçirme en başta bizzat bilişim sisteminden olabilir. Bununla birlik daha önce bilgi depo edilen disket, CD, flash disk gibi şeylerin bu halleriyle elde edilmesi ile de gerçekleşebilecektir[425]. Bir başka anlatımla, suç bilişim sisteminden doğrudan ele geçirme şeklinde olabileceği gibi, daha önceden bilişim siteminden kayıtlı verilerin dolaylı olarak ele geçirilmesi şeklinde de gerçekleştirilebilir. Ancak, bu noktada, Fikir ve Sanat Eserleri Kanunu'nun hükümlerini de incelemek gerekmektedir. Kanuna göre ele geçirme, esasında yetkisiz erişilen bilişim

[422] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 93
[423] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s.188
[424] age, s. 94
[425] Dülger, *Bilişim Suçları*, s. 123

sistemindeki elektronik bilginin öğrenilmesidir[426]. Bilişim alanındaki bu suçun işlenmesi için yapılması gerekenler iki grupta toplanabilir. Birincisi bilişim yazılımlarına (programlarına) zorla girmek, ikincisi ise herhangi bir suçu işlemek için bilişimi araç olarak kullanmaktır[427]. Konumuz olan suç tipinde bir bilişim aracı olan bilgisayar fiilin aracısı olarak kullanılmaktadır. Kişisel verilerin elde edilmesi için bir kurumun bilgisayarına ya da kişisel bir bilgisayara ulaşılması için yine bilişim sisteminin bir parçası olan bilgisayarın kullanılması gerektiğinden bilişim araç olarak kullanılmaktadır.

Öte yandan, dünyada teknolojinin çok hızlı ilerlemesi, iç internet (intranet) ağlarında da özellikle resmi kurum ve şirketlerin koruma önlemlerini daha fazla artırmalarını gerekli kılmaktadır. Sanal terörizm acısından, bugün için özellikle devlet kurumlarının verilerinin güvenliğinin sağlanması için kapalı devre veri iletim ağı olarak tanımlanabilecek intranetin devlet kurumlarında kullanılması, bir yönüyle sanal terörizme karşı etkin bir yol olarak önerilmektedir. Ancak ağ büyüdükçe bu sistemin de güvenlik açıkları vermesinin kaçınılmaz olduğu vurgulanmaktadır[428]. Bir bakıma iç internet ağı ile (dünya çapındaki) dış internet ağının risk bakımından farkı kalmamıştır. İç internet ağı kullanan kuruluşların, bilişim suçlarına (yetkisiz erişimlere) karşı iyi tanımlanmış yapıda, sistematik ve güncel güvenlik paketleri kullanmaları kaçınılmazdır. Böylece, yetkisiz erişimleri engellemeleri ve ticari işlemlerini korumaları mümkün olabilecektir[429].

TCK'nin 244. maddesinin (1) numaralı fıkrasında seçimlik hareketler söz konusudur; bunlar, bilişim sisteminin işleyişini "engelleme" veya "bozmadır". Bilişim sisteminin işleyişinin engellenmesi, sistem aracılığıyla veri işleme faaliyetinin gerçekleşmesinin önlenmesi[430], çeşitli yollarla, bilişim sistemini daimi

---

[426] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 132
[427] Erdönmez, Erhan, *Investigation Of Computer Crimes*, Thesis Prepared For The Degree Of Master Of Science, University Of North Texas, August 2002, s. 13
[428] Özcan, *Siber Terörizm ve Ulusal Güvenlik,* s.335 -336
[429] Visa Public, "Incident Response Procedure For Account Compromise", www.visaasia.com/secured (Erişim: 02.07.2012), s.2.
[430] Ketizmen. *Türk Ceza Hukukunda Bilişim Suçları*, s. 129

veya geçici olarak durdurmak[431], bilişim sisteminin işleyişini geçici olarak kesintiye uğratmak[432], bilişim sisteminin geçici veya sürekli olarak çalışmasını herhangi bir şekilde kesintiye uğratmak[433], sistemin her türlü işlem görmesini engellemek[434] biçimlerinde tanımlanmıştır. Burada, sistemin işleyişi bozulmamakta, fakat gereği gibi işlemesi herhangi bir şekilde önlenmektedir[435]. Engelleme, bilişim sistemine her türlü müdahale edilmesi, sisteme zararlı ve işleyişi engelleyici bir yazılımın yerleştirilmesi, sistemi şifreleme veya mevcut şifrenin değiştirilmesi vb. hareketlerle yapılabilir[436]. Bir kısım yazarlar tarafından engellemenin sistemin ancak geçici olarak devre dışı bırakılması halini kapsadığı kabul edilse dahi, genel kabul engellemenin geçici veya sürekli olmasının sonuca etkili olmadığı yönündedir[437].

Bilişim sisteminin bozulması ise yapılacak bir saldırı ile sistemi tamamen yok etmek veya artık yararlanamaz hale getirmek[438], haksız müdahale ile sistemin sağlıklı işleyişini geçici veya sürekli olarak ortadan kaldırmak, sistemin işleyişini sağlıksız hale getirmek[439], kalıcı şekilde sistemden istifade edilmesini engellemek[440], sistemin normal koşullarda yapması gereken işlevlerinin değişikliğe uğratılması[441], sistemin veri işleme faaliyeti yapamayacak hale getirilmesi[442] biçimlerinde tanımlanmıştır. Sistemin işleyişi, sistemin genel çalışma sistemine yapılacak bir müdahale ile bozulabileceği gibi, sistemin bir kısmına veya içerdiği verilere yapılan bir müdahale ile de bozulabilir, sistemde yer alan verilere yapılan müdahaleler, sistemin işleyişini engellemiş veya bozmuş ise maddenin birinci fıkrası, bu müdahale sistemin işleyişini değil, sadece verileri bozmuş veya engellemiş ise, ikinci fıkrası hükümleri uygulanır[443]. Yine bilişim sistemine virüs gönderilmesi, yazılım sisteminin

---

[431] Dönmezer**,** *Kişilere ve Mala Karşı Cürümler*, İstanbul: Beta Yayınları, 2004, s. 623
[432] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler,* s.4661
[433] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 187
[434] Meran, Sahtecilik-Mal Varlığı-Bilişim Suçları İle Ekonomi ve Ticaret Alanında Suçlar, s.571
[435] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 187
[436] Meran, *Sahtecilik-Mal Varlığı-Bilişim Suçları İle Ekonomi ve Ticaret Alanında Suçlar*, s.571
[437] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler,* s.4661
[438] Dönmezer**,** *Kişilere ve Mala Karşı Cürümler,* s. 623
[439] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 188
[440] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler*, s.4661
[441] Meran, *Sahtecilik-Mal Varlığı-Bilişim Suçları İle Ekonomi ve Ticaret Alanında Suçlar*, s.571
[442] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler*, s.4661
[443] age, s.4662

çökertilmesi, sistemin işlemez hale getirilmesi, donmasının sağlanması gibi hareketlerle bu fıkrada düzenlenen suç işlenebilir[444].

Bu suç serbest hareketli bir suçtur, engelleme veya bozma eyleminin hangi hareketlerle yapılmış olduğunun herhangi bir önemi bulunmamaktadır. Ayrıca bu eylemlerden ikisi birlikte gerçekleştirilmiş olsa bile, eylem tek suç oluşturmaya devam edecektir. Ayrıca bu suç bir zarar suçudur, bilişim sisteminin işleyişinin engellenmesi veya bozulması ile tamamlanır, bu nedenle engelleme ve bozulma tehlikesi yaratılmış olması suçun tamamlanması için yeterli değildir[445]. Avrupa Konseyi Siber Suç Sözleşmesi'nin "Sistemin bütünlüğünün ihlâli" başlıklı 5. maddesinde, "Her taraf, iç hukukuna uygun olarak, bilişim verilerinin girilmesi, nakledilmesi, bozulması, silinmesi, tahrip edilmesi, ortadan kaldırılması suretiyle bir bilişim sisteminin işletilmesine kasten ve haksız olarak engel olunmasını suç haline getirmek için gerekli görülen kanuni tedbirleri ve diğer tedbirleri kabul eder"[446] denilmektedir. Sözleşmenin 5. maddesinde ayrıntılı şekilde belirtildiği üzere, bilişim sisteminin işleyişinin engellenmesi; sisteme bilişim verilerinin girilmesi, nakledilmesi, bozulması, silinmesi, tahrip edilmesi, ortadan kaldırılması suretiyle olabilmektedir. Buradaki seçimlik hareketler, sonuçta sistemin işleyişini engellemektedir.

TCK'nin 244. maddesinin 2. fıkrasında, "bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır." hükmüne yer vermiştir. Maddedeki 1. fıkrada, daha fazla ceza öngörülerek daha önemli görülen doğrudan bilişim sisteminin işleyişinin engellenmesi veya bozulması fiilleri karşısında, 2. fıkradaki suçun, bilişim sisteminin işleyişini engelleme ya da bozmaya ulaşmayan seviyede olması gerektiği anlaşılmaktadır. Bir başka anlatımla, 2 numaralı fıkradaki, bilişim sistemindeki

---

[444] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 94
[445] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6759
[446] Aksoy, Eylem, "Avrupa Konseyi Siber Suçluluk Sözleşmesi", İstanbul: *Galata Saray Üniversitesi Hukuk Fakültesi Dergisi*, Sayı 1, 2002. s. 872

verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme veya verileri başka yere gönderme seçimlik hareketleriyle, bilişim sisteminin işleyişi engellenmiş veya sistemin işleyişi bozulmuş ise bu takdirde, 2 numaralı fıkrayı değil, 1 numaralı fıkrayı uygulamak gerekmektedir[447].

Söz konusu fıkradaki hareketler de, TCK'nin 244/1 'de olduğu gibi seçimlik hareketlerdir ve sadece birinin gerçekleşmesi halinde suç tamamlanmış sayılır. Bu çerçevede fıkrada düzenlenmiş ilk seçimlik hareket "verinin bozulmasıdır." Verinin bozulması, verinin içeriğine ya da yapısına müdahale suretiyle verinin kısmen ya da tamamen kullanılamayacak hale gelmesidir[448]. Bu durumda artık mevcut veriden amaçlanan veya planlanan faydanın elde edilememesi durumu söz konusudur[449]. Bu suç kapsamındaki bir diğer seçimlik hareket ise bilişim sistemi içerisindeki "verinin yok edilmesidir". Dülger'e göre "verinin yok edilmesi" bilişim sistemi açısından sözlük anlamından farklı bir kapsama sahiptir. Yazara göre verinin yok olması demek, söz konusu veriye erişimin engellenmesi anlamına gelmektedir[450]. Kurt ise; verinin yok edilmesinin veriye bir daha ulaşılamaması anlamına geldiğini belirterek kavrama daha dar bir anlam yüklemektedir. Kurt, bu hususta da, verinin yok edilmesinin veriye bir daha ulaşılamaması anlamına geldiğini ifade ederek, verinin silinmesinin yukarıda aktarıldığı şekliyle verinin yok edilmesi anlamına gelmediğini, 244. maddenin 1. fıkrasında düzenlenen verinin erişilmez kılınması şeklindeki diğer bir hareketi oluşturduğunu ifade etmektedir[451]. Ketizmen'de; verinin yok edilmesinin, verinin varlığına son verilmesi, ortadan kaldırılması ve verinin tamamen ya da büyük güçlüklerle elde edebilecek şekilde tasarrufundan çıkartılması olarak tanımlandığında, verinin silinmesinin de verinin yok edilmesi olarak değerlendirilebileceğini kabul etmiştir[452]. Bu bağlamda yazar verinin teknik olarak tekrar edilebilmesi olanağı ya da olasılığının varlığından dolayı verinin silinmesinin, verinin yok edilmesi kapsamı dışında tutulabilmesine ilişkin gerekçeyi kabul

[447] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 189
[448] Dülger**,** *Bilişim Suçları*, s.235, Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s.139, Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu,* s. 6759.
[449] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 6760.
[450] Dülger**,** *Bilişim Suçları*, s.235
[451] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması,* s. 168
[452] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s.139

etmemektedir. Koca'ya göre ise verinin yok edilmesi verinin ortadan kaldırılması anlamına gelir[453]. Bu anlamda yok etme verinin silinmesini de içerir. Burada önemli olan verinin mağdurun tasarruf alanından çıkartılmış olması ve normal yollardan ulaşılmasının güçleştirilmesidir[454].

Verinin yok edilmesinden anlaşılması gereken, söz konusu verinin kayıtlı olduğu bellekten silinmesi suretiyle erişiminin mümkün olmaktan çıkarılmasıdır. Bu çerçevede bir veriye erişimin engellenmesi, o verinin yok edildiği anlamına gelmez. Ayrıca Ketizmen'inde ifade ettiği gibi, bir verinin kayıtlı olduğu bellekten kesin bir şekilde, geriye dönüşü imkânsız olarak yok edilmesi söz konusu değildir. Bu anlamda verinin yok edilmesini, genel bir bakış açısıyla, o veriye erişim için verilen komutun sonuçsuz kalmasına neden olacak şekilde kayıtlardan silinmesi olarak ifade etmek yerinde olacaktır. Bu çerçevede veriye tekrar ulaşabilme imkanının varlığı suçun oluşmasını engellemez.

Bir diğer seçimlik hareket ise "verinin değiştirilmesi veya erişilmez kılınmasıdır." Burada verinin değiştirilmesinden kastedilen şey, bir verinin bulundurulma ve kullanma amacı dışında, başka bir formata dönüştürülmesidir[455]. Verinin erişilmez kılınması ise, genel olarak verinin içerdiği bilgi ya da enformasyona müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup, burada veri içerik bakımından bütünlüğünü korumaktadır. Veri ne yok edilmekte ne de bozulmakta fakat verilere ulaşım için gereken işlem bağı koparılmakladır. Örneğin sisteme yönlendirilen virüs saldırıları ile bunun gerçekleştirilmesi mümkündür[456]. Bunun dışında TCK'nin 244/1. maddesinin düzenlenişi bakımından; bu virüs saldırıları bir bütün olarak bilişim sistemin işleyişine yönelik bir saldırı niteliğinde olması halinde, sistemin işleyişinin engellenmesi ve kimi durumlarda da işleyişinin bozulması söz konusu olacağından burada sisteme yönelik saldırılar sonucunda veriye erişilememesi halinin 1. fıkra

---

[453] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 94
[454] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.861
[455] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s.139, Dülger**,** *Bilişim Suçları*, s.237, Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 6760.
[456] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.861

kapsamında olduğunu söylemek mümkündür. Veriye erişilmesi bakımından erişimin engellenmesinin geçici ya da daimi olması arasında bir fark yoktur[457].

Bu fıkra hükmü kapsamında yer alan seçimlik hareketten en tartışmalı olanlardan biri "sistem içerisindeki verinin başka bir yere gönderilmesidir." Her şeyden önce kanun koyucu bu seçimlik hareketi çok muğlak olarak düzenlemiş ve gerçek amacını ortaya koyamamıştır. Çünkü bir bilişim sisteminde gerçekleşecek her türlü işlem için mutlak suretle bir veri iletimi gerçekleşmek zorundadır. Bunun en basit bir komut veya kompleks bir işlem olması arasında bir fark yoktur. Veri iletiminden maksat da kanun koyucunun TCK'nin 244/2'de kabul ettiği anlamda sistem içerisindeki verinin başka bir yere gönderilmesi olarak düşünülebilir[458]. Fakat bir ağ aracılığı ile bilgisayarlar arası kurulan her türlü iletişim bir veri aktarımını zorunlu kılar. Bir "e-mail" ya da eş zamanlı çoklu ortam yaratılarak gerçekleştirilen sohbetler, haber veya bir konu üzerine tartışma sayfasına yüklenen görüşler, paylaşım sitelerine gönderilen videolar ve hatta daha sonra özellikle üzerinde durulacağı üzere internet üzerinden gerçekleştirilen bankacılık hizmetleri de bir veri aktarımı esasına dayanmaktadır. Bu yönüyle bu düzenleme suçun sınırlarını çizme yönünden yetersiz kalmaktadır. Denilebilir ki burada kanun koyucu bilişim sistemini değil bilgisayarı merkeze alarak bu düzenlemeyi yapmış gibi görünmektedir. Bununla beraber farklı bir problemli nokta daha dikkati çekmektedir. Ketizmen'e göre, verinin başka bir yere gönderilmesi verinin aslının veya kopyasının transfer edilmesidir. Verinin kopyalanması verinin çoğaltılması anlamına gelmektedir[459]. Verinin çoğaltılması ise verinin kendisine, verinin kullanımı ya da erişebilirliği açısından herhangi bir etkide bulunmayacak bir harekettir. Bu durumda verinin aslının bilişim sistemi içerisinde kalması halinde sistem içerisindeki veriye yönelik herhangi olumsuz bir hareketin gerçekleşmediği anlamına gelmektedir. Bu durum ise maddenin düzenleniş amacı ile bağdaşmamaktadır. Yine Ketizmen'e göre, bu kapsamda verinin başka bir yere gönderilmesinin yine verinin bütünlüğünü bozmayan fakat sistem içerisindeki veriye erişimi zorlaştıran bir hareket olarak dar

---

[457] Dülger**,** *Bilişim Suçları,* s.237
[458] Yaycı, *Bilişim Suçları,* s. 92, Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması,* s. 170
[459] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s.140

yorumlanabilmesi, bu haliyle de veriye erişimin engellenmesi kapsamına girebilecek bir olasılığın maddede ayrıca düzenlendiği sonucuna varılabilmesi mümkündür[460].

244. maddenin (2) numaralı fıkrası, Siber Suç Sözleşmesi'nin "Veriye Müdahale" başlıklı 4. maddesindeki, "1 - Her bir taraf devlet, bir kimsenin bilgisayar verisine hakkı olmadığı halde, bilerek ve isteyerek zarar verme, silme, bozma, değiştirmeye ya da ortadan kaldırma fiilleri işlemesini suç olarak düzenlemek üzere gerekli kanuni düzenlemeyi yapmalı ve gerekli diğer önlemleri almalıdır. 2- Taraf devlet 1. paragrafta belirtilen durumun oluşmasını ciddi zarar oluşma olasılığına bağlı tutma hakkına sahiptir"[461] hükmüyle, paralel görünmektedir. TCK'nin 244/4. maddesine göre, bir kimsenin bilişim sisteminin işleyişini engelleyerek ya da bozarak ya da bilişim sistemi içindeki verileri bozarak, yok ederek, değiştirerek, erişilmez kılarak, sisteme veri yerleştirerek, var olan verileri başka bir yere göndererek, kendisinin veya başkasının yararına haksız bir çıkar sağlaması durumunda, eylem başka bir suçu oluşturmamakta ise, bu maddeye göre cezalandırılır. Burada söylenecek ilk husus, bu suçun işlenebilmesi için öncelikle failin, birinci veya ikinci fıkrada düzenlenen eylemlerden birisini gerçekleştirmesi gerekir. Burada failin birinci veya ikinci fıkrada belirlenen eylemlerden yalnız birisini gerçekleştirmesi, suçun oluşması için yeterlidir, birden fazlasını gerçekleştirmesine gerek yoktur. Ayrıca failin bu eylemleri gerçekleştirdikten sonra, kendisi veya başkası yararına haksız bir çıkar sağlaması gerekir[462]. Çıkarın mutlaka maddi olması şart değildir, herhangi bir yarar, bu arada manevi bir yarar da çıkar kapsamına dahildir. Örneğin bir öğrencinin bilişim sistemi aracılığıyla notlarını olduğundan daha fazla göstermesi durumunda, yarar manevi olmakla birlikte çıkar hususu gerçekleşmiş sayılmalıdır[463]. Anılan suç bu özelliği gereği, TCK'nin 42. maddesinde düzenlenen bileşik (mürekkep) suç niteliğindedir. Burada birinci ve ikinci fıkrada düzenlenen suçlar, üçüncü fıkrada düzenlenen suçun, unsuru haline gelmiştir. Ancak dördüncü fıkradaki suçun oluşabilmesi için, failin bu hareketleri, kendisi veya başkası için haksız bir

[460] age, s.142
[461] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s.297
[462] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6763
[463] Parlar ve Hatipoglu, *Türk Ceza Kanunu Yorumu,* s. 1703

çıkar sağlamak amacıyla yapmış olması gerekir[464]. Elde edilen bu çıkarın haksız olması gerekir. Hukuken tasvip edilmeyen her türlü menfaat, haksız çıkar kavramı içinde mütalaa edilebilir[465]. O halde, failin elde ettiği bu çıkar, haklı olarak elde edilmiş bir çıkar ise, anılan suç oluşmayacaktır. Bu suçun oluşması için, failin haksız bir çıkar sağlaması yeterlidir, bu eylem sonucu, bilişim sistemi üzerinde hak sahibi olan kimsenin veya bir başkasının zarar görmesine gerek yoktur veya mağdurun zarar görmesi bu fıkranın uygulanması için zorunlu değildir[466]. Ancak genellikle failin, yararına, mağdurun zararına olmaktadır.

Bu fıkrada düzenlenen suçun tamamlanabilmesi için, haksız çıkarın sağlanmış olması gerekir. Failin, birinci ve ikinci fıkrada tanımlanan eylemleri yapmasına karşın çıkar sağlanmamış, elde edilememiş ise, anılan suç teşebbüs aşamasında kalmış sayılacaktır. Burada haksız çıkarın failin zilyetliğine girmesi ile suç tamamlanır, bizzat ve fiziken elde etmiş olmasına gerek yoktur. Bu haksız çıkarın failin kendisi veya bir başkası için sağlamış olması, suçun oluşumu açısından fark etmez, önemli olan failin eylemi sonucu, bir çıkar elde edilmiş olmasıdır. Ancak bu çıkar mağdurun rızası olmamasına karşın, mağdurun yararına yapılmış ise, anılan suçun çıkar sağlama unsuru gerçekleşmeyecek, hatta çıkar da haksız sayılmayacaktır[467]. Bu suçtan söz edebilmek için, kişilere karşı herhangi bir hileli hareketin kullanılmaması gerekir, bilişim sistemine karşı hile kullanılması bu suç kapsamında değerlendirilecek iken, kişilere karşı hile kullanarak yarar sağlanması durumunda, dolandırıcılık suçu gündeme gelecektir.

Bu fıkranın uygulanabilmesi için son şart ise, failin eyleminin başka bir suçu oluşturmamasıdır. Her ne kadar madde gerekçesinde "daha ağır cezayı gerektiren başka suçtan" söz edilmekte ise de, madde metni çok açık olduğundan artık bu başka suçun ağır veya hafif cezayı gerektirmesine bakılmadan, özel bir düzenleme var ise o

---

[464] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6763
[465] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 94
[466] Malkoç, *Açıklamalı YeniTürk Ceza Kanunu*, s. 1682
[467] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6763

hüküm uygulanacaktır[468]. Başka bir deyişle fail, eylemi ile başka bir suçun, örneğin hırsızlık, dolandırıcılık, güveni kötüye kullanma veya zimmet gibi bir suçun oluşumuna sebep olmuş ise, artık bu madde uyarınca değil, o suçun düzenlendiği madde uyarınca cezalandırılacaktır[469]. O halde TCK'nin 244. maddesinin dördüncü fıkrasındaki kural tali norm niteliğindedir. Asli norm sayılan hükümlerin uygulandığı durumlarda, bu madde hükmü artık uygulanamaz.

2.1.1.2. Netice

Bilişim sistemi kullanılarak kişisel verilerin elde edilmesi ve kullanılması yolu ile işlenen suçlarda netice önemlidir. Suçun meydana gelmesi için yapılan fiilin aşamaları TCK'de suç olarak vasıflandırıldığından fiilin bir başka suçu oluşturması ihtimali oldu gibi teşebbüs aşaması olarak da değerlendirilmesi mümkündür. Netice icra edilen fiilin dış dünyada meydana getirdiği değişikliktir. Ancak, bu şekilde meydana gelen her değişiklik suçu oluşturmaz, sadece suçun kanuni tarifinde unsur olarak yer alan değişiklikler ceza hukuk açısından önem taşımaktadır[470]. Suçun maddi unsurlarından olan sonuç eylemin bir alt unsuru olmayıp, eylemden ayrı, suçun maddi unsurlarından birini oluşturur. Netice bazen zarar, bazen de tehlike şeklinde ortaya çıkar. Bunu kanuni tip belirler. Ancak neticenin gözle görülür olması da gerekmez. Bir zarar tehlikesinin bulunması da neticenin varlığı için yeterlidir. Neticesiz suç yoktur. Neticenin maddi olarak ortaya çıkmaması o suçu neticesiz hale getirmez. Tehlike de bir neticedir. Bu anlamda hareketin olası sonuçları da netice kavramı içerisinde kabul edilmelidir[471]. Çoğu suçlar açısından fiilin icra edilmesiyle suç tamamlanmaktadır. Bu suçlara doktrinde "sırf hareket suçları" denilmektedir[472]. Kanuni tanımda hareketten ayrı olarak, hareketin konusu üzerinde, ondan yer ve

---

[468] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 193-194, Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları,* s. 177

[469] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları,* s.276

[470] İçel, Kayıhan; Sokullu – Akıncı, Füsun; Özgenç, İzzet; Sözüer, Adem; Mahmutoğlu, Fatih Selami ve Ünver, Yener, *Suç Teorisi. Suç Kavramına İlişkin Genel Bilgiler, Suçun Yapısal Unsurları, Suçun Özel Oluşum Biçimleri*, 2. Kitap, İstanbul: Beta Yayınları. 2004, s. 66 ve 67

[471] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler* s.214

[472] Dönmezer, Sulhi ve Erman, Sahir, *Nazari ve Tatbiki Ceza Hukuku*, Cilt: I, 12. Baskı, İstanbul: Beta Yayınları, 1997, s. 516

zaman olarak ayrılabilen bir etkiyi gerektiren, yani kanuni tanımda, dış dünyada hareketten ayrılabilen bir neticenin meydana gelmesinin arandığı bu tür suçlara doktrinde "neticeli suçlar" denilmektedir[473]. Bu ayırımın önemi suçun işlendiği yer ve zaman ile teşebbüs bakımından önemlidir[474].

TCK'nin 135. maddesinde düzenlenen suçun oluşması için, kişisel verisi kaydedilen kimsenin, herhangi bir zarara uğraması zorunlu değildir. Kişisel verinin kaydedilmesiyle bu suç oluşmaktadır[475]. Örneğin, kişilerin sağlık bilgilerinin hastanelerce tutulması, kişilerin ekonomik, sosyal ve diğer özelliklerinin emniyet tarafından kayıt altına alınması, kişilerin özgeçmişlerinin ve görüntülerinin istihbarat birimlerince kaydedilmesi, genetik bilgilerinin Sağlık Bakanlığı tarafından kaydedilmesi kolluk birimleri tarafından önceden hakkında soruşturma yapılan kimselerle ilgili kayıtların tutulması kişisel verilerin kaydedilmesi anlamında olmakla beraber hukuka uygunluk nedenlerinin bulunup bulunmadığının araştırılması gerekir. Yani bu suçun oluşması için, kişisel verilerin kaydedilmesi yeterlidir. Ayrıca, bu kişisel verilerin kullanılması veya bu verilerden bir fayda sağlanması zorunlu değildir.

Bu açıklamalara göre bu suç neticesi bakımından ani bir suçtur; kaydedilme ile tamamlanır. Bunun için belli bir süre geçmiş olması, kişisel verinin belli bir süre kayıtlı bulunması şart değildir. Bu yönüyle suç kesintisiz (mütemadi) bir nitelik taşımaz. Suç neticesi harekete bitişik olduğundan kişisel veri hukuka aykırı kaydedilmekle tamamlanır ve suç bu yönüyle kural olarak teşebbüse elverişli değildir. Suçun tamamlanmış sayılması için kişisel verinin hukuka aykırı olarak kaydedilmesi yeterlidir; bundan bir zarar doğmasının şart olmadığı için suç bir tehlike suçudur. Suç tipinde hareketin bir tehlike yaratabilecek nitelikte olması gerektiğine ilişkin düzenlemenin yer almaması suçun soyut tehlike suçu olarak kabul edilmesi sonucunu ortaya çıkarır[476]. Kişisel verilerin hukuka uygun şekilde bilgisayar ortamındaki veri kütüğüne kaydedilmesi ve böylece veri tabanı oluşturulması

---

[473] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler,* s. 116
[474] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.215
[475] Parlar ve Hatipoglu, *Türk Ceza Kanunu Yorumu*, s. 1037
[476] Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s.520

mümkündür. Yeter ki kanun izin versin veya ilgili rıza göstersin. Kişinin parmak izi, fiziki özellikleri, kimlik bilgileri, sosyal ve iktisadi durumu, telefon numaraları, sağlık durumu gibi bilgilerin bilgisayar ortamına kaydında olduğu gibi. Bir veri tabanı oluşturularak, numaraları gösteren telefon görüşme kayıtlarının tutulması da yine kişisel verilerin kayıt altına alınması kapsamına girecektir. Bunun için ortada bir hukuka uygunluk sebebinin ve verileri kullanma amacının dışına çıkılması gerekir[477].

TCK'nin 136. maddesinde düzenlenen "Veriler hukuka aykırı olarak verme veya ele geçirme suçu" ise sırf hareket suçu olarak düzenlenmiştir. Söz konusu hareketlerin gerçekleştirilmesiyle suç da tamamlanmış olur. Suç kesintisiz bir nitelik taşımaz. Özellikle ele geçirme fiili bakımından ele geçirildikten sonra belli bir sürenin geçmesi, verinin bir süre saklanması şart değildir. Veri hukuka aykırı olarak ele geçirilmekle tamamlanmış olur. Bu yönüyle suç neticesi bakımından ani bir suçtur[478]. Suçun tamamlanmış sayılması için kişisel verinin hukuka aykırı olarak verilmesi, yayılması ya da ele geçirilmesi yeterlidir; bundan bir zarar doğması da şart değildir[479]. Bu nedenle suç bir tehlike suçudur. Suç tipinde hareket ile tehlike neticesi arasında bir nedensel ilişkinin varlığını araştırmak yönünde zorunluluk bulunduğuna ilişkin ifade yer almaması, suçun soyut tehlike suçu olarak kabul edilmesi sonucunu ortaya çıkartır[480].

TCK'nin 243. maddesinde düzenlenen bilişim sistemine girme suçu kapsamında iki ayrı suç yer almaktadır. Bunlardan birincisi 1. fıkrada düzenlenen ve maddeye adını veren bilişim sistemine girme ve orada kalma suçu bir diğeri ise 3. fıkrada düzenlenen bilişim sistemindeki verilerin yok edilmesi veya değiştirilmesi suçudur. Her ne kadar öğretide 3. fıkrada düzenlenen hal bir nitelikli hal yani ağırlaştırıcı sebep olarak gösterilse de ortaya çıkan netice aslında neticesi sebebiyle ağırlaşan bir suça vücut vermektedir[481]. Bilindiği üzere neticesi sebebiyle ağırlaşan suçlarda, kasten işlenmiş temel suç tipi yanında onun işlenmesiyle sebep olunan

[477] Soyaslan, *Ceza Hukuk Özel Hükümler*, s. 342
[478] Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s.527
[479] Taşdemir, *Bilişim-Banka veya Kredi Kartlannın Kötüye Kullanılması-Dolandıncılık Suçları*, s. 261
[480] Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s.528
[481] Parlar, *Türk Ceza Kanunu Yorumu,* s. 3746

başka veya daha ağır bir netice mevcuttur. Bu açıdan neticesi sebebiyle ağırlaşan suçlarda aslında temel suçta tipik olarak yer alan tehlike gerçekleşir. Diğer bir deyişle, ağır veya başka neticenin gerçekleşme tehlikesi temel suçun içinde yer alır[482]. Bu açıklamalar ışığında TCK'nin 243/1. maddesine bakıldığında, bilişim sistemine girildikten ve orada kalındıktan sonra verilerin yok olması veya değişmesi, temel suç tipi olan bilişim sistemine girme ve orada kalma içinde yer alan bir tehlikedir ve bu tehlike temel suç tipinin gerçekleşmesiyle ortaya çıkmıştır. Bu nedenle TCK 243/3. maddesi ayrı bir suç olarak değerlendirilebilir[483]. Bu nedenle 243. maddenin 1. ve 3. maddelerini ayrı ayrı ele almak incelemeyi kolaylaştıracaktır.

Bir bilişim sistemine kısmen veya tamamen hukuka aykırı olarak girme ve orada kalmaya devam etme eylemini ikiye ayırarak incelemek mümkündür. Bunlardan birincisi bilişim sistemine girme diğeri ise orada kalmaya devam etmedir. Maddenin kapsamı anlamında "girmek" kavramı, Türkçeye "erişim" olarak çevrilen "access" teriminin karşılığıdır[484]. Bilişim sistemine hukuka aykırı olarak girmek tabiriyle ifade edilmek istenen, bilişim sisteminin çalışmasıyla oluşan sanal alana girmektir. Hukuka aykırı olarak bir bilişim sistemine girmenin, TCK'nin 243/1. maddede düzenlenen suçu oluşturabilmesi için öncelikle ilgili bilişim sistemine erişimin sınırlandırılmış olması gerekmektedir[485]. Belirtilen sınırlandırma ile kastedilen, bilişim sisteminin ancak, işlem yapma yetkisi bulunanlarca gerçekleştirilmesidir. Bu doğrultuda, bilişim sistemine girmeye yetkili bir kullanıcının kendi kullanıcı hesabı dışında sisteme girmesi bakımından ölçüt, sistem içerisindeki kısımlara giriş konusunda kullanıcılar arasında bir sınırlandırma ve de farklılık yaratılıp yaratılmadığıdır. Özellikle okuma yetkisi ile ilgili olarak bir sınırlandırma ve farklılık yaratılmış olması halinde, kullanıcı düzeyi ne olursa olsun, girişi sınırlandırılmış bölüme girilmesi hukuka aykırı olacaktır[486]. Diğer bir anlatımla herkesin istediği her an erişilebildiği bilişim sistemleri TCK'nin 243/1. maddenin

---

[482] Gençay, Meriç, "Neticesi Sebebiyle Ağırlaşmış Suçlar", http://www.turkhukuksitesi.com/makale_1393.htm, (Erişim: 29.09.2014)
[483] Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s.842
[484] Çölkesen, Rifat ve Ören, Bülent, *Bilgisayar Haberleşmesi ve Ağ Teknolojileri*, İstanbul: Papatya Yayınevi, 2003, s.390
[485] Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s.843
[486] Ketizmen, *Türk Ceza hukuknda Bilişim Suçları*, s. 126

konusunu teşkil etmemektedir. Bugün yetkiyle erişim hem özel hemde kurumsal web sitelerinde çok sık kullanılan yapılardır[487]. Örneğin, kişisel e-posta adresleri, bankaların internet bankacılığı, öğretmenlerin e-okul uygulaması çerçevesinde öğrencilere ilişkin tuttuğu not vb. gibi kişisel bilgiler kullanıcı adı ve parola girilerek erişimin sağlanabildiği ve açıklanan kapsamdaki programlardır. Bu tür durumlarda bahsi geçen sisteme erişmek ve sistemi işletmek sadece bu yönde yetki almış kullanıcılara özgülenmiştir. Bir bakıma erişim sınırlandırılmıştır.

Burada dikkat edilmesi gereken bir konuda bilişim sistemi içinde kalmaya devam etme eylemidir. TCK'nin 243/1. maddesi bakımından, bir bilişim sistemine hukuka aykırı olarak girilmesinin suç teşkil etmesi için, hareketin ikinci kısmının yani "erişilen bilişim sisteminde, kalmaya devam etmek" gerekmektedir. Başka bir anlatımla TCK'nin 243/1. maddesinde düzenlenen suçun gerçekleşmesi için sadece sistemin bütününe ya da bir kısmına hukuka aykırı olarak girme yeterli olmamakta, sistemde kalınmaya devam edilmesi de gerekmektedir[488]. Bu düzenleme ile "sistemde kalmaya devam etmek" ile "bilişim sistemine hukuka aykırı olarak girmek" tek bir hareketin iki unsuru haline getirilmiştir. Bilişim sistemine girme ve orada kalmaya devam etmenin birbirinden bağımsız iki farklı hareketi oluşturmadığının kabul edilmesi halinde, maddede düzenlenen suç mütemadi (kesintisiz) bir suç olarak kabul edilecektir. Bu durumda sisteme girme sonrasında, sistemde kalmaya devam edilmesi şart koşulduğu takdirde, suçun tamamlanmış sayılabilmesinin belirli bir sürenin aranmasını da beraberinde getirecektir[489]. Düzenlemenin bu haliyle suçun neticesiz bir suç olduğu söylenebilir. Yani, 243/1. maddede suçun neticesi üzerinde durulmamıştır. Bir başka anlatımla, bu suçta netice değil, hareketin niteliği ve istenilen süreci, yani yeterli süreyi tamamlaması önemlidir. Bu nedenle, maddeye uygun hareketin sonuçları bu maddede dikkate alınmamıştır[490]. Suç tipine uygun hareketin gerçekleşmesinden sonra suç tamamlanmaktadır. Bu yüzden, suçun oluşması için, neticeye değil, harekete

[487] Dülger, *Bilişim Suçları*, s. 217
[488] Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s.845
[489] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 168
[490] 243. madde gerekçesi, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, (Erişim: 29.09.2014)

bakılması gerekir. Sanığın eylemi sırasında, suçun konusunu oluşturan sistemden bir takım şeyler öğrenmiş olması veya öğrenmemiş olması, bu suçta etkili değildir; ancak, eylem sürecinde sanık, sistemin içerisindeki verilerin yok olmasına veya değişmesine neden olmuşsa koşulları varsa 243. maddenin (3) numaralı fıkrasındaki suçun nitelikli halinden hüküm verilir[491]. Suçun bu şekli, bir hareket suçu niteliği taşımaktadır. Bu anlamda suçun oluşması için bir neticenin meydana gelmesi şart değildir. Hatta bir tehlikenin meydana gelip gelmediğinin belirlenmesi yönünde tipte bu açıklık bulunmadığına göre suçun bu şeklinin soyut tehlike suçu olduğu söylenmelidir[492].

Suçun oluşması için sisteme girmek ve orada kalmaya devam etmek zorunlu olduğundan suçun birden fazla hareketli bir suç olduğu söylenmelidir. Öte yandan suç serbest hareketlidir. Zira tipte suçu meydana getiren hareket tanımlanmış değildir. O halde girme ve kalma herhangi bir hareketle gerçekleştirilebilir. Örneğin bluetooth ile ya da kablolu erişim gibi. Bilişim sistemine yetkisiz erişimle suç gerçekleşmediği için, neticesi harekete bitişik bir suç söz konusu değildir. Yetkisiz erişimden sonra sistemde kalmaya devametme unsuru nedeniyle, burada temadi niteliğinde bir suç söz konusudur[493]. Karagülmez'e göre, madde metninde yer alan "orada kalmaya devam eden" ifadesinin "kalan" ifadesinden daha geniş bir anlamı çağrıştırmaktadır. Yazar "kalmaya devam etmenin", "kalmaya " göre daha nitelikli olduğunu, daha uzun süren bir temadiyi işaret ettiğini ve sonrasında kalmaya devam etme unsuru için yeterli süre araştırmasının her somut olayın özelliğine göre belirlenmesi gerektiğini savunmaktadır[494]. "Kurt" ise, sisteme girdikten sonra orada kalmaya devam etmenin sisteme giren failin sistem içerisinde bir süre kalması şeklinde gerçekleşebileceğini belirtmiştir. Bu süre zarfı içerisinde yetkisiz erişimi sağlayan fail sistem içerisindeki verileri kontrol edebilir, veri akışını izleyebilir, veriler üzerinde oynama yapabilir veya sistemi bozmaya yönelik işlemler yapabilir

[491] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 171
[492] Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s.846
[493] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s.171
[494] age, s.168-169

yahut da hiçbir şey yapmayabilir[495]. Yazıcıoğlu'na göre de suçun "sisteme girme ve orada kalmaya devam etme" şeklinde düzenlenmesi bilgisayar sistemlerinin güvenirliği ve bütünlüğünün korunması ilkesine ters düşmektedir[496]. Zira failin sisteme girme eylemiyle yetinmeyerek ayrıca kalmasını aramak, hem karışıklıklara yol açacak nitelikte hem de Avrupa Siber Suç Sözleşmesinin 2. maddesinde öngörülen amaçtan uzaklaştıracak niteliktedir. Diğer yandan ne kadar kalırsa suç gerçekleşmiş olacaktır, bu konu belirsizdir. Yazara göre aslında her girme zorunlu olarak kalma eylemini de içermektedir. Kaldı ki girilmekle zaten suçla korunan hukuki yarar ihlal edilmiş olunacak, veriler ve sistemin gizliliği ihlal edilmiş bulunacaktır.

TCK'nin 243/3. maddesine göre, aynı maddenin birinci fıkrasında yer alan ve yukarıda da değerlendirilen eylemlerin gerçekleştirilmesiyle birlikte sistemin içerdiği veriler yok olur veya değişirse, bu durumda birinci fıkradan daha ağır bu cezai müeyyide öngörülmektedir. Daha önce de ifade edildiği üzere, öğretide bu hükmün bir nitelikli hal olarak değerlendirilmesi gerektiği yönünde görüşlere rastlamak mümkünse de TCK'nin 243/3. maddesi münferit bir suç olarak, daha özel bir ifadeyle neticesi sebebiyle ağırlaşmış bir suç olarak kabul etmek gerekmektedir[497]. Çünkü cezai müeyyide altına alınan hareket tek başına bilişim sistemine girme ve orda kalma değil, bu hareket dolayısıyla sistemde yer alan bir verinin yok edilmesi veya değiştirilmesidir. TCK'nin 23. maddesinde yer alan neticesi sebebiyle ağırlaşan suç düzenlemesi hatırlanacak olursa; "işlenen bir fiil sonucunda, işlenmesi kastedilenden daha ağır veya başka bir neticenin oluşması hâlinde, failin bu eyleminden dolayı sorumlu tutulabilmesi için meydana gelen sonuç bakımından en azından taksirle hareket etmesi gerekmektedir." O halde TCK'nin 243/3. maddesi bakımından failin en azından taksirle hareket etmesi zorunludur[498].

Özetlemek gerekirse; bilişim sistemine girme suçu, yalnızca bilişim

---

[495] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 149
[496] Yazıcıoğlu, *Bilgisayar Suçları*, s. 83
[497] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6748
[498] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.846

sisteminin tamamına veya bir kısmına girilmesi ve orda bir müddet kalınması ile tamamlanır. Anılan suçun oluşması için, verilerin ele geçirilmesi şart değildir. Fail, bilişim sistemine girip hiçbir veriyi elde etmeden ve hiçbir bilgi edinmeden sistemden çıksa dahi, sisteme girmiş olması ve belli süre orada kalması suçun oluşumu için yeterli sayılacaktır[499]. Bu özelliği nedeniyle anılan suç sırf hareket suçudur, suçun oluşması için belli bir neticenin gerçekleşmiş olmasına gerek yoktur. Yine bu suç, bir tehlike suçudur, failin bilişim sistemine girmesi ve orada kalmaya devam etmesi ile bilişim sisteminde kayıtlı verilerin güvenliği tehlikeye düşmektedir, bu nedenle bilişim sistemine girmek ve orada kalmaya devam etmenin sonucu olarak bilişim sisteminin veya içerdiği verilerin herhangi bir zarara uğramasına veya zarar tehlikesi ile karşı karşıya kalmasına gerek yoktur. Bu nedenle anılan suç bir soyut tehlike suçudur[500].

TCK'nin 244/l. maddesinde yer alan suç ise sırf hareket suçu niteliği taşır. Suç tipinde ayrıca bir neticenin gerçekleşmesi gerektiğine ilişkin açıklık bulunmaz. Dolayısıyla suçun tamamlandığını kabul bakımından engellemek ya da bozmak suretiyle bir zararın meydana gelmiş olması da aranmaz. Ancak 244/4. madde ile bu suretle haksız bir çıkar sağlanması nitelikli hal olarak düzenlenmiştir. Bir kişisel veriyi elde ederek suç işleme amacı için bilişim sistemine girilmesi durumunda TCK 244/4. madde niteliğine bakılarak neticenin öne çıktığı söylenebilir. 244/4. madde de bilişim sistemindeki verilerin sadece menfaat elde edilmesi durumu düzenlenmektedir[501]. Halbuki bilişim siteminde tutulan kişisel verilerin bir suç işleme kararının icrası için kullanılması da mümkün olduğu için bu durumda da neticenin öne çıktığı görülecektir. Bilişim sistemine girerek verilerin kullanılması yoluyla suç işlenmesi durumunda elde edilecek neticenin suçun niteliğini belirleyeceği açıktır. Örneğin fail, bilişim sisteminde bulunan faile ait kişisel veriyi elde ederek banka hesaplarını boşaltırsa veya kendi kişisel verilerini değiştirerek maaşında artış sağlarsa burada hırsızlık ve dolandırıcılık suçları oluşacaktır. Yine kişi

---

[499] Ergün, İsmail, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Ankara: Turhan Kitapevi, 2008, s. 89
[500] Yazıcıoğlu, "Bilişim Sistemine Girme Eylemi", s. 84
[501] Parlar, *Türk Ceza Kanunu Yorumu,* s. 3749

bilişim sistemine girerek hastane kayıtlarını değiştirerek kişinin ölümüne neden olmuşsa artık burada adam öldürme suçu meydana gelecektir. Görüldüğü üzere bilişim sistemleri vasıta kılınarak kişisel verilerin elde edilmesi veya değiştirilmesi sonucu işlenecek suçta netice suçun vasfını belirleme yönünden ön plana çıkmaktadır.

2.1.1.3. Nedensellik Bağı

Bir suça ilişkin kanunî tarifte fiilin icrasının suçu oluşturmaya yetmediği, bunun yanı sıra bir neticenin gerçekleşmesinin de arandığı suçlarda, netice ile icra edilen fiil arasında nedensellik bağının bulunması gerekir. İcra edilen fiil ile gerçekleşen netice arasında illiyet bağının mevcudiyeti sorumluluk için şarttır. Nedensellik bağlantısı, fail ve icra ettiği fiil ile gerçekleşen netice arasındaki objektif ilişkiyi tesis etmektedir. Başka bir deyişle, gerçekleşen netice failin fiilinin eseri değilse, sorumlulukla ilgili bir tartışmaya gerek yoktur[502]. Sırf hareket suçlarında, suçun oluşması için hareketin yapılması yeterli olduğundan, bu suçlarda nedensellik bağı problemi ortaya çıkmaz. Yukarıda bahsettiğimiz gibi nedensellik bağı, kanuni tanımında hareketin yanı sıra neticeye de yer verilen suçlarda gerekli olan bir olgudur. Bu suçlarda, failin hareketinin neticenin meydana gelmesi bakımından nedensel olması, onun cezalandırılabilirliği bakımından zorunlu bir şartı oluşturmaktadır[503]. Nedensellikle ilgili kanunda hüküm bulunmaması bu konudaki çözümün öğretiye bırakıldığı anlamına gelebilir. Fakat öğretide de bu konuda bir birlik bulunmayıp, gerek yargı ve gerekse öğretinin üzerinde yoğunlaştığı iki teorinin şart ve uygunluk teorisi olarak ön plana çıktığı görülmektedir[504].

Araştırma konusunu ilgilendiren yönüyle nedenselliği incelemek için TCK'de düzenlenen ilgili suç tiplerinin neticesinin gerçekleşip gerçekleşmediğinin incelenmesi gerekir. Neticesiz suçlarda hareketin yapılması yeterli olup, kısaca tehlike suçu dediğimiz suç meydana gelmektedir. Fakat bir zarar doğması sonucu

---

[502] Özgenç, *Türk Ceza Hukuku, Genel Hükümler,* s.167
[503] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 165
[504] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 216

aranan suç tipleri yönünden ise nedensellik bağı cezalandırılmanın şartı olarak karşımıza çıkacaktır. Buna göre, TCK'nin 135. maddesinde düzenlenen kişisel verilerin kaydedilmesine ilişkin suçun neticesi harekete bitişik olduğundan kişisel veri hukuka aykırı kaydedilmekle tamamlanır ve suç bu yönüyle kural olarak teşebbüse elverişli değildir. Suçun tamamlanmış sayılması için kişisel verinin hukuka aykırı olarak kaydedilmesi yeterlidir; bundan bir zarar doğması da şart değildir. Bu nedenle suç bir *tehlike suçudur.* Suç tipinde hareket ile tehlike neticesi arasında bir nedensel ilişkinin varlığını araştırmak yönünde zorunluluk bulunduğuna ilişkin ifade yer almaması, diğer bir deyişle suç tipinde hareketin bir tehlike yaratabilecek nitelikte olması gerektiğine ilişkin düzenlemenin yer almaması suçun *soyut tehlike suçu* olarak kabul edilmesi sonucunu doğurur[505].

Verileri hukuka aykırı olarak verme veya ele geçirmeye ilişkin 136. maddede de düzenlenen suç da sırf hareket suçu olarak düzenlenmiştir. Söz konusu hareketlerin gerçekleştirilmesiyle suç da tamamlanmış olur. Suç kesintisiz bir nitelik taşımaz. Özellikle ele geçirme fiili bakımından ele geçirildikten sonra belli bir sürenin geçmesi, verinin bir süre saklanması şart değildir. Veri hukuka aykırı olarak ele geçirilmekle tamamlanmış olur. Bu yönüyle suç neticesi bakımından ani bir suçtur. Suçun tamamlanmış sayılması için kişisel verinin hukuka aykırı olarak verilmesi, yayılması ya da ele geçirilmesi yeterlidir; bundan bir zarar doğması da şart değildir. Bu nedenle suç bir *tehlike suçudur.* Suç tipinde hareket ile tehlike neticesi arasında bir nedensel ilişkinin varlığını araştırmak yönünde zorunluluk bulunduğuna ilişkin ifade yer almaması nedeniyle, bu suç *soyut tehlike suçu* olarak kabul edilmelidir[506].

Genel itibarı ile TCK'nin 243. maddesindeki düzenleme TCK'dekinin aksine karşılaştırmalı hukukta malvarlığının korunmasına ilişkin bir düzenlemedir. TCK'de bilişim alanında işlenen suçlar içerisinde 243. maddede düzenlenen yetkisiz erişim suçunda bir zarar tehlikesinin esas alındığı görülmektedir. Bu haliyle de yetkisiz

---

[505] Özbek, Veli Özer; Kanbur, Mehmet Nihat; Doğan, Koray; Bacaksız, Pınar ve Tepe, İlker, 2011, *Türk Ceza Hukuku Özel Hükümler,* Ankara: Seçkin Yayınevi, s. 515

[506] Taşkın, *Bilişim Suçları,* s. 26, Özbek ve diğerleri, *Türk Ceza Hukuku Özel Hükümler*, s. 529

erişim suçunun hukuki konusu, 243. maddede düzenlendiği şekliyle, malvarlığının korunması kapsamında mala zarar verme suçunun özel şekli olarak düzenlenen 244. maddenin hukuki konusu ile paralellik arz etmektedir. Bu açıdan 243. maddede düzenlenen yetkisiz erişim suçunun hukuki konusu, sisteme ve veriye yönelik zarar verici fiillerin engellenmesi anlamında bir tehlike suçu olarak, genel bir ifade ile mülkiyetin korunmasıdır[507]. Bu şekli ile suç, bir hareket suçu niteliği taşımaktadır. Bu anlamda suçun oluşması için bir neticenin meydana gelmesi şart değildir. Hatta bir tehlikenin meydana gelip gelmediğinin belirlenmesi yönünde tipte bu açıklık bulunmadığına göre suçun bu şeklinin *soyut tehlike suçu* olduğu söylenmelidir. Maddi unsuru oluşturan hareketin neticede bir zarar meydana getirmesi gerekmez. Zarar olasılığının varlığı yeterlidir. Yani suçun oluşması için sisteme girilmesi sonucu sistemdeki verilerin öğrenilmesi, kopyalanması, yok edilmesi, değiştirilmesi vb. bir tehlikenin varlığı, kanun tarafından cezalandırılmayı gerektirmektedir. Kanun metninde eylemden başka somut bir tehlikenin de gerçekleşmesi düzenlenmediğinden, suçun soyut tehlike suçu olduğunu söyleyebiliriz[508].

244. maddenin son fıkrasında failin amacı, hukuka aykırı olarak çıkar sağlamaktır. Fıkradaki haksız çıkar ifadesiyle kastedilen budur**.** Bu çıkarın maddi olması gerektiği belirtilmiştir[509]. Bunun aksine, haksız yararın maddi yarar yanında manevi yararı da kapsadığını ileri süren yazarlar da vardır. Bunlara göre, buradaki yarar ekonomik değeri olan mali bir yarar olabileceği gibi ekonomik bir getirisi ve değeri olmayan tamamen duyguları tatmine yönelik manevi yarar da olabilecektir. Kanun metninde de yararın mutlaka maddi olması gerektiğine işaret edilmemiştir[510]. Bu suçun oluşabilmesi için failin sağladığı çıkarın haksız olduğunun farkında olması da zorunludur. Fail, maddenin 1. ve 2. fıkralarında olduğu gibi, bilişim sistmine veya verilere zarar vermek kastını taşımamaktadır. Onun hedefi hukuka aykırı yarar sağlamaktır. Bu nedenle maddenin son fıkrasın 1. ve 2. fıkralarda olduğu gibi zarar

---

[507] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 119.
[508] Doğan, Koray, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", *Hukuk ve Adalet Eleştirel Hukuk Dergisi,* Yıl:2, Sayı:6-7, Ekim 2005, s. 295
[509] Erdağ, Ali İhsan *5237 sayılı TCK Ders Notları, Bilişim Alanında Suçlar*, Ankara: Hakim-Savcı Eğitim Merkezi, 2004, s. 17
[510] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 175

suçu değil tehlike suçu olduğu ileri sürülmüştür[511]. Fail hukuka aykırı yararı kendisine ya da üçüncü şahsa sağlayabilir. Hukuka aykırı yararın elde edilmesiyle suç tamamlanacaktır. Sonuç itibarı ile TCK'nin 135, 136 ve 244/4. maddeleri soyut tehlike suçu niteliğinde olduğu için elektronik ortamdaki bir kişisel verinin kullanılarak suç işlenmesi durumunda hareketin meydana gelmesi yeterli olup, sonuç doğmasa dahi kişi eyleminden sorumlu tutulacaktır, sonuçta meydana gelen netice yönünden nedensellik bağı aranmayacaktır.

2.1.2. Negatif Unsurlar

Negatif unsurlar başlığı altında, aşağıda açıklanacak olan hallerin bulunması durumunda meydana getirilen fiilin sonucunun suç oluşturmayacağı anlatılmaya çalışılmaktadır. Diğer bir deyişle negatif unsurlardan birinin bulunması eylemi hukuka aykırı olmaktan çıkartır. Hukuka uygunluk nedenleri olarak da tanımlanabilen bu hallerin inceleme konusu suç için ne şekilde gerçekleştiğinin tespiti ancak her bir suç için ayrı ayrı incelenerek mümkün olabilecektir.

2.1.2.1. Hukuka Aykırılık Unsuru

Özünde bir haksızlık olarak ortaya çıkan ve suç teşkil eden fiilin vasıflarından biri, hukuka aykırı olmasıdır. Hukuka aykırılık, işlenen fiilin hukuk düzenince caiz görülmediğinin, yapılmasının mahzurlu sayıldığının bir ifadesidir[512]. Bir fiilin hukuka aykırı olması, sadece ilgili olduğu yasa değil, bunun bütün hukuk sistemine aykırı olmasını ifade etmektedir[513]. Kısaca bir tanımlama yapılacak olursa suçu belirleyen özellik, suç ceza hukukunun ihlali olduğundan, hukuk düzeniyle çatışma olmaktadır. Bu çatışmaya doktrinde "hukuka aykırılık" denilmektedir[514].

---

[511] Dülger, *Bilişim Suçları*, s.247
[512] Dönmezer ve Erman, *Nazari ve Tatbiki Ceza Hukuku,* Cilt: I, s. 665
[513] Katoğlu, Tuğrul*, Ceza Kanunlarının Zaman Yönünden Uygulanması*, Ankara: Seçkin Yayınevi, 2008, s. 23, 24, 149 ve 155
[514] Hafızoğulları, Zeki ve Özmen, Muharrem, *Türk Ceza Hukuku Genel Hükümler*, Ankara: Us-a Yayıncılık, 2012, s. 219

Hukuka aykırılığın muhtevasını davranış normları tayin eder[515]. Ahlak ve hukukun müşterek kaynağı davranış normlarıdır. Bu itibarla hukuki olan bir davranış, aynı zamanda ahlakidir, ahlaka aykırı bir davranış hiçbir zaman hukuki koruma altına alınamaz[516]. Pozitif hukuk, ahlaki yükümlülüklerin yerine getirilmesine insanı mecbur eden bir araç olarak değil, bunların yerine getirilmesini insana mümkün kılan bir araç olarak anlaşılacaktır[517]. Örf ve adetler ise bir fiilin hukuka uygun kabul edilmesinin gerekçesini oluşturamazlar[518]. Hukuka aykırılık ve haksızlık kavramlarını da birbirinden ayırmak ve birbiriyle karıştırmamak gerekir. Hukuka aykırılık, suç oluştursun ya da oluşturmasın, fiilin bir vasfıdır. Fakat haksızlık, hukuka aykırı olan fiilin bizatihi kendisini ifade etmektedir[519]. Bu anlamda hukuka aykırılığın bir derecelendirmeye tabi tutulması kabil değildir. Bu itibarla basit bir yaralamanın, ağır bir yaralamaya nazaran daha az hukuka aykırı olduğu söylenemez. Sonuç itibarı ile bir fiil ya hukuka aykırı ya da uygundur. Hukuka aykırı olan bir fiilin ifade ettiği haksızlık ise niceliksel, yönden bir derecelendirmeye tabi tutulabilecektir[520]. Hukuka aykırılık, tipe uygunluktan sonra, suçun yapısında ikinci aşamayı oluşturur. Başka bir anlatımla, işlenen fiille tipik haksızlığın gerçekleştirildiğinin tespit edilmesinden sonraki aşamada, yine bu fiille ilgili olarak hukuka aykırılık yönünden bir değerlendirme yapılacaktır. Bu değerlendirme tipiklikten soyut olarak değil, bilakis ilişkili olarak yapılmaktadır[521]. Hukuka aykırılığın tespitini ise suç tanımına, tipe uygun bir fiilin bir izinle, yani bir hukuka uygunluk nedeni ile örtüşüp örtüşmediğinin tespiti ile yapabiliriz. Bir fiil tipe uygun olmakla hukuka da aykırı kabul edilir. Dolayısıyla suç tipleri hukuka aykırılığın karinesini oluşturur. Diğer bir deyişle, suç tipinde fiilin ayrıca hukuka aykırı da olduğu konusunda bir açıklığa gerek bulunmaz.

---

[515] Kunter, Nurullah ve Yenisey, Feridun, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, İstanbul: Beta Yayınları, 2000, s. 86

[516] Hatemi, Hüseyin, *Hukuka ve Ahlaka Aykırılık Kavramı ve Sonuçları*, İstanbul: Sulhi Garan Matbaası, 1976, s. 33

[517] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 280

[518] Özgenç, İzzet: *Ekonomik Çıkar Amacıyla İşlenen Suçlar*, Ankara: Seçkin Yayınevi, 2002, s. 141 vd.

[519] İçel ve diğerleri, *Suç teorisi*, s. 103

[520] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 283

[521] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 236

Öte yandan kanun koyucu bazen hukuka aykırılıktan özel olarak söz eder; yani hukuka aykırılığı ayrıca düzenler. Hukuka özel aykırılık olarak da adlandırılan bu durumda fiilin tipe uygun olmakla hukuka da aykırı olduğunu söyleyebilmek mümkün olmaz[522]. Bu hallerde hakim fiilin hukuka aykırı da olduğunu ayrıca belirlemek zorundadır. Bu suçlarda failin kusuru hukuka aykırılığı da kapsamalıdır. Yani fail tipte yer alan diğer unsurlar yanında yine tipte özellikle ve ayrıca belirtilmiş bulunan hukuka aykırılık unsurunu da biliyor ve istiyor olması gerekir. Hukuka özel aykırılık ile yasaklılık yanılması olarak ifade edilen hukuka aykırılık bilinci aynı şeyler değildir. TCK'nin 30/4. maddesi konuyu "İşlediği fiilin haksızlık oluşturduğu hususunda kaçınılmaz bir hataya düşen kişi, cezalandırılmaz" şeklinde ifade etmiştir[523].

Kanun koyucu bazı suç tiplerinde fiilin hukuka aykırı olarak işlendiğini failin bilmesi gerektiğini yani işlenen suçun hukuka aykırı olduğu hususunda doğrudan kastla hareket etmesini aramıştır. Başka bir deyişle, ilgili suç tanımında fiilin hukuka aykırılığına özellikle işaret edilmiş olan hallerde, bu suç ancak doğrudan kastla işlenebilir. TCK'nin 135, 136 ve 243. maddelerinde açıkça hukuka aykırılık unsurunun arandığı görüldüğünden bu suçların oluşabilmesi için failde suç işleme kastının bulunması gereklidir. Somut olayın özelliğine göre bir hukuka uygunluk nedeni bulunması halinde, artık fiil hukuka aykırıdır denilemez. Hukuka uygunluk nedenleri, fiilin ve dolayısı ile suçun hukuka aykırılığını ortadan kaldırmaktadır. 135, 136 ve 243. maddede yer alan "'hukuka aykırı olarak" ibaresine verilecek anlamı bu şekilde yorumlamak mümkündür. O halde kişisel veri hukuka aykırı olarak kaydedilmediği sürece suç oluşturmaz ve hakim mevzuatta buna imkan veren düzenlemelerin mevcut olup olmadığını araştırmak zorundadır. Hukuka uygunluk nedenleri içerisinde de inceleneceği üzere yetkili amirin emrini yerine getirmek veya kişinin rızası gibi nedenlere bağlı veri kayıtları ve bu verilerin kullanılması eylemi suç olmaktan çıkartmaktadır. Kaldı ki zaten hergün kişisel veriler milyonlarca kez bir

[522] Dönmezer ve Erman, *Nazari ve Tatbiki Ceza Hukuku*, s. 149
[523] Centel, Nur; Zafer, Hamide ve Çakmut, Özlem, *Türk Ceza Hukukuna Giriş*, İstanbul: Beta Yayınları, 2011, s. 18 vd

yerlerde işlenmektedir. Burada amaç bu kişisel verilerin hukukun yasakladığı şekilde işlenmesi ve kullanılmasına yöneliktir[524].

Zarar oluşmasının aranıp aranmamasına göre bu suç tiplerinde öncelikle bilişim sistemine izinsiz yollardan girilerek kişisel verilerin kanuni olmayan şekilde elde edilmesi gerektiğinden ve bilişim sistemine yöneltilen ızrar fiilleri özel bir suç haline getirilmiş olduğu için her halükarda zarar olmasa da suç oluşacaktır[525]. TCK'nin 135, 136 ve 243. maddelerinin metninde, eylemin hukuka aykırı olması özel olarak aranmıştır. Ancak TCK'nin 244. maddesinde düzenlenen eylemler yönünden özel hukuka aykırılık aranmamıştır. Bu madde kapsamında gerçekleştirilecek eylemler hukuka aykırı olarak kabul edilir. Bu suçlarda sahibinin veya kullanıcısının rızası, hukuka aykırılığı ortadan kaldırır[526].

Hırsızlık, dolandırıcılık ve yağma suçlarında, kişinin hukuki alacağını tahsil amacıyla hareket etmesi durumunda, bu husus bir indirim sebebi kabul edilmişken, bilişim suçlarında bu konuda bir düzenlemenin bulunmaması eleştirilerek, sattığı bir bilgisayarın parasını ödemeyen müşteriden, bu bilgisayarı çalan ya da zorla elinden alan satıcının bu durumu, indirim nedeni sayılırken, sattığı yazılımın parasını vermeyen müşterisinin programını ağ üzerinden sisteme girerek sildiğinde, verileri bozma suçunun tam cezasının uygulanacağı örneği verilmektedir[527]. Zarar öğesi madde metninde açıkça belirtilmemişse de, bu husus gerekçede vurgulanmıştır. Gerekçeye göre, Sistemlere yöneltilen ızrar fiileri özel bir suç haline getirilmiştir. Bilişim sisteminin fiziki varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır[528].

---

[524] Taşkın, *Bilişim Suçları,* s. 102 ve 108
[525] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 255
[526] age, s. 269
[527] Yazıcıoğlu, *Bilgisayar Suçları*, s.145
[528] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 273

2.1.2.2. Hukuka Uygunluk Nedenleri

Hukuka uygunluk nedenleri, hukuka aykırılık unsuru ile sıkı sıkıya bağlantılıdır[529]. Bir fiil hukuka aykırı ise artık o fiil bütün hukuk sistemine aykırıdır[530]. Örneğin bir fiilin sadece bir hukuk disiplinine, yani medeni hukuka veya ceza hukukuna aykırılığından söz edilemez[531]. TCK'nin 135. maddesinde olduğu gibi hukuka aykırılığın ilgili suç tanımında özellikle vurgulandığı durumlarda; ceza sorumluluğu için failin, işlediği fiille ilgili olarak suçun maddi unsurlarının yanı sıra, bu fiilin hukuka aykırılığının da bilincinde olup olmadığının ayrıca araştırılması gerekir. Aksi takdirde kastının varlığından söz edilemez[532]. İşte hukuka uygunluk sebebinin varlığı halinde, artık fiilin hukuka aykırılığından söz edilemeyecektir. Hukuka uygunluk sebepleri, fiilin ve dolayısı ile suçun hukuka aykırılığını ortadan kaldırmaktadır[533].

2014 tarihli Kişisel Verilerin Korunması Kanun Tasarısının hukuka uygunluk nedenlerine ilişkin düzenlemeleri de bu konuda önem kazanmaktadır. 2008 tarihli Tasarının *"Hukuka uygunluk nedenleri"* başlıklı 6. maddesinde kişisel verilerin işlenmesinde hukuka uygunluk nedenleri öngörülmekteyken[534], bu durum 2014 tarihli Tasarıda biraz farklı düzenlenerek tasarının 5. maddesinde "Kişisel Verilerin İşlenme Şartları" başlığının 2. fıkrasında ve Tasarının 6. maddesinde "Özel Nitelikle Kişisel Verilerin İşlenme Şartları" başlığı altındaki düzenlemenin 2. fıkrasında istisnai hal olarak gösterilmiştir. Tasarının 5. maddesin düzenlemesine göre kişinin açık rızası olmadan kişisel verinin işlenebilme halleri kapsam içine alınmıştır. Bu madde de rıza hususu 1. fıkrada açıkça yazılarak kişisel verinin işlenebilmesinin şartı haline getirilen rıza, 6. madde kapsamına göre özel nitelikte olan ve işlenmesi yasak olan kişisel verilerin işlenmesine ilişkin bir istisna getirerek ilgili kişinin açık rızasıyla işlenebileceği düzenlenmektedir.

---

[529] Dönmezer ve Erman *Nazari ve Tatbiki Ceza Hukuku*, Cilt: I, s. 665
[530] Katoğlu, Tuğrul, *Ceza Hukukunda Hukuka Aykırılık*, 2003, s. 23, 24, 149
[531] İçel ve diğerleri, *Suç Teorisi*, s. 101
[532] Özgenç, İzzet ve Şahin, Cumhur, *Uygulamalı Ceza Hukuku*, 3. Bası, Ankara: Seçkin Yayınevi, 2000, s.104/205
[533] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 285
[534] TBMM, "Kişisel Verilerin Korunması Kanun Tasarısı", http://www2.tbmm.gov.tr/d23/1/1-0576.pdf, (Erişim: 18.02.2015)

Tasarının 5. maddesi kapsamında ilgilinin rızası verilerin işlenebilmesinde temel şart olarak öngörülmekle beraber, hukuka uygunluk sebepleri olarak sayılabilecek mahiyette verilerin işlenmesini meşru gösterecek sebepler yazılmıştır. Buna göre kişisel veriler ancak aşağıdaki hallerde işlenebilecektir:

- Kanunlar tarafından açıkça işlenebileceğinin düzenlenmiş olması,
- Rızanın açıklanmasının fiilen imkansızlığı bulunan kişiler ile rızasına kısıtlılık gibi nedenlerle hukuki geçerlilik tanınmayan bir kişinin, kendisinin veya bir başkasının yaşamı veya vücut bütünlüğünün korunması için zorunluluk bulunması,
- Bir sözleşmenin taraflarına ait kişisel verilerin işlenmesinin, sözleşmenin düzenlenmesi veya ifası ile doğrudan ilgili olması,
- Veri işleme sorumlularının görevlerini ifa edebilmesi için zorunlu bulunması,
- Kişisel verinin sahibinin bizzat kendisi tarafından alenileştirme işleminin yapılmış olması,
- Bir hakkın oluşturulması, kullanılması veya korunması için veri işlemenin zorunlu olması[535].

Tasarının 6. maddesinde işlenmesinin yasak olduğu bildirilen kişinin ırkı, etnik kökeni, siyasi düşüncesi, dini vb. gibi özel nitelikli kişisel verilerin yeterli önlemler alınması halinde işlenebileceği düzenlenmiştir. Bunlar;

- "İlgilinin açık rızasının bulunması,
- Kanunun açıkça öngörmesi,
- Siyasi parti, vakıf, dernek veya sendika gibi kar amacı gütmeyen kuruluş ya da oluşumların, tabi oldukları mevzuata ve amaçlarına uygun olmak, faaliyet alanlarıyla sınırlı olmak ve üçüncü kişilere açıklanmamak kaydıyla kendi üyelerine ve mensuplarına yönelik verilerin işlenmesi,

[535] Başbakanlık Kanunlar ve kararlar Genel müdürlüğü tarafından TBMM adalet komisyonuna 26.12.2014 tarihinde sunulan tasarı, Adalet Bakanlığı Kanunlar Genel Müdürlüğü, "Tasarılar" http://www.kgm.adalet.gov.tr/Tasariasamalari/Tbmmkms/Tbmmkom/kisiselveriler.pdf, (Erişim: 07.06.2015), s. 4

- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi kullanılması veya korunması için veri işlenmesinin zorunlu olması,
- Kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler[536] tarafından işlenmesi[537].”

Bu düzenlemeye paralel olarak incelenmesi gereken “*İstisnalar”* başlıklı 24. maddesinde ise genel olarak, belirtilen hallerde bu kanun hükümlerinin uygulanmayacağı öngörülmektedir. Konuya 5. ve 6. maddeler açısından bakıldığında 22. maddedenin öngördüğü bu sınırlandırmalar Tasarıda yer alan diğer hukuka uygunluk nedenleri olarak nitelindirilebilir.

Sağlam tarafından dile getirilen ve özel hayatın gizliliğine ilişkin olarak kişisel verilerin de yer aldığı birçok hususu bünyesinde barındıran[538], “pratik uyuşum ilkesi[539]” çerçevesinde yapılacak sınırlandırılma halleri hariç Anayasanın 20/1. maddesi uyarınca sınırlandırma nedeni bulunmamalıdır. Yani kişisel verilerin işlenmesine ilişkin düzenlemelerde, Anayasanın 20/1. maddesi gereğince hiçbir sınırlandırma nedeni bulunmayan düzenlemeye uyulması zorunludur[540].

TCK’de hukuka uygunluk nedenleri dört ana gurupta toplanmıştır. Bunlar;

---

[536] Tıp etiğininde en önemli konularından biri olan ve hekim ile hasta arasındaki sözleşme uyarınca hekimin kendi gözlemleri veya tesadüfen öğrendiği hastası hakkındaki bilgilere sır olarak tutmakla yükümlüdür. Bkz. Karasu, Sinem, *Hekimin Sır Saklama yükümlülüğü,* İstanbul: Vedat Kitapçılık, 2009, s. 51-52

[537] Kişisel Verilerin Korunması Hakkında ki Kanun Tasarısı, s. 5

[538] Sağlam, Fazıl, *Temel Hakların Sınırlandırılması ve Özü*, Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, 1982, s. 47 vd.

[539] **Pratik uyuşum ilkesi**: Bu ilkeye göre, bir temel hakkın başka bir temel hak ya da anayasanın koruduğu başka bir değerle çatışması halinde öyle bir çözüm bulunmalıdır ki, gerek temel hak gerek anayasanın koruduğu hukuki değer, varlık ve etkilerini optimal düzeyde korusun. Görüldüğü gibi, burada bir özgürlüğün diğer bir özgürlüğü bertaraf etmesi söz konusu değildir. Her özgürlük, oranlı bir düzeyde korunarak optimal etkilerini sürdürecektir. (Sağlam, *Temel Hakların Sınırlandırılması ve Özü,* s. 40)

[540] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 213

Hakkın Kullanılması (TCK m. 26, f.1),

Kanun hükmünü yerine getirme (TCK m. 24, f.1),

Meşru müdafaa (TCK m. 25, f.1),

İlgilinin Rızası (TCK m. 26, f.2).

Burada sayılan hukuka uygunluk nedenlerinin inceleme konusu içerisinde değerlendirmesini yapmak yararlı olacaktır.

2.1.2.2.1. Hakkın Kullanılması

Hukuk düzeni bir kimseye belirli bir hakkı kullanma yetkisi verirken, o hakkın icrası fiillerini de hukuka uygun saymaktadır. Hukuka uygunluk nedeni olarak hakkın kullanılmasından söz edebilmek için, önce, kişiye hukuk düzenince tanınmış bir sübjektif hakkın varlığı gereklidir. Ayrıca, kişinin bu hakkını, sınırları içerisinde kullanması gerekir[541]. Hakkın kullanılması hallerine örnek olarak, zilyetliğin korunması, ruhsat ve yetkiye dayanan bir hakkın kullanılması, mesleğin veya sanatın icrası (basın, tıp, avukatlık gibi), spor hareketleri, savunma ve şikayet hakkı verilebilir.

İncelemenin ana teması olan bilişim sitemindeki kişisel verilerin korunması genel başlığı çerçevesinde bilişim sitemine girme konusu altında düzenlenen TCK'nin 243. maddesindeki suç tipi esasen yaygın ismi ile yasak erişim suçunda hakkın kullanılması hukuka uygunluk sebebi olarak kullanılamaz. Çünkü suç tanımı zaten hukuka aykırı erişimi engellemeye çalışmaktadır. Bir hakkın kullanılarak yasak erişim yapılması mümkün olmayacağı için bu suç tipinde hakkın kullanılması hukuka uygunluk sebebi var denilemez. 244. madde de düzenlenen suç içinde aynı şeyleri söylemek mümkündür. Bu suç tipinde de hukuka aykırılık unsuru ana şart

[541] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 287

haline getirildiği için bir hakkın kullanılması suretiyle bu suçun hukuka uygun hale getirilmesi düşünülemez[542].

TCK'nin 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunda bir avukatın vekaletini aldığı bir kişi ile ilgili özel hayatını ilgilendiren konularda bilgi toplaması ve bunları elektronik ortamda saklamasında mesleğinin gereği olarak bir sakınca yoktur[543]. Örneğin bir boşanma davasında kişilerin yatak odalarına kadar giden kişisel bilgiler yargılamada delil olarak kullanılmak üzere paylaşılmaktadır. Burada da yine ölçü işin gerekleri ile sınırlıdır. Avukatlık mesleği ile ilgili olarak karşımıza çıkan bir diğer sorun ise yürütmesi istenilen dava ile ilgili karşı taraf hakkında toplanan kişisel verilerin kaydedilmesinin suç oluşturup oluşturmayacağıdır. Burada da yine işin mahiyetinin önem kazanacağını söylemek gerekir. Görülen dava ile ilgili müvekkiline karşı sorumlu olan avukatın davanın kazınılması için toplaması gereken bilgiler arasında kişisel verilerin de bulunması durumunda olayla sınırlı kalmak ve sadece davada kullanılması koşuluyla bu bilgilerin kaydedilmesinde yasada düzenlenen suç oluşmayacaktır[544]. Aksi düşünüldüğünde mesleğin yapılması sınırlandırılmış olacaktır. Fakat bu konunun suistimale açık olduğu düşünülürse, Avukatlık Kanununa bu konu ile ilgili düzenlemeler konulması gerekmektedir.

TCK'nin 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunda ise zaten yukarıda yapılan açıklamalarda da bahsedildiği üzere madde başlığında eylemin hukuka aykırı olarak gerçekleştirilmesi gerektiği anlatıldığından bir hakkın kullanılmasından kaynaklı olarak kişisel verinin meslek icabı kullanılması veya aynı kapsamda ele geçirilmesi hukuka aykırılık unsurunun bulunmaması nedeni ile suç oluşturmayacaktır. Yine bir doktorun hastasının sağlık kayıtlarını arşivlemesi işinin gereği olacağından eyleminde hukuka aykırılık yoktur. Ne var ki bu veri depolama işleminin kişinin doktora başvurduğu

---

[542] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s.158

[543] Kızıltan, *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, s. 65

[544] Akıllıoğlu,Tekin, "İdari Usul ve Kişisel Verilerin Korunması", http://www.idare.gen.tr/akillioglu-idariusul.htm. (Erişim: 15.8.2010)

sebeple sınırlı kalması gerekir. Başka amaçlar ile tedavide kullanılmayacak bilgilerin saklanması durumunda suçun oluşmadığı söylenemez[545]. Yukarıda 135. madde kapsamında yapılan açıklamalar, bu maddede düzenlenen suç tipi içinde geçerli olacaktır.

2.1.2.2.2. Meşru Müdafaa

Meşru müdafaa, bir kimsenin, kendisinin, kendisini veya başkasını hedef alan bir tecavüz, saldırı karşısında, savunma amacına matuf olarak ve bu saldırıyı def edecek ölçüde kuvvet kullanılmasını ifade eder. Meşru müdafaa halinde, şartlarına uygun olarak gerçekleştirilen fiil, hukuka uygundur ve dolayısı ile herhangi bir sorumluluğu gerektirmez, kişiye ceza verilmez[546]. Bilişim suçu mağdurları, kimi zaman ihkak-ı hak yoluna gitmeyi tercih etmektedirler Başka bir söyleyişle, kendilerini meşru müdafaa ettiklerini düşünmektedirler. Oysa ceza kanunlarındaki meşru müdafaa, cana veya ırza yönelik, defedilmesi için başka olanak bulunmayan zorunlu bir tehlike karşısında, sanığa karşı koyabilme hakkıdır. Bu açıdan bakıldığında, örneğin, banka hesabından bilişim yoluyla para çalınmasına maruz kalan mağdurun, bu kez sanığın banka hesabından aynı şekilde para hırsızlamasında, cana veya ırza yönelik bir tehlikeden söz etmek mümkün değildir. Başka bir anlatımla, burada meşru müdafaa hakkından söz edilemez. Bir an için bilişim suçlarında meşru müdafaa hakkı olabilir denildiğinde, bunun koşullarını ve ölçüsünü koyabilmek olanaklı değildir ve zaten böyle bir hakka, meşru müdafaa da denilemez. Bu varsayımdaki yaklaşım, bilişim suçlarını çok daha fazlalaştırır. Bir bakıma bilişim suçlarının işlenmesini teşvik eder. Çünkü bilişim suçunu işleyen hemen herkes, uğramış olduğum saldırıya karşılık veriyordum savunmasına yönelebilecektir[547].

Kişisel verilerin korunmasına ilişkin düzenlemeler yönünden de yukarıda belirtilen ana fikir geçerli olacaktır. Meşru müdafaanın bu suç tiplerinde hukuka uygunluk nedeni olarak kullanılması düşünülemez. Kendine karşı işlenen veya

[545] Soyaslan, *Ceza Hukuk Özel Hükümler*, s. 348
[546] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 318
[547] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 58

işlenecek olan bir suçun engellenmesi amacı ile kişisel verilerin kaydedilmesi veya bunların ele geçirilmesi ve kullanılması ancak şantaj vb. ayrı bir suç oluşturacağından meşru müdafaa hakkı kullanıldı denilemeyecektir.

2.1.2.2.3. Kanun Hükmünün Yerine Getirilmesi

Kanun bir kişiye belli hususlarda bir hak ve yetki vermişse, bunun öngörüldüğü şekilde uygulanması durumunda hukuka aykırılık söz konusu olmaz. Burada ki kanun deyiminden pozitif hukuk metinlerini yani yazılı hukuk kurallarını anlamak gerekir. Kanun hem şekli hem de maddi anlamda kanundur. Dolayısı ile kanun hükmünde kararname (KHK), tüzük, yönetmelik de bu çerçevede değerlendirilmelidir. Aslında, kanunun hükmünün yerine getirilmesinin söz konusu olduğu hallerde, kişi açısından bir görev vardır. Bir anlamda bu hukuka uygunluk nedeni görevin yerine getirilmesi anlamındadır. Çünkü bir davranışın hukuka uygun olup olmadığını belirlerken, yerine getirilen görevin mahiyeti göz önünde bulundurulmaktadır. Ancak yürütülen görevle bağlantılı olarak, bu hukuka uygunluk nedeninin sınırının aşılıp aşılmadığını belirlemek mümkün olacaktır. Bazı durumlara bir yetki kullanılması söz konusu ise de, bu yetkinin bir görevle bağlantılı olduğunu gözden uzak tutmamak gerekir[548]. Kanun hükmünün yerine getirilmesini hakkın icrasından ayıran esas itibarı ile onun görev ya da yetki niteliğinde olmasıdır[549]. Ancak tüzük ve yönetmelikler kanuna aykırı bulunmadıkları sürece fiili hukuka uygun hale getirebilir[550].

Konuyla ilgili olarak bu hukuka uygunluk nedeni TCK'nin 135. maddesi kapsamında ilk akla gelen hukuka uygunluk sebebidir. Özel veya kamu kurumlarının veri memurlarının bir hukuki düzenlemenin amir hükmüne dayanarak bu kişisel verileri kaydetmiş olması durumunda suç oluşmayacaktır[551]. Veri işleyenin sorumluluğunda ayrıntılı olarak incelenen bu konu hakkında kısaca bir hatırlatma

[548] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 287
[549] Artuk, Mehmet Emin; Gökçen, Ahmet ve Yenidünya, Ahmet Caner, (2002), *Ceza Hukuku Genel Hükümler*, Ankara: Adalet Yayınevi, s. 507
[550] age, s. 509
[551] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 4121

yapılacak olursa, veri işleyenin verilerin toplanması için açıkça görevlendirilmiş olması ve yetki ve sorumluluklarının yine hukuki düzenlemeler ile çerçevesinin belirlenmiş olması gerekir[552]. Örneğin, CMK 80/2. madde uyarınca genetik inceleme sonucu bir mahkumiyet hükmünün varlığı halinde kaydedilebilir. TCK'nin 136. maddesinde düzenlenen kişisel verilerin hukuka ayıkırı olarak verilmesi veya ele geçirilmesi suçunda ise aynı şekilde kanunun emrini icra sorumsuzluk nedenidir. Bu kapsamda kolluk görevlilerinin suç ve suçlunun takibi anlamında kişilere ait seyahat, ekonomi, sağlık gibi konulara ait kişisel verilerini elde etmeleri ve bunları kanuni sürecin yürütülmesi için kullanılması verilen yetki kapsamını aşmadıkça sorumsuzluk hali olarak değerlendirilebilir. Yine müdafilerin ilgili oldukları davalar ile ilgili olarak topladıkları verilerin de bu kapsamda değerlendirilmesi gerekir. Ancak avukatların sır saklama yükümlülükleri çerçevesinde elde ettikleri verilerle ilgili olarak örneğin basın açıklaması yapma gibi bir yetkileri yoktur. Müdafiliğin bu konudaki çerçevesini de yine TCK'nin ilgili maddeleri ile Avukatlık Kanunu belirlemektedir.

Bilişim sistemine girme suçunun düzenlendiği TCK'nin 243. maddesinde hukuka aykırılık unsurunun uzantısı olan hukuka uygunluk sebeplerinden kanunun hükmünü yerine getirme hususu maddenin düzenleniş şekli ile birlikte incelenmelidir. Bilindiği üzere, bilişim sistemine girme ve orada kalma eyleminin suç teşkil etmesi için bu eylemlerin hukuka aykırı bir şekilde gerçekleşmesi gerekmektedir. Görülmektedir ki kanun koyucu bu suç tipi için özel olarak hukuka aykırılığı aramaktadır. O halde anılan eylemlerin hukuka aykırı olmaması halinde, eylem bir suç oluşturmayacaktır. Bir bilişim sistemine girme ve orada kalma eyleminin, bir kanun hükmünün gereği olduğu hallerde hukuka aykırılık söz konusu olmayacaktır. Bu konuya en açık örnek CMK'nin 134. maddesinden düzenlenen "bilgisayarlarda, bilgisayar programlarında ve kütüklerde arama, kopyalama ve el koymadır[553],,[554]. Anılan hükmün birinci fıkrasına göre; "Bir suç dolayısı ile yapılan

---

[552] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 87

[553] *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*

Madde 134 – (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde,

soruşturmada, başka suretle delil etme imkanın bulunmamaması halinde, cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin haline getirilmesine hakim tarafından karar verilir." O halde kolluk tarafından soruşturma makamlarının kararı gereğince şüphelinin bilgisayarına yani bilişim sistemine, onun rızası hilafına girer ve orada kalmaya devam ederse, bu eylem dayanağını CMK'nin 134. maddesinden aldığı için hukuka aykırı sayılmayacaktır. Bu anlamda eylem hukuka uygun olacaktır[555].

TCK'nin 244. maddesinde düzenlenen suçlar yönünden ise, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 8. maddesine göre uygulanan internet erişiminin engellenmesi uygulaması örnek verilebilir. Bahsi geçen kanunun 8. maddesinde iki değişik erişimin engellenmesi uygulamasına rastlanmaktadır. Bunlardan birincisi koruma tedbiri olarak erişimin engellenmesi, bir diğeri ise idari yaptırım olarak erişimin engellenmesidir. Bir koruma tedbiri olarak erişimin engellenmesinde öncelikle suç teşkil eden içeriğin 8/1-a ve b maddesinde sayılan suçlardan biri olması gerekmektedir. Kanun burada sınırlı sayıda suç tipinden ibaret olan bir katalog oluşturmuştur[556]. Hemen belirtelimki Kanunu 8. maddesinde sayılan katalog suçlardan ötürü, erişimin engellenmesi kararı ya bir hakim veya savcı

Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

[554] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 6747

[555] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 848

[556] age, s. 868

ya da iletişim başkanlığı tarafından verilebilmektedir[557]. Buna göre erişimin engellenmesi kararı verilebilmesi için TCK'de düzenlenen *"intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkan temini"* suçları ile birlikte "*Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da"* yer alan suçlar söz konusu olmalıdır. Ancak bir içeriğe erişimin engellenmesi için anılan suçların işlenmiş olması gerekmemektedir, bu suçların işlendiğine yönelik yeterli şüphenin varlığı aranmaktadır[558]. İşte bu süreç içerisinde gerçekleştirilen erişimin engellenmesi, internetin de birbilişim sistemi olduğu kabulünden hareketle TCK'nin 244. maddesinde düzenlenen suçlar açısından hukuka aykırı kabul edilmeyecektir[559]. Yine CMK'nin 134. maddesi kapsamında yapılan arama, kopyalama ve el koyma işlemleri TCK'nin 244/2. maddesi anlamında bir suça vücut vermeyecektir. Görüldüğü üzere kişisel verilerin elde edilmesi suretiyle işlenen suçlar yönünden, 244. maddenin 4. fıkrası kapsamında yapılacak eylemlerin önlenmesi açısından 5651 sayılı kanun kapsamındaki uygulamalar hukuka uygunluk nedenlerinden yararlanacaktır.

Buraya kadar yapılan açıklamalar doğrultusunda kanun hükmünün uygulanması bilişim alanında saklanan kişisel verilerin yine bilişim sitemi aracı kullanılarak elde edilmesi ve suçta kullanılması durumunda hukuka uygunluk sebebi sayılacaktır. Özellikle veri işleme görevlisinin eylemi yönünden bu konunun önem arz ettiği barizdir. Veri işleme görevlilerinin görevlerini ifa ederken bu suçun oluşmamasına karşın, görevi dışında aynı eylemi gerçekleştirmesi durumunda suçun tipiklik unsuru oluştuğu için veri işleme memurunun da cezalandırılması kaçınılmaz olacaktır.

---

[557] Bozel, Savaş, "5651 sayılı Kanuna istinaden Bazı İnternet sitelerine Erişimin Engellenmesi Tedbirine Eleştirel bir yaklaşım", http://www.e-akademi.org/makaleler/sbozel-5.htm, (Erişim: 22.08.2010)

[558] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 868

[559] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 19

2.1.2.2.4. İlgilinin Rızası

Hukuka uygunluk nedenleri arasında yukarıda yapılan sıralamaya göre sonuncusu olarak yer alan ilgilinin rızası inceleme kapsamındaki konular yönünden uygulama yeri bulmaktadır. Fakat ilgilinin rızasının sınırları ve kullanılış şekli hukuka uygunluğun sınırlarını da belirleyeceği için bir miktar detaya girmekte yarar bulunmaktadır. İlgilinin rızası hukuka uygunluk nedeni TCK'nin 26/2. maddesinde "*Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez.*" şeklinde düzenlenmiştir. Ayrıca kanunun çeşitli suç tanımlarında "rızası olmaksızın" veya "rızası olmadan" ibareleri kullanılmıştır. Rızanın yokluğu, ilgili suçun maddi unsurları bağlamında mütalaa edilmesi gereken bir olumsuz unsuru oluşturmaktadır. Kişinin hukuki yetkisini kullanmak suretiyle açıklamış bulunduğu rızaya dayalı olarak başkaları tarafından gerçekleştirilen davranışlar hukuka aykırı değildir. Belli konular ile ilgili olarak belli tasarruflara yönelik hukuken geçerli rızaya dayanılarak gerçekleştirilen davranışlar hukuka uygundur.[560]

İlgilinin rızası hukuka uygunluk sebebi bakımından;

1. Mağdurun üzerinde serbestçe tasarrufta bulunabileceği bir hakkın varlığı,
2. Rızaya Ehliyet ve
3. Rızanın açıklanması gerekir[561].

Rıza açıklamasının bir hukuka uygunluk sebebi oluşturabilmesi için, rızanın ilişkin bulunduğu konu üzerinde ve hukuken tanınan sınırlar kapsamında bir tasarrufta bulunulması gerekir[562]. Bunun için; öncelikle, kişinin üzerinde tasarrufta bulunabileceği bir konunun varlığı gereklidir. Bu konuda kriter olarak gerek korunan hak ve yararın ve gerekse haraketin yönelik olduğu ve suç tipinde belirtilen konunun

[560] Ekici Şahin, Meral: *Ceza Hukukunda Rıza*, İstanbul: Oniki Levha Yayıncılık, 2012, s. 50 vd.
[561] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 526
[562] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 331

kişiye ait olması gerekir. Bu iki kavram aynı kişide birleşiyorsa rıza geçerlidir[563]. Örneğin kişi, vücudu üzerinde, sahip bulunduğu malvarlığı üzerinde belli tasarruflarda bulunma yetkisini haizdir, buna karşın, hayatı ve şerefi üzerinde tasarrufta bulunma yetkisine sahip değildir[564]. Bu nedenle, kişi kendisine hakaret edilmesine rıza gösterse dahi, bu rıza, hakaret fiilini hukuka uygun hale getirmez[565]. Rıza, kişinin üzerinde tasarrufta bulunabileceği bir konuya ilişkin olmakla birlikte hukuk düzeni, konu üzerindeki tasarruf biçimi bakımında da rıza açıklamasına sınırlama getirmektedir. Örneğin, kişi sahibi bulunduğu kendisine ait fotoğrafın kullanılmasına izin verebilir ancak toplu halde çektirilmiş bir fotoğrafın kullanılmasına izin veremez[566].

Kişisel verinin hukuka aykırı olarak kaydedilesi suçu ile verileri hukuka aykırı olarak verme veya ele geçirme suçu "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında düzenlenmiş olduğuna göre korunan hukuki değer esas alındığında bu suç bakımından mağdurun üzerinde mutlak şekilde tasarrufta bulunabileceği bir hakkın bulunduğu kanısı oluşabilir. Fakat mağdurun tasarrufta bulunabileceği haklar konusunda ki bir diğer kriter ise şikayete tabi olmasına göre değerlendirmedir. Kişisel verinin hukuka aykırı olarak kaydedilmesi suçu şikayete tabi değildir (TCK m. 139[567]). Bu durumda kanun koyucunun bu bölümde düzenlenen suçlar bakımından bireyin değil, kamunun menfaatinin daha ağır bastığını kabul ettiği söylenebilir. O halde kişisel verilerin hukuka aykırı olarak kaydedilesi suçu bakımından ilgilinin rızası hukuka uygunluk sebebi uygulanabilir değildir. Mevzuat hükümleri çerçevesinde yapılacak kayıt ilgilin rızası değil, kanun hükmünün yerine getirilmesi hukuka uygunluk sebebi bakımından düşünülmelidir. Kısacası hukuka uygun olarak gerçekleşmeyen kaydı, ilgilinin rızası hukuka uygun hale getirmez[568]. "Yaşar, Gökçen ve Artuç'un" mağdurun rızasının bulunması

---

[563] Önder, *Ceza Hukuk Genel Hükümleri,* s. 213
[564] Soyaslan, *Ceza Hukuk Özel Hükümler*, s. 75
[565] Özgenç. *Türk Ceza hukuk, Genel Hükümler*, s. 333
[566] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s. 69
[567] **"Madde 139-** (1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır."
[568] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 526

halinde suçun oluşmayacağına dair görüşlerine yukarıda açıklanan nedenlerle katılmak mümkün görünmemektedir[569].

Bilişim sistemine girme ve orada kalma eylemi yönünden ise şayet bir kişiye ait bilişim sistemine, sistem sahibinin rızası ile girilmesi ve orada kalınması söz konusuysa, burada sistem sahibinin üzerinde tasarrufta bulunabileceği bir hakkın varlığından hareketle eylem hukuka aykırı kabul edilmeyecektir[570]. Eğer kişi, sistem sahibinin rızasını almadan bilişim sistemine girmiş ve fakat sistemdeyken sistem sahibi tarafından sistemde kalmasına izin verilmişse, bu durumda suçun mütemadi bir suç olduğu ve temadi kesilene kadar hareketinde devam ettiği kabul edilecek olursa, suç henüz tamamlanmadan verilen rızanın eylemi hukuka uygun hale getireceği söylenebilir[571]. TCK'nin 244. maddesinde düzenlenen bilişim sistemini engellemek, bozmak, verileri yok etmek veya değiştirmek suçları yönünden ise suçun konusunun veri veya bilişim sistemi sahibinin üzerinde serbestçe tasarrufta bulunma hakkına sahip olabileceği konular olduğundan, TCK'nin 244/1 ve 2'deki eylemler bakımından bu kişinin göstereceği rıza, eylemi hukuka uygun hale getirir. Fakat rıza hukuka uygunluk sebebine ilişkin olarak yukarıda yapılan genel açıklamalarda belirtilen kısıtlamalara uygun verilen rıza suç olmaktan çıkartmaktadır[572].

Hukuka uygunluk nedenleri açısından konuyu oluşturan suç tipleri tek tek incelenmiş olmakla birlikte, asıl olarak bilişim alanında saklanan kişisel verilerin elde edilmesi ve kullanılması yolu ile işlenecek suçlarda durum ne olacaktır. Görüldüğü üzere hem bilişim alanına karşı işlenen suçlarda (TCK'nin 243. ve 244. maddeleri) hem de kişisel verilerin korunmasına ilişkin suç tiplerinde (TCK'nin 135. ve 136. maddeleri) meşru müdafaa ve bir hakkın kullanılması hukuka uygunluk nedenlerinin özellikleri gereği uygulama yeri yoktur. Bunun yanında bir kanun emrinin (görevin) yerine getirilmesi ve rıza yönünden bu iki suç tipinin

---

[569] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu,* s. 4121
[570] age, s. 6746, Dülger, *Bilişim Suçları,* s. 220
[571] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.848
[572] Hafızoğulları, Zeki, "Türk Ceza Hukuk Ders Notları", http://www.baskent.edu.tr/zekih/uygulamaci/cezahukuk.doc, s. 309 vd. (Erişim: 21.08.2013)

değerlendirilmesine ihtiyaç vardır. Bir kanun emrinin yerine getirilmesi hukuka uygunluk sebebi hem kişisel verilerin korunması hem de bilişim alanında işlenen ilgili suçlar yönünden hukuka aykırılığı ortadan kaldıran sebepler olduğundan elektronik ortamda saklanan bir kişisel verinin elde edilmesi ve kullanılması yolu ile icra edilen eylemlerde de uygulama alanı bulacaktır. Çünkü bir kanun emrini yerine getirmek için bilişim sistemine girerek burada kalan ve burada ki kişisel verileri alarak yine kanunun emrettiği şekilde kullanan kişinin (veri hazırlama memuru) eyleminin suç oluşturduğu söylenemez.

Asıl sorun ilgilinin rızasının hukuka aykırılığı ortadan kaldıracağına ilişkin hukuka uygunluk sebebi yönünden çıkmaktadır. Bu hukuka uygunluk sebebi TCK'nin 243 ve 244. maddeleri için bir hukuka uygunluk nedeni iken TCK'nin 135 ve 136. maddeleri için suç tipinin düzenlendiği bölüm itibarı ile rızanın hukuka uygunluk sebebi sayılamayacağı görüşünün hakim olduğu görülmektedir. Burada temel fonksiyonun ne olduğunu belirlemek konunun çözümünde yol gösterici olacaktır. Her ne kadar kişisel verinin bulunduğu yer bilişim alanı olsa dahi, burada korunmak istenen hukuki yarar kişisel veriler olduğundan bilişim alanında işlenen suçlar değil, kişisel veriler yönünden hukuka uygunluk nedenlerinin bulunup bulunmadığının esas alınması gerekir. Bu durumda rıza hukuka uygunluk nedeni bilişim alanında bulunan kişisel verilerin elde edilmesi veya kullanılması yolu ile işlenen suçlarda hukuka uygunluk nedeni olarak değerlendirilemez.

2.2. SUÇUN MANEVİ UNSURU

Ceza hukukunda failin cezalandırılması için eyleminin iradi olması gerekir. Fail kusurlu davranmış ve olayda kusurluluğunu ortadan kaldıran bir hal bulunmamış olmalıdır. Kusurluluk, suçun kanunilik unsuru, maddi unsur ve hukuka aykırılık unsurundan oluşan objektif nitelikteki unsurları ile olan psikolojik ilişkisinin değerlendirilmesidir. Bu psikolojik ilişki kast veya taksir şeklinde ortaya çıkabilir[573]. Tipikliğin manevi unsurlarının varlığı halinde, ancak o fiil sübjektif olarak da failine

[573] Özgenç, *Türk Ceza Kanun Gazi Şerhi(Genel Hükümler)*, Ankara: Seçkin Yayınevi, 2005, s.241

isnat edilebilir. Bu nedenle failin, tipik haksızlık unsurlarının tümü bakımından kasten veya taksirle hareket etliğinin de belirlenmiş olması gerekir[574]. Suçun bu unsuru eylem açısından incelendiğinde "kusurluluktan", fail açısından incelendiğinde ise "kusurdan" söz edilecektir. Kusur cezalandırılabilir olma, kusurlu davranış ise failin yaptığı için cezalandırıldığı harekettir. Ancak fail, bazı hallerde eylemi kasten veya taksirle gerçekleştirdiği halde, kınanmayabilir. Failin kınanmasına neden olan hususlar eylemle değil, failin özellikleri (*kusur yeteneği)* ile ilgilidir. Bu nedenle, kast-taksir ve kınanabilirlik farklı anlamlar içeren kavramlar olmaktadır[575].

TCK'nin 21. maddesinde "suçun oluşması kastın varlığına bağlıdır" şeklinde ifade edildiği üzere manevi unsur çerçevesinde iki farklı husus göz önünde bulundurulmalıdır; ilk olarak, kasten işlenen bir suçun sübjektif tipinin zorunlu gereği olarak, failin yazılı olsun, olmasın her bir tipiklik unsuru bakımından kasten hareket ettiği belirlenmelidir. Özetle, ceza hukuku sübjektif tipiklik bakımından kural olarak kastı aramaktadır, cezalandırılan taksirli hareketler ise istisnadır. Bu nedenle ancak kasten işlenen hareketler cezalandırılabilir, kanunda açıkça ve ayrıca belirtilmedikçe taksirli hareketler cezalandırılmaz (TCK m. 21/1 c. 1, m. 22/1). Dolayısıyla kural olarak kast**,** istisnai olarak da taksir manevi unsurun temel iki şeklini oluşturmaktadır. Neticesi sebebiyle ağırlaşan suçlarda ise kast ve taksir birlikte bulunmaktadır.

TCK'de "Ceza Sorumluluğunun Esasları" üst başlığı altında iki alt başlık yer almaktadır: "Kast-Taksir" ile "ceza sorumluluğunu kaldıran veya azaltan nedenler". Ceza sorumluluğunu kaldıran veya azaltan nedenler alt başlığında yer alan konular şunlardır. Öğretide; hukuka aykırılığı ortadan kaldıran nedenler başlığıyla incelenen nedenler[576], kusurluluğun önşartı olarak değerlendirilen kusur yeteneğini etkileyen haller[577], kusurluluğu ortadan kaldıran veya azaltan haller olarak ortaya konulan

---

[574] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 131
[575] Centel ve diğerleri, *Türk Ceza Hukukuna Giriş*, s. 344
[576] "Kanunun hükmünü ve amirin emrini ifa, meşru savunma ve zorunluluk hali, hakkın kullanılması ve ilgilinin rızası. (TCK. m.24-27)"
[577] "Yaş küçüklüğü, akıl hastalığı, sağır ve dilsizlik, geçici nedenlerle alkol veya uyuş madde etkisinde olma. (TCK. m.31-34)"

nedenler[578]. Ancak, "kusur yeteneğini etkileyen haller" denilen özelliklerin eyleme değil, faile ilişkin özellikler olduğu, kusur yeteneğinin, suçun bir unsuru olmadığı açıkça belirtilmiştir[579].

TCK'nin 135. ve 136. maddelerinde düzenlenen kişisel verilerin kaydedilmesi suçu genel kast ile işlenen bir suçtur. Failin mağdurun kişisel verilerini kaydedecek nitelikteki davranışları bilerek ve isteyerek gerçekleştirmesi suçun oluşması için yeterlidir. Saik önemli değildir. Genel kast ile işlenen suçun kural olarak olası kast ile işlenmesi de mümkündür. Bu kişisel verinin kaydedilmesi suçu bakımından da geçerlidir. Olası kast, failin neticeyi öğrenmesi ancak meydana gelmesi konusunda kayıtsız kalması, meydana gelmemesi için çaba sarf etmemesi, neticeyi göze alması olarak anlaşılmalıdır. Bu suçlar taksirle işlenemez. Bu suçlar kasten işlenebilir. Bir bilişim sistemine giren ve bu fiili ile kişisel verileri elde ederek suç işleyen kişinin eylemini izinsiz olarak gerçekleştirdiğini ve hukuka aykırı olarak davrandığını bilmeli ve bu sonucu istemelidir. Genel suç işleme kastı yeterlidir. Bu suçlar icrai veya ihmali hareketle işlenebilir ancak taksirle işlenemez[580].

TCK'nin 243. maddesinde düzenlenen suç kasten işlenebilen bir suçtur. Bir bilişim sistemine giren bu fiili izinsiz olarak gerçekleştirdiğini ve hukuka aykırı olarak davrandığını bilmeli ve bu sonucu istemelidir. Madde gerekçesinde de belirtildiği üzere, 243. madde kapsamındaki suç genel kast ile işlenebilir[581]. Sisteme haksız ve kasten girilmesi ve orada kalmaya devam edilmesi ile suç oluşur. Genel suç işleme kastı yeterlidir. Bu suç icrai veya ihmali hareketle işlenebilir ancak taksirle işlenemez[582]. Failin eylemi gerçekleştirirken, iyi ya da kötü niyetli olması, merakını giderme, sistemin güvenliğini deneme gibi düşünceleri suç oluşumunu etkilemez. Fail yetkisiz olduğu halde bir bilişim sistemine girip orada kalmaya devam ederse TCK'nin 243/1. maddesindeki suçu işlemiş olur. Bilişim sistemine

---

[578] Cebir ve şiddet, korkutma ve tehdit, haksız tahrik, hata (TCK. m.28-30).
[579] İçel ve diğerleri, *Suç Teorisi*, s. 198; Erem, Faruk; Danişman, Ahmet ve Artuk, Mehmet Emin, *Ceza Hukuku Genel Hükümleri;* Ankara: Seçkin Yayınevi, 1997, s. 429; Demirbaş, Timur, *Ceza Hukuku Genel Hükümler,* İstanbul: Seçkin Yayınevi, 2011, s. 288.
[580] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 526-530
[581] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 172
[582] Dülger, *Bilişim Suçları*, s.221

giren ve orada kalmaya devam eden failin sistemdeki verileri değiştirmesi, verileri yok etmesi kastını taşıması halinde eylem, 244/2. maddesindeki suçu oluşturacaktır. Failin tesadüfen bir bilişim sistemine girmesi ancak bunu fark ettiği halde sistemde kalmaya devam etmesi halinde de suçun oluşacağı düşünülmelidir[583] . 243. maddenin (3) numaralı fıkrası ile 244. maddenin (1) ve (2) numaralı fıkralarının uygulanmasında, faildeki manevî unsur belirleyici olmaktadır. 243. maddenin (3) numaralı fıkrasının uygulanabilmesi için;

a. Failin 244. maddenin (1) ve (2) numaralı fıkralar kapsamında bir kastının olmaması,
b. Failin fiiline ilişkin kastının haksız olarak sisteme girip orada kalmaya devam etme şeklinde olması ve
c. Failin bu kast ile işlediği fiilinin sonucunda sistemin içerdiği verilerin yok olması veya değişmesi, koşulları birlikte gerçekleşmiş olmalıdır[584].

TCK'nin 244. maddesinde düzenlenen suç ancak kasten işlenebilir. Fail suç oluşturan eylemleri bilerek yapmalı, sağladığı çıkarın haksız olduğunun da farkında olması gerekir. Fiil, olası kastla da işlenebilir. Suçun taksirle işlenmesi olanaklı değildir. Saik aranmaz, 244. maddenin (1) ve (2) numaralı fıkralarındaki suçların manevî unsuru genel suç işleme kastıdır. Failin kastı, (1) ve (2) numaralı fıkralardaki fiilleri bilerek ve isteyerek işlemeye yönelik olmalıdır. 244. maddenin (4) numaralı fıkrasında yani, sanığın yukarıdaki fıkralardaki fiilleri, kendisinin veya başkasının yararına haksız bir çıkar sağlamak amacıyla işlemesinde ise, özel kast söz konusudur[585].

Eğer fail sisteme girip orada kalmaya devam ederken (bu sırada) niyetini

---

[583] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 260

[584] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 530, Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu,* s. 6745, Parlar, *Türk Ceza Kanunu Yorumu,* s. 3744, Kızıltan, *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, s.71

[585] Parlar, *Türk Ceza Kanunu Yorumu,* s. 3753, Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu,* s. 6766

değiştirir ve sistemdeki veriyi kasten değiştirirse, ne olacağı tartışılmalıdır. Acaba bu halde, 243. madde ile 244. madde uygulaması nasıl olacaktır? Bilişim sistemindeki veriyi kasten değiştirme, eğer sistemin işleyişini engellemiyor ve işleyişini bozmuyorsa, 244. maddenin (2) numaralı fıkrasının uygulanması söz konusudur. Bir bilişim sistemine haksız olarak girip orada kalmaya devam etmede ise, 243. maddenin (1) numaralı fıkrası gündeme gelmektedir. Tartışma konusu olayda, hem 243. maddenin (1) numaralı fıkrası ve hem de 244. maddenin (2) numaralı fıkrası birlikte uygulanmamalıdır. Her ne kadar failin başlangıçta kastı yalnızca sisteme haksız girip orada kalmaya devam etme ile sınırlıyken sonradan veri değiştirme kastına da dönüşmüş olsa bile, burada gerçek içtima kuralları uygulanmamalıdır. Çünkü veri değiştirme suçunun işlenebilmesinde, doğal olarak önce bilişim sistemine haksız girmek ve orada kalmak gerekebilir. Bir başka ifadeyle, bilişim sistemine haksız girip orada kalmaya devam etme, sistemden veri değiştirme suçunun unsuru haline gelir ve yalnızca 244. maddenin (2) numaralı fıkrasından hüküm kurulmalıdır[586].

Bilişim sistemi içine kayıtlı bir kişisel verinin değiştirilmesi veya elde edilmesi ile işlenecek suçlarda ise failin suç işleme kastının bulunması gerekir. Bu suçlar taksir ile işlenemez, failde suç işleme iradesinin bulunması gerekir. Her ne kadar bu suçun işlenebilmesi için öncelikle bir bilişim sistemine girilmesi ön koşulu bulunuyor ise de failin asıl amaca kişisel verilere yönelik bulunduğu için burada bilişim sistemine girilmesi ve burada bir müddet kalınmasına yönelik kast değil, kişisel verinin elde edilerek yahut değiştirilerek bir çıkar sağlanmasının veya bir suç işlenmesinin amaçlanmış olması gerekir.

2.3. SUÇUN SÜJELERİ

Her suçta tipikliğe uygun fiili işleyen ve suçtan dolayı hakkı zayi olan, zarara uğrayan kişi ya da kişiler vardır. Bu kapsamda teknik olarak suçun süjesinden

[586] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 190

anlaşılması gereken suçun faili ve mağdurudur[587]. Fail ve mağdur yönünden ayrı ayrı inceleme yapılması lüzumu bulunan bu bölümde öncelikle suçun süjesi olması bakımından kişilik kavramı üzerinde durulması gerekmektedir. Gerçek ve tüzel kişiler hakkındaki genel açıklamalar kişi ve kişilik kavramaları bölümünde incelediği için bu bölümde sadece gerçek ve tüzel kişilerin suç süjeliği yönünden incelemelerde bulunulması yararlı olacaktır. Konunun daha iyi anlaşılabilirliğini sağlamak amacıyla öncelikle tüzel kişilerin ceza sorumluluğu üzerinde durulması daha sonra fail ve mağdur konusunun ayrıntılı olarak ele alınması daha uygun olacaktır.

2.3.1. Suçun Süjesi Olarak Tüzel Kişilerin Sorumluluğunun İncelenmesi

Suç süjesi olabilme açısından kanunun genel düzenlemesinin gerçek kişilerin suç işleyebileceği yönündedir. Ancak bazı suçlar için suçun failinin bir tüzel kişi olup olamayacağı tartışmalı olduğundan bu konudaki tartışmalara yer verildikten sonra inceleme konusu suç açısından tüzel kişilerin sorumluluğunun bulunup bulunmadığının tespiti önem arzetmektedir.

2.3.1.1. Tüzel Kişi Kavramı

Suçun faili ve mağduru olması açısından tüzel kişiliğin ayrıca incelenmesine ihtiyaç vardır. Bazı amaçların gerçekleştirilebilmesinin tek başına mümkün olmaması insanları güçlerini birleştirmeye ve örgütlenmeye sevk etmiş, sonuçta kurumsallaşan bu olgu şeklinde anayasal bir kurum olarak karşımıza çıkmıştır. Kişi veya mal topluluğu biçimindeki bu birliklere hukuk sistemleri tarafından, zamanla "kişilik" tanınmştır. İşte gerçek kişilerin yanı sıra, ayrı bir kişilik olarak tüzel kişiler hukuk düzeni içerisinde yer bulmuşlardır[588]. Hak ve özgürlüklerden yararlanabilme

[587] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 95
[588] Özsunay, Ergün, *Medeni Hukukumuzda Tüzel Kişiler (Tüzel Kişilerin Genel Teorisi- Dernekler-Vakıflar)*, İstanbul: İÜHF Yayınları, No: 549, 1982, s. 3-8

noktasında tüzel kişiler, Anayasada yer alan temel hak ve özgürlükler arasından, nitelikleri ile bağdaşanlardan yararlanabilecektir[589].

Hak ehliyetleri yönünden tüzel kişilerin bazı sınırları bulunmaktadır. Fiziki bir varlığı bulunmayan tüzel kişilerin insanlara has bazı haklardan yararlanma imkanları bulunmamaktadır. Bir kimsenin kendi fiiliyle haklar edinmek ve borçlar üstlenmek şeklinde tanımlanan fiil ehliyeti içerisinde hukuki işlem yapma ehliyeti ve hukuka aykırı fiillerden sorumluluk ehliyeti (isnat yeteneği) birlikte bulunmaktadır. Tüzel kişilerin de fiil ehliyetini, her iki ehliyeti birden kapsayacak şekilde sahip olup, bu haklarını organları aracılığı ile kullanırlar[590]. Haksız fiili kusuru ile gerçekleştiren tüzel kişiye ait organ ile tüzel kişinin TMK'nin 48. maddesi uyarınca, borçlar hukuku bakımından müteselsil sorumluluğunun bulunduğu söylenebilir[591]. Ceza sorumluluğu yönünden ise, bunun toplumsal bir gereklilik olma özelliğinin yanında, özellikle iradesinin olmaması gibi bazı nitelikleri nedeni ile ceza hukukunun bazı temel ilkelerine aykırılık oluşturması karşısında, tartışmalı bir konu olarak durmaktadır[592].

2.3.1.2. Tüzel Kişilerin Ceza Sorumluluğu

Tüzel kişilerin cezai sorumluluğu oldukça tartışmalı bir konudur. Sorumluluğunun bulunduğu yolunda görüş ortaya koyanlar; fiziki bir yapısı bulunmamasının, iradi haraket etmeyeceği anlamına gelmediğini, bünyelerindeki gerçek kişilerin iradelerinden farklı ve onların görüşlerini aşan toplu nitelik kazanmış bir iradenin oluştuğunu, bu niteliği gereği tüzel kişilikle bağdaşan bazı cezai yaptırımların uygulanabileceğini, bu haliyle suç ve cezanın kişiselliği ilkesi ile de çatışmayacağını savunmaktadırlar[593]. Tüzel kişilerin ceza sorumluluğu bulunmadığını savunanlara gelince; tabi olarak tüzel kişilerin kendisine özgü bir iradesinin bulunmadığını, gerçek bir irade olmayınca da kişilikten söz edilemeyeceğini, bu sebeplerle, bizzat

---

[589] Aslan, M. Yasin, "Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu*", Ankara Barosu Dergisi.* http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2010-2/2010-2-aslan.pdf, (Erişim: 13.01.2013), s. 11

[590] Özsunay, *Medeni Hukukumuzda Tüzel Kişiler,* s. 70-74.

[591] Aslan, *Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu,* s. 9

[592] Artuk ve diğerleri, *Ceza Hukuku Genel Hükümler*, s. 230.

[593] Yarsuvat, Duygun, *Tüzel Kişilerin Ceza Sorumluluğu*, Prof.Dr. Sahir Erman'a Armağan, İstanbul: Beta Yayınları, 1999, s. 889.

tüzel kişinin suçun faili sayılmayacağını, ancak suçu işlemek konusunda iradesini kullanan organ gerçek kişilerin ceza hukuku bakımından sorumlu tutulabileceği görüşündedirler[594].

Bu görüşler hakkında bir değerlendirme yapıldığında, tüzel kişilerin ceza sorumluluğunun toplumun korunması ve suçluluğun önlenmesi amacıyla dahi olsa kabul edilemediği, bu nedenle de ceza kanunlarında tüzel kişilerin ceza sorumluluğuna yer verilmediği sonucuna ulaşılmaktadır. Aksine bir yaklaşım ceza hukukunun temel ilkelerinden olan cezaların şahsiliği ilkesiyle çatışacağından diğer ilkelerine de aykırı düşmüş olur. Suç ve cezaların şahsiliği ilkesinin ihlali anlamına gelecek şekilde tüzel kişilerin sorumluluğuna dair yapılacak düzenlemeler Anayasaya da aykırılık oluşturacaktır[595]. Ceza hukukunda, suçun maddi unsurunu oluşturan fiil, mutlaka bir insan davranışı olmalıdır. Tüzel kişilerin organları olan kişilerin eylemlerinden dolayı tüzel kişinin sorumlu tutulması, başkasının fiilinden sorumlu tutulma sonucunu doğuracaktır ki, böyle bir düzenleme ise, Anayasanın 38. maddesinin altıncı fıkrasına açıkça aykırı düşecektir. Yeni TCK'nin kabul ettiği sistemde tüzel kişiler işlenen bir suçtan dolayı cezalandırılamazken, tüzel kişiliğin faaliyetleri kapsamında işlenecek bir suçun, niteliği ve amacı farklı olduğu için, tüzel kişiye idari para cezası mahiyetinde cezalar verilebilecektir. Günümüzde bazı ceza hukukçuları tüzel kişilerinde suçun faili olabileceğini savunmaktadırlar. Tüzel kişilerin, para cezası, müsadere, faaliyetten alıkoyma gibi cezaları öngören suçların faili olmamaları için sebep yoktur[596]. Bu açıklamalar kapsamında inceleme konusu suçun failinin ve mağdurunun ayrı ayrı incelenmesi gerekecektir.

2.3.2. Suçun Faili

Bilişim kaynaklı kişisel verilerin korunması hakkında ceza sorumluluğu yönünden her saldırının arkasında bir bilgisayar olduğu düşünülürse bireyler yönünden yapılması gerekeni tespit önemlidir. Birleri ve sıfırları yargılamayacağımıza göre

---

[594] Dönmezer ve Erman, *Nazari ve Tatbiki Ceza Hukuku*, s. 465–470.
[595] Aslan, *Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu, s. 12*
[596] Soyaslan, Doğan, *Ceza Hukuk Genel Hükümler*, Ankara: Yetkin Yayınları, 2012, s. 239.

kişisel bazda ceza sorumluluğunun kimde olduğunu tespit edilmesi gerekir[597]. Fail; suçun aktif süjesidir. Her suçun bir aktif süjesi vardır. Mademki suç devlet tarafından düzenlenen bir yasağın ihlalidir. O halde bu yasağı ihlal eden bir kişi yoksa suç da yoktur. Fail, TCK'nin 37. maddesinde, suçun kanuni tarifindeki fiili gerçekleştiren kişi olarak tanımlanmıştır. Suçun kanuni tarifinde yer alan fiil üzerinde hâkimiyet kuran, kanuni tanıma uygun haksızlığı gerçekleştiren kişi faildir[598].

Ceza hukukunun giderek kişinin iradesini gözönüne alan bir ceza hukuku olması suçun aktif süjesinin şart ve niteliklerini artırmıştır[599]. Bu suçların kanuni tarifinde faille ilgili olarak "kişi", "her kim" gibi ifadelere yer verilir. Bu itibarla, hareket yeteneğine sahip olan her gerçek kişi bu suçların faili olabilir. İşte bu tür suçlara "genel suçlar" denir. İnceleme kapsamındaki suç tipleri bu kapsamda ki suçlardır. Buna karşılık bazı suçların kanuni tanımında, bu suçların ancak özel bir yükümlülük altında bulunan ve belli faillik özelliğini taşıyan kişiler tarafından işlenebileceği belirtilmektedir. İşte, kanuni tanımında belli özelliğe sahip olanların fail olabileceği belirtilen bu tür suçlara "özgü suçlar" denilmektedir. Bu tür suçlar özel faillik vasfını taşıyanlar tarafından işlenebilmektedir. Örneğin TCK'nin 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunun nitelikli hali olan 137. maddede ki düzenlemede ki fail ancak kamu görevlisi, yetki sahibi bir kişi ya da bir meslek sahibi tarafından işlenebilir[600].

Fail kapsamında inceleme konusu bilişim alanındaki kişisel verilerin korunması olduğu için bilişim alanının failleri ile birlikte kişisel verilerin korunması kapsamında bu suçu işleyebilecek kişiler olarak sınıflandırmamız daha doğru olacaktır. Buna göre, bu suçların failleri öncelikle bilgisayar kullanıcıları olacaktır. Bilgisayar kullanıcıları hakkında kısaca bir inceleme yapacak olursak; genel olarak belli bir düzeyin üzerindeki bilgisayar kullanıcılarında değişik özelliklerin görülebildiği ortaya konulmaktadır. Bu özelliklerin başlıcaları; meraklı olmak,

---

[597] Mueller, Robert S., "The Cyber Threat Planning for the Way Ahead", http://www.fbi.gov/news/stories/2013/february/the-cyber-threat-planning-for-the-way-ahead, (Erişim:16.01.2013)
[598] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 103
[599] Soyaslan, *Ceza Hukuk Genel Hükümler*, s. 239
[600] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 104

detaylarla ilgilenmek, kendi meslek veya tutkularıyla ilgili problem veya sıkıntılı konuları çözmek, sezgiye dayalı düşünmeye yönelmek, zor konularda orijinal çözümler üretmektir. Bilgisayarlar, daha önce hiçbir suçta görülmemiş bir biçimde suç işleyenlere, kimliklerini gizleme olanağı sunmaktadır ve bilişim sistemlerindeki bireylerin ve şirketlerin özel ve gizli alanlarına kolaylıkla izinsiz girme ve orada kalma imkânı vermektedir[601].

Bilişim araçlarını vasıta kılarak suçu işleyenler de, bilişim teknolojisinden yararlanmaktadırlar. Bilişim teknolojisindeki katlanarak artan ilerlemeler, hem bilişim suçlarına konu alanı ve olanakları artırmakta ve hem de bu teknoloji bilişim suçu faillerine yeni suç işleme kolaylıkları sağlamaktadır. Bu suçun faillerinin teknolojideki yenilikleri suç işlerken kullanmaları ise, suçla mücadele eden görevlileri bilişim suçlarıyla mücadelede yeterli olmaktan uzak tutmaktadır. Bu bakımdan, bu suçlarla mücadele eden birimlerin, faillerin suç işleme tekniklerini, kullandıkları teknolojiyi ve faillerin niteliklerini bilmeleri ve buna göre stratejiler üretmeleri zorunludur[602]. Bilişim suçlarına ilişkin bölümde anlatılan fail portresine atıfta bulunup bu genel açıklamalardan sonra kişisel veriler ile ilgili olanlara göre bir sınıflandırma yapılarak fail konusunu incelemekte yarar bulunmaktadır. Öncelikle kişisel verilere en yakın olan ve en kolay şekilde kişisel verilere ulaşabilen veri işleyenin cezai sorumluluğu üzerinde durmak gerekecektir.

2.3.2.1. Veri İşleyenin Sorumluluk ve Yükümlülükleri

"Kişisel Veri İşleme" kavramı son derece geniş bir kavramdır. Bu kavram, otomatik olarak yapılıp yapılmadığına bakılmaksızın kişisel veriler üzerinde gerçekleştirilen herhangi bir işlem veya işlem dizisine de uygulanmaktadır.[603]. Veri koruması mevzuatının uygulanması otomatik işleme ve otomatik olmayan işleme ile sınırlıdır. Kişisel verilerin hukuka uygun ve dürüst bir şekilde toplanması ve işlenmesi; amaçla

---

[601] Loren, D. Mercer, M. F. S, "Computer Forensic Characteristics And Preservation of Digital Evidence", *FBI Law Enforcement Bulletin*, Vol. 73, Number, March 2004

[602] Carter, David, L, "Computer Crime Categories How Techno-Criminals Operate", *FBI Law Enforcement Bulletin*, V.64, July 1995, s. 26.

[603] Başalp, *Kişisel verilerin Korunması ve Saklanması*, s. 33.

bağlılık olarak da adlandırılan, belirli ve önceden belirtilmiş amaçlar için kullanılması, belirlenen amaçlarla bağdaşan şekilde kullanılması; belirlenen amaçlarla uygunluk göstermeyen kişisel verilerin toplanmaması ve işlenmemesi, belirlenen amaçlar için gerekli olduğu süreden daha fazla saklanmaması; kişisel verilerin işlenmesine ilişkin usul ve esaslara göre işlenmemesi durumunda veri işleyicisinin bu durumdan sorumlu tutulması hususları bu başlık altında toplanabilir[604]. Bunlardan başka Bennet'in güvenlik ilkesi olarak adlandırdığı, veri işleyen tarafından verilerin hukuka aykırı olarak üçüncü kişilerin eline geçmesini önleyici tedbirlerin alınması[605] da bu başlık altında düşünülebilir.

2008 tarihli Kişisel Verilerin Korunması Kanun Tasarısının 3. maddesinin birinci fıkrasının (ı) bendinde, "veri kütüğü sahibi" kavramına yer verilmiş iken 2014 tarihli tasarıda bu kavram metinden çıkarılmış yerine "Veri sorumlusu" getirilmiştir. Veri kütüğü sahibi, "Kişisel verilerin işlenmesinin amaç ve metodlarını tek başına veya başkaları ile birlikte belirleyen gerçek ve tüzel kişiler" olarak ifade edilmiştir. 2014 tarihli Kişisel Verilerin Korunması Kanun Tasarısının 3. maddesinin birinci fıkrasının (ğ) bendinde düzenlenen "veri Sorumlusu", "Birim, kurum veya kuruluşlarda veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi" ifade etmektedir. Ayrıca madde gerekçesinde, kişisel veriler üzerindeki tüm kontrol yetkisi ve sorumluluğun veri sorumlusuna ait olduğu ve bu kişilerin gerçek veya kamu kurumları, dernekler, şirketler veya vakıflar gibi tüzel kişi olabileceği belirtilmiştir. Grup şirketlerde ise, gruba dahil olan her şirket ayrı ayrı veri kütüğü sahibi olarak kabul edilecektir[606]. Kişisel verileri işleyenler ise, veri sorumlusunun verdiği yetkiye dayanarak, onun adına verileri işleyen gerçek ve tüzel kişilerdir. Bu kişiler verileri işlemekte ancak kişisel veriler üzerinde kontrol yetkisi ve sorumluluk veri sorumlusuna ait bulunmaktadır. Veri işleyenlere örnek olarak

---

[604] Cate, Fred H., *Privacy in the Information Age,* Washington, D.C.: Brookings Institution Press, 1997,s. 46

[605] Bennet, J. Colin, *Regulating Privacy: Data Protection and Public Policy in Europe and United States*, London: Cornell University Press, 1992, s. 110

[606] Şen, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa Ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", s. 1198

muhasebeciler, acenteler gibi başkası adına veri işleyen kurumlar sayılabilir[607]. Keser Berber ise veri sorumlusunu "veri koruması görevlisi" olarak betimlemektedir. Buna göre Keser Berber veri koruması görevlisini "Tek başına veya başkalarıyla ortaklaşa kişisel veri işlemenin amaçlarını, araçlarını ve yöntemlerini belirleyen gerçek veya tüzel kişi" olarak tanımlamaktadır[608]. Veri işleyen tipik olarak, kişisel verilerin sıralanması ve kombinasyonu gibi işlemenin teknik yönlerini yürütmek üzere, veri sorumlusu tarafından görevlendirilmiş uzmanlaşmış taraf olacaktır[609].

Kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan birinci ilke kişisel verilerin hukuka uygun ve dürüst bir şekilde toplanması ve işlenmesidir. Kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan dürüst toplama ve işleme ilkesi ile ilgili olarak, kişisel verilerin kişinin nasıl kullanıldığının anlaşılamayacağı tarzda kullanılamaması şeklinde yorumlanması gerektiği, bu ilkeye yer verilmeyen bir durumda kişisel verinin kullanımının sınırlandırılamayacağı dile getirilmiştir[610]. Kişisel verilerin hukuka aykırı olarak kaydedilmesinin ve ele geçirilmesinin TCK'de suç olarak düzenlenmesi ve kişisel verilerin işlenmesine ilişkin genel bir düzenleme bulunmaması karşısında hukukumuz bakımından da dürüst ve hukuka uygun işlemenin hangi hallerde gerçekleşebileceğinin tespiti önem taşımaktadır.

Kişisel verilerin işlenmesi, temel hak ve hürriyetlere ve özellikle özel hayatın gizliliğine bir müdahale teşkil etmektedir. Bu açıdan kişisel verilerin işlenmesine ilişkin bir düzenlemede her şeyden önce Anayasanın 13. maddesinde belirtilen temel hak ve hürriyetlerin sınırlandırılması koşullarına uyulmak zorundadır. Bu maddeye göre, temel hak ve hürriyetler ilgili maddesinde belirtilen sınırlandırma nedenlerine bağlı olarak ancak kanunla sınırlandırılabilir. Bu açıdan kişisel verilerin işlenebilmesi için de genel ya da özel kanunlarda, Anayasanın 13. maddesinde belirtilen şartlara uygun olarak Anayasanın 20. vd. maddelerinde düzenlenmiş

---

[607] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.104
[608] Keser Berber ve diğerleri, *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*, s. 122
[609] Study On Legal And Regulalory Aspects Of E-Health: Legally E-Health, Deliverable 2, Processing Medical Data: Data Protection, Conlidentiality And Security, 2006, s. 13.
[610] Cate**,** *Privacy in the Information,* s. 189 vd.

bulunan özel hayatın gizliliğine ilişkin sınırlandırma sebepleri doğrultusunda, kişisel verilerin işlenmesine izin veren ya da zorunlu kılan bir düzenlemenin bulunması zorunludur. Bu açıdan öncelikli olarak TCK ve özel kanunlarda yer alan ve Anayasanın 13. ve 20. maddelerine uyan hukuka uygunluk nedenlerinin varlığı halinde kişisel verilerin hukuka uygun bir şekilde işlendiğini söylemek mümkündür. Ayrıca, kişisel verilerin korunması devlet ve birey arasında dikey bir koruma sağlamasına yönelik olması yanında bireyler arası ilişkilerde ortaya çıkan yatay bir etkiye sahiptir. Bu açıdan kişisel verilerin korunması, Türk Medeni Kanunun ilgili maddeleri uyarınca kişilik hakkının korunması anlamına da gelmektedir[611]. Sonuç olarak dürüst ve hukuka uygun toplama ve işleme, diğer ilkelerle birlikte, temel hak ve hürriyetlere ve özellikle özel hayatın gizliliğine, kişisel verilerin işlenmesi alanında hukuka uygun müdahalenin esasını göstermektedir. Bu açıdan kişisel verilerin işlenmesine ilişkin düzenlemelerde temel hak ve hürriyetlerin ve özelde özel hayatın gizliliğinin sınırlandırılması koşullarına uyulması zorunludur. Yukarıda adı geçen düzenlemelerin hepsinde açıkça yer alan dürüst ve hukuka uygun toplama ve işleme ilkesi de bu hususun vurgulanması anlamını taşımaktadır.

Dürüst toplama ve işleme ilkesi kişisel verilerin işlenmesi alanında işlenme amacı ile sıkı sıkıya bağlantılıdır. Nitekim kişisel verilerin korunması alanında amaçla bağlı olma, işleme sürecinin kapsam ve sınırını belirlemekte ve aynı zamanda dürüstlük hukuka uygun toplama ve işleme ilkesine uyulup uyulmadığının saptanmasında belirleyici kıstas olarak karşımıza çıkmaktadır. Bununla birlikte, olası kullanıma olanak yaratılması için verilerin toplanması yasaktır[612]. Kişisel verilerin özellikle üçüncü kişilere aktarımı sonucu ilgililerinin zarara uğramaları durumunda, verileri doğru olarak tutmayan veya güncellemeyen veri sorumlusu, ilgili kişilerin uğradıkları zararlar nedeniyle sorumlu olacaktır. Ayrıca, veri sorumlularının, verilerin saklanma sürelerini açıkça belirlemeleri gerekmektedir. Herhangi bir veri, daha fazla saklanması için geçerli bir sebep yoksa mutlaka silinecek veya yok edilecektir[613]. Gelecekte kullanma ihtimali gerekçesiyle veri saklanamaz. Bu durum özel hayatın

---

[611] Başalp, *Kişisel verilerin Korunması ve Saklanması*, s. 10
[612] Kılıç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", s. 1111.
[613] Keser Berber ve diğerleri, *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*, s. 122

gizliliği ilkesi açısından çok önemli olup, koruma alanının sınırının geniş tutulmasında ve devletin özel alana müdahalesinin dar tutulmasında önemli bir yer arz etmektedir.

Bu kapsamda kişisel veriler önceden belirlenmiş ve hukuka uygun amaç ya da amaçlar için toplanması ve bu amaçlarla bağdaşmayan şekillerde işlenmemesi olarak özetlenebilecek olan amaçla bağlılık ilkesi ise, kişisel verilerin dürüst ve hukuka uygun olarak işlenip işlenmediğinin somut bir durumda gerçekleşip gerçekleşmediğinin tespiti bakımından önem taşır. Amaçla bağlılık, kişisel verilerin toplanma miktarının ve somut bir durumda kişisel verinin meşru işleme sınırlarının tayini, ayrıca toplanan kişisel verinin niteliği yani verinin doğru, tam ve işlenme amacı ile ilgili olması bakımından merkezi bir konuma sahiptir[614]. Amaçla bağlılık ilkesi, aynı zamanda, kişisel verilerin meşru amaç ya da amaçlar için işlenebileceği anlamına gelmekte olup, bu haliyle kişisel verilerin işlenmesinde sınırlandırıcı bir etkiye sahiptir. Bu ilke uyarınca, kişisel veriler kural olarak önceden belirlenmiş ve şüpheye yer vermeyecek şekilde belirli olan amaç ya da amaçlar için işlenebilir ve gelecekte ortaya çıkma ihtimali olan ve hâlihazırda bilinmeyen amaç ya da amaçlar için kişisel veriler işlenemez[615]. Aynı şekilde, kişisel veri ancak toplanma anında belirtilmiş amaç doğrultusunda amaca uygun bir şekilde işlenebilir; belli olan bu amaçla ilgisiz başka amaçlar için işlenemez.

Amaçla bağlılık ilkesi, kişisel verilerin rızaya bağlı olarak işlenmesi durumunda rızanın varlığı ve kapsamının belirlenmesi bakımından önemlidir. Belirsiz ve çok genel amaçlar için kişisel verilerin işlenmesi yasaklanmış bulunmaktadır. Bu açıdan, kişinin rızası da toplanma ve işlenme anında kişiye bildirilen amaç ya da amaçlar için geçerli olup belirtilen bu amaçlar dışındaki amaçlar için, kişisel verilerin işlenmesine ilişkin geçerli bir rızanın varlığından söz edilemez. Bu açıdan, geçerli bir rızanın varlığının tespiti bakımından da geriye dönük

---

[614] Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, s. 225

[615] Spiros, Simitis, *Reviewing Privacy ın an Information Society*, Pennsylvania**:** University of Pennsylvania Law Review**,** 1986-1987**,** Vol. 135, No. 3 (March, 1987). http://www.jstor.org/stable/331207910.2307/3312079. (Erişim: 21.03. 2014) s. 740

bir inceleme yapılması ve toplanma ve işlenmeye başlandığı andaki amaç ya da amaçların belirlenmesi gerekmektedir[616]. Özetle, amaçla bağlılık kişisel verilerin çok işlevli kullanılmasını sınırlandırma ve kişisel verilerin işlenmesinde keyfiliğin önlenmesi amacıyla getirilmiş bir ilkedir. Kişisel verilerin toplanma miktarının (asgarilik ilkesi) ve somut bir durumda kişisel verinin meşru işleme sınırlarının tayini (kullanımının sınırlandırılması ilkesi); toplanan kişisel verinin niteliği (doğru, tam ve işlenme amacı ile ilgili olması) bakımından merkezi bir konuma sahiptir. Ayrıca, kişisel verilerin amacın gerçekleştirilmesi sonunda imha edilmesi ya da anonim haline getirilmesi yükümlülüğü bakımından da amaca bağlılık ilkesi önemlidir[617].

Kişisel verilerin işlenmesinde idarecilerin dikkat etmesi ve mutlaka uyması gereken ilkeler bulunmaktadır. Bu ilkeler özetle şu şekildedir;

Kişisel veriler mutlaka hukuka ve dürüstlük ilkelerine uygun işlenmelidir. **(Hukuka Uygunluk İlkesi)**

Kişisel veriler ancak sınırlı olarak, belirli amaçların gerçekleştirilmesi için kaydedilebilir. **(Amaca Uygunluk İlkesi)**

Kişisel veriler ancak toplanma amacına uygun olarak gerektiği kadar işlenebilir, başka amaçlar için kullanılmaz. **(Veri Tasarrufu İlkesi)**

Kişisel veriler objektif olarak işlenmeli ve doğru olmalıdır. **(Doğruluk İlkesi)**

Kişisel veriler gerektiğinden fazla saklanamaz kayıt altında tutulamaz. **(Sınırlı Tutulma İlkesi)**

Kişisel veriler ilgili kişinin kişisel veriler hukukuna uygun bir biçimde işlenebilir.**(Kişilik Haklarına Riayet İlkesi)**

---

[616] Ketizmen. *Türk Ceza Hukukunda Bilişim Suçları*, s. 226
[617] age, s. 227

Kişisel veriler sadece güvenli bir ortamda işlenebilir. **(Güvenlik İlkesi)**

Kanuni bir dayanak olmadan kişisel veriler üçüncü kişilere verilemez ve paylaşılamaz. **(Verilerin Paylaşılmazlığı İlkesi)**[618]

2.3.2.2. Bilişim Alanında Saklanan Kişisel Verilere Yönelik Suçlar Yönünden Fail

Kişisel verilerin kaydedilmesine ilişkin TCK'nin 135. maddesindeki suçun faili herkes olabilir[619], fakat öncelikle bu suçun failleri gerçek kişiler olabilir. Gerçek kişileri de kendi içinde şu şekilde sınıflandırarak mümkündür. Eylemin sonucunda doğacak menfaatten yararlanacak kişiler bu işlemi bizzat yapabilirler. Bir başkasına ait kişisel verileri hukuka aykırı olarak kaydederek, bunu suçta kullanan kişinin eylemi de bu madde kapsamında değerlendirilebilir. Fakat bu suçun oluşması hukuka aykırı şekilde kişisel verinin kaydedilmesi ile olur. Ayrıca verinin suçta kullanılması aranmamaktadır. Bir başkası adına hareket edenler de bu suçun failleri arasında kabul edilmelidir. Çünkü suç kişisel verinin hukuka aykırı olarak kaydedilmesi ile oluştuğu için kişinin namına çalıştığı kişi ki bu eylemi karşılığında maddi menfaati olsun ya da sadece yardım veya eğlence için bunu yapıyor olsun fark etmez, bu eylem sonucu elde edilen kişisel veriyi bir suç işlemekte kullanmamış olsa dahi kişisel verinin hukuka aykırı olarak kaydedilmesi ile suç oluşur. Bu durumda ki kişilerin eylemi iştirak kapsamında düşünülebilir. Kişisel verilerin hukuka aykırı kaydedilmesi bazen örgütlü suçlara da konu olabilmektedir. Burada amaçlanan şantaj, menfaat temini gibi konularda kullanılmak üzere kayıt yapılmakla birlikte, bazen sadece kayıt yapılarak (fişleme gibi) ileride kullanılmak üzere de saklanabilir. Örgütlü suçta fail kamu görevlileri olabileceği gibi özel hukuk kişileri tarafından da örgütlü olarak bu eylemin gerçekleştirildiği görülmektedir. Çete tabir edilen suç örgütlerinin kişilerin aile, cinsel yaşam, sağlık, ekonomik durum gibi kişisel

---

[618] Ersoy, *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, s.103, Kılınç, *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, s. 1113

[619] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.4117 ve 4124, Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.528

verilerini elektronik ortamda elde ederek kişilerden şantaj ve tehditle maddi menfaat elde ettikleri yaygın kullanılan bir yöntem olarak karşımıza çıkmaktadır[620].

Genel olarak buradaki hukuka aykırı kayıt eylemi açısından kişisel verinin kayıt biçimi önemli olmayıp, mekanik, manyetik, elektronik veya başka herhangi bir yöntemle veya kağıt gibi bir meteryal üzerinde kayda alınması arasında bir ayırım gözetilmez. İnceleme konusu kapsamı içerisinde ise bu kaydı tutan kişinin bilişim alanında gerçekleştirmiş olması gerekmektedir. Eylemi veri toplama yükümlülüğü veya yetkisi bulunan kişinin hukuka aykırı olarak yapması bu suçu oluşturacağı gibi, üçüncü bir kişinin de gerçekleştirmesi mümkündür. Genelde bu eylemin gerçekleştirilmesinde saik farklı nedenler olabilir. Klasik suçların bilişim alanında da işlenilmesi imkanı vardır. Bunun için kişisel veriye ihtiyaç duyulduğunda TCK'nin 135. maddesindeki yasaklamaya aykırı olarak elde edilen kişisel veriler kullanılarak suç işlenebilecektir. Kanunda 136. maddede düzenlenen, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek suçunun faili, herkes olabilir. Madde metninde suçun faili olmakla ilgili özel bir hüküm yer almamaktadır. Açıklanan nedenle bu suçun faili ile ilgili olarak 135. maddede düzenlenen suç tipinde ve genel açıklamalarda yapılan faile dair açıklamalar yeterlidir. Fail yönünden özel bir düzenleme ise 135 ve 136. maddeler için 137. maddede düzenlenmiştir. Kanunun bu maddesine göre kişisel verilerin kaydedilmesi suçu, kamu görevlisi tarafından ve görevinin gerektirdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenirse, bu husus artırım nedenidir[621].

TCK'nin 243. maddesindeki suçun faili herkes olabilir, suçun faili olabilmek için maddede herhangi bir özelliğe sahip olmak aranmamıştır, madde metninde "kimse"den söz edilmiş, ancak bu kişinin hangi özelliklere sahip olması gerektiği konusuna değinilmemiştir. Bu nedenle anılan suçun faili herhangi bir kimse olabilir, bu suç faili bakımından özgü suçlardan değildir. Bilişim sistemine hukuka aykırı

---

[620] Parlar ve Hatipoğlu, *Türk Ceza Kanunu Yorumu*, s. 2088,
[621] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.4117 ve 4124, Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.528

olarak giren veya orada kalmaya devam eden kimse, bu suçun failidir. Bu kimsenin eylemi gerçekleştirmedeki niyetinin, amacının, saikinin bir önemi bulunmamaktadır, bu kişi bir şeyler çalmak için de girse, eğlenmek, güvenliği denemek, protesto etmek gibi bir nedenle de girse anılan suç oluşur, burada failin amacının bir önemi bulunmamaktadır, önemli olan bilişim sistemine girmesi ve orada kalmaya devam etmesidir. Bu tür suçların işlenebilmesi için elbetteki belirli bir düzeyde bilgi donanımına sahip bulunmak gerekse de, bu husus sadece şahsın bu suçu gerçekleştirebilmesini becerebilmesi için gerekli olup kanunen istenen bir özellik değildir. TCK'nin 244. maddesinde düzenlenen suçun faili "kişi" olarak düzenlenmiş olduğundan, bu suçun faili de herkes olabilir. Fail yönünden herhangi bir özelliğe sahip olma kriteri de düzenlenmemiştir. Bilişim sisteminin işleyişini engelleyen, bozan, bilişim sistemindeki verileri bozan, yok eden, değiştiren, erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka yere gönderen kişi, bu suçun failidir[622].

Faille ilgili bir konunun da açıklanmasında fayda bulunmaktadır. Bilindiği gibi, ancak belli sıfatı ya da nitelikleri taşıyan kişiler tarafından işlenebilen suçlar vardır. Mesela rüşvet alma ve zimmet suçları veya görevi suiistimal ya da görevi ihmal suçları gibi. Herkesin zimmet suçunun faili olabilmesi mümkün değildir. Çünkü suçun oluşabilmesi için görevi nedeniyle faile teslim edilmiş mal üzerinde suçun işlenmesi gerekmektedir. Sıradan birisinin görevi bulunmadığından doğal olarak suç da gerçekleşmiş olmayacak demektir. Zimmet suçunun bilişim alanındaki mukabili 244. maddede tanımlanmıştır[623]. Örneğin bir kamu bankasındaki bir memurun kendisine görevi nedeniyle tevdi edilmiş ya da erişim imkanı verilmiş ticari değeri çok yüksek bir kısım sırları kendisinin veya bir yakınının menfaat elde etmesi için bilişim ortamında başka bir yere gönderse (hesabına para aktarması gibi bir veri aktarımı değil, belli bilgileri içeren veriler söz konusu) aktarılan veri mal olarak kabul edilseydi şahıs da memur olduğundan bunun zimmet olarak değerlendirilmesi söz konusu olacaktı. Ancak veri mal olarak tanımlanmadığından

[622] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6756.
[623] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 640 ve 846.

244/son maddesinin açık hükmü de göz önüne alınarak, fail bu madde uyarınca cezalandırılacaktır.

Genel olarak; bu suçların faili genellikle hacker olarak adlandırılır. Hacker, bilişim suç faillerinin tamamını anlatmak için kullanılmaktadır. Hacker, ceza hukukunda "sahip bulunduğu teknolojik aygıt ve bilgi birikimi ile bir bilişim sistemine kişisel verileri elde etmek veya sahtecilik ve dolandırıcılık gibi çeşitli suçları işlemek için yetkisiz olarak işleme erişebilen kimse" anlamında kullanılmakladır. Bu kimseler çoğu zaman bilişim sistemini alaya almak ve bu sistemi yaratanlardan daha çok bu sisteme hakim olduklarını göstermek için bu yola başvurmaktadırlar[624]. Bilişim vasıta kılınarak kişisel verilerin kullanılması yolu ile işlenen suçlarda bilişim sistemine girme ve buradaki verileri değiştirme ve bozma suçunun faili yönünden bir özellik getirilmediği için bu suçtan menfaat temin eden ile birlikte menfaat temin edecek kişi adına bu işi yapan kişi de suçun faili olacaktır. Ancak burada fikri içtima kuralları gereği menfaat temin eden adına hareket eden kişinin eylemi TCK'nin 244/2. maddesinde ki suçu oluştururken, bu eylem sonucu menfaat temin eden kişi için elde edilen menfaatin türüne göre TCK'nin 244/4. maddesi veya dolandırıcılık vb. gibi suçlar olacaktır. Kişinin kendi kişisel verileri üzerinde bu eylemi gerçekleştirmesi halinde ise fail kişisel veri sahibi olurken mağdur, aleyhine suç işlenen kamu veya özel kuruluş olacaktır. Örneği kişi SGK kayıtlarına girerek kendi emeklilik şartlarını lehine değiştirdiğinde burada fail sonuçta elde edilecek menfaatten yararlanan kişi olup TCK 244/2 anlamında bir suç işlemiş olurken, mağdur Sosyal Güvenlik Kurumu (SGK) olacaktır[625].

Fail konusunda önemli bir konuda yazılım şirketlerinin sorumluluğudur. Bilgisayarın yazılım (Softwere) donanımı, bilgisayarın çalışmasına yarayan değişik kodlamalardır. Peki bu yazılımların sorumluluk açısından önemi varmıdır? Hacker'lar ve virüs yazarları sık sık ticari yazılımların güvenlik açıklarını istismar

---

[624] Tulum, *Bilişim Suçları ile Mücadele,* s. 48 vd.
[625] Artuk, Mehmet Emin; Gökçen, Ahmet ve Yenidünya, Ahmet Caner, *Türk Ceza Kanunu Şerhi*, Ankara: Turhan Kitapevi, 2009, Cilt 5, s. 4638

ederek internet üzerinden saldırırlar[626]. Bilgisayar güvenlik uzmanlarının çoğu, yazılım üreticilerinin bu pazarda kendi ürünlerini satabilmek için önce bu kusurları en çok bilen olması gerektiğini söylemektedir. Ancak, birçok işletmeler ve devlet kurumlarının yazılım güvenlik açıkları yoluyla saldırıya uğradı ve zararların milyarlarca dolar olduğu ortaya kunulmuştur. Antivirüs ürünleri üreten yazılım satıcılarının sorumluluğunu gerektiren hiçbir kanun bulunmamaktadır. Aynı şekilde, hiçbir yazılım şirketi hiç bir ürününden dolayı, bilinen bir güvenlik kusurundan kaynaklanan zararlardan sorumlu olmamıştır. Yazılım satıcıları müşterilerin bu ürünler kullanmadan önce kabul etmesi gereken son kullanıcı lisans sözleşmeleri (EULA - End User License Agreement[627]) içine feragatname ekleyerek sorumluluktan kaçınmışlardır. Genel olarak, lisans sözleşmelerinin ürün ile ilgili tüm riskleri kullanıcılarına açıklaması gerekir.Yazılımın modern dünyada oynadığı önemli rolü göz önüne alındığında, bilgisayar güvenlik uzmanları yazılım şirketinin yazılım ürünleri üretmek için sorumluluk alma zamanının geldiğini söylemektedirler.

2.3.2.3. Fail yönünden eylemin nitelikli hali

Kişisel verilerin korunmasına dair fail konusunda TCK özel durumları 137. maddede düzenlemiştir[628]. Madde kapsamında kişisel verilerin kaydedilmesi suçu, kamu görevlisi tarafından ve görevinin gerektirdiği yetkiyi kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenirse, bu husus cezanın arttırılması nedeni sayılmıştır[629]. Madde ağırlaştırıcı hali iki durum için belirlemiştir. Bunlardan birincisi suçun kamu görevlisi tarafından ve görevinin verdiği yetkiyi kötüye kullanmak suretiyle işlenmesi halidir. Bu halde eylemin

---

[626] Tulum, *Bilişim Suçları ile Mücadele,* s. 50

[627] Wikipedia, "Son Kullanıcı Sözleşmesi", http://en.wikipedia.org/wiki/End-user_license_agreement, (Erişim: 16.09.2014)

[628] **"Nitelikli hâller**
MADDE 137. - (1) Yukarıdaki maddelerde tanımlanan suçların;
a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,
b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,
İşlenmesi hâlinde, verilecek ceza yarı oranında artırılır."

[629] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, Cilt: I, s. 4117

sadece kamu görevlisi tarafından gerçekleştirilmiş olması yeterli olmayıp ayrıca görevin verdiği yetkinin kötüye kullanılması suretiyle işlenmiş olması gerekir[630].

Kamu görevlisi tabirinden kamu kesiminde çalışan herkes gibi bir anlam çıksa bile genel bir tanımlama ile kamu görevlisi; kamu tüzel kişileri tarafından bir kamu hukuk rejimine göre çalışan herkesi kapsamaktadır[631]. İdare Hukuku anlamında bir kişinin kamu görevlisi olması için kamu kesimindeki bir örgüte bağlı olarak çalışması gerekir. Anayasanın 128. maddesine göre, kamu görevlilerinin ayırt edici niteliği, bunların genel idare esaslarına göre yürütülen kamu hizmetlerinin gerektirdiği asli ve sürekli görevleri görmeleridir. Böylece Anayasada, dar anlamdaki kamu görevlilerinin, *memurlar ve öteki kamu görevlilerinden* oluştuğu kabul edilerek diğer kamu görevlileri deyimiyle kamu hukuku kurallarına tabi olarak çalışanlar ifade edilmektedir. Örneğin, hakimler ve savcılar, kamu iktisadi teşebbüsü personeli, Türk Silahlı Kuvvetleri personeli, üniversite öğretim elemanları devlet memurlarından ayrı bir personel rejimine tabi olmakla, diğer kamu görevlilerini oluşturmaktadır[632]. Maddede geçen kamu görevlisi kavramı, TCK'nin 6. maddesinin c bendinde; "Kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi" biçiminde tanımlanmıştır[633]. Bu bakımdan, ceza kanunu açısından idare hukuku anlamındaki kamu görevlisi yerine daha geniş manadaki kamu görevlisi kavramının nazara alınması gerekir. Örneğin mesleklerinin icrası bakımından avukat veya noter kamu görevlisidir. Bunun gibi bilirkişilik, tercümanlık ve tanıklık faaliyetinin icrası kapsamında kamu görevlisidir[634]. Özetle bir kişinin kamu görevlisi sayılması için ayırıcı ölçüt yaptığı faaliyetin kamusal bir faaliyet sayılmasıdır. Bu anlamda söz konusu nitelikli halin varlığını kabul için kişinin kamu görevlisi olması yeterli değildir; görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi gerekir. Öte yandan fiilin kamu görevi sırasında işlenmesi mümkün ise de yeterli değildir. Fiilin görevin verdiği yetki kötüye kullanılmak suretiyle işlenmesi gerekir. Görevin verdiği

---

[630] Parlar ve Hatipoğlu, *Türk Ceza Kanunu Yorumu*, s.2096
[631] Fındıklı, s. 106
[632] Özbek, *TCK İzmir Şerhi,* s. 951
[633] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s 4130
[634] Parlar ve Hatipoğlu, *Türk Ceza Kanunu Yorumu*, s 2096

yetkinin kötüye kullanılmasından ne anlaşılmalıdır? TCK'nin 137. maddesi nitelikli hal olarak düzenlenmiş olsa da 135. madde ve 136. madde ile birlikte düşünüldüğünde 257. maddede düzenlenen görevi kötüye kullanmanın özel şeklini ifade etmektedir[635]. Bu nedenle görevin verdiği yetkinin kötüye kullanılması kavramını açıklanması bakımından 257. maddedeki düzenlemeden yararlanılabilir.[636] Eğer yapılan fiil kamu görevlisinin görev alanına girmiyor ise bu nitelikli halin uygulanması mümkün olmamalıdır. Örneğin polis memurları, jandarma görevlileri veya istihbarat elamanlarının gerektiğinde mahkemeden karar alarak kişilerin özel hayatlarına müdahale edebilirler. Ancak, herhangi bir hukuka uygunluk nedeni olmadan örneğin, 2559 sayılı PVSK'nın 5. maddesi uyarınca karakola gelen kişilerin fotoğrafları çekilerek bilgisayar ortamına atılması ve burada saklanması bu suçu oluşturur[637].

Hareketin görev gereklerine ne zaman aykırı olacağı konuyu düzenleyen mevzuat özellikle idare hukuku kuralları ve bu doğrultuda oluşmuş genel uygulamaya göre belirlenir. Öreğin CMK'nin 81. maddesi "fizik kimliğin tespiti" tedbirini düzenlemekte olup, kişisel veri niteliğinde olan kişinin "fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntülerinin" kayda alınabilmesine imkan sağlamaktadır (CMK m.81/1). Ancak bunun için kişinin üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanık olması gerekir. İşte kişinin bu niteliklileri taşımamasına rağmen söz konusu kişisel verilerinin kaydedilmesi durumunda TCK m. 137/1-a'daki nitelikli hal uygulanabilir. Tipte

---

[635] **"Görevi kötüye kullanma**
MADDE 257. - (1) Kanunda ayrıca suç olarak tanımlanan hâller dışında, görevinin gereklerine aykırı hareket etmek suretiyle, kişilerin mağduriyetine veya kamunun zararına neden olan ya da kişilere haksız bir kazanç sağlayan kamu görevlisi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."
"(2) Kanunda ayrıca suç olarak tanımlanan hâller dışında, görevinin gereklerini yapmakta ihmal veya gecikme göstererek, kişilerin mağduriyetine veya kamunun zararına neden olan ya da kişilere haksız bir kazanç sağlayan kamu görevlisi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır."
"(3) İrtikâp suçunu oluşturmadığı takdirde, görevinin gereklerine uygun davranması için veya bu nedenle kişilerden kendisine veya bir başkasına çıkar sağlayan kamu görevlisi, birinci fıkra hükmüne göre cezalandırılır."

[636] Özbek, *TCK İzmir Şerhi,* s. 952

[637] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 4131

açıkça yer almadığına göre kişisel verilerin bu şekilde kaydedilmesi ile bir zararın ortaya çıkmış olması şart değildir. Önemli olan fiilin kamu görevlisinin görevini kötüye kullanmak suretiyle işlemiş olmasıdır[638].

Ağırlaştırıcı durumlardan diğerinin bağlandığı hal ise suçun belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesidir. Bu nitelikli halin uygulanabilmesi için kamu görevlisi olmayan failin, eylemi icra etmekte olduğu belli bir meslek veya sanatın sağladığı kolaylıktan yaralanarak işlemiş olmaları gerekir[639]."*Belli bir meslek ve sanatın sağladığı kolaylıktan* " ne anlaşılması gerektiği konusunda karşılaşılan bir sorun da "Meslek ve Sanat" ibaresidir. Buradan yapılan uğraşının her iki niteliğe de sahip olması gerektiği gibi bir anlam ortaya çıkarmaktadır. Halbuki söz konusu nitelikli halin de uygulanması bakımından yapılan uğraşının hem meslek hem de sanat niteliğinde olması gerekmez; bunlardan biri olması yeterlidir. Meslek ve sanat farklı kavramları ifade etmekte olup[640], herhangi bir meslek ve sanat bu nitelikli halin uygulanması bakımından gerekir ve yeterlidir. Ancak bunun için söz konusu meslek ve sanatın sağladığı kolaylıktan yararlanılmak gerekir. Bu yönüyle meslek ve sanatın söz konusu suçu işlemek yönünde elverişli olması gerekir. Yani meslek ve sanatın icrası ile suçun işlenmesi arasında bir nedensellik bağlantısı kurulabilmelidir[641]. O halde failin yaptığı meslek ve sanat kişisel verilerin kaydedilmesi konusunda faile bir kolaylık sağlaması ve bu kolaylığı kullanarak failin bu suçu işlemesi gerekir[642]. Örneğin bir bilgisayar tamircisinin sistemde depolanan başkalarına ait kişisel verileri ele geçirmesi, bir sauna işçisinin yerleştirdiği gizli kamera ile müşterilerine ait görüntüleri kaydetmesi, bir doktorun mesleğinin sağladığı kolaylıktan yararlanarak elde ettiği hastasının özel

---

[638] Özbek, *TCK İzmir Şerhi*, s. 953
[639] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 4131
[640] Bu konuda bakınız:
Türk Dil kurumu sözlüğü, "Meslek Nedir", http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTs.52b48b85df 2970.46760857, (Erişim:: 20.12.2013)
Türk Dil kurumu sözlüğü, "Sanat Nedir", http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTs.52b48b8de4efa2.10698734 (Erişim:: 20.12.2013)
[641] Şen, *TCK'nin Yorumu*, Cilt:1, s. 609
[642] Parlar ve Hatipoğlu, *Türk Ceza Kanunu Yorumu,* s. 2097

hayatına ilişkin bilgi ve görüntüleri hukuk dışı bir amaç için biriktirmesi durumlarında TCK'nin 137. maddesindeki nitelikli hal uygulanacaktır[643].

2.3.2.4. Failin İnternet Yönünden İncelenmesi

İnternet vasıta kılınarak işlenen suçlar yönünden fail konusu da önem arzetmektedir. İnternet artık çoğu kimsenin günlük yaşamına girmiş ve hatta vazgeçilmezlerinden olmaya başlamıştır. İnternet sadece bir haberleşme aracı olmaktan çıkmış, iş, eğlence ve hatta suç işleme aracı olarak kullanılmaya başlamıştır. İnternet yolu ile işlenen suçlara ilişkin 5651 sayılı kanunun getirdiği hükümler önemlidir.

İnternet, teknik olarak birden çok bilgisayarın ve bilgisayar ağlarının birbirine bağlanmasına dayalı bir iletişimi öngören bilişim – iletişim ağıdır[644]. Diğer bir söyleyişle İnternet, dünya üzerindeki milyonlarca bilgisayarın birbirlerine bağlanmaları ile oluşan dünya çapında bir bilgisayar ağları sistemini ifade etmektedir[645]. İnternet, insanların küresel çapta iletişim kurduğu yeni ve benzeri olmayan bir ortamdır[646]. İnternetin en önemli özelliği eskiden olduğundan farklı olarak çift yönlü iletişime imkan tanımasıdır.[647]. Bu yönü ile bireysel ve kitle iletişim aracı haline gelmiştir[648]. İnternet, 1973 yılında Birleşik Devletler Savunma Konulu İleri Araştırma Projeleri Dairesi (Defense Advanced Research Projects Agency-DARPA) tarafından ağa bağlı çok sayıda bilgisayar arasında paket anahtarlamalı veri iletimini destekleyen iletişim protokolleri geliştirmek amacıyla başlatılan ve "İnternetting Project" adı verilen bir araştırma projesinden esinlenerek ortaya

---

[643] Örneğin Amerikan Tıp Birliği, bir sigorta şirketine karşı sorumluluğu olan veya bir kurumda çalışan hekimlerin muayene sırasında sahip olduğu kişisel verileri yasal zorunluluk olmadıkça veya önceden verilmiş bir rıza bulunmadıkça açıklanamayacağı görüşünü savunmaktadır. Riddick, Frank A, "American Medical Association, Council on Ethical and Judicial Affairs. Code of Medical Ethics, Current Opinions with Annotations.", *The Oschner Journal*, 2003, s.146

[644] İçel, Kayıhan ve Ünver, Yener, *Kitle Haberleşme Hukuku: Basın-Radyo-Televizyon-Sinema-Video-İnternet,* İstanbul: Beta Yayınları, 2009, s. 465

[645] Erkan, Boğaç ve Songür, Murat, *Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü,* Ankara: Hacettepe-Taş yayını, 1999, s. 282

[646] Sırabaşı, *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz,* s. 52

[647] İçel ve Ünver, *Kitle Haberleşme Hukuku,* s. 476

[648] Dülger, Bilişim Suçları, 2004: s. 50

çıkmıştır[649]. İnternet kelimesi, İngilizce *International Network'un* (Uluslararası Çalışma Ağı) kısaltılmışı olarak da tanımlanmaktadır[650]. İnternet insanların bulundukları yerlerden bilgiye bağımsız bir şekilde erişebilmeleri ve bilginin paylaşımı hayalinin bir sonucudur[651].

İnternet, teknik özelliği açısından ağlardan oluşmaktadır. Fakat bu ağların herbiri kendi içinde bağımsız yönetilmekte ve denetlenmektedir. İnternetin bu özelliğinden dolayı bireysel olarak denetlenebilen fakat küresel anlamda yönetim ve denetimi tam olarak yapılamayan bir yapıyı ifade etmektedir[652]. İnternetin denetimi, piramit gibi yukarıdan aşağıya doğru değildir. İnternet bir düzlem üzerinde iki nokta arasındaki birden fazla iletişim ağının bulunduğu bir yapıya sahip olduğundan denetleme ancak her bir ağ üzerinde yapılabilmektedir[653]. İnternet Erişim Sağlayıcılar (İnternet Access Provider – IAP) ise, kullanıcıların İnternet ağına erişmelerini sağlamakla görevli bir internet süjesidir. Bu süjenin görevi sadece erişim sağlamak olduğundan verileri kendi sunucularında depolayarak bu bilgilere İnternet üzerinden erişilebilirlik imkanı verme gibi bir hizmet sunmamaktadır[654]. Genelde telefon/telekomünikasyon idareleri tarafından mevcut telefon hatları üzerinden özel hatlara internet bağlantısı hizmetini sunmaktadır[655]. İnternet Servis Sağlayıcılarının (İnternet Service Provider-ISP) görevi ise, kullanıcıların bu servis sağlayıcılara ait bilgisayarlar üzerinden, internete giriş yapabilmeleri için bir kapı görevi görmektedirler. Yalnız İnternet Servis Sağlayıcılar bu hizmeti bir sunucu (server) kullanarak yapabilmektedir. Yani her internet servis sağlayıcının sunucu'su bulunmak zorundadır. Sunucu bilgisayar ve bu

---

[649] Cerf, V.G, "İnternet History", www.isocilt:org/internet/history/cerf.shtml, (Erişim: 31.07.2011)

[650] Bozel, Savaş, "5651 sayılı Kanuna istinaden Bazı İnternet sitelerine Erişimin Engellenmesi Tedbirine Eleştirel bir yaklaşım", http://www.e-akademi.org/makaleler/sbozel-5.htm. (E.T: 22.08.2010) s. 749

[651] Yıldırım, Mustafa Fadıl, "Bilgisayar Programlarında Akdi ve Teknik Kullanım Sınırlamaları ve Kullanıcının Hukuki Konumu", *Erzincan: EÜHFD*, Cilt. VII, Sayı. 1-2, 2003, s. 23

[652] Yıldız, Sevil, *Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden incelenmesi*, http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler/SevilYILDIZ/YILDIZ,SEVİL.pdf (Erişim: 03.08.2011)

[653] Sarıhan, Tan Deniz, *Herkes İçin Internet*, İstanbul: Desnet Yayınları. 1998, s.19; Savaş, Abdurrahman. *İnternet Ortamında Yapılan Sözleşmeler,* 2005, Yayımlanmamış Doktora Tezi, Konya: Selçuk Üniversitesi Sosyalbilimler Enstitüsü, s. 19

[654] Güran, Sait; AkünAl, Teoman; Bayraktar, Köksal; Yurtcan, Erdener; Kendigelen, Abuzer; Beller, Önder ve Sezer, Bülent, "İnternet ve Hukuk Temel Metni", İstanbul, 2000, http://www.superonline.com/hukuk/hukuk.htm. (Erişim: 21.07.2011), s. 20

[655] Yıldız, Sevil, *Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden incelenmesi,* s.613

hizmet için üretilmiş programdan oluşmaktadır[656]. Bir bilginin sunucu üzerinden internette yayınlanması sunucunun önemi ortaya çıkartmaktadır. Kullanıcılar kendilerinin veya başkalarının olsun tüm bu bilgileri önce bir sunucuda depoladıktan sonra yayınlayabilirler. Bu durum; kullanıcı gerçek veya tüzel kişileri internet erişimi hizmeti alabilmek için bir İnternet Servis Sağlayıcı ile anlaşmak zorunda bırakmaktadır. Her bilgi internet üzerinden yayınlanacak şekilde olmadığından İnternet İçerik Sağlayıcılar (İnternet Content Provider- ICP), bu görevi yerine getiren kişi ya da kuruluşlardır. Bilgileri internette yayınlanacak şekilde düzenleyen süjelerdir. İnternetin en son ucunda kullanıcılar bulunmaktadır. Kullanıcılar ise; internet üzerinden yayınlanan bilgi ve belgeleri okuyan, görüntüleri izleyen ve kişisel bilgisayarlarına yükleyen gerçek kişilerdir. Kullanıcıların en önemli özelliği, "İnternet Ceza Hukukunda" hem sanık hem de mağdur rolünde karşımıza çıkmakta olmasıdır[657]. Portal, internet sitelerine bağlantıların, genellikle alfabetik olarak listelendiği sitelerdir. Sanal alemde ise, internet hizmetlerinin ana kapısıdır. Kurumun internetteki yüzüdür. Bunlara Excite, AOL, Google, MSN, Netvibes, Yandex ve Yahoo gibi internet portalları örnek verilebilir[658].

2.3.2.5. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna (5651 sayılı İnternet Kanunu) göre İnternet Süjelerinin Sorumluluğu

Genel Olarak, 5651 sayılı kanunun (sk) 1. maddesinde, Kanunun amaç ve kapsamını; "içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülükleri ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir" şeklinde belirlemiştir. İnternet süjelerinin ayırımı, gördükleri fonksiyona göredir. Bu nedenle somut olayda bir internet süjesinin sorumluluğunun belirlenebilmesi için öncelikle bu süjenin niteliğinin belirlenmesi gereklidir. Çünkü erişim sağlayıcı olarak

---

[656] Sınar, Hasan, *İnternet ve Ceza Hukuku,* İstanbul: Beta Yayınları, 2001, s. 41

[657] Demir, Vedat. "Türkiye'de Özel Radyo ve Televizyonların Çıkışı ve Bu Konuda Devlet Tekelinin Kalkması", *Marmara İletişim Dergisi*. Sayı: 7.7.1994. s. 3.

[658] Wikipedia, "Portal", https://tr.wikipedia.org/wiki/portal, (Erişim: 05.08.2011)

faaliyet gösteren bir internet süjesi, aynı zamanda yer sağlayıcı, hazırlayıp sunduğu içerikler yönünden de içerik sağlayıcı da olabilir[659].

Yargıtay 9. Ceza Dairesi bir kararında; *"...Mahkemece üniversitelerin bilgisayar ve ceza hukuku kürsüsünden seçilecek internet konusunda uzman bilirkişi kurulu ile keşif yapılarak ... AŞ'nin bir internet servis sağlayıcı mı, erişim sağlayıcı mı yoksa her iki fonksiyona birlikte mi sahip olduğu, internet servis sağlayıcı olması durumunda sahibinin kim olduğu, ayrıca dava konusu yazının yayımlandığı forumun sitesi sisteminin bir işletene (moderatör) bağlı olup olmadığı hususların saptanmasından sonra sanığın hukuki durumunun takdir ve tayini gerekirken eksik soruşturma ile hüküm kurulması,"* şeklinde[660], henüz internet süjelerinin sorumluluklarına ilişkin kanuni bir düzenleme bulunmadığı dönemde, başkası tarafından gönderilen içerik dolayısıyla cezai sorumluluğunun, web sayfasını işleten kişinin "yer sağlayıcı" mı, yoksa "erişim sağlayıcı" mı olduğunun belirlenmesine bağlı olduğuna yerinde olarak karar vermiştir.

5651 sayılı Kanun, internet hizmeti sunmaları açısından dört süje belirlemiştir. Yükümlülükleri ve sorumluluklarıyla birlikte düzenlen Kanunda süjelerin tanımı şu şekilde yapılmıştır: "*İçerik sağlayıcı*, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri (5651 sk. m.2/1, f), *Yer sağlayıcı,* hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri (5651 sk. m.2/1, m), *Erişim sağlayıcı,* kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri (5651 sk. m.2/1, e), *Toplu kullanım sağlayıcı,* kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı (5651 sk. m.2/1, i) ifade etmektedir."

---

[659] Yıldız, Ali Kemal, "2007 Tarihli Yeni Türk İnternet Kanunu ve İnternet Süjelerinin Cezalandırılabilirliği", *Alman–Türk Karşılaştırmalı Ceza Hukuku*, http://www.jura.uni-wuerzburg.de/fileadmin/02150100/IWAS/ Materialien/Dtt_Yildiz.pdf. (Erişim: 03.08.2011) s. 383

[660] Yargıtay 9. CD, 25.10.2001 tarih ve E.2001/1854, K.2001/2649 sayılı karar, http://www.ozgureralp.av.tr/web/2013/09/21/t-c-yargitay-9-ceza-dairesi-e-20011854-k-20012649-t-25-10-2001/, (Erişim: 30.07.2014)

Süjelerin Sorumluluğunu tek tek alarak incelemekte yarar bulunmaktadır; 5651 sk. m.4/l'e göre, içerik sağlayıcı yönünden bir ayırım yapmak gerekir. İçerik sağlayıcının bizzat kendisinin, internet ortamında hizmete sunduğu her türlü içerikten sorumludur, ancak bağlantı sağlamakla birlikte başkasının olan içerikten sorumlu değildir. Ancak içerik sağlaycı kendi sunmadığı fakat başka içerik sağlayıcıların erişim sağladığı içerikler yönünden sorumsuz kılmak adil olmayacaktır. Çünkü konusu suç teşkil edecek bir içeriğe erişim sağlanması da iştirak kurallarınca suç teşkil edecektir. Bu durumda bir değerlendire yapılarak içerik sağlayıcı, bu içeriğin sunuş şeklinden, bağlantı sağladığı içeriği benimsediği ve kullanıcıların bu içeriğe erişimine imkan sağlamayı amaçladığı belli oluyorsa genel hükümlere göre sorumludur (5651 sk. m.4/2,). 5651 sk. m.4/2'de, yerinde bir hüküm getirmiştir. Gerçekten de içerik sağlayıcı, kendi içeriği vasıtasıyla başka bir içeriğe bağlantı sağlamakla birlikte (link vermekte), bu içeriği denetleme imkanına sahip bulunmamaktadır. Böyle durumlarda, içerik sağlayıcının bağlantı sağladığı bir içerikten sorumlu tutulabilmesi için, m.4/1 anlamında bu içeriğin bilindiğinin ve mal edinildiğinin belirlenmesi gerekir[661]. Çünkü 5651 sk. m. 4/2, içerik sağlayıcının ancak kendisinin kusurlu fiilinden sorumlu tutulabileceğini ve objektif sorumluluğa yer verilmediğini göstermektedir[662].

Yer Sağlayıcı ya da servis sağlayıcısı, kullanıcıların internetle erişimim sağlayan doğrudan internet bağlantısına sahip olma yanında, başkaları taralından hazırlanan verileri, kendi sunucularında depolayarak internet ortamına aktarma işlevini de üstlenir[663]. 5651 sk. m. 5/1. maddesine göre, "*Yer sağlayıcı, sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.*" Bu hüküm, yer sağlayıcıların ceza sorumluluğunu önleyebilecek ve dolayısıyla internetin gelişimine katkı sağlayabilecek niteliktedir[664]. Ancak, 5/2. maddesine göre, "*Yer sağlayıcı, yer sağladığı hukuka aykırı içerikten,*

---

[661] Erman, Barış R., "Alman Hukukunda İnternetten Kaynaklanan Ceza Sorumluluğu", *İÜHFD*, Cilt: 59, Yıl: 2001**,** Sayı. 1-2, s. 214

[662] Yıldız, "2007 Tarihli Yeni Türk İnternet Kanunu ve İnternet Süjelerinin Cezalandırılabilirliği", s. 383

[663] Sınar, *İnternet ve Ceza Hukuku*, s.87

[664] İçel ve Ünver, *Kitle Haberleşme Hukuku,* s. 490

ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, bu Kanunun 8. ve 9. maddelerine göre haberdar edilmesi halinde ve teknik olarak imkan bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür", "*Koruma tedbiri niteliğindeki erişimin engellenmesi kararını yerine getirmeyen yer sağlayıcısı, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde altı aydan iki yıla kadar hapis cezası ile cezalandırılır*" (5651 sk. m. 8/10).

Erişim sağlayıcı, başkalarına ait verileri depolama imkânına sahip olmayan ve fakat doğrudan internet bağlantısına sahip olan internet süjesidir. Erişim sağlayıcı, başkalarına ait verileri saklayabileceği sunuculara sahip olmaması nedeniyle, işlevsel olarak servis sağlayıcıdan ayrılmaktadır. Bu ayırımın sonucu ise, sadece erişim sağlama hizmeti veren bu süjenin ceza sorumluluğunun kabul edilmemesidir[665]. Nitekim, 5651 sk. m. 6/2'de, "*Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir"* şeklinde, bu durum belirtilmiştir. Erişim sağlayıcının sorumluluğu bulunmamakla birlikte, 5651 sk. 6/1. madde uyarınca yükümlülükleri; *"a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikte bu kanun hükümlerine uygun olarak haberdar edilmesi halinde erişimi engellemek, b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlene kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamak, c) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usullere uygun olarak Kuruma teslim etmek"* olarak belirlenmiştir. Yukarıdaki görevleri ile ilgili olarak cezai yaptırmlarda hüküm altına alınarak "Bu yükümlülüklerden (b) ve (c) bentlerinde yer alanlardan birini yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin Türk Lirasından ellibin Türk Lirasına kadar idari para cezası verilir (5651 sk. m.6/3)" düzenlemesine yer verilmiştir.

---

[665] Sınar, *İnternet ve Ceza Hukuku*, s. 89

Toplu Kullanım Sağlayıcı; 5651 sk. 7/1. maddede, *"Ticari amaçla toplu kullanım sağlayıcılar, mahalli mülki amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahalli mülki amir tarafından Kuruma bildirilir"* ve 5651 sk. 7/2. maddede *"Ticari amaçla olup olmadığına bakılmaksızın bütün toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlüdür"* şeklinde, ticari amaçla toplu internet ulaşımını sağlayan yerlerle ilgili olarak (örneğin internet kafeler), AB tavsiye kararları doğrultusunda, toplu kullanım sağlayıcıların yükümlülüklerini, düzenlemiş ve bunlara uymamanın yaptırımını da, *"üçbin Türk Lirasından onbeşbin Türk Lirasına"* kadar idari para cezası olarak öngörmüştür (5651 sk. m.7/3).

2.3.3. Suçun Mağduru

Suçun mağduru ya da suçun pasif süjesi kavramı ceza ve ceza muhakemesi hukuku bakımından önemli sonuçlar doğurmaktadır. Bu nedenle kavramın doğru tanımlanması, sınırlarının belirlenmesi gerekir. Ceza hukuku alanında, tüzel kişilerin ve devletin suç mağduru olup olamayacakları tartışılmakla beraber genel görüş olarak tüzel kişiler ve bir tüzel kişi olan devletin de suç mağduru olabileceği yolundadır. Bunun yanı sıra, tüzel kişiliği bulunmayan toplum, aile, devletler topluluğu gibi topluluklara karşı da suç işlenebilir. Ceza hukuku da dahil olmak üzere hukuk alanında süje daima kişidir. Şeyler, ancak hukuki işlem, hukuki fiil ya da ilişkilerin konusunu, objesini oluşturabilir[666]. Uygulamada suçun mağdurunun tespiti açılan kamu davasında taraf tespiti ve teşkili açısından önem arz etmektedir[667].

Suçun konusu ile mağdur kavramı da birbirine karıştırılmamalıdır. Suçun mağduru, suçun konusunun ait olduğu kişidir. Örneğin, TCK'nin 135 ve 136. maddelerinde düzenlenen suçun konusu kişisel verilerdir. Buna karşılık, mağduru, bu

---

[666] Toroslu, Nevzat, *Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu*, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayını, 1970, s. 141

[667] Yargıtay CGK, 26.12.2012, E:2012/11-1065, K:2012/1438, *http://emsal.yargitay.gov.tr /VeriBankasiIstemciWeb/GelismisDokumanAraServlet.* (Erişim: 15.06.2014)

verilerin sahibi olan, kişidir[668]. Suçun konusuna zarar verilmesi veya bunun zarar tehlikesine maruz bırakılması suretiyle, korunan hukuki değer ihlal edilmiş olmaktadır[669]. Suçun mağduru ile suçtan zarar gören kavramlarını da birbirine karıştırmamak gerekir[670]. Kural olarak mağdur, aynı zamanda bir suçun işlenmesi dolayısı ile zarar gören kişidir. Örneğin, kişisel verileri ele geçirilen kişi suçunun mağduru, aynı zamanda bu suçun işlenmesi dolayısı ile zarar gören kişidir. Fakat suçtan zarar gören kişi, her zaman bu suçun işlenmesi dolayısı ile mağdur edilen kişi değildir[671]. Örneğin bir veri işleme memuruna cebir veya tehdit tatbiki suretiyle ya da hileye maruz bırakılması ile kişisel verilerin ele geçirilmesi ve bu verilerin bir suçta kullanılması halinde, suçun mağduru, kendisine cebir veya şiddet tatbik edilen ya da hileye maruz bırakılan görevlidir. Buna karşılık, suçtan zarar gören, bu suretle kişisel verisi kullanılan kişidir.[672].

Bilişim alanındaki kişisel verilerin elde edilmesi suçları, hem bilişimi ve hemde kullanıcıları etkilemektedir. Esasında bu suçlardan, bilgisayarlar, bilgi sistemleri, kullanıcılar ve daha ötesi devlet ve toplum zarar görmektedir (geniş anlamda mağdur). Bunun yanında, bilişim suçları, bireyleri ve organizasyonları da mağdur etmektedir. Fiilin, kişisel verileri elde edilerek zarara uğratılan bir kişi olması kadar bir kurum veya kuruluşun bilişim sistemleri aracılığıyla yerine getirdiği kamu hizmetlerini aksatması halinde toplumu oluşturan fertleri de mağdur etmesi nedeni ile mağdur kavramını genişletmek mümkündür.

Bununla beraber, mağduru olmayan bir suç bulunmadığına göre, bütün suçlarda mağdurun gerçek kişi olma zorunluluğu olup olmadığı, tüzel kişilerin suç mağduru olması konusu tartışmalıdır. Özgenç ve Ünver'e göre suçun mağduru sadece gerçek kişilerdir, tüzel kişiler, bir suçun işlenmesi dolayısı ile zarar görmüş

---

[668] Özgenç, İzzet: *Düşünceyi Açıklama Hürriyeti ve Ceza Hukuk*, 75. Yılında Cumhuriyet ve Hukuk Sempozyumu, Diyarbakır, 22-23.10.1998, s.191
[669] İçel ve diğerleri, Suç Teorisi, s. 87 vd.
[670] Dönmezer ve Erman, *Nazari ve Tatbiki Ceza Hukuku*, Cilt: II, s. 1174
[671] Ünver, Yener, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, s.144, 145
[672] Özgenç, İzzet, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayınevi, Ankara: 2012, s. 211

olabilirler, ancak mağdur olamazlar[673]. Aksi görüşte olan yazarlara göre ise tüzel kişi de hukuken "kişi"'dir. Bu nedenle farklı varlık ya da menfaatlerin hamili ve hak sahibi olması önünde bir engel yoktur. Bir tüzel kişi tacirin, malvarlığına karşı suçların mağduru, pasif süjesi olması mümkündür.

Aile, toplum ya da bir devletler topluluğu gibi tüzel kişiliği olmayan kişi topluluklarının dahi suçun mağduru olup olamayacağı konusunda farklı görüşler bulunmaktadır. Bu kişilerin sayıları belirsiz de olsa, söz konusu suçlar aslında ancak bu kişilere karşı işlenebilir. Bu anlayışın sonucu olarak, söz konusu suçlarda çok sayıda mağdur bulunduğunu kabul etmek gerekecektir. Bir başka görüşe göre, aileye, topluma ya da devletler topluluğuna ait olduğu ileri sürülen varlık ya da menfaatler, aslında bireylere ya da devlete aittir. Bu nedenle, aileye ya da topluma ait varlıklardan bahsedilmesi ve bunların suçun mağduru, pasif süjesi olarak kabul edilmesi mümkün değildir[674].

Devletin suçun mağduru olup olmayacağı konusu da tartışmalıdır. Bir görüşe göre, devlet hak süjesi değildir. Bu anlayışa göre, sadece bireyler hak süjesi olabilirler. Bu nedenle de devletin suç mağduru ya da suçun pasif süjesi olması hukuken olanaksızdır[675]. Fakat suç mağduru sıfatının ya da mağdur kavramının, hak süjeliği ile sınırlandırılması da doğru değildir. Ceza hukuku düzeni, hak düzeyine ulaşmamış birçok varlık ya da menfaati de korumaktadır. Cezai korumanın konusu, sadece haklar değildir. Bu nedenlerle, tüzel kişilere ait varlık ya da menfaatlerin cezaen korunması halinde bu tüzel kişilerin suç mağduru olarak kabul edileceği açıktır. Devleteya da topluma karşı suçlarda her bireyin suç mağduru olarak kabulünün ceza ve ceza muhakemesi hukuku bakımından vahim sonuçları olacaktır. TCK'de, Üçüncü Kısmın başlığı için "Topluma Karşı Suçlar", Dördüncü Kısmın başlığı için ise, "Millete ve Devlete Karşı Suçlar" ifadeleri kabul edilmiştir. Bu

---

[673] Ünver, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, s. 141, Özgenç*, Türk Ceza Hukuku, Genel Hükümler,* s. 205
[674] Toroslu, *Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu*, s. 180 - 181.
[675] Ünver, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, s. 142,

düzenleme, aslında topluma yani tüzel kişiliği olmayan bir kişi topluluğuna ve bir tüzel kişi olan devlete karşı suç işlenebileceğinin kabulü olarak anlaşılmalıdır[676].

TCK'nin 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunun mağduru olmakla ilgili özel bir düzenleme yer almamaktadır. Bu nedenle bu suçun mağduru herkes olabilir[677]. Kişisel verilerin elde edilmesi/kullanılması suretiyle işlenen suçların ilk aşaması sayabileceğimiz kişisel verilerin kaydedilmesi suçunda öncelikle doğal olarak mağdur, kişisel verinin sahibi olacaktır. Kişisel veri sahibinin yukarıda suçun mağduruna ilişkin olarak yaptığımız açıklamalar doğrultusunda tüzel kişilerinde mağdur sıfatını taşıyıp taşımayacağı konusu üzerinde durulması gerekecektir.

TCK'nin "Kişisel Verilerin Kaydedilmesi" başlıklı 135. maddesi gerekçesinde, "*gerçek kişi ile ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiği*" belirtilmiştir. Madde metni ile çelişen bu yorumda gerçek ya da tüzel kişi olarak kısıtlama getirmeyen madde metnine rağmen gerekçe, sadece gerçek kişilerin bu suçun mağduru olabileceklerine işaret ederek, madde metnini ve amacını aşan bir yorum getirmiştir. Korunması gereken kişisel verinin tüzel kişiyede ait olabileceği gerçekliği karşısında sadece gerçek kişilere ait kişisel verinin korunmasına hasretmek doğru olmayacaktır. Kaldı ki her ne kadar bünyesinde bulundurduğu gerçek kişilerden ayrı bir hukuki varlıkları ve kimlikleri bulunan tüzel kişilerin de kendi yapılarına özgü kişisel verilerinin olacağı tartışmasızdır. Kanun koyucunun, "kişi" ve "kişisel" kavramları ile yalnızca gerçek kişilere güvence sağlamayı hedeflemiş olduğunun kabulü yasanın amacı ile de çelişir. Bu yoruma en uygun düzenleme 135. maddenin ikinci fıkrasında bulunmaktadır, ancak asıl suçu tanımlayan 135/1. maddesi, korunan hukuki yararın mağduru olabilecek kişiler bakımından gerçek kişi-tüzel kişi ayırımı yapmamıştır. Açıklanan nedenlerle, tüzel kişilere ait verilerinde TCK'nin 135 ile 136. maddeleri kapsamında korunabileceğini belirtmek yanlış olmayacaktır. Her ne kadar yukarıda açıklanan sonucun çıkacağı

---

[676] Katoğlu, Tuğrul, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları", *AÜHFD*, 61 (2) 2012, s.657-693 http://dergiler.ankara.edu.tr/dergiler/38/1679/17897.pdf. (Erişim: 13.01.2014)

[677] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 4117 ve 4125.

vurgulansada, TCK'nin 2. maddesinde düzenlenen "suçta ve cezada kanunilik" ilkesine dayanılarak yapılacak bir itirazla karşılaşılmaması için, TCK'nin 135. maddesini de kapsayacak şekilde tüzel kişilere ait verilerin korunmasına yönelik kanuni değişikliklerin yapılmasında yarar bulunmaktadır. Kaldı ki TCK'nin 239. maddesin de "Ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması" suçunun tüzel kişileri koruduğu savunulabilir. Ancak bu madde de korunan hukuki yararın ekonomi, sanayi ve ticarete dair verilerdir. Özel hayat ve hayatın gizli alanına ilişkin hukuki yarar kapsamında düzenleme getiren TCK'nin 135. maddesinin uygulama açısından, gerçek kişiler kadar olmasa bile tüzel kişilerin de özel hayat kapsamında ele alınabilecek ticari hayatlarının bulunduğunu dikkate alarak madde koruması kapsamına dahil etmek daha uygun olacaktır. Tasarının 3. maddesinin gerekçesinde, kişisel verilere örnek olarak kişilerin telefon numarası, pasaport numarası, özgeçmişi, parmak izleri, genetik bilgileri, psikolojik, fiziki, kültürel ve sosyal özellikleri sayılmıştır. 2008 tarihli Kişisel Verilerin Korunması Kanunu Tasarısı'nın 3/1,a-c maddesi hükümleri, korunması gereken "kişisel veri" kavramının kapsamına, gerçek kişilerin yanında tüzel kişilere ait verileri dahil etmiş olmasına karşın 2014 tarihli Kişisel Verilerin Korunması Kanunu Tasarısı sadece gerçek kişilerden bahsetmektedir. Yine Tasarının 2. maddesinin birinci fıkrasında, "Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen, otomatik olan veya olmayan yollarla herhangi bir veri kütüğüne dahil olacak şekilde işleyen gerçek ve tüzel kişiler hakkında uygulanır" şeklinde düzenleme getirerek kişisel verisi işlenen kişiler yönünden gerçek kişiyi, veri işleyen yönünden hem gerçek hem de tüzel kişiyi hüküm altına almıştır. Bu halde tüzel kişilere ait verilerin düzenleme kapsamına dahil edilmemesi açısından Tasarının isabetli olmadığını ve TCK ile uyumlu düzeltmelerin yapılması gerektiği söylenebilir[678].

TCK'nin 243 ve 244 kapsamında düzenlenen suçların tümünde mağdur ile

[678] Şen, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", s.1196

ilgili özel bir tercihte bulunulmamıştır[679]. Başka bir ifade ile herkes bu suçların faili veya mağduru olabilir. TCK'nin 243. maddesindeki suç, özgü suçlardan değildir. Failin hukuka aykırı olarak tamamen veya kısmen girdiği ve kalmaya devam ettiği bilişim sistemi üzerinde hak sahibi olan kimse, bu suçun mağduru durumundadır. Aynı eylem ile birden çok kişinin hakkı ihlal ediliyorsa, bu durumda bu kişilerin hepsi anılan suçun mağduru pozisyonundadırlar. Örneğin bir bankanın bilişim sistemine girerek, müşteri bilgilerinin kullanılarak suç işlenmesi halinde, bilgileri kullanılan tüm müşteriler suçun mağduru olduğu gibi, bankanın tüzel kişiliği de, suçtan zarar gören durumundadır[680].

Burada özellikle 243. madde yönünden mağdurluk sıfatı için, bilişim sistemi üzerinde hak sahibi olma kriteri esas teşkil etmektedir. Buradaki hak sahipliği, o bilişim sistemine erişim açısından gerekli yetkiye sahip olmak ve bu yetkiyi doğrudan kullanabilmek ile ilişkilendirilmelidir. Bu hususta sadece TCK'nin 244/3'te düzenlenen nitelikli hal bakımından; TCK'nin 244/1 ve 2'de düzenlenen eylemlerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, söz konusu kurum veya kuruluşların mağdur mu yoksa suçtan zarar gören olarak mı değerlendirileceği sorunu bulunmaktadır. Öğretide, sayılan kurum ve kuruluşların suçun mağduru olduğu görüşü hâkimdir[681]. Bilişim sisteminin üzerinde ya mülkiyet hakkı sahibi olmak, ya da sözleşmeyle kullanım hakkı elde etmekle (kira, ariyet, finansal kiralama gibi) hak sahibi olunabilir. Örnek olarak bir finansal kiralama kuruluşundan kiraladığı bilgisayarları ticari işletmesinde üretim amaçlı olarak kullanan kiracının, bilgisayarlar üzerinde ki hakkı zilyetlik iken, finansal kiralama şirketi ise mülkiyet sahibidir. Bu durumda kiracı konumunda bulunan kişilerin bu sistemler üzerinde bulunan zilyetlik hakkı uyarınca bu sistemlere karşı işlenen suçların mağduru olduğunun kabul etmek gerekecektir. Finansal kiralama şirketi bu sistemler üzerinde mülkiyet hakkına sahip olsa dahi, bu suçun düzenlenmesindeki temel fikir mülkiyet hakkını korumak olmadığından, suçun mağduru olarak kabulü mükün değildir.

---

[679] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 531, 641 ve 856
[680] Yazıcıoğlu, "Bilişim Sistemine Girme Eylemi", s. 82
[681] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.6739

Çünkü verilerinin gizliliği ihlal edilen ve kişisel verileri tecavüze uğrayan taraf, bilişim sisteminin zilyedi olan kiracıdır.

TCK'nin 244. maddesine yönelik olarak failin işleyişini engellediği, bozduğu, verilerini yokettiği veya değiştirdiği bilişim sistemi üzerinde hak sahibi olan kimse, bu suçun mağduru durumundadır. Eğer failin eylemi ile birden fazla kimsenin hakkını ihlal ediyorsa, bu suçtan etkilenen herkes bu suçun mağduru konumundadır. Örneğin bir kişinin banka hesabına girerek, hesaptaki paraların başka bir hesaba aktarılması olayında, hesap sahipleri suçun mağduru durumundadır. Maddenin üçüncü fıkrası ile bilişim sisteminin bir banka veya kredi kurumuna ya da bir kamu kurum ve kuruluşuna ait olması durumunda faile verilecek ceza artırılacaktır. Başka bir deyişle, bu suçun bilişim sistemi üzerinde hakkı olan mağdurunun, bir banka veya kredi kurumu ya da kamu kurum ve kuruluşu olması artırım nedeni sayılacaktır. Burada kişinin kendi kişisel verileri üzerinde değişiklik yaparak menfaat temin etmesi halinde suçun mağdurunun kim olacağının tartışılması gerekir. Kişisel verinin sahibinin eyleminin burada kişisel verilere yönelik değil veriyi saklayan kuruma karşı olduğu gözetilerek burada mağdurun kurum olduğunu söylemek mümkündür.

2.4. YER BAKIMINDAN YETKİ

Bilişim alanındaki ihlallere yönelik maddi ceza hukuku alanında meydana gelen gelişmeler, ceza muhakemeleri hukuku alanında yaşanmamaktadır. Ceza usul kanunlarının genel olarak iletişimin denetlenmesi, arama, el koyma, uluslararası yetki, araştırma ve soruşturma faaliyetlerini düzenleyen hükümler, kıyas yolu ile bilişim suçlarına da uygulanmaktadır. Bilişim alanı sanal bir ortam oluşturduğu için maddi varlıklar üzerinde, mesken araması ve telefon görüşmelerinin dinlenmesi gibi konulardaki gereksinimleri karşılayan bu hükümler doğal olarak bilişim alanı ile ilgili suçların araştırılması ve soruşturulmasında yeterli olmamaktadır. İnternet ortamında işlenen suçlarda hangi ülke kanunlarının uygulanacağı ve uyuşmazlığın nasıl çözümleneceği ceza hukuku, borçlar hukuku, fikir ve sanat eserleri hukukunda tartışılan konulardan biridir. İnternet, bir ülkenin coğrafyası ve hukuku ile sınırlı olmayıp yeryüzündeki bilgisayarları birbirine bağlamak suretiyle bilgi alış verişini

sağlamaktadır. İnternet ulusal sınırları aştığı için milli hukuklar çoğu zaman yetersiz kalmaktadır. Bu nedenle uluslararası bir hukuk yaratılmak zorundadır.

Sanal bir ortam olan Siber Uzay'da (Cyberspace) ülkelerin cezalandırma yetkilerini belirlemek oldukça zordur. Ülkelerin hukuki egemenlik alanlarının ve yetkilerinin sınırını belirleme konusunda üçyüz yıl önce kurallar getiren "Westphalia Sözleşmesi'nin[682]" ve bu konuda bu yüzyılın başında uluslararası hukuk alanında kurallar belirleyen "Montevideo Konvansiyonu'nun[683]" oluşturduğu ortak bir anlayış vardır. Buna göre bu iki uluslararası belge çerçevesinde şekillenen ilkeler, geleneksel anlamda devletin egemenlik alanının sınırlarını belirlemektedir. Bu düzenlemelerde devletlerin egemenlik alanı iki kritere göre belirlenmektedir; bunlan genel olarak ülkenin coğrafi sınırları ve vatandaşlık kriterleridir. "Egemen devlet teorisi" olarak adlandırılan ve fikir temellerini Thomas Hobbes'un attığı teoriye göre devletin vatandaşlarını iç ve dış tehlikelere karşı koruması bir zorunluluktur. Bu fikirden yola çıkan ülkeler "egemen devlet teorisini" yansıtır biçimde egemenlik yetkilerini siber uzaya, dolayısıyla internet ortamına doğru genişletme eğilimindedirler. Bu durumda bazen siber uzay ve internet ortamında cezalandırma yetkisinin kime ait olacağı konusunda ülkelerin egemenlik yetkileri çatışmakta, ve bu sorunu çözmeye klasik kurallar yeterli olmamaktadır. Gerçekten bilişim alanında gerçekleştirilen ve suç niteliği taşıyan bir eylemin, nerede ve ne zaman

---

[682] Bu sözleşme devletlerin egemenlik prensiplerinin ana hatlarını belirleyen ve günümüzde de geçerli olan kurallardır. Buna göre:

"Devletler vatandaşları üzerinde kendi yönetimine sahiptir.

Devletlerin içişlerinde diğer devletlerin baskısından uzak olarak hareket edebilme özgürlükleri vardır

Devletlerin dışişleri ve bu alanda izleyecekleri politikalarını belirlemekte ayrıcalıkları vardır."

Ayrıntılı bilgi için Bkz. Harris, David John, *Cases and Materials on International Law,* 6th Edition, London Sweet & Maxwell, 2004, s. 102-108; aynı zamanda bkz. Krasner, Stephen D. "Compromising Westphalia", *International Security*, Winter 1995/96. Volume: 20, Number: 3, The MIT Press, s.115-151

[683] Genel anlamda görev ve yetki yönünden ülkelerin prensiplerini ortaya koyan konvansiyon Amerika Kıtasındaki 19 ülke tarafından 26.12.1933 tarihinde imzalanmış ve 26.12.1934 tarihinde ise yürürlüğe girmiştir. Bu konvansiyonda 16 madde bulunmakta olup, uluslararası hukuk alanında ülkelerin hukuki statüsünü belirlemesi ve Westphalia Sözleşmesi ile belirlenen egemenlik anlayışını kodifiye etmesi yönünden önemlidir. Konvansiyonun 9. maddesi ülkelerin egemenlik yetkisinin sınırlarını şu şekilde belirlemektedir: "*Devletlerin yetkisi, ülkenin ulusal sınırları içersinde bulunan tüm kişilere uygulanır*". Bkz. "Montevideo Convention on the Rights and Duties of States", aynı zamanda Bkz. Harris, *Cases and Materials on International Law*, s. 102-108.

gerçekleştirilmiş sayılacağı, çözülmesi gereken sorunlar olarak karşımıza çıkmaktadır.

Bugün için genel ilke olarak Türk hukuk sisteminde, suçun işlendiği yerdeki mahkemelere yetki verilmektedir. Bu yer bilinmiyorsa, yedek kurallarla yargı yeri belirlenmeye çalışılacaktır. Bu tür kurallara ihtiyaç olduğu da açıktır, çünkü ceza yargılamasında, fiili yargılayacak mahkeme bulunmadığı için yargılamayı yapamamak hiçbir şekilde söz konusu olamaz. Ceza muhakemesi kanunlarının yer yönünden uygulanmasında benimsenen ilke, ülkesellik (mülkilik) ilkesidir. Türk mahkemelerinin bir suçu yargılama konusunda milli yargı yetkisinin bulunduğu hallerde (TCK m. 8-13), Türk kanunlarına göre yargılama yapılır. Başka bir anlatımla, Türk adli makamları muhakemeyi Türk Ceza Muhakemesi Kanunu hükümlerine göre yürütürler. Özellikle, yurt dışında işlenen suçlarda suçun işlendiği ülkenin muhakeme kurallarının uygulanması söz konusu olamaz[684]. Ancak, bazı durumlarda Türkiye'de yürütülen muhakeme kapsamında başka ülkelerde de muhakeme işlemi yapılması gerekebilir.

Günümüzde devletler kendi ülkelerinde yürütülen muhakeme sırasında artık başka devletlerin soruşturma makamlarından yardım almaktadırlar. Türkiye'de yürütülen bir muhakeme dolayısıyla Almanya'da tanık beyanına başvurulması örnek olarak verilebilir. Bu konuları düzenlemek üzere Avrupa Konseyi üyesi ülkeler, "Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi'ni " hazırlamışlardır[685]. Bu Sözleşme'nin 3. maddesine göre, bir ceza davasının yürütülmesi veya delillerin, dosya ve belgelerin gönderilmesi hakkında başka ülkeden yardım istenirse, yardım eden ülke o işlemleri kendi kanunlarına göre yürütür. Böyle bir durumda, yurt dışında yapılan muhakeme işlemleri, bizim kanunlarımıza göre yapılmadığı halde, geçerli sayılır. Ayrıca, ülkesellik ilkesi muhakeme sonucunda verilen hükmün sadece o ülkede geçerli olmasını gerektirdiği halde, günümüzde muhakeme sonucunda verilen hükümlerin başka ülkelerde de geçerli olması için önlem alınmaktadır.

---

[684] Centel ve Zafer, *Ceza Muhakemesi Hukuku*, s. 62
[685] 18.03.1967 gün ve 1034 sayılı kanun (Resmi Gazete, Tarih: 23.03.1968, No: 12856)

Örneğin, aynı konuda aynı kişi için evvelce verilmiş bir hüküm varsa, tekrar yargılama yapılamaması, yani "non bis in idem" ilkesi, uluslararası sözleşmelerde yerini almıştır. Türkiye'nin imzaladığı " Ceza Yargılarının Milletlerarası Değeri Konusunda Avrupa Sözleşmesi"[686], sözü edilen durumlarda tekrar yargılama yasağını açıkça öngörmektedir (m.53/1)[687].

Mahkemelerin karar verme yetkisini içeren yargı yetkisi, genel olarak coğrafi egemenliğe dayalıdır. İnternet ortamında işlenen suçlarda ise coğrafi sınırlar farklıdır. İnternet sayesinde fiziksel anlamdaki ülke sınırları ortadan kalktığından, internet ortamında işlenen suçlarda, dünyanın her hangi bir yerinden, mesafe ve fiziksel sınır olmaksızın suç işlenebilmektedir[688]. Yetki konusunda suçun internet kullanılarak işlenmesi hali ile doğrudan verilerin yüklü olduğu sistemin kullanılması arasında fark oluşacaktır. Suçun veri işleme memuru tarafından işlenmesi veya failin bilişim sisteminin bulunduğu binaya girerek verileri elde etmesi durumunda hiç kuşkusuz suçun işlenme yeri bilgilerin alındığı yer olacaktır. Ne var ki internet aracı kılınılarak bu suç işlenildiğinde ortaya yetki sorunu çıkacaktır.

Bilişim suçunun Türkiye içerisinde işlenmesi durumunda ortaya tartışılacak önemli bir sorun çıkmamaktadır. Bilişim suçu ülke içerisinde işlendiğinde, ceza muhakemesindeki genel yetki kuralları uygulanarak yetkili mahkeme belirlenir. Yani CMK'nin 12. maddesine göre suçun işlendiği yer mahkemesi belirlenir. Eğer suç teşebbüs aşamasında kalmışsa, son icra hareketinin yapıldığı, kesintisiz suçlarda kesintinin gerçekleştiği, zincirleme suçlarda son suçun işlendiği yer mahkemesi yetkilidir. İnternet yoluyla işlenen bir suçta, failin internete girerek suçu işlediği yer mahkemesinin yanında mağdurun kullandığı bilgisayarının bulunduğu yer mahkemesi de CMK'nin 12. maddesinin (5) numaralı fıkrası[689] uyarınca yetkili

---

[686] Resmi Gazete, Tarih: 13.03.1977, No: 15877

[687] Cihan, Erol ve Yenisey Feridun, (1997), *Ceza Muhakemesi Hukuku,* İstanbul: Beta Yayınları, s. 324

[688] Kızıltan, *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, s. 102

[689] **"CMK'nın 12/5 maddesi:** Görsel veya işitsel yayınlarda da bu maddenin üçüncü fıkrası hükmü uygulanır. Görsel ve işitsel yayın, mağdur yerleşim yerinde ve oturduğu yerde işitilmiş veya görülmüşse o yer mahkemesi de yetkilidir."

olacaktır. Çünkü İnternet de, görsel bir yayın olduğundan ve maddedeki "görsel veya işitsel yayın" kavramında, yayının çeşidi değil, niteliği sonucu önemli bulunduğundan uygulama yeri bulacaktır.

Ne var ki CMK'nin 12/5. maddesi (3) numaralı fıkraya[690] yollama yapmaktadır. Burada karşımıza çıkan sorun ise internet yoluyla işlenen suçlarda, "eserin yayım merkezi" ve "eserin yayım merkezi dışındaki baskısı" kavramlarının nasıl değerlendirilmesi gerektiğidir. Suça konu eylemin işlenme yeri genelde web siteleridir. Sanal alemdeki web sitesi merkezi, basılmış eserin merkezi kadar kolay tespit edilebilen bir yapı içermez. İnternet ortamında, internete bağlanan herhangi bir kişi (istisnai olarak bir engel yoksa) rahatlıkla bir web sitesi kurabilir. Kurulan bu site, çoğunlukla bir ana web sitesi üzerinden kurulmaktadır ve bu sitenin kurulduğu adla faaliyette bulunmaktadır. Bu gibi hallerde, bir ana web sitesi ve bir de yeni kurulmuş web sitesi bulunmaktadır. Ana web sitesinin kurulduğu merkez belirlenebilir. İnternet kullanıcısının kurduğu web sitesinin merkezi, CMK'nin 12/3. maddesindeki gibi bir yapı taşımaz. 12/3 maddesindeki eserin yayım merkezi, normal şartlarda bir organizasyonu, bir işletmeyi ve alt yapısını anlatır. Oysa internet kullanıcısının birey olarak kurduğu web sitesinde, kurum yapısı değil, bir kişi söz konusudur. Bu bakımdan, CMK'nin 12/5 yollamasıyla 12/3. maddesindeki, eserin yayım merkezi kavramı, içerik olarak internet ortamında birey tarafından kurulan web sitesine nitelik olarak uymamaktadır. Bu durum, bilişim suçlarının işlendiği alanın (internetin) kendine özgü yapısından kaynaklanmaktadır[691].

Siber Suç Sözleşmesinin 22. maddesinde düzenlenen yargı yetkisine ilişkin hükümde, Sözleşmeyi onaylayan taraf devletlerin, Sözleşmedeki ceza hukukuyla ilgili 2 ile 11. maddeler arasındaki yargı yetkilerini düzenlerken uymaları gereken ölçütler sıralanmıştır. Öncelik ülke sınırlarındaki yetki kuralına verilmiş, buna göre, ulusal devlet sınırları içerisinde işlenen suçlarda yargı yetkisini oluşturmasının

---

[690] **"CMK'nın 12/3 maddesi:** Suç, ülkede yayımlanan bir basılı eserle işlenmişse yetki, eserin yayım merkezi olan yer mahkemesine aittir. Ancak, aynı eserin birden farklı yerde basılması durumunda suç, eserin yayım merkezi dışındaki baskısında meydana gelmişse, bu suç için eserin basıldığı yer mahkemesi de yetkilidir."

[691] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 327.

gereklililği üzerinde durulmuştur. Türk iç hukuku açısından zaten tüm suçlar bakımından durum bu şekildedir[692]. Sözleşmenin 22. maddesindeki diğer bir ölçüt ise, faile göre kişisellik ilkesidir. Buna göre, bir devlet vatandaşı, ülke dışında (başka ülkede) suç işlediğinde, fiil, suçun işlendiği yerde de suç olmak koşuluyla, kendi vatandaşını yargılama yetkisine sahiptir.

Bir kişi tarafından oluşturulan web sitesinin merkezinin, bireyin web sitesini kurarken kullandığı bilgisayarın bulunduğu yerdir ya da bireyin oturduğu yerdir denildiğinde, internet ortamında bir web sitesi kurmak için bireyin oturduğu yerdeki kendi bilgisayarını kullanması şart olmadığından bu kuralı uygulamak mümkün olmayacaktır. Örneğin herhangi bir internet kafedeki veya bir şekilde ulaşılan bilgisayar kullanılarak da web sitesi kurulabilir. Üstelik birey web sitesini bir şehirde kullandığı bilgisayarla internete bağlanarak kurduktan sonra, ikamet ettiği başka şehre dönüp, web sitesini burada kullanmaya başlayıp ve bu sitede yaptığı yayınlarla internet ortamında suç işleyebilir. Bu durumda CMK'nin 12/5 yollamasıyla, (3) numaralı fıkradaki eserin yayım merkezi kavramı, her zaman bilişim suçlarına uymayacağından burada uygulanamayacaktır. Esasında, bu şekilde internet ortamında birey tarafından oluşturulan web siteleriyle işlenen suçlarda, suçun birey tarafından işlendiği yerin, CMK'nin 12/3 maddesine göre değil, 12/1 maddesine[693] göre belirlenmesi daha yerinde olacaktır.

CMK'nin 12/3 maddesinde bulunan "eserin yayım merkezi dışındaki baskısı" kavramı ile eserin birden çok yerde basılması halinde, farklı basım yerleri de yetkili kılınmaktadır. Bu düzenleme de internet ortamında işlenen suçlara uygulanamayacaktır. Zira internet ortamındaki yayınların dünya çapında olması ve bir anda internet ağındaki her yerde aynı yayın görünmesi nedeniyle düzenlemede geçen "yayının farklı baskısı" kavramına uygun bir alan düşünülmesi zordur. Bu

---

[692] Keskin, Serap,"Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine ilişkin Hükümlerin Değerlendirilmesi", *İÜHFD*, Sayı 1-2, 2001, s.177.

[693] **"Madde 12 –** (1) Davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir."

nedenlerle, CMK'nin 12/5 yollamasıyla, 12/3 fıkrasındaki hüküm, nitelik olarak internet ortamındaki suç teşkil eden yayınlara uymamaktadır[694].

Suç vasfı taşıyan eylemin yurt dışından yapılması ya da diğer bir ifadeyle yurtdışından kaynaklanıyor olması durumunda, suça ilişkin fiilin yurtdışında icra edildiği ülkede mi yoksa sonucunun oluştuğu ülkelerde mi işlenmiş sayılacağının belirlenmesi bir zorunluluk olarak karşımıza çıkmaktadır. Bu noktada iki farklı görüş bulunmaktadır. Bir görüşe göre, internet yayını şeklinde gerçekleştirilen bir suç, kural olarak, ancak o yayının yapıldığı ülkede işlenmiş sayılır ve bu yayının sonucu başka ülkelerde ortaya çıkmış olsa dahi, bu ülkeler suçun işlendiği yer olarak kabul edilemezler. Bu görüşün gerekçesi olarak, bu tarz suçların "sonuçsuz suçlar" ya da daha doğru bir ifadeyle "sonucu harekete bitişik suçlar"[695] olduğu ve hareketin yapılması ile birlikte artık suç tamamlanacağı için, bu suçlar hakkında bağlama noktası olarak sonucun gerçekleştiği yer kıstasını uygulama olanağı bulunmadığı ileri sürülmektedir[696]. Karşı görüşe göre ise, internetin global yapısı gözetildiğinde, internet yoluyla işlenen suçlarda, yalnızca suç teşkil eden yayının yapıldığı yeri yetkili saymak yerinde olmaz; bu suçlar "mesafe suçları" niteliğindedir ve hareket ile netice çok farklı yerlerde gerçekleşebilir. Burada önemli olan failin kastıdır. Fail, hareketinin sonuçlarının farklı ülkelerde gerçekleşmesini istemiş ise, sonucun gerçekleştiği her ülkedeki ilgili mahkeme yetkili sayılacaktır[697].

Suç içerikli yayınlar açısından sadece yayının yapıldığı ülkenin suçun işlendiği yer olarak kabul edilmesi, internet'in küresel karakterinin gözardı edilmesi sonucunu yaratacağı da düşünülmelidir. Gerçekten bu suçlar, hareket ve sonucun farklı yerlerde gerçekleşmesi nedeniyle birer "mesafe suçu"[698] olma özelliği gösterirler. Mesafe suçlarında ise, suç, doğrudan doğruya veya aralıksız sonucun doğduğu veya failin kast ve niyetinin sonucun orada gerçekleşmesi yönünde

---

[694] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 326 vd.
[695] İçel ve diğerleri, *Suç Teorisi*, s. 44.
[696] Erksen, Roland, *Uluslararası Bilgisayar Ağlarında Yayınlanan Suç İçerikli Bilgilerden Doğan Cezai Sorumluluk*, (Çev: Barış Erman), Yayımlanmamış Yüksek Lisans Seminer Ödevi, İstanbul, 1999, s. 5.
[697] Sınar, *İnternet ve Ceza Hukuku*, s. 127
[698] İçel ve diğerleri, *Karşılaştırmalı ve Uygulamalı Ceza Hukuku*, s. 162 vd.

bulunduğu her yerde işlenmiş sayılır[699]. O halde, hareket bir ülkede yapılmakla birlikte, sonuç başka ülkelerde, hatta daha doğru bir ifadeyle, internete bağlı her ülkede gerçekleşebileceği için, artık bu suçların sonucun oluştuğu her ülkede işlenmiş olduğunu kabul etmek gerektiği savunulmaktadır[700].

TCK'de internet ortamında işlenen suçlarla suçun işlendiği yerin tespiti hususunda özel bir düzenleme yapılmamış, ancak 8. maddesinde[701] hem "suçun işlendiği yer" hem de "sonucun gerçekleştiği yer" esas alınarak genel bir düzenleme yapılmıştır. Bu nedenle uluslararası alanda işlenen bilişim suçlarında sorun 8. madde gereğince çözümlenmelidir. TCK'nin 8. maddesinde mülkilik ilkesi kabul edilmiştir. Türkiye'de işlenen suçlar hakkında Türk Kanunları uygulanacaktır. Buna göre suçu işleyen failin veya suçtan zarar gören mağdurun Türk veya yabancı olması ya da bu suçun Devlet aleyhine işlenmesi arasında fark yoktur. Suçu işleyen kim olursa olsun veya suç, kimin aleyhine işlenirse işlensin, Türkiye'de işlenmesi halinde Türk Ceza Kanunları uygulanacak, bozulan huzurun eski hale getirilmesi ve toplumsal barışın sağlanması Türk Kanunları ile olacaktır. Türk Ceza Kanunlarının uygulanması, Türkiye Cumhuriyeti Devletinin egemenliğinin bir sonucu ve gereğidir.

Özellikle internet bankacılık hesabı bulunan banka hesap sahibi mağdurların bir şekilde ele geçirilen şifreleri kullanılarak internet üzerinden hesaplarındaki paraların şüpheli başka hesaplara havale edilmesi durumunda yetkili mahkemenin neresi olacağı hep tartışma konusu olmuştur. Bu konuda mağdur hesabın bulunduğu yer ile paranın aktarıldığı hesabın bulunduğu yeri suç yeri kabul eden görüşler ve bu görüşlere göre verilmiş yetkisizlik kararları mevcuttur. İnternet vasıtası ile işlenen

---

[699] Dönmezer ve Erman, *Nazari ve Tatbiki Ceza Hukuku*, s. 246

[700] Sınar, *İnternet ve Ceza Hukuku***,** s. 128

[701] **"8. madde**; (1) Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi hâlinde suç, Türkiye'de işlenmiş sayılır.
(2) Suç;
a) Türk kara ve hava sahaları ile Türk karasularında,
b) Açık denizde ve bunun üzerindeki hava sahasında, türk deniz ve hava araçlarında veya bu araçlarla,
c) Türk deniz ve hava savaş araçlarında veya bu araçlarla,
d) Türkiye'nin kıt'a sahanlığında veya münhasır ekonomik bölgesinde tesis edilmiş sabit platformlarda veya bunlara karşı, işlendiğinde Türkiye'de işlenmiş sayılır."

suçlar açısından olaya yaklaştığımızda, ilk belirleyeceğimiz sonuç, İnternet vasıta kılınarak işlenen suç yönelik eylemin gerçekleştirilmesi ile suç teşkil eden neticenin kendiliğinden doğmasıdır. Bu durumda, suçun işlendiği yerin tespitinde güçlük yoktur. Suçun işlendiği yere yargı yetkisi vermek uygun bir çözüm olacaktır. Bunun yanı sıra, özellikle kişilere yönelik suçlarda, bu kişilerin ikametgahlarının bulunduğu yer mahkemesinde de yetki vermek yargılamayı kolaylaştıracaktır.

Günümüzde suç işlemekte vasıta olarak internet ortamı kullanılmaktadır. Fakat bunların büyük bir çoğunluğunun faaliyetlerini yurt dışında yaptığı bilinmektedir. Dolayısıyla failleri tespit ve yakalamak imkansız hale gelmektedir. Bu sorunun çözüm yolu, Uluslararası alanda yapılacak ve İnternet yolu ile işlenen suçların engellenmesine ve hatta faillerin iadesini düzenleyen bir anlaşma yapılmasıdır. Yurt içinde işlenen suçlarla ilgili olarak ise; esasen mevzuatımızdaki suç tanımlamaları bakımından önemli bir sorun olmamakla birlikte fail ve fiil arasındaki ilişkiyi kurma hususunda güçlükler vardır. Bu konuda yapılması gereken temel çalışma, İnternet vasıtasıyla suç işleyen faillerin tespiti ve suç ile fail arasındaki illiyet bağını net bir şekilde ortaya koyabilecek teknolojik donanıma kavuşulmasıdır[702].

Artuk - Gökçen - Yenidünya'ya göre; bilişim sistemine fiziksel temas ile girilmesi halinde eylem nerede yapılmışsa suç orada işlenmiştir[703]**.** Buna karşılık bilişim sistemine ağ üzerinden erişilmiş ise bu takdirde suçun araç bilişim sisteminin bulunduğu yerde mi, yoksa hedef bilişim sisteminin bulunduğu yerde mi işlendiği konusunda net bir görüş bulunmamaktadır. Hareketin parçaları veya hareket ile netice arasında siyasi ve coğrafi sınır bulunan bu tür suçlara mesafe suçu denilmektedir. Burada bilişim suçlarının özellikleri dikkate alınarak suç, hareket, hareketin kısım ve neticenin gerçekleştirildiği her yerde işlenmiş sayılmalıdır. Böylece bilişim suçlarının cezasız kalması önlenmiş olacaktır. Nitekim TCK'nin 8. maddesinde; "fiilin kısmen veya tamamen Türkiye'de gerçekleşmesi halinde suç,

---

[702] Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 252

[703] Artuk ve diğerleri, Cilt:5, *Ceza Hukuku Genel Hükümler*, s. 4633-4634,

Türkiye'de işlenmiş sayılır" denilerek sınır aşan mesafe suçları bakımından ortaya çıkabilecek tartışmalara son vermiştir. Şu halde, gerek içeriden dışarıya (failin ağa bağlandığı bilişim sistemi Türkiye'de, hedef bilişim sisteminin yurt dışında olması), gerekse dışarıdan içeriye (failin ağa bağlandığı bilişim sisteminin yurt dışında hedef bilişim sisteminin Türkiye'de olması) mesafe suçları Türkiye'de işlenmiş sayılır. Bilişim suçları bakımından yetkisizlik kararlarının azaltılması ve yargılamanın makul sürelerde bitirilmesi için kanuni düzenlemelere gidilmesi gerekli görülmektedir. Ancak bu konuda uygulamada ağırlık kazanan "her yerdelik teorisi" gereğince suçun işlendiği yeri, hem icra hareketlerinin yerine getirildiği yer, hem de neticenin ortaya çıktığı yer olarak kabul edilmesinin yararlı bir çözüm olacağı ileri sürülmektedir[704]. Sonuç olarak; bilişim alanında ki ihlalleri uluslararası ölçekte kimin yargılama yetkisine sahip olduğu konusunda ülkelerin birbirlerinin egemenlik haklarına saygı duyarak varacakları uzlaşıyla çözülebileceği söylenebilir.

Yetki sorunuyla delillerin elde edilmesi aşamasında da karşılaşmaktayız. Türkiye'de delillerin elde edilmesi konusunda yeterli alt yapının hazırlanmamış olması ve bu konuda kanuni düzenlemelerin hala yapılmamış olması delillerin toplanmasında çok büyük güçlükler çıkartmaktadır. Uluslararası polis ile işbirliği yapılmadan Türkiye'de mevzuat anamında delillerin hukuki niteliği ve internet servis sağlayıcılardan delil elde edilmesi konusularında her türlü düzenleme yapılsa dahi, suç ve suçlular ile mücadele yönünden istenilen sonuç alınamayacaktır. Çünkü özellikle internet kullanılarak işlenen suçlarda internetin yapısal özelliği gereği birçok erişim noktası bulunabilmektedir. Bu noktalarda genellike tek bir ülkede bulunmamaktadır. Hal böyle olunca, yurt dışındaki bir servis sağlayıcı üzerinden işlenen bir olayın soruşturmasında ilgili ülke polis teşkilatı işbirliği yapılması zorunlu hale gelmektedir. Aksi halde olayın soruşturması belirli bir aşamadan sonra devam edemeyecektir. Açıklanan bu amaç doğrultusunda ülkeler arası ikili polis işbirliği sözleşmelerinin yapılması gerekir. Hatta bu sorunlar aşılsa dahi, eğer soruşturma konusu suç, işlendiği diğer ülkede suç olarak düzenlenmemiş ise, gerekli bilgiler alınması imkansız hale gelecektir. Bu amaçla İnterpol, AB ve Avrupa

[704] Tanrıkulu, *Bilişim Hukuku İle İlgili Alman Federal Yüksek Mahkemesinden Örnek Kararlar*, s. 11

Konseyinde uluslararası suçun tanımının yapılmasına dair çalışmalar bulunmaktadır. Ülkemiz açısından bu çalışmalar dikkatle takip edilmeli ve kanunlarımız buna paralel olarak yeniden düzenlenmelidir.

Bilişim suçları artık teknolojinin girmediği ülke çok az kaldığından bütün ülkelerin ortak sorunu haline gelmiştir. Özellikle ABD ve Avrupa ülkelerinde bilişim alanındaki hukuki ve idari yapılanmaların düzenlenmesi için yoğun bir çalışma başlatılmıştır. Bilişim teknolojileri alanındaki gelişmeler internet ve bilgisayar ağları sayesinde milli sınırları aştığından ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmıştır. Teknolojik gelişmeler ile küreselleşen dünyamızda; tüm ülkelerin işbirliği ile bu tip suçlara karşı mücadele etme zorunluluğu bulunmaktadır[705].

2.4.1. Sınır Ötesi Veri Aktarımı

Telekomünikasyon araçlarının çok gelişmesi sonucu, ülkeler hatta kıtalar arasındaki hızlı sınır ötesi bilgi akışı karşısında, kişilik haklarının korunmasına hizmet eden milli mevzuatlarının yetersiz kalması, bu alanda uluslararası sözleşmeler hazırlanmasını zorunlu kılmıştır. Uluslararası aktarım yapılan kişisel verilerin yeterli şekilde korunabilmesi için öncelikle hem gönderen, hemde gönderilen ülke mevzuatlarında veri gönderimine izin veren düzenleme bulunması gerekirken, aynı zamanda verinin gönderileceği ülkede en azından veri gönderen ülke kadar koruma sağlanması gerekir[706]. Avrupa ülkeleri kişisel verileri korumak için daha çok özel kanun çıkartmayı tercih etmekte iken diğer devletlerden bir kısmınında bu şekilde kanun yaptığı görülmektedir[707]. Kişisel Verilerin Korunması Kanunu Tasarısının genel gerekçeside kanunun yapılış amaçlarından birininde bu olduğunu açıklamaktadır[708]. Ülke dışına aktarılan kişisel verilerin gönderilebilme şartı olan, gönderilen ülkenin de eşdeğer ve etkin bir korumaya sahip olması kuralının

[705] Dokurer, 'Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri', s.56.
[706] Kılınç, *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, s. 1154
[707] Pekşirin, Hülya, Bilişim Şurası Gurup Yöneticisi, "Kişisel Verilerin Korunması", *Bilişim Şurası Hukuk Raporu,* http://tr.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu (Erişim: 2.12.2013), s. 34
[708] Adalet Bakanlığı Kanunlar Genel Müdürlüğü, "Tasarılar", s.14

istisnaları; ilgili kişinin açık rızasının bulunması, verinin ilgili olduğu kimsenin hayatı veya beden bütünlüğü için bu aktarımda zorunluluk buluhnması, suçun koğuşturulması ve önlenmesi için lüzumlu olması, verinin ilgili olduğu kişi ile veri kütüğü sahibi arasında bir sözleşme ilişkisinin bulunması ve aktarımın kamuya açık bulunan sicillerden yapılması halidir. Eğer bu şartlar gerçekleşiyorsa veri aktarılan ülkede eşdeğer ve etkin bir koruma bulunmasa bile kişisel veriler aktarılabilecektir[709].

Konuya ABD yönünden bakıldığında, kişisel verilerin korunması için özel bir kanun bulunmamakta, daha çok özel yaşamın gizliliği olarak ele alınarak sorunun çözümü özel ve ceza hukuku alanında kişiler için getirilen güvencelere havale edilmektedir. Genelde dünya ülkelerince, ya Avrupa Konseyince kabul edilmiş olan 108 sayılı Sözleşmenin koyduğu model ya da ABD tarafından uygulanan mahremiyet ilkelerine dayanan sistemden birisini seçmek durumunda bulunmaktadır. Bu yaklaşım ayrılığı son yıllarda AB ile ABD arasında çok ciddi bir hukuk çekişmesine dönüşmüş bulunmaktadır[710]. Bu ihtilaf e-ticareti etkilediği kadar, ticari amaçlar dışında kalan ve ceza kovuşturması veya insan kaynakları araştırması gibi amaçlar için kişisel verilerin aktarılması açısından da önem arzetmektedir. Latin Amerika ülkelerinin bu sorunu çözmek için getirdikleri "Habeas Data" adı verilen sistemle kişisel verilerilerle ilgili işlem yapan kurum ve kişilerin kötü uygulamalarının önlenmesi için anayasal güvence getirilmektedir. Avrupa ve Amerika yaklaşımları arasında bir noktada yer alan ve Latince olan Habeas Data'nın sözlük anlamı "veriye sahip olmalısın" şeklinde verilebilir. Ülkeler arası bazı farklılıklar göstermekle beraber bu sistemde; kişisel verisinin korunmasını isteyen kişinin anayasal bir mahkemeye başvurarak, özel yaşamının, onurunun ve bilgiye erişim özgürlüğünün korunmasını istemesi bulunmaktadır. Habeas Data dilekçesi, kişisel verilerle ilgili gerçek ya da tüzel kişiler hakkında verilebilir ve kişi kendisi ile ilgili bilginin düzeltilmesini, güncellenmesini ve hatta yok edilmesini isteyebilir. Habeas Data dilekçesini verme hakkı kişiye bağlı bir haktır. Mahkemenin konuyu re'sen ele alması mümkün bulunmadığından kişinin

[709] Kılınç, *Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*, s. 1154
[710] Boz, Ahmet, *Kişisel Verilerin Korunması; Türkiye, ABD ve AB Örnekleri*, s. 84 vd.

bizzat kullanması gerekmektedir. Türkiye bu konudaki seçimini Avrupa Konseyinin Kabul ettiği 108 sayılı sözleşmeyi imzalamak suretiyle yapmış bulunmaktadır[711]. Mevcut durum itibarıyla ülkemizde sınır ötesi veri aktarımı ile ilgili bir kısıtlama yoktur[712].

2.5. SUÇUN İŞLENDİĞİ ZAMAN SORUNU

Suçta ve cezada kanunilik ilkesinin yanı sıra; ceza hukukunun kişi hak ve hürriyetleri açısından güvence oluşturması amacıyla kabul edilen diğer bir kurala göre; fiili işlediği zaman yürürlükte olan kanunlara göre suç teşkil ediyorsa kişi cezalandırılabilecektir. Bir fiil işlendikten sonra yürürlüğe giren kanunda suç olarak tanımlanmışsa; bu kanun geçmişe yürütülerek fail cezalandırılamaz. Yeni suçlar ihdas eden bir kanun, ancak yürürlüğe girdiği tarihten sonra işlenen fiiller bakımından uygulama kabiliyeti bulur (geriye yürüme yasağı)[713]. Yani bir suçun unsurlarında, suçun karşılığında öngörülen yaptırımlarda, bu suçtan dolayı mahkûmiyetin kanuni neticelerinde sonradan yürürlüğe giren bir kanunla failin aleyhine olacak şekilde değişiklikler yapılması durumunda; bu kanun, yürürlüğe girdiği tarihten önce işlenmiş olan fiiller bakımından uygulanamayacaktır. Ancak, sonradan yürürlüğe giren kanun, bir suçun unsurlarında, yaptırımlarında, bu suçtan dolayı mahkûmiyetin kanuni neticelerinde failin lehine olacak şekilde değişiklikler yapması durumunda, yürürlüğe girdiği tarihten önce işlenmiş olan fiiller bakımından da uygulanabilecektir[714]. Ceza hukuku kurallarının zaman bakımından uygulanmasına ilişkin bu ilkeler, TCK'nin "Zaman bakımından uygulama" başlıklı 7. maddesinde düzenlenmiştir[715]. TCK'de zaman bakımından uygulama kuralı

---

[711] Pekşirin, "Kişisel Verilerin Korunması", s. 35

[712] BSA (The Software Alliance), "Global Cloud Computing Scorecard", *Ülke Raporu 2013: Türkiye* http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Turkey.pdf, (Erişim: 17.09.2014)

[713] Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s.119

[714] Katoğlu, *Ceza Hukukunda Hukuka Aykırılık*, s. 121.

[715] **"Madde 7** - (1) İşlendiği zaman yürürlükte bulunan kanuna göre suç sayılmayan bir fiilden dolayı kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. İşlendikten sonra yürürlüğe giren kanuna göre suç sayılmayan bir fiilden dolayı da kimse cezalandırılamaz ve hakkında güvenlik tedbiri uygulanamaz. Böyle bir ceza veya güvenlik tedbiri hükmolunmuşsa infazı ve kanunî neticeleri kendiliğinden kalkar.

belirlenirken; bunun, sadece cezalarla ilgili olarak değil, güvenlik tedbirleri bakımından da, yani ceza hukuku yaptırımlarının bütünü için geçerli olduğu vurgulanmıştır[716].

Daha önce de ifade edildiği üzere, bilişim suçları, genelde sonucu harekete bitişik suçlar kapsamında yer alırlar. Dolayısıyla bu suçlarda hareketin gerçekleştirilmesi ile birlikte sonuç ta meydana gelir ve suç, o anda oluşur. Ancak İnternetle işlenen suçlar bu suçların mütemadi ve müteselsil suç şeklinde olmaları da mümkündür. Bu takdirde suç, temadi ve teselsülün bittiği anda işlenmiş olur. Bu nedenle, suçun işlendiği zamanın belirlenmesinde ciddi bir güçlük yaşanmaz[717]. Buna karşın, internet yayınının farklı yerlerde yapılması durumunda önem taşıyan husus, söz konusu internet yayınının Türkiye'de etki gösterip göstermediğidir. Eğer bu suç içerikli yayın, Türkiye'de etki gösteriyorsa, bu takdirde belirtilen olasılıklar, "failin lehine yorum" kuralına öncelik vermek suretiyle çözüme kavuşturulabilir.

Bu konuda dikkat edilmesi gereken bir konuda bilişim sistemleri kullanılarak işlenebilen bu suçun soruşturulması ve kovuşturulması aşamalarında zaman farkları nedeni ile doğru delillere ulaşılamamasıdır. Bilindiği üzere ülkeler arasında coğrafi uzaklık nedeniyle saat farklılıkları bulunmaktadır. Bu nedenle ülkemiz dışından bildirilen bir suç ile ilgili IP no araştırılırken ülkeler arasındaki zaman farklarının göz önüne alınması gerekmektedir. Genel olarak Ülkemiz dışından intikal eden bilişim suçlarında tespit edilen IP no ve tarihi dışında bilgi bulunmamaktadır. Eğer tespit edilen IP no ve tarihinin yanı sıra ülkeler arası zaman farklarını gösteren + GMT, - GMT bilgileri ve bağlantı saat, dakika ve saniyesi yoksa tespit edilen IP no ile ilgili verilen tarih baz alınarak o IP numarası ile o tarihte o günde bağlanan tüm kullanıcıların belirlenmesi ve tek tek incelenmesi gerekmektedir. Bu ise çok ciddi bir

---

(2) Suçun işlendiği zaman yürürlükte bulunan kanun ile sonradan yürürlüğe giren kanunların hükümleri farklı ise, failin lehine olan kanun uygulanır ve infaz olunur.
(3) Hapis cezasının ertelenmesi, koşullu salıverilme ve tekerrürle ilgili olanlar hariç; infaz rejimine ilişkin hükümler, derhal uygulanır.
(4) Geçici veya süreli kanunların, yürürlükte bulundukları süre içinde işlenmiş olan suçlar hakkında uygulanmasına devam edilir."

716 Erem ve diğerleri, *Ceza Hukuku Genel Hükümleri,* s. 140
717 Pekşirin, "Kişisel Verilerin Korunması", s. 34

iş kaybı ve masum kişilerin de mağdur edilmesine sebebiyet verecektir. Suçun saat dakika ve saniyesinin kaydedilmesi ve suçlunun tespitindeki bir başka sorun ise farklı bilişim sistemlerindeki saatlerin dakika ve saniye olarak birbirleriyle aynı olmamasıdır. Kısaca Suçun işlendiği zamanı tespit eden polisin kullandığı sistem saati ile ISS'nin sistem saatinin saniyesine kadar aynı olması gereklidir. Yoksa araştırmalar güvenlik kuvvetlerini yanlış kişilere götürebilir. Sorunun çözümü ise, tüm ülkelerin birbirleriyle internet saati adı verilen saat birimini esas alarak yazışmalarıdır ve yazışmalarında mutlaka bağlantı saatinin tüm ayrıntıları, yazışmalarda bildirilmelidir. İnternet saati; 24 saatlik zaman aralığının 1000'e bölündüğü ve dünyanın her yerinde aynı anda aynı zamanda aynı rakamlarla ifade edildiği bir uygulamadır. Aynı uygulamaya Türkiye'de savcılıklar ve kolluk kuvvetleri tarafından şikayet ve dava dilekçelerini kabul ederken de uyulması yararlı olacaktır[718].

2.6. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

Suçun özel görüş şekillerinden kasıt, suçu meydana getiren eylemin işleniş şekline, sonuç meydana getirip getirmemesine ve birden fazla kişi ile birlikte işlenmesi durumunda kanunda düzenlenen yalın haliyle cezalandırmaya esas alınıp alınamayacağı hakkındaki düzenlemelerdir. Ceza kanununda bu konular; teşebbüs, zincirleme suç, içtima ve iştirak olarak dört başlık altında incelenmiştir. TCK'nin bu düzenlemesine uyularak konuya açıklık getirilmesi yerinde olacaktır.

2.6.1. Teşebbüs

Ceza kanunlarının özel kısmında düzenlenmiş olan suçlar belli bir süreç içerisinde gerçekleştirilmektedir. Bu süreç içerisinde fail, belli bir suçu işlemek hususunda karar vermekte, daha sonra bunun icrasına yönelik hazırlık yapmakta ve nihayet icra hareketlerinin işlenmesiyle veya neticenin gerçekleştirilmesiyle suç tamamlanmaktadır. İcrasına başlanan ancak elde olmayan sebeplerle

[718] Şen, Bilal, *Bilişim Suçları ile Mücadele,* Yayımlanmamış Ödev, Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2003, s. 50.

tamamlanmayan suçlara, teşebbüs halinde kalmış suçlar denilmektedir. Teşebbüs, suçun icraya başlamasıyla tamamlanması arasında söz konusu olan hukuki bir durumdur. Hareket ile neticesi arasında yer ve zaman farkı bulunabilen suçlara neticesi hareketten ayrık suçlar denir. Bu suç tiplerinde netice hareketten ayrı olduğu için teşebbüs mümkündür[719].

Teşebbüste sübjektif (manevi) unsurları yönünden tamam olan bir suçun objektif (maddi) unsurları itibarıyla eksik kalması söz konusudur. Teşebbüs aşamasında kalmış suçlarda kanuni tanıma göre eksik kalan husus; sırf hareket suçları olarak tarif edilen ve hareketin meydana gelmesi ile tamamlanan suçlarda icra hareketinin tamamlanmamış olması, suçun kanuni tarifinde ayrıca neticeye yer veren suçlar bakımından ise, icra hareketlerinin tamamlanmaması veya icra hareketleri tamamlanmış olmasına rağmen neticenin gerçekleştirilmemesidir[720]. Burada biri tamamlanamamış suça ilişkin tanım, diğeri ise teşebbüse ilişkin olmak üzere iki normun bir araya gelmesiyle uygulanabilen suçun özel bir görünüş biçimi söz konusudur. Teşebbüse ilişkin hükümler yardımcı norm niteliği taşımaktadır[721]. Teşebbüs aşamasında kalan suç ile tamamlanmış suç arasında unsurlar yönünden temel bir farklılık yoktur. Sadece failin elinde olmayan sebeplerle icra hareketlerinin tamamlanamaması veya hareketlerin tamamlanmış olmasına rağmen neticenin gerçekleştirilememesi olarak ortaya çıkar[722].

TCK'nin getirdiği sistemde teşebbüsün meydana gelebilmesi için; failin kast ile hareket etmesi, suçun işlenmesi için elverişli hareketlerin gerçekleştirilmesi, suç işlemeye yönelik harekete başlaması, hareketlerini elinde olmayan nedenlerle tamamlayamaması gerekir. Bu hususlar teşebbüsün şartlarını oluşturur[723]. Teşebbüs halinde kalan suçlar için ceza tayininde teşebbüs hükümlerinin uygulanmasını

---

[719] Taşkın, Ahmet ve Zengin, İbrahim, *Ceza Hukuku El Kitabı*, Ankara: Savaş Kitap ve Yayınevi 2004, s. 40
[720] Özgenç, *Türk Ceza Hukuku Gazi Şerhi*, s. 458
[721] Sözüer, Adem, *Suça Teşebbüs,* İstanbul: Kazancı Yayınları, 1994, s.54
[722] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s.360 vd.
[723] Barut, Muharrem ve Karayol, Muharrem, *Bilişim Suçları*, 2005, Yayımlanmamış Proje Ödevi, Ankara: TODAİ, s. 235

sağlayan asli suç dikkate alınacaktır. Buna göre teşebbüs halinde kalmış suç için tamamlanmış şekline göre indirimli ceza uygulaması gerekmektedir.

TCK'nin 135. maddesinde düzenlenen suçun teşebbüse elverişli olup olmadığı konusunda görüş birliği yoktur. Özbek/Kanbur/Doğan/Bacaksız/Tepe, bu konudaki görüşlerini "neticesi harekete bitişik bir suç olmakla kural olarak teşebbüse elverişli değildir. Ele geçirilmiş ancak henüz kaydedilmemiş olması durumunda da teşebbüsten söz etmek mümkün değildir. Zira verileri hukuka aykırı olarak ele geçirme de ayrıca suç olarak düzenlenmiş bulunmaktadır (TCK m. 136)." şeklinde ortaya koyarken[724],Yaşar/Gökçen/Artuç ise TCK'nin 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçunun tamamlanması için, mağdurun herhangi bir zarara uğramasına gerek olmadığını, bu nedenle bu suçun, sırf hareket suçu olduğunu ve hareketlerin bölünebildiği oranda teşebbüse elverişli olduğunu, örneğin, bir failin mağdur hakkında kişisel verileri depolamaya başladığı anda yakalanması durumunda eylem teşebbüs aşamasında kalmış olacağını belirtmektedirler. Yine aynı gerekçe ile TCK'nin 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak başkalarına verme, yayma veya ele geçirme suçuna da teşebbüsün mümkün olduğunu, örneğin, bir polis memurunun dinlediği kişilerin konuşma kayıtlarını bir basın mensubuna vermesi konusunda anlaşıp da, tam verirken yakalandığında eylem teşebbüs aşamasında kalmış olacağını savunmaktadırlar[725]. Suçun tamamlanmış sayılması için kişisel verinin hukuka aykırı olarak kaydedilmesi yeterlidir; bundan bir zarar doğması da şart değildir. Bu nedenle suç bir tehlike suçudur. Suç tipinde hareket ile tehlike neticesi arasında bir nedensel ilişkinin varlığını araştırmak yönünde zorunluluk bulunduğuna ilişkin ifade yer almaması, diğer bir deyişle suç tipinde hareketin bir tehlike yaratabilecek nitelikte olması gerektiğine ilişkin düzenlemenin yer almaması suçun soyut tehlike suçu olarak kabul edilmesi sonucunu doğurur[726].

---

[724] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.527
[725] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.4122 - 4127
[726] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s. 951

Genel olarak; TCK'nin 243 ve 244. maddelerinde düzenlenen suçlara teşebbüs olanaklıdır. TCK'nin 244. maddede düzenlenen suç teşebbüse elverişle olan neticesi hareketten ayrık suçtur. 243. maddede belirtilen bilişim sistemine girmek ve orada kalmaya devam etmek suçu mütemadi bir suçtur. Neticenin meydana gelmesinden sonra hemen bitmeyip devam eden suçlara mütemadi suçlar denilmektedir. Bilişim sistemine giren bir fail orada kalmaya devam ettiği sürece hareket kesilmemiş, yani suç devam ediyor demektir. Tüm bu suçlar teşebbüse elverişlidir[727]. İcra hareketleri başlandığı halde örneğin sisteme "girme" eylemi gerçekleşmediyse (örneğin, elektrik kesildiyse) ya da "girme" gerçekleştiği halde kişisel veriler alınmadan ya da alındığı halde kullanılmadığı hallerde teşebbüs gündeme gelecektir[728]. Bunun dışında bir zararın varlığı aranmamıştır. Maddenin 3. fıkrasındaki ağırlatıcı halin, failin taksirli hareketlerinin sonucu oluşması gerektiğinden, teşebbüs söz konusu olmaz. Hukuka aykırı olarak bilişim sistemine girmeye çalışma veya girdikten sonra orada kalmayı başaramamak suça teşebbüs halidir[729].

Yetkisiz erişim yapıp sistemden çıkan kişinin fiilinde, suça teşebbüsten söz etmek güçtür. Çünkü yetkisiz erişim tek başına suç değildir. Bu nedenle, hukuka aykırı olarak bilişim sistemine girmeye çalışmak, bu suça teşebbüs sayılmaz. Bilişim sistemine girdikten sonra, orada kalmayı başaramamak ise, fiilin niteliğine göre değerlendirilmelidir. Bu suçta teşebbüsten söz edebilmek için, yetkisiz erişimden sonra, sistemde kalmaya başlanmış ve fakat henüz suçun tamamlanmasını sağlayacak kadar bir sürenin geçmemiş olması gerekir. Bir başka anlatımla, yetkisiz erişimden sonra, hemen sistemden çıkılmamış ve orada kalmaya başlanılmış; ancak orada kalmaya devam edecek kadar yeterli süre geçmemişse, suça teşebbüs söz konusudur[730]. Bunun sonucu olarak, bilişim sistemine girdikten sonra, orada kalmayı başaramamak, eğer anlık olmuşsa, yine suça teşebbüsten söz etmek güçtür; ancak anlık değil de, orada kalmaya başlandıkta sonra sistemde kalma başarılamamışsa, bu

[727] Barut ve Karayol, *Bilişim Suçları*, s. 237
[728] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 236
[729] Erdağ, Ali İhsan, "Ekonomi, Sanayi Ve Ticarete İlişkin Suçlar-Bilişim Alanında Suçlar (TCK'nin 9. ve 10. bölümleri)", s. 16, http://www.ceza-bb.adalet.gov.tr/makale.htm. (Erişim: 09.09.2013)
[730] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s.239

takdirde teşebbüs düşünülebilir[731].

TCK'nin 244. maddesinde düzenlenen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna teşebbüs mümkündür. Birinci fıkra açısından failin, bilişim sisteminin işleyişini bozmak veya engellemek için icra hareketlerine başlayıp, örneğin bilişim sistemine girip, elinde olmayan nedenlerle, engelleme veya bozma sonucunu gerçekleştiremezse; ikinci fıkrası açısından; fail bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek, erişilmez kılmak, sisteme veri yerleştirmek veya var olan verileri başka yere göndermek için harekete geçip, bu sonuçları kendisi dışında bir nedenle elde edemezse, üçüncü fıkra açısından ise; hareketleri yapmasına karşın amaçladığı haksız çıkarı elde edemezse, eylem teşebbüs aşamasında kalmış sayılacaktır. Ancak şunu belirtmekte fayda vardır ki, 244/3. fıkradaki suç yönünden fail başkasının banka hesabındaki parayı, kendi kontrolünde bulunan bir hesaba aktardığında, suç tamamlanacaktır, artık bu paranın çekilip çekilmemesi, fiilen zilyet haline gelip gelmemesi önemli değildir[732].

TCK'nin 244/4. fıkrası açısından failin eylemi teşebbüs aşamasında kalmış ise, bu durumda TCK'nin 244/1 ve 2. maddesi ile 4. fıkrasına teşebbüs eylemi arasında fikri içtima hükümleri uygulanacak, hangisi daha fazla cezayı gerektiriyorsa, o suç oluşacaktır. Örneğin fail, haksız bir çıkar sağlamak amacıyla bilişim sistemindeki bir veriyi değiştirdikten sonra, elinde olmayan nedenlerle, çıkar sağlayamaz ise, ikinci fıkrayla, dördüncü fıkraya teşebbüs eylemi arasında hangisi ağır cezayı gerektiriyor ise, o hüküm uygulanacaktır. Yine fail, 244. maddenin birinci ve ikinci fıkrasındaki suçu işlemek amacıyla eyleme başlayıp da, belirlenen sonuçları elde etmeden pişmanlık duyar ise, başka bir deyişle eyleminden gönüllü olarak vazgeçer ise, failin eylemi TCK'nin 243. maddesindeki suçu oluşturabilecektir[733]. O halde, burada failin amacının yalnızca bilişim sistemine girip orada kalmak mı, yoksa bilişim sisteminin işleyişini veya bilişim sistemindeki bir verinin bozulması, yok edilmesi veya değiştirilmesi mi, yoksa haksız bir çıkar sağlamak mı, bunun tespiti

[731] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s.172
[732] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s. 6767-6768
[733] Artuk ve diğerleri, *Yeni Türk Ceza Kanunu Şerhi*, Cilt 5**,** (2009), s. 4669

çok önemlidir, failin maksadı suçun vasfını ve teşebbüs aşamasında kalıp kalmadığını belirleyecektir[734]. Suçun gerçekleşmesi için haksız çıkarın sağlanması zorunludur. Aksi halde suç teşebbüs aşamasında kalır ki bu nedenle bilişim sistemi aracılığıyla haksız çıkar sağlamak teşebbüse elverişlidir. Örneğin; failin verilere müdahalede bulunamaması veya bulunmasına rağmen çıkar elde edememesi hallerinde suç teşebbüs aşamasında kalmış olacaktır.

Bu noktada failin bilişim sistemindeki verilere yönelik müdahaleyi hangi maksatla yaptığının tespiti önem taşımaktadır. Zira haksız çıkar sağlamak için bu fiilleri gerçekleştirmiş ancak menfaati sağlayamamışsa 244. maddenin 4. fıkrasına teşebbüsten; buna karşılık failin maksadı, yalnızca verilere veya sisteme zarar vermekse, 244. maddenin 1. veya 2. fıkralarından dolayı cezalandırılması gerekir. Belirtilen ölçüler çerçevesinde 243 ve 244. maddelerde tanımlanan ve teşebbüse elverişli olan suçların teşebbüs aşamasında kaldığı tespit edildiğinde, 61. maddeye göre belirlenen temel ceza TCK'nin 35/2 maddesi gereğince dörtte birinden dörtte üçüne kadar indirilecektir. İndirim miktarı iki limit arasında olacak şekilde meydana gelen zarar ve tehlikenin ağırlığına göre tespit edilecektir[735].

Görüldüğü üzere, inceleme konusu suçun kanuni dayanağını oluşturan kanun maddelerinden kişisel verilerin korunmasına yönelik olanlara teşebbüsün mümkün olup olmadığı tartışmalı iken, bilişim alanında işlenen suçlarla ilgili düzenlemelerdeki suç tipinde teşebbüs bulunmaktadır. Konunun bütün olarak değerlendirilmesi bilişim alanındaki kişisel verilere yönelik bir saldırı olduğunda ve bu suçun tamamlanamamış hali bulunduğunda teşebbüsün mümkün olacağı sonucuna götürmektedir. Örneğin, bir kişinin bilişim sistemine işlenmiş hastane kayıtlarına girerek sağlık verilerini değiştirmek suretiyle zarar vermek isteyen kişinin eylemini tamamlayamaması durumunda TCK 244/2. maddedeki suç teşebbüs aşamasında kalmış olacaktır.

---

[734] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 98
[735] Barut ve Karayol, *Bilişim Suçları*, s. 235

Bu tür suçları esastan incelemekle görevli olan Yargıtay 11. Ceza Dairesi ir ilamında[736]; "… bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından EFT'nin şikâyetçi şirketin hesabından sahte olarak açtırmış olduğu hesaba intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini aleyhe temyiz olmadığından bozma sebebi sayılmamıştır." değerlendirmesinde bulunmuştur. Yine 11. Ceza Dairesi konu ile ilgili bir ilamında[737] "… bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından havalenin şikayetçilerin hesaplarından kendi hesabına intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini", yine aynı Daire bir başka ilamında[738] "… sanığın mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdığı hesaplara internet yoluyla göndererek, yine sahte kimliklerle bu paraları çekmek istemesinden ibaret eylemlerinin; paranın sanığın açtırdığı hesaplara intikaline kadar gerçek kişilere yöneltilmiş hile bulunmayıp eylemlerin tamamen bilişim sistemi içinde gerçekleştiğinden, her bir mağdura karşı işlenmiş ayrı ayrı TCK'nin 244/4. maddesine uyan suçu oluşturduğu ve paranın açtırdığı hesaplara transferiyle suçun tamamlanacağı gözetilmeden, suçun vasıflandırılmasında yanılgıya düşülerek nitelikli dolandırıcılığa teşebbüs suçundan mahkumiyet hükmü kurulması yasaya aykırıdır" demek suretiyle suçun, paranın mağdur hesaptan şüpheli hesaba geçmesiyle tamamlandığını belirtmiştir. Bilişim suçlarını incelemekle daha sonra görevli hale gelen Yargıtay 8. Dairesi ise teşebbüs konusundaki kararlarında benzer görüşleri takip etmiştir[739]. Bu durumda, kişisel verileri elde ederek veya kullanarak bir suç işlenmesi amaçlanarak bilişim sistemine girilmesi ve suç işlenemeden sonlandırılması, bilahere bilişim sisteminden çıkılması durumunda bilişim sistemine

---

[736] Yargıtay 11. CD., 25.06.2007 gün ve 2007/2168 esas, 2007/4372 karar sayılı ilamı, UYAP, (Erişim: 22.12.2014)

[737] Yargıtay 11. CD., Tarih:18.09.2007, Esas: 2007/6963, Karar: 2007/5533 sayılı ilamı, Yargıtay, UYAP, (Erişim: 17.06.2014)

[738] Yargıtay 11. CD., Tarih: 27.09.2007, Esas: 2007/6709, Karar: 2007/6012 sayılı ilamı, Yargıtay, UYAP, (Erişim: 17.06.2014)

[739] Yargıtay 8. CD. Tarih: 25.04.2014, Esas: 2013/16038, Karar: 2014/10648, Yargıtay 8. CD. Tarih: 31.10.2013, Esas: 2013/10737, Karar: 2013/25854, Yargıtay 8. CD. Tarih: 03.04.2014, Esas: 2013/2941, Karar: 2014/8585, sayılı ilamları, Yargıtay, UYAP, (Erişim: 17.06.2014)

girme suçu (TCK m. 243) oluşacak fakat asıl hedeflenen suç gerçekleşmediği için bu suç yönünden teşebbüs aşamasında kalmış olacaktır.

Bu başlık altında çözümlenmesi gereken bir başka konu ise, bilişim suçlarında, faal nedamet ve ihtiyariyle vazgeçme durumlarında ne yapılması gerektiğidir. Teşebbüsü, gönüllü vazgeçmeden ayırmak gerekir. Elde olmayan sebeplerle icra hareketlerinin tamamlanamaması veya neticenin gerçekleştirilememesi teşebbüsün kurucu unsurunu oluşturmaktadır. Buna göre icra hareketlerinin tamamlanmaması veya neticenin gerçekleşmemesi failin elinde olan sebeplerden kaynaklanmışsa teşebbüsten söz edilemeyecektir. Bilindiği gibi gönüllü vazgeçme, suçu tamamlama imkanına sahip olan failin kendi iradesiyle icra hareketlerinin tamamlanmasından vazgeçmesi, faal nedamet ise icra hareketlerini tamamladıktan sonra kendi çabalarıyla suçun tamamlanmasını veya neticenin gerçekleşmesini önlemesi demektir[740]. Gönüllü vazgeçme olarak nitelendirilen bu durum kısaca failin kendi isteğiyle icra hareketlerine devam etmemesi veya bu hareketleri tamamladıktan sonra iradi etkin davranışlarıyla tipik neticenin meydana gelmesini önlemesi olarak tanımlanabilir[741]. Bu durumda, faile işlemek istediği suça teşebbüsten ceza verilmez. Ancak, vazgeçinceye kadar yaptığı hareketler başka bir suçu oluşturuyorsa o suçun cezası verilir (TCK m. 36). Mesela, fail kişisel verileri elde etmek üzere bilişim sistemine giriş yapsa fakat kişisel verilere ulaşmadan eyleminden vazgeçse ve bilişim sisteminden çıksa kişisel verilerin elde edilmesine ilişkin 135. maddeye teşebbüsten cezalandırılmaz. Ancak, o ana kadar işlediği eylem bilişim sistemine girme suçunu oluşturduğundan, bu suçun cezası verilir. Yine bir doktorun hastahane kayıtlarında bulunan bir hastaya ait hasta bilgilerini bir başka doktora internet üzerinden göndermek üzere hastane kayıtlarına ulaşsa fakat sonuçlarından çekinip vazgeçerek göndermemesi durumunda TCK'nin 136. maddesi yönünden failin durumu faal nedamete örnek olarak verilebilir[742].

---

[740] Barut ve Karayol, *Bilişim Suçları*, s. 240
[741] Sözüer, *Suça Teşebbüs*, s. 240; Özgenç, *Türk Ceza Hukuku, Genel Hükümler*, s. 428
[742] Barut ve Karayol, *Bilişim Suçları*, s. 240

Sanık bilişim sistemindeki verilere zarar vermek üzere bilişim sistemine girse, burada bir süre kalsa, zarar vermek istediği verilerin yerini sistem içerisinde bulsa, ancak nedense sonra tahrip etmekten vazgeçse ya da verileri bir süre uğraşarak değiştirdikten sonra ceza alacağını düşünerek tekrar eski haline getirse, 244/2 maddesinde tanımlanan suçtan ötürü cezalandırılamayacaktır, ancak o ana kadar yaptığı eylem, bir bilişim sistemine girmek ve orada kalmaya devam etmek tanımlamasına uyduğu için 243. maddesi gereğince cezalandırılacaktır[743]. Kişi kendisine ait kişisel verileri değiştirerek menfaat elde etmek üzere bilişim sistemine girmiş ise ve bu eylemini tamamlamadan vazgeçmiş ise eylemi TCK'nin 136. maddesi yönünden bir suç teşkil etmemekle birlikte fiilin şekline göre bilişim alanında ki suçlar için düzenlenen 243 ve 244. maddeler yönünden suç teşkil edebilecektir.

2.6.2. Suçların İçtimaı

Kanunun suç saydığı bir fiil, icrası esnasında, bir tek icra veya ihmal hareketi ile gerçekleştirilebileceği gibi, birden çok icra veya ihmal hareketi ile de gerçekleştirilebilir. Birden çok icra ya da ihmal hareketi, bazen birlikte bir bütün olarak kanunun suç saydığı bir fiili, dolayısı ile bir suçu oluştururken, bazen de birden çok fiili, dolayısı ile birden çok suçu oluşturmaktadır. Bir kimsenin birden çok kez ceza kanununu ihlal etmesi, bu yüzden de birden çok suçtan sorumlu olması halinde, suçların içtimaı[744] söz konusu olmaktadır. Suçların içtimaı; bir kimsenin, bir veya birden çok fiille, ceza kanununun aynı hükmünü veya farklı hükümlerini bir veya birden çok kez ihlal etmesi, dolayısı ile failin birden çok suçtan değil, ama tek bir suçtan sorumlu tutularak cezalandırılmasıdır[745]. Suçların içtimaı ya maddi içtima ya da şekli içtima olarak ortaya çıkmaktadır. Maddi içtimada, birden çok suç, birden çok fiille gerçekleşirken, şekli içtimada, birden çok suç, bir tek fiille gerçekleşmektedir. Esasen, kanundan ötürü, bileşik suç, zincirleme suç, fikri içtima hukuki yapılarını oluşturan birden çok cürmi fiil, tek bir fiil sayılmakta ve faile tek

---

[743] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 235
[744] Kelime anlamı, toplamak birleştirmektir.
[745] Centel ve diğerleri, *Türk Ceza Hukukuna Giriş*, s.502

bir ceza verilmektedir. Bu nedenle suçların içtimaı, cezaların içtimaının bir istisnasını oluşturmaktadır[746].

Suçların içtimaına benzer sonuçlar doğuran kurumlarda bulunmaktadır. Her netice, kural olarak bir suç teşkil eder ve fail kaç netice meydana getirmişse, o kadar suç işlemiş sayılarak her birinden dolayı ayrı ve müstakil cezalara maruz kalır. Ancak bir haraketle birden fazla neticenin meydana gelmesi durumunda faile tek bir ceza verilmesini gerektiren hâller vardır ve bunlardan biri müteselsil suçtur[747]. TCK'nin 43. maddesinde "Bir suç işlemek kararının icrası cümlesinden olarak kanunun aynı hükmünün birkaç defa ihlal edilmesi, muhtelif zamanlarda vaki olsa bile bir suç sayılır" demek suretiyle bu hususu açıklamıştır[748]. Bu kapsamda "Bileşik Suç" kavramı üzerinde durmak yararlı olacaktır. Kanunda her biri başlı başına bir suç olarak tanımlanmış olan fiiller, kanundan ötürü, bir suçun unsuru veya bir suçun ağırlaştırıcı nedeni olabilmektedir. Buna bileşik suç denmektedir. TCK'nin 42. maddesinde bileşik suç "Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir." şeklinde tanımlanmaktadır. Bundan başka, kanunda suç olarak düzenlenen bir fiil, başka bir suçun ağırlatıcı nedeni olabilmektedir. Bu durumda temel suç herhangi bir değişikliğe uğramaz, aynı kalır, sadece suçun cezasında arttırıma gidilir[749].

TCK'nin beşinci bölümünde düzenlenen suçların içtimaı başlakla bölümde sırasıyla bileşik suç, zincirleme suç ve fikri içtima düzenlenmiştir. Belirtilen bu müesseselerin inceleme konusu suçta nasıl uygulunacağını incelemek özellikle gereklidir.

2.6.2.1. Zincirleme Suç

Bir suç işleme kararının icrası kapsamında aynı suçun birden çok işlenmiş olması hâlinde zincirleme suç söz konusudur. Yani bu suçlar birbirleriyle sübjektif bir

---

[746] Soyaslan, *Ceza Hukuk Genel Hükümler*, s. 266
[747] Dönmezer ve Erman, *Nazari ve Tatbiki Ceza Hukuku*, s.450.
[748] Yenidünya ve Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, s.80
[749] Soyaslan, *Ceza Hukuk Genel Hükümler*, s. 269

şekilde bağlı bulunmaktadırlar. Zincirleme suçun söz konusu olabilmesi için aranan ilk şart, birden çok fiilin bulunmasıdır. Ancak, işlenen fiillerden her birinin aynı suçu oluşturması gerekir. "Bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır" (TCK, m. 43, f. 1, ikinci cümle). Zincirleme suç halinde, ortada birden fazla suç mevcut olup, aynı suçun birden çok kez aynı kişiye karşı işlenmesi, yani her suçun mağdurunun aynı kişi olması gerekir. Her gün aynı kişinin e posta adresine girilerek kişisel verilerinin elde edilmesi (TCK m. 135) veya aynı kişinin kişisel verilerinin kullanılarak suç işlenmesi (TCK m. 136) gibi durumlarda, aslında örneğin hakaret ve cinsel taciz gibi suçlar birden fazla işlenmektedir. Ancak, bu suçlar arasındaki manevi bağ dolayısıyla, zincirleme suçun varlığı kabul edilmektedir. Keza, bir kişiye karşı müteaddit defa kişisel verileri, örneğin banka hesap kayıtları kulanılarak hırsızlık suçunun işlenmesi halinde de, zincirleme suç söz konusudur.

Zincirleme suç, icrai hareketle işlenebilen suçlarda mümkün olduğu gibi, ihmali suçlarda da söz konusu olabilir[750]. Zinciri oluşturan hareketlerden örneğin 243. maddede olduğu gibi bir kısmının icrai, bir kısmının ihmali olması halinde de zincirleme suç kabul edilmektedir[751]. Ancak bu durumda, ihmali hareketlerin ayrı bir suç oluşturmaması gerekir[752]. Birden fazla suçlardan hepsinin teşebbüs durumunda bulunması veya bazılarının tamamlanmasına karşılık diğer bazılarının teşebbüs derecesinde kalması halinde de zincirleme suç gerçekleşebilir. Zincire dâhil olan suçlardan birisi tamamlanmış diğerleri teşebbüs derecesinde kalmışsa, zincirleme suçun da tamamlandığı kabul edilerek, ceza artırımı bunun üzerinden yapılır[753]. Bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır (m. 43, f. 1, üçüncü cümle).

---

[750] Hakeri, Hakan, "İhmali Suçlar", *Ceza Hukuk Dergisi*, Yıl: 2, 2007/4, s. 303.
[751] İçel, Kayıhan: *Suçların İçtimai, Genel Bilgiler - Fikrî İçtima - Müteselsil Suçlar - Görünüşte İçtima,* 1972, İstanbul: Sermet Matbaası, s. 114; Sancar, Türkan Yalçın, *Müteselsil Suç*, 1995, Seçkin Yayınevi, Ankara: s. 70; Hakeri, *İhmali Suçlar*, s. 304
[752] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler,* s.441
[753] İçel, *Suçların İçtimai*, s. 114; Dönmezer ve Erman, *Nazari ve Tatbiki Ceza Hukuku*, Cilt: I, s. 530.

Sonuçları yönünden, zincirleme suçun şartlarının gerçekleştiği tespit edildiğinde, işlenen suçlardan dolayı faile sadece bir suçun cezası verilecektir ancak, bu ceza, dörtte birinden dörtte üçüne kadar artırılır[754]. İfade edelim ki, burada teşebbüse ilişkin hükmün uygulanması, ancak zincirleme suça dâhil olan tüm suçların teşebbüs aşamasında kalması halinde mümkündür. Şayet suçlardan birisi tamamlanmışsa artık teşebbüs aşamasında kalan suç cezanın belirlenmesinde dikkate alınmayacak, sadece suçun sayısının tespitinde fonksiyon ifa edecektir. Diğer taraftan suçlardan birisi olası kastla işlenmişse 61. madde de dikkate alınmayacaktır[755].

Kişisel verilerin kaydedilmesi suçunu düzenleyen TCK'nin 135. maddesinde de, bu suç aynı kişiye karşı birden fazla defa, aynı suç işleme kararının icrası kapsamında işlenirse, zincirleme suç hükümleri uygulanacaktır. Ayrıca, tek bir hareketle birden fazla kimsenin kişisel verilerin kaydedilmesi halinde, zincirleme suç hükümleri uygulanmayacaktır. Hukuka uygun veya hukuka aykırı olarak kaydedilen verileri hukuka aykırı olarak başkasına verme, açıklama ve yayma fiillerinin yapılması halinde ise kanunun 136. maddesi ihlal edilmiş olur. Fail birden fazla kişinin kişisel verisini hukuka aykırı şekilde toplarsa, topladığı sayı kadar suç işlemiş olur. Meselâ insanlardan kimlik bilgilerini alarak kişisel verilere ulaşmada veri sayısınca suç işlenmiş sayılacaktır[756]. TCK'nin 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek suçu, aynı suç işleme kararının icrası kapsamında olmak üzere aynı kişiye ait verilerin birden fazla kişiye verilmesi halinde, zincirleme suç hükümleri uygulanacaktır. Ayrıca, tek bir hareketle birden fazla kimsenin kişisel verilerinin başkasına verilmesi halinde, zincirleme suç hükümleri uygulanmayacaktır.

TCK'nin 243. maddesinde belirtildiği üzere fail, bir bilişim sistemine (tamamına ya da bir kısmına) hukuka aykırı olarak girdikten sonra orada kalmaya

---

[754] Üzülmez, İlhan, "Yeni Ceza Kanunun Sisteminde Cezanın Belirlenmesi ve Bireyselleştirilmesi", *EÜHFD*, Cilt: II, Sayı: 2007/1-2, s. 224-225
[755] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 446
[756] Soyaslan, *Ceza Hukuk Genel Hükümler,* s. 344

devam etmelidir. İşte failin bilişim sisteminde kalmasıyla temadi (sürme, sürüp gitme, uzama) gerçekleşmiş olmaktadır. Temadinin bitmesiyle suç tamamlanmış olacağından, dava zamanaşımı da bu tarihte işlemeye başlayacaktır. Örneğin, bir kişinin kişisel bilgilerini arkadaşına ait bilgisayarda ki bir dosyada muhafaza ettiği düşünülecek olursa, bu bilgisayara erişim sağlanarak, bu dosyaya müdahale edilmesi durumunda, eylem hem bilgisayarın sahibine hem de veri sahibine karşı işlenmiş olur. Bu durumda, diğer koşulları da oluşmak şartıyla TCK'nin 43/2. maddesi uygulanabilir[757].

Burada bir diğer sorun da, TCK'nin 244. maddesindeki suç oluştuğu zaman, aynı zamanda 243/1. maddesindeki suçun da oluştuğu kabul edilecek ve ayrı ayrı cezalar mı tayin edilecek, yoksa yalnızca 244. maddesindeki suçtan mı ceza verileceği hususudur. Gerçekten de, 244. maddedeki fiiller zorunlu olarak 243/1. maddedeki suçu da içermektedir. Burada Yazıcıoğlu geçitli suç hükümleri uygulanarak iki suçtan değil, yalnızca sonuç suçtan (TCK m. 244) ceza verilmesi gerektiğini belirtmektedir[758]. Bir bilişim sistemine girme fiili, TCK'nin 243. maddesinde bağımsız suç olarak düzenlenmiştir. 244. maddedeki fiiller ise ancak bir bilişim sistemine girmek suretiyle işlenmektedir. Burada geçitli suç hükümleri uygulanarak iki ayrı suçtan değil yalnızca sonuç suçtan (TCK m. 244) ceza tayini gerekmektedir. Burada farklı neviden fikri içtimanın (TCK m. 44) varlığını kabul eden görüşler de vardır. Bu yöndeki görüşlere göre, fikri içtimada bir suçun icra hareketlerinin bir başka suçun icra hareketleriyle kısmen veya tamamen örtüşmesi gerekli ve yeterlidir. Bir bilişim sistemindeki verileri değiştirmek isteyen fail, bu suçun icra hareketlerini gerçekleştirirken, sisteme de girmekte ve dolayısıyla 243. maddeyi de ihlal etmektedir. Bu itibarla, failin bu suçlardan yalnızca en ağır cezayı gerektiren 244. maddedeki suçtan dolayı cezalandırılması gerekecektir[759]. TCK'nin 244. maddesinde düzenlenen bilişim sistemindeki verilere zarar verme eylemi, değişik zamanlarda aynı kişiye karşı, birden fazla işlenirse, zincirleme suçtan (TCK

---

[757] Artuk ve diğerleri, *Ceza Hukuku Özel Hükümler,* s.703-704; Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 261.

[758] Yazıcıoğlu, *Bilgisayar Suçları*, s. 27, Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 263

[759] Koca, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s.8-9

m. 43) bahsetmek olanaklıdır. Dördüncü fıkradaki suç, değişik zamanlarda, aynı kişiye karşı, birden fazla işlenebilir. O zaman zincirleme suç gerçekleşir (TCK m. 43/1). 244. maddenin 4. fıkrasındaki suçun gerçekleşmesi halinde artık aynı maddenin 2. veya 3. fıkrasından ceza verilmeyecektir.

2.6.2.2. Fikri İçtima

Fikri içtima; tek bir fiille kimine göre tek bir icra veya ihmal hareketi ile ceza kanununun aynı anda birden çok hükmünün ihlal edilmesi, dolayısı ile birden çok suç işlenmesi, ancak bunlardan sadece en ağır olandan ceza verilmesi olarak tanımlanmaktadır. Fikri içtimada, suçlar birbirinden bağımsızdır. Herhangi bir nedenle cezası en ağır suç oradan kalktığında, fail serbest kalmaz, kalan diğer suçtan sorumlu olur. TCK'nin 44. maddesinde düzenlenen fikri içtima; " İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır." şeklinde tanımlamak mümkündür[760]. Burada fail tarafından işlenen birden fazla eylem bulunmasına rağmen her bir eylem için ayrı bir suç teşkil etmemekte bir suç işleme kararının icrası cümlesinden hareket eden fail kendisinde var olan tek suç işleme kastı nedeniyle cezalandırılmaktadır. Örneğin öğretmeninin bilgisayarına ayrı günlerde müteaddit defalar girerek kendine ait sınav notlarını peyderpey değiştiren bir öğrencinin her girişi ve sonrasında elde ettiği kişisel verileri değiştirmesi eylemi için ayrı bir suç işlediği kabul edilmeyecek, bir suç işleme kararının cümlesinden, yani belirli bir derse ait sınav notlarını değiştirme kastıyla gerçekleştirdiği bu fiillerin tamamı bir suç sayılacak ve ona göre hüküm kurulacaktır.

Kişisel verilerin hukuka aykırı olarak kaydedilmesini düzenleyen TCK'nin 135. maddesi ile verileri hukuka aykırı olarak verme veya ele geçirmeyi düzenleyen TCK'nin 136. maddesindeki suçların zincirleme suç şeklinde işlenmesi mümkündür. Öte yandan fail hukuka aykırı olarak kişisel veriyi kaydetmekle başkasına vermek ya da yaymak fiillerini aynı anda gerçekleştirebilir. Örneğin, kişisel verinin ulaşılabilir

[760] Hafızoğulları, Zeki ve Özmen, Muharrem, *Türk Ceza Hukuku Genel Hükümler*, 5. Bası, Us-A Yayıncılık, Ankara: 2012, s. 374 vd.

bir internet sitesinde kaydedilmesi ile aynı zamanda yaymak fiili de gerçekleşmiş olur. Bu durumda fikri içtima düşünülebilir. Gerçekten kişisel verileri hukuka aykırı olarak yaymak 136. maddede ayrıca suç olarak düzenlenmiştir. Bu durumda fikri içtima hükmü gereği en ağır cezayı gerektiren 136. madde hükmü uygulanmalıdır. Zira verileri kaydetmenin haksızlık içeriği, verileri yayma fiilinin haksızlık içeriğinde erimiş olur[761].

Bir bilişim sistemine girmenin suç olarak düzenlendiği TCK'nin 243. maddesi, zincirleme suç hükümlerinin uygulanmasına elverişlidir. Yani fail aynı suç işleme kararıyla bir kişiye ait bir bilişim sitemine değişik zamanlarda birden fazla girip orada kalabilir. Bu durumda zincirleme suç hükümleri uygulanır. Bunun dışında bir bilişim sitemine girmek ve orada kalmak suretiyle sistem sahibinin veya bir başka kişinin kişisel verileri elde ediliyor veya kullanılarak suç işleniyorsa (TCK m. 135 ve 136) bu durumda da ortaya çıkan suçlar arasında fikri içtima hükümleri uygulanabilir. Bu hususta üzerinde durulacak son nokta, bileşik suça ilişkindir. Şayet bir suçun işlenmesi için TCK'nin 243'deki suçlar bir unsur veya ağırlaştırıcı neden olarak düzenlenmişse bu durumda artık bilişim sistemine girme ve orada kalmaktan dolayı ceza verilemez[762].

TCK'nin 135. ve 136. maddelerinde belirtilen suçun işlenmesi için, TCK'nin 243. maddesinde düzenlenen hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunun da işlenmesi halinde, yalnızca TCK'nin 135. veya 136. maddesinde öngörülen ceza faile verilecektir. Çünkü fikri içtimayı düzenleyen TCK'nin 44. maddesi gereğince fail, en ağır cezayı gerektiren suçtan dolayı cezalandırılır[763]. Burada TCK'nin 243 ve 244. maddeleri arasındaki ilişkiye de değinmek gerekir. TCK 244. maddede yer alan suçun işlenebilmesi için kural olarak bilişim sitemine girmek ve orada kalmak gerekir. Bu yönüyle iki hüküm arasında bir "geçitli suç" ilişkisinin bulunduğu söylenebilir. Bu çerçevede faile 244. maddede düzenlenen suç oluştu ise bu maddede yer alan ceza yanında bir de 243. maddede

---

[761] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.527 - 530
[762] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, Cilt: V, s.6571
[763] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 181

düzenlenen suçtan dolayı ceza verilemez[764].

TCK'nin 244. maddesinde düzenlenen bilişim sistemini engellemek, bozmak, verileri yok etmek veya değiştirmek suçları açısından içtimaın her türü mümkündür[765]. Örneğin bir kişiye ait bilişim sisteminin işleyişini farklı zamanlarda birden fazla engelleyen veya bozan kişinin eylemi bakımından zincirleme suçtan bahsetmek mümkündür. Yine aynı şekilde; bir kişinin başka bir kişiyle internet üzerinden gerçekleştirdiği haberleşme esnasında üçüncü bir kişi tarafından haberleşmenin gerçekleştiği bilgisayara haberleşme esnasında trojen programı yerleştirilerek bir takım kişisel veriler elde edilse TCK'nin 244/1 ile TCK'nin 135. maddesindeki suçlar arasında fikri içtima ilişkisi kurulabilir. Çünkü fail gerçekleştirdiği tek bir hareketle birden fazla suçun gerçekleşmesini sağlamıştır. Bunun dışında suçun TCK'nin 244/1 ve 2'nin seçimlik hareketli suçlardan olmaları dolayısıyla, seçimlik hareketlerden birden fazlasının gerçekleştirilmesi halinde de sadece tek suç işlenmiş kabul edilecektir. Fakat fail aynı suç işleme kararıyla farklı zamanlarda bu seçimlik hareketleri gerçekleştirirse o zaman zincirleme suç hükümleri devreye girecektir. Bunun dışında TCK'nin 244/4'deki suçun gerçekleşmesi halinde, TCK'nin 244/1 ve 2 bu suçun unsuru haline dönüştüğü için bileşik suç söz konusu olacaktır ve ayrıca TCK'nin 244/1 ve 2'den ceza verilmeyecektir. Burada uygulamada güçlük oluşturması nedeni ile 244. maddenin (4) numaralı fıkrada, "başka bir suç oluşturmaması" ibaresi, "daha ağır başka bir suç oluşturmaması" şeklinde gerekçeye uygun olarak düzeltilmelidir[766].

TCK'nin 243. maddesinde düzenlenmiş bulunan "hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu" kişisel verilerin kaydedilmesi ve verileri hukuka aykırı olarak başkasına verme, yayma veya ele geçirme suçları açısından geçit suçu oluşturmaktadır. Gerçekten de birçok olayda anılan suçların oluşması için öncelikle bilişim sistemine hukuka aykırı olarak girilmesi ve orada

[764] Soyaslan, *Ceza Hukuk Özel Hükümler*, s. 613
[765] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.870
[766] Karagülmez, *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, s. 194

hukuka aykırı olarak kalınması gerekecektir. Bu durumda faile yalnızca 135. maddede öngörülen ceza verilecektir[767].

135. maddede düzenlenen kişisel verilerin kaydedilmesi suçuyla 136. maddede düzenlenen kişisel verileri hukuka aykırı olarak verme ve ele geçirme suçu arasında da suçların içtiması söz konusu olabilecektir. Örneğin fail düşmanlık beslediği bir kişinin özel yaşantısını yaymak için bu kişi hakkındaki verileri öncelikle kaydetmek zorunda kalabilecektir. Bu durumda da 135. maddede düzenlenen suç tipi 136. maddede düzenlenen suç tipi açısından geçit suç teşkil edecek, fail sadece 136. madde uyarınca cezalandırılacaktır[768]. Bir kimse 135. maddesindeki suçu işledikten sonra, aynı zamanda 136. maddedeki eylemi de gerçekleştirirse, içtimanın uygulanıp uygulanmayacağı konusunda görüş birliği yoktur. Malkoç ile Yaşar/Gökçen/Artuç' göre burada gerçek içtima hükümleri uygulanarak her iki suçtan ayrı ayrı ceza verilmesi gerekir. Ancak aynı eylemle, farklı konularda bile olsa, elde edilen verilerin verilmesi veya ele geçirilmesi durumunda tek suç oluşacaktır[769]. Özbek/Kanbur/Doğan/Bacaksız/Tepe ise fail hukuka aykırı olarak kişisel veriyi kaydetmek ile başkasına vermek ya da yaymak fiillerini aynı anda gerçekleştirmesi durumunda örneğin, kişisel verinin ulaşılabilir bir internet sitesine kaydedilmesi ile aynı zamanda yaymak fiili de gerçekleşmiş olması halinde fikri içtimanın olabileceğini düşünmektedirler. Kişisel verileri hukuka aykırı olarak yaymak 136. maddede ayrıca suç olarak düzenlendiğine göre, fikri içtima hükmü gereği en ağır cezayı gerektiren TCK'nin 136. maddesi hükmü uygulanmalıdır düşüncesinde oldukların beyan etmektedirler ve bu düşüncelerini bu durumda verileri kaydetmenin, verileri yayma fiilinin haksızlık içeriğinde erimiş olacağına dayandırmaktadırlar[770]. Buna karşın kişisel verileri başkasına veren, yayan veya ele geçiren kişinin eylemi TCK'nin 136. maddesinde düzenlenen suçu oluşturacaktır. Ancak, kişisel bilgileri alanın eylemi ile ilgili kanunda herhangi bir düzenleme yer almamaktadır.

---

[767] Dülger, *Bilişim Suçları*, s.275
[768] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu*, s.4122 ve 4128
[769] Malkoç, *Açıklamalı Yeni Türk Ceza Kanunu*, s. 913, Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu,* s.4122 ve 4128
[770] Özbek ve diğerleri, *Türk Ceza Hukuku Genel Hükümler*, s.201

Fikri içtimaya bir başka örnek de şu şekilde verilebilir. Bir kamu bankasının bilişim sistemine giren ve orada bulunan 5.000,00 TL olan hesabını 50.000,00 TL olarak değiştiren kişi, bu eylemi ile hem 243. maddede tanımlanan bir bilişim sistemine girme ve orada kalmaya devam etme suçunu işlemiş, hem de 244/son maddesinde tanımlanan bir bilişim sistemindeki verileri değiştirerek kendine haksız çıkar sağlama suçunu işlemiştir. Fail 44. madde hükmü gereğince bunlardan en ağır olan 244/son maddesi uyarınca cezalandırılacak, diğer suçtan ayrıca bir ceza verilmeyecektir.

İçtima ile ilgili bir başka ihtimal ise fail tarafından işlenen fiilin bir başka suçun ağırlaştırıcı nedeni ya da unsuru olmasıdır. Mürekkep suç denilen bu durumda bağımsız bir suç sayılan netice, diğer bir neticenin içinde erimekte ve faile daha ağır cezayı gerektiren neticeden dolayı ceza verilmektedir. Bu suçlar da mürekkep, karma ve geçitli suçlara benzer. Ancak aralarında bazı farklar bulunmaktadır. Öncelikle mürekkep suç iki ayrı suçtan meydana gelir. Bu suçlardan biri diğerinin ya unsurunu ya da ağırlaştırıcı sebebini oluşturur[771]. Bilişim sistemine girme (TCK m. 243) ve sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK m. 244) suçları ile birlikte işlenen kişisel verilerin kaydedilmesi (TCK m. 135) ile verileri hukuka aykırı olarak verme veya ele geçirme suçları (TCK m. 136) TCK'de ayrı ayrı düzenlendiği halde bu araştırmanın konusunu da oluşturan bilişim alanındaki kişisel verilerin korunmasına yönelik ayrı bir düzenleme yoktur. Bu nedenle mürekkep suç konusuna bir örnek vermek mümkün olmayacaktır.

En son ihtimal ise, failin birden fazla hareketi ile kanunun birden fazla maddesini ihlal etmesidir. Burada failin birden fazla hareketi bulunmakta ve bunların her birisi kanunun başka hükmünü ihlal etmektedir. Sanık ilk gün kendi yeteneklerini denemek amacıyla bir bilişim sistemine örneğin Adalet Bakanlığının adli sicil bilgilerinin tutulduğu bilişim alanına girse ve orada kalmaya devam etse, ertesi gün bu sefer aynı bilişim sistemine tekrar girse ve orada kalmaya devam ederek bu sistemde yar alan kişisel verileri (adli sicil kayıtlarını) yok etse, sonrasında bilişim

[771] Centel ve diğerleri, *Türk Ceza Hukukuna Giriş*, s.522

sistemine de zarar verse burada faili ilk günkü eylemi nedeniyle hakkında bilişim sistemine girme suçundan 243. maddesi uyarınca, ikinci gün ise bilişim sistemine girme ve orada kalmaya devam etme suçu, verilere zarar verme suçu ile içtima ettiğinden bunlardan ağır olan verilere zarar verme suçunu düzenleyen 244/2 maddesi uyarınca, nihayet verilere zarar vermekle yetinmeyip ayrıca bilişim sistemine de zarar vermişse bu eylemi nedeniyle 244/1 maddesi uyarınca ayrı ayrı cezalandırılacaktır.

İçtima konusuyla ilgisi olmasa da bu bölüm altında işlenmesinin uygun olacak en son konu ise karma suç kavramıdır. Her neticenin bağımsız bir suç meydana getirmesi kuralının iki istisnası vardır. Birincisi, yukarıda belirtilmiş olan müteselsil suç, diğeri ise "muhtelif" (karma) *suç*tur. Bu tür suçlarda diğer tüm neticeler bir neticenin içinde erir ve kaybolurlar. Sonuçta da faile tek bir neticeden dolayı ceza verilir. Suç teşkil eden bir fiil, zorunlu olarak daha hafif bir suçu da içine alıyorsa ortada "karma suç" vardır. Bu durumda faile daha ağır olan suçun cezası verilir[772]. Örneğin veri almak amacıyla bir bilişim sistemine girerek orada bir süre kalan ve sistem içinde bulunan verileri başka yere gönderen failin eylemindeki bilişim sistemine girme ve orada kalmaya devam etme suçu, verileri başka yere gönderme suçu içinde eriyecektir. Fail veriyi başka bir yere gönderme fiilini bilişim sistemine girerek ve orada bir süre kalarak gerçekleştirmektedir. Bu tarzda suçun işlenmesi durumunda karma suç oluşacaktır. Ancak verileri başka bir yere göndermek teknik olarak bilişim sistemine girmeksizin ve orada bir süre kalmayı gerektirmeksizin de işlenebilen durumlarda bu suçun görünüş şekli karma suç şeklinde olmayacaktır.

2.6.4. İştirak

Kanunda düzenleniş şekline ve niteliği gereği tek kişinin işleyebileceği bir suçun, birden fazla kimsenin aralarında anlaşma yaparak birlikte işlemesi durumunda, suçun özel görünüş şekillerinden iştirak ortaya çıkar ve bu suçlara iştirak halinde suçlar adı

[772] Taşkınve Zengin, *Ceza Hukuku El Kitabı*, s.42

verilir[773]. Bu durumda, fiilin icrasına katılan suç ortaklarının hepsi de fiilin oluşumuna bir katkıda bulunmaktadırlar ve bu katkıları nedeniyle sorumlulukları söz konusudur. Suçun icrasına iştirak etmekle beraber, suçun işlenişine bulunduğu katkı suçun kanundaki tarifine uygun olmayan, örneğin azmettiren veya yardım eden diğer suç ortaklarının da gerçekleşen haksızlıktan sorumlu tutulabilmeleri gerekir[774]. TCK'de suça iştirak, faillik ve şerikliği kapsayan üst bir kavram olarak kabul edilmiştir. Şeriklik ise, azmettirme ve yardım etmeyi kapsamaktadır[775]. İştirak halinde işlenen suçlarda failler ile şerikler arasında cezalandırma bakımından ayrım yapılmış, ayrıca dar fail anlayışından hareketle suç tipindeki fiili gerçekleştiren kimseler fail olarak nitelendirilmiştir[776].

TCK'nin 135, 136, 243 ve 244. maddelerinde düzenlenen suçlara iştirak, diğer suç tiplerinden farklılık göstermez. Bilişim sistemine giren ve verileri elde etmek isteyen kişi kendi verileri üzerinde bu işlemi gerçekleştirirse suçun faili olarak yer alırken, bu eylemi kendisi bilgisayar kullanmayı bilmediği için bir başkasına yaptırırsa (örneğin; bir hecker'e ya da veri işleme memuruna) suçun iştirakçisi olarak cezalandırılacaktır. Bu suçlara iştirakle ilgili özel bir hüküm bulunmayıp genel hükümler uygulanacaktır. TCK'nin 37. maddesinin birinci fıkrasında, suçun kanuni tanımına uygun bir şekilde eylemi birlikte gerçekleştiren kişilerden her birinin fail olarak sorumlu tutulacağı, ikinci fıkrasında ise, suç işlenirken bir başkası araç olarak kullanılırsa, kullanan kişinin de fail olarak sorumlu tutulacağı, kusur yeteneği olmayanları suçun işlenmesinde araç olarak kullanan kişinin cezasının da üçte birden yarısına kadar arttırılacağı düzenlenmiştir[777]. Sahip olduğu bilgisayarı ve internet hattını bilişim korsanına tahsis ederek bilişim sistemine girme ve orada kalma suçu ile birlikte kişisel verilerin kullanılarak bir suç işlenmesine yardım eden, bu suçu işleme fikri bulunmayan faili bu konuda ikna eden, suçun nasıl işleneceği konusunda teknik bilgi sunan, bu suçu işledikten sonra ceza soruşturmasından kurtulma

---

[773] Yenidünya ve Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, s.80
[774] Hafızoğulları, *Türk Ceza Hukuk Ders Notları*, s. 428
[775] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 241
[776] Erdem, Mustafa Ruhan,"Yeni TCK'de Faillik ve Suç Ortaklığı", *Hukuki Perspektifler Dergisi*, Sayı: 2005/5, s. 205
[777] Kurt, *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, s. 240

konusunda yardım vaat eden, bilişim sistemine girmeyi temin edecek yazılımları temin eden kişi yardım eden sıfatıyla bu fiillerinden ötürü cezalandırılacaktır.

2.7. GÖREVLİ MAHKEME VE KOVUŞTURMA

TCK'nin 243 ve 244. maddelerinde düzenlenen bilişim suçlarının tamamı şahsi dava ve şikayete bağlı olmayıp re'sen kovuşturulması gereken suçlardandır. Bilişim suçlarının Asliye Ceza mahkemesinde görüleceği konusunda genel bir kabul bulunmaktadır[778]. Ancak görevli olan mahkemenin hangisi olduğu ile ilgili uygulamada ihtilaflar çıkması nedeniyle Yargıtay konuyu bir içtihatla çözümlemiştir. Bilişim suçları ile ilgili verilen ilk derece mahkemelerinin kararlarının temyiz inceleme mercii olan Yargıtay 8. Ceza Dairesinin, konu ile ilgili bir kararında "...Sanık hakkında düzenlenen iddianamedeki isnat olunan ''Bilişim sistemindeki verileri bozma, yok etme, erişilmez kılma, sisteme veri yerleştirme'' suçunun TCK'nin 244/2. madde ve fıkrasına uygun bulunduğu ve anılan madde hükmünde öngörülen cezanın üst sınırına göre 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri hakkındaki Kanunun 11. maddesi uyarınca Asliye Ceza Mahkemesinin görevli olduğu gözetilerek görevsizlik kararı verilmesi gerekirken, görevsiz Sulh Ceza Mahkemesince yargılamaya devamla hüküm kurulması..." denilmek suretiyle Asliye Ceza Mahkemesinin görevli olduğu belirtilmiştir[779]. Bilişim suçlarının Asliye Ceza Mahkemesinde görülmesine ilişkin Yargıtayın kararlı bir duruşu bulunmaktadır[780]. Alt dereceli bir mahkeme bu suçlara ilişkin bir dava geldiğinde durumu re'sen dikkate alarak görevsizlik kararıyla dosyayı görevli mahkemeye göndermelidir.

---

[778] Yazıcıoğlu, *Bilgisayar Suçları*, s.291; Taşdemir, *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, s. 391

[779] Yargıtay 8. CD., Tarih: 05.05.2014, Esas: 2013/9417, Karar: 2014/11384 sayılı ilamı, Yargıtay, UYAP, (Erişim: 18.06.2014), diğer bir örnek için bkz. Yargıtay 8. CD., Tarih: 16.04.2014, Esas: 2013/2817, Karar: 2014/9715 sayılı ilamı, Yargıtay, UYAP, (Erişim: 18.06.2014),

[780] Yargıtay 8.CD., Tarih: 31.03.2014, Esas: 2013/10240, Karar: 2014/8042 sayılı ilamı, Yargıtay 8.CD., Tarih: 14.04.2014 Esas: 2013/10778, Karar: 2014/9482 sayılı ilamı, Yargıtay, UYAP, (Erişim: 18.06.2014)

Görev konusunda dikkat edilmesi gereken bir konu da, bilişim suçunun bir başka suç daha oluşturması ve bu suçun incelenmesi görevinin daha üst görevli bir mahkemeye verilmesi durumudur. Eğer bilişim sistemi vasıta kılınarak işlenen suç örneğin aynı zamanda TCK'nin 158/1-f maddesinde düzenlenen bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu da oluşturuyorsa görevli mahkeme artık Asliye Ceza Mahkemeleri olmayacak, bu ikinci suçu inceleme görevine sahip olan Ağır Ceza Mahkemeleri olacaktır. Nitekim Yargıtay 8. CD. bir kararında; "…Oluşa ve dosya kapsamına göre sanığın üzerine atılı, şikayetçinin MSN adresini ve şifresini bir şekilde ele geçirerek bu adresten şikayetçi gibi yazışmak suretiyle kendine yarar sağlamak amacı ile kontör talep edip şifrelerinin kendisine gönderilmesini temin etmeye çalışmaktan ibaret eylemin, TCK'nin 244/2. maddesinde düzenlenen bilişim sistemindeki verileri değiştirme ve erişilmez kılma suçunun yanında, ayrıca TCK'nin 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu da oluşturup oluşturmayacağına ilişkin delilleri takdir ve tartışmanın 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 12. maddesi uyarınca ağır ceza mahkemesinin görevinde bulunduğu gözetilerek görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı biçimde hüküm kurulması…" şeklindeki hüküm ile görevli mahkemenin daha üst derece mahkemesince görüleceğini hükme bağlamıştır[781]. TCK'nin 135. ve 136. maddelernde düzenlenen suçları yargılama görevi, 5235 sayılı Kanunun 10-14. maddeleri uyarınca asliye ceza mahkemesine aittir. Kısaca bir değerlendirme yapılacak olursa, sulh ceza hakimliği ve ağır ceza mahkemelerinin görevleri içinde olmayankalan, özel kanunlarla asliye ceza mahkemelerince görülüp karara bağlanacağı düzenlenen veya özel kanunlarda görülüp karara bağlanacağı mahkemenin açıklanmamasına karşın sulh ceza hakimliği ve ağır ceza mahkemesinin görevi içinde olmayan tüm ceza davalarına asliye ceza mahkemeleri bakmakla görevli olduğundan, bilişim suçlarına da bakmakla görevli olacaktır.

[781] Yargıtay 8. CD., Tarih: 14.05.2014, Esas: 2013/11730, Karar: 2014/12386 sayılı ilamı, Yargıtay, UYAP, (Erişim: 18.06.2014)

243. maddede tanımlanan bilişim sistemine girme ve orada kalmaya devam etme, 244. maddesinin 1. fıkrasında tanımlanan sistemin engellenmesi, 244. maddesinin 2. fıkrasında tanımlanan bilişim sistemindeki verilerin erişilmez kılınması suçlarında suç olarak tarif olunan fiiller süregelen yani temadi eden eylemlerdir. Mütemadi suç dediğimiz bu suçlarda fiil temadinin bittiği anda meydana gelmiş sayılır. Mütemadi suç, neticenin hemen sona ermeyip zaman içinde devam ettiği suçtur. Mütemadi suç, temadinin[782] sona erdiği anda işlenmiş sayılır ve o anda yürürlükte olan kanun uygulanır[783]. 243. maddede tanımlanan suçun ağırlaştırıcı halini düzenleyen 3. fıkrasındaki bu eylemler sebebiyle sistemin içerdiği verilerin yok olması veya değişmesi durumunda ise temadinin kesildiği anda değil verilerin yok olması ya da değişmesi anında suçun oluştuğu tabiidir. 244. maddesinin 1. fıkrasında tanımlanan sistemin bozulması 2. fıkrasında tanımlanan verilerin bozulması, yok edilmesi, değiştirilmesi, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi 245. maddede tanımlanan banka veya kredi kartının kötüye kullanılması fiilleri ise neticesi hareketten ayrı olan suçlardır[784]. Bu maddeler yönünden uygulanacak kanunda bu özelliklerine göre fiilin tamamlanmış olduğu tarihe göre belirlenecektir.

TCK'nin 135. ve 136. maddesinde düzenlenen suçun soruşturulması ve kovuşturma yapılmasına gelince, TCK'nin 139. maddesi ile bu suçlar ayrık tutulduğundan, şikâyete bağlı değildir; soruşturulması ve kovuşturulması re'sen yapılmalıdır. Suçun kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılması suretiyle işlenmesi ya da belli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde, 5235 sayılı Kanunun 14. maddesi uyarınca mahkemelerin görevlerinin belirlenmesinde ağırlaştırıcı veya hafifletici nedenlerin gözetilmeyeceği hükmüne göre, görevli mahkeme değişmeyecektir[785]. Yukarıda yapılan açıklamalar ışığında bilişim sisteminde kayıtlı bir kişisel verinin elde edilmesi ve kullanılması yoluyla bir suç işlenmesi durumunda

---

[782] Temadi: Sürüp gitme, süregelme, sürme, uzama
[783] Taşkın ve Zengin, *Ceza Hukuku El Kitabı*, s.42
[784] Bu konuda bakınız; Ünver, Yener, (2001), "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", İstanbul: *İÜHFM*, Cilt: LIX Sayı:1-2.
[785] Yaşar ve diğerleri, *Yorumlu-Uygulamalı Türk Ceza Kanunu,* s. 4123 ve 4129

konuyu ilgilendiren TCK maddelerinin hepside Asliye Ceza Mahkemelerinin görev alanı içerisinde düzenlediğinden görevli mahkemenin Asliye Ceza Mahkemesi olduğu yönünde hiçbir şüphe bulunmamaktadır ve şikayete tabi suç olmayıp re'sen kovuşturulması gerekir.

2.8. ZAMANAŞIMI

Ceza hukukunda, devletin cezalandırmaya yetkili organlarının suçu zamanında kovuşturmaması, mahkumiyet hükmünü zamanında yerine getirmemesi, devletin suçu kovuşturma ve cezayı çektirme hakkını ortadan kaldırır[786]. Zamanaşımının "dava zamanaşımı" ve "ceza zamanaşımı" olmak üzere iki türü bulunmaktadır. Dava zamanaşımı, bir suçla ilgili olarak kovuşturma yapılmasına engel olurken; ceza zamanaşımı, kesinleşmiş mahkumiyet hükmünün gereği olan cezanın infazını engellemektedir.[787]. Dava ve ceza zamanaşımı, res'en uygulanır. Bundan şüpheli, sanık ve hükümlü vazgeçemezler (TCK m. 72/2), çünkü zamanaşımı, kamu düzenindendir. Bu demektir ki, taraflar, her zaman zamanaşımı iddiasında bulunabilirler[788]. Hakim, zamanaşımını, res'en, yani kendiliğinden göz önüne almak zorundadır. Hakimin kararı, bir tespit hükmüdür. Tespitin doğru olmadığının, yani hesabın yanlış yapıldığının ileri sürülmesi mümkündür[789].

Dava zamanaşımı Kanunda, tamamlanmış suçlarda suçun işlendiği günden, teşebbüs halinde kalan suçlarda son hareketin yapıldığı günden, zincirleme suçlarda son suçun işlendiği günden başlatılmaktadır (TCK m. 66/6). Öte yandan, kesintisiz suçlarda dava zamanaşımı kesintinin gerçekleştiği anda başlar (TCK m. 66/6)[790]. Dava zaman aşımının kanunda yazılan nedenlerle durması[791] halinde, durma,

---

[786] Hafızoğulları, *Türk Ceza Hukuk Ders Notları*, s.484
[787] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 611.
[788] Hafızoğulları, *Türk Ceza Hukuk Ders Notları*, s.525.
[789] Özgenç, *Türk Ceza Hukuk Genel Hükümler,* s. 752, Hafızoğulları, *Türk Ceza Hukuk Ders Notları*, s.520
[790] Centel ve diğerleri, *Türk Ceza Hukukuna Giriş*, s. 253
[791] "*Dava zamanaşımı süresinin durması veya kesilmesi*
TCK. m.67: Soruşturma ve kovuşturma yapılmasının, izin veya karar alınması veya diğer bir mercide çözülmesi gereken bir meselenin sonucuna bağlı olduğu hallerde, izin veya kararın

zamanaşımı süresini uzatmaz[792]. Örneğin kamu görevlisinin görevi sebebiyle bu suçu işlemesi halinde (*Veri İşleme Memuru*), soruşturma 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre, yetkili merciden soruşturma izni alındıktan sonra yapılması gerekir. Ön soruşturmacının atanmasından soruşturma izni kararının kesinleşmesine kadar zamanaşımı duracaktır[793]. Zamanaşımı kesildiğinde[794], daha önce geçmiş olan süre göz önüne alınmaz. Zamanaşımı süresi, sıfırdan, yeniden işlemeye başlar[795].

İnceleme konusu suç açısından, öncelikle TCK'de düzenlenen maddelere bakmamız gerekmektedir. Buna göre, kişisel veriler ile ilgili düzenlemeler bakımından, 135. madde de düzenlenen verilerin hukuka aykırı olarak kaydedilmesi suçu için altı aydan üç yıla kadar hapis cezası öngörülmüştür. TCK 136. maddesinde düzenlenen suç için ise bir yıldan dörtyıla kadar hapis cezası verileceği yazılıdır. Görüldüğü üzere cezaların üst sınırı beş yılı geçmeyen hapis cezaları olduğu için TCK'nin 66. maddesinin 1. fıkrasının "e" bandi uyarınca sekiz yıllık dava zamanaşımına tabidirler. Yalnız 66. maddenin 3. fıkrasında "Dava zamanaşımı süresinin belirlenmesinde dosyadaki mevcut deliller itibarıyla suçun daha ağır cezayı gerektiren nitelikli hâlleri de göz önünde bulundurulur." düzenlemesi bulunmaktadır. Kişisel verilerin korunmasına ilişkin suçların nitelikleri hallerini düzenleyen 137. madde uyarınca işlem yapılmasını gerektiren durumlarda ceza, 135. madde yönünden dava zamanaşımının belirlediği beş yılı geçmediği için bir değişiklik getirmemektedir. Ne var ki 136. madde de ceza üst sınırı dört yıl olarak belirlenmiştir. 137. madde uyarınca cezanın yarı oranında arttırılması durumunda ceza üst sınırı 6 yıl olacağı için ceza zaman aşımı yönünden 66. maddenin "d" bendi devreye girecek ve ceza zamanaşımı süresi onbeş yıl olacaktır.

---

alınmasına veya meselenin çözümüne veya kanun gereğince hakkında kaçak olduğu hususunda karar verilmiş olan suç faili hakkında bu karar kaldırılıncaya kadar dava zamanaşımı durur"

[792] Hafızoğulları, *Türk Ceza Hukuk Ders Notları*, s.522

[793] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, s. 610.

[794] "Dava zamanaşımı, şüpheli veya sanığın savcı önünde ifadesinin alınması veya sorguya çekilmesi, şüpheli veya sanık hakkında tutuklama kararı verilmesi, suçla ilgili olarak iddianame düzenlenmesi, sanık hakkında mahkumiyet kararı verilmesi hallerinde kesilir.(m. 67/2, a, b, c, d)"

[795] Hafızoğulları, *Türk Ceza Hukuk Ders Notları*, s. 523

Bilişim suçlarının düzenlendiği 243. madde de düzenlenen suçun üst sınırı bir yıl olup nitelikleri halleri dahi beş yıllık dava zamanaşımı süresini aşmadığı için 243. madde için zamanaşımı süresi sekiz yıl olarak devam edecektir. Buna karşın 244. madde açısından dava zamanaşımının tespiti bu kadar kolay değildir. Bu maddenin her bir fıkrası için ayrı inceleme gerekecektir. Buna göre, birinci fıkrada cezalandırılan bir bilişim sisteminin işleyişini engelleyen ve bozan eylemler için beş yıllık bir ceza söz konusudur. Bu suçun nitelikli hali olan üçüncü fıkra uyarınca suça konu eyleme verilecek ceza yarı oranında arttırılacağı için bu halde dava zamanaşımı için uygulanacak madde 66/1-e bendi değil, "d" bendi olacak ve süre onbeş yıl olarak uygulanacaktır. 244. maddenin dördüncü fıkrası ise eylemin yarar doğurması halinde cezanın arttırılacağı düzenlenmiştir. Bu durumda üst sınır altı yıl olarak belirlendiği için bu madde uyarınca açılacak davalarda dava zaman aşımı olarak yine "d" bendi uygulanacak ve süre onbeş yıl olacaktır.

Topluca yapılacak bir değerlendirme sonucunda; eldeki suç tipi bilişim alanında saklanan kişisel verilerin elde edilmesi suretiyle işlenen suçlar olduğuna göre eylemin işleniş şekli dava zamanaşımının belirlenmisi için önem arzetmektedir. Buna göre 244. maddenin dördüncü fıkrasında "işlenen eylemin yarar doğurması durumunda eylem bir başka suçu oluşturmuyorsa" denilerek bir tahdid getirilmiştir. Eylem örneğin bilişim sistemi kullanılarak kişisel verilerden olan sağlık kayıtlarının değiştirilerek kişinin ölümüne ya da sakatlığına neden olmaya ilişkin ise netice itibarı ile başka bir suç oluştuğundan burada örneğin adam öldürme suçunun tabi olduğu dava zamanaşımı süresi uygulanacaktır. Başka suç oluşturmayan ve yarar sağlamaya ilişkin eylemler 244. maddenin dördüncü fıkrası kapsamında kalacağı için onbeş yıllık süreye tabi olacaktır. Yarar sağlama dışında kişisel verilere yönelik tüm fiiller 135 ve 136. maddeler kapsamında kalan eylemler ise beş, 137. madde uyarınca nitelikli hal içinde kalan suçlar için onbeş yıllık dava zamanaşımı uygulanacaktır.

Yukarıda yapılan açıklamaları ceza zamanaşımı yönünden uygulamakta mümkündür. Buna göre ceza zamanaşımını düzenleyen TCK'nin 68. maddesi ceza üst sınırını esas alarak süreleri belirlemiştir. Buna göre 68/1-e bendinde üst sınırı beş yıldan fazla olan hapis cezaları için yirmi yıl, beş yıla kadar olan hapis cezaları için on yıl ceza zamanaşımı süresi vardır. Buna göre 244/4. madde kapsamındaki suçlar

için yirmi yıl, 243, 244/2 ile 135 ve 136. maddeler için on yıl, 137. madde kapsamında suçun nitelikli halleri için ise yine yirmi yıl, 244/1. madde kapsamında kalan eylemler için beş yıllık bir ceza öngörüldüğünden bu suçun nitelikli hali olan üçüncü fıkra uyarınca suça konu eyleme verilecek ceza yarı oranında arttırılacak ve bu halde ceza zamanaşımı yirmi yıl olarak uygulanacaktır.

2.9. MÜEYYİDE

TCK'nin 135. maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak kaydedilmesi suçunun cezası altı aydan üç yıla kadar hapistir. İkinci fıkra hükmü özel bir düzenleme getirmekle birlikte cezada bir değişiklik yapmamakta, birinci fıkra uyarınca cezalandırılacağını belirtmektedir. 136. maddede ise kişisel verilerin hukuka aykırı olarak verilmesi ve ele geçirilmesi düzenlenmiştir. Bu düzenlemeye göre bir kişiye ait kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dörtyıla kadar hapis cezası ile cezalandırılır. Her iki maddede de öngörülen ceza hapis cezası olup, para cezası düzenlenmemiştir. Bu durum kanun koyucunun kişisel verilerin korunmasına karşı hassas olduğu şeklinde yorumlanabilir. Her iki suç için nitelikli halini düzenleyen 137. madde de öngörülen suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi durumunda cezanın yarı oranında arttırılacağı belirtilerek ceza arttırılmıştır.

TCK'nin 243. maddesinde düzenlenen bilişim sistemine girme ve orada kalmaya devam etme suçunun müeyyidesi bir yıla kadar hapis veya adli para cezasıdır. Yani ya para cezasına ya da hapis cezasına hükmedilecektir. Bu fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde cezanın yarı oranına kadar indirileceği belirtilmiştir. Son fıkrada ise, bu fiil nedeniyle sistemin içirdiği verilerin yok olması veya değişmesi durumunda altı aydan iki yıla kadar hapis cezasının verileceği belirtilmiştir. Bu son hal ağırlaştırıcı bir durumdur. İkinci fıkrada belirtilen ceza miktarının yarı oranına kadar indirilmesi halini hakim olayın şartlarına göre takdir edecektir. En çok indirilecek miktar cezanın yarı oranında indirilmesidir.

Sistemi engelleme bozma verileri yok etme veya değiştirme başlıklı 244. maddenin birinci fıkrasında, bir bilişim sisteminin işleyişini engelleyen veya bozan kişiye, bir yıldan beş yıla kadar hapis cezası verileceği, ikinci fıkrasında bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişiye, altı aydan üç yıla kadar hapis cezası verileceği, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek cezanın yarı oranında artırılacağı, son fıkrasında ise, yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunacağı belirtilmiştir.

TCK'de, kişisel verilerin kaydedilmesi suçunu işleyenler hakkında suçun cezası olarak altı aydan üç yıla kadar hapis cezası öngörülmüştür. TCK'nin 140. maddesi gereğince, bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması halinde, bunlara TCK'nin 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır. Kanunda, kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunu işleyenler hakkında suçun cezası olarak bir yıldan dört yıla kadar hapis cezası öngörülmüştür. İlk iki maddede cezanın alt ve üst sınırları belirlenmiş olup, iki sınır arasında cezanın miktarı hakim tarafından TCK'nin 61. maddesindeki hususiyetlere göre belirlenecektir. 244. maddenin 3. fıkrasında cezanın artırım nedeni düzenlenmiş olup, temel ceza kurulduktan sonra bu ceza üzerinden yarı oranında artırım yapılarak cezaya hükmolunacaktır. Her üç fıkranın uygulanmasının söz konusu olduğu bir durum kurgularsak; bir devlet bankasının bilişim sistemine girerek hesabındaki paranın miktarını yükselten birisi, verileri değiştirme nedeniyle ikinci fıkrayı, bir bankanın bilişim sistemine girmek suretiyle 3. fıkra hükmünü, veriyi değiştirme nedeniyle haksız bir çıkar sağladığından 4. fıkrayı ihlal etmiş demektir. Dördüncü fıkrada "yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle" tarzında bir giriş yapıldığından bu fıkra bünyesinde diğer fıkralardaki maddi unsurda mündemiç[796] demektir ve bu

[796] Barut ve Karayol, *Bilişim Suçları*, 236

durumda sadece 4. fıkra uyarınca hüküm kurulacaktır.

Bilişim suçlarına ilişkin maddelerdeki her maddede alt ve üst sınırlar dahilinde tayin edilmiş olan cezalar 61. maddede belirtilen; suçun işleniş biçimi, suçun işlenmesinde kullanılan araçlar, suçun işlendiği zaman ve yer, suçun konusunun önem ve değeri, meydana gelen zarar veya tehlikenin ağırlığı, failin kast veya taksire dayalı kusurunun ağırlığı, failin güttüğü amaç ve saik hususları göz önünde bulundurularak tespit edilecektir. Ancak, burada belirtilen hususlar suçun unsurunu da oluşturuyorsa temel cezanın belirlenmesinde tekrar göz önünde bulundurulmazlar. Bu maddelerde yer alan adli para cezası ilk defa TCK ile getirilen yeni bir uygulamadır. 765 sayılı TCK'de cari olan hafif ve ağır para cezası yeni yasayla ortadan kaldırılmış, cürüm ve kabahat ayırımı da kaldırıldığından buna paralel olarak para cezalarında sistem değişikliğine gidilmiştir.

TCK'nin 52. maddesinde adlî para cezasının, "Beş günden az ve kanunda aksine hüküm bulunmayan hallerde yediyüzotuz günden fazla olmamak üzere belirlenen tam gün sayısının, bir gün karşılığı olarak takdir edilen miktar ile çarpılması suretiyle hesaplanan meblağın hükümlü tarafından Devlet Hazinesine ödenmesinden ibaret olduğu" belirtilmiştir. Hakim, öncelikle 52. maddede alt ve üst sınırı belirlenmiş olan para cezasının ihlal edilen maddedeki suç nedeniyle ne kadar takdir edileceğini belirleyecektir. Bunu belirlerken de suçun işleniş biçimini, suçun işlenmesinde kullanılan araçları, suçun işlendiği zaman ve yeri, suçun konusunun önem ve değerini, meydana gelen zarar veya tehlikenin ağırlığını, failin kast veya taksire dayalı kusurunun ağırlığını, failin güttüğü amaç ve saiki, göz önünde bulunduracaktır (TCK m. 61). Bu belirlemeden sonraki aşama ise, bir gün karşılığı olarak ne miktar paranın takdir edileceğidir. Bu miktar da kişinin ekonomik ve diğer şahsi halleri göz önünde bulundurularak en az yirmi ve en fazla yüz Türk Lirası[797]

[797] Bu ifade 28.01.2004 tarih ve 5083 sayılı Türkiye Cumhuriyeti devletinin para birimi hakkındaki kanun hükümleri dikkate alınarak belirlenmiş olup, bu konuyla ilgili olarak yeni TCK'nin yürürlük ve uygulamasına ilişkin kanunda da düzenleme yer almaktadır. Yılmaz, Zekeriya, "Yeni Türk Ceza Kanununda Para Cezası Uygulaması", *Türkiye Noterler Birliği Hukuk Dergisi*, Sayı:124, 2004, s.74

olacak şekilde hakim tarafından belirlenecektir. Bu belirleme de yapıldıktan sonra bulunan bu iki rakam çarpılarak netice para cezası bulunacaktır.

Mahkeme kararında bu iki adlî para cezasının belirlenmesinde esas alınan tam gün sayısı ile bir gün karşılığı olarak takdir edilen miktar ayrı ayrı gösterilir (md. 52/3). Hakim, ekonomik ve kişisel durumlarını göz önünde bulundurarak, kişiye adlî para cezasını ödemesi için hükmün kesinleşme tarihinden itibaren bir yıldan fazla olmamak üzere süre verebileceği gibi, bu cezanın belirli taksitler halinde ödenmesine de karar verebilir. Taksit süresi iki yılı geçemez ve taksit miktarı dörtten az olamaz. Kararda, taksitlerden birinin zamanında ödenmemesi halinde geri kalan kısmın tamamının tahsil edileceği ve ödenmeyen adlî para cezasının hapse çevrileceği belirtilir (md. 52/4). 243. maddede düzenlenen para ve hapis cezası seçimlik cezalardan olup, hakim tarafından olayın özelliklerine göre birisi takdir edilecektir. 244/4. maddede düzenlenen cezalarda her iki tür cezaya da hükmolunacaktır. 244/4 maddesinde belirtilen para cezasının asgari haddi belirtilmediği için 52/1 maddesi gereğince adli para cezasının beş günden az olamayacağı göz önüne alınarak en az bu kadara hükmolunacaktır.

Müeyyide konusunda üzerinde durulması gereken bir hususda bilişim sahasında çalışan şirketlerinde başvurduğu bir yöntem olan sanık ile anlaşma uygulamasıdır. Bu yöntemin henüz ülkemizde uygulaması olmamakla birlikte Amerika'da uygulanmaktadır. Buna göre siber saldırı yapan kişilerin tespit edilen IP adreslerinden kendilerine ulaşılarak anlaşma yapılmaktadır. Buna göre kişi ya öngörülen cezayı alacak ya da işbirliğine giderek bilgi birikimini bu suçla mücadele eden birimlere aktararak siber suçluların bulunmasına yardım edecektir. Bu konuda FBI tarafından yapılan uygulamaların örnekleri mevcuttur[798].

[798] Mueller, Robert S., "The Cyber Threat Planning for the Way Ahead", http://www.fbi.gov/news/stories/2013/february/the-cyber-threat-planning-for-the-way-ahead/the-cyber-threat-planning-for-the-way-ahead, (Erişim: 21.03.2014)

SONUÇ

Belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade eden kişisel verilerin, kaydedilmesi ve depolanması bilişim teknolojilerinin icadı ve yaygınlaşması ile artık fizik alandan sanal aleme taşınmıştır. Bu gelişme birçok avantajının yanında bağrında oldukça tehlikeli riskleride barındırmaktadır. Bu tehlikenin farkına varılması ile ulusal düzeyde yapılan koruma çalışmalarının uluslararası alana taşınması ile BM ve AB gibi uluslararası kuruluşlar tarafından bir takım düzenlemelere gidilmiştir. Fakat suçun, sürekli gelişme halinde olan teknolojiye olan bağımlılığı nedeni ile değişken yapısına bu düzenlemelerin ayak uydurabildiğini söylemek pek mümkün olmamaktadır. Günlük yaşamın bir parçası haline gelen bilişim teknolojileri vasıtasıyla kişisel verilerimizin her gün siber alemde dolaşımda olduğu düşünülecek olursa bu konuda yapılacak düzenlemelerin nedenli ehemmiyetli olduğu yapılan açıklamalar ile yeterince ortaya konulmuş oldu. Bu konuda bilişim sistemlerinin ilk olarak ortaya çıkmaya başladığı ABD'nin ilk düzenlemeleri yapmış olmasına karşın, ihlal yöntemlerinin sınırsız sayıda olması nedeni ile halen bu ülkede dahi istenilen korumanın sağlanamadığı her gün yaşanan kişisel veri ihlalleri ile görülmektedir.

Kişisel veriler üzerinde yapılan hileli işlemler ile kişisel tatmin, menfaat temini, siber terör, adi suçların bilgisayar yoluyla işlenmesi vb. isimlendirilebilen amaç ne olursa olsun binlerce insan mağdur olmaktadır. Dahası, siber alemde kişisel verilere karşı işlenen suçlar daha kolay hale geldiği için kötü niyetli insanların daha fazla ilgisini çeker hale gelmiştir. Bunun sonucu olarak sadece kişisel verisi ihlal edilen fertler değil, toplum hatta kamunun kendisi zarar görmeye başlamıştır. Meydana gelen zarar manevi olabildiği gibi değeri milyon dolarlarla anılan maddi zararlarda oluşmaktadır. Yargıya yansıyan bu tür ihlallerin aslında var olanın çok az bir kısmı olduğu düşünülecek olursa sorunun bilinenden çok daha büyük olduğu anlaşılmaktadır. Bu durum bizi sonuç olarak teknolojideki hızla yarışamayacak derecede statik bir yapıya sahip olan hukukun düzenleme olarak yeterli kalmadığını göstermektedir. Özellikle Türkiye gibi henüz ayrı bir hukuk dalı haline getirilmeyen ve ceza hukuku açısından ceza kanunu, tazminat yönünden ise özel kanunlara havale edilmiş ülkelerde siber suçlarla mücadele oldukça yetersiz kalmaktadır. Halen bir

tasarı olarak beklemekte olan Kişisel Verilerin Korunması Kanunu'da mevcut hali ile artık ihtiyaçları karşılayacak düzeyde olmayıp, yeniden revize edilmesi gerekmektidir.

Belirttiğimiz gibi kişisel verilerin ihlallerinin artık fizik ortamdan sanal aleme kayması ile bu özel durumun gözetildiği bir kişisel verilerin korunması kanununun acil olarak çıkartılması gerekmektedir. Özellikle TCK'de düzenlenen dolandırıcılık ve hırsızlıkdan başlayarak adam öldürmeye kadar uzanan suç tipleri ile ilgili olarak kalsik suçların siber ortamda işlenmesi halinde ortaya çıkan karmaşanın giderilmesi için daha özel düzenlemeler getirilmelidir. TCK'de bilişim alanındaki kişisel verilerin korunması için, kişisel verilerin korunması bölümündeki iki madde ile bilişim alanında işlenebilecek suçlar için getirilen üç maddelik düzenleme dış dünyadaki suç ve suçlu kapatesine bakılarak yetersiz kaldığını söylemek hiç de zor olmayacaktır. Bu genellemenin yanında çözülmesi gereken sorunları ortaya koyacak olursak;

Öncelikle kişisel verilerin ençok işlem gördüğü bilişim alanı ile ilgili kanuni düzenlemelerin yürürlüğe girmesinde acele edilmelidir.

Veri işleyenin yetkileri ve sorumlulukları net bir şekilde belirlenmelidir.

Kişisel veri sahiplerinin kişisel verilerinin paylışımı konusunda biliçlendirilmesi için gerekli eğitim verilmelidir.

Bilişim sisteminin fail ve mağdur dışında kalan ve araç olarak faydalanılan sistemleri kullanma imkanı sağlayan server vb. yapısal unsurların da sorumluluğu hakkında düzenlemeler yapılmalıdır.

Suçun özel durumu gereği yetkili adli merci, suçun işlendiği yer gibi konular yoruma bırakılmadan, açık ve net düzenlenmelidir.

Bu suç için getirilecek müeyyide hapis ve tazminat dışında suçlunun ıslahı yönünden bilişim sitemleri ile olan ilişkisini düzene koyacak şekilde olmalıdır.

Yukarıda sıralanan bu önlemlerin alınması önleyici mahiyette olacaktır fakat bu tedbirler alınmasa dahi ceza kanununda ve ilgili mevzuatta yer bulan kanuni tanımda belirtilen eylemlerin gerçekleştirilmesiyle suç işlenmiş olacağından faillerin cezalandırılabilirliği oluşacaktır. Ancak ceza hukukunun ikincil nitelikte olan bir hukuk disiplini olduğu unutulmamalıdır. Asıl olan sosyal hayatı suçtan arındıracak caydırıcı önlemlerin alınmasıdır. Bu önlemler alınarak suç işlenmesi engellenebilecek ve sadece bu önlemlerden geçebilmeyi başaran belli sayıdaki olay yargılamaya konu olacaktır. Toplumsal barışa hizmet eden bu önlemlerden de önemlisi bilişim alanının insanlara sunduğu hizmetin kesintisiz ve sağlıklı verilebilmesidir. Artık yaşamsal önem taşır hale gelen bilişim sistemleri ile bu sistemlerin oluşturduğu ağların güvenilirliği ve kesintisiz çalışması sağlanmalı ve bu tür suçlar sonucunda gerçekleşebilecek zararların asgarit düzeyde tutulabilmesi için gerekli çalışmaların yapılması gerekir.

Son yirmi yıllık neslin bilişim teknolojileri ile büyüdüğü dikkate alınacak olursa, teknolojinini suça açık yönlerinin öğrenilmesinin önüne geçilmesi için aileden başlamak üzere okul ve sosyal çevrenin bu konuda biliçlendirilmesinin kanuni düzenlemelerin sürekli güncellenmesinden de önemli olduğu açıktır. Özellikle kişisel verilerin sanal alemde paylaşılması konusunda insanların düşebileceği tuzaklar topluma açıklanarak önleyici güvenlik tedbirlerin alınması hem mağduriyetleri önleyecek, hemde kolluk ve yargının bu konudaki yükünü hafifletecektir. Sanal alemde suç işleme cazibesinin düşürülememesi nedeni ile önleyici tedbirlerin arttırılması felaketin önünü almakta yararlı olacaktır.

Bunun yanında, suçun işlendiği yer ve zaman konusunda ülkeler arası iş birliğine gidilmesi bir zorunluluktur. Bilişim alanı vasıta kılınarak yapılan kişisel veri ihlalleri (günümüz itibari ile fiziki ortamda bu suçun işlenmesi yok denilecek kadar azalmıştır) fizik bir ortam gerektirmediği ve zaman açısından da ülkeler arası saat ve zaman uygulaması farkları nedeni ile uygulanacak hukuk kuralı ile yetki sorunlarının fazlaca görüldüğü bir ceza hukuku alanıdır. Bu suçun çok uluslu olarak işlenmesine zemin hazırlayan yapısı ülkeleri iş birliğine veya ülkelerin yetkisini kabul edecekleri bir üst kuruluşa ihtiyaç hissettirmektedir. Teknik alt yapısı iyi kurulmuş ve teknolojideki değişim hızına ayak uydurarak sürekli yenilenebilen bir birimin,

internetin uluslararası özelliği göz önünde bulundurularak kişi hak ve özgürlüklerini ihlal etmeden ve casusluk vb. gibi uluslararası krizlere yol açmadan denetlenebilir bir faaliyet ile bu konudaki suçların takibi sağlanabilmelidir.

Bilişim teknolojilerinin ve özelliklede internet kullanan kısmının suç alanı olmaktan çıkartılması konusunda, bundan sonra üretilecek cihaz ve yazılımların kişisel verilerin korunması hakkında duyarlı olması sağlanamayacak bir durum değildir. Bilişime ilişkin yazılımların güvenlik açıklarının daha önceki uygulamalardan edinilen tecrübe ile onarılması, kullanıcıya uyaran sesli yada görüntülü uyarıcıların kullanılması vb. uygulamalar geliştirilmesi bilişim teknolojilerinin yapabilecekleri arasında bulunmakatadır. Bilişim teknolojisi kullanıcılarını kötü niyetli kişilerin eline bırakmak yerine sistemi baştan önleyici tedbirler ile donatmak daha yararlı olacaktır. Bu konuda yararlanılabilecek kişilerin başında suçlunun bizzat kendisi gelmeketedir. Güvenlik açığını en iyi bilen ve bu konuya yatkın kişilerin bilgi ve tecrübelerinden yararlanmak bir adım önde gitmek anlamında olacaktır. Bu konuda Avrupa ve Amerika'da uygulamalar bulunmaktadır.

Çalışmanın genelinden de anlaşılacağı üzere bilişim ve bilişim araçları kullanılarak işlenen kişisel verilere yönelik suçlar ile mücadele alanında, ülkemizde elbet umut verici çalışmalar ve kısmi düzenlemeler vardır. Ancak ülkemizdeki yapı, bilişim suçlarının etkilerinin sebep olabileceği zararların ve bu alandaki hızlı gelişmenin gerisindedir. Bu sebeple hukuki, idari, teknik ve eğitsel açısından çok ciddi düzenleme ve çalışmalara ihtiyaç vardır. Bu çalışmalar kişisel verilerin korunması alanında güven ortamını sağlayacağı gibi dünya çapında Türk adalet sisteminin etkinliği açısından da önem taşımaktadır.

KAYNAKLAR

BASILI KAYNAKLAR:

Akbulut, Berrin Bozdoğan, (1999), *Türk Ceza Hukukunda Bilişim Suçları*, Yayımlanmamış Doktora Tezi, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Akbulut, Berrin Bozdoğan,(2000), "Bilişim Suçları", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi,* Cilt:8, Sayı: 1-2.

Akbulut, Berrin Bozdoğan, (2003), "Bilişim Suçlarının Tanımı, Tasnifi, Avrupa Hukukundaki Yeri", *Bilişim Suçları ile Mücadele Semineri,* Ankara: Jandarma Okullar Komutanlığı Yayınları.

Akdağ, Hale, (2010), *Türk Ceza Kanunu Kapsamın da Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Akdeniz, Yaman, (2004), "Çağdaş İnternet Yönetimi", *Güncel Hukuk Dergisi*, İstanbul, Sayı: Haziran 2004,

Akdeniz, Yaman, (2003), *Internet Governance: Towards the Modernization of Policy Making Process in Turkey*, İstanbul: TBV Series:1, Papatya Publication Education.

Akipek Öcal, Şebnem, (2011), *Medeni Hukuk -I-,* Eskişehir: Anadolu Üniversitesi Yayınları.

Aksoy, Hüseyin Can, (2010), *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, 1. Baskı, Ankara: Seçkin Yayınevi.

Aksoy, Eylem, (2002), "Avrupa Konseyi Siber Suçluluk Sözleşmesi", İstanbul: *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi,* Sayı 1.

Aras, Ümit Yaşar, (2010), *İnsan Hakları Temelinde Özel Hayat Hakkının Ulusal ve Uluslararası Alanda Uygulamaları,* Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü.

Arpacı, Abdulkadir, (2000), *Kişiler Hukuku (Gerçek Kişiler)*, İstanbul: Beta Yayınları.

Arslan, Çetin ve Azizağaoğlu, Bahattin, (2004), *Yeni Türk Ceza Kanunu Şerhi*, Ankara: Asil Yayın Dağıtım.

Artuk, Mehmet Emin; Gökçen, Ahmet ve Yenidünya, Ahmet Caner, (2002), *Ceza Hukuku Genel Hükümler*, Ankara: Adalet Yayınevi.

Artuk, Mehmet Emin; Gökçen, Ahmet ve Yenidünya, Ahmet Caner, (2007), *5237 Sayılı Kanuna Göre Hazırlanmış Ceza Hukuku Özel Hükümler,* Ankara: Turhan Yayınevi.

Artuk, Mehmet Emin; Gökçen, Ahmet ve Yenidünya, Ahmet Caner, (2009), *Türk Ceza Kanunu Şerhi*, Ankara: Turhan Kitapevi, Cilt: 5.

Ayan, Mehmet ve Ayan, Nurşen, (2011), *Kişiler Hukuku*, Konya: Mimoza Yayınevi.

Aydın, Emin, (1992), *Bilişim Suçları ve Hukukuna Giriş*, Ankara: Doruk Yayınları.

Balık, Hasan Hüseyin (Ed.), (2003), *Temel Bilgisayar Teknolojileri Kullanımı*, Elazığ: Fırat Üniversitesi Basım Evi.

Barut, Muharrem ve Karayol, Muharrem, (2005), *Bilişim Suçları*, Yayımlanmamış Proje Ödevi, Ankara: TODAİE.

Başalp, Nilgün, (2004), *Kişisel Verilerin Korunması ve Saklanması*, Ankara: Yetkin Yayınevi.

Başalp, Nilgün, (2004), "Kişisel Verilerin Korunması ve İnternet", *İnternet ve Hukuk Dergisi*, Derleyen: Yeşim M. Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Başbakanlık Dış Ticaret Müsteşarlığı Avrupa Birliği Genel Müdürlüğü, (2002), *Avrupa Birliği ve Türkiye*, Ankara: Doğuş Matbaacılık.

Benneth, J. Colin, (1992), *Regulating Privacy: Data Protection and Public Policy in Europe and United States*, London: Cornell University Press.

Boz, Ahmet, (2014), *Kişisel Verilerin Korunması; Türkiye, ABD ve AB Örnekleri*, Yayımlanmamış Yüksek Lisans Tezi, Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü,

Bozlak, Ayhan, (2013), *Avrupa İnsan Hakları Mahkemesi Kararları Çerçevesinde Türk Ceza Hukukunda Özel Hayatın Korunması*, Yayımlanmamış Doktora Tezi, Ankara: Polis Akademisi, Güvenlik Bilimleri Enstitüsü.

Carter, David, L, (1995), "Computer Crime Categories How Techno-criminals Operate", *FBI Law Enforcement Bulletin*, v. 64.

Casey, James E., (2000), *Digital Evidence and Computer Crime,* London: Academic Press

Cate, Fred H., *Privacy in the Information Age,* (1997), Washington, D.C.: Brookings Institution Press.

Centel, Nur ve Zafer, Hamide, (2011), *Ceza Muhakemesi Hukuku*, 8. Bası, İstanbul: Beta Yayınları.

Centel, Nur; Zafer, Hamide ve Çakmut, Özlem, (2011), *Türk Ceza Hukukuna Giriş*, 7. Baskı, İstanbul: Beta Yayınları.

Cerrah, İbrahim, (2002), "Bilişim Teknolojileri ve Etik: Bilişim Teknolojilerinin Güvenlik Hizmetlerinde Kullanımının 'Etik Boyutu' ve 'Sosyal' Sonuçları", *Polis Bilimleri Dergisi*. Ankara, Cilt: 4, Sayı: 1-2.

Çeken, Hüseyin, (2003), *Council of Europe's Convention 2001 on Cybercrimes and Turkey*, Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi Avrupa Birliği Enstitüsü.

Cihan, Erol ve Yenisey Feridun, (1997), *Ceza Muhakemesi Hukuku,* İstanbul: Beta Yayınları.

Civelek, Dilek Yüksel, (2011), *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi,* Yayımlanmamış Uzmanlık Tezi, Ankara: Devlet Planlama Teşkilatı.

Çölkesen, Rifat ve Ören Bülent, (2003), *Bilgisayar Haberleşmesi ve Ağ Teknolojileri*, İstanbul: Papatya Yayınevi.

Danışman**,** Ahmet, (1991), *Ceza Hukuku Açısından Özel Hayatın Korunması***,** 1. Baskı, Konya, Selçuk Üniversitesi Yayınları.

Değirmenci, Olgun, (2002), *Bilişim Suçları*, Yayımlanmamış Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Demir, Vedat. (1994), "Türkiye'de Özel Radyo ve Televizyonların Çıkışı ve Bu Konuda Devlet Tekelinin Kalkması", İstanbul: *Marmara İletişim Dergisi*. Sayı: 7

Demirbaş, Timur, (2005), *Ceza Hukuku Genel Hükümler,* 9. Baskı, İstanbul: Seçkin Yayınevi.

Dinç, Engin, (2006), *Kişisel Verilerin Korunmasında Uluslar Arası Düzenlemeler ve Türkiye'nin Durumu,* Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır: Dicle Üniversitesi, Sosyal Bilimler Enstitüsü.

Doğan, Koray, (2005), "Bilişim Suçları ve Yeni Türk Ceza Kanunu", *Hukuk ve Adalet Eleştirel Hukuk Dergisi,* Yıl:2 Sayı: 6-7.

Dokurer, Semih, (2003), "Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri", *Polis Dergisi*, Sayı: 37.

Dönmezer**,** Sulhi, (2004), *Kişilere ve Mala Karşı Cürümler*,17. Bası, İstanbul: Beta Yayınları.

Dönmezer, Sulhi ve Erman, Sahir, (1997), *Nazari ve Tatbiki Ceza Hukuku*, Cilt: I ve II, 12. Baskı, İstanbul: Beta Yayınları.

Dural, Mustafa ve Öğüz, Tufan, (2006), *Türk Özel Hukuku*, *Kişiler Hukuku*, Cilt: 2, 8. Bası, İstanbul: Filiz Kitapevi.

Dülger, Murat Volkan, (2004), *Bilişim Suçları*, 1. Baskı, Ankara: Seçkin Yayınevi.

Dülger, Murat Volkan, (2005), "Bilişim Suçları ve Yeni Türk Ceza Kanunu", İstanbul: *Kazancı Hukuk, İşletme ve Maliye Bilimleri Dergisi*. İstanbul, Sayı:5, Ocak 2005

Dülger, Murat Volkan, (2004), "Bilişim Suçlarına İlişkin Düzenlemelerin Eleştirisi", Türk Ceza Kanunu Tasarısı: İstanbul Barosu-Türk Ceza Hukuku Derneği Toplantısı (10.07.2004): Kurumsal Raporlar-Toplantılara Sunulan Raporlar-Bilimsel Raporlar, İstanbul: İstanbul Barosu-Galatasaray Üniversitesi-Türk Ceza Hukuku Derneği Ortak Yayını.

Dülger, Murat Volkan, *Bilişim Suçları İle Mücadele,* 2. Polis Bilişim Sempozyumunda Sunulan Bildiri, (14-15.04.2005) Ankara.

Ekici Şahin, Meral, (2012), *Ceza Hukukunda Rıza*, İstanbul: Oniki Levha Yayıncılık.

Erem, Faruk; Danışman, Ahmet ve Artuk, Mehmet Emin, (1997), *Ceza Hukuku Genel Hükümleri;* 14. bası, Ankara: Seçkin Yayınevi.

Erdağ, Ali İhsan, (2004), *5237 sayılı TCK Ders Notlan, Bilişim Alanında Suçlar*, Ankara: Hakim-Savcı Eğitim Merkezi.

Erdem, Mustafa Ruhan, "Yeni TCK'de Faillik ve Suç Ortaklığı", *Hukuki Perspektifler Dergisi*, Sayı: 2005/5.

Erdönmez, Erhan, (2002), *Investigation Of Computer Crimes*, Thesis Prepared For The Degree Of Master Of Science, University Of North Texas.

Ergül, Ozan, (1998), "Özel Yaşamın Gizliliği Hakkı ve Korunması", Yayımlanmamış Yüksek Lisans Tezi, Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Ergün, İsmail, (2008), *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Ankara: Turhan Kitapevi.

Ergün, İsmail, (2005), "Yeni Türk Ceza Kanunu'nda Bilişim Suçları", *2. Polis Bilişim Sempozyumunda Sunulan Bildiri*, Ankara.

Erkan, Boğaç ve Songür, Murat, (1999), *Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü,* Ankara: Hacettepe-Taş Yayınları,

Erksen, Roland, (1999), *Uluslararası Bilgisayar Ağlarında Yayınlanan Suç İçerikli Bilgilerden Doğan Cezai Sorumluluk*, (çev: Barış, Erman), Yayımlanmamış Yüksek Lisans Seminer Ödevi, İstanbul, 1999.

Erman, Barış R., (2001), Alman Hukukunda İnternetten Kaynaklanan Ceza Sorumluluğu, *İÜHFD*, Cilt: 59, Sayı: 1-2.

Ersoy, Uğur, (2009), *Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi, Sosyal Bilimler Enstitüsü.

Etter, Barbara, (2002), Leadership in the Hi-Tech Crime Environment, Australasian Cemre For Policing Research To 2/2002 Pelp At The Aipm Sydney.

Fındıklı, Remzi ve Bilgiç, Veysel, (2006), *İdare Hukuku,* Ankara: Anadolu Yayıncılık.

Gürbüz, Meral, (2015), "Özel Hayatın Gizliliği Bağlamında Kişisel Sağlık Verilerinin Korunması", *Legal Hukuk Dergisi,* Cilt: 13, Sayı: 149

Güney, Niyazi; Özdemir, Kenan ve Balo, Yusuf Solmaz, (2004), *Yeni Türk Ceza Kanunu,* Ankara: Adil Yayınevi.

Hafızoğulları, Zeki ve Özmen, Muharrem, (2012), *Türk Ceza Hukuku Genel Hükümler*, 5. Bası, Ankara: Us-a Yayıncılık.

Hakeri, Hakan, "İhmali Suçlar", *Ceza Hukuk Dergisi*, Yıl:2, 2007/4

Hakeri, Hakan ve Ünver, Yener, (2008), *Ceza Muhakemesi Hukuku*, Ankara, Adalet Yayınevi, 2. Baskı.

Harris, David John, (2004), *Cases and Materials on International Law,* 6th Edition, London Sweet & Maxwell.

Hatemi, Hüseyin, (1976), *Hukuka ve Ahlaka Aykırılık Kavramı ve Sonuçları*, İstanbul: Sulhi Garan Matbaası.

Helvacı, Serap*,* (2001), *Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar*, İstanbul: Beta Yayınları.

Helvacıoğlu, Aslı Deniz, (2004), "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi" İstanbul: *İnternet ve Hukuk Dergisi*, İstanbul Bilgi Üniversitesi Yayınları.

İçel, Kayıhan, (1972), *Suçların İçtimai, Genel Bilgiler - Fikrî İçtima - Müteselsil Suçlar - Görünüşte İçtima*, İstanbul: Sermet Matbaası.

İçel, Kayıhan, (2001), "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", *İÜHFD,* Cilt: LIX, Sayı: 1-2.

İçel, Kayıhan ve Donay, Süheyl, (1999), *Karşılaştırmalı ve Uygulamalı Ceza Hukuku*, İstanbul: Beta Yayınları.

İçel, Kayıhan; Sokullu, Akıncı, Füsun; Özgenç, İzzet; Sözüer, Adem; Mahmutoğlu, Fatih Selami ve Ünver, Yener, (2004), *Suç teorisi. Suç Kavramına İlişkin Genel Bilgiler, Suçun Yapısal Unsurları, Suçun Özel Oluşum Biçimleri*, 2. Kitap, Yeniden Gözden Geçirilmiş 3. Bası, İstanbul: Beta Yayınları.

İçel, Kayıhan ve Ünver, Yener, (2009), *Kitle Haberleşme Hukuku: Basın-Radyo-Televizyon-Sinema-Video-İnternet,*9. Bası, İstanbul: Beta Yayınları,

Jascheck, Hans Hainrich, (1989), *Almanya Federal Cumhuriyeti Ceza hukukuna Giriş* (Çeviri: Feridun Yenisey; Kayıhan, İçel ve Köksal Bayraktar, Türk Ceza hukukuna İlişkin Açıklamalar), İstanbul, Beta Yayınları.

Johnson, David R. ve Post, David G. (1997), "And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law", *Coordinating the Internet*, MIT Press, Massachusetts, USA.

Karagülmez, Ali, (2005), *Bilişim Suçları ve Soruşturmu Kovuşturma Evreleri*, 1. Baskı, Ankara, Seçkin Yayınevi.

Karasu, Sinem, (2009), *Hekimin Sır Saklama yükümlülüğü,* İstanbul, Vedat Kitapçılık

Kataoğlu, Tuğrul*,* (2008), *Ceza Kanunlarının Zaman Yönünden Uygulanması*, 1. Baskı, Ankara: Seçkin Yayınevi.

Kataoğlu, Tuğrul, (2003), *Ceza Hukukunda Hukuka Aykırılık*, 1. Baskı, Ankara: Seçkin Yayınevi.

Kaya, Cemil, (2011). *Assessing the Transfer of Personal Data in the European Union,* 1. Baskı, İstanbul: On İki Levha Yayıncılık.

Kaya, Cemil, (2011), "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", *İÜHFD,* Cilt: 69, Sayı: 1-2.

Kaya, Cemil, (2005), *İdare Hukukunda Bilgi Edinme Hakkı*, Ankara: Seçkin Yayınevi.

Keser Berber, Leyla; Ülgü, Mahir M ve Er Cüneyd, (2009), *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*, 1. Baskı, İstanbul: Karakter Color AŞ.

Keskin, Serap, (2001),"Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", *İÜHFD*, Sayı 1-2,

Ketizmen, Muammer, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, 1. Baskı, Ankara: Adalet Yayınevi.

Kılıçoğlu, Ahmet*; (*1993), *Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk*, 2. Baskı, Ankara: Ankara Üniversitesi Basımevi.

Kızıltan, Mehmet Burak, (2007), *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, Yayımlanmamış Yüksek Lisans Tezi, İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Koca, Mahmut, (2003), "*Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku"*, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, Ankara, Beta Yayınları, Cilt: 3.

Koca**,** Mahmut, (2009), "Hukukumuzda TCK'nin 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", *Bilişim Hukuku Konferansı,* T.C. Yargıtay Başkanlığı, (09-10.10.2008) Ankara.

Koca, Mahmut ve Üzülmez, İlhan, (2011), *Türk Ceza Hukuku Genel Hükümler*, 5. Baskı, Ankara: Seçkin Yayınevi.

Krasner, Stephen D. (1996), "Compromising Westphalia", *International Security*, Winter 1995/96. Volume: 20, Number: 3, The MIT Press.

Kunter, Nurullah ve Yenisey, Feridun, (2000), *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, 11. Bası, İstanbul: Beta Yayınları.

Kurt, Levent*,* (2005), *Bilişim Suçları ve Türk Ceza Kanunudaki Uygulaması*, Ankara: Seçkin Yayınları.

Küzeci, Elif, (2010), *Kişisel Verilerin Korunması*, Ankara: Turhan Kitabevi.

Loren, D. ve Mercer, M.F.S., (2004), "Computer Forensic Characteristics and Preservation of Digital Evidence", *FBI Law Enforcement Bulletin*, Vol.73, Number 3.

Malkoç*,* İsmail*,* (2007), *Açıklamalı-İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu*, Ankara: Malkoç Kitapevi, Cilt: I.

Memiş, Tekin, (2001), "İki Uluslararası Sempozyum ve Bir Özet", *Erzincan: Ankara Üniversitesi Erzincan Hukuk Fakültesi Dergisi*, Cilt: V.

Meran, Necati, (2008), *Sahtecilik-Mal Varlığı-Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar,* 2. Baskı, Ankara: Yetkin Yayınevi.

Millard, Christopher, Hon, W. Kuan, "Defining Personal Data in E-Social Science", London, *Information, Communication & Society Journal*, Volume: 15, Issue: 1, February 2012.

Miller, Atthur B, (1971), *The Assault on Privacy: Computers, Data Banks and Dossiers*, The University of Michigan Pres, 2. Edition.

Mungo, Paul ve Clough, Bryan, (1999), *Sıfıra Doğru Veri Suçları ve Bilgisayar Yeraltı Dünyası* (Çev: Emel Kurma), İstanbul: İletişim Yayınları.

Nuhoğlu, Ayşe; Yenisey, Feridun ve Nurullah, Kunter, *Muhakeme Hukuku dalı olarak Ceza Muhakemesi Hukuku*, 17. Baskı, İstanbul: Beta Yayınları.

Önder, Ayhan (1992), *Ceza Hukuk Genel Hükümleri,* Cilt: II-III, İstanbul: Filiz Kitapevi.

Özbek, Veli Özer, (2005), *TCK İzmir Şerhi*, Ankara: Seçkin Yayınevi.

Özbek, Veli Özer; Kanbur, Mehmet Nihat; Doğan, Koray; Bacaksız, Pınar ve Tepe, İlker, (2010), *Türk Ceza Hukuku Genel Hükümler*, Ankara: Seçkin Yayınevi.

Özbek, Veli Özer; Kanbur, Mehmet Nihat; Doğan, Koray; Bacaksız, Pınar ve Tepe, İlker, (2011), *Türk Ceza Hukuku Özel Hükümler*, Ankara: Seçkin Yayınevi.

Özcan, Mehmet, (2004), "Siber Terörizm ve Ulusal Güvenlik", *İnternet ve Hukuk*, Derleyen: Yeşim M. Atamer, İstanbul: İstanbul Bilgi Üniversitesi Yayını.

Özdemir, Hayrunnisa, (2009), *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması*, Ankara: Seçkin Yayınevi.

Özdemir, Muammer, (2000), "Suç ve Ceza", *PC Magazine Türkiye*, Sayı: Mayıs 2000.

Özel, Cevat, (2001), "Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", *İstanbul Barosu Dergisi*, İstanbul, Cilt: 75, Sayı: Eylül 2001

Özel, Sibel; (2004), *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, Ankara: Seçkin Yayınevi.

Özgenç, İzzet, (2012), *Türk Ceza Hukuku, Genel Hükümler*, 7. Bası, Ankara: Seçkin Yayınevi.

Özgenç, İzzet, (2002), *Ekonomik Çıkar Amacıyla İşlenen Suçlar*, Ankara: Seçkin Yayınevi.

Özgenç, İzzet: *Düşünceyi Açıklama Hürriyeti ve Ceza Hukuk*, 75. Yılında Cumhuriyet ve Hukuk Sempozyumu, Diyarbakır, 22-23.10.1998.

Özgenç, İzzet ve Şahin, Cumhur, (2000), *Uygulamalı Ceza Hukuku*, 3. Bası, Ankara: Seçkin Yayınevi.

Özsunay, Ergün, (1982), *Medeni Hukukumuzda Tüzel Kişiler (Tüzel Kişilerin Genel Teorisi- Dernekler-Vakıflar)*, Gözden Geçirilmiş 5. Bası, İstanbul: İÜHF Yayınları, Sayı: 549.

Öztan, Bilge; (2000), *Medeni Hukukun Temel Kavramları*, Ankara: Turhan Kitabevi.

Öztan, Bilge; (2001), *Şahsın Hukuku, Hakiki Şahıslar*, Ankara: Turhan Kitabevi.

Öztürk, Bahri; Tezcan, Durmuş; Erdem, Mustafa Ruhan; Sırma, Özge; Saygılar, Yasemin F.; Alan, Esra, (2010), *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, Ankara, Seçkin Yayınevi.

Parlar, Ali ve Hatipoğlu, Muzaffer, (2010), *Türk Ceza Kanunu Yorumu*, Ankara: Seçkin Yayınevi.

Prisella, M Regan, (1995), *Legislating Privacy. Technology, Social Values, and Public Polity*, the University Of North Carolina Press.

Riddick, Frank A, (2003), "American Medical Association, Council on Ethical and Judicial Affairs". Code of Medical Ethics, Current Opinions with Annotations.", *The Oschner Journal.*

Robinson, Neil; Graux, Hans; Botterman, Maarten ve Valeri, Lorenzo, (2009), *Review of the European Data Protection Directive*, United Kingdom: Published by the Rand Corporation.

Sağlam, Fazıl, *Temel Hakların Sınırlandırılması ve Özü*, (1982), Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını.

Sancar, Türkan Yalçın, (1995), *Müteselsil Suç*, Ankara: Seçkin Yayınevi.

Sarıhan, Tan Deniz, (1998), *Herkes İçin İnternet,* İstanbul: Desnet Yayınları.

Savaş, Abdurrahman, (2005), *İnternet Ortamında Yapılan Sözleşmeler,* Yayımlanmamış Doktora Tezi, Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.

Schjolberg, Stein, *Cyber Crime,* http://www.mosstingrett.no/info/legal.html, 31.08.2006; Aktaran: Demircan, Tunç, (2007), *Bilişim Alanında Suçlar***,** Yayımlanmamış yüksek lisans tezi, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Sınar, Hasan, (2001), *İnternet ve Ceza Hukuku,* İstanbul: Beta Yayınları.

Sırabaşı, Volkan; (2003), *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz,* Ankara: Adalet Yayınevi.

Singleton, Susan, (1998), *Data Protection*, *The New Law*, Jordans, Published by Bristol.

Sokullu Akıncı, Füsun, (2001), "Avrupa Konseyi Siber Suç Sözleşmesi'nde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve İnternette Çocuk Pornografisi", *İÜHFD*, Cilt: LIX Sayı:1-2.

Soyaslan, Doğan, (2005), *Ceza Hukuk Özel Hükümler*, 3. bası, Ankara: Yetkin Yayınları.

Soyaslan, Doğan, (2012), *Ceza Hukuk Genel Hükümler*, 4. bası, Ankara: Yetkin Yayınları.

Soykan, Cavidan, (2006), *Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı: Özel Hayatın Gizliliği & İfade Özgürlüğü*, Ankara, Ankara Üniversitesi Siyasal Bilgiler Fakültesi İnsan Hakları Merkezi Çalışma Metinleri.

Soysal, Tamer, (2007), Elektronik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk, *Ankara Barosu Dergisi*, Cilt: Kış 2007, Sayı: 1.

Sözüer, Adem, (1994), *Suça Teşebbüs,* İstanbul: Kazancı Yayınları,

Spiros, Simitis, *Reviewing Privacy In an Information Society,* Pennsylvania: University of Pennsylvania Law Review, 1986 -1987, Vol. 135, No. 3 (March, 1987).

Study on legal and Regulatory Aspects of e-health: Legally e-Health, Deliverable 2, (2006), Processing Medical Data: Data Protection, Confidentiality and Security,

Şen, Ersan, (2006), *Türk Ceza Kanunu Yorumu*, Ankara: Vedat Kitapçılık.

Şen, Ersan, "Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi", *İstanbul Barosu Dergisi*, Cilt: 2009/3, Sayı: Mayıs-Haziran, Cilt:83,

Şen, Bilal, *Bilişim Suçları ile Mücadele,* (2003), Yayımlanmamış Ödev, Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü.

Şimşek, Oğuz, (2008), *Anayasa Hukukunda Kişisel Verilerin Korunması,* İstanbul, Bata Yayınları.

Tan, Mehmet, *Türk Ceza Kanunu Genel Hükümler*, (2011), 1. Baskı, Ankara: Seçkin Yayınevi.

Tandoğan, Haluk*, "Şahsiyetin Akit Dışı İhlallere Karşı Korunmasının İşleyiş Tarzı ve Basın Yoluyla Olan İhlallere Karşı Özel Hayatın Korunması", AÜHFD*. Yıl. 1963, Cilt: XX, sayı.1-4.

Tanrıkulu, Cengiz, "Bilişim Hukuku ile İlgili Alman Federal Yüksek Mahkemesinden Örnek Kararlar", *Bilişim Hukuku Konferansı* 9-10.10.2008, Yargıtay Bilişim Sempozyumu, Ankara: Yargıtay Yayınları.

Tanyol, Tuğrul, (2002), "Anarşizm ve İnternet", Cogito İnternet: Üçüncü Devrim, Yapı Kredi Yayınları, Sayı: 30, Yıl: Kış 2002.

Taşdemir, Kubilay, (2009) *Bilişim-Banka veya Kredi Kartlarının Kötüye Kullanılması-Dolandırıcılık Suçları*, Ankara: Turhan Kitapevi.

Taşkın, Alim, (1991-1992), "Tüzel Kişilerin Kişilik Haklarının Korunması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Cilt.42, Sayı: 1991-1992.

Taşkın, Ahmet ve Zengin, İbrahim, (2004), *Ceza Hukuku El Kitabı*, Ankara: Savaş Yayınevi.

Taşkın, Şaban Cankat, (2008), *Bilişim Suçları,* Bursa: Beta Yayınları,

Tavukçuoğlu, Cengiz, (2004), *Bilişim Terimleri Sözlüğü*, Ankara: Asil Yayın Dağıtım.

Tezcan, Durmuş, Erdem, M. Ruhan, Sancakdar, Oguz, (2004), *Avrupa İnsan Haklan Sözleşmesi Işığında Türkiye'nin İnsan Haklan Sorunu*, Ankara: Seçkin Yayınevi.

Thomas, Douglas and Loader, Brain D., (2000), *Introduction – Cyber crime: Law Enforcement, Security and Surveillance in the Information age*. in B. & B. Loader (Eds.), London: Routledge

Toroslu, Nevzat, (1970), *Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu*, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayını.

Toroslu, Nevzat, (2008), *Ceza Hukuku, Genel Kısım*, 12. Baskı, Ankara: Savaş Yayınevi.

Tosun, Öztekin, (1977), "Özel Hayatın Gizliliğini İhlal Suçları"*, Değişen Toplum ve Ceza Hukuku Karşısında TCK'nin 50. Yılı ve Geleceği Sempozyumu*, İstanbul, 22-26 Mart 1976, İstanbul Üniversitesi Hukuk Fakültesi Yayınları No: 2270.

Tulum, İsmail, (2006), *Bilişim Suçları ile Mücadele,* Yayımlanmamış Yüksek Lisans Tezi, Isparta: Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü.

Türkiye Bilişim Derneği, Kamu Bilişimi Platformu 2. Çalışma Grubu Nihai Raporu, (2008), *Kişisel Verilerin Korunması,* Ankara: TBD/Kamu-BDB/2008-CG2.

Uygun, Murat, (2010), *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması,* Yayımlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

Ünver, Yener, (2001), "Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", *İÜHFD*, Cilt: LIX Sayı:1-2.

Ünver, Yener, (2003), *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, Ankara: Seçkin Yayınevi.

Üzeltürk, Sultan, (2004), *Özel Hayatın Gizliliği Hakkı*, İstanbul: Beta Yayınları.

Üzülmez, İlhan, "Yeni Ceza Kanunun Sisteminde Cezanın Belirlenmesi ve Bireyselleştirilmesi", *EÜHFD*, Cilt. II, Sayı: 2007/1-2,

Wacks, Reymond, (1989), *Personal Information: Privacy And Law,* Oxford: Clarendon Pres.

Westin, Alan F, (1970), *Privacy and Freedom*, London, Bodley Head.

Wong, Rebecca. (2007). "Data Protection Online: Alternative Approaches to Sensitive Data", *Journal of International Commercial Law and Journal of International Commercial Law and Technology,* Vol. 2, Issue 1, Law Department, University of Sheffield

Yazıcıoğlu, Yılmaz, (2004), *Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile*, İstanbul: Alfa Basım Yayım Dağıtım.

Yazıcıoğlu, Yılmaz, "Hukukumuzda TCK'nin 243. maddesi kapsamında Bilişim Sistemine Girme Eylemi", *Bilişim Hukuk Konferansı Kitabı,* Ankara: Yargıtay Başkanlığı, (09-10.10.2008)

Yardımcı, Murat, (2009), *Türk Hukukunda İletişimin Denetlenmesi*, Ankara: Seçkin Yayınevi.

Yargıtay Başkanlığı, (2008), *Bilişim Hukuku Konferansı*, Ankara: Yargıtay Basımevi.

Yaşar, Osman; Gökçen, Hasan Tahsin ve Artuç, Mustafa, (2010), *Yorumlu-Uygulamalı Türk Ceza Kanunu*, Ankara: Adalet yayınevi.

Yarsuvat, Duygun, (1999), *Tüzel Kişilerin Ceza Sorumluluğu*, *Prof.Dr. Sahir Erman'a Armağan*, İstanbul: Beta Yayınları.

Yaycı, Esra, (2007), *Bilişim Suçlar,* Yayımlanmamış Yüksek Lisans Tezi, Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü,

Yenidünya, Caner ve Olgun Değirmenci, (2003), *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, İstanbul: Legal Yayıncılık.

Yıldırım, Mustafa Fadıl, (2003), "Bilgisayar Programlarında Akdi ve Teknik Kullanım Sınırlamaları ve Kullanıcının Hukuki Konumu", *EÜHFD*, Cilt: VII, Sayı 1-2.

Yılmaz, Zekeriya, (2004), "Yeni Türk Ceza Kanununda Para Cezası Uygulaması", *Türkiye Noterler Birliği Hukuk Dergisi*, Sayı:124,

Zevkliler, Aydın; Acabey, M. Beşir ve Gökyayla, Emre, (1999), *Medeni Hukuk*, 6. Baskı, Ankara: Seçkin Yayınevi.

İNTERNET KAYNAKLARI:

Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü İnsan Hakları Daire Başkanlığı, "Avrupa İnsan Hakları Sözleşmesi", http://www.inhak.adalet.gov.tr/temel/aihs.pdf. (E.T: 17.02.2014)

Adalet Bakanlığı Kanunlar Genel Müdürlüğü, "Tasarı Aşamaları", http://www.kgm.adalet.gov.tr/Tasariasamalari/Tbmmkms/Tbmmkom/kisiselveriler.pdf, (E.T: 24.05.2015)

Ahi, M. Gökhan**, "**Doğal olmayan yoldan yapılan cinsel davranışlar ne demektir?", http://www.bilisimhukuk.com/2009/08/"dogal-olmayan-yoldan-yapilan-cinsel-davranislar"-ne-demektir/2/, (E.T: 16.01.2010)

Aktif Haber, "Müzik Videoları Youtube'dan Kaldırılıyor", http://www.aktifhaber .com/muzik-videolari-youtubedan-kaldiriliyor-923286h.htm (ET: 08.05.2014)

Ankara Barosu, "Avrupa İçin Bir Anaysa Oluşturan Antlaşma", http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/until2007/ avrupaicin.pdf, (E.T: 11.02.2014)

Ankara Barosu, "Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı", http://www.ankarabarosu.org.tr/Siteler/1940-2010/Kitaplar/pdf/a/sibersuclar. pdf. (E.T: 19.02.2014)

Ankara Barosu, "Avrupa İnsan Hakları Evrensel Bildirisi", http://www.ankarabarosu .org.tr/Siteler/abihm.org/iheb.htm. (E.T: 17.02.2014)

Aslan, M. Yasin,"Türk Hukukunda Tüzel Kişilerin Ceza Sorumluluğu*", Ankara Barosu Dergisi,* http://www.ankarabarosu.org.tr/siteler/ankarabarosu/ tekmakale/2010-2/2010-2-aslan.pdf, (E.T: 13.01.2013)

Avrupa Birliği Bakanlığı, "2003 Tarihli Katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_ Ort_ Belg_2003.pdf. (E.T: 20.05.2011)

Avrupa Birliği Bakanlığı, "2006 Tarihli Katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_ Ort_ Belg_2006.pdf. (E.T: 20.05.2011)

Avrupa Birliği Bakanlığı, "2007 Tarihli Katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_ Ort_ Belg_2007.pdf. (E.T: 20.05.2011)

Avrupa Birliği Bakanlığı, "2014 Tarihli Katılım Ortaklığı Belgesi", http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_ Ort_ Belg_2003.pdf. (E.T: 20.05.2011)

Avrupa Birliği Bakanlığı, "İlerleme Raporları" http://www.ab.gov.tr/index.php?p=46224, (E.T: 20.05.2011)

Avrupa Birliği Bakanlığı, "İlerleme Raporları" http://www.abgs.gov.tr/index.php?p=123&l=1. (E.T: 20.05.2011)

Avrupa Konseyi, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme*"* http://www.avrupakonseyi.org.tr/antlasma /aas_108.htm, (E.T: 26.01.2013)

Başalp, Nilgün ve Keser Berber, Leyla, "Kişisel Verilerin Korunması Projesi", http://www.bilgiedinmehakki.org/tr/index.php?option=comcontent&task=view&id=83&Itemid=24, (E.T:16.02.2014)

Başbakanlık Avrupa Birliği Genel sekreterliği, "Avrupa Birliği Antlaşması ve Avrupa Birliği'nin İşleyişi Hakkında Antlaşma", http://www.ab.gov.tr/files/pub/antlasmalar.pdf. (E.T: 07.06.2015)

Başpınar, Veysel, (2008) "Elektronik Tapu Sicili Düzenlenirken, Tapu Sicilinin Aleniyeti ve Diğer Alanlarla İlgili Alınması Gereken Tedbirler", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 52, Sayı: 3 (97-132), http://auhf.ankara.edu.tr/dergiler/auhfd-arsiv/AUHF-2008-57-03/AUHF-2008-57-03-baspinar.pdf, (E.T: 09.01.2014),

Benoit, Rohmer Florence ve Klebes, Heinrich, (2006), *Avrupa Konseyi Hukuku Pan-Avrupa Hukuk Alanına Doğru,* Ankara: Avrupa Konseyi Yayını, http://www.dispolitika.org.tr/dosyalar/kitap_akh.pdf, (E.T: 17.06.2015)

Beyli, Ceylin, "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler, Türkiye Bilişim Şurası Hukuk Çalısma Grubu Kişisel Veriler Raporuna ait Görüşler", www.bilisimsurasi.org.tr/hukuk/docs/tbs_kisisel_veri_ceylin_beyli_gorus1.pdf-, (E.T: 08.07.2010)

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları hakkında Kanun Tasarısı gerekçesinden alıntı, Türkiye Bilişim Derneği, http://www.tbd.org.tr/index.php?dummy=1&sayfa=raporlar&vkid=194&t=1300665963&jfr=true&keepThis=true&TB_iframe=true&height= 500&width=800, (E.T: 12.05.2013)

Bozel, Savaş, "5651 Sayılı Kanuna İstinaden Bazı İnternet Sitelerine Erişimin Engellenmesi Tedbirine Eleştirel Bir Yaklaşım", http://www.e-akademi.org/makaleler/sbozel-5.htm. (E.T: 22.08.2010)

BSA (The Software Alliance), "Global Cloud Computing Scorecard", *Ülke Raporu 2013: Türkiye,* http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Turkey.pdf, (E.T: 17.09.2014)

BThaber.com, "CISPA: İnsan Hakları İhlalinin Yasal Yolu (Mu?)", http://www.bthaber.com/cispa-insan-haklari-ihlalinin-yasal-yolu-mu/, (E.T: 23.01.2014)

Cerf, V.G, "İnternet History", www.isocilt:org/internet/history/cerf.shtml, (E.T: 31.07.2011)

Çeken, Hüseyin, "ABD'de İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğunun Hukuki Esası", http://archiv.jura.uni-saarland.de/turkish/HCeken1.html (E.T: 25.2.2015)

Değirmenci, Olgun, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", http://www.caginpolisi.com.tr/37/59-60-61-62-63-64.htm, (E.T: 28.7.2011)

Doğan, Mehmet,"Kişisel Verilerin Korunmasında AB Standartları ve Türkiye'nin Durumu", EGM Asayiş Dairesi Başkanlığı, http://www.egm.gov.tr/egitim/dergi/eskisayi/35sayi/yeni/web/makaleler/MehmetDOGAN.htm, (E.T: 05.10.2009)

Döner, Ayhan, (2006), *Kişisel Verilerin Korunması Hakkında Federal Kanun*, EÜHFD, Cilt: X, Sayı: 1-2, http://www.erzincan.edu.tr/birim/HukukDergi/makale/2006_X_18.pdf. (E.T: 01.02.2014)

Dülger, Murat Volkan; "Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti", *Hukuk Günlüğü,* http://www.hukukgunlugu.org/saglik-hukukunda-kisisel-verilerin-korunmasi-ve-hasta-mahremiyeti/, (E.T: 21.06.2015)

Eralp, Özgür, "Bilişim Suçları", http://www.ozgureralp.av.tr/makaleler/bilisimsuçlarisistemi engelleme 244.html, (E.T: 16. 03. 2012)

Erdağ, Ali İhsan, "Ekonomi, Sanayi ve Ticarete İlişkin Suçlar-Bilişim Alanında Suçlar", http://www.ceza-bb.adalet.gov.tr/makale.htm (E.T: 09.01.2014)

Erdağ, Ali İhsan, *Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)*, webftp.gazi.edu.tr/hukuk/dergi/14_2_10.pdf. (E.T:09.01.2014)

Ersoy, Eren; "Gizlilik, Bireysel Haklar, Kisisel Verilerin Korunması", http://www.ab.org.tr/ab06/bildiri/6.doc, (E.T: 08.07.2010)

Federal Bureau of İnvestigation, "Election Hack, Stealing Votes the Cyber Way", https://www.fbi.gov/news/stories/2013/august/election-hack-stealing-votes-the-cyber-way/election-hack-stealing-votes-the-cyber-way, (E.T: 15.01.2014)

Forumtr, "GBT nedir", http://www.frmtr.com/hukuk/359142-gbt-nedir.html, (E.T:22.04.2014)

Gençay, Meriç, "Neticesi Sebebiyle Ağırlaşmış Suçlar", http://www.turkhukuksitesi.com/makale_1393.htm, (E.T: 29.09.2014)

General Comment 1, U.N. DoCilt: Hrı\Gen\1\Rev.1 At 21 (1994) http://www1.umnedu/humanrts /gencomm/hrcom16.htm, (E.T: 14.02.2014),

Güngör, Zehra, "Türk Şirketlerin Bilgisayar Güvenlik Planları Yok", Milliyet, http://www.milliyet.com.tr/1997/06/16/ekonomi/turkfir.html, (E.T: 08.05.2014)

Güran, Sait; Akün, Teoman; Bayraktar, Köksal; Yurtcan, Erdener; Kendigelen, Abuzer; Beller, Önder ve Sezer, Bülent, (2000), "İnternet ve Hukuk Temel Metni", http://www.superonline.com/hukuk/hukuk.htm. (E.T: 21.07.2011)

Hafızoğulları, Zeki, "Türk Ceza Hukuk Ders Notları", http://www.baskent.edu.tr/-zekih/uygulamaci/cezahukuk.doc" (E.T: 21.08.2013)

Hansen, Brian, "Cyber Crime, Should penalties be tougher?", *Kean University*, http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2002041200&type=query&num=cyber+crime&#.UtlbJ9JRbIU. (E.T: 23.01.2014)

Hürriyet, "687 Bin Öğretmenin Kimlik Numaraları Çalındı" http://www.hurriyet.com.tr/gundem /10988928.asp, (E.T: 11.02.2014)

Hürriyet, "Ankara'da Vatandaşların Tapu Bilgileri Çalındı", http://www.hurriyet.com.tr/gundem/27662013.asp, (E.T: 30.11.2014)

Internet Crime Complaint Center, http://www.ic3.gov/about/default.aspx, (E.T: 15.01.2014)

İlkiz, Fikret, "Kişisel Veriler ve Gizliliği", İstanbul, *BİA Haber Merkezi*, http://www.bianet.org/bianet/hukuk/154921-kisisel-veriler-ve-gizliligi, (E.T: 23.07.2014)

İnternet Medya ve Bilişim Federasyonu, "Avrupa siber Suç sözleşmesi" www.imef.org.tr/uluslararasi-ıliskiler/257-avrupa-konseyi-siber-suclar-sozlesmesi-.html. (E.T: 22.08.2011)

Karaarslan, Enis; Koç, Serhat ve Akın Gökhan, "Vatandaşlık Numarası Bazlı E-devlet Sistemlerinde Kişisel Veri Mahremiyeti Durum Saptaması",

http://web.itu.edu.tr/akingok/ubhk10/E-devletSistemlerindeVeriGuvenligi.pdf (E.T: 25.06.2015)

Karakehya, Hakan, "Gözetim ve Suçla Mücadele", AÜHFD, auhf.ankara.edu.tr/ dergiler/.../AUHF-2009-58-02-karakehya.pdf, (E.T: 09.01.2014)

Katoğlu, Tuğrul, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları"*, AÜHFD*, 61 (2) 2012, http://dergiler.ankara.edu.tr/dergiler/38/1679/ 17897.pdf. (E.T: 13.01.2014)

Kesmez, Necdet "Kişisel Verilerin Korunması Üzerine" Bilişim Şurası, http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0044/01-KISISELVERILER IN KORUNMASI.doc, (E.T: 14.02.2014)

Kılınç, Doğan, (2012), "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", AÜHFD, Cilt: 61, sayı: 3, http:/dergiler.ankara.edu.tr/dergiler/38/1690/18020.pdf, (E.T:06.01.2014)

Korff, Douwe**,** (2002), Ec Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49): *Comparative Summary of National,* Humen Right Centre, Colchester (UK): University of Essex, http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE, (E.T: 21.06.2015)

Kyung-Shick, Choi, *Computer Crime Victimization and Integrated Theory:An Empirical Assessment*,http://www.cybercrimejournal.com/Choiijccjan2008.htm. (E.T: 23.01.2014)

Lee, A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Right Treaties"*, International Journal of Law and Information Technology*, Vol.6, No.3. http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf. (E.T: 14.02.2014)

Legally e-Health Putting e Health in its European Legal Context, Legal and Regulatory Aspects of e-health, Study Report, (March 2008), http://www.epsos.eu/uploads/tx_epsosfileshare/Legally-eHealth-Report_01.pdf, (E.T:03.01.2014)

Mahmutoğlu, F. Selami, "Türk Ceza Kanununda Yer Alana Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", http://fsmahmutoglu.av.tr/pdf/aec4ba0684aa8f46aec75249e66d910173a2f8f47818077253.pdf, (E.T: 21.9.2013)

Mueller, Robert S., "The Cyber Threat Planning for the Way Ahead", http://www.fbi.gov/news/stories/2013/february/the-cyber-threat-planning-for-the-way-ahead, (E.T: 21.03.2014)

Mynet, "Lisede Şifre Skandalı, 300 Ögrenci Mağdur" http://www.mynet.com/haber/guncel/lisede-sifre-skandali-300-ogrenci-magdur-653206-1, (E.T:25.11.2013)

Nedir.com, "Atm Nedir", http://atm.nedir.com/#ixzz2zTJKIneY, (E.T: 21.04.2014)

NTVMSNBC, "2000 Hacker'ların Yılı Oldu", http://arsiv.ntvmsnbc.com/news/51092.asp, (E.T: 08.05.2014)

OECD, " OECD Guidelines On The Protection Of Privacy And Transborder Flows of Personal Data", http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, (E.T: 17.02.2014)

OECD, "Guidelines on The Protection of Privacy and Transborder Flows of Personal Data", http://www.oecd.org/document/18/0,2340, en 2649 34255 1815186 111 1,00.html, (E.T: 03.05.2012)

Önok, Murat, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, http://dosya.marmara.edu.tr/huk/fak%C3%BCltedergisi/nurcentel/muratonok. pdf. (E.T: 31.03.2014),

Özcan Mehmet, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu", http://adlibilirkisi.org/index.php?sayfa=makaleoku&kategori=5&id=18 (E.T: 12.11.2014)

Özdemir, Hayrunnisa, Haberleşmenin Gizliliği ve Kişisel Veriler, *Erzincan Üniversitesi Hukuk Fakültesi Dergisi (EÜHFD)*, Cilt: XIII, Sayı 1-2 http://www.erzincan.edu.tr/birim/hukukdergi/makale/2009%20XIII_1-11.pdf, (E.T: 28.01.2014)

Özdilek, Ali Osman, "Bilgisayar Suçları Ne Kadar Ciddi?", http://www.hukuk rehberi.net/Details.aspx?id=88, (E.T. 20.02.2014)

Özdilek, Ali Osman, "Port Tarayıcı Kullanımı Hukuka Aykırımıdır?-2", http://www.turk-internet.com/portal/yaziyaz.php?yaziid=7068 (E.T:23.03.2014)

Pekel, Ahmet, (2011), "Siber Tehditler ve Bilgi Güvenliği", www.slideshare.net/mobile/AhmetPekel/siber-tehditler-ve-bilgi-gvenlii. Ankara: Nisan, (E.T: 12.03.2015)

Pekşirin, Hülya, Bilişim Şurası Gurup Yöneticisi, "Kişisel Verilerin Korunması", *Bilişim Şurası Hukuk Raporu,* http://tr.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu, (E.T:02.12.2013).

Privacy And Human Rights 2002; "An International Survey of Privacy Laws and Developments", http.privacyinternatonal.org/survey/phr2002/phr2002-part1. pdf, (E.T: 25.7.2012)

Raman, Jari, *Computer Crime*, ENLIST, Nov. 7, 2000, http://itlaw.law.strath.ac.uk/ ENLIST/subjects/is/commentary, (E.T:06.05.2012)

Resmi Gazete, http://www.resmigazete.gov.tr/eskiler/2010/05/20100513.htm&main, (E.T: 05.05.2011)

Salihpaşaoğlu, Yaşar, "Özel Hayatın Kapsamı, Avrupa İnsan Hakları Mahkemesi İçtihatları Kapsamında Bir Değerlendirme", *GÜHFD*, Cilt:17/3 (Temmuz 2013), http://webftp.gazi.edu.tr/hukuk/dergi/17_3_8.pdf, (E.T: 20.02.2014)

Schjolberg, Stein, "The Legal Framework – Unauthorized Access to Computer Systems", *Penal Legislation in 44 Countries*, www.mossbyrett.of.no/info/legal.html, (E.T: 15.01.2013)

Son Dakika, "Siber Suçların Maliyeti 445 Milyar Dolar", *Haberler*, http://www.sondakika.com/haber/haber-siber-suclarin-maliyeti-445-milyar-dolar-7001053/ (E.T: 07.06.2015)

Şeker, Güven, "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum", *İnsan Bilimleri,* www.insanbilimleri.com/makaleler/kamuyönetimi/bilişim-suçlarinin.htm, (E.T: 25.06.2010)

Şen, Bilal, "Elektronik Gözetim", http://hkmcengiz.tr.gg/ELKTRNK-GZTIM.htm, (E.T: 10.07.2015)

Tansuğ, Avniye, "AB'nin Yeni Ekonomik Silahı: Veri Saklama Hukuku", http://www.acikradyo.com.tr/i/rss/Bilgi_Caginin_Hukuku.xml, (E.T:14.02.2014)

TBMM, "Tasarı ve Teklifler", http://www.tbmm.gov.tr/develop/owa/tasari_teklif_gd.sorgu_yonlendirme, (E.T: 27.11.2014).

TBMM, "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)", http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf. (E.T: 29.11.2014)

TBMM, "Kişisel Verilerin Korunması Kanun Tasarısı", http://www2.tbmm.gov.tr/d23/1/1-0576.pdf, (E.T: 18.02.2015)

Tiftikçi, Mehmet, "Özel Hukuk ve İnternet", http://inet-tr.org/inetconf/tammetin/hukuk.html, (E.T: 27.10.2010)

Türk Dil Kurumu, "Politika Nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=politika&ayn=tam. (E.T: 30.01.2014)

Türk Dil Kurumu, "Din Nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=din&ayn=tam. (E.T: 30.01.2014)

Türk Dil Kurumu, "Felsefe Nedir" http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=felsefe&ayn=tam. (E.T: 30.01.2014)

Türk Dil Kurumu, "Meslek Nedir" http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=tdk.gts.52b48b85df2970.46760857. (E.T: 12.09.2010)

Türk Dil Kurumu, "Sanat Nedir" http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.52b48b8de4efa2.10698734 (E.T: 12.09.2010)

Türk Dil Kurumu, "Veri ve Bilgi Nedir" http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5425839dc592e5.35646613, (Erişim: 26.09.2013)

Türk Hukuk Sitesi, "70 Milyon Kişinin Kimlik Bilgileri Çalındı", http://www.turkhukuksitesi.com/showthread.php?t=52705, (E.T: 11.02.2014)

Türk Dil Kurumu Sözlüğü, "Verme, Yayma ve Ele Geçirme Nedir", http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK (E.T: 21.03.2014)

Ülkü, Muhammet Murat, "5237 Sayılı TCK. 132-140. Maddelerinde Yer Alan Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar", *Ankara: Adalet Bakanlığı*, s.3. http://www.ceza-bb.adalet.gov.tr/makale/150.pdf, (E.T: 05.10.2009)

Visa Public, *Incident Response Procedure For Account Compromise,* http://www.visa-asia.com/secured, (E.T: 02.07.2012)

Wikipedia, "Cyber Intelligence Sharing and Protection Act", http://tr.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act, (E.T: 28.04.2012)

Wikipedia, "Portal", https://tr.wikipedia.org/wiki/Portal_(Internet) (E.T: 05.08.2011)

Wikipedia, "End User License Agreement", http://en.wikipedia.org/wiki/End-user_license_agreement, (E.T: 16.09.2014)

Yargıtay CGK, 26.12.2012, E:2012/11-1065, K:2012/1438, http://emsal.yargitay.gov.tr/VeriBankasiIstemciWeb/GelismisDokumanAraServlet. (E.T: 15.06.2014)

Yazıcıoğlu, Yılmaz, "Türk Mevzuatında Bilişim Suçları" , AB Uyum Komisyonu Çalısması, http://www.taa.gov.tr/duyurularana/130606/bilisimsempozyum/sunum/makale.pdf (Erişim: 03.05.2011)

Yıldız, Ali Kemal, (2010), "2007 tarihli Yeni Türk İnternet Kanunu ve İnternet Süjelerinin Cezalandırılabilirliği", *Alman–Türk Karşılaştırmalı Ceza Hukuku,*http://www.jura.uni-wuerzburg.de/fileadmin/02150100/IWAS/Materialien/Dtt_Yildiz.pdf. (E.T: 03.08.2011)

Yıldız, Sevil*, Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi*, http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler/SevilYILDIZ/YILDIZ, SEVİL.pdf,(E.T:03.08.2011)

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : **Alaattin BÜK**

Doğum Yeri : **Karabük**

Mesleği : **Hakim**

Eğitim Durumu

Lisans Öğrenimi : Ankara Üniversitesi Hukuk Fakültesi

Yüksek Lisans Öğrenimi : Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü

Bildiği Yabancı Diller : İngilizce

Yabancı Dil Puan ve Türü : 51,25 (ÜDS)

Bilimsel Faaliyetler :

I- Türkiye Adalet Akademesi Bünyesinde;

1- Kişisel Haktan Kaynaklanan Tapu İptali ve Tescil, Mera, Yaylak ve Kışlak Davaları,

2- Hukuk Muhakemeleri Usulü,

3- Geçit, Mecra ve Tapu Kaydında Kimlik Bilgisi Düzeltilmesi konularında öğretim görevlisi olarak görev aldım.

II- 6100 sayılı Hukuk Muhakemeleri Kanunun, hukuk hakimlerine tanıtılması programı kapsamında Afyonkarahisar, Ankara, Eskişehir, Konya ve Türkiye Adalet Akademisinde verilen seminerlerde sunum yaptım.

III- Avrupa Konseyi ile birlikte yürütülen Mahkeme Yönetimi Projesi kapsamında Eskişehir ve Salihli'de Yargıtay Başkanlığını temsilen katılımcı olarak bulundum.

IV- HSYK'nın Hukuki Müzakereler Toplantısı kapsamında Eser sözleşemesinden Kanaklanan Davaları ve Arsa Payı Karşılığı İnşaat Sözleşmesinden Kaynaklanan Davalar ile ilgili çalışmada sunum yaptım ve sonuç belgesinin raportörü olarak bulundum.

V- Türkiye Adalet Akademisi ders notu kitaplaştırma çalışmalarında "Tapu Kaydında Kimlik Bilgisi Düzeltilmesi" konusunu hazırladım.

VI- Yetişkin eğitimi konusunda Türkiye Adalat Akademisi tarafından hazırlanan seminer programları kapsamında Türkiye Adalat Akademisi İncek Kampüsü, Bolu ve Afyonkarahisar'da ders aldım.

VII- TCK'de Çocuk Suçları, Türk Medeni Kanunu, Türk Ceza Kanunu, Ceza Muhakemesi Kanunu ve AİHM kararaları ile ilgili eğitim programlarında katılımcı olarak bulundum.

VIII- HSYK tarafından mesleki araştırma kapsamında gönderildiğim Amerika'nın Newjersey eyaletinde bulunan Kean Üniversitesinde öğretim görevlisi olarak bulundum.

İş Deneyimi

Stajlar	: Zonguldak Barosu: Avukatlık Stajı
	Adalet bakanlığı Hakim ve Savcı Eğitim Merkezi:
	Hakim Adaylığı
Çalıştığı Kurumlar	: Karabük Barosu (Serbest Meslek - Avukat)
	SSK Hukuk Müşavirliği (Avukat)
	Adalet Bakanlığı Bolu Adliyesi (Hakim)
	Adalet Bakanlığı Hozat Adliyesi (Hakim)
	Yargıtay Başkanlığı (Tetkik Hakimi)
	Türkiye Adalet Akademisi (Öğretim Görevlisi)
	Adalet Bakanlığı Urla Adliyesi (Hakim)

İletişim

E-posta : alaattinbuk@hotmail.com

Tel. : 0.505.7710377

Tarih : 25.12.2015