

**T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

TÜRK CEZA HUKUKUNDA BİLİŞİM SUÇLARI

Doktora Tezi

Muammer KETİZMEN

Ankara-2006

**T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI**

TÜRK CEZA HUKUKUNDA BİLİŞİM SUÇLARI

Doktora Tezi

Muammer KETİZMEN

Tez Danışmanı
Prof. Dr. Metin FEYZİOĞLU

Ankara-2006

İÇİNDEKİLER

KISALTMALAR	vii
GİRİŞ	1

BİRİNCİ BÖLÜM

GENEL BİLGİLER

I. BİLİŞİM– BİLİŞİM SİSTEMLERİ, BİLGİSAYAR, İNTERNET	7
<i>A. Genel Olarak Bilişim – Bilişim Sistemleri</i>	7
<i>B. Bilişim Sistemi Olarak Bilgisayar</i>	13
<i>C. Bilişim Sistemi Olarak İnternet</i>	20
1. Kavram, Tarihçe	20
2. İnternete İlişkin Hukuki Düzenleme ve İnternet Süjelerinin Sorumluluğu	24
II. SOSYO-EKONOMİK DÖNÜŞÜM AÇISINDAN BİLİŞİM SUÇLARI	33
III. BİLİŞİM SUÇLARI	45
<i>A. Terim, Tanım ve Kapsam Sorunu</i>	45
<i>B. Bilişim Suçları Açısından Avrupa Konseyi Sıbersuç Sözleşmesi</i>	54
<i>C. Bilişim Suçları Açısından Türk Ceza Kanununun Kapsamı</i>	60

İKİNCİ BÖLÜM

BİLİŞİM ALANINDA SUÇLAR

I. GENEL OLARAK	65
II. BİLİŞİM ALANINDA SUÇLAR AÇISINDAN TÜRK CEZA KANUNUNUN SİSTEMATİĞİ	67
III. VERİNİN ELE GEÇİRİLMESİ VE BİLİŞİM SİSTEMİNE YETKİSİZ ERİŞİM	79
<i>A. Verinin Ele Geçirilmesi</i>	79
1. Genel Olarak Verinin Gizliliğinin Korunması	79
2. 765 Sayılı Türk Ceza Kanununda Verinin Ele Geçirilmesi	88
<i>B. Bilişim Sistemine Yetkisiz Erişim</i>	93
1. Genel Olarak	93
2. Türk Ceza Kanununda Bilişim Sistemine Yetkisiz Erişim – Bilişim Sistemine Girme ve Orada Kalmaya Devam Etme	95
a. Genel Olarak	95
b. Suçun Hukuki Konusu	98
i. Genel Olarak	98
ii. Mameleki Bir Değerin Korunması Açısından Sibera lan	99
iii. Özel Hayatın Gizliliğinin Korunması Kapsamında Sibera lan	103
iv. Sırrın Korunması Kapsamında Verinin Gizliliğinin Dolaylı Olarak Korunması	105
v. Türk Ceza Kanunda Düzenlenen Yetkisiz Erişim Suçunun Hukuki Konusu	106
c. Suçun Maddi Unsuru Olarak Bilişim Sisteminin Bütününe veya Bir Kısma na Girme ve Orada Kalmaya Devam Etme	120

d. Suça Etki Eden Nedenler	132
IV. BİLİŞİM SİSTEMİNE VE VERİYE MÜDAHALE	136
A. Genel Olarak	136
B. Türk Ceza Kanununda Bilişim Sistemi ve Veriye Müdahale	141
1. Genel Olarak	141
2. Sisteme ve Veriye Müdahale Suçunun Hukuki Konusu	145
a. Genel Olarak	145
b. Suçun Hukuki Konusu Açısından Mala Zarar Verme Suçu Karşısında Sisteme Ve Veriye Müdahale	148
c. Türk Ceza Kanununda Düzenlenen Bilişim Sistemine ve Veriye Müdahale Suçunun Hukuki Konusu	153
3. Suçun Maddi Unsuru	157
a. Sistemin İşleyişini Engelleme ve Bozma	157
i. Genel Olarak	157
ii. Mala Zarar Verme Suçu Kapsamında Sistemin İşleyişinin Engellenmesi ve Bozulması	159
b. Bilişim Sistemi İçerisindeki Verileri Bozma, Yok Etme, Değiştirme, Verileri Başka Bir Yere Gönderme	168
i. Genel Olarak	168
ii. Müdahalenin Konusu Olarak Bilişim Sistemi İçerisindeki Veri	175
4. Suça Etki Eden Nedenler	177
V. BİLİŞİM SİSTEMLERİ ARACILIĞIYLA YARAR SAĞLAMA	178
A. Genel Olarak	178
B. Bilişim Sistemleri Aracılığıyla Yarar Sağlamanın Ayrı Bir Suç Olarak Düzenlenmesinin Nedenleri	181

1. Genel Olarak	181
2. Kişiyeye Karşı Hileli Bir Hareketin Olmaması	182
3. Bilişim Sistemleri Aracılığıyla Yarar Sağlama Suçu Olarak Eşya Kapsamında Değerlendirilemeyen Verinin Elde Edilmesi	187
<i>C. Türk Ceza Hukukunda Bilişim Sistemleri</i>	
<i>Aracılığıyla Yarar Sağlama Suçu</i>	191
1. Genel Olarak	191
2. Bilgileri Otomatik İşleme Tabi Tutmuş Sistemi Kullanarak Hukuka Aykırı Yarar Sağlama (765 Sayılı TCK 525b/2)	193
a. Genel Olarak	193
b. Haksız Olarak Ele Geçirilen Banka Kartı Kullanılması Suretiyle “ATM”lerden Para Çekilmesi	197
c. Kişiyeye Karşı Hileli Hareketler Yapılması ve Bilişim Sistemi Kullanılması Sonucunda Yarar Sağlanması	203
d. Kişiyeye Karşı Hile Yapılmaksızın Bilişim Sistemi Kullanılmak Suretiyle Yarar Sağlanması	208
3. Türk Ceza Kanununda Bilişim Sistemleri Aracılığıyla Yarar Sağlama	218
a. Genel Olarak	218
b. Suçun Kapsamı	219
i. Maddi Unsur Açısından	219
ii. Düzenleme Şekli Açısından	221
c. Bilişim Sistemleri Aracılığıyla Yarar Sağlama Suçunun Kapsamının Daraltılmasından Çıkan Sonuçlar	224
i. Hırsızlık Suçu Karşısında Bilişim Sistemi Aracılığıyla Yarar Sağlama	224

ii. Dolandırıcılık Suçu Karşısında Bilişim Sistemi Aracılığıyla Yarar Sağlama	227
iii. Banka ve Kredi Kartlarının Kötüye Kullanılması	230

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI

I. GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI	236
II. KİŞİSEL VERİLERİN KORUNMASININ AMACI – VERİ/ENFORMASYON MAHREMİYETİ	239
III. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN SUÇLAR	253
<i>A. Genel Olarak</i>	253
<i>B. Kişisel Verilerin Korunmasına İlişkin Suçların Hukuki Konusu Olarak Özel Hayatın Gizliliği</i>	257
<i>C. Kişisel Verilerin İşlenmesine İlişkin Usul ve Esaslar – Kişisel Verilerin Korunmasına İlişkin İlkeler</i>	268
1.Genel Olarak	268
2. Veri İşleyenin Sorumluluk ve Yükümlülükleri	272
a. Genel Olarak	272
b. Dürüst ve Hukuka Uygun Toplama ve İşleme	273
c. Amaçla Bağlılık	281
<i>D. Kişisel Verilerin Korunmasına İlişkin Suçlar Bakımından Kişisel Veri</i>	285
<i>E. Kişisel Verilerin Kaydedilmesi Suçu</i>	287
1. Genel Olarak	287

2. Dürüst ve Hukuka Uygun Toplama – Amaçla Bağlılık İlkesi	
Karşısında Kişisel Verinin Hukuka Aykırı Olarak Kaydedilmesi	289
<i>F. Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme</i>	298
<i>G. Verileri Yok Etmeme</i>	300
SONUÇ VE DEĞERLENDİRME	303
KAYNAKÇA	320

KISALTMALAR*

a.g.e.	: Adı geçen eser
a.g.m.	: Adı geçen makale
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
Am J. Comp L.	: American Journal of Comparative Law
Am. Crim. L. Rev.	: American Criminal Law Review
Am. J. Crim L	: American Journal of Criminal Law
Ank. Ün.	: Ankara Üniversitesi
AÜHF	: Ankara Üniversitesi Hukuk Fakültesi
Ann. Surv. Am. L.	: Annual Survey of American Law
AYM	: Anayasa Mahkemesi
AYMK	: Anayasa Mahkemesi Kararı
B. C. Int'l & Comp. L. Rev.	: Boston College International and Comparative Law Review
B.	: Baskı
BM	: Birleşmiş Milletler
C.	: Cilt
Cal. Crim. Law. Rev.	: California Criminal Law Review

* Kısaltmalarda kullanılan ABD menşeli dergiler için “*A Uniform System of Citation*” esas alınmıştır.

Cal. W. L. Rev.	: California Western Law Review
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
Çev.	: Çeviren
der.	: Derleyen
Duke J. Comp. &	
Int'l	: Duke Journal of Comparative & International Law
E.	: Esas
Edit.	: Editör
EMORY L. J.	: Emory Law Journal
Har. L. Rev.	: Harvard Law Review
Harv. J. on Legis.	: Harvard Journal on Legislation
İHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	: Karar
m.	: Madde
N. Ill. U. L. Rev.	: Northern Illinois University Law Review.
No.	: Numara
OECD	: Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü) İktisadi İşbirliği ve Gelişme Teşkilatı
parag.	: Paragraf
pp	: Pages
Rutgers L. Rev.	: Rutgers Law Review
s.	: Sayfa

S.	: Sayı
SBFD	: Siyasal Bilgiler Fakóltesi Dergisi
Seton Hall L. Rev.,	: Seton Hall Law Review
St. Mary's L. J.	: St. Mary's Law Journal
T.	: Tarih
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: 5237 Sayılı Türk Ceza Kanunu
Tex. Int'l L.J.	: Texas International Law Journal
TDK	: Türk Dil Kurumu
TMK	: Türk Medeni Kanunu
U. Pa. L. Rev.	: University of Pennsylvania Law Review
V.	: Volume
vb.	: ve benzeri
vd.	: ve devamı
vs.	: ve sair

GİRİŞ

Günümüzde, bilgi ve enformasyonun etkin olarak işlenmesinde en önemli yere sahip olan bilişim teknolojisinin gelişimi ve özellikle modern bilgisayarın icadı ile birlikte, 20 yüzyılın ikinci yarısından itibaren etkisini hissettirmeye başlayan sosyo-ekonomik dönüşüm, toplumsal kurumları çeşitli yönleriyle etkilemektedir. Söz konusu etkinin kapsamı ve boyutları, dönüşümün dinamikleri ve derinliğiyle bağlantılıdır.

Bilgi toplumu, bilişim toplumu ya da enformasyon toplumu gibi çeşitli adlarla adlandırılan sosyo – ekonomik dönüşümün temel özelliği, öncelikli olarak bilgi ve enformasyonun değerinin artması ve merkezi bir konum edinmesidir. Bunun yanında bilişim ve özellikle sistemlerinin yaygın olarak kullanılması dönemin diğer bir özelliğine işaret etmektedir. Bu özellik, birçok faaliyetin sürdürülmesinde ve genel olarak toplumsal ilişkilerde sayısal kodların etkin bir araç olarak kullanılmaya başlanması anlamında sayısallaşmadır. Enformasyon ya da bilginin bilgisayar sistemleri aracılığıyla belirli bir yazılıma bağlı olarak veri şeklinde işlenmesi, sayısallaşma olgusunu gündeme getirmiştir.

Sosyo-ekonomik dönüşüm içerisinde bilgi ve enformasyonun artan önemi ve sayısallaşma toplumsal kurumları etkileyen unsurlardır. Toplumsal bir kurum olan hukuk da birçok yönüyle söz konusu gelişimden etkilenmektedir. Bu bağlamda bilişim suçları, bilgisayar suçları gibi birçok ad altında incelenen suçlar, dönüşümün maddi ceza hukukuna etkisini oluşturmaktadır.

Bilişim suçları olarak adlandırılan suçların ceza mevzuatları içerisinde yer edinmeye başlaması, bu tür suçların konusunu ve unsurlarını oluşturan bilişim

sistemi, bilgisayar gibi kavram ve terimlerin açıklanması zorunluluğunu doğurmaktadır. Bu nedenle birinci bölümün ilk konusunu, terim ve tanım sorunu olarak bilişim, bilgisayar ve İnternet oluşturmaktadır. Bir bilim dalı olarak bilişim ve bir bilişim sistemi olarak bilgisayar ve özellikle 1990'lı yıllardan itibaren yaygın olarak kullanılmaya başlayan İnternete birinci bölümde değinilmiştir.

Bilişim suçları olarak adlandırılan suçlar, tek başına ne bir bilim dalı olarak bilişim ne de bir bilişim sistemi olarak bilgisayar ya da İnternet'in kullanılmaya başlanmasıyla açıklanabilmektedir. Bilişim suçlarının özellikle anlam kazandığı sosyo-ekonomik dönüşüme değinilmesi gerekmektedir. Dönüşümün dinamikleri, bilişim suçları olarak adlandırılan suçların anlam ve kapsamının belirlenmesinde önemli olmakta ve aynı zamanda, bilişim suçları başlığı altında incelenen suçların öneminin açıklanmasında değinilmesi gereken bir konuyu oluşturmaktadır. Bu nedenle, enformasyon toplumu, bilgi toplumu, bilişim toplumu gibi birçok ad altında incelenen sosyo-ekonomik dönüşüm, birinci bölümde değinilen diğer bir konudur.

Bilişim suçlarına ilişkin bir inceleme yapılırken özellikle bilişim suçlarının tanım ve kapsam sorununa değinilmesi de gerekmektedir. Bilişim suçları, bilgisayar suçları, siber suçlar gibi çeşitli adlar altında incelenen suçlara ilişkin çeşitli tanımlar yapılmaktadır. Bilişim suçlarını kategorik olarak ayrı bir suç grubunu içermemesi ve sosyo –ekonomik dönüşümün etkisinin boyutları ile paralel olarak bilişim suçları adı altında incelenen suçların günden güne genişlemesi karşısında bilişim suçlarına ilişkin kategorik bir tanım yapılmasını zorlaştırmaktadır. Birinci bölümde bu hususa da yer verilmiştir.

Bilişim sistemlerinin kullanılmasının sosyo – ekonomik dönüşüm içerisinde ceza hukukuna etkisi olarak anlaşılması karşısında, bir çok suçun bilişim suçları

başlığı altında incelenmesi mümkündür. Örnek oluşturması bakımından, bilişim suçlarına ilişkin ilk ve tek uluslar arası bir sözleşme olan, Avrupa Konseyi Siberaş Sözleşmesinde düzenlenen suçlara birinci bölümde değinilmektedir.

Farklı nitelikteki birçok suçun bilişim suçları adı altında gündeme gelmesi bilişim suçlarının incelenmesine ilişkin belirli bir sınırlandırılmaya gidilmesi zorunluluğunu doğurmaktadır. Bu nedenle konu, 5237 Sayılı TCK'nin 243 vd. maddelerinde düzenlenen, Kanunun ifadesiyle “Bilişim alanında suçlar” ve 135 vd. maddelerinde düzenlenen kişisel verilerin korunmasına ilişkin suçlar ile sınırlı tutulmuştur. Söz konusu suçlar, ilgili bölümlerde görüleceği, üzere ceza mevzuatlarına yeni suçların girmesi anlamında niteliksel bir etki olarak karşımıza çıkmaktadır. Her iki suç grubunun incelenmesi, sosyo-ekonomik dönüşüm içerisinde anlam kazanan ve bilişim suçları adı altında suç olarak düzenlenen fiiller yönünden, düzenleme yeri ve kapsamına ilişkin soruna ve sorunun çözümüne ilişkin 5237 Sayılı TCK'de hakim olan yaklaşımın ve yöntemin tespiti bakımından önem arz etmektedir.

Bu nedenle bilişim sistemleri ve özellikle İnternet kullanılarak işlenen çocuk pornografisi, ırkçılık ve yabancı düşmanlığı gibi suçlar ile telif haklarının korunmasına ilişkin suçlar, kapsam dışı bırakılmıştır. Gerçekte bu tür suçların bilişim suçları arasında incelenmesinin nedeni, bilişim sistemlerinin kullanılması suretiyle işlenme oranlarının artması ve yaygınlaşmasından kaynaklanmaktadır.

TCK'deki ifadesiyle, “*bilişim alanında suçlar*” hem 765 Sayılı TCK hem de 5237 Sayılı TCK'nin çeşitli yönleriyle düzenlenmiştir. 765 Sayılı TCK'nin 525a vd. maddelerinde “bilişim alanında suçlar” başlığı altında düzenlenen suçlar, sosyo – ekonomik dönüşüm içerisinde bilişim sistemleri ve özellikler bilgisayar sistemlerinin

kullanımının bir etkisi olarak ilk defa ceza mevzuatımız içerisinde yer edinmiştir. 5327 s. TCK'nin 243 vd. maddelerinde yer alan suçların, 765 S. TCK'de düzenlenen suçlardan unsurları ve niteliği itibariyle kimi yönlerden farklı bir şekilde ele alındığı ve düzenlendiği görülmektedir. Ayrıca “*bilişim alanında suçlar*” başlığı altında düzenlenen suçların, 5237 S. TCK içerisindeki düzenlenme yeri bakımından da 765 S. TCK'ye göre farklı bir tercihe yer verildiği görülmektedir.

Bunun yanında, 5237 S. TCK'de, 765 S. TCK'den farklı olarak, kişisel verilerin korunmasına ilişkin suçlara Kanunun 135 vd. maddelerinde yer verilmiş bulunmaktadır. Her ne kadar genel olarak bilişim suçları başlığı altında incelenmese ve Sibera suç Sözleşmesinde yer verilmemiş olsa da kişisel verilerin korunması da sosyo-ekonomik dönüşüm içerisinde bilişim sistemlerinin kullanımının bir önemli etkisi olarak ortaya çıkmakta ve kişisel verilerin korunmasına ilişkin suçlar bu etkinin bir sonucu olarak ceza mevzuatlarında yer edinmektedir.

Hukuk sistemi içerisinde ve özelde ceza hukukunda sosyo – ekonomik dönüşümün etkilerinin doğru bir şekilde algılanması, ortaya çıkabilecek sorunların çözümü bakımından da önemlidir. Bu husus, ceza hukuku kurumlarının , dönüşümün dinamikleri ile uyumlu bir hale getirilmesi ve dönüşüm ile birlikte ceza hukuku kurumlarının evrimini gündeme getirmektedir. Halihazırda tartışılması gereken sorun, öncelikli olarak yeni bir hukuki konunun söz konusu olup olmadığıdır. Aynı şekilde ceza mevzuatları içerisinde yer alan suçların, dönüşümün etkisiyle bilişim sistemlerinin kötüye kullanımları olarak ortaya çıkan fiilleri kapsayıp kapsamadığı da tartışma konusudur.

Ceza hukuku bakımından sorunun bir yönü bilgi ve enformasyonun, korunmasıyla ilgilidir. Sorunun diğer bir yönü sayısallaşma olarak adlandırılan

durum ile ilgilidir. Sosyo – ekonomik faaliyetlerin ağırlıklı olarak bilişim ve bilgisayar sistemleri aracılığıyla gerçekleştiriliyor olması karşısında, bilişim alt yapısının korunması da önemli hale gelmiştir. Bu tür sorunlar, bir bütün olarak, bilişim sistemlerine, ayrıca bilgi ve enformasyonu temsil eden veriye yönelik bir kısım fiillerin suç olarak düzenlenmesine ilişkin tartışmaları beraberinde getirmiştir.

Söz konusu sorunlara ilişkin olarak ceza hukukunda tartışmaların merkezini oluşturan hususlar, hangi değer korunduğu ve bununla bağlantılı olarak bu değerlere yönelik saldırıları ifade eden hangi tür fiillerin suç olarak düzenlenmesi gerektiğidir. Nitekim bilişim suçları olarak adlandırılan suçlarda, öncelikli olarak ceza müeyyidesiyle koruma altına alınan değer ne olduğunun tespiti önemlidir. Bu husus bir yandan korumanın amacını ve meşruiyetini göstermektedir. Diğer bir yandan da suçun hukuki konusunun saptanması sonucunu doğurmaktadır. Suç olarak düzenlenen fiiller ise, söz konusu değerlere yönelik ihlal yöntemlerinin ne şekilde olduğunun ya da olabileceğinin belirlenmesi suretiyle tespit edilmiştir.

Sorunun odak noktasının suçun hukuki konusunun ve bununla bağlantılı olarak özellikle suç olarak düzenlenecek fiillerin belirlenmesi olarak ortaya çıkması, söz konusu suçların incelenme yöntemini de belirlemiştir. Bu doğrultuda, tartışmanın merkezinin suçun hukuki konusu ve suç olarak düzenlenen fiiller olması, incelemenin ağırlıklı olarak bu iki husus etrafında toplanmasına yol açmıştır.

Bilişim suçları olarak adlandırılan suçların hukuki konularına ilişkin inceleme, bu suçlarda yeni hukuki konu veya konuların esas alınıp alınmadığının ya da ceza mevzuatlarında mevcut suçlarla hukuki konu bakımından örtüşüp örtüşmediğinin saptanması bakımından önemlidir. Bu sorunun çözümü, bilişim suçlarına ilişkin suçların ceza kanunlarında düzenlenmesi bakımından da çeşitli

sonular doęurmadır. zellikle ceza kanunları ierisinde belirli bir sisteme gre dzenlenmiř olan zel kısımlar bakımından biliřim sularına iliřkin hkmlerin alacaęı yer bunlardan biridir. Dzenlendięi yer bakımından ortaya ıkan hkm ve sonular nemli hale gelmektedir. Ayrıca bu husus kimi yazarlarca

¹ suun unsurları arasında incelenen bunun yanında kimi yazarlarca² suun unsurları dıřında tutulan hukuka aykırılıęın ierięinin tespiti bakımından nemlidir

Bu ynde irdeleme, sosyo – ekonomik dnřmn ceza mevzuatına etkisi bakımından ortaya ıkan ve ıkabilecek sorunların zmnde de etkilidir. Biliřim sistemlerinin ktye kullanımına iliřkin fiillere ynelik olarak ceza kanunlarına hakim olan sistemler bozulmadan zm getirilmesi, hukuki konunun incelenmesi ile mmkndr. Bu sylenen husus 5237 Sayılı TCK'nin zel kısmına hakim olan sistem aısından da geerlidir.

Biliřim sistemlerinin kullanılmasının eřitli ynlerini esas alan fiiller bakımından sorun, suların hukuki konuları ile baęlantılıdır. Biliřim suları olarak adlandırılan suların, yeni hukuki konuları ieren sular olduęunun kabul halinde, suun maddi unsurunu oluřturan fiillerin kendileri de tamamen yeni bir olguyu oluřturur. Sz konusu suların hukuki konularının ceza mevzuatlarında yer alan kimi suların hukuki konularıyla rtřtęnn kabul edilmesi halinde, bu tr fiiller mevcut suların hukuki konularına ynelik yeni ihlal řekillerini ifade eder.

¹ Bkz., Ayhan NDER, Ceza Hukuku Genel Hkmler, C. II-III, İstanbul, 1992, s. 5 vd. Ayrıca bkz., Sulhi DNMEZER, Ceza Hukuku Dersleri, İstanbul, 2003, s. 84 – 86.

² Bkz., Yksel ERSOY, Ceza hukuku Genel Hkmler, Ankara, 2002, s. 73 – 74; TOROSLU, Nevzat Ceza Hukuku Genel Kısımlar, 8. Baskı, Ankara, 2005. s. 106 – 107.

Her iki sonuç farklı etkilere sahiptir. Bu tür fiillerin tamamen yeni bir olguya işaret ettiğinin kabulü bu tür fiilleri esas alan suçların yeni ve bağımsız bir suç kategorisini oluşturduğu sonucuna götürür. Bun karşın, söz konusu fiillerin yeni ihlal şekilleri olduğunun kabulü, ceza mevzuatları içerisinde mevcut suçların bu tür fiilleri kapsayıp kapsamadığına ilişkin sorunu ortaya çıkartır. Bu durumda sorun özellikle suçun maddi unsurundadır. Bu ikinci durumda, bilişim sistemlerinin kullanımlarının çeşitli yönlerini esas alan yeni suçların ceza mevzuatlarında yer verilmesinde suçun maddi unsurunda ortaya çıkan sorunun iyi bir şekilde tespiti önemlidir. Aksi bir davranış mevcut suçlar ile yeni suçlar arasında kapsam sorununu doğurur. Bu husus, suçların içtimai bakımından da önemlidir.

Açıklanan nedenlerle, bilişim suçlarına ilişkin bir incelemede ağırlıklı olarak suçların hukuki konuları ve suçun olarak düzenlenen fiiller ön plana çıkmaktadır. Bilişim suçlarına ilişkin 5237 Sayılı TCK açısından inceleme yapılırken de bu iki nokta esas alınmıştır. Bilişim suçlarına ilişkin suçun manevi unsuruna yönelik olarak özel herhangi bir sorun ya da tartışmanın söz konusu olmaması, bu hususun ayrıntılı olarak incelenmemesi tercihini doğurmuştur. Aynı husus suçun faili ve suçtan zarar gören gibi hususlar bakımından da geçerlidir. Bu nedenle suçların incelenmesinde, söz konusu suçların hukuki konularına ve suç olarak düzenlenen fiillere ağırlık verilmiştir.

İkinci bölümün ilk konusunu, 5237 sayılı TCK'nin 243. maddesinde düzenlenen bilişim sistemine yetkisiz erişim suçu oluşturmaktadır. Bilişim sistemine yetkisiz erişim suçuna, 765 S. TCK'de yer verilmemiştir. Adı geçen Kanunda, verinin ele geçirilmesine ilişkin 525a maddesi yer almaktaydı. 5237 Sayılı TCK'de ise verinin ele geçirilmesi suçu yerine, bilişim sistemine yetkisiz erişim suçuna yer

verilmiştir. Karşılaştırmalı hukuk incelendiğinde, verinin ele geçirilmesi ve yetkisiz erişim suçlarının her ikisine de kimi mevzuatlarda yer verildiği görülmektedir. ABD, ABD’deki kimi federe devletlerin ceza mevzuatlarında bu tercih yapılmıştır. Kimi ülkelerin ceza mevzuatlarında ise tercih yetkisiz erişim suçuna yer verilmesi şeklinde olmuştur. İtalyan Ceza Kanunu ve yeni Fransız Ceza Kanundaki düzenlemeleri örnek vermek mümkündür. Buna karşın Alman Ceza Kanununda ise verinin ele geçirilmesi suçuna yer verilmiştir. Her ne kadar 5237 Sayılı Kanunda tercih yetkisiz erişim suçuna yönelik olsa da verinin ele geçirilmesi suçunun da incelenmesi, Türk Ceza Hukukunda bilişim suçlarına ilişkin düzenlemeler hakkında bilgi verilmesi bakımından önemlidir. Verinin ele geçirilmesi suçuna ilişkin olarak karşılaştırmalı hukukta ortaya çıkan, ceza hukuku bakımından verinin hukuki niteliğine yönelik tartışma ve çözümlerin bilinmesi de gereklidir. Ayrıca, “*Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı*”³’nda söz konusu suçun tekrar düzenlenmek istenmesi karşısında, verinin ele geçirilmesi suçuna ilişkin açıklamalara yer verilmesi zorunluluğu doğmuştur.

İkinci bölümde incelenen diğer bir konuyu, ceza mevzuatları içerisinde mala zarar verme suçu ile birlikte değerlendirilen ve bu kapsamda tartışılan, sistem ve veriye müdahale suçu oluşturmaktadır. Söz konusu suç, 765 Sayılı TCK’nin 525b maddesinin 1. fıkrasında düzenlenmiş iken, 5237 Sayılı TCK’de iki parçaya ayrılarak 244. maddesinin 1. fıkrasında sisteme müdahale 2. fıkrasında veriye müdahale düzenlenmiştir. Bu suçun Türk Ceza Hukukunda gelişimi açısından da 765 Sayılı TCK’nin 525b 1. fıkrasında yer alan suç hakkında da bilgi verilmesi zorunludur. Bu nedenle 765 Sayılı TCK’de yer alan suça gerekli olduğu ölçüde yer verilmiştir.

³ Tasarı için bkz., <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm>

İkinci bölümün son konusunu, karşılaştırmalı hukukta klasik dolandırıcılık suçunun unsurlarında ortaya çıkan eksikliği tamamlamak için ceza mevzuatına giren bilişim sistemi aracılığıyla yarar sağlama suçu oluşturmaktadır. Söz konusu suç, 765 Sayılı TCK'de genel olarak 525b 2. fıkra düzenlenmekteydi. 5237 Sayılı TCK'de ise 244. maddenin son fıkrasında yer almıştır. 765 Sayılı Kanunun yürürlükte olduğu dönemde en çok uygulama alanı bulan hüküm 525b 2. fıkradır. Bu hüküm nedeniyle uygulamaya ortaya çıkan sorunlar, 5237 Sayılı TCK'nin 244. maddesinin son fıkrasının düzenlenme şeklini etkilemiştir. Bu nedenle söz konusu düzenlemeye ilişkin olarak uygulamada ortaya çıkan sorunlar, Yargıtay kararları doğrultusunda ayrıntılı olarak incelenmektedir. Yukarıda adı geçen Tasarıda 765 Sayılı TCK'nin 525b 2. fıkrasında yer alan suça benzer bir düzenlemeye yer verilmek istenmesi de söz konusu hükmün incelenmesini zorunlu kılmıştır. Ayrıca, bilişim sistemleri aracılığıyla yarar sağlamaya ilişkin olarak özellikle dolandırıcılık suçu merkezinde karşılaştırmalı hukukta tartışılan bilişim sistemi aracılığıyla yarar sağlama suçunun Türk Ceza Hukukunda gelişimi ve 765 Sayılı TCK ve 5237 Sayılı TCK'deki görünümünün değerlendirilmesi açısından her iki suçun incelenmesi önemlidir.

İkinci bölümde karşılaştırmalı hukuktaki ve uluslar arası düzenlemelerden ağırlıklı olarak yararlanılmıştır. Karşılaştırmalı hukuktaki düzenlemelere ayrı bir başlık altında yer verilmesi yerine, ilgili bölümlerde incelenmesi tercih edilmiştir. Belirli bir suçun diğer devletlerin mevzuatlarında nasıl şekillendiğinin ve TCK'de yer alan düzenleme ile benzerlik ya da farklılıklarının tespitini kolaylaştırması nedeniyle bu tercih yapılmıştır. Bu kapsamda, ağırlıklı olarak ABD, İtalya, Fransa ve Alman ceza mevzuatları esas alınmıştır. Ayrıca 5237 Sayılı TCK'deki hükümlerin anlaşılabilmesi amacıyla 765 S. TCK'nun uygulanmasına yönelik olarak Yargıtay

kararlarına zorunlu olarak değinilmiştir. Bu nedenlerle ikinci bölüm, kapsam bakımından geniş tutulmuştur.

Üçüncü ve son bölümün konusu ise, bilişim sistemlerinin toplumsal hayatın tüm alanlarında girmesi ve kullanılmasıyla birlikte ortaya çıkan diğer bir sorunu kapsamaktadır. 1970’li yıllardan itibaren tartışılmaya başlanan sorunun kaynağı da dönemin özelliğini oluşturan bilgi ve enformasyonun artan öneminde yatmaktadır. Kişiyile ilgili bilgi ve enformasyonun da öneminin artması bu nitelikteki verilerin bilişim sistemleri aracılığıyla işlenmesi sonucunu doğurmuştur. Bu husus, kişiyile ilgili bilgi ve enformasyonun işlenmesi merkezinde, özel hayatın gizliliğinin korunması sorununu derinleştirerek gündeme getirmiştir.

Kişiyile ilgili bilgi ve enformasyonun yoğun olarak işlenmeye başlanması 1970’li yıllardan itibaren kişisel verilerin korunmasına ilişkin özel düzenlemelerin yapılmasına ve bunlara ilişkin suçların ceza mevzuatları içerisinde yer verilmesine yol açmıştır. 5237 Sayılı TCK’de bu gelişimden etkilenmiş ve kişisel verilerin korunmasına ilişkin suçlar TCK’nin 135 vd. maddelerinde yer almıştır.

Bilgi ve enformasyonun ayrıca bilişim altyapısının korunmasının bir etkisi olarak ikinci bölümde incelenen suçlar yanında, bilgi ve enformasyonun işlenme sürecinde özel hayatın gizliliğinin korunmasının incelenmesi de gerekmektedir. Bu hususun incelenmesi, dönemin dinamiklerinin ceza hukukuna etkisinin boyutlarının tam olarak anlaşılabilmesi bakımından zorunludur. Nitekim, kişisel verilerin korunmasına ilişkin suçlar, sosyo – ekonomik dönüşüm içerisinde bilişim sistemlerinin kullanımının etkisinin en açık şekilde hissedildiği suçlardandır. Aynı zamanda, 5237 Sayılı TCK’de, bilişim sistemlerinin kullanılmasının etkisi olarak düzenlenen suçlara ilişkin olarak, tercihin ne şekilde yansıdığı belirlenmesinde

etkilidir. Bu husus, özellikle TCK'nin sistemi bakımından önemli sonuçlar doğurmaktadır. Bu nedenlerle TCK'nin 135 vd. maddelerinde düzenlenen suçlar incelenmektedir, Söz konusu suçlar kişisel verilerin korunmasına ilişkin düzenlemelerin konusunu oluşturan kişisel verilerin işlenmesine ilişkin usul ve esaslar doğrultusunda ele alınmıştır. Kişisel verilerin işlenmesine ilişkin usul ve esasların incelenmesinde ağırlıklı olarak uluslar arası düzenlemelerden yararlanılmıştır.

Çalışmada, İnternet aracılığıyla ulaşılan veri tabanlarından, yerli ve yabancı yazılı kaynaklardan ve ayrıca Yargıtay kararlarından yararlanılmıştır.

BİRİNCİ BÖLÜM

GENEL BİLGİLER

I. BİLİŞİM– BİLİŞİM SİSTEMLERİ, BİLGİSAYAR, İNTERNET

A. Genel Olarak Bilişim – Bilişim Sistemleri

Bilişim ya da bilgisayar suçları olarak adlandırılan suçların ceza mevzuatlarına girmesi, bilişim ve bilgisayar ile ilgili birçok terime suçun unsurları arasında yer verilmesine yol açmıştır Bu durum, bilişim ve bilgisayar ile ilgili birçok terimin ceza hukukunda da kullanılmaya başlanması sonucunu doğurmuştur. Bundan dolayı, söz konusu terim ve kavramların açıklanması gerekir. Çalışmanın konusunun “*bilişim suçları*” olması, öncelikli olarak “*bilişim*” teriminin ne anlama geldiğinin belirlenmesini zorunlu kılmaktadır.

TDK sözlüğünde “*bilişim*”, “*insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi*”

olarak tanımlanmaktadır. Bilişim terimi, aynı sözlükte, Fransızca kökenli “*enformatik*”, “*informatik*” terimleri karşılığı olarak kullanılmaktadır⁴.

İlk olarak 1962 yılında, *Philippe Dreyfus* tarafından, Türkçede karşılığı bilişim olarak kullanılan “*enformatik*” terimi⁵, enformasyon ve otomatik kelimelerinin bir araya getirilmesiyle türetilmiş olup, genel olarak enformasyonun otomatik makineler aracılığıyla işlenmesi anlamındadır. Fransız Akademisi tarafından 1967 yılında, ortaya çıkan yeni bilim dalını tanımlamak amacıyla kabul edilen bu terim, Almanca “*informatik*” İngilizcede “*informatic*” ve İtalyancada “*informatica*” olarak kullanılmaktadır⁶. Bir disiplin olarak informatik ise, bilimsel enformasyonun yapısını ve özelliklerini ve aynı zamanda bilimsel enformasyonun düzeni, teorisi ve metodolojisini araştıran bir bilim dalı olarak tanımlanmıştır⁷.

⁴ Bkz., Güncel Türkçe Sözlük, www.tdk.gov.tr

Aydın, bilişimin “*bilginin ve iletişim sisteminin yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler; ve öte yandan da: bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan temel olarak alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleri*” içeren bir bilgi bilimi ve teknolojisi olarak tanımlandığını ifade etmektedir. Emin D. AYDIN, Bilişim Terimleri Sözlüğü, 1. B., 1992, s. 307.

⁵ Georges IFRAH, Rakamların Evrensel Tarihi -IX-, *Bilgisayar Ne Sayar*, (Çev. Kurtuluş Dinçer), 2. B , 2002, s. 69.

⁶ Michael FOURMAN, Informatics, s. 1. <http://www.inf.ed.ac.uk/publications/online/0139.pdf>. Ayrıca bkz., <http://www.techno-science.net/?onglet=glossaire&definition=162>, <http://en.wikipedia.org/wiki/Informatics>

⁷ Mikhailov, A.I., Chernyl, A.I., and Gilyarevskii, R.S. (1966) Informatika – novoe nazvanie teorii naučnoj informacii. Naučno tehničeskaja informacija, 12, pp 35—9; Aktaran, FOURMAN, s. 1.

Fouman bu tanımın üç yönden değiştirildiğini ifade etmektedir. İlk olarak “*bilimsel bilgi*”ye ilişkin sınırlandırmanın tanımdan çıkarılmıştır. ikinci olarak enformasyonun günümüzde yaygın bir şekilde sayısal olarak saklanması nedeniyle bilgisayar ile ilgili hesaplama (computation) merkezi hale gelmiştir. Bunun sonucunda enformatik enformasyon bilimi ve bilgisayar biliminin bir araya gelmesi olarak da tanımlanmaktadır. Son olarak, enformasyonun işlenmesi ve iletimi de dahil olmuştur. **FOUMAN**, s. 1.

Bilişim Bilimi (Enformatik), bilginin özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimidir. Bilgi işlemlerinde uygulanabilen (soyut)

Bilişim ya da Fransızca karşılığı “enformatik”in, “*enformasyonun otomatik olarak işlenmesi*” şeklinde tanımlanması karşısında, bağlantılı diğer terimlerin de açıklanması gerekmektedir. Bu kapsamda “*bilişim teknolojisi*”, “*bilişimde kullanılan bütün araç ve gereçlerin oluşturduğu sistem*”⁸ olarak tanımlanmaktadır. Üzerinde durulması gereken diğer bir terim ise, bilişim teknolojisi içerisinde ele alınabilen “*bilişim sistemi*”dir.

Headrick, bilgi ya da enformasyonun otomatik olarak işlenmesine yarayan bilişim sistemlerinin de dahil olduğu enformasyon sistemlerini, geniş anlamda, insanların enformasyonu düzenleyip idare ettikleri sistem olarak tanımlamaktadır. Yazara göre; enformasyon sistemleri birbiriyle iç içe geçebilmekle ve birden fazla işlev görebilmekle birlikte, söz konusu sistemlerin sınıflandırılmaya tabi tutulmaları mümkündür. Bu açıdan enformasyon sistemlerinin, enformasyonun toplanmasına ilişkin sistemler (araştırmacılık, gazetecilik, araştırma laboratuvarları faaliyetleri, anketler vs.), enformasyonun miktarıyla doğru orantılı olarak artan bunların adlandırılması, düzenlenmesi ve sınıflandırılmasına ilişkin sistemler (kütüphanecilikte kullanılan dewey sistemi vs.), enformasyonun dönüştürülmesine ilişkin sistemler (istatistik vs.), enformasyonun saklanmasına ve arandığında kolay bir şekilde bulunmasını sağlayan sistemler (sözlük, ansiklopedi vs.) ve son olarak

matematiksel yapıları inceler. Amacı ve görevi bir yandan (saf matematiğin alt dalı olarak) temel aksiyomatik matematiksel teoriler üretmek (Kuramsal Bilişim Bilimi), ikinci olarak - yardımcı bilim şeklinde- tüm diğer uzmanlık dallarının nesnelerini ve süreçlerini çözümleyip soyut matematiksel yapılara ve Algoritmalara dönüştürmek (Bilgisayar Bilimi) ve üçüncü olarak soyut matematiksel yapıların aktarılabilceği, saklanabilceği ve algoritmalarla otomatik olarak işlenebileceği matematiksel makinaları tasarlamaktır (Teknik Bilişim ya da Bilgisayar Mühendisliği). <http://tr.wikipedia.org/wiki/Bili%C5%9Fim>

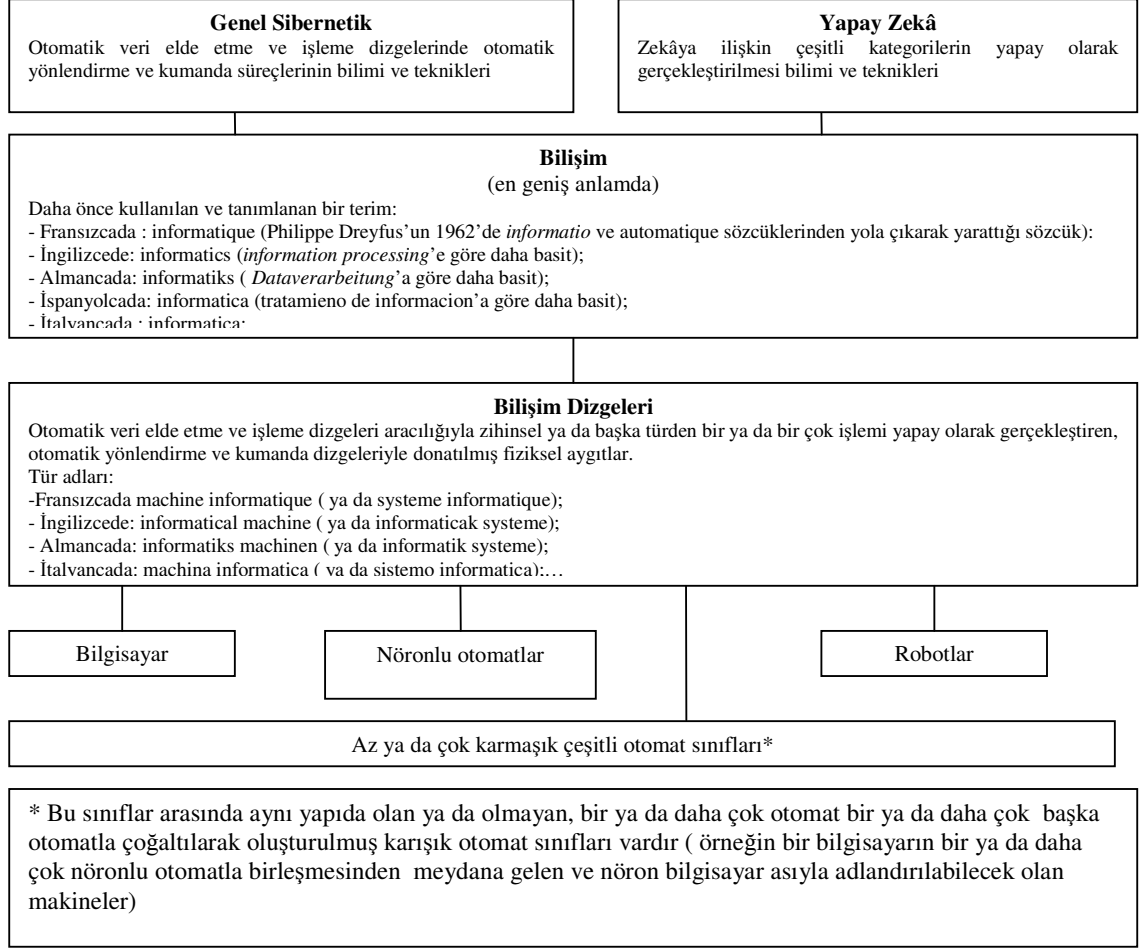
⁸ Bkz. <http://www.tdk.gov.tr>

enformasyonun iletilmesiyle ilişkili sistemler (posta hizmetleri, gazete, radyo, İnternet) olarak sınıflandırılabilir⁹.

Yazarın enformasyon sistemleri olarak incelediği ve sınıflandırdığı sistemlerin bilişim tanımının ve bilişim teknolojisinin kapsamının ötesinde geniş bir anlam ve kapsama sahip olduğu görülmektedir. Bilişimin Fransızca tanımında yer alan “*otomatik makineler aracılığıyla işleme*” unsuru ile birlikte düşünüldüğünde, bilişim sistemleri, enformasyon sistemlerinin bir kısmına işaret etmektedir. Bu doğrultuda bilişim sisteminin, yukarıda aktarılan sınıflandırma içerisindeki her türlü işlevi içerebilmekle birlikte, sadece “*enformasyonun otomatik makineler aracılığıyla ve otomatik olarak işlenmesini sağlayan sistemler olarak*” tanımlanması mümkündür. Görüleceği üzere bu tanım işlevsel olmaktan çok araçsal bir tanımdır. Bu husus, aşağıdaki şemada daha iyi anlaşılabilir.

⁹ Daniel R. **HEADRICK**, Enformasyon Çağı, Akıl ve Devrim Çağında Bilgi Teknolojileri 1700 – 1850, Çev. Zülal Kılıç, 1. B., İstanbul, 2002, s. 13 – 15; Ayrıntılı bilgi için ayrıca bkz., Stephen **SAXBY**, The Age of Information : The Past Development and Future Significance of Computing and Communications, London : Macmillan, 1990, s. 41 vd.

Genişletilmiş bilişim makineleri¹⁰



Bilişim ile ilgili diğer bir terim ise, “*bilişim ağı*”dır. TDK Sözlüğünde bilişim ağı, “*teknik, ekonomik ve toplumsal alanlardaki iletişim sistemi*” şeklinde tanımlanmış olup, bu tanımın bilişim tanımı ile birlikte değerlendirilmesi gerekmektedir. Bu nedenle, bilgi ya da enformasyonun elektronik makinelerle işlenmesi bilişimin ana unsuru olarak ortaya çıkması sonucunda, bilişim ağının da,

¹⁰ **IFRAH**, s. 69. “*Robot*”, genel olarak, “*Sibernetik*” çalışmaları kapsamında olup, insanın yerine belirli işleri görmek üzere yapılmış, kendilerini çevrelerine uyarlama yeteneğiyle donatılmış mantık otomatını ifade etmektedir. “*Nöronlu otomatlar*”, önceden kendine verilmiş bilgileri kullanarak kendini yeniden düzenleyen ve uyarlayan sistem anlamına gelmektedir. Sinir sistemini taklit eden bu otomatlar, “*nöron*” (sinir hücresi) denen ve bellek, aktarım, karmaşık ilişkiler kurma işlevleri olan, bir iç ilişkiler ağıyla birbirine bağlı çok büyük sayıda temel organdan oluşmuştur. **IFRAH**, s. 67 – 68

araçsallığa yapılan vurgu ile özellikle elektronik makine olarak bilişim sistemlerinin birbirine bağlanması suretiyle iletişim olarak düşünülmesi mümkündür¹¹.

Bilişimin, genel olarak bilgisayarın gelişimi ile aynı dönemlerde ortaya çıkan bir terim, bilgisayarın da bilgi ya da enformasyonun işlenmesinde en yaygın kullanılan araç olması, bilişimin kendisinin bilgisayar ile birlikte anılması ve birbirine bağlantılı olarak tanımlanması sonucunu doğurmuştur¹². Aynı şekilde, bilişim, bilgi toplumu ya da enformasyon toplumu gibi birçok adla adlandırılan dönüşümün kendisinin de, bilgisayar sistemlerinin kullanımını ve etkisini esas alan incelemelere konu olması sonucunu doğurmuştur. Nitekim, “*Türkiye Bilişim Şûrası*”nda, bilgi toplumu olarak adlandırılan dönüşümün, genel olarak bilişim sistemi olarak bilgisayar sistemlerinin gelişimi açısından değerlendirilmesinde, bu etkiyi görmek mümkündür¹³. Ayrıca, bilişimin kendisinin bilgisayar ile bağlantılı olarak ele alınmasına ilişkin izleri, “*Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı*”nında da yer bulmuştur. Tasarının 2. maddesinin “d” bendinde “*bilişim sistemi*”ne ilişkin, bilgisayar ile bağlantılı olarak, “*bilgisayar, çevre birimleri, iletişim altyapısı ve yazılımlardan oluşan veri işleme, saklama, iletmeye yönelik sistem*” tanımına yer verilmiştir¹⁴.

¹¹ “*Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı*”nın 2. maddesinin “e” bendinde bilişim ağı, “*en az iki bilişim sistemi arasında veya bir bilgisayar ile bir çevre birimi arasında veri iletişimini ve karşılıklı etkileşimi her türlü iletişim tekniği ile sağlayan ortam*” şeklinde tanımlanmaktadır. <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm>

¹² Örnek olarak bkz., Yılmaz **YAZICIOĞLU**, Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları İle, 1. B. 1997, s. 130 – 131; Michael S. **MAHONEY**, *The History of Computing in the History of Technology*, Annals of the History of Computing, Volume 10, Number, 2, 1988, s. 113. <http://web.mit.edu/STS.035/www/PDFs/mahoney.pdf>

¹³ Türkiye Bilişim Şûrası, Ankara, 2002, s. 7 vd.

¹⁴ Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm>

Bir bilişim sistemi olarak bilgisayarın yaygınlaşması ve etkin bir şekilde kullanılması, bilişim suçları şeklinde adlandırılan suçların, bilgisayarın kullanımı ile bağlantılı olarak ortaya çıkması ve bilişim suçlarının bilgisayar sistemlerinin kullanımının belirli yönlerinin esas alınması suretiyle düzenlenmesi sonucunu doğurması nedeniyle, bir bilişim sistemi olarak bilgisayara ve İnternete ayrıca değinilmesi gerekmektedir.

B. Bilişim Sistemi Olarak Bilgisayar

Bilişimde en önemli araç olarak ve yeri geldiğinde bilişim ile bütünleşen bilgisayar sistemleri, gündelik yaşamın her alanında kullanılmakta ve kullanımını giderek yaygınlaşmaktadır. Bunun ötesinde, bilgisayar sistemleri, aşağıda kısaca açıklanacağı üzere, sosyo – ekonomik dönüşümün teknik altyapısı olarak her alanda etkin bir şekilde kullanılmakta ve bu etkinlik giderek artmaktadır.

Bilgisayarın tarihi açısından, bir çok başlangıç noktasına işaret edilmekle birlikte, üzerinde uzlaşmaya varılmış kesin bir başlangıç noktasının verilmesi mümkün gözükmemektedir. Nitekim, İngilizce “*computing*” (hesaplama) sözcüğünden türetilmiş olan “*computer*” (bilgisayar) tarihi, hesaplamada kullanılan araçların icadı ile birlikte de açıklanmaktadır¹⁵. İlk elektronik ve genel amaçlı

¹⁵ Örnek ve bilgisayarın tarihi gelişimi için bkz, Bkz. An Overview Of Computational Science, “3 A Brief History of Computer Technology”

http://www.ipp.mpg.de/de/for/bereiche/stellarator/Comp_sci/CompScience/csep/csep1.phy.ornl.gov/ov/node8.html#SECTION00030000000000000000;

“Timeline of Computing History”
http://www.computer.org/portal/cms_docs_computer/computer/timeline/timeline.pdf ;

Maggie JOHNSON, Background and History, s. 3.
<http://cse.stanford.edu/class/cs103a/h2Background.pdf>; The Journey InsideSM: History of Computers http://www97.intel.com/discover/images/tji/TJI_Intro_back.pdf; *Bilgisayar Aşkımız 60 Yaşında*, Bilişim, Yıl 35, S. 93, 20 vd.

bilgisayar ise, 1945 yılında ABD’de üretilen, ENIAC (Electronic Numerical Integrator and Computer) adlı bilgisayardır¹⁶. ENIAC, modern bilgisayarın ya da bilgisayar teknolojisinin başlangıcı olarak ifade edilmiştir¹⁷.

TDK Sözlüğünde bilgisayar, “çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin” olarak tanımlanmaktadır¹⁸.

Bilgisayarın bir elektronik beyin olarak adlandırılmasına karşı çıkan Ifrah, bilgisayarı, “bir giriş – çıkış aygıtı, bir karakter zincirleri biçiminde dile getirilmiş veriler üzerinde her türlü dönüştürme işlemini yapabilen bir işletim organından oluşan; fiziksel olanakların sınırları içerisinde her türlü simgesel hesabı yapabilen (dolayısıyla çözümü bir algoritma biçiminde dile getirilebilen her türlü problemi çözebilen); bütün bunları da belleğe kaydedilmiş programlarla yönetilen (dolayısıyla işlenecek verilerle aynı şekilde gerçekleştirilecek yönergeler kullanan) bir kumanda organının denetiminde yapan yapay bir otomat” olarak tanımlamıştır¹⁹.

Bilgisayarın tarihi ile ilgili olarak ayrıca bkz., Luciano **FLORIDI**, Philosophy and Computing: An Introduction, Routledge, 1999, s. 21 vd; Mustafa **TOPALOĞLU**, Bilişim Hukuku, 1. B., 2005, s. 1 – 2.

¹⁶ An Overview Of Computational Science, “3.2 First Generation Electronic Computers (1937-1953)”

http://www.ipp.mpg.de/de/for/bereiche/stellarator/Comp_sci/CompScience/csep/csep1.phy.ornl.gov/ov/node10.html#SECTION00032000000000000000

¹⁷ Bkz., **YAZICIOĞLU**, Bilgisayar Suçları, s. 33 – 34; A.Caner **YENİDÜNYA** – Olgun **DEĞİRMENCİ**, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, 1. B., 2003, s. 13 – 14.

¹⁸ Güncel Türkçe Sözlük, <http://www.tdk.gov.tr>.

¹⁹ **IFRAH**, s. 38.

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı’nın 2. maddesinin “e” bendinde bilgisayar, “belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçlar” şeklinde tanımlanmaktadır.

Bilgisayarın çok çeşitli tanımları yapılabilmesi mümkündür²⁰. Yukarıda aktarılan tanımlar ise, bilgisayarın yapısı, işleyiş şekli ve unsurları hakkında genel bir bilgi vermektedir. Bu kapsamda bir bilgisayardan bahsedilebilmesi için öncelikli olarak fiziksel bir yapısının yani donanımının olması gerekir. Bu yönüyle bilgisayar, elektronik bir araç olarak karşımıza çıkmaktadır. Merkezi işlem birimi (CPU) , Salt okunur bellek (ROM, read only bellek), rastgele erişimli bellek (RAM, random Access memory), çevre birimleri (giriş, çıkış birimleri input-output) bilgisayarın fiziksel yönünü yani donanımını oluşturmaktadır²¹. Bilgisayarın diğer bir yönü ise, verilen işi ya da girilen problemi bir program aracılığıyla yapabilmesi ve çözebilmesidir. Bu ise, bilgisayarın yazılım yönüne işaret etmektedir. İşin yapılması ya da belirli bir algorithmaya göre problemin çözülmesi anlamında bir görevin nasıl yerine getirileceğine ilişkin yönerge olarak program, bilgisayarın yazılım unsurunu gündeme getirmektedir. İşletim sistemi olarak adlandırılan yazılım, bilgisayarın genel olarak işlev görebilmesini sağlayan bir program olarak karşımıza çıkarken; uygulama programı, bir ya da birden fazla işlevin yerine getirilmesine yarayan program olarak tanımlanmaktadır²². Bunun yanında, bilgisayara verilen görevin belirli bir şekilde kodlanması gerekmekte; bu ise, bilgisayar verisini gündeme

²⁰ Tanımlar için bkz., Levent **KURT**, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınevi, 1. B., Ankara, 2005, s. 27 – 31; **TOPALOĞLU**, Bilişim Hukuku, s. 1; **YENİDÜNYA**, **Bilişim Suçları**, s. 17 vd; **AYDIN**, Bilişim Terimleri Sözlüğü, s. 123.

²¹ Tanımlar için bkz., **YENİDÜNYA**, **Bilişim Suçları**, s. 23 – 24; **KURT**, **Bilişim Suçları**, s. 31 – 34; Murat Volkan **DÜLGER**, Bilişim Suçları, 1. B., Ankara, 2004, s. 38 – 40; **TOPALOĞLU**, Bilişim Hukuku, s. 3; **YAZICIOĞLU**, **Bilgisayar Suçları**, s. 31.

²² Tanımlar için bkz., **YENİDÜNYA**, **Bilişim Suçları**, s. 23, 24; **KURT**, **Bilişim Suçları**, s. 34 – 36, 39; **DÜLGER**, Bilişim Suçları, s. 40 – 41; **TOPALOĞLU**, Bilişim Hukuku, s.4 vd; **YAZICIOĞLU**, **Bilgisayar Suçları**, s. 31 – 32.

getirmektedir²³. TDK Sözlüğünde bilişimde veri, “*olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi*” anlamındadır. Aynı sözlükte veri karşılığı olarak “*data*” ve “*bilgi*” de kullanılmaktadır²⁴. Avrupa Konseyi Sıbersuç Sözleşmesinde ise, bilgisayar verisi, “*bilgisayar sisteminin herhangi bir işlevi gerçekleştirmesine neden olan programı da içermek üzere, olgu, enformasyon ya da kavramların bilgisayar sistemleri içerisinde işlenmeye uygun bir biçimde temsili*” olarak tanımlanmıştır²⁵.

Bilgisayarların yaygın olarak kullanılmaya başlanmasının ceza hukuku bakımından etkisi, sosyo – ekonomik dönüşümün alt yapısı olarak kullanılması açısından, bilgisayarlarla ilgili çeşitli fiillerin suç olarak düzenlenmesi şeklinde kendini gösterir. 765 Sayılı TCK’de ve TCK’de “*bilişim alanında suçlar*” başlığı altında düzenlenen suçlar da genel olarak bilgisayarların kullanımı ile ilgili çeşitli fiillerin esas alınarak cezalandırıldığı suçları içermektedir.

ABD ve İngiltere’de bilgisayarlar ile ilgili suçların düzenlenmesinde suçun unsurlarının belirlenmesi bakımından, “*computer*” terimi tercih edilmiştir. Buna

²³ Tanımlar için bkz., YENİDÜNYA, **Bilişim Suçları**, s. 47 – 48; DÜLGER, **Bilişim Suçları**, s. 48 – 50; KURT, **Bilişim Suçları**, s. 37 – 39; YAZICIOĞLU, **Bilgisayar Suçları**, s. 227.

²⁴ Güncel Sözlük, <http://www.tdk.gov.tr/>

²⁵ Tanım için bkz, “*Avrupa Konseyi Sıbersuç Sözleşmesi*”, 1/b maddesi.

<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

Her ne kadar günlük dilde bilgi ve enformasyon ya da veri ayırımı yapılmamasına rağmen, birbirleriyle bağlantılı olmakla birlikte farklı kavramlardır. TDK sözlüğünde “bilgi” sözcüğü ile ilgili olarak çeşitli tanımlar verilmektedir. Nitekim Sözlükte yer alan diğer anlamlar yanında bilgi, “*insanın aklının erebileceği, olgu, gerçek ve ilkelerin bütünü*”; “*insan zekasının çalışması sonucu ortaya çıkan, düşünce ürünü*”; “*bilişimde kurallardan yararlanılarak kişinin veriye yönelttiği anlam*” olarak tanımlanmaktadır. Aynı Sözlükte enformasyon için danışma, tanıtma; haber alma, haberleşme tanımları yapılmıştır. Yukarıda aktarıldığı üzere veri de farklı bir tanıma sahiptir. Nitekim *Headrick* bilgi ve enformasyon ayırımına değinmekte ve bilginin insanın aklının kavradığı ve içselleştirdiği düşünce ve verilerle ilgili bir kavram olduğunu belirtmektedir. Bilgi edinmek için beyne çok miktarda enformasyonun yığılması gerekir (*HEADRICK*, s. 13.) Özellikle enformasyon hakkında bkz, *IFRAH*, s. 73 vd.

karşın, Fransa’da bilgisayar karşılığı olarak “*ordinateur*” sözcüğü kullanılmakla birlikte, Fransız Ceza Kanununda, “*verileri otomatik işleme tabi tutan sistem*” ifadesi yer almıştır. İtalyada ise bilgisayar terimi karşılığı olarak “*elaboratore*”, “*elaboratore elettronico*” kullanılmakla birlikte, Kanunda “*informatico*”, ve “*telematico*” sözcükleri tercih edilmiştir. Alman Ceza Kanununda ise, genel olarak veri ver veri işleme terimleri kullanılırken bilgisayar terimi de kullanılmıştır. Avrupa Konseyi Sıbersuç Sözleşmesinde ise bilgisayar terimi kullanılmıştır²⁶. 765 Sayılı TCK’de, söz konusu hükümlerin aktarıldığı Fransız Ceza Kanununda yer alan ifadeden etkilenilmiş, veri sözcüğü yerine bilgi sözcüğü kullanılarak “*bilgileri otomatik işleme tabi tutan sistem*” ifadesi kullanılmıştır. TCK’de ise “*bilişim sistemi*” ifadesi yer almaktadır.

765 Sayılı TCK’de yer alan “*bilgileri otomatik işleme tabi tutan sistem*” ifadesi yerine, 5237 Sayılı TCK’de “*bilişim sistemi*” ifadesinin kullanılmış olması karşısında, bu iki ifadenin farklı olup olmadığı da gündeme gelmiştir. Kanunun gerekçesinde bilişim sistemi, “*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir*” şeklinde açıklanmaktadır. Gerekçede yer alan tanım, 765 Sayılı TCK’de yer alan bilgileri otomatik işleme tabi tutan sistem ifadesinden, verilerin toplanıp yerleştirilmesi ve sistemin manyetik olması bakımından farklılık göstermektedir. TDK Sözlüğünde *bilişim* açısından “*manyetik*”, “*yüzeyine manyetik kayıt yoluyla bilginin depolanabildiği müknaıslanabilir kaplaması olan plak şekilli tabaka*” olarak tanımlanmaktadır.

²⁶ Sıbersuç Sözleşmenin 2. maddesinin “a” bendine göre bilgisayar sistemi, bir veya birden fazlası, belirli bir programa göre verinin otomatik olarak işlenmesini gerçekleştirebilen, herhangi bir aygıt ya da birbirine bağlı ya da birbiriyle ilgili bir grup aygıt olarak tanımlanmaktadır. Bkz., <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

Madde gerekçesindeki tanımda yer verilen, sistemin manyetik olması, tanımı, kapsam ve içerik bakımından sınırlandırmaktadır. Bu nedenle madde gerekçesi esas alındığında, manyetik olmayan fakat tanımda yer verildiği diğer işlemleri yapabilen bir sistem, bilişim sistemi kapsamına girmemektedir.

Bunun yanında doktrinde, 765 Sayılı TCK'de yer alan "*bilgileri otomatik işleme tabi tutan*" sistem teriminin bilgisayarı da kapsayan fakat bilgisayardan daha geniş bir anlama sahip olduğu ifade edilmiştir²⁷. Aynı zamanda bilişim sisteminin de, bilgileri otomatik işleme tabi tutan sisteme göre, daha geniş bir anlam taşıdığı vurgulanmıştır²⁸. Bilgileri otomatik işleme tabi tutan sistemin kapsamının ne olduğu yargı kararlarına da konu olmuştur. Yargıtay 4. Ceza Dairesi, muhasebe şefi olan sanığın, bilgisayara yanlış veri vererek (input) maaşındaki kesintiyi olduğundan fazla göstermesine ilişkin eylemin nitelendirilmesinde; 765 Sayılı TCK'nin 525/a vd. maddelerinde düzenlenen sistemin, dar anlamda fiziki olarak bir bilgisayar anlamına geldiğinin kabulü halinde, sonradan yanlış girilen verilerin sistem içinde sayılamayacağını ve 765 Sayılı TCK'nin 240. maddesinde yazılı suç oluşturacağı; sistemin, girilen verileri (input) de kapsayacak

²⁷ **YENİDÜNYA - DEĞİRMENCİ**, s.44 -45; **YAZICIOĞLU, Bilgisayar Suçları**, s. 224 – 225; **DÜLGER**, s. 45.

²⁸ **DÜLGER**, s. 46; Bilgisayarın sadece veri işleme işlevine sahip olması, bilişim sisteminin ise, veri işleme yanında veri iletme işlevine de sahip olması, *Yenidünya ve Değirmenci*'ye göre bilişim sistemi ve bilgisayar arasındaki farkı oluşturmaktadır. Bkz., **YENİDÜNYA - DEĞİRMENCİ**, s. 31; **YAZICIOĞLU, Bilgisayar Suçları**, s. 224. Yargıtay ise, şifreli yayınların çözülmesinde kullanılan şifre çözme cihazını ve telsiz telefonunu bilgileri otomatik işleme tabi tutmuş sistem olarak kabul etmemiştir. Bkz., **Yargıtay CGK. E. 1996/6-151 K. 1996/152 T. 25.6.1996**, <http://www.kazanci.com.tr/kho2/ibb/files/cgk-1996-6-151.htm> ; **Yargıtay 6. CD., E. 1997/8266, K. 1997/8841, T. 9.10.1997**, <http://www.kazanci.com.tr/kho2/ibb/files/6cd-1997-8266.htm>, *Yazıcıoğlu*, şifre çözme cihazlarının belirli bir açıdan bilgisayar olduğunu ifade etmekle birlikte bilgileri otomatik işleme tabi tutmuş sistemin, genel amaçlı, tek yönde veya tek düze olmayan bilgi – işlem yeteneğine sahip cihaz olması gerektiğini, bu hususun şifre çözme cihazında eksik olduğunu vurgulamaktadır. Ayrıntılı bilgi için bkz., **YAZICIOĞLU, Bilgisayar Suçları**, s. 217 – 219.

biçimde, bilişim sistemi olarak kabulü durumunda ise, 525/b maddesindeki suç oluşturacağı kanaatine varmıştır²⁹.

Öncelikli olarak belirtmek gerekir ki, bilişim bilimsel bir terimdir; bilgi ya da enformasyonun özellikle elektronik araçlarla otomatik olarak işlenmesine ilişkin sürece işaret etmektedir. Bu açıdan bilişim sistemi terimi, yukarıda aktarıldığı ve şemada örnek olarak gösterildiği üzere, bilgisayardan daha geniş bir anlama sahiptir. TCK'nin 243. vd. maddelerinde belirtildiği şekliyle bilişim sistemi terimi de, bir bilim dalı olarak bilişimden alınmıştır. Bu durumda, maddelerde yer alan bilişim sisteminin, otomatik yani insan müdahalesi olmadan işlem yapabilmesi önemli hale gelmektedir. Aynı şekilde, 243 vd. maddelerde, veriden bahsedilmesi karşısında sistemin veri işleyebilmesi de gerekmektedir. Bu unsurları taşıyan bir sistemin, bilişim sistemi olarak kabul edilebileceğini söylemek mümkündür³⁰. Gerekçede yer alan, sistemin manyetik olması, ise zorunlu bir unsur olarak kabul edilmemelidir.

Doktrinde genel olarak, bilgisayarın ve bilişim sisteminin, diğer belirli düzeyde veri işleyebilen araçlardan ayırt edilebilmesi için, genel amaçlı kullanılabilme özelliği de eklenmektedir³¹. Bu husus, özellikle belirli fonksiyonların yerine getirmesi için mikroçiplerin yerleştirildiği araçlar bakımından önemlidir. Bu tür araçlarda, genel olarak bilgi ya da enformasyonun işlenmesi yerine, belirli işlemlerin otomatik olarak yapılması esas olduğundan, söz konusu görüşe katılmak mümkündür.

²⁹ **Yargıtay 6. CD., 4212 E., 4966 K. 9.6.1998 T.,** Aktaran, İsmail **MALKOÇ,** Açıklamalı Türk Ceza Kanunu, Ankara, 2002, s. 5063.

³⁰ Tasarının 2. maddesinde ise bilişim sistemi bilgisayar ile bağlantılı bir şekilde tanımlanmaktadır. Nitekim 2. maddenin d bendinde, bilişim sistemi, bilgisayar, çevre birimleri, iletişim altyapısı ve yazılımlardan oluşan veri işleme, saklama, iletmeye yönelik sistem, olarak tanımlanmaktadır. <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm>

³¹ **YAZICIOĞLU, Bilgisayar Suçları,** s. 27, 218; **KURT, Bilişim Suçları,** s. 141.

*C. Bilişim Sistemi Olarak İnternet*³²

1. Kavram, Tarihçe

Bilişim sistemleri ve özellikle bilgisayar sistemlerinin, birbirleriyle iletişim kurabilmesi ya da bilişim sistemleri aracılığıyla iletişim kurma isteği, birden çok bilgisayarın teknik bazı protokollerle birbirine bağlanması olgusunu doğurmuştur. Bilgisayar ağı ya da bilişim ağı olarak adlandırılabilen bu olgu, genel olarak, veri işleme faaliyeti merkezinde çalışan bilgisayar sistemlerinin, veri iletimi esaslı, elektronik iletişim olanaklarını kazanması anlamına gelmektedir.

Birden çok bilgisayar sisteminin çeşitli şekillerde birbirine bağlanması anlamında bilgisayar ya da bilişim ağı, kendisine bağlanan bilgisayarların sayısı ya da nitelikleri bakımından bir çok ad almaktadır. Bilgisayarların coğrafik olarak birbirine yakın olduğu bağlantı tipleri yerel ağ (LAN) olarak adlandırılmakta, bunun yanında coğrafi konum olarak birbirinden uzakta bulunan bilişim sistemleri arasında bağlantı kurulması ise geniş alan ağı (wide area network “wan”) olarak adlandırılmaktadır.³³

İnternet ise, teknik olarak birden çok bilgisayarın ve bilgisayar ağlarının birbirine bağlanmasına dayalı bir iletişimi öngören bilişim – iletişim ağıdır³⁴.

³² İnternetin tarihi, yapısı ve işlevleri hakkında kısa açıklamalarla yetinilecek olup ayrıntılı bilgi için bkz. Katie **HAFNER** – Matthew **LYON**, İnternet Tarihi: Sihirbazların Gecelediği Yer, (Çev. Sinem Yazıcıoğlu), 1. B., İstanbul, 2000; **FLORIDI**, s. 56 vd. ; **İÇEL –ÜNVER**, s. 465 vd; Gordon **GRAHAM**, The Internet: A Philosophical Inquiry, Routledge, 1999, s. 22 vd. (Ebrary); Hasan **SINAR**, İnternet ve Ceza Hukuku, 1. B., İstanbul, 2000, s. 21 vd.

³³ <http://www.webopedia.com/TERM/n/network.html>, Ayrıca bkz., **YENİDÜNYA – DEĞİRMENCİ**, s., 34-36.

³⁴ **İÇEL –ÜNVER**, s. 465.

Özellikle bilgisayar ağlarına dayalı olarak çalışan İnternet teknik bir araç olmaktan öteye gitmemekte birlikte, İnternetin günümüzde yaygın bir iletişim ağı olarak kullanılmaya başlanması ve her geçen gün yaygınlaşması sonucu önemini artmış ve çeşitli yönleriyle tartışılan bir olgu haline gelmiştir.

Floridi, İnternetin gelişimini genel olarak üç aşamada incelemektedir. Yazar, birinci aşamayı 1968-84 yıllarını kapsayan “buluş”, ikinci aşamayı, “reform”, üçüncü aşamayı ise “yayılma” aşaması olarak adlandırmaktadır³⁵. Birinci aşama, bir savaş durumunda askeri ve idari kurumların birbirleriyle olan iletişiminin kopmamasının sağlanması fikriyle ortaya çıkmıştır. Bu fikir, karakteristik özelliğini, merkezi yapıda olmayan bir iletişim sisteminin kurulması ve bu bunun bilgisayar temelli olmasında göstermektedir. Bu amaca hizmet etmek üzere 1968 yılında ABD’nin ARPANET olarak adlandırılan bir projeyi destekleme kararı alması, İnternetin doğuşu anlamına gelmektedir. Bu proje kapsamında ARPANET, herhangi bir nükleer saldırı sonrasında bile bir iletişim sisteminin ayakta kalmasını sağlayacak bir ağı oluşturulmasına yönelik bir yapı olarak öngörülmüştür. Bu ağı temel özelliği ise, merkezi ve hiyerarşik bir yapısı olmamasıdır. Bu dönem içerisinde bilgisayar sistemlerinin birbiriyle bağlantı kurabilmesini sağlayan teknolojilerin gelişimi, TCP/IP protokolü, enformasyonun gönderildiği hedefe ulaşabilmesi amacıyla küçük paketlere ayrılması ve öngörülen hedefe bu şekilde gönderilmesi anlamına gelen paket anahtarlama³⁶ teknolojisi, alan adı sistemi bugünkü anlamıyla İnternetin altyapısının oluşturulması anlamında önemli adımları oluşturmaktadır³⁷.

³⁵ **FLORIDI**, s. 56

³⁶ Bkz., TDK, “**Bilgisayar Terimleri Karşılıklar Kılavuzu**”, <http://tdk.org.tr/bilterim/>

³⁷ **FLORIDI**, s. 56 - 59. Barry M. **LEINER** - Vinton G. **CERF** - David D. **CLARK** - Robert E. **KAHN** - Leonard **KLEINROCK** - Daniel C. **LYNCH** - Jon **POSTEL** - Larry G.

Bu dönem içerisinde askeri amaçlı kullanım amacıyla “MILNET” adı altında yeni bir ağ kurulmuş ve askeri amaçlı faaliyetler bu ağa taşınmıştır. Ayrıca ARPANET gibi bir çok ağ, bu dönem içerisinde ortaya çıkmıştır³⁸. Bu dönem içerisinde İnternet, kuruluş amacına hizmet edecek şekilde askeri kimliği baskın olmakla birlikte akademik bir kimlik de kazanmıştır.

Floridi’nin reform aşaması olarak ifade ettiği 1984-95 yılları arasında, İnternetin özellikle ticari alanda kullanılması gündeme gelmiştir³⁹. 1995 yılı ve sonrasında ise, İnternet, günümüzde yaygın şekilde kullanılan, ağ halini almıştır. 1990’lı yıllarda ticari ve eğitim amaçlı İnternet servis sağlayıcıların ortaya çıkması 1995 yılında NSFNET aracılığıyla yürüten alan adları hizmetlerinin serbest bırakılması bu süreci tamamlayan bir unsurlardır⁴⁰.

Günümüzde ağırlıklı olarak bilgisayar ağlarından oluşan İnternetin temel işlevi, ağ içerisinde etkileşimli/çift yönlü (interaktif) veri aktarımıdır⁴¹. Bu haliyle de İnternet bireysel ve kitle iletişim aracı olarak kullanılabilir. Klasik kitle iletişim araçlarından farklı olarak tek yönlü iletişim yerine etkileşimli/ çift yönlü bir iletişime olanak sağlaması ise İnterneti klasik kitle iletişim araçlarından ayırmaktadır. İnternet aracılığıyla iletişim ise dosya transfer protokolü (ftp), http

ROBERTS - Stephen **WOLFF**, A Brief History of the Internet, “*The Initial Internetting Concepts*”, “Proving the Ideas”, <http://www.isoc.org/internet/history/brief.shtml>

³⁸ **LEINER**, A Brief History of the Internet, “*Transition to Widespread Infrastructure*”. <http://www.isoc.org/internet/history/brief.shtml#Transition>; **SINAR**, s. 22- 23.

³⁹ **FLORIDI**, s. 59 – 60. **LEINER** A Brief History of the Internet, “*Commercialization*”, <http://www.isoc.org/internet/history/brief.shtml>

⁴⁰ **FLORIDI**, s. 60 – 61, **İÇEL - ÜNVER**, s. 474. Türkiye’de İnternet’e ilk bağlantı ise 12 nisan 1993’de Ankara-Washington 64K’lık bağlantı ile gerçekleştirilmiştir. Mustafa **AKGÜL** (der.), Türkiye İnternetinin ve İnternet Kurulunun Kısa Tarihi, <http://kurul.ubak.gov.tr/dok20.htm>.

⁴¹ **İÇEL - ÜNVER**, s. 476, **FLORIDI**, s. 63

protokolü, e-mail protokolü gibi çok çeşitli iletişim kanalları ile gerçekleştirilmektedir⁴².

Uluslar arası bir iletişim ağı niteliğini kazanan ve bir çok avantajı beraberinde getiren İnternet, aynı zamanda suç oluşturan bir çok fiilin gerçekleştirilmesi için uygun bir zemin de sağlamıştır⁴³. Özellikle, uluslar arası bir iletişim ağı olması nedeniyle, İnternet, bir çok fiilin uluslar arası nitelik kazanmasına neden olmuştur. Günümüzde çocuk pornografisi, ırkçılık ve yabancı düşmanlığına ilişkin fiiller İnternetin kullanımının yaygınlaşmasına paralel olarak en çok tartışılan sorunları oluşturmaktadır. Nitekim aşağıda aktarılacağı üzere, içerikle ilgili suçlar başlığı altında incelenen çocuk pornografisi ve ırkçılık ve yabancı düşmanlığı Avrupa Konseyi Siber Suçlar Sözleşmesinin ve de bu sözleşmeye ek protokolün konusunu oluşturmuştur. Bunun yanında İnternet bir iletişim aracı olarak birçok fiilin işlenmesinde de kolaylık sağlamaktadır.

İnternetin kullanımının yaygınlaşması bir yandan bir iletişim aracı olarak İnternetin hukuki bir düzenlemeye tabi tutulması diğer bir yandan da İnternet sùjeleri olarak da adlandırılan ve verinin internet üzerinden iletilmesinde çeşitli şekilde rol üstlenen kişilerin sorumluluğuna ilişkin düzenlemelerin yapılmasını gündeme getirmiştir. Bireysel haberleşme (iletişim) ve kitle haberleşmesi (iletişim) aracı olarak kullanılabilen İnternetin⁴⁴ özellikle kitle haberleşme aracı olarak kullanılması

⁴² İnternetin gelişimi, yapısı ve işlevleri hakkında ayrıntılı bilgi için bkz, **SINAR; İnternet ve Ceza Hukuku**, s. 33 vd. Murat Volkan **DÜLGER**, Bilişim Suçları, 1. B., Ankara, 2004, s. 50 vd.

⁴³ Fatih S. **MAHMUTOĞLU**, *Karşılaştırmalı Hukuk Bakımından İnternet Sùjelerinin Cezai Sorumluluğ*, İHFM, C. LIX, S. 1-2, 2001, s. 39.

⁴⁴ Haberleşme bir yönüyle yukarıda aktarıldığı şekliyle ayırıma tabi tutulabilmektedir. *İçel* ve *Ünver* bu ayırımı yaptıktan sonra İnternet'i kitle haberleşmesi kategorisine sokmaktadır. Fakat bir haberleşme (iletişim) aracı olarak İnternet teknik olarak hem bireyler

durumunda etkisini yoğun bir şekilde hissettirmektedir. Bunun yanında, elektronik ticaret gibi bir çok faaliyetin İnternet aracılığıyla gerçekleştirilebilmesi karşısında, İnternet s jelerin s z konusu faaliyetler a ısından sorumluluklarının incelenmesi  nem arz etmektedir.

Her ne kadar bu b l mde, terim, tanım ve kapsam sorununa deėinilmesine raėmen, ikinci ve    nc  b l mde TCK'de d zenlenen su ların incelenecek olması kar ısında, konunun  nemi nedeniyle, İnternetin hukuki olarak d zenlenmesine ve yaygın bir  ekilde İnternet s jeleri olarak adlandırılan ki ilerin sorumluluėuna ili kin geli melere de bu b l mde ayrıca deėinilecektir.

2. İnternete İli kin Hukuki D zenleme ve İnternet S jelerinin Sorumluluėu

Bireysel haberle me a ısından bakıldığında, bir ileti im aracı olarak İnternetin bu y nde kullanımının haberle menin gizliliėi kapsamında deėerlendirilmesi m mk nd r. Bu  ekliyle bir haberle me aracı olarak İnternetin kullanımı, Anayasa'nın 22. maddesinde d zenlendiėi  ekliyle haberle me h rriyeti kapsamındadır. Bireysel haberle me aracı olarak İnternetin kullanımının 5369 Sayılı Kanunda da ifade edildiėi  zere elektronik haberle me kapsamında deėerlendirilmesi m mk nd r⁴⁵. Bu a ıdan İnternetin ara sal niteliėi  n planda olup, bu t r faaliyetler

arası hem de kitle haberle me aracı olarak kullanılması m mk nd r. Bu a ıdan yazarın y zy ze ileti im aracı olarak tanımladıėı elektronik posta İnternetin bireylerarası haberle me aracı olarak kullanılmasına, İnternet aracılığıyla web sayfalarının sunumu ise İnternetin kitle haberle me aracı olarak kullanılmasına  rnek g sterilebilir. Bkz., **   EL -    VER**, s. 5 – 8.

⁴⁵ “Evrensel Hizmetin Saėlanması Ve Bazı Kanunlarda Deėi iklik Yapılması Hakkında Kanun” RG. 25.06.2005 T. , RG No. 25856.

Kanunun 2. maddesinde elektronik haberle me “i aret, sembol, ses, g r nt  ve elektrik i aretlerine d n  t r lebilir her t rl  verinin kablo, telsiz, optik, elektrik, manyetik,

açısından İnternetin düzenlenmesinde devletin negatif bir rolü söz konusu olmaktadır. Bu nedenle de Anayasanın 22. maddesinin ikinci fıkrasında düzenlenen sınırlandırma sebepleri olmaksızın, bireysel haberleşme aracı olarak İnternetin, İnternet kullanımı suretiyle yapılan haberleşme açısından, içeriğine ilişkin bir düzenleme yapılması söz konusu değildir⁴⁶.

İnternetin haberleşme/iletişim aracı olarak kabul edilmesi sonucunda Anayasanın 26. maddesinde düzenlenen ifade hürriyeti ile haber verme ve haber alma hakkı kapsamında da değerlendirilmesi de mümkündür. Nitekim Avrupa İnsan Hakları Mahkemesi kararlarında düşünceyi açıklamada kullanılan araç ile (sözlü ya da yazılı basın, radyo TV vb) açıklamanın aldığı şekil (söz, yazı ya da artistik ifade vb.) arasında fark gözetilmeksizin, genel olarak ifade hürriyetinin ve haber verme ve alma hakkının düzenlendiği, Avrupa İnsan Hakları Sözleşmesinin 10. maddesi kapsamında olduğu belirtilmiştir⁴⁷. İfade hürriyeti ile haber verme ve alma hakkının kullanılmasında bir araç olarak ortaya çıkan İnternetin, bu yönüyle düzenlenmesinde de AİHS'in 10. maddesi ve Anayasanın 26. maddesinde düzenlenen koşullara uyulması zorunludur.

elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması”, şeklinde tanımlanmıştır.

⁴⁶ 5369 s. Kanunun 3. maddesinde, Türkiye Cumhuriyeti sınırları içerisinde yaşayan herkesin, bölge ve yaşadığı yer ayrımı gözetilmeksizin evrensel hizmetken yararlanacağı ifade edilmiştir. Kanunun 2. maddesinde evrensel hizmet; “*coğrafi konumlarından bağımsız olarak Türkiye Cumhuriyeti sınırları içinde herkes tarafından erişilebilir, önceden belirlenmiş kalitede ve herkesin karşılayabileceği makul bir bedel karşılığında asgari standartlarda sunulacak olan, temel internet erişimi de dahil elektronik haberleşme hizmetleri*” şeklinde tanımlanmıştır. Bu haliyle Kanunda, İnternet erişimi de dahil olmak üzere elektronik haberleşme olanağının sağlanmasına ilişkin pozitif bir yükümlülüğün getirildiğini söylemek mümkündür.

⁴⁷ Bkz., Feyyaz **GÖLCÜKLÜ** – A. Şeref **GÖZÜBÜYÜK**, Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 1. B., Ankara, 1994, s. 276. Ayrıca bkz, Durmuş **TEZCAN** - M. Ruhan **ERDEM** - Oğuz **SANCAKDAR**, **Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye’nin İnsan Hakları Sorunu**, 2. B., Ankara, 2004, s. 426.

Böylece ifade hürriyetinin ya da haber verme ve alma hakkının sınırlandırılması bakımından İnternet, bir araç olarak önemli hale gelmektedir. Söz, yazı, resim vs. gibi şekillerde ortaya çıkan ifadenin içeriğinin suç oluşturup oluşturmadığının tespitine ilişkin sorun, bunların ifade edilmesinde araç olarak ortaya çıkan İnternet'ten bağımsız bir nitelik kazanmaktadır. İfade hürriyetinin kullanımında bir araç olan İnternete ilişkin bu yönde bir düzenleme ise ifade hürriyeti, haber verme ve alma hakkı kapsamında ele alınması gerekmektedir.

İfade hürriyetinin kullanılmasında günümüzde en önemli araçlar basın ve radyo – televizyondur⁴⁸. Bilindiği üzere, kitle iletişim araçları olarak basın ve radyo-televizyon farklı hukuki rejimlere tabidir. Bir kitle iletişim aracı olarak basınının düzenlenmesi ile ilgili olarak, Anayasasının Basın hürriyeti başlıklı 28. maddesinin birinci fıkrasında, “*Basın hürdür, sansür edilemez. Basımevi kurmak izin alma ve malî teminat yatırma şartına bağlanamaz.*” hükmüne yer verilmiştir. Aynı maddenin ikinci fıkrasında basın hürriyetinin sınırlandırılmasında Anayasanın 26. ve 27. maddelerinde düzenlenen koşullara uyulacağı düzenlenmiş ve basın hürriyeti ile haber alma hürriyetinin sağlanmasına ilişkin gerekli tedbirlerin alınması yönünde devlete pozitif bir yükümlülük getirilmiştir. Buna ilişkin olarak Anayasanın 28. maddesinde ifade edildiği şekliyle basın hürriyetinin kullanılmasına ilişkin olarak basın faaliyeti 5187 Sayılı Basın Kanunu ile ayrıntılı olarak düzenlenmiştir.

Radyo – televizyon yayıncılığı da basın hürriyeti ile aynı yönde ifade hürriyeti ile haber verme ve alma hakkı kapsamında değerlendirilmektedir⁴⁹.

⁴⁸ Ayrıntılı bilgi için bkz. **TEZCAN, Avrupa İnsan Hakları Sözleşmesi**, s. 433 vd.

⁴⁹ Ayrıntılı bilgi için bkz., **TEZCAN, Avrupa İnsan Hakları Sözleşmesi**, s. 439 vd. Ayrıca bkz., Halit **YILMAZ**, İdarenin Görsel – İşitsel İletişim Alanındaki İşlevi, Ankara, 2006 s. 5 vd.

Basından farklı olarak radyo – televizyon yayıncılığı Anayasanın 26.maddesinde belirtildiği üzere izne bağlanabilmektedir. Bu doğrultuda Türkiye’de radyo – televizyon yayıncılığı 3984 Sayılı Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun ile düzenlenmiş bulunmaktadır.

Bir kitle haberleşme/iletişim aracı olarak İnternetin düzenlenmesi gereği ise, özellikle İnternet üzerinden çocuk pornografisi, ırkçılık ve yabancı düşmanlığına ilişkin fiillerin ve diğer hukuka aykırı fiillerin gerçekleştirilmesi sonucunda bu tür fiillerin önlenmesi ve bu fiillere ilişkin sorumluluk rejimlerinin tespiti noktasında ortaya çıkmıştır. Bir web sayfasının İnternet aracılığıyla sunulması ve bu sayfaya ulaşma örneğinde olduğu gibi bu tür bir faaliyetin gerçekleştirilmesi birden çok kişinin katkısının olabilmesi, İnternet sükeleri olarak adlandırılan kişilerin sorumluluklarının düzenlenmesi sonucunu doğurmuştur. Sorun, özellikle başkasına ait içeriğin İnternet aracılığıyla erişilebilir kılınmasını ya da bu içeriğe erişilebilmesini sağlayan kişilerin sorumlu olup olmayacakları noktasında toplanmaktadır. Bunun sonucunda, kitle iletişim aracı olarak İnternetin düzenlenmesi, ağırlıklı olarak sorumluluk rejimine ilişkin olarak ortaya çıkmaktadır.

Aynı şekilde, İnternet de dahil olmak üzere, telekomünikasyon araçları ile elektronik ticaret vs. gibi her türlü hizmetin dahil olduğu faaliyetlerin gerçekleştirilmesi nedeniyle, bu tür faaliyetlerde çeşitli şekillerde rol alan kişilerin sorumluluğu gündeme gelmiştir. Bu açıdan, İnternet sükelerinin sorumluluğu başlığı altında incelenen sorun, telekomünikasyon aracılığıyla her türlü hizmetin sunulmasına katılan kişilerin işlevlerine göre sorumluluklarının tespitine ilişkin bir rejimdir. Bunun sonucunda, enformasyon ya da bilgi servisleri olarak adlandırılan hizmetlerin sunumunu yapan kişilerin ve bunların sunumunda aracı olan kişilerin,

aracılık faaliyetlerindeki işlevlerine göre, sorumluluk rejiminin tayini yoluna gidilmiştir. Nitekim Avrupa Birliği'nin "*Elektronik Ticarete İlişkin Yönerge*"sinde bu husus, elektronik ticaretin düzenlenmesi esassından hareketle ele alınmıştır⁵⁰.

Türkiye'de genellikle, bir kitle iletişim aracı olan İnternetin kullanılmasında İnternet sùjelerinin sorumluluđu başlıđı altında, Alman "*Teleservisler Kanunu*"nda yer alan düzenlemeler esas alınmaktadır. Avrupa Birliđi *Elektronik Ticaret Yönergesi* esas alınarak tekrar düzenlenen Kanunun 2. maddesinde, Kanunun kapsamı belirlenmiş olup telekomünikasyon servisleri aracılığıyla yapılan her türlü elektronik enformasyon ve iletişim hizmeti sunan kişiler, servis/hizmet sağlayıcı (teleservisler) olarak tanımlanmıştır. Nitekim, aynı maddede teleservislerin kapsamı İnternet'e erişimi de kapsayacak şekilde ve daha geniş olarak tanımlanmıştır⁵¹.

Türk Hukukunda adı geçen kanunda yer alan sorumluluk rejimine ilişkin düzenleme genel olarak İnternet sùjelerinin sorumlulukları başlıđı altında incelenmiştir. Adı geçen Kanunda sorumluluk rejimine ilişkin hükümler esas alınarak İnternet sùjeleri, Kanunda sadece hizmet/servis sağlayıcıdan bahsedilmesine karşın, işlevlerine göre, içerik sağlayıcı, erişim sağlayıcı ve servis sağlayıcı olarak

⁵⁰ Bkz., **Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')**, *Official Journal L 178* , 17/07/2000 P. 0001 – 0016, (32000L0031), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML>.

Yönergenin 2. maddesinde servis/hizmet sağlayıcı, Enformasyon toplumu hizmeti/serisi yapan gerçek ve tüzel kişi olarak tanımlanmıştır. Enformasyon toplumu hizmeti/servisi tanımında 98/34/EC sayılı Yönergedeki tanım esas alınmıştır. Söz konusu Yönergenin 1. maddesinde enformasyon toplumu hizmeti/servisi , tarafların aynı zamanda hazır bulunmaksızın elektronik araçlarla bireyin talebi üzerine belirli bedel karşılığında sunulan her türlü hizmet olarak tanımlanmıştır. Bkz., *Directive 98/34/EC of the European Parliament and of The Council Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations and Of Rules on Information Society Services* , http://ec.europa.eu/enterprise/tris/consolidated/index_en.pdf .

⁵¹ Kanunun İngilizce metni için bkz., <http://www.iuscomp.org/gla/statutes/TDG.htm>

üçlü bir ayırım yapılarak incelenmektedir. *İçerik sağlayıcı* genel olarak İnternet kullanıcıları tarafından erişilebilen herhangi bir İnternet yayınının içeriğini hazırlayan ya da bilgiyi bizzat üreten kişi; *erişim sağlayıcı* kullanıcıların İnternet ağına erişmelerini sağlayan, başkalarına ait içeriklere yalnızca aracılık eden kişi; *servis sağlayıcı* ise, başkalarına ait içeriği kendi bünyesinde saklayan ve İnternet üzerinden erişebilmesine olanak sağlayan kişi olarak tanımlanmaktadır. Kanunda söz konusu kişilerin sorumlulukların belirlenmesinde de işlevlerine göre ayırma gidilmektedir. Buna göre içerik sağlayıcı, söz konusu fiillerinden dolayı sorumluluğa ilişkin genel kurallara göre sorumludur. Erişim sağlayıcı, sırf bu erişim faaliyetinden dolayı sorumlu tutulmamaktadır. Geçici depolama işleminden ise, depolanan veriye, kaynağı edinilme süreci ve iletildiği kişi veya kişilere müdahale etmemesi halinde, sorumlu tutulmamaktadır. Erişim sağlayıcının bu yönde bir müdahalesi söz konusu olduğunda ise, içerik sağlayıcı gibi sorumlu tutulmaktadır. Servis sağlayıcı kural olarak kendi bünyesinde barındırdığı başkasına ait içerikten sorumlu değildir⁵².

İnternet sùjelerinin , işlevlerine göre sorumluluklarının belirlendiğı benzer bir ayırım Fransa’da “İletişim Özgürlüğü Kanunu”nda yapılmıştır. Adı geçen Kanunda üçlü ayırma yer verilmiş ve içerik sağlayıcıların genel hükümlere göre cezai sorumluluklarının bulunduğu belirtilmiş, servis sağlayıcıların ise sunulan hizmetin içeriğinden dolayı yalnızca adli bir makam tarafından bildirilmesine karşın

⁵² Servis sağlayıcının sorumluluğuna ilişkin ayrıntılı olarak bkz, R. Barış **ERMAN**, *Alman Hukukunda İnternette Kaynaklanan Ceza Sorumluluğı*, İHFM, C. LIX, S. 1-2, 2001, s. 217 vd. İnternet sùjelerinin sorumluluğı hakkında ayrıntılı olarak bkz., F. Selami **MAHMUTOĞLU**, *Karşılaştırmalı Hukuk Bakımından İnternet Sùjelerinin Cezai Sorumluluğı*, İHFM, C. LIX, S. 1-2, 2001, s. 39 vd; Veli Özer **ÖZBEK**, *İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 4, S. 1, 2002, s. 109 – 113; **SINAR**, , s. 86 vd; Önder **DEMİR**, *İnternet Servis Sağlayıcılarının Hukuki Sorumluluğı*, Uluslararası İnternet Hukuku Sempozyumu, İzmir 2002, s. 476 vd.

içeriğe erişimin engellenmesi yönünde harekete geçmemeleri durumunda sorumlu olacakları düzenlenmiştir. Erişim sağlayıcıları için İnternete erişim yönünden özel bir sorumluluk hükmüne yer verilmemiştir⁵³.

Bu ayırımın Yargıtay tarafından da belirli ölçülerde kabul edildiği görülmektedir. Nitekim Yargıtay 9 Ceza Dairesi, İnternet üzerindeki bir forum alanına gönderilen mesajın içeriğinin suç oluşturduğu iddiası ile açılan ceza davası ile ilgili olarak, forum alanı yöneticisinin sorumluluğunun bulunup bulunmadığı konusunda, “...A.Ş.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 ve web sitesi sisteminin bir işletene (moderatör) bağlı olup olmadığı hususlarının saptanmasından sonra sanığın hukuki durumunun takdir ve tayini gerekirken eksik soruşturma ile hüküm kurulması”, gerektiği görüşünü dile getirmiştir. Henüz İnternet sükelerinin sorumluluklarına ilişkin genel bir düzenleme bulunmamakla birlikte, Yargıtay söz konusu kararda, başkalarına ait ya da başkası tarafından gönderilen içerikle ilgili olarak, cezai sorumluluk açısından işleten kişinin “müdahale etme görev ve yetkisinin bulunup bulunmadığı” ölçütünü esas almıştır⁵⁴.

⁵³ Ayrıntılı bilgi için bkz., Zeynel KANGAL, *Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu*, İHFM, C. LIX, S. 1-2, 2001, s. 230 vd.

⁵⁴ YARGITAY, 9. CD, E. 2001/1854, K. 2001/2649, T. 25.10.2001, <http://www.kazanci.com.tr/kho2/ibb/files/9cd-2001-1854.htm>

5846 Fikir ve Sanat Eserleri Kanunun EK-4. maddesinin üçüncü fıkrasında da yukarıda aktarılan ayırıma, “servis sağlayıcısı” ve “bilgi içerik sağlayıcısı” şeklinde yer verilmiştir⁵⁵.

“Bilişim Ağı ve Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı”nda ise içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, hizmet sağlayıcı, toplu kullanım sağlayıcı şeklinde beşli bir ayırıma yer verildiği görülmektedir. Kanunun 2. maddesinin “h” bendinde içerik sağlayıcı, “bilişim ağı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler”; “ı” bendinde yer sağlayıcı, “hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler” ; “i” bendinde erişim sağlayıcı, “kullanıcılarına bilişim ağına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler”; “j” bendinde hizmet sağlayıcı “bilişim ağı üzerinde her türlü hizmet sunanlar”; “k” bendinde ise toplu kullanım sağlayıcı “kişilere belli bir

⁵⁵ Maddenin 3. fıkrasına göre “Dijital iletim de dahil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi içerik sağlayıcılar tarafından eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış haklarının ihlâli halinde, hak sahiplerinin başvuruları üzerine ihlâlê konu eserler içerikten çıkarılır. Bunun için hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlâlê durdurulmasını ister. İhlâlê devamı halinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlâlê devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir. İhlâlê durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır. Servis sağlayıcılar, bilgi içerik sağlayıcılarının isimlerini gösterir listeyi her ayın ilk iş günü Bakanlığa bildirir. Servis sağlayıcılar ile bilgi içerik sağlayıcıları, Bakanlıkça istendiği takdirde her türlü bilgi ve belgeyi vermekle yükümlüdür. Bu maddede belirtilen hususların uygulanmasına ilişkin usul ve esaslar Bakanlık tarafından çıkarılacak bir yönetmelikle belirlenir.” Aynı maddenin dördüncü fıkrasına göre, “Birinci fıkrada bahsi geçen fiilleri kasten ve yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında bu Kanunun 72 nci maddesinin (2) numaralı bendi hükümleri uygulanır”

yerde ve belli bir süre bilişim ağını kullanım olanağını sağlayan” olarak tanımlanmıştır⁵⁶.

Tasarının 2. maddesindeki bu tanımlar incelendiğinde yukarıda aktarılan üçlü ayırım yanında hizmet sağlayıcısı şeklinde dördüncü bir kategori yarattığı görülmektedir. Yukarıda belirtildiği üzere, hizmet sağlayıcı hem Avrupa Birliği Yönergesinde hem de Alman Teleservisler Kanununda kullanılan bir terimdir. Hizmet sağlayıcının sorumluluğu ise üstlendiği işleve göre belirlenmiştir. İnternetin araç olarak kullanılmasında, kişilerin faaliyetlerine ilişkin işlevsel bir ayırım esasından hareketle sorumlulukların belirlenmesi ise erişim sağlayıcı, içerik sağlayıcı, servis sağlayıcı başlıkları altında incelenmesine sebep olmuştur.

Tasarıda ise, hizmet sağlayıcının ayrı bir kategori olarak ifade edildiği görülmektedir. Nitekin Tasarının 2. maddesinde hizmet sağlayıcı, bir yandan içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcıyı da kapsar bir şekilde tanımlanmaktadır.. Tasarıda asıl olarak içerik sağlayıcısının, bilişim ortamına sunduğu iletişimden dolayı sorumluluğuna yer verilmiştir⁵⁷. Hizmet sağlayıcısının, yer sağlayıcısının⁵⁸ ve

⁵⁶ Tasarıda bilişim ağı hizmetlerine ilişkin faaliyetlerde serbestlik ilkesi benimsenmiş olup Tasarının 4. maddesinde bu husus “(1) Bilişim ağı hizmetlerine ilişkin faaliyetler serbesttir. Bu faaliyetlere başlama, yürütme ve sona erdirmeye, izne, bildirim veya başka bir koşula bağlı değildir.” şeklinde ifade edilmiştir.

⁵⁷ **“İçerik sağlayıcıların sorumlulukları” MADDE 5:** “(1) İçerik sağlayıcı, bilişim ortamında kullanıma sunduğu her türlü içerikten sorumludur. (2) İçerik sağlayıcı, bağlantı sağladığı, başkalarına ait içeriklerden sorumlu değildir. Ancak, kendilerine ait olan içeriğin sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur.”

Bunun yanında Tasarının 6. ve 7. maddelerde içerik sağlayıcıların genel ve özel bilgilendirme yükümlülükleri düzenlenmiştir.

⁵⁸ Yer sağlayıcısının, içeriği kontrol etme yükümlülüğü de olmadığı açıkça düzenlenmiştir. **“Yer sağlayıcının sorumlulukları” MADDE 8:** (1) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

erişim sağlayıcısının içerikten sorumlu olmasına ilişkin olarak özel bir düzenlemeye yer verilmemiş ve genel olarak yükümlülükleri düzenlenmiştir. Tasarıda hizmet, yer ve içerik sağlayıcılarına ilişkin cezai sorumluluk sadece 31. maddede düzenlenmiştir. Sorumluluk ise genel olarak, içerikten sorumluğa ilişkin olmayıp, Tasarının 15. ve 37. maddelerinde düzenlenen içeriğin engellenmesi ve düzeltilmesine ilişkin hükümler uyarınca, usulüne göre verilmiş hakim ve mahkeme kararının yer, erişim ve hizmet sağlayıcısının tarafından yerine getirilmemesi haline hasredilmiştir⁵⁹.

II. SOSYO-EKONOMİK DÖNÜŞÜM AÇISINDAN BİLİŞİM SUÇLARI

Bilginin ya da enformasyonun üretim, saklama değişim ve genel olarak işlenme sürecinin bilişim ve iletişim teknolojileri merkezinde gerçekleştiriliyor olması, içinde bulunduğumuz dönemin genel karakterini oluşturmaktadır. Özellikle bilgisayar sistemleri, günümüzde bilgi ve enformasyonun işlenmesinde en etkin araç olarak yoğun bir şekilde kullanılmaktadır. Kullanım yoğunluğunun artması ile birlikte hukukun da içerisinde yer aldığı toplumsal kurum ve yapıları çeşitli şekillerde etkilemektedir. Bu durumun maddi ceza hukuku üzerindeki etkisi ise bilişim sistemlerinin kullanımının etkisiyle olarak yeni suç tiplerinin ortaya çıkması ve de ceza mevzuatları içerisinde hali hazırda yer alan bir kısım suçların işlenme olarak ve oranlarını artmasıdır.

(2) “Yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, bu Kanunun 15 inci ve 37 nci maddelerine göre haberdar edilmesi ve engelleme yeteneği bulunması durumunda hukuka aykırı içeriğe erişimi engellemek zorundadır.”

⁵⁹ “**Kararın yerine getirilmemesi**” **MADDE 31:**“(1) Bu Kanunun 15 inci ve 37 inci maddelerinde belirtilen usule göre verilmiş hâkim veya mahkeme kararını yerine getirmeyen yer, erişim ve hizmet sağlayıcısına bir yıldan üç yıla kadar hapis cezası verilir.”

Bu etkinin, sadece teknolojik bir gelişimin etkisi olarak incelenmesi yerine, gelişimin koşullarının oluştuğu ve de bu gelişimden etkilenen soysal, ekonomik ve politik yeniden yapılanma içerisinde incelenmesi, özellikle ceza hukuku alanında bilişim suçları başlığı altında düzenlenen ve incelenen ve sayıları her geçen gün artan suçların kapsamının ve içeriğinin belirlenmesinde daha yararlı olacaktır⁶⁰. Bu açıdan bilişim suçları, siber suçlar gibi çeşitli adlarla incelenen ve içeriği her geçen gün zenginleşen bu suçları, yeni bir olgu olarak anlayabilmek için, dünya çapında bir çok ülkeyi etkileyen geniş çaplı politik, sosyal ve ekonomik yeniden yapılanmanın bir yönü olarak kabul etmek gereklidir⁶¹. Bir bilişim teknolojisi olarak enformasyon ya da bilginin işlenmesi aracı olan bilgisayar sistemlerinin ve ayrıca iletişim aracı olarak karşımıza çıkan İnternetin maddi ceza hukukuna etkisi şeklinde görülebilen bilişim suçları, içinde bulunduğumuz, sosyo-ekonomik dönüşümün parçası olarak anlam kazanabilmektedir. Sadece teknolojik bir etki olarak anlaşılması ise, sorunun kapsam ve boyutlarına ilişkin bir inceleme yapılmasına olanak sağlamamaktadır.

Nitekim, bilişim suçlarının günümüzde çok yaygın bir şekilde tartışılıyor ve ceza hukukuna ilişkin sorunlar arasında gündemin önemli bir kısmını işgal ediyor olması, kimi yazarlarca bu suçlara ilişkin genel bir yaklaşımdan hareketle açıklanmaktadır. Bu noktada *Sieber*, ceza mevzuatlarının yeni suç tiplerini kapsayacak şekilde geliştirilmesinin sadece teknolojik bir gelişim nedeniyle olmadığını, asıl olarak temel bir değişimin bu gelişimin kaynağını oluşturduğunu

⁶⁰ Douglas **THOMAS**, *Criminality in The Electronic Frontier: Corporality and Judicial Construction of the Hacker*, Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Ed. Douglas Thomas & Brian D. Loader, Routledge, 2003, s.22

⁶¹ Douglas **THOMAS**, – Brian D. **LOADER** : *Cybercrime in the Information Age*, , Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Ed. Douglas Thomas & Brian D. Loader, Routledge 2003, s.2.

ifade etmektedir. Yazar, 20. yüzyılın ortalarına kadar, bütün ülkelerin ceza mevzuatlarında yer alan suçların, ticari sır, patent, telif hakları gibi maddi varlığı olmayan şeyleri de sınırlı bir şekilde kapsamına rağmen, ağırlıklı olarak, maddi şeylerin korunması esas alınarak düzenlendiği; 20 yüzyılın sonlarına doğru ise, enformasyon/bilişim toplumunun ortaya çıkışının, maddi varlığı olmayan değerlerin ve enformasyonun öneminin artmasına neden olduğu görüşündedir. Bu değerlerin maddi varlığı olan şeylerin korunmasına benzer bir şekilde korunamayacağını ve yeni hukuki düzenlemelere ihtiyaç gösterdiğini belirtmektedir⁶².

Aşağıda inceleneceği üzere, bilişim suçları olarak adlandırılan suçlarda, kategorik olarak yeni hukuki değerlerin ortaya çıkışı ve bunların cezai himayesinden çok, var olan hukuki değerlerin somutlaştığı şeylerin değişimi sonucu özellikle suçun unsurları bakımından ortaya çıkan sorunların giderilmesi söz konusudur. Bunun yanında bir takım niceliksel sorunların çözülmesi de bu kapsamda değerlendirilmektedir. Bu yönüyle bilişim suçları, teknolojik bir gelişimden çok, gelişimin etkileri ile birlikte sosyo-ekonomik dönüşümün bir yönü olarak karşımıza çıkmaktadır. Söz konusu sosyo-ekonomik dönüşüm ise, Türkçede yaygın olarak kullanıldığı şekliyle bilgi toplumu, bilişim, enformasyon toplumu ya da

⁶² Ulrich **SIEBER**, Legal Aspects of Computer – Related Crime, in the Information Society, - COMCRIME-Study -, 1998, s. 39. <http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc>

Aşağıda da aktarılacağı üzere Yazar, bilişim suçları olarak incelenen suçları, genel olarak yeni bir hukuksal değer ortaya çıkışı ve bunların korunması merkezinde incelemekte, ceza mevzuatları içerisinde cezai müeyyidelerle korunan halihazırdaki hukuki değerlerin somutlaştığı bir şeyin olmaması ya da somutlaştığı şeyin enformasyon olarak ortaya çıkması nedeniyle bunların korunmasına ilişkin çözüm yolları olarak incelemektedir.

Wall, da bu dönemi farklılaştıran karakteristik özelliğin parasal bir değer maddi varlığı olan şeylerden çok fikirler üzerinde somutlaşması olduğunu vurgulamaktadır. Yazara göre bu durum, özellikle fikri sına-i haklar alanındaki ihlaller bakımından etkisini göstermektedir. David S. **WALL**, *Cybercrimes and Internet*, Crime and the Internet, Edit. David S. Wall, Routledge, 2003, s. 2 – 3.

enformasyon devrimi gibi çok farklı şekillerde adlandırılan dönüşüme işaret etmektedir⁶³.

Bir çok ad altında incelenen, özellikle 20. yüzyılın ikinci yarısından itibaren etkisini hissettirmeye başlayan sosyo-ekonomik dönüşümde, bilişim sistemlerinin kullanımı önem arz etmekte ve merkezi bir konumda bulunmaktadır⁶⁴. Sosyo-ekonomik dönüşümde, temel bir etken oluşturan bilişim teknolojisinin kendisi ve

⁶³ Yukarıda bahsedildiği üzere sosyo-ekonomik dönüşüm, kendi başına çeşitli açılardan farklı yaklaşımlar doğrultusunda incelenebilecek bir konu olup, konunun önem derecesi ve kapsamı bu çalışmanın sınırlarını aşan boyuttadır. Burada bu dönemin genel bir tahlilinin yapılması yerine konunun anlaşılabilirliği açısından kısa bir açıklamaya yer verilecektir. Neden bilişim sistemi, neden veri önemlidir ve çeşitli yönleriyle ceza mevzuatlarında bunlara yönelik çeşitli fiiller suç olarak düzenlenir soruları, sosyo-ekonomik dönüşümde cevabını bulmaktadır.

Sosyo-ekonomik dönüşüm çeşitli yönleri ve farklı yaklaşımlarla bir çok ad altında ele alınıp incelenmiştir. Nitekim *Köksal* bilişim toplumunun tanımında, toplumsal kurumlardaki değişimleri vurgulayan çeşitli yaklaşımlar önerildiğini ve devamında : “*Verimliliğin öne çıktığı üretim ilişkileri, üretim araçları, işgücü ve çalışma koşullarındaki değişimi vurgulayan endüstriyel yaklaşım; bölgesel, ulusal ya da küresel düzeyde ekonomide ortaya çıkan yeniden yapılanma süreçlerinin vurgulandığı ekonomik yaklaşım; devletlerin ulusal yetki ve sorumluluklarıyla uluslararası örgütlerin ve çokuluslu ortaklıkların yetki ve sorumluluklarını, kişisel bilgilerin gizliliği de içinde, yurttaşların bireysel hak ve özgürlüklerini vurgulayan tüzel ya da siyasal yaklaşım; yeni mesleklerin gerektirdiği insangücünü yetiştirme koşullarını ve çalışma kurallarını öne çıkaran eğitimsel yaklaşım; bireyin yaşamındaki olumlu-olumsuz değişiklikleri betimleyen davranışbilimsel yaklaşım; yeni toplum düzenini olanaklı kılan altyapıyı temel alan teknikbilimsel yaklaşım vb*” yaklaşımlar esas alınarak tanımlar yapıldığını ifade etmektedir. Aydın **KÖKSAL**, Bilişim Toplumu, kurultay.tbd.org.tr/kurultay20/Bildiriler/Aydin_Koksal/bildiri.pdf

Timisi, sosyo-ekonomik dönüşüme ilişkin farklı bakış yaklaşımlar esas alınarak yapılan incelemeleri, “*enformasyon toplumu yaklaşımı*”, “*yeni iletişim teknolojileri ve post-fordizm*”, “*enformasyon ve post modernizm*”, “*küreselleşme*” başlıkları altında değerlendirmiştir. Bkz., Nilüfer **TİMİSİ**, Yeni İletişim Teknolojileri ve Demokrasi, 2003, s. 87 vd. *Bozkurt* ise, konuyu “*post-endüstriyel dönüşüm*” adı altında incelemiştir. Bkz., Veysel **BOZKURT**, Endüstriyel – Post-Endüstriyel Dönüşüm, İstanbul, 2005, s. 20 vd. *Şaylan* konuyu “*yeni teknolojik devrim*” ya da “*yeni teknolojik paradigma*” adları altında ele almıştır. Gencay **ŞAYLAN**, Değişim ve Küreselleşme ve Devletin Yeni İşlevi, 2. B., 2003, s. 169 vd.

Sosyo-ekonomik dönüşümün konu edinildiği ve farklı adlarda incelendiği çalışmaların listesi hakkında ayrıca bkz., James A. **BENIGNER**, The Control Revolution: Technological and Economic Origins of Information Society, Harvard University Press, 1986, s. 4 – 5.

⁶⁴ Manuel **CASTELLS**, The Rise of The Network Society: The Information Age, Economy, Society and Culture, Vol I, 2. edition, Oxford, 2000 s. 60.

bilişim teknolojilerinin kullanımının sosyal organizasyonlar üzerindeki etkileri, yeniden yapılanma sürecinin gelişimi ve karakteristik özellikleri tarafından yönlendirilen koşullar altında belirlenmektedir⁶⁵. *Bozkurt*, sosyo-ekonomik dönüşümün temel dinamiklerinden olan bilgisayar teknolojisinin, bir yandan zihinsel emeğin yerinin tutarak diğer yandan ise insanın zihinsel emeğinin çevresini genişleterek, yaşanan değişimde önemli bir faktör olarak damgasını vurduğunu ifade etmektedir⁶⁶.

Sosyo-ekonomik dönüşüm içerisinde, kendisi enformasyon ve bilgiye duyulan ihtiyacın bir sonucu olarak ortaya çıkan bilişim teknolojisinin kullanımı⁶⁷, özellikle ekonomik açıdan etkilerini ağırlıklı olarak göstermektedir. Bu açıdan, bilgiye ve enformasyona dayalı ve bilişim sistemlerinin altyapısını oluşturduğu küresel ekonomik yapılanmayı karşımıza çıkarmakta ve genel olarak bilgiye, enformasyona dayalı ekonominin ortaya çıkmasına neden olmaktadır⁶⁸. Bilgiye veya enformasyona dayalı ekonomi denmesindeki neden ise *Castells*'e göre; mal ve hizmet üretiminin bilişim sistemleri aracılığıyla gerçekleştirilmesi yanında, enformasyon ve bilginin hammadde olarak bilişim sistemleri aracılığıyla işlenmesi ve sonuçta ortaya çıkan ürünün klasik mal veya hizmet olması yerine enformasyon ve bilgi olmasıdır⁶⁹.

⁶⁵ Manuel **CASTELLS**, *Informational City: Information Technology, Economic Restructuring and The Urban-Regional Process*, Oxford, Blackwell, 1989, s. 2.

⁶⁶ **BOZKURT**, s. 29

⁶⁷ The Knowledge-Based Economy, Paris, OECD. OCDE/GD(96)102. OECD, s. 21, <http://www.oecd.org/dataoecd/51/8/1913021.pdf>

⁶⁸ **CASTELLS**, *Informational City*, s. 76. vd.

⁶⁹ **CASTELLS**, *Informational City*, s. 78. Aynı yönde, Gencay **ŞAYLAN**, *Değişim ve Küreselleşme ve Devletin Yeni İşlevi*, 2. B., 2003, s. 169. OECD raporunda ise bilgiye dayalı ekonomi teriminin bilginin ve teknolojik gelişimin ekonomik büyüme içerisindeki

Stratton, bilişim ve iletişim teknolojilerinin gelişimini “siber alanın gelişimi” başlığı altında, kapitalist üretim ve tüketim ilişkilerinin gelişimi süreci içerisinde incelemektedir. Yazar, siber alanın 19. yüzyılda ortaya çıktığını ve temelinde, dolaşım zamanını hızlandırma çabasının yattığını ifade etmektedir. Yazar bu açıdan siber alan olarak da adlandırılan şeyin üretiminin, bilgisayarların ortaya çıkışıyla değil, uzak mesafelerle iletişim hızının, bir iletinin mesafeyi açma zamanının, alıcıya ve göndericiye önemsiz geldiği bir süreye indirgendiği bir noktaya kadar yükselişle başladığını ifade etmektedir. Devamında ise, coğrafik bir alanı aşmak için geçen zamanın azalmasının, simgelerin etkin olduğu, bu bağlamda bilginin maddeleştiği, siber alan olarak adlandırılan bir hiperalana yol açtığını ifade etmektedir⁷⁰. Coğrafik alanın sömürgeleştirilip kapitalist değişim sistemi içinde bir

rolünün tam olarak kabullenilmesi sonucu ortaya çıktığı ifade edilmiştir. İnsanoğlunun kendisinde ve teknolojide somutlaşan bilgi ekonomik büyümede her zaman için merkezi bir yer edinmiştir. Fakat son yıllarda göreceli önemi kabul edilmiş olup bu önemi artmaktadır. **OECD, The Knowledge-Based Economy**, s. 9,

Ayrıntılı bilgi için ayrıca bkz., Hüsnü **ERKAN**, Bilgi Toplumu ve Ekonomik Gelişme, Türkiye İş Bankası Kültür Yayınları, 4. B., 1998, s. 10 vd., s. 71 vd; Hasan **ÇOBAN**, Bilgi Topluma Geçiş, Gelecekte Kaçılmaz, İstanbul, 1997, s. 12 vd.

⁷⁰ Bu noktada *Castells* gerçekliğin kendisinin simgesel olanla ayrı tutulamayacağını, bütün toplumlarda insanların simgesel bir çevre içinde var olduğunu ve bu çevre içinde hareket ettiğini belirtmektedir. Buradan hareketle B.lı iletiden görsel – işitsel iletiye bütün iletişim tarzlarının elektronik bütünleşme çerçevesinde örgütlendiği yeni iletişim düzeninin tarihsel açıdan özgül yönü, sanal gerçekliği devreye sokması değil, sanal gerçekliği kurgulamasındadır. Yazar bu hususu Oxford Günümüz İngilizcesi sözlüğünden hareketle sanalı, ismen değilse de gerçekte, uygulamada öyle olan ve gerçeği, gerçekte var olan şeklindeki tanımlarından hareketle açıklamaktadır. Bu açıdan yaşandığı şekliyle gerçeklik her zaman için sanal olmakta çünkü gerçekliğin her zaman için uygulamaya belli anlam çizen simgeler aracılığıyla algılanması söz konusu olmaktadır. Gerçekler simgeler aracılığıyla iletilmekte ve gerçek sanallık olarak adlandırılan iletişim sistemi, gerçekliğin kendisinin bütünüyle bir sanal imge düzeninde hayal dünyasında yakalandığı, ona gömüldüğü bir sistem olmaktadır. Yazar İnternetin de dahil olduğu çok sayıda iletişim tarzının sayısal, ağ bağlantılı tümleştirilmesine dayalı yeni iletişim sisteminin ayırt edici özelliğinin bütün kültürel anlatıları içermesi olduğunu belirtmektedir. Burada kimin interaktif iletişimi gerçekleştirdiği, kimin bu interaktif iletişimin alıcısı olduğu, bilgi toplumunda egemenlik düzeninin ve özgürlük süreçlerinin sınırlarını çizmektedir. Manuel **CASTELLS**, *Gerçek Sanallık Kültürü*, Çev. Kemal Akay, İnternet: Üçüncü Devrim?, Cogito, Sayı 30, 2002, s. 212- 214..

retim ve tketim blgesine dntrldđ yerde, hiperalanın kendisi ise, kapitalizm ierisinde gelitirilmi iletiim teknolojilerinin bir rn olarak ortaya ıkmaktadır. Bu sre, blgesel pazardan kresel bir pazar olarak tek bir pazarın oluması olgusuna iaret etmektedir. Geliim ierisinde kresel sistemlerin gelimesi ve yayılması ise bilgisayar sistemlerinin giderek gelimesi yanında bunların uluslar arası boyutta telekomnikasyon sistemleri ile birbirine bađlanmasıdır⁷¹. Bu kapsamda İnternetin yaygınlaması ve bunun tevik edilmesi de sz konusu sre ile bađlantılı olarak ortaya ıkmaktadır⁷².

Mulgan ise, enformasyon devriminin genel olarak, enformasyonun retim, ilenme ve dađıtımı gibi hususlarda ortaya ıkan dnm olarak grldđn, ifade etmektedir. Yazara gre, bu srece odaklanma, beraberinde ciddi ekonomik ve politik etkileri ortaya ıkarmaktadır. Ekonomik etkiler genel olarak, enformasyon temelinde retim hangi koullarda rekabet edilebilir bir ekilde yapılabileceđi, ticaretin ne ekilde dzenleneceđi ve enformasyonun kendisinin bir mal olarak nasıl kontrol edilebileceđi noktasında toplanmaktadır. Politik sorun ise kimin enformasyona eriebileceđi noktasındadır⁷³.

Yazar enformasyon devrimini, esas olarak enformasyon ile ilgili gren bu yaklaımın yanıltıcı olduđunu, enformasyonun ancak belirli bir kapsam dahilinde anlam kazanabileceđini ifade etmektedir. Herhangi bir makine, makineyi yapan ya da programlayan kii tarafından tanımlanan karar verme sreleri ve amaları

⁷¹ Jon **STRATTON**, *Siberalan ve Kltrn Kresellemesi*, İnternet: nc Devrim?, Cogito, Sayı 30, 2002, s. 81 -84.

⁷² Bkz., **STRATTON**, s. 87 vd.

⁷³ Geoffrey J. **MULGAN**, *Communication and Control: Networks and the New Economies of Communication*. 1991, s. 10.

kapsamında kontrol aracı olması dışında, kendiliğinden herhangi bir bilgi ya da enformasyona ihtiyaç duymamaktadır. Günümüzde bilişim teknolojisi, telematik ya da enformatik olarak teknolojik gelişimin amacı, belirli bir zaman ve mekânda olayların ve şeylerin daha etkili, kapsamlı koordinasyon ve kontrolünün sağlanmasıdır. Koordinasyon ve kontrol isteği, özellikle daha fazla karmaşılaşmış ve birbiriyle bağlanmış toplum ve ekonomilerde oluşan bir taleptir. Bu nedenle, daha fazla enformasyon ve bilgiye olan talep ve bunların işlenmesi, modern endüstriyel toplumların gelişimine bir tepki olarak ortaya çıkmaktadır. Bu dönemin öncekilerden farkı, sosyal ve ekonomik olarak ortaya çıkan karmaşıklıkla başa çıkabilmek için kullanılan kontrol teknik ve teknolojilerinin farklılığında yatmaktadır. Bilişim teknolojileri ise yeni bir şey yaratmasından çok, eskiden yapıla gelen şeylerin gerçekleştirilmesi usullerinde yeniden yapılandırma anlamında devrimsel bir nitelik taşımaktadır⁷⁴.

Benigner de, enformasyon toplumu olarak adlandırılan ortaya çıkan sosyal değişimde, bilişim ve iletişim teknolojilerinin gelişiminin ve bilişim sistemlerinin yaygın olarak kullanımının bir neden olarak ortaya çıkmadığını bu dönemin sosyal değişimin bir sonucu olarak görülmesi gerektiğini, belirtmektedir. Bu değişim yazara göre; endüstri devrimi ile birlikte ortaya çıkan ve bir yüzyıldan daha uzun bir zamandır devam eden “*kontrol devrimi*” olarak adlandırdığı bir sürecin doğal uzantısı olarak ortaya çıkmaktadır. Özellikle kitle iletişim ve telekomünikasyon teknolojisinin gelişimi açısından kontrol devriminin, ekonomik ve politik kontrol alanında yeniden yapılanmaya yol açtığı, yazar tarafından ifade edilmiştir. Bu dönemden önce, yönetimin ve pazarın kontrolü daha çok kişisel ilişkilere ve yüz

⁷⁴ **MULGAN**, s. 14 – 17.

yüze etkileşime dayanmakta iken, günümüzde kontrol, bürokratik organizasyon, yeni ulaştırma ve telekomünikasyon teknolojileri altyapıları ve yeni kitle iletişim araçlarıyla yeniden yapılandırılır hale gelmiştir⁷⁵. Yazara göre, enformasyon toplumu, endüstri devrimi ile birlikte ortaya çıkan sosyo-ekonomik yapıdaki değişimin sürdürülebilir kılınması ve politik ve ekonomik alanda kontrolün sağlanması ve krizlerin önlenmesi ya da krizin çözümlenmesi anlamında kontrol devriminin önemli bir sonucu olarak ortaya çıkmıştır⁷⁶.

Headric, de farklı bir bakış açısından, enformasyon çağı olarak adlandırdığı dönemin herhangi bir başlangıcının olmadığını ve insanlıkla yaşıt olduğunu ifade etmektedir. Yazara göre; tarih boyunca insanların ulaşabilecekleri enformasyon miktarında ve bununla başa çıkmak için üretilen enformasyon sistemlerinin artışında keskin hızlanmaların olduğu dönemler söz konusudur. Yazar, enformasyonun hızlanmasında makinelerin önemli olduğunu vurgulamakla birlikte, bunun tek neden olmadığını, enformasyon yönetim makinelerinden çok enformasyon sistemleri açısından “Akıl Çağı” (17. yüzyıl sonu ve 18. yüzyılın başı) ve “Devrim Çağı”nın (1776’dan 19 yüzyılın sonuna kadar) enformasyon sistemlerindeki kültür devrimini (yazılım) oluşturduğunu ifade etmekte ve bu haliyle maddi (donanım) devriminden önce gerçekleştiğini ifade etmektedir. Yazara göre; özellikle 1700 – 1850 döneminde yeni enformasyon sistemlerinin ortaya çıkması toplumsal, iktisadi ve siyasi değişimlerin yönlendirdiği bir kültürel dönüşüme işaret etmektedir. Yazar, söz konusu dönüşümü arz ve talep kavramları içerisinde açıklamakta, bu açıdan bu dönemde demografik ve ekonomik büyümenin enformasyona olan ihtiyacı, ekonomi

⁷⁵ **BENIGNER**, s. 6 – 7 .

⁷⁶ **BENIGNER**, s. 21 vd.

ve ticaretin düzenlenebilmesi, devlet idaresinin ve ordunun gereksinimlerinin yerine getirilmesi, mesleki uzmanlaşma, 1776’da Amerika’da başlayan Devrim Çağı, halkın siyasal temsiline sağlanması gerekçesiyle enformasyon talebinin artmasının enformasyona duyulan ihtiyacı arttırdığını ifade etmektedir⁷⁷.

Headrick’in enformasyon/bilişim sistemlerinin ortaya çıkışı ile ilgili olarak 1700 – 1850 yılları açısından arz ve talep kavramları içerisinde açıkladığı enformasyon ve bilgiye artan talep olarak daha çok sosyo-ekonomik nedenlerin etkili olduğu dönüşüm, *Benigner* ve *Mulgan* tarafından genel olarak “*kontrol devrimi*” başlığıyla günümüz açısından dile getirilmiştir. *Stratton*, bilgisayar sistemleri aracılığıyla oluşturulan iletişim sistemlerinin yaygınlaşmasını, kapitalist üretim ve tüketim ilişkileri içerisinde pazarın genişlemesi ve bütünleşmesi olgusuyla açıklamaktadır. *Castells* ise, sosyo – ekonomik dönüşümde bilgisayar sistemlerinin ağırlıklı olarak kullanılmasının karşılıklı olarak birbirini etkileyerek, hem küresel bir ekonominin gelişimini ortaya çıkardığını hem de üretimin niteliğinin değiştiğini ifade etmektedir. Bu hususlar topluca değerlendirildiğinde, enformasyon ve bilgi belirli bir amaçların gerçekleştirilebilmesi açısından talep edilmekte ve bu da değerini arttırmakta, enformasyon ve bilginin miktarının artması ise, bunların düzenlenmesi ve sistematik olarak işlenebilmesi bakımından enformasyon / bilişim sistemlerinin geliştirilmesine yol açmaktadır. Söz konusu talep ve sistemlerin gelişimi ise, belirli bir dönemde ortaya çıkan sosyo – ekonomik koşullarla bağlantılıdır

Kısaca değinilen hususlar doğrultusunda, genel olarak bilişim suçları olarak adlandırılan suçların ortaya çıkması, sadece teknolojik gelişimden çok sosyo-ekonomik değişim ya da dönüşüm ile birlikte anlam kazanabilmektedir. Sosyo-

⁷⁷ **HEADRICK**, s. 17 – 22.

ekonomik dönüşüm genişliği ve derinliği, dönüşümün teknik altyapısı olarak kullanılan bilişim sistemlerinin araç olarak kullanılması suretiyle ihlal edilebilecek bireysel veya toplumsal değerlerin de günden güne artmasına neden olmaktadır. Nitekim, ikinci bölümün konusunu da oluşturan bilişim alanında suçlar başlığı altında incelenecek olan suçlar, sosyo-ekonomik dönüşüm içerisinde enformasyona ve bilgiye artan ihtiyaç sonucunda, bunların özellikle bilgisayar sistemlerinde işlenebilmesine olanak sağlayan verinin korunması ve dönüşümün teknik altyapısını oluşturan bilgisayar sistemlerinin korunması bakımından gündeme gelmektedir. Bu husus, ağırlıklı olarak ekonomik dönüşümün bir etkisi olarak kendisini hissettirmekte olup, aşağıda incelenecek olan sisteme ve veri müdahaleyi esas alan suçların, Avrupa Konseyi ve Avrupa Birliğinde, bu suçların ekonomik suçlar kategorisi altında değerlendiriliyor olmasında da görmek mümkündür⁷⁸.

Aynı şekilde, üçüncü bölümün konusunu oluşturan, kişisel verilerin korunması da sadece bilişim sistemlerinin kullanımı ile açıklanamayacak olan bir olguya işaret etmesi bakımından önemlidir. Genel olarak, ilgili kişi hakkında, kim olduğu belirlenebilecek şekilde bilgi toplanması ve işlenmesi anlamına gelen kişisel verilerin toplanması ve işlenmesi, özel hayatın gizliliğine ilişkin bilişim sistemleri merkezinde bir ihlal türü olarak ortaya çıkmıştır. Bunun sonucunda ortaya çıkan kişisel verilerin korunması, sosyo-ekonomik dönüşüm içerisinde toplumsal kurum ve

⁷⁸ Avrupa Konseyinde bilişim suçlarının genel olarak ekonomik suçlar kategorisinde ele alınmasına ilişkin bkz., “Combating Economic Crime” <http://www.coe.int/T/E/Legal%5FAffairs/Legal%5Fco%2Doperation/Combating%5Feconomic%5Fcrime/>.

Avrupa Birliği için bkz., “**Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime**”, COM(2000) 890 final, http://eur-lex.europa.eu/LexUriServ/site/en/com/2000/com2000_0890en01.pdf

kuruluşların etkin karar alma süreçlerinde ve faaliyetlerinin rasyonel bir biçimde yürütülmesinde kişisel verilere artan ihtiyaç ile bağlantılı olarak karşımıza çıkmaktadır. Kişisel verilerin işlenmesine ilişkin usul ve esasların belirlenmesi ve kişisel verilerin korunmasına ilişkin suçlar sosyo-ekonomik dönüşüm içerisinde anlam kazanır.

Bunun yanında, “*Avrupa Konseyi Sibersuç Sözleşmesi*”nde içerik ile ilgili suçlar kategorisinde yer alan çocuk pornografisine ilişkin düzenlemeler, aynı Sözleşmeye ilişkin ek protokolde yer alan ırkçılık ve yabancı düşmanlığına ilişkin düzenlemeler ve ayrıca adı geçen Sözleşmede ayrı bir başlık altında ele alınan fikri-sınai haklara ilişkin düzenlemeler, sosyo-ekonomik dönüşümün belirli yönlerini göstermesi bakımından anlamlıdır. Sosyo-ekonomik dönüşümün bir yönü olarak ortaya çıkan bireysel ve toplumsal iletişimin sayısallaşması ve de İnternet sayesinde küresel hale gelmesi söz konusu iletişim olanaklarının kullanılması suretiyle birçok suçun işlenmesini kolay hale getirmiştir. Buna tepki olarak da özellikle çocuk pornografisi ve de ırkçılık ve yabancı düşmanlığına ve ayrıca fikri-sınai hakların ihlaline ilişkin fiillerin uluslar arası boyutta ele alınması gündeme gelmiştir.

Özetle 20. yüzyılın sonlarına doğru hızı ve yoğunluğu artan sosyo-ekonomik dönüşüm toplumsal kurumları her yönüyle etkilemektedir. Sosyo-ekonomik dönüşümün bilişim sistemleri üzerine inşa edilmesi sonucu karşılıklı etkileşim içerisinde, sayısallaşma olarak adlandırabileceğimiz bir olgu ve süreci ortaya çıkmaktadır. Sosyo – ekonomik dönüşümün dinamikleri ile şekillenen sayısallaşma olgusu ve sürecinin toplumsal kurumları ve bir toplumsal kurum olarak hukuk sistemlerini etkilemesi kaçınılmazdır. Söz konusu etkiyi sadece teknik bir gelişime dayandırmak ya da buna indirgemek, ortaya çıkan sorunlara ve sorunlara ilişkin

özüm arayışlarında teknik gelişimin kendisinin de çeşitli şekillerde etkilediğı asıl nedenin gözden kaçırılması sonucunu doğurur. Bu neden ise yukarıda aktarıldığı üzere sosyo-ekonomik dönüşümdür.

III. BİLİŞİM SUÇLARI

A. Terim, Tanım ve Kapsam Sorunu

Bilişim ve özellikle bilgisayar sistemlerinin yaygınlaşması ile birlikte ceza hukuku alanında, bunların kötüye kullanımlarına ilişkin fiillerin cezalandırılabilirliği ve kötüye kullanımının ortaya çıkardığı sorunların çözümü ya da çözüme ilişkin yaklaşımlar sonucu, birçok tanım yapılmış ve bu tanımları ifade etmek üzere birçok terim kullanılmıştır.. “*Bilgisayar suçları*”, “*bilgisayar suçluluğu*”, “*bilişim suçları*”, “*internet suçları*” ve Sibersuç sözleşmesinde de ifade edildiğı şekliyle “*siber suçlar*” terimler kullanılmaktadır⁷⁹.

Tanım ve terim zenginliği yanında bu alanda ortaya çıkan ihlallerin cezalandırılabilmesine ilişkin suçlar esas alınarak, bilgisayarın ya da bilişim sisteminin suçun maddi konusu ya da suçta kullanılan araç olması gibi hususlar esas

⁷⁹ Koca, bilişim teknolojisindeki gelişmelere paralel olarak kavramların da değıştiğini önceleri “ bilgisayar suçu” ya da bilgisayar ile ilgili suç kavramlarının kullanıldığını, sonrasında bu tanım ve terimlerin zenginleştğini, enformasyon ceza hukuk kavramının kullanılmaya başladığını; bilgisayar teknolojisinin hukuka aykırı içeriğın yayılması için kullanılan “multimedya suçu” kavramına gidildiğı, son olarak da sibersuç kavramında ulaşıldığını belirtmiştir. Yazar siber suç kavramının da aslında bilgisayar sistemlerine karşı ya da bilgisayar aracılığıyla işlenen suçlar anlamına geldiğini bu anlamda bilgisayar suçu kavramından farkının bulunmadığını belirtmiştir. Mahmut **KOCA**, *Avrupa Siber Suç Sözleşmesi’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku*, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp’e Armağan, C. III, s. 787 vd.

alınarak birçok sınıflandırma yapılması⁸⁰ kapsam sorunlarını da beraberinde getirmiştir.

Nitekim Yazıcıoğlu, “Konuyu ifade için kullanılan terimler arasındaki farklılık (yani terim sorunu) bir sonrakinin bir öncekine oranla konunun özünü veya kriminolojik yanını veyahut sistematliğini daha iyi anlattığı, daha çok kapsadığı iddiasından kaynaklanmaktadır. Tercih edilen terimin önemiye asla küçümsenmemelidir, zira her biri konunun boyutunu değiştirdiği gibi, konuya gösterilmesi gereken yaklaşımın belirlenmesinde de önemli bir rol oynamaktadır⁸¹.” demektedir. Yazar, devamında, bilgisayar suçlarının ne olduğu üzerinde herkesin ittifakla kabul edebileceği bir tanımın yapılabilmesinin zor olduğunu ve bunun yerine bilgisayar suçlarına ilişkin genel bir kategori suçtan bahsetmenin daha doğru olduğunu ifade etmektedir. Yazara göre, bu gruptaki suçları “ceza kuralları uyarınca bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller” olarak belirlemek yerinde olacaktır⁸². Ayrıca yazar bilişim ve bilgisayarın farklı anlamlara sahip olduğunu ve “bilgisayar suçu” ile “bilişim suçu”nun birbirinden farklı şeyleri ifade ettiğini; pratikte ise bilgisayarın en yaygın

⁸⁰ Çeşitli ayrımlar için bkz., Stephen P. HEYMANN, *Legislating Computer Crime*, 34 Harv. J. on Legis, 1997, s. 375 vd. Ayrıca bkz., Laura J. NICHOLSON – Tom F. SHEBAR – Meredith R. WEINBERG, *Computer Crimes*, 27 Am. Crim. L. Rev. (2000), s. 211.

⁸¹ YAZICIOĞLU, *Bilgisayar Suçları*, s. 130.

⁸² YAZICIOĞLU, *Bilgisayar Suçları*, s. 142. Kurt ise bilişim suçunu verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içinde işlenen, bir bilgisayar ya da ağına yönelik olara ya da onların kullanılarak icra edilen her türlü yasadışı haksız eylem olarak tanımlanabileceğini ifade etmektedir. KURT, s. 53.

Yazarın yukarıda aktarılan tanımı OECD tarafından 1982 tarihli raporda yer alan tanım ile paralellik arz etmektedir. Raporda bilgisayar suçları, “Bilgisayarın kötüye kullanılması, bilgileri otomatik işleme tabi tutmuş ve verilerin nakline ilişkin kanuna ve meslek ahlâkına aykırı davranışlardır” şeklinde tanımlanmıştır. OECD, “Computer – Related” Criminality” den aktaran, Sulhi DÖNMEZER, *Kişilere ve Mala Karşı Cürümler*, 16. B., İstanbul 2001, s. 614.

bilişim aracı olması nedeniyle “*bilişim suçları*” yerine “*bilgisayar suçları*” teriminin kullanıldığını belirtmektedir⁸³.

Bilişim ve bilgisayar terimlerinin farklı anlamlara sahip olduğu, bu kavramların birbiri yerine geçecek şekilde kullanılmasının hatalı olduğu *Yenidünya ve Değirmenci* tarafından da ifade edilmiştir. Yazarlara göre bilişim terimi, bilgisayara göre, daha geniş bir alanı kapsayıp bir üst kavramdır. Bilgisayar verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetlerini, diğer bir anlatımla veri-işleme tek başına gerçekleştirebilmektedir. Bilişim ise, hem verilerin işlenmesini hem de verilerin aktarımını kapsar. Bilişim sistemlerinin en yaygın kullanılan unsurunun bilgisayarlar olması, “bilgisayar suçu” teriminin yaygınlık kazanmasına neden olmuştur. Bu açıklama doğrultusunda yazarlar bilişim suçu terimini kullanmayı uygun bulduklarını belirtmektedirler⁸⁴.

Ersoy da bilişim suçu ve bilgisayar suçu ayrımını yapmakta, bilişim suçunun bilgisayarı da kapsayan ancak daha geniş olan bilişim araçlarına karşı ya da bilişim

⁸³ Yazara göre, bilişim alanının bilgisayarı da kapsayan ve özellikle bilgisayar ve bunun yanında bu alandaki bütün aygıt ve cihazların yer aldığı bir alanı ifade eder. Pratikte bilişim araçlarının en yaygın olanının bilgisayar olması ve bir yandan da “bilgisayar suçları”terimini kullanmanın bir alışkanlık teşkil etmesi nedeniyle, genelde “*bilişim alanında suçları*” ifade etmek için de “*bilgisayar suçları*” terimi kullanılmaktadır. Bu sebeple “bilgisayar suçları” denilince bazen daha geniş bir alan kastedilmektedir. Başka bir ifade tarzı ile “bilgisayar suçları” tabiri, yanlış da olsa, genelde “bilişim suçları veya suçluluğu” tabirine eş anlamda kullanılmaktadır yani bununla içinde daima bilgisayarın yer aldığı ve buna veya bunun birimlerinden birine karşı işlenen veya sistemlerin araç edinilmesi suretiyle gerçekleştirilen fiiller ifade edilmek istenmektedir. Böylece bilgisayar suçlarından bahsedebilmek için ortada mutlaka bir bilgisayarın bulunması gerekmektedir. **YAZICIOĞLU, Bilgisayar Suçları**, s. 131.

⁸⁴ **YENİDÜNYA –DEĞİRMENCİ**, s. 31. Yazarlar, siber suç terimi ile de aslında bilişim suçlarının ifade edildiğini, bununla birlikte bilişim suçlarının tek bir bilişim sisteminde işlenen şekli değil, bilişim sistem ağları vasıtasıyla (özellikle İnternet) işlenen suçların kastedildiğini, bilişim suçları teriminin siber suçları da içine aldığını belirtmektedirler. a.g.e., s. 32 – 33.

araçları ile işlenen suçları da kapsar şekilde anlaşılması gerektiğini ifade etmektedir⁸⁵.

Türk hukukunda özellikle bilişim suçu ya da bilgisayar suçu terimleri tercih edilmekte ve bu iki terim arasında anlam ve kapsam farklılığı yaratılmaktadır. Söz konusu ayırım “*bilişim sistemi*” ve “*bilgisayar*” terimlerinin farklılığından hareketle dile getirilmektedir. Bunlar arasında yapılan ayırım sonucunda, bilişim suçu teriminin bilgisayar suçlarını da içeren geniş bir kapsama sahip olduğu vurgulanmaktadır. Yazarların bu ayırımı , özellikle bilişim suçları açısından suçun konusu ya da suçta kullanılan araç olarak “*bilgisayar*”, 765 Sayılı TCK’de belirtildiği şekliyle, “*bilgileri otomatik işleme tabi tutmuş sistem*” ve TCK’de 243 vd. maddelerinde yer alan “*bilişim sistemi*”nin kapsamının ne olduğuna ilişkin tartışmalardan kaynaklanmaktadır.

765 Sayılı TCK’nin 525a vd. ve TCK’nin 243 vd. maddelerinde düzenlendiği şekliyle, suçun konusunun ya da suçta kullanılan aracın tespitinden önce bilişim suçu ile neyin anlaşılması gerektiğinin tespiti gerekmektedir. Yukarıda yapılan tanımlara dikkat edilecek olursa, Türk Hukukunda bilişim ya da bilgisayar suçları, bilişim sistemi, bilgileri otomatik işleme tabi tutan sistem ve bilgisayar terimlerinin anlam ve kapsamı belirlenmek suretiyle tanımlanmaktadır. Bu doğrultuda, bilişim ve bilgisayarın anlamlarından yola çıkılarak ve ayrıca bilişim sistemi olarak değerlendirilen araç ve aygıtlar ve de bilgisayar arasındaki farklar da

⁸⁵ Yüksel **ERSOY**, *Genel Hukuki Koruma Çerçevesinde Bilgisayar Suçları*, Prof. Dr. Yılmaz Günel’a Armağan Ank. Ün. SBFD, C. 49, Haziran-Aralık 1994, No. 3-4, Ankara 1995, s. 153 vd.

Yukarda kısmen aktarıldığı üzere, bilişim sistemleri ve özellikle bilgisayar sistemlerinin kötüye kullanımlarının suç olarak düzenlenmesine ilişkin bilişim suçu, bilgisayar suçu ayırımları yapıldığı görülmekte ve bilişim suçu teriminin daha geniş bir kapsama sahip olduğu ifade edilmektedir. Bu konu hakkında ayrıca bkz, **DÜLGER**, s. 63 vd.

esas alınarak bilişim ya da bilgisayar suçu tanımları yapılmaktadır. Aynı şekilde söz konusu suçların sınıflandırılmasında da suçta kullanılan araç ya da suçun maddi konusu olan bilgisayar ya da bilişim sistemi esas alınmaktadır.

Bilindiği üzere suçların sınıflandırılmasında suçun maddi konusu ya da suçta kullanılan araç esas alınabilmekte ve suçlar bu şekilde de ayırıma tabi tutulabilmektedir⁸⁶. Bu ayırım ise, *Toroslu*'nun ifade ettiği üzere, öncelikli olarak maddi konusu olmayan suçların bulunup bulunmadığına ilişkin tartışmalar nedeniyle çeşitli sorunlara yol açabilmekte, bir yandan da farklı nitelikteki suçların bir araya toplanması sonucunu doğurarak, suçların sınıflandırılmasında beklenen yararın sağlanmasına engel olmaktadır⁸⁷. Suçta kullanılan araç ise bazı suçlarda özellikle suça etki eden neden olarak önem taşıyabilmektedir.

Suçların, maddi konu ya da suçta kullanılan aracın esas alınarak sınıflandırılmaya tabi tutulmasında ortaya çıkan sakınca, aynı şekilde suçun maddi konusu ya da suçta kullanılan araç esas alınarak suçların tanımlanması durumunda da ortaya çıkmaktadır. Bu doğrultuda, suçta kullanılan araç ve suçun maddi konusu esas alınarak bilişim ya da bilgisayar suçlarının tanımı yapılması da sosyo-ekonomik dönüşüm içerisinde bilişim sistemlerinin hukuka etkisinin ve ortaya çıkardığı sorunların doğru biçimde tespitini zorlaştırmaktadır. Bilişim sistemlerinin kullanımının sorunları ne şekilde etkilediğinin saptanması bakımından maddi konu ya da kullanılan araç kapsamında bu suçların topluca incelenmesi kısmen yarar sağlamaktadır. Aynı şekilde, ceza mevzuatları içerisinde yer alan suçların

⁸⁶ Tanım ve sınıflandırma için örnek olarak bkz., **ERSOY**, s.159 – 162; **DÜLGER**, s. 111 vd.

⁸⁷ Nevzat **TOROSLU**, Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Ankara Üniversitesi Yayınları No:273, Ankara 1970, s. 61; Faruk **EREM** – Nevzat **TOROSLU**, Türk Ceza Hukuku Özel Hükümler, Savaş Yayınevi, 9. B., Ankara, 2003, s. 28 – 29.

unsurlarının bu tür fiilleri kapsayıp kapsamadığının tespiti bakımından da yarar sağlayabilmektedir. Fakat bu tür fiillerle hangi değere yönelik saldırının söz konusu olduğunun tespitinde yetersiz kalmaktadır. Nitekim bilişim ve özellikle bilgisayar sistemlerinin kullanımın yaygınlaşma oranına bağlı olarak, çok çeşitli fiillerin işlenebilir hale gelmesi, bu tanımların kapsamının çok farklı amaçlara yönelik suçları da kapsayacak şekilde genişletilmesine ya da kendi içerisinde alt ayırımlar yapılmasına neden olmaktadır⁸⁸.

Bilişim sistemlerinin kullanımının yaygınlaşması, özellikle bilgisayar sistemlerinin ağırlıklı olarak kullanımı, kullanıldığı amaç ve yere göre hukuki sorunlara yol açabilmektedir. Ceza hukuku bakımından ortaya çıkan sorunlar, suçun unsurlarından kaynaklanabildiği gibi cezalandırma siyaseti açısından daha önce suç olarak düzenlenmeyen bir fiilin, suç haline getirilmesinin gerekli olup olmadığı şeklinde ortaya çıkmaktadır. Özetle, suç ve cezada kanunilik ilkesi açısından mevcut suçların unsurlarının bu tür fiilleri kapsayıp kapsamadığı ya da bu tür fiillere ilişkin yeni suçların düzenlenmesi, sorunun odak noktasını oluşturmaktadır.

⁸⁸ Yazıcıoğlu, 2005 tarihli 5237 Sayılı TCK'de yer alan bilişim alanında suçları değerlendirdiği çalışmasında, üçlü bir ayırıma giderek; TCK'nin 244. vd maddelerindeki suçları “doğrudan bilişim suçları” ya da “dar anlamda bilişim suçları” bilişim teknolojilerinin getirdiği imkânlar dolayısıyla ortaya çıkan “haberleşmenin gizliliğini ihlal”, “haberleşmenin engellenmesi”, “kamu kurumu veya kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinin engellenmesi”, “kişisel verilerin kaydedilmesi” gibi suçları “dolayısıyla bilişim suçları” ve son olarak “müstehcenlik”, “kumar oynanması için yer ve imkan sağlanması” gibi suçları ise “bilişim teknolojileri marifetiyle işlenen klasik suçlar” şeklinde belirlemiştir. Yılmaz **YAZICIOĞLU**, *Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi*, Yeditepe Hukuk Fakültesi Dergisi, C. 2, S. 2, 2005, s. 396 – 397.

Suçun hukuki konusu açısından bakıldığında bunun anlamı, ortaya çıkan yeni fiiller karşısında, halihazırda çeşitli suçlar ile korunan hukuki değerlerin, bu tür yeni fiiller karşısında korunmasına ilişkin yöntemin saptanmasıdır.

Sieber, 1998 tarihli çalışmasında, bilgisayar suçları teriminin ilk olarak 1960'lı yıllarda ortaya çıktığını ve ilk başlarda sadece ekonomik çıkar amacıyla işlenen suçlar kapsamında değerlendirilen bilgisayar suçlarının, 1980'li yıllardan itibaren daha da genişleyerek, telif haklarına ilişkin ihlalleri, daha önce kişisel verilerin korunması olarak ayrı başlık altında incelenen hususları ve İnternetin yaygınlaşması ile birlikte, yasadışı içeriklerin dağıtımı gibi birçok konuyu da kapsamına aldığını ifade etmiştir. Bunun sonucunda “bilgisayar suçları” ve “bilgisayar ile ilgili suçlar” terimlerinin daha geniş bir şekilde her türlü kötüye kullanımları da kapsayacak şekilde genişletildiğini, sonrasında veri veya enformasyon suçu gibi çeşitli terimlerin de kullanıldığını ifade etmiştir. Yazara göre; çeşitli terim ve tanımlar bilgisayarın herhangi bir alanda kullanılması sonucu ortaya çıkan ve o alana ilişkin sorunlara işaret eden tanım ve terimlerdir. Bu nedenle yazar, belirli bir alanda ortaya çıkan sorunlara ya da amaca özgülenen veya teknik açıdan yapılan tanımların ve bunları ifade eden terimlerin, hukuki açıdan sınırlı bir değere sahip olduğunu ifade etmektedir. Bugüne kadar yapılan tanımların yerine, bilgisayar aracılığıyla gerçekleştirilen fiillerin, bu fiiller nedeniyle korunmak istenen hukuki değerlere göre tanımlanması ve incelenmesi gerektiğini savunmuştur. Yazar bu açıdan, “bilgisayarların kötüye kullanımları”, “*bilgisayarlarla ilgili ekonomik*

suçlar”, “bilgisayarla ilgili özel hayatın gizliliğini ihlal” ve diğer hukuki değerlere yönelik saldırı başlıkları altında üç grupta toplamıştır⁸⁹.

Sieber’in aktardığı şekliyle, bilişim, bilgisayar suçları, bilişim suçları gibi gibi birçok adlar altında incelenen suçlar, spesifik bir soruna işaret etmekten çok sosyo-ekonomik dönüşüm içerisinde bilişim sistemlerinin kötüye kullanımlarının yarattığı sorunlara çözüm arayışlarını kapsamaktadır. *Sieber’in* üç grup altında topladığı etki, bilişim alanındaki gelişime paralel olarak kendi bünyesine yeni konuları da katmaktadır. Bu husus aynı zamanda, bilişim suçu veya bilgisayar suçu gibi çeşitli adlar altında incelenen suçların niteliksel farklılıklarının olduğunu ve zamanla niteliksel farklıların artacağını gösterir.

Bünyesine yeni konuları da ekleyen söz konusu gelişim karşısında, bilişim ya da bilgisayar suçları olarak adlandırılan suçların yukarıda aktarılan, “*ceza kuralları uyarınca bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller*⁹⁰” örneğinde olduğu gibi suçun maddi konusu ya da suçta kullanılan araç olarak bilişim ya da bilgisayar sistemlerinin esas alınarak tanımlanması, farklı nitelikte ve farklı değerleri korumaya yönelik bir çok suçun bir araya toplanması ve incelenmesi sonucunu doğurur.

Aktarılan hususlar doğrultusunda bilişim ya da bilgisayar suçları olarak adlandırılan suçlara ilişkin bir tanım yapılması zordur. Suçta kullanılan araç ya da suçun maddi konusunun bilişim ya da bilgisayar sistemlerinin esas alınarak tanım yapılması ise, özellikle suçun hukuki konusu farklı olan birçok suçun bilişim ya da bilgisayar suçu olarak toplu bir şekilde incelenmesine neden olur. Bu durum

⁸⁹ **SIEBER**, s. 19 vd., ayrıca bkz dipnot 11.

⁹⁰ **YAZICIOĞLU, Bilgisayar Suçları**, s.142.

niteliksel olarak farklı olan bir çok suçun bir araya toplanması anlamına gelir. Bu tür tanımlar sadece ,ortak özelliği bilişim ya da bilgisayar sistemlerinin kullanılması olan suçların, bilişim suçları ya da bilgisayar suçları adı altında incelenmesi açısından etkinin yönü, boyutları ve derinliği hakkında bilgi verir. Bunun ötesinde niteliksel bir anlam taşımaz.

Özetle, bilişim suçları ya da bilgisayar suçlarına ilişkin bir tanım yerine, bilişim ya da bilgisayar suçları adı altında incelenen suçların, bilişim ya da bilgisayar sistemlerinin kullanımının belirli bir dönemde ceza hukukuna etkisi olarak nitelendirilmesi mümkündür. *Sieber*'in ifade ettiği şekliyle, ceza hukuku bakımından etki, farklı hukuki değerlere yönelik ihlalleri içermektedir.

İhlal edilen değere göre de ayırım yapılabilecek olan bu etki yeni suç tiplerinin ceza mevzuatı içerisine girmesi bunun yanında halihazırdaki suçların işlenme kolaylığının ortaya çıkması ya da işlenme oranının artması şeklinde, ayırıma tabi tutulabilir.

Sonuç olarak, “*bilişim suçu*”, “*bilgisayar suçu*”, adları altında incelenen suçlar, hukuki konu açısından kategorik bir nitelik taşımamaktadır. Bunlara ilişkin tanımlar da “*bir kavramın niteliklerini eksiksiz olarak belirtme veya açıklama*⁹¹” anlamında, tanımdan beklenen faydayı göstermekten uzaktır. Bilişim suçları, bilgisayar suçları gibi adlar altında incelenen suçlar ise, bilişim sistemlerinin ceza mevzuatlarına etkisi bakımından belirli bir dönemde ceza mevzuatlarında yer verilen suç tiplerini ifade etmektedir. Bunun yanında halihazırda ceza mevzuatları içerisinde yer alan bazı suçların bilişim suçu vs. adlar altında incelenmesi, söz konusu suçların işlenme yoğunluğunun bilişim sistemlerinin kullanılması ile artmasında yatmaktadır.

⁹¹ Bkz. “Güncel Türkçe Sözlük” <http://www.tdk.gov.tr>

İncelemede “*bilişim suçu*” teriminin kullanılması, belirli bir tanımın esas alınmasından çok, bu ad altında incelenen suçların sosyo-ekonomik dönüşümle bağlantısının daha rahat kurulabilmesine olanak sağlamasından dolayı tercih edilmiştir.

B. Bilişim Suçları Açısından Avrupa Konseyi Siberaç Sözleşmesi

Sosyo-ekonomik dönüşüm içerisinde bilişim sistemlerinin kullanımının ceza hukukuna etkisi sadece ülkesel düzeyde düzenlemelerin konusu olmakla kalmamış aynı zamanda “*Avrupa Konseyi Siberaç Sözleşmesi*”nin de konusunu oluşturmuştur. 23. 11. 2001 tarihinde Macaristan’ın başkenti Budapeşte’de imzaya açılan Sözleşme ve Türkiye tarafından da imzalanmıştır. 48 maddeden oluşan Sözleşme, 1.07. 2004 tarihinde yürürlüğe girmiştir.

Sözleşmede, bir bilişim sistemi olarak bilgisayar sistemlerinin ceza hukukuna etkisi ve ortaya çıkardığı sorunlar, hem maddi ceza hukuku açısından hem de ceza yargılaması açısından ele alınmış ve bu alanlarda bilgisayar sistemlerinin kullanılması merkezinde ortaya çıkan sorunlara ilişkin çözümler getirilmek istenmiştir. Sözleşmenin ikinci kısmını oluşturan maddi ceza hukukuna ve ceza yargılamasına ilişkin sorunlar iki ana bölüme ayrılmış ve birinci bölümde maddi ceza hukukuna ilişkin düzenlemelere yer verilmiştir⁹². İkinci bölümde ise, ceza

⁹² Sözleşmede yer alan suçların genel değerlendirmesi için bkz., Füsun **SOKULLU-AKINCI**, *Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi*, İHFM, C. LIX, S. 1-2, 2001, s. 11 vd. Ayrıca bkz., Indira CARR, *Draft Cyber Crime Convention, Criminalization and the*

yargılamasına ilişkin sorunlar ele alınarak özellikle delillerin elde edilmesi, korunması ve saklanması ile ilgili olarak ortaya çıkan sorunlara çözüm getirilmek istenmiştir⁹³.

Bunun yanında, bilişim suçları olarak adlandırılan suçların özellikle bilişim ağları ile işlenmesinin yaygın bir hal alması ve İnternetin hızla yaygınlaşması, bu suçlara ilişkin sorunların ulusal bir sorun olmaktan çok uluslar arası bir sorun haline gelmesi gerçeğinden hareketle üçüncü bir kısma yer verilmiştir. Bu kısmın konusu ise, Sözleşmeye taraf devletlerin birbirleri arasında adli yardımlaşmaları ve suçluların iadesidir.

Sözleşmenin amaçları, “1.Siber suçlar alanında ülkelerin maddi ceza hukuku hükümlerini uyumlu hale getirmek, 2. Bu suçların ve bilgisayar sistemi kullanılarak işlenen ya da delilleri elektronik formda olan başka suçların soruşturulması ve koğuşturulması için gerekli olan ulusal ceza muhakemesi hukuku yetkilerini belirlemek, 3. Hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmak” şeklinde sıralanmaktadır⁹⁴.

Council of Europe (Draft)Convention on Cyber-Crime, Computer Law & Security Report Vol.18, no. 2, 2002, s. 84 vd.

⁹³ Sibera suç sözleşmesinin ceza yargılamasına ve özellikle delillerin elde edilmesi, korunması ve saklanması ile ilgili hükümler hakkında bkz., Serap **KESKİN**, *Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*, İHFM, C. LIX, S. 1-2, 2001, s. 162. vd.

⁹⁴ **KOCA**, s. 791; Kayıhan **İÇEL**, *Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında “Avrupa Siber Suç Politikasının Ana İlkeleri* İHFM, C. LIX, S. 1-2, 2001, s. 6. Yazar Sözleşmeden yola çıkarak bu alanda ortaya çıkan ceza sorumluluğunun düzenlenmesi sırasında göz önünde bulundurulması gereken ana ilkelerin saptanabildiğini belirtmektedir. “İnternet Ortamında Ceza Sorumluluğunun Avrupa Ana İlkeleri” olarak adlandırdığı ilkeleri şu şekilde sıralamaktadır: 1. Siber suçlarla ilgili ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce özgürlüğü olmak üzere tüm temel hak ve özgürlüklerin gereklerine uyulması; 2. Bilgisayarlarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde ortak minimum standarda uyulması; 3. Eylemin hukuka aykırı olması; 4. Eylemin kasten işlenmesi.

Sözleşmede yer ver verilen suçlarda ortak amaç, bu tür suçlara ilişkin olarak taraf devletlerin ceza mevzuatlarında uyum sağlamadır Sözleşmede yer alan suçlar, daha önceki dönemlerde çeşitli ülkelerin ceza mevzuatları içerisinde düzenlenmiş olan suçların uluslar arası düzeyde ele alınması şeklinde olmuştur. Aşağıda bu suçlara genel olarak değinilecektir.

Sözleşmenin ikinci kısmında “ *Bilgisayar Veri ve Sistemlerinin Gizliliğine, bütünlüğüne ve Erişilebilirliğine karşı suçlar*” başlığı altında yetkisiz erişim (2. madde) yetkisiz müdahale (3. madde), verilere müdahale (4. madde), sisteme müdahale (5. madde) ve aygıtların kötüye kullanılması (madde 6) suçlarına yer verilmiştir.

“*Yetkisiz erişim*”, Sözleşmenin 2. maddesinde, kasten ve hukuka aykırı bir şekilde bir bilgisayar sisteminin tamamına veya bir kısmına girme şeklinde tanımlanmıştır. Aynı maddede, yetkisiz erişim suçunun taraf devletlerin ceza mevzuatlarında düzenlenirken, güvenlik önlemlerinin ihlal edilmesi suretiyle işlenebileceğine, verinin elde edilmesi ya da diğer gayri meşru bir niyetle sisteme girilmesi ya da bilgisayar ağları vasıtasıyla birbirine bağlı bilgisayar sistemleri aracılığıyla işlenebileceğine ilişkin ek unsurları getirebilecekleri belirtilmiştir.

“*Yetkisiz müdahale*” ise Sözleşmenin 3. maddesinde düzenlenmiş olup buna göre, bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, bunlara teknik yöntemler kullanılmak suretiyle müdahale edilmesinin suç haline getirilmesi

öngörülmüştür. Bu maddeye göre, taraf devletlerin bu suçun oluşmasını kötünîyet ya da bilgisayar ağları aracılığıyla işlenmesi şartına bağlayabilmeleri mümkündür⁹⁵.

Sözleşmenin 4. maddesinde veriye müdahale, 5. maddesinde sisteme müdahale düzenlenmiştir. Sözleşmenin 4. maddesinde göre, veriye zarar verilmesi, verinin bozulması, değiştirilmesi veya ortadan kaldırılmasının suç olarak düzenlenmesi gerekmektedir. Madde incelendiğinde, verinin bilgisayar içinde bulunması ya da herhangi bir saklama aygıtı içerisinde olması arasında fark yaratılmadığı görülmektedir. Aynı maddenin ikinci fıkrasında, taraf devletlerin söz konusu suçun gerçekleşmesi için ciddi zararın varlığı şartına yer verebilecekleri ifade edilmiştir.

Beşinci maddede ise sisteme müdahale düzenlenmiştir. Sözleşmenin beşinci maddesinde sistemin işleyişinin ciddi olarak engellenmesinin suç haline getirilmesi gerektiği belirtilmiştir. Sistemin işleyişinin engellenmesine ilişkin müdahaleler ise sisteme veri yoluyla müdahale edilmesi ya da sistem içerisindeki verilere müdahale edilmesi esas alınarak düzenlenmiştir. Bu açıdan fiziki müdahaleler sözleşmede sistemin işleyişine müdahale kapsamında değerlendirilmemiştir.

⁹⁵ Sözleşmenin açıklayıcı raporunda bu suçun geleneksel haberleşmenin gizliliğini korumaya yönelik olduğu ifade edilmiştir. Maddede yer alan kamuya kapalı olan veri iletimi verinin içeriğinden bağımsız olarak ele alınmakta ve tarafların bu tür verilerin iletimi sırasında bunların gizli kalmasına ilişkin niyetlerinin önemli olduğu bu şekliyle de şekli sırrın söz konusu olduğu belirtilmektedir. Aynı şekilde ticari bir amaç için bu tür verilerin gizli tutulmasının da söz konusu olabileceği raporda belirtilmiştir. Rapora göre verinin iletiminin kamusal ağlar aracılığıyla yapılıp yapılmaması önemli değildir. Maddede bilgisayarlar aracılığıyla iletilen veriye müdahale bakımından tek bir bilgisayarın parçaları arasında verinin iletilmesi ya da bilgisayarlar arasında verinin iletilmesi bakımından bir farklılık yaratılmamıştır. Elektromanyetik dalgalara müdahalenin de madde içerisinde yer almasına ilişkin raporda bunların Sözleşmede yapılan tanım gereği veri kapsamında olmadığı, bunların bilgisayarlar aracılığıyla dönüştürüldüğü ifade edilmiştir. Bkz., **Convention on Cybercrime (ETS No. 185), Explanatory Report**, parag. 51. vd. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>. Ayrıca bkz., **KOCA**, s. 796 vd

Sözleşmenin 6. maddesinde ise birtakım hazırlık hareketlerinin suç olarak düzenlenmesi yoluna gidildiği görülmektedir. Nitekim 6. maddenin 1. fıkrasına göre Sözleşmenin 2-5. maddelerinde düzenlenen suçların işlenmesi için öncelikli amacının söz konusu suçların işlenmesine yönelik tasarlanmış ya da uyarlanmış olan program da dahil cihazların (m. 1/a.i); söz konusu suçların işlenmesi amacıyla, bir bilgisayarın tamamına ya da bir kısmına erişimi sağlayabilecek bir bilgisayar şifresinin, erişim kodunun ya da benzer verinin (m. 1/a.ii), üretiminin, satışının, kullanılmak için tedarikinin, ithal edilmesinin, dağıtılmasının ya da diğer şekilde erişilebilir kılınmasının taraf devletlerce suç olarak düzenlenmesi hükmüne yer verilmiştir.

Aynı maddenin “b” bendinde, Sözleşmenin 2 ila 5. maddeleri arasında düzenlenen suçların işlenmesi amacıyla, “a” bendinde sayılan hususların elde bulundurulmasının suç olarak düzenlenmesi gerektiği ifade edilmiştir. Elde bulundurmanın suç sayılabilmesi için taraf devletlerin yukarıda sayılanların belirli bir sayıda olmasına ilişkin ek şart getirebilecekleri hükmüne yer verilmiştir.

Maddenin 2. fıkrasına göre yukarıda sayılan hükümler, bu tür aygıt ya da programların, bir bilgisayarın korunması ya da test amacı gibi Sözleşmenin 2 ila 5. maddelerinde belirtilen suçların işlenmesi amacını gütmeyen meşru amaçlar için üretimi, satışı, kullanılmak için tedariki, ithal edilmesi, dağıtılması ya da diğer şekilde erişilebilir kılınmasını cezalandıracak şekilde yorumlanamaz

Aynı maddenin son fıkrasında ise, bilgisayar şifreleri, erişim kodlarının ya da benzer verilerin satışının, dağıtımının ya da diğer şekillerde erişilebilir kılınmasının cezalandırılabilmesine ilişkin hükümler saklı tutulmak kaydıyla, taraf devletlerin

ceza mevzuatları içerisinde birinci fıkrada düzenlenen hususları kapsam dışı bırakabileceği belirtilmiştir.

Sözleşmenin 7. ve 8. maddelerinde, bilgisayar aracılığıyla sahtekarlık ve bilgisayar aracılığıyla dolandırıcılık fiilleri düzenlenmiştir. Yedinci maddeye göre bilgisayar aracılığıyla sahtekarlık, *“verilerin açıkça okunabilir ya da anlaşılabilir olup olmadığına bakılmaksızın Bilgisayar verilerinin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi ya da hareket edilmesi amacıyla verilerin orijinalliğinin bozulması sonucunu doğuran, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme, fiillerin hukuka aykırı olarak kasten işlenmesi”* şeklinde tanımlanmıştır. 8. maddede düzenlenen bilgisayar aracılığıyla dolandırıcılık, sistemin işleyişine ekonomik bir yarar sağlanması amacıyla müdahale edilmesi ve yarar sağlanması şeklinde tanımlanmış ve maddede sisteme yeni veri yerleştirilmesi, verinin değiştirilmesi, silinmesi veya erişilmez kılınması, bunların yanında sistemin işleyişine diğer herhangi bir müdahale seçimsel hareketler olarak düzenlenmiştir.

Sözleşmenin 9.maddesinde ise içerikle ilgili suçlar başlığı altında çocuk pornografisinin yasaklanmasına ilişkin hükümler getirilmiştir. Bu kapsamda yasaklanan fiiller, bilgisayar sistemleri aracılığıyla dağıtmak amacıyla çocuk pornografisinin üretilmesi (m. 9/1.a), sunulması veya temin edilebilir hale getirilmesi (m. 9/1.b) ; dağıtılması ya da iletilmesi (m. 9/1.c); kendisi ya da başkası için bilgisayar sistemi aracılığıyla elde edilmesi (m.9/1.d); son olarak, bilgisayar sistemi içerisinde ya da bilgisayar veri depolama ortamında çocuk pornografisi bulundurulmasıdır (m. 9/1.e). Maddede çocuk pornografisi, bir küçüğün cinsel

içerikli bir eylemde kullanılması, küçük gibi görünen bir kişinin cinsel içerikli bir eylemde kullanılması ya da bir küçüğün cinsel içerikli bir eylemde yer aldığını temsil eden gerçekçi imaj olarak tanımlanmıştır. Maddeye göre, küçük 18 yaşından küçükleri ifade etmekte, taraf devletlerin 16 yaşına kadar indirilebilmelerine imkan tanınmaktadır⁹⁶.

10. maddede ise, telif hakları ve bağlantılı hakların korunmasına ilişkin uluslar arası düzenlemelerde yer alan hükümlerin etkin bir şekilde uygulanabilmesi ve de ihlallerin cezalandırılabilmesine ilişkin cezai hükümlerin getirilmesi düzenlenmiştir.

Sözleşme incelendiğinde, bilişim suçlarının, Sözleşmedeki ifadesiyle siber suçların kapsamının sadece bilgisayar ve veriye yönelik fiilleri esas almadığı bilişim sistemlerinin kullanılmasıyla ve özellikle İnternetin yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan sorunları da kapsadığı görülmektedir. Bu açıdan çocuk pornografisi, telif haklarına ilişkin ihlaller ve son olarak Sözleşmeye yapılan ek protokolle kapsama alınan, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler de bu grubu oluşturmaktadır. Sözleşmede bu suçların minimum bir uzlaşmayı temsil ettiği ve taraf devletlerin kendi mevzuatlarında başka suçları da öngörebilecekleri belirtilmiştir.

C. Bilişim Suçları Açısından Türk Ceza Kanununun Kapsamı

⁹⁶ Sıbersuç sözleşmesinde yer alan çocuk pornografisine ilişkin hükümlerin tahlili ve çocuk pornografisinin genel görünümü ve etkileri hakkında bkz., . SOKULLU-AKINCI, s. 28. vd.

Sibersuç Sözleşmesinden aktarıldığı üzere günümüzde bilişim suçları, bilgisayar suçları ya da siber suçlar gibi adlar altında incelenen suçlar, sadece yetkisiz erişim, sisteme ve veriye müdahale, bilişim sistemi aracılığıyla sahtekarlık ya da dolandırıcılık suçları ile sınırlı tutulmamaktadır. Söz konusu suçlar, bilişim sistemlerinin ceza hukukuna etkisi bakımından belirli dönemlerde ortaya çıkan niceliksel ve niteliksel etkilere bir tepki olarak gündeme gelmiştir.

Sosyo – ekonomik dönüşüm içerisinde bilişim sistemlerinin ceza hukukuna etkisi bakımından, bir çok ülkede öncelikli olarak yukarıda sayılan suçların ceza mevzuatları içerisinde düzenlendiği görülmektedir. 765 Sayılı TCK'nin da bu gelişimin etkisiyle 1991 yılı değişiklikleri ile birlikte bilişim alanında suçlar başlıklı 11. babında çeşitli suçlar düzenlenmiştir. 525a maddesinde genel olarak verinin ve programın ele geçirilmesi ve ayrıca ele geçirilen veri ya da programın başkasına zarar vermek üzere kullanılması fiilleri suç olarak düzenlenmiştir. 525/b 1. fıkrasında bilgileri otomatik işleme tabi tutmuş sisteme ve veriyle müdahale fiilleri, 2. fıkrasında bilgileri otomatik işleme tabi tutan bir sistemi kullanılarak yarar sağlama fiilleri suç haline getirilmiştir. Aynı şekilde bilgileri otomatik işleme tabi tutmuş sistem aracılığıyla sahtekarlık suçuna 525c maddesinde yer verilmiştir.

5237 Sayılı TCK'de ise bilişim alanında suçlar başlığı altında 765 Sayılı TCK'nin 525a vd. maddelerinde düzenlenen suçlar yeniden ele alınmış ve kimi yönleriyle farklı bir düzenlemeye gidilmiştir. Nitekim 765 Sayılı TCK'nin 525a maddesinde suç olarak düzenlenen fiillere TCK'de yer verilmemiş bunun yerine Sibersuç Sözleşmesinde olduğu şekliyle yetkisiz erişim suçu düzenlenmiştir. Aynı şekilde sisteme ve veriye müdahale fiilleri farklı bir şekilde ele alınmış ve 765 Sayılı TCK'nin 525b 1. fıkrasında topluca tek bir fıkra düzenlenmiş suç 244. maddenin

1. ve ikinci maddelerinin konusunu oluřturmuřtur. Bu aıdan suun unsurlarında da 765 Sayılı TCK’nin 525/b 1. fıkrasından farklılıa gidilerek 244. maddenin 1. fıkrasında sisteme mdahale, 2. fıkrasında ise biliřim sistemi ierisinde veriye mdahale dzenlenmiřtir. Biliřim sistemi aracılıėıyla dolandırıcılık 765 Sayılı TCK’nin 525b 2. fıkrasından farklı bir řekilde ele alınmıř ve sisteme ve veriye mdahale fiillerin gerekleřtirilmesi suretiyle yarar saėlamaya iliřkin bir dzenleme yapılmıřtır. Bunun yanında biliřim sistemin kullanılması TCK’nin 142. maddesinde, hırsızlık suunun, biliřim sisteminin ara olarak kullanılması ise, TCK’nin 158. maddesinde, dolandırıcılık suunun aėırlatıcı nedeni olarak dzenlenmiřtir. Ayrıca, 765 Sayılı TCK’nin yrrlkte olduėu dnemde, banka ve kredi kartlarının hukuka aykırı kullanımını ieren bir takım fiiller bakımından, zellikle biliřim alanına iřlenen sular ile diėer sular arasında ortaya ıkan itima sorunlarının mlenme amacına ynelik olduėunu ifade edebileceėimiz, banka ve kredi kartlarının hukuka aykırı kullanımına iliřkin eřitli fiilleri ieren sular, biliřim alanında sular arasında TCK’nin 245. maddesinde dzenlenmiřtir. TCK’nin 765 Sayılı TCK’de yer alan ve Siberau Szleřmesinde de dzenlenen biliřim sistemi aracılıėıyla sahtecilik suuna iliřkin zel bir dzenlemeye yer verilmediėi grlmektedir⁹⁷.

⁹⁷ “*Biliřim Aėı Hizmetlerinin Dzenlenmesi ve Biliřim Suları Hakkında Kanun Tasarısı*”nda ise yetkisiz eriřim suunun yeniden dzenlendiėi, bunun yanında yetkisiz eriřim suuna iliřkin 17. maddenin 1. fıkrasının b bendinde verinin ele geirilmesi suuna da yer verildiėi grlmektedir. Aynı řekilde Tasarının 18. maddesinde Siberau Szleřmesinin de konusunu oluřturan yetkisiz mdahalenin “hukuka aykırı” izleme adı altında dzenlenmiřtir. Tasarının 19 ve 20. maddelerinde veriye mdahale ve sisteme mdahale sularının yeniden dzenlendiėi grlmektedir. Bunun yanında Tasarının 22. maddesinde biliřim sistemi kullanılarak sahtecilik ve 23. maddesinde biliřim sistemi aracılıėıyla yarar saėlama suları 765 Sayılı TCK’nin 525c ve 525b/ 2. maddesindeki sulara unsurları itibarıyla benzer bir řekilde dzenlenmiřtir. Biliřim sularının listesinin Tasarıda daha da geniřletildiėi grlmektedir. Bu ynde Tasarının 24. maddesinde “yanılarak bilgi toplama” ve 25. maddede “*taklit yoluyla yanılmak*” sularına yer verilmiřtir.

Bilişim suçları, sosyo – ekonomik dönüşüm içerisinde bilişim sistemlerinin kullanımının ceza hukukuna etkisi olarak geniş anlamda ele alındığında, bilişim suçları arasında incelenebilecek olan diğer bir grup suça 765 Sayılı TCK'den farklı olarak TCK'nin 135 vd. maddelerinde rastlanmaktadır. Kişisel verilerin korunmasına ilişkin suçlar olarak adlandırılabilir söz konusu suçlar, Siberaş Sözleşmesinin içerisinde yer almamakla birlikte üçüncü bölümde inceleneceği üzere kişisel verilerin korunmasına ilişkin Avrupa Konseyi Sözleşmesinin konusunu oluşturmaktadır. 1970'li yıllardan itibaren bir çok ülkenin mevzuatında yer almaya başlayan kişisel verilerin korunmasına ilişkin kanunlarda öngörülen, kişisel verilerin işlenmesine ilişkin usul ve esasların ihlali olarak düzenlenen kişisel verilerin korunmasına ilişkin suçlar, her ne kadar ülkemizde kişisel verilerin korunmasına ilişkin bir kanun olmasa da, TCK'de düzenlenmiştir. TCK'nin 135. maddesinde “*kişisel verilerin kaydedilmesi*”, 136. maddesinde “*verileri hukuka aykırı olarak verme, ele geçirme*”, 138. maddesinde “*verileri yok etmeme*” suçları yer almaktadır.

Siberaş Sözleşmesinin ve Siberaş Sözleşmesine ek protokolün konusunu oluşturan bilişim sistemlerinin kullanımının niceliksel bir etkisi olarak ortaya çıkan çocuk pornografisi, ırkçılık ve yabancı düşmanlığına yönelik suçlara ise, Türk Ceza

Siberaş Sözleşmesinde “içerikle ilgili suçlar” arasında düzenlenen TCK'de ise, müstehcenlik suçu içerisinde düzenlenen çocuk pornografisine ilişkin fiillerin de Tasarının 26. maddesinde düzenlendiği görülmektedir. Söz konusu maddede çocuk pornografisi suçunun unsurlarının “*çocuk gibi görünen veya çocuk olduğu izlenimi veren bir kişiye ait gerçek ya da temsili görüntü, yazı veya sesleri içeren pornografik ürünler*” şeklinde genişletildiği ve bu tür ürünlerin üretimi dağıtımı gibi çeşitli fiiller suç olarak düzenlenmiştir.

Tasarının 27, 28 ve 29. maddelerinde ise kişisel verilerin korunmasına ilişkin suçların da dahil olduğu TCK'de düzenlenen bir takım suçların bilişim ağı üzerinden işlenmesi ağırlıca neden olarak düzenlenmiştir. Tasarının 30. maddesinde ise bilişim ağı üzerinden kumar oynatma suçuna yer verilmiştir.

Tasarı için bkz., <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm> .

Kanununda ilgili bölümlerde yer verildiği görülmektedir. Nitekim TCK'nın 216. maddesinde *“halkı kin ve düşmanlığa tahrik veya aşağılama”* suçu adı altında düzenlenen suç özellikle ırkçılık ile ilgili fiilleri içermektedir. Aynı şekilde çocuk pornografisine yönelik fiiller, çocukların müstehcen içerikli ürünlerden korunmasına ilişkin fiillerin de yer aldığı, TCK'nın 226. maddesindeki *“müstehcenlik”* suçu içerisinde yer almaktadır.

İKİNCİ BÖLÜM

BİLİŞİM ALANINDA SUÇLAR

I. GENEL OLARAK

Sosyo-ekonomik dönüşüm içerisinde bilişim sistemlerinin kullanımının yaygınlaşmasına paralel olarak, bunların kötüye kullanımlarının cezalandırılabilirliği sorunu ya da bu tür kötüye kullanımlar açısından bilişim sistemlerinin ceza hukukuna etkisine ilişkin tartışmaların ağırlıklı olarak ortaya çıktığı fiiller ceza mevzuatımız içerisinde de yer edinmiştir. Söz konusu suçlar, 765 Sayılı TCK'nin 525a vd. maddelerinde ve 5237 Sayılı TCK'nin, kredi kartlarının kötüye kullanımına ilişkin suçlar bir yana bırakılacak olursa, 243 vd. maddelerinde düzenlenmiştir. Bilgisayar ve bilişim suçlarına ilişkin ilk tartışmalardan birisini oluşturması, sadece bu tür fiillerin bilişim ya da bilgisayar suçu olarak adlandırılmasına da yol açmıştır.

Bilişim alanında suçlar başlığı altında TCK'nin 243 vd. maddelerinde “yetkisiz erişim”, “sisteme ve veriye müdahale”, “bilişim sistemleri aracılığıyla yarar sağlama” ve “banka ve kredi kartlarının kötüye kullanımı” suçlarına yer verilmiştir. Bu suçlar içerisinde bu bölümün konusunu “verinin ele geçirilmesi ve yetkisiz erişim”, “sisteme ve veriye müdahale” ve son olarak “bilişim sistemi aracılığıyla yarar sağlama” şeklinde ortaya çıkan ve birçok ülkenin ceza mevzuatları içerisinde düzenlenen suçların 5237 Sayılı TCK'deki görünümü

oluşturmaktadır. Her ne kadar yürürlükten kalkmış olsa da 765 Sayılı TCK'nin 525a vd. maddelerinde düzenlenen suçlara da gerekli olduğu ölçüde değinilecektir. Bu husus, bilişim alanında suçların Türk Ceza Hukukunda gelişimi hakkında bilgi verme açısından ve TCK'de bilişim alanında suçların düzenlenmesinde 765 Sayılı TCK'nin 525a vd. maddelerinin ortaya çıkardığı sorunlardan kimi yönlerden etkilenilmesi bakımından önem arz etmektedir. Ayrıca "*Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı*"nda yer alan kimi suçlarda 765 Sayılı TCK'nin 525a vd. maddelerinde düzenlenmiş bulunan suçlardan da etkilenilmiş olması, 765 Sayılı TCK'de yer alan suçlara da değinilmesi zorunluluğunu doğurmaktadır.

İkinci bölümde inceleme bölümde incelenen suçlarda, söz konusu suçların hukuki konularının ve suç olarak düzenlenen fiillerin karşılaştırmalı hukuk ve Türk Ceza hukukunda tespitine ağırlık verilmiştir. Bu iki konuya ağırlık verilmesinin nedeni karşılaştırmalı hukukta da ortaya çıktığı üzere, bilişim alanında suçlarda neyin nasıl korunduğunun asıl soru olarak gündeme gelmesidir. Bu noktadan bakıldığında, 5327 s. TCK'de 243. vd maddelerinde düzenlenen suçlar bakımından suçun manevi unsurunun tespiti ikincil bir sorun olarak karşımıza çıkmaktadır. Nitekim TCK'de bilişim alanında suçların düzenlenişinde suçların kural olarak genel kast ile işlenmeleri esas alınmıştır. 243. maddenin son fıkrasında ise, sorumluluk esasının TCK'nin 23. maddesinde düzenlendiği şekliyle neticesi sebebiyle ağırlaşan suçun bir görünümüne yer verilmiştir. Ayrıca 244. maddenin son fıkrasında düzenlenen bilişim sistemi aracılığıyla yarar sağlama suçu için yarar sağlama amacına yönelik özel kast aranmaktadır.

Suçun faili bakımından incelendiğinde de TCK'nin 243. vd. maddelerinde düzenlenen suçlar için failde herhangi bir özellik aranmadığı görülmektedir. Bu nedenle 243. vd. maddelerinde düzenlenen suçların faili herkes olabilir. Bu anlamda bu suçlar “*genel suç*” niteliğindedir.

II. BİLİŞİM ALANINDA SUÇLAR AÇISINDAN TÜRK CEZA KANUNUNUN SİSTEMATİĞİ

Birinci bölümde aktarıldığı üzere, *Yazıcıoğlu* tarafından dar anlamda bilişim suçları olarak adlandırılan, Kanundaki ifadesiyle “*Bilişim Alanında Suçlar*”, ilk olarak 765 Sayılı TCK’de, 1991 yılında 3765 Sayılı kanunla yapılan değişiklikler sırasında düzenlenmiştir. Hukuki konu kriteri esas alınarak cürümlerin 10 bab halinde düzenlendiği 765 Sayılı TCK’ye bilişim alanında işlenen suçlar, toplu bir şekilde, 11. bab olarak eklenmiştir. Bilişim suçlarının 765 Sayılı TCK’de düzenlenmesinde ise, genel olarak 1989 tarihli Türk Ceza Kanunu Tasarısı esas alınmış olup, bu tasarıda yer alan hükümlerde ise Yeni Fransız Ceza Kanununun Öntasarının 323-1 - 323-7 maddelerinde yer alan -88-19 no.lu Kanun ile eklenen 462-2 - 462-9 maddelerinin model alındığı- hükümlerden esinlenilmiştir⁹⁸.

Bilişim alanında işlenen suçların, 765 Sayılı Türk Ceza Kanununda, özel kısmının sistematığında esas olan hukuki konu kriterinin bir yana bırakılarak ayrı bir bab altında toplanması, sistematik bir düzenleme kaygısı güdülmediğini göstermektedir. Nitekim bu husus, “*Yabancı kanunlardan bir kısmı, bilişim*

⁹⁸ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 613, Ayrıca bkz. Ayhan **ÖNDER** Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul, 1994, s. 505, Yılmaz **YAZICIOĞLU**, Bilgisayar Suçları, s. 207

alanındaki suçları ayrı bir bölümde toplamayarak ilgili suç bölümlerine yerleştirmektedirler. Kanunda ise bu suçların uygulamada kolaylık sağlamak üzere ayrı bir bölümde düzenlenmesi tercih edilmiştir.” şeklinde ifade edilmiştir⁹⁹.

Bilişim alanında suçların bu şekilde düzenlenmesi doktrinde kimi yazarlarca eleştiri konusu yapılmış iken kimi yazarlarca da savunulmuştur. Düzenlemeye ilişkin eleştiriler, 765 Sayılı TCK’de bilişim alanında işlenen suçların, hukuki konularına göre tasnif edilmeksizin bir arada ayrı bir babda düzenlenmesi noktasında toplanmaktadır¹⁰⁰.

⁹⁹ TBMM Tutanak Dergisi 6.6.1991, Dönem 18, Y.4, C. 61, Birleşim 119-131, s. 17, Sayfa Sayısı 513, aktaran **YAZICIOĞLU, Bilgisayar Suçları**, s. 212.

¹⁰⁰ “Kanunumuzun 525a, b, c, d maddelerinde Fransız Projesinin 307. maddesinden yararlanılarak bir bâb oluşturulmuş, bilgisayar ortak özellik teşkil etmek suretiyle, hukuki konuları birbirinden farklı hükümlere bir sıra içinde yer verilmiştir. Bu sistemin sakıncası açıktır. Gerçekten, bilgisayar suçlarının düzenlenmesinde yalnız hukukçu olmak yetmemekte, bilgisayar tekniğinden de yararlanmak gerekmektedir. Bundan başka, böyle bir sistemde, korunan hukuki konular birbirinden ayrılmamış birbiri yanında yer almış olmalarının sonucu, bir hükmün yorumunda hangi esasın ve yararın izlenmekte olduğu saptanamayacaktır”. **ÖNDER**, s. 506.

Bunun yanında 3765 Sayılıyılı Kanunla 765 Sayılıyılı TCK’ye 11. bab olarak eklenen bilişim alanında suçların, TCK’nin sistematığına tamamen ters bir düzenleme olduğunu ifade edilmiştir. **EREM - TOROSLU, Özel Hükümler**, 9. B., Ankara, 2003, s. 41. Aynı yönde *Hafizoğulları*, da 765 Sayılı TCK’de bilişim alanında işlenen suçların “Onbirinci Bab” olarak eklenmesiyle yeni bir suç kategorisine dolayısıyla yeni bir hukuki değere yer verildiğini ifade etmekle birlikte bilişim suçlarının diğer bablarında düzenlenen suçların yeni türevleri mi olduğu yoksa bu değerlerden bağımsız hukuki bir değeri mi ifade ettiğinin tartışılması gerektiğini ifade etmiştir. Zeki **HAFIZOĞULLARI, Türk Ceza Hukuku’nun Seksen Yılı**, Cumhuriyetim Kuruluşundan Bugüne Türk Hukukunun Seksen Yıllık Gelişimi, Ankara Üniversitesi Hukuk Fakültesi Yayınları No: 538, 30-31 Ekim 2003, Sempozyum, s. 202.

Ersoy, da 765 Sayılıyılı TCK’nin 11. babında düzenlenen fiillerin belirli bir sistematik içerisinde değerlendirilmesinin zor olduğunu ifade etmektedir. Yazar devamında 765 Sayılı TCK’nin 525/a, 525/ b maddelerinde düzenlenen suçların malvarlığına yönelik suçlar olduğunu, 525/c maddesinde düzenlenen suçun ise sahtekarlık cürümlerindeki ile aynı nitelikte bir menfaatin korunmak istediğine işaret ederek TCK’nin sistematığı içerisinde 11. babda düzenlenen suçlar itibarıyla yeni bir hukuki konunun söz konusu olmadığını vurgulamıştır. **ERSOY**, s.166 – 167.

Siber Suçlar Sözleşmesinin açıklayıcı raporunda Sözleşmede yer alan suçlarla korunmak istenen değerlerin halihazırda çeşitli suçların hukuki konusunu oluşturduğu ifade

TCK’de ise bilişim alanında suçlar, Kanunun “*Topluma Karşı Suçlar*” başlıklı üçüncü kısmının, “*Bilişim Alanında İşlenen Suçlar*” başlıklı onuncu bölümünde düzenlenmiştir. TCK sistematik olarak incelendiğinde, bilişim alanında işlenen suçların düzenlenmesinde, bu suçların hukuki konularına ve söz konusu hukuki konular arasında yapılan tercihe göre sistematik olarak düzenlenmesi şeklindeki Alman ve İtalyan Ceza Kanunlarına hakim olan yaklaşımdan, 765 Sayılı TCK’de olduğu gibi ayrıldığı görülmektedir. Bu açıdan tercih edilen sistem, yürürlükteki Fransız Ceza Kanununun 323 vd maddelerinde olduğu gibi bu suçların bir arada düzenlenmesi şeklindedir. Ayrıca bilişim alanında suçların “*Topluma Karşı Suçlar*” arasında düzenlenmesi nedeniyle de TCK’nin, bilişim alanında suçlar bakımından sistemiği hem Alman ve İtalyan ceza kanunlarında yer alan sistematikten hem de maddelerin esin kaynağını oluşturan Fransız Ceza Kanunundaki sistematikten farklılık göstermektedir¹⁰¹.

Bilişim alanında suçlar hukuki konuları bakımından incelendiğinde, TCK’deki yaklaşım, 765 Sayılı TCK’deki düzenleme ile aynı yönde olup bu suçlar bakımından suçun hukuki konusunun esas alınmadığı görülmektedir. Nitekim aşağıda ayrıntılı olarak inceleneceği üzere, karşılaştırmalı hukukta ve doktrinde verinin ele geçirilmesi ya da TCK’de düzenlenen yetkisiz erişim suçunda genel olarak malvarlığı ya da sırrın korunması amaçlanmaktadır. Bilişim sistemine ve

edilmiştir. Bkz Bkz., Convention on Cybercrime, Explanatory Report <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>, parag. 35.

Aksi görüş için bkz., **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 615.

¹⁰¹ Fransız Ceza Kanununda bilişim alanında işlenen suçlar genel olarak “*malvarlığına karşı işlenen suçlar*” arasında “*malvarlığına karşı işlenen diğer suçlar*” başlığı altında düzenlenmiştir. Kanun metni için bkz., <http://www.legifrance.gouv.fr/WAspad/ListeCodes> , İngilizce çevirisi için bkz., http://www.legifrance.gouv.fr/html/codes/traduits/code_penal_soman.htm

verilere müdahale ise malvarlığına karşı suçlar kapsamında düzenlenmiş olup genel olarak kişiye ait mameleki bir değerin korunması esas alınmıştır. Bilgisayar aracılığı ile dolandırıcılık ya da bilgisayar aracılığıyla hukuka aykırı yarar sağlamaya ilişkin düzenlemelerde de mameleki değerin korunması amaçlanmaktadır. 765 Sayılı TCK'de düzenlenen fakat TCK'de yer verilmeyen ve bilişim sistemi ya da bilgisayar ile sahtecilik suçu olarak adlandırılan suçta ise, klasik evrakta sahtecilik suçları ile aynı nitelikte bir yararın korunması amaçlanmaktadır¹⁰² Bu hususlar bilişim suçlarının kimi ceza kanunları içerisinde düzenlenmesinde de sistematik bakımından etkisini göstermiştir.

Bu açıdan, Kanundaki ifadesiyle bilişim alanında suçlar, özel kanunlar bir yana bırakılacak olursa, ceza kanunları içerisinde ya Fransız Ceza Kanununda ve ABD'de federe devletler örneğinde olduğu gibi toplu olarak malvarlığına karşı suçlara arasında ya da İtalyan ve Alman Ceza Kanunlarında olduğu gibi suçun hukuki konusunda yapılan tercihe göre kişi hürriyetine karşı suçlar ve malvarlığına karşı suçlar arasında düzenlenmektedir.

Nitekim 765 Sayılı TCK'de bilişim alanında işlenen suçlar da ayrı bir bab altında düzenlenmesine rağmen, aşağıda ayrıntılı olarak değinileceği üzere, doktrinde bu suçların hukuki konusunun, 525c maddesi bir yana bırakılacak olursa, sırrın korunması ya da malvarlığının korunması olduğu genel olarak ifade edilmiştir. Bu açıdan bilişim alanında işlenen suçlarında karşılaştırmalı hukukta asıl olarak kişiye

¹⁰² Bu açıdan, bilişim alanında işlenen suçlara ilişkin yürürlükteki maddelere çeşitli değişiklikler yapılmış olsa da TBMM'ye sunulan Türk Ceza Kanunu Tasarısının genel gerekçesinde yer alan “Üç ayrı kısım içinde yer alan bölümlerin maddelerinde, korunmak istenen hukuki yarar göz önünde bulundurulmak suretiyle sıralama yapılmış ve böylece aynı hak ve yararı ihlal eden suçlar aynı bölüm içerisinde toplanmıştır.” ifadesine, bilişim alanında işlenen suçlar bakımından katılmak mümkün değildir. Tasarının gerekçesi için bkz., Niyazi **GÜNEY** - Kenan **ÖZDEMİR** - Yusuf S. **BALO**, Yeni Türk Ceza Kanunu, 1. B., 2004, s. 1403.

ait deęerlerin esas alınarak dzenlendięi ve de doktrinde de genel olarak halihazırdaki suların kiřiye ait deęerleri koruduęunun kabul edildięi sonucuna varmak mmkndr.

TCK'de ise, bu suların hukuki konusu bakımından ileri srlen grřler maddelerin dzenlenmesine yansıtılmamıř ve biliřim alanında iřlenen sular yukarıda belirtildięi zere, toplu olarak topluma karřı sular arasında dzenlenmiřtir. Dzenleme yeri aısından bakıldıęında, TCK bakımından biliřim alanında iřlenen sularda korunan hukuki varlık ya da menfaatin ya da dięer bir deyiřle hukuki konunun hamilin karřılařtırmalı hukukta grlenin ve doktrinde belirtilenin aksine topluma ait olduęu sonucuna varıldıęını ilk bakıřta sylemek mmkndr. Bu durum 765 Sayılı TCK dneminde biliřim alanında suların dzenlemesinde, suların hukuki konusu merkezinde ortaya ıkan sistematike iliřkin tartıřmaya ikinci bir boyut kazandırmıřtır. Bu aıdan hukuki konu merkezinde ortaya ıkan sorun ve tartıřmaya eklenen dięer boyut, TCK'de biliřim alanında iřlenen suların dzenlenmesinden yola ıkılarak, biliřim alanında iřlenen sularda sula korunan hukuki varlık veya menfaatin hamilinin genel olarak toplum mu olduęudur. Bu sorunun pratikte yansıması ise zellikle, biliřim alanında iřlenen sularda bu suların iřlenmesinde TCK'de bir hukuka uygunluk nedeni olarak dzenlenen ilgilinin rızasına iliřkin hkmlerin uygulanabilip uygulanamayacaęı ve mmknse rızayı kimin gsterebileceęi řeklinde karřımıza ıkmaktadır¹⁰³.

Burada ncelikli olarak biliřim alanında suların topluma karřı sular arasında dzenlenebilecek řekilde topluma ait bir yararın korunmasına ynelik olup

¹⁰³ "... bir hukuksal deęer ihlaline rıza gsterilip gsterilemeyeceęi ve bunu kimin yapabileceęi, kimin bir řeyi kendi hakkına saldırıya karřı gelerek savunabileceęi, bu hukuksal deęerin hangi nitelikte olduęu ile ilgilidir." NVER, **Hukuksal Deęer**, s. 550-551.

olmadığının tartışılması gerekir. Bir suçun topluma karşı bir suç olarak nitelendirilmesinde ölçüt bulma gereği burada kendini hissettirmektedir. Bu konuda geçerli olan ölçüt ise *Toroslu'nun* belirttiği üzere kısaca fiilin topluma zarar verebilecek nitelikte olup olmadığıdır¹⁰⁴.

Değirmenci, TCK'de bilişim alanında suçların topluma karşı suçlar arasında düzenlenmesi ile ilgili olarak şu görüşü dile getirmiştir: “Ayrıca bilişim sistemlerine karşı veya bilişim sistemleri aracılığıyla işlenen suçların kişilerin hak ve menfaatlerini ihlal etmesi olasılığı mevcuttur. Ancak bu olasılıktan öte düşünülmesi gereken, bu suçların aracı edilmesi suretiyle toplumun hak ve menfaatlerinin ihlal edilmesi, bir başka açıdan toplum hayatının felç edilmesi ihtimalidir. Kullandığı bilişim ağıları vasıtasıyla kişisel bir bilgisayara sızan bilgisayar suç failinin eyleminin önemi, yine bu ağı kullanmak suretiyle trafik sinyalizasyon sistemi veya havaalanı kontrol bilgisayarlarını işlev dışı bırakan failin eylemi yanında göz ardı edilebilecek düzeydedir. Bilişim suçları vasıtasıyla ihlal edilen hak ve menfaatlerden topluma ait olanların daha önemli olması sebebiyle ‘Bilişim alanında Suçlar’ın düzenleme yerinin uygun olduğu kanaatindeyiz. Ancak unutulmamalıdır ki, mevcut düzenleme ile bireylerin hak ve menfaatleri de koruma altına alınmaktadır¹⁰⁵. ”

Bilişim alanında işlenen suçlar ya da bilişim suçları başlıkları altında düzenlenen ve incelenen suçların toplumsal bir değeri esas alarak bu kapsamda

¹⁰⁴ **TOROSLU**, *Cürümlerin Tasnifi*, s. 344.

¹⁰⁵ Olgun **DEĞİRMENCİ**, 2004 *Türk Ceza Kanununun Bilişim Suçları Bakımından Değerlendirilmesi*, Türkiye Barolar Birliği Dergisi, S. 58, 2005, s. 198-199

topluma karşı suçlar altında düzenlenmesi herhalde mümkündür¹⁰⁶. Fakat burada sorun TCK’de bilişim alanında işlenen suçlar başlığı altında düzenlenen suçların hukuki konusunun toplumsal bir değere işaret edip etmediğidir. Yazar, bilişim sistemleri bakımından bu suçların toplumsal zararlara da yol açabileceğini vurgulayarak bu suçların boyutları hakkında doğru bir noktaya temas etmekle birlikte, TCK’nin 243 vd. devamı maddelerinde yer alan suçlar esas alındığında, aşağıda açıklanacağı üzere, yazarın bu görüşüne katılmak mümkün değildir.

Burada vurgulanması gereken diğer bir nokta ise, yazarın bilişim suçlarının toplumsal bir tehlike ya da zarar yaratabileceğine ilişkin örneklerin TCK’de yer alan suçlar bakımından gerçeği yansıtmadığıdır. Yazar , bilişim suçlarının önemi açısından trafik ve sinyalizasyonuna verilebilecek zararlardan bahsetmekle birlikte TCK incelendiğinde, bu tür fiillerin “*Topluma Karşı Suçlar*” kısmının “*Genel Tehlike Yaratan Suçlar*” başlıklı birinci bölümünün 179. maddesinde bilişim sistemlerine müdahale yi de kapsayacak şekilde düzenlendiği görülmektedir. “*Trafik Güvenliğini Tehlikeye Sokma*” başlıklı söz konusu maddede kara, deniz, hava trafiğinin tehlikeye sokulması düzenlenmiştir. Maddenin 1. fıkrasında bu suçun teknik işletim sistemine müdahale yoluyla da gerçekleştirilebileceği ifade edilmektedir. Bu açıdan bu fiil teknik işletim sistemi kapsamında olabilecek olan bilişim sistemine müdahale yoluyla da gerçekleştirebilir. Bu kapsamda yazarın bilişim suçları bakımından verdiği örneklerin TCK’de ayrı bir suç olarak değerlendirildiği görülmektedir. Yani TCK’de bilişim alanında işlenen suçların topluma karşı suçlar arasında düzenlenmesinin yerinde olduğuna ilişkin yazarın

¹⁰⁶ Nitekim, İtalyan Ceza Kanununun 630bis maddesinde bilişim ve telematik sistemlerine ve veri ve programlara müdahale genel olarak düzenlenmiş iken Kanunun 420 maddesinde bu suçun özel şekline yer verilmiştir.

gerekçesinde ileri sürdüğü örnek, halihazırda topluma karşı bir suç olarak ayrıca düzenlenmiştir. Bu nedenle yazarın yukarıda belirtilen örneğe dayanarak bilişim alanında işlenen suçların topluma karşı suçlar arasında düzenlenmesinin yerinde olduğu yönündeki görüşüne, gerekçesi esas alındığında katılmak mümkün değildir. Bu açıklamalar, 243 vd devamı maddelerin neden topluma karşı suçlara arasında düzenlendiğine ilişkin soruna çözüm getirmekten uzaktır.

Öncelikli olarak belirtmek gerekirse TCK'nin genel gerekçesinde, bilişim alanında suçlar arasında suç olarak düzenlenen fiillerin topluma zarar verebilecek nitelikte olup olmadığına ilişkin herhangi bir açıklamaya yer verilmemiştir. Madde gerekçeleri incelendiğinde ise, bilişim alanında işlenen suçlar arasında 245. maddede düzenlenen banka ve kredi kartlarının kötüye kullanılması suçunun gerekçesinde, bu maddede düzenlenen fiillerin kişiye ait hukuki yararları korumaya yönelik olduğunu açık bir şekilde dile getirilmektedir.

Söz konusu maddenin gerekçesinde, maddede düzenlenen fiillerle ilgili olarak *“Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmeleri uygun görülmüştür.”* ifadesine yer verilmiştir.

765 Sayılı TCK döneminde işleniş şekline göre farklı maddeler kapsamında değerlendirilen ve 525/b. 2. fıkrasının eklenmesinden sonra uygulamada çeşitli içtihat farklılıklarına yol açması nedeniyle ortaya çıkan sorunun çözümlenmesi amacıyla bu maddenin konulmuş olduğundan gerekçede bahsedilmesi, bu maddenin hukuki konusunun kişiye ait bir yarar olduğunu onaylar niteliktedir.

244. maddenin son fıkrasında yer alan 244. maddede belirtilen fiillerin işlenmesi suretiyle yarar sağlamaya ilişkin düzenlemenin gerekçesinde de benzer bir vurgu farklı bir şekilde yapılmıştır. Söz konusu maddenin gerekçesinde maddede yer alan fiilin başka bir suçu oluşturmadağı takdirde bu maddeye göre cezalandırılacağına ilişkin açıklamada *“Üçüncü fıkra ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.”* ifadesine yer verilmiştir. Burada da vurgunun ağırlıklı olarak malvarlığına ilişkin bir değerin saldırıya uğramasına ve ihlal edilmesine yönelik olduğu görülmektedir.

Ayrıca bu fıkranın gerekçesinden ayrı olarak, aşağıda inceleneceğı üzere, bu fıkra ve benzeri hükümlerin özellikle kıta Avrupası hukuku bakımından, klasik dolandırıcılık fiilinde yer alan kişiye karşı hilenin yapılması ve kişinin hataya düşürülmesi unsurlarının, bilişim sistemine müdahale edilmesi durumunda genel olarak gerçekleşmediğı olgusundan hareketle bu fiilleri de kapsayacak şekilde dolandırıcılık suçunun unsurlarında ortaya çıkan eksiklikleri gidermek amacıyla yapılan bir düzenleme olarak ortaya çıktığı düşünülürse, buradaki düzenlemenin de topluma ait olmaktan çok kişiye ait yararın korunmasına yönelik olduğu söylenebilir.

Aynı şekilde, 244. maddenin birinci ve ikinci fıkralarında düzenlenen fiiller bakımından da bu suçun toplumsal bir yarardan çok kişiye ait bir yararı koruduğunu söylemek mümkündür. Maddenin gerekçesinde her iki fıkra da yer alan düzenleme

ile ilgili olarak sistemlere yöneltilen ızzar fiillerinin özel bir suç haline getirildiđi belirtilmektedir. Bu gerekçede de malvarlığına karşı bir suç olarak kişiye ait yararın korunmasını amaçlayan mala zarar verme suçunun özel şeklinin düzenlendiđi ifade edilmekle yetinilmekte bunun ötesinde herhangi bir toplumsal yarardan bahsedilmemektir.

Madde gerekçeleri topluca değerdendirildiđinde, kanun koyucunun “*bu suçların uygulamada kolaylık sağlamak üzere ayrı bir bölümde düzenlenmesi*” tercihini 5237 sayılı TCK bakımından da devam ettirdiđini ve tercihi Kanunda somutlaştırırken, söz konusu suçların hukuki konuları ya da bu hukuki konuları oluşturan yarar ya da değerdelerin ait olduđu süjeye ilişkin herhangi bir inceleme yapmadıđını söylemekte sakınca yoktur.

Nitekim bu husus, 245. maddede 5377¹⁰⁷ sayılı Kanunla yapılan değışiklikte kendisini daha açık bir şekilde göstermektedir. 5377 sayılı Kanunun özellikle (4) no.lu fıkrası ile getirilen düzenleme, aslında bu maddede düzenlenen fiillerin düzenleme yeri bakımından sorunların var olduđunu göstermekte ve bunların ötesinde bu madde ile korunan yararın kişiye ait bir yarar olduđunu açıkça göstermektedir.

Maddenin 4. fıkrası incelendiđinde bu fıkra ile maddenin ilk şeklinde olmayan şahsi cezasızlık sebeplerinin madde metnine eklendiđi görölmektedir. (4)¹⁰⁸

¹⁰⁷ “Türk Ceza Kanununda Deđişiklik Yapılmasına Dair Kanun” R.G. 08.07.2005 T., 25869 No.

¹⁰⁸ TCK 245/ (4): “...**4**) Birinci fıkrada yer alan suçun; **a**) Haklarında ayrılık kararı verilmemiş eşlerden birinin, **b**) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,**c**) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.”

no.lu fıkrada yer alan şahsi cezasızlık sebepleri malvarlığına karşı suçlarla ilgili olarak TCK'nin 167. maddesinde de düzenlenen şahsi cezasızlık sebepleri ile paralellik arz etmektedir¹⁰⁹. Bu durum söz konusu maddede kişiye ait mameleki bir değer korunduğunun zımni olarak belirtilmesi bakımından önem arz etmektedir..

Yukarıda aktarılan hususlar topluca değerlendirildiğinde, Türk Ceza Hukukunda bilişim alanında suçlar bakımından, özel bir kanunda düzenlenmesi yerine ceza kanunları içerisinde düzenleme tercihinin yapıldığı; bu tercih yapıldıktan sonra ise hem 765 Sayılı TCK hem de TCK bakımından suçların hukuki konusu ve TCK bakımından ise suçların hukuki konusunun hamili bakımından yeterli bir inceleme ve değerlendirilme yapılmaksızın bu suçların topluca düzenlenmesi yoluna gidildiği söylenebilir. Bu açıdan 765 Sayılı TCK'de bilişim alanında işlenen suçların Kanuna “11. Bab” olarak eklenerek yeni bir hukuki konunun ortaya çıktığı izlenimi yaratılmış; TCK'de ise Kanunun sistematigi içerisinde karşılaştırmalı hukukta ve doktrinde kural olarak kişiye karşı suçlar olarak kabul edilen bilişim alanında işlenen suçların topluma karşı suçlar arasında düzenlenmesi sonucu, bu suçların hukuki konusunun hamilinin genel olarak toplum olduğu ön kabulü yaratılmak istenmiştir. Bu yaklaşım ise bu maddelerin uygulanması ve yorumu bakımından bazı sorunları beraberinde getirmiştir.

Bu açıdan bilişim alanında suçların hukuki konu ve yorumunda Kanunun sistematigin esas alınması yerine yukarıda aktarılan gerekçelerle her maddede düzenlenen normun kendisinin esas alınması bilişim alanında işlenen suçların Türk

¹⁰⁹ 5237 S. TCK 167/(1): “*Yağma ve nitelikli yağma hariç, bu Bölümde yer alan suçların; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin,*

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.”

Ceza Hukuku sistemi içerisinde sağlıklı bir yer edinebilmesi ve uygulanabilmesi bakımından önem arz etmektedir.

Kanunun sistematığının esas alınması başta pratik bir sorun olarak nitelendirilen ve bilişim alanında işlenen suçlar bakımından birçok olasılıkta ortaya çıkabilecek olan “*ilgilinin rızası*” şeklindeki hukuka uygunluk nedeninin geçerli olabilmesi bakımından sorun yaratabilecektir. Nitekim, TCK’de düzenlenen bilişim alanında işlenen suçların konusunu oluşturan fiillerin kapsamı ve bunun ötesinde bilişim sistemi ve ağları üzerindeki işlemler dikkate alındığında ilgili kişinin rızası bu faaliyetlerin gerçekleştirilebilmesi açısından bir ön koşul olarak olmaktadır¹¹⁰. Buna rağmen, Kanunun sistematığından hareketle bu suçların topluma karşı işlenen suçlar olduğu ve dolayısıyla toplumsal bir yararın korunmakta olduğu kabul edilirse, bir hukuka uygunluk sebebi olan ilgilinin rızasının bilişim alanında işlenen suçlar bakımında geçerli olduğunun kabul edilmesi mümkün değildir. Bu durumun somut olarak ortaya çıkardığı sorunlardan biri ise sistem açıklarının tespit edilmesi amacıyla ilgili kişinin rızası ile gerçekleştirilen erişimde, kanundaki ifadeyle bilişim sistemine girilmede ilgilinin rızasının geçerli olup olmayacağıdır.

¹¹⁰ Örnek olarak vermek gerekirse İnternet üzerindeki bir web sayfasına erişim, genel olarak web sayfası sahibi kişinin web sayfasının barındırıldığı bilgisayara(hizmet sunucusu) ne şekilde bağlanılabileceğini ve hangi verilere ulaşılabilceğini önceden belirlemesi anlamına gelmektedir ki, burada ilgili kişi ya da kişilerin web sayfasına erişim amacıyla bu web sayfasının barındırıldığı hizmet sunucusuna bağlanması ya da diğer ifade ile erişmesi ilgili kişi ya da kişilerin rızasına göre gerçekleştirilmektedir.

III. VERİNİN ELE GEÇİRİLMESİ VE BİLİŞİM SİSTEMİNE YETKİSİZ ERİŞİM

A. Verinin Ele Geçirilmesi

1. Genel Olarak Verinin Gizliliğinin Korunması

Bilgisayar suçları, gelişimi itibariyle genel olarak iki unsurun korunması merkezinde ortaya çıkmaktadır. Bunlar “*verinin*” korunması ve “*veri işleme faaliyetinin*” korunmasıdır. Bu korumanın temelinde yatan neden ise enformasyon toplumu olarak da adlandırılan sosyo-ekonomik dönüşüm içerisinde, bilgi ve enformasyonun ve bilgi ve enformasyon işleme faaliyetinin artan önemidir. Enformasyon ve bilginin üretimi, iletimi, genel olarak işlenmesi, bilişim, enformasyon toplumu olarak da adlandırılan sosyo-ekonomik dönüşümün ana unsurunu oluşturmaktadır.

Enformasyonun ve bilginin işlenmesi ise bu dönem içerisinde veri ve veri işleme faaliyeti şeklinde gerçekleştirilmeye başlanmıştır. Bu açıdan, genel olarak enformasyonun bilgisayar sistemleri aracılığıyla işlenebilmesine olanak sağlamak amacıyla, bu sistemler içerisinde temsil edilmesi anlamına gelen verinin ve veri işleme faaliyetinde merkezi bir konumda bulunan ve dönemin teknik altyapısını oluşturan bilişim ve özellikle bilgisayar sistemlerinin ve bu sistemlerin işleyişinin çeşitli yönleriyle korunması sorunu gündeme gelmiştir.

Verinin yetkisiz kişilerin eline geçmesinin ve dolayısıyla verinin içeriğini oluşturan ve gizli kalması istenen bilgi ya da enformasyonun yetkisiz kişiler tarafından öğrenilmesinin engellenmesi, diğer bir ifadeyle veriyi elinde bulunduran

kişinin verinin içeriğinin gizli kalmasına ilişkin tasarrufunun¹¹¹ korunması bu korumanın bir yönünü oluşturmaktadır. Verinin bu yönüyle korunması ise, verinin hukuki niteliği esas alınarak iki farklı yaklaşımın ortaya çıkmasına neden olmuştur. Bunlardan birincisi, verinin de hukuken eşya/mal olarak kabul edilerek¹¹², veri üzerindeki zilyedliğin ve dolayısıyla mülkiyetin korunmasıdır İkincisi ise, verinin sır olarak korunmasıdır. Birinci yaklaşımdan hareketle yapılan düzenlemeleri genel olarak “*veri hırsızlığı*” olarak adlandırmak mümkündür. İkinci yaklaşımı esas alan düzenlemeler ise “*verinin ele geçirilmesi*” suçu olarak adlandırılabilir. Her iki yaklaşımın ortak özelliği verinin 3. kişiler tarafından hukuka aykırı olarak elde edilmesidir. Verinin elde edilmesi, verinin içerdiği bilgi ya da enformasyonun elde edilmesi ve genel olarak öğrenilmesi¹¹³ anlamına geldiğinden her iki yaklaşımda da veriyi elinde bulunduran kişinin tasarruf yetkisinin, verinin gizliliğinin korunması sağlanarak gerçekleştirildiğini söylemek mümkündür. Bu açıdan bu şekilde ortaya çıkan düzenlemeleri, teknik olarak verinin gizliliğinin korunmasına yönelik düzenlemeler başlığı altında toplamak da mümkündür.

¹¹¹ Christian **SCHWARZENEGGER**, Computer crimes in Cyberspace: A comparative analysis of criminal law in Germany, Switzerland and Northern Europe, parag. 28, <http://www.rwi.unizh.ch/schwarzenegger/unterlagen/pdf/ComputerCrimeCyberSpace2002.pdf>

¹¹² Stein **SCHOLBERG** & Amanda M. **HUBBARD**, Harmonizing National Legal Approaches on Cybercrime, International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva, 28, June – 1 July 2005, Documnet: CYB/04, 10 June 2005, s. 12, http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (kontrol tarihi 20.03.2006)

¹¹³ The National Information Infrastructure Protection Act Of 1996, Legislative Analysis, Sec. II, http://www.cybercrime.gov/1030_anal.html, Ayrıca bkz, Scott **CHARNEY** – Kent **ALEXANDER**, *Computer Crime*, 45 EMORY L. J. s. 951; Jonathan B. **WOLF**, *War Games Meets The Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money*, 28 AM.J. CRIM L. 95, s. 112.

Önder de 525/a maddesinde geçen ele geçirme teriminin kullanılmış olmasının hatalı olduğunu, bu terimle bilgisayardaki bilginin ele geçirilmesi değil, bu bilgiye ulaşma, bilgisayarın delinmesi ve sisteme girilmesi, bilginin öğrenilmiş olmasının kastedildiğini ifade etmiştir. **ÖNDER**, s. 507

Yukarıda belirtildiği üzere, verinin hukuki niteliğinin ne olduğunun saptanması, verinin elde edilmesine ilişkin düzenlemelerde merkezi bir konumdadır. Burada genel olarak tartışılan sorun ise cismani bir şeyle bağlantısı olmayan bilginin ya da enformasyonun kendisinin hırsızlık suçunun konusunu oluşturup oluşturamayacağıdır. Ya da diğer bir ifadeyle, bilgi ve enformasyonu temsil edici bir işlevi olan verinin ele geçirilmesinin hırsızlık suçunun konusunu oluşturup oluşturamayacağıdır¹¹⁴. Bu maddi varlığı olmayan verinin kendisinin hukuken eşya olarak kabul edilip edilemeyeceği ve özellikle ceza hukuku anlamında hırsızlık suçunun konusunu teşkil eden taşınabilir mal kapsamında değerlendirilip değerlendirilemeyeceği sorununun gündeme getirmektedir.

Bilindiği üzere Türk Hukukunda, maddi varlığı olan, yani cismani şeyler eşya olarak kabul edilmekte ve bunlar aynı hakların konusunu oluşturabilmektedir¹¹⁵. Verinin kendisinin ise maddi bir varlığı bulunmamaktadır. Bunun sonucunda maddi bir varlığı bulunmayan verinin, Türk Hukuku bakımından eşya kapsamında değerlendirilmesi mümkün değildir¹¹⁶. Aynı şekilde verinin Türk Ceza Hukuku anlamında hırsızlık suçunun konusunu oluşturan taşınabilir mal kapsamında kabul edilmesi mümkün değildir. Türk Hukuku bakımından durum böyle iken veri hırsızlığı şeklinde düzenleme yapılan ABD'nin birçok federe devletinde, verinin kendisi hukuken eşya olarak kabul edilmektedir. Nitekim federe devletlerin

¹¹⁴ Ian J. **LLOYD**, Information Technology Law, 3. edition Butterworths, London, Edinburg, Dublin 2000, s.254. Aynı yönde, **SIEBER**, s.88, [http://eurpa.eu.int/ISPO/legal/en/comcrime/SIEBER, -COMCRIME- Study.doc](http://eurpa.eu.int/ISPO/legal/en/comcrime/SIEBER,-COMCRIME-Study.doc). Kit BUDEN & Creole Palmer - Barlow yde & Gilbert, Cybercrime –A new Breed of Criminal, Computer Law & Security Report Vol. 19, no. 3, 2003, s.224.

¹¹⁵ **SİRMEN**, s. 5., Özcan **ÇELEBİCAN**, Roma Eşya Hukuku, 2. B., Ankara, 2005, s. 31.

¹¹⁶ **DÖNMEZER**, Kişilere ve Mala Karşı Cürümler, s.619.

bilgisayar ile ilgili suçların düzenlendiği kanunlarında, verinin eşya olarak kabul edildiği açıkça ifade edilmektedir¹¹⁷. Bunun sonucunda ilgili kanunlarda verinin ele geçirilmesi genel olarak “*veri hırsızlığı*” başlığı altında düzenlenmektedir¹¹⁸. Örnek vermek gerekirse, Georgia “*Bilgisayar Sistemleri Koruma Kanunu*”nun 16-9-92/(7) no.lu maddesinde veri ve bilgisayar programlarının eşya kapsamında olduğu ifade edilmiştir. Aynı Kanunun 16-9-93/ (a) (19) maddesinde de veri ve program da dahil olmak üzere 16-9-92/(7) maddesinde belirtilen malın hırsızlığı suçu

¹¹⁷ Bkz., Anne W. **BRANSCOMB**, *Rogue Computer Programs and Computer Crimes: Tailoring the Punishment to Fit the Crime*, 16 Rutgers Computer & Tech. L. J. (1990), s 32-36; Carl **BENSON** – Andrew V. **JABLON** – Pal J. **KAPLAN** - Mara Elena **ROSENTHAL**, *Computer Crimes*, 34 Am. Crim. L. Rev. (1997), s. 432; **BUDEN**, *Cybercrime*, s.223.

¹¹⁸ Federe devletlerin kanunlarında yer alan suçlar hakkında ayrıca bkz., Sheri A. **DILLON** – Douglas E. **GROENE** – Todd **HAYWARD**, *Computer Crimes*, 35 Am. Crim. L. Rev. 1997-1998, s, 529 vd; **BENSON**, *Computer Crimes*, s. 430 vd; Robert **DITZION** – Elizabeth **GEDDES** – Mary **RHODES**, *Computer Crimes*, 40 Am. Crim. L. Rev. 2003, s .328 vd.

Verinin hukuken eşya olup olmadığı ya da eşya olarak kabul edilip edilmemesi gerektiği Kanada da gündeme gelmiştir. Nitekim “*R. v. Stewart.*” davasında bir otelin çalışanlarının listesinin yer aldığı bilgisayar verisinin hukuka aykırı olarak elde edilmesine ilişkin olayda, bu gibi gizli bilgilerin Kanada Ceza Kanununda düzenlenen hırsızlık ve dolandırıcılığa ilişkin suçlar bakımından eşya/mal kapsamında olduğu Ontario Yüksek Mahkemesinde karara bağlanmıştır. Kanada Yüksek Mahkemesi ise bu şekildeki gizli bilgilerin hırsızlığın ya da dolandırıcılığın konusunu oluşturabilecek bir mal olmadığını bu anlamda hırsızlık ya da dolandırıcılık gibi suçların konusunu oluşturamayacağını ifade etmiştir.

Bilişim suçlarına ilişkin Kanada Ceza Kanununa ek yapılmasına yönelik yasa tasarısında verinin eşya olarak kabul edilmesine ilişkin öneri gündeme gelmiş fakat bu kabul görmemiş ve yasama sürecinde kurulan alt komitenin önerileri doğrultusunda, bilişim suçlarına ilişkin malvarlığına karşı suçlar içerisinde sisteme yetkisiz erişim ve sistemin kullanılması, sisteme ve veriye müdahaleye ilişkin suçlara yer verilmiştir. Bkz., Monique **HÉBERT** - Marilyn **PILON**, *Computer Crime*, [http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/BP/bp87-e.htm#\(25\)txt](http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/BP/bp87-e.htm#(25)txt); Lisa A. **MENNELLY**, *Prosecuting Computer-Related Crime in the United States, Canada, and England: New Laws for Old Offenses*, 8 B. C. Int'l & Comp. L. Rev. 1985, s 554 vd; Martin **WASIK**, *Following in American Footsteps? Following Computer Crime Developments in Great Britain and Canada*, 14 N. Ky. L. Rev. 1997-1998, s .252 vd; Dona **MACODRUM** – Hedieh **NASHERI** – Timothy J. **O’HEARN**, *Spies in Suits: New Crimes of the Information Age from the United States and Canadian Perspectives*, Information & Communications Technology Law, Vol. 10, No. 2, 2001, s. 141 vd.

“*R. v. Stewart*” kararının İngilizce metni için bkz., <http://www.jurisdiction.com/rvstewar.htm>

düzenlenmiştir¹¹⁹. Iowa eyaletinde de verinin eşya kapsamında olduğu açıkça ifade edilmiş¹²⁰ ve aynı kanunun “bilgisayar hırsızlığı” başlıklı 9. ve devamı maddelerinde veri hırsızlığına ilişkin düzenlemelere yer verilmiştir¹²¹. Özetle veri hırsızlığı şeklinde ortaya çıkan bu düzenlemelerde verinin elde edilmesi, malvarlığına yönelik suçlara ve özellikle hırsızlık suçuna¹²² paralel bir şekilde düzenlenmiştir.

ABD’de bilişim suçları ile ilgili federal düzeydeki Kanunda (18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers) ise, bu yaklaşımdan çok içerik bakımından belirli niteliği sahip verinin ele geçirilmesi suç haline getirilmiştir. İlgili maddeler incelendiğinde söz konusu maddelerde, içeriği gizli kalması gereken verilerin, bunun yanında finans kurumları veya kamu kurumlarına ait verilerin, ülke içi ticarete kullanılan bilgisayarlarda yer alan verilerin ele geçirilmesi gibi kanunda belirtilen niteliği haiz verilerin bilgisayar sistemlerine yetkisiz erişim ya da yetki aşımı sonucunda elde edilmesi düzenlenmiştir. Bu açıdan verinin mal kapsamına dahil edilmediği bu Kanunda, malvarlığına ilişkin bir değer olarak verinin korunmasından çok devlet sırrı, ticari sırlar gibi maddede sayılan

¹¹⁹ Kanunun 16-9-93/ a (1). maddesinde veri hırsızlığı da dahil olan bilgisayar hırsızlığı, sahibinin zilyetliğinden yoksun bırakma amacıyla olsun ya da olmasın başkasının malını alma şeklinde düzenlenmiştir. Bkz., Georgia Advance Legislative Service, House Bill No. 822, 1991 Ga. ALS 822 1991 Ga. HB 822, <http://nsi.org/Library/Compsec/computerlaw/Georgia.txt>

¹²⁰ Code Of Iowa 1989 Title XXXV Criminal Law Chapter 716a Computer Crime, Iowa Code @ 716A.1 (1989), 716A.1/7. f. <http://nsi.org/Library/Compsec/computerlaw/Iowa.txt>

¹²¹ Iowa Code @ 716A.9 (1989) vd.

Her iki eyaletin bilgisayar ile ilgili olarak hırsızlık suçlarına ilişkin düzenlemelerde bilgisayarın donanım unsurları da suçun konusunu oluşturabilmektedir.

¹²² *Dönmezer* Amerika’da hırsızlığa ilişkin geleneksel mülkiyet hükümlerinin, bilgisayardan bilgi alınması hallerinde de uygulandığını ifade etmiştir. **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 621.

hallerde sırrın korunmasının esas alındığı söylenebilir. Bu haliyle federe düzeydeki düzenlemeler ile federal düzeydeki düzenleme arasında bir yapısal farklılığın olduğunu söylemek mümkündür¹²³.

Maddi varlığı olmayan şeylerin, ve dolayısıyla verinin, eşya olarak kabul edilmediği ve hırsızlık suçu bakımından taşınabilir mal kapsamında değerlendirilmediği hukuk düzenlerinde genel olarak “*veri hırsızlığı*” şeklinde düzenlemelere yer verilmemiştir¹²⁴. Verinin elde edilmesi, verinin içerdiği bilgi ya da enformasyon esas alınarak sırrın korunması kapsamında değerlendirilmiş ve sırrın öğrenilmesi paralelinde düzenlemeler yapılmıştır¹²⁵. Verinin ele geçirilmesi olarak da adlandırılabilen, sırrın ya da daha açık bir ifade ile sır olarak kabul edilen verilerin

¹²³ Bunun yanında bilgisayar verisinin malvarlığı kapsamında değerlendirilememesinin, verinin ele geçirilmesinin de dahil olduğu, bilgisayarlarla ilgili suçların yer aldığı bu Kanunun düzenlenmesine ilişkin temel gerekçe olduğu hakkında bkz., Joseph M. **OLIVENBAUM**, <CTRL> <ALT>: *Rethinking Federal Computer Crime Legislation*, 27 Seton Hall L. Rev., 1996-1997, s. 637 vd. Yazar federal düzeydeki bilişim suçlarına ilişkin özel düzenlemeleri eleştirerek bunun yerine eşya tanımının veriyi de kapsayacak şekilde genişletilmesi ve malvarlığının korunmasına ilişkin suçların unsurlarının söz konusu fiilleri kapsayacak şekilde düzenlenmesini önermektedir.

Adı geçen kanunda yer alan suçlar hakkında bkz., ; The Computer Crime and Intellectual Property Section United States Department of Justice, The National Information Infrastructure Protection Act of 1996: Legislative Analysis, http://www.usdoj.gov/criminal/cybercrime/1030_anal.html; **DILLON**, **Computer Crimes** s. 507 vd; **BENSON**, **Computer Crimes**, s. 413 vd; **DITZION**, **Computer Crimes**, s. 290 vd; Frank P **ANDREANO**, *The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem*, 27 Am. J. Crim L. 1999-2000, s. 85 vd.

¹²⁴ *Dönmezer*’ın 525/b 2. fıkra düzenlenmiş suç için “...hırsızlık, dolandırıcılık gibi suçların oluşması için alınacak ve elde edilecek şeylerin cisminin olması, yerine göre bir mal olması, bilgisayar bakımından ise durumun farklı bulunmasıdır...” yönündeki ifadesi bu kapsamda aslında verinin gizliliğinin korunması bakımından geçerli bir gerekçe olarak kabul edilmelidir. **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 617-618.

¹²⁵ Nitekim enformasyonun ya da verinin maddi varlığının bulunması karşısında mal kapsamında değerlendirilmediği İngiliz hukukunda da verinin gizliliğinin korunmasının sırrın korunması kapsamında düzenlenmesi alternatif bir model olarak tartışılmaktadır. Bkz, **LLOYD**, s. 266 vd.

İsviçre Ceza Kanununda ise verinin ele geçirilmesi malvarlığına karşı işlenen suçlar bölümünde düzenlenmekle birlikte burada verinin kendisine ya da başkasına yarar sağlamak amacıyla ele geçirilmesi suç olarak düzenlenmiştir. Art 143. <http://www.admin.ch/ch/i/rs/311.0.it.pdf>

korunmasına ilişkin düzenlemelerde, ağırlıklı olarak verinin üçüncü kişilerin eline geçmemesi esasından hareket edilmiş ve verinin gizliliğinin korunması amaçlanmıştır. Sır olarak saklanan verinin içeriğinin öğrenilmesi¹²⁶ ya da içeriği hakkında bilgi edinilmesi bu yöndeki düzenlemelerin içeriğini oluşturmaktadır¹²⁷. Bu şekliyle de geleneksel olarak ceza kanunlarında sır niteliğindeki bilgileri içeren belgelerin ele geçirilmesi ve sırrın öğrenilmesine ilişkin düzenlemelerle paralellik arz etmektedir. Burada sözü edilen sır ise verinin içerdiği bilgi ya da enformasyonun içeriğinin maddi olarak sır niteliğinde olmasından çok, üçüncü kişiler tarafından öğrenilmesinin engellenmesi amacıyla gizli tutulmasının sağlanması amacını taşıyan şekli anlamda sırrı ifade etmektedir¹²⁸.

Alman Ceza Kanunun 202a maddesinde düzenlenen veri casusluğu suçunu, bu kategoride değerlendirmek mümkündür. Nitekim bilgisayar sistemine yetkisiz erişime ilişkin açık bir düzenlemeye yer verilmeyen¹²⁹ Alman Ceza Kanununda, verinin ele geçirilmesi ya da Kanundaki ifadesiyle veri casusluğu özel hayatın gizliliğine yönelik suçların düzenlendiği 15. bölümde 202a maddesinde yer almıştır.

¹²⁶ Önder, 525/a maddesinde geçen ele geçirme teriminin kullanılmış olmasının hatalı olduğunu, bilgisayardaki bilginin ele geçirilmesi değil, bu bilgiye ulaşma, bilgisayarın delinmesi ve sisteme girilmesi, bilginin öğrenilmiş olmasının anlaşılması gerektiğini ifade etmiştir. **ÖNDER**, s. 507.

¹²⁷ “Özellikle İtalya, Fransa ve Almanya’da hakim olan görüşe göre bilişim şeyleri kuramsal açıdan bile ne cismi şeylerle ne de enerjiyle özdeşleştirilebilirler... Bu kuramsal imkansızlık, sözü edilen bilişim şeylerinin aşınabilir şeyler gibi çalınmaya, elden alınmaya, yani bir mülkiyetten başka birine geçirilmeye uygun olmamasından ileri gelir; bu sebepten, mülkiyeti korumaya yönelik ceza normları bunlara uygulanamaz. Bir bilgiye sahip olma o bilgiyi bilme ile gerçekleşir: şu halde sahiplenme sırf bilme ile gerçekleşir...Bu sebepten bilişim suçlarını engellemeye yönelik kanunu olan ülkelerde bilişim şeyleri hırsızlığını öngören ve cezalandıran bir norm yoktur.” Carlo Sarzana di S. IPPOLITO, *Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalyadaki Durum*, (Çev. Vesile Sonay Daragenli) İHFM, C: LV, S. 3, 1997, s. 395.

¹²⁸ **SCHWARZENEGGER**, parag. 28.

¹²⁹ Alman Ceza Kanununun verinin ele geçirilmesinin düzenleyen 202a maddesinin bu gibi fiillere de uygulanabileceğine ilişkin tartışmalar hakkında bkz., **SCHWARZENEGGER**, parag. 33.

Adı geçen maddeye göre, suçun konusunu üçüncü kişilerin yetkisiz erişiminden özellikle korunan ya da diğer bir ifade ile gizli kalması istenen veriler oluşturmaktadır¹³⁰. Maddenin 2. fıkrasında veri, sadece doğrudan algılanamayan/görülemez biçimde elektronik ya da manyetik olarak saklanan veya iletilen veri anlamındadır. Bu maddede verinin ele geçirilmesi bakımından bilgisayar sistemine erişim koşulu aranmamıştır. Bunun sonucu olarak verinin bilgisayar sistemi içerisinde veya bir veri saklama aygıtı içerisinde olması arasında fark yoktur.

Bilgisayar sistemine yetkisiz erişiminin bir ön koşul olarak aranmadığı Yunanistan Ceza Kanununun 370C §2. maddesinde benzer bir düzenlemeye yer verilmiştir. Adı geçen maddede sadece yetkisiz erişim suretiyle bilgisayar sistemindeki verinin ele geçirilmesi esas alınmamış, bilgisayar sisteminde bulunan veri de dahil olmak üzere, veri saklama aracında kayıtlı olan ya da telekomünikasyon sistemleri aracılığıyla iletilen ve ilgili kişi tarafından özellikle erişilmesine ilişkin yasakların ya da güvenlik önlemlerinin ihlali suretiyle verinin ele geçirilmesi suç haline getirilmiştir¹³¹. Adı geçen Kanunda da verinin elde edilmesi ya da maddede geçen ifadesiyle veriye erişim, Alman Ceza Kanununa benzer şekilde, sırrın ve özel hayatın gizliliğinin ihlaline ilişkin suçların düzenlendiği 370-371. maddeleri arasında yer almaktadır. Düzenleniş yeri itibarıyla Yunanistan Ceza

¹³⁰ Bu madde ile verinin içeriğinin sır olması aranmamakta ve verinin veriyi elinde bulunduran kişi tarafından saklı tutulması esas alınmakta ve şekli anlamda sır korunmaktadır. Bkz., **SCHWARZENEGGER**, parag. 28

¹³¹ Bkz., <http://www.cybercrimelaw.net/countries/greece.html>, Adı geçen maddede verinin içeriğinin uluslararası ilişkiler veya Devletin güvenliği ile ilgili olması halinde aynı Kanunun 148. maddesinin uygulanacağı hükme bağlanmıştır

Kanununda da verinin gizliliğinin korunmasının, sırrın korunması kapsamında değerlendirildiği sonucuna varmak mümkündür.

Portekiz’de ise, genel olarak “*enformasyon sistemine*” ya da “*enformasyon ağına*” erişim suretiyle ve güvenlik önlemlerinin ihlali suretiyle veriye ulaşılması veya yine sisteme erişim suretiyle ticari sır içeren ya da ilgili yasalar gereği gizli kalması gereken veriler hakkında bilgi edinilmiş olması sisteme yetkisiz erişimin ağırlatıcı nedenleri olarak düzenlenmiştir¹³².

Bu söylenenler doğrultusunda, genel olarak veriyi elinde bulunduran kişinin veri üzerindeki tasarruf yetkisini korumaya yönelik olarak her iki şekilde ortaya çıkan düzenlemelerin özelliği, bilgisayar sisteminden çok verinin korunmasını esas almasıdır. Bu tür düzenlemelerde tasarruf yetkisi, verinin doğrudan korunması suretiyle korunmaktadır. Bu koruma ise yukarıda incelendiği üzere, kimi düzenlemelerde verinin eşya olarak kabul edilmesi suretiyle veri hırsızlığı şeklinde olmakta¹³³ kimi düzenlemelerde ise veri, sır kapsamında ele alınmakta ve bu kapsamda korunmaktadır.

¹³² Portekiz’de bilişim suçlarına ilişkin kanunun 7. maddesinin birinci fıkrasında enformasyon sistemine ya da ağı herhangi bir şekilde erişilmesi suretiyle fayda sağlanması veya kullanılması düzenlenmiş, 2. fıkrasında ise ilgili kişinin (1 . fıkrada belirtilen fiili gerçekleştiren kişinin) güvenlik önlemlerini ihlal suretiyle veri elde etmesi düzenlenmiştir. 3. fıkrasında ise verinin elde edilmesi suretiyle ticari sırrın ya da yasa gereği gizli kalması gereken verinin öğrenilmesi ağırlatıcı neden olarak düzenlenmiştir. Adı Geçen Kanunun ilgili maddeleri için bkz., <http://www.cybercrimelaw.net/countries/portugal.html>.

¹³³ Bu tür düzenlemelerde verinin elde edilmesi sonucunda ortaya çıkan zararın parasal olarak miktarı, öngörülen cezada farklılıklara yol açabilmektedir Örnek olarak bkz., Iowa Code @ 716A.9 (1989),

<http://nsi.org/Library/Compsec/computerlaw/Iowa.txt>.

2. 765 Sayılı Türk Ceza Kanununda Verinin Ele Geçirilmesi

Bilişim sistemlerinin ve özellikle bilgisayar sistemlerinin ve veri işleme faaliyetinin yaygınlaşması, bu faaliyetlerin gizliliğinin korunmasına ilişkin düzenlemelerin yapılması sonucunu doğurmuştur. Türk Ceza Hukukunda da bu eğilim kendisini göstermiş ve 1991 yılında 765 Sayılı Türk Ceza Kanununda yapılan değişiklikler sonucunda, verinin gizliliğinin korunmasına yönelik olan, 525/a maddesi 765 Sayılı TCK'ye eklenmiştir. Kanunun 525/a maddesine göre; *“Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye....cezası verilir... Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkra yazılı ceza verilir.”*

Bu suç genel olarak, *“Ele Geçirme¹³⁴”, “Bilgisayar İçeriğinden Yararlanma¹³⁵”, “Verilerin Ele Geçirilmesi¹³⁶”, “Sır Aleyhinde İşlenen Suç (525a/1.)¹³⁷”* başlıkları altına incelenmiştir. Ersoy ise 1. fıkra da yer alan düzenlemeyi *“Ele Geçirme Suçu”*, ikinci fıkra da yer alan düzenlemeyi *“Tasarruf Suçu”* başlıkları altında incelemiştir. Yazıcıoğlu da 1. fıkra da yer alan düzenlemeyi, *“Sistemde Yer Alan Bilgiyi Öğrenme, Sır Aleyhinde Suç”*, ikinci fıkra da yer alan

¹³⁴ Faruk EREM, *Bilgisayar Suçları ve Türk Ceza Kanunu*, Yargıtay Dergisi, C. 17, S. 4, Ekim 1991, s. 442

¹³⁵ DÖNMEZER, *Kişilere ve Mala Karşı Cürümler*, s. 620

¹³⁶ DÜLGER, s. 114.

¹³⁷ ÖNDER, s.506.

düzenlemeyi de “*Başkasına Zarar Vermek İçin Sistemin İçeriğini Kullanma, Nakletme veya Çoğaltma Suçu*” başlıkları altında incelemiştir¹³⁸.

Dönmezer 1. fıkra da yer alan düzenleme ile korunan hukuki yararın başta bilgisayar sisteminin güvenliğinin ve bilgisayarın müdahale edilmezliğinin oluşturduğunu ve bu suçun özel hayata bir müdahale teşkil ettiğinin de söylenebileceğini belirtmiştir. Yazar, 2. fıkra da yer alan düzenleme ile korunan hukuki yararın ise maddede yer alan icra hareketlerinin türüne göre değişiklik arz ettiğini, kullanmak ve nakletmek şeklindeki icra hareketleri bakımından hukuken korunan yararın bilgisayara özgü dokunulmazlık olduğunu, çoğaltmak bakımından ise telif haklarına yönelik bir tecavüzün söz konusu olduğunu ve maddede belirlenen varlıkların içerdiği fikri hakların güvence altına alındığını belirtmiştir¹³⁹.

Yazıcıoğlu’da, *Dönmezer* ile aynı yönde, ikili ayırıma giderek 525a/1. fıkra da yer alan düzenleme ile birden fazla hukuki yararın korunduğunu ve öncelikle bilgisayar sisteminin içeriğinin, sistemde yer alan bilginin dışarıdan gelecek müdahalelere karşı korunduğunu; bunun yanında sistemde yer alan bilginin ancak sisteme yapılacak müdahalelerle elde edilebileceğinden, bu hükümle aynı zamanda sistemin kendisinin ve güvenliğinin de korunduğunu ve her iki yönün kaynağını özel hayatın gizliliğini düzenleyen Anayasanın 20. maddesinden aldığını belirtmiştir. Yazara göre; ilgili bakımından biçimsel olarak sistemdeki bilginin gizli kalması konusundaki herhangi bir yararının bulunması yeterlidir¹⁴⁰. 525a/2. fıkra da yer alan düzenleme ile ilgili olarak da yazar, burada korunan hukuki yararın fıkra da yer alan

¹³⁸ **YAZICIOĞLU, Bilgisayar Suçları**, s. 233 vd.

¹³⁹ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 620 – 622.

¹⁴⁰ **YAZICIOĞLU, Bilgisayar Suçları** s. 234, **YENİDÜNYA - DEĞİRMENCİ**, s. 53-54.

icra hareketlerine göre deðiřtiđini fakat öncelikli olarak özel hayatın gizliliđinin korunduđunu, bunun yanında veri ve yazılımların ortaya çıkardıđı mülkiyet hakkına ve bununla bađlantılı olarak fikri haklara iliřkin bir koruma sađlandıđını belirtmiřtir¹⁴¹.

Önder, 525a/1. fıkrada düzenlenen suçun, bilgisayarın vasıta olarak kullanılması suretiyle sır aleyhinde işlenmiş bir suç olduđunu, bilgisayardaki sırrın veya bu bilgi ile olan alakanın sır olarak saklanması veya sır olarak kalmasının şart olmadığını, bir bilgisayar sistemi içerisinde bulunmasının ve ilgilinin bu bilginin biçimsel bakımdan gizli kalması konusundaki herhangi bir yararının yeterli olduđunu ifade etmiştir.¹⁴²

Ersoy ise bu suçla korunan hukuki değerin saptanmasında suçun TCK’de düzenlendiđi yerin belirleyici olmamakla birlikte bir anlamı bulunduđunu ve bundan yola çıkarak, TCK’nin 11. babında yer alan suçlarda korunmak istenen menfaatin, kiřinin malvarlıđı olduđunu ifade etmektedir. Yazara göre 525a maddesinin her iki fıkrasında yer alan düzenleme ile malvarlıđı korunmaktadır¹⁴³.

Dülger ise yukarıda aktarılan açıklamaları eleřtirerek, 525a 1. fıkrasında yer alan düzenleme ile korunan hukuki değerin karma bir yapı gösterdiđini ve failin suçu işlediđi anda güttüđü amacın bu suçla korunan hukuki değeri oluřturduđunu, bu nedenle aynı anda birden çok hukuksal değerin varlıđının dahi söz konusu olduđunu ve bunun her somut olayda farklılık gösterebileceđini belirtmiřtir¹⁴⁴. Yazar 2. fıkrada

¹⁴¹ **YAZICIOđLU, Bilgisayar Suçları** s. 247. Aynı yönde **YENİDÜNYA - DEđİRMENCİ**, s. 92 – 93.

¹⁴² **ÖNDER**, 507.

¹⁴³ **ERSOY**, s. 166.

¹⁴⁴ **DÜLGER**, s. 118

yer alan düzenleme ile de kişilik hakkı ya da malvarlığına ilişkin hakların korunduğunu belirtmiştir¹⁴⁵.

Suçun maddi unsuru, 1. fıkarda yer alan düzenleme bakımından bilgisayar sistemi içerisindeki verinin, programın ve diğer herhangi bir unsurun ele geçirilmesi şeklindedir. 2. fıkarda yer alan düzenleme bakımından fıkarda belirtilen seçimlik hareketlerden birinin gerçekleştirilmesi suçun tamamlanması için yeterlidir. Maddede yer alan hareketler ise bilgisayar sistemi içerisindeki verinin, programın ya da diğer herhangi bir unsurun kullanılması, nakledilmesi veya çoğaltılmasıdır.

Bu maddede yer alan düzenlemeyle ilgili olarak TCK'nin yürürlükte olduğu dönemde tartışılan husus, "bilgileri işleme tabi tutmuş sistem"den ne anlaşılması gerektiği, özellikle verinin, programın ya da diğer herhangi bir unsurun ele geçirilmesi ya da ikinci fıkarda yer alan fiillerden birinin gerçekleştirilmesi bakımından, bunların bilgisayar sistemi dışında ve bunlardan bağımsız olarak cd, disket vb. saklama aygıtlarında bulunması durumunda, 1. ve 2. fıkarda düzenlenen suçların gerçekleşip gerçekleşmeyeceği noktasında toplanmıştır.

Yazıcıoğlu, bilgileri otomatik işleme tabi tutmuş sistem kavramının bilgisayar ile sınırlı tutulması halinde, bilgisayardan bağımsız veri saklama aygıtlarında bulunan verinin ele geçirilmesinde, 525/a maddesinin uygulanamayacağını belirtmektedir. Yazar devamında, maddede yer alan bilgileri otomatik işleme tabi tutmuş sistemden, *"fizik ve soyut yanı bulunan birçok unsurun bir araya gelmesinden oluşmuş bir bütün"*nün anlaşılması gerektiğini, bu durumda veri saklama aygıtlarının da, sistemde kullanılan ve sistemin bir unsurunu teşkil eden herhangi bir veri taşımaları halinde, sistemin bir parçası sayılacağını ve verinin

¹⁴⁵

DÜLGER, s. 138

bunlar marifetiyle elde edilmesi halinde de 525a maddesinin uygulanabileceğini ifade etmiştir¹⁴⁶.

Buna karşın suçun unsurları dikkate alındığında, ele geçirilen veri, program ya da diğer unsurların, içerisinde bulunduğu bilişim sisteminden alınmasının şart olduğu; disket ya da “cd”de yer alan veri ya da programın hukuka aykırı olarak ele geçirilmesinde bu maddenin uygulanmasının mümkün olmadığı da ifade edilmiştir¹⁴⁷.

765 Sayılı TCK’nin 525a 1. fıkrasında düzenlenen suçun genel kast ile işlenebileceği¹⁴⁸ 2. fıkarda düzenlene suçun ise özel kast ile işlenebileceği belirtilmiştir¹⁴⁹. Başkasına zarar verme kastı 2. fıkarda düzenlenen suçta özel kastı oluşturmaktadır. *Yazıcıoğlu*, bazı hallerde failin kendisine çıkar sağlamasının da fıkradaki ifadeyle “*başkasına zarar vermek üzere*” şeklinde özel kastı oluşturabileceğini, fail tarafından kendisine veya başkasına sağlanan haksız menfaatin başkasının zararını da içerdiğini ifade etmiştir¹⁵⁰.

5237 Sayılı TCK ile Kanundaki ifadesiyle “*Bilişim Alanında Suçlar*” yeniden düzenlenmiştir. TCK’de, 765 Sayılı TCK’nin 525a maddesinde yer alan “*verinin ele geçirilmesi*” suçuna yer verilmemiştir. Verinin ele geçirilmesine ilişkin bir suç yerine, TCK’nin da “*sisteme hukuka aykırı olarak girme*” ya da genel ifade ile

¹⁴⁶ **YAZICIOĞLU, Bilgisayar Suçları**, s.237. Aynı yönde **DÜLGER**, , s. 124; Hatice **AKINCI**– A. Emre **ALI** – Cüneyd **ER**, *Türk Ceza Kanunu ve Bilişim Suçları*, İnternet ve Hukuk, Der. Yeşim Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 221.

¹⁴⁷ **YENİDÜNYA - DEĞİRMENCİ** s. 65.

¹⁴⁸ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 621, **YAZICIOĞLU, Bilgisayar Suçları**, s. 244, **DÜLGER**, s. 130

¹⁴⁹ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler** s. 622, **ERSOY**, s. 176, **YAZICIOĞLU, Bilgisayar Suçları** s. 251.

¹⁵⁰ **YAZICIOĞLU, Bilgisayar Suçları**, s. 252

“bilgişim sistemine yetkisiz erişim” suçuna yer verilmiştir. Aşağıda *“bilgişim sistemine yetkisiz erişim”* suçu ayrıntılı olarak incelenecektir.

B. Bilgişim Sistemine Yetkisiz Erişim

1. Genel Olarak

Bilgişim, enformasyon toplumu gibi adlarla adlandırılan sosyo-ekonomik dönüşüm içerisinde, verinin gizliliğinin korunması yanında enformasyon veya bilginin işlenmesi faaliyetinde merkezi bir konumda yer alan bilgişim sistemlerine yönelik müdahalelerin artması, bu sistemlerin yetkisiz üçüncü kişilerin müdahalelerinden çeşitli yönleriyle korunmasını gündeme getirmiştir.

Sorun, veri ve veri işleme faaliyetinin yetkisiz kişilerin müdahalesinden uzak bir şekilde gerçekleştirilmesi olduğunda, özellikle ağ üzerinden bilgişim sistemleri ile iletişim kurma imkanlarının artması karşısında, sadece verinin ele geçirilmesi ya da veriye zarar verilmesi şeklindeki suçların düzenlenmesi yetmemiş bu faaliyetin ana unsurunu oluşturan bilgişim sistemlerinin yetkisiz müdahalelerden uzak bir kullanımının sağlanmasının da önemi artmıştır.

Bilgişim suçları kapsamında sadece veriye yönelik müdahaleler esas alınması yerine, verinin işlendiği bilgişim sistemlerini de kapsayacak şekilde koruyucu düzenlemelerin yapılması gerekmiştir. Nitekim bu dönem içerisinde sadece içerdiği enformasyon ya da bilgi nedeniyle verinin kendisi önemli olmamakta verinin saklandığı ve de işlendiği bilgişim sistemleri de önem arz etmektedir.

Bu açıdan bilişim sistemlerinde yetkisiz üçüncü kişilerin işlem yapabilme yetkisini elde etme anlamına gelen bilişim sistemlerine yetkisiz erişim, veri ve veri işleme faaliyeti açısından cezalandırılabilir bir fiil olarak nitelendirilmesi gerekmiştir.

Bilişim sistemine erişimin, kural olarak söz konusu bilişim sistemi içerisinde erişim düzeyi doğrultusunda her türlü işlemi yapabilmesi anlamına gelebilmektedir. Bu durumda bilişim sistemlerine erişim fiilinin, bilişim sistemi aracılığıyla her türlü fiilleri kapsamı düşünülebilir. Bilişim sistemine yetkisiz olarak erişen kişi, sayılanlarla sınırlı olmamakla birlikte, bilişim içerisindeki verileri ve bu verilerin içeriğini öğrenebilir, veriler üzerinde her türlü değişikliği yapabilir, verileri kopyalayabilir, başka bir bilişim sistemine gönderebilir, programları çalıştırabilir, silebilir veya değiştirebilir.

Bilişim aracılığıyla gerçekleştirilebilen diğer ihlaller esas alındığında bilişim sistemine erişim, ceza mevzuatlarında yer alan suçların işlenmesinde bir araç olarak gerçekleşebilmektedir. Bu açıdan yetkisiz erişimin ayrı bir suç olarak düzenlenmesi, bu tür hareketlerin gerçekleştirilmesi olanağına sahip olan kişinin somut durumda bunları gerçekleştirip gerçekleştirmediğine veya belirli bir zarar verip vermediğine bakılmaksızın cezalandırılabilmesine olanak sağlamaktadır ve bu haliyle tehlike suçu olarak karşımıza çıkmaktadır.

Yukarıda aktarılan bu hususlar esas alındığında bilişim sistemlerine erişim suçu ile bilişim sistemlerinin kullanılabilmesi açısından çeşitli değerlerin doğrudan veya dolaylı olarak korunduğu sonucuna varmak mümkündür.

2. Türk Ceza Kanununda Bilişim Sistemine Yetkisiz Erişim – Bilişim Sistemine Girme ve Orada Kalmaya Devam Etme

a. Genel Olarak

TCK'nin 243. maddesinin birinci fıkrasında yetkisiz erişim suçu “*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.*” şeklinde düzenlenmiştir¹⁵¹. 243. maddenin 2. fıkrasında, birinci fıkrada tanımlanan fiilin bedeli karşılığı yararlanılabilen sistemler üzerinde gerçekleştirilmesi hali cezada indirim sebebi olarak öngörülürken, aynı maddenin son fıkrasında düzenlenen verinin yok olması ya da değişmesi, ağırlatıcı sebep olarak düzenlenmiştir.

¹⁵¹ “Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı”nın 17. maddesinde ise, “(1) Bir bilişim ağı aracılığıyla; a) Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren veya her hangi bir şekilde sistemde kalmaya devam eden kimseye altı aydan iki yıla kadar hapis cezası veya ikiyüz günden sekizyüz güne kadar adlî para cezası verilir. b) Bir bilişim sistemine hukuka aykırı olarak girerek, veri veya program elde eden kimseye bir yıldan üç yıla kadar hapis ve ikiyüz günden aşağı olmamak üzere adlî para cezası verilir. c) (b) bendinde belirtildiği şekilde elde edilen veri ve programların başkalarına gönderilmesi hâlinde, verilecek ceza yarı oranında artırılır. d) (a) bendinde tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir. (2) Bu maddede yer alan suçların soruşturma ve kovuşturulması mağdurun şikâyetine bağlıdır.” hükmüne yer verilerek hem yetkisiz erişim suçunun hem de yetkisiz erişim suretiyle verinin ele geçirilmesi suçunun düzenlenmek istendiği görülmektedir. Söz konusu Tasarının gerekçesinde 17. maddede düzenlenmek istenen suçun oluşabilmesi için fiilin, “bilişim ağı aracılığı ile” işlenmesi gerekli olduğu aksi halde Türk Ceza Kanununun “*bilişim sistemine girme*” başlıklı 243 üncü maddesinin uygulanabileceği ifade edilmektedir.

Tasarının bu maddesi incelendiğinde öncelikli olarak 765 Sayılı TCK'nin 525a maddesinde düzenlenen verinin ele geçirilmesi suçunun yeniden düzenlenmek istendiği görülmektedir. Bunun yanında söz konusu madde TCK'nin 243. maddesinde düzenlenen suçun yerine geçecek bir suç şeklinde düzenlenmemiş, bunun yerine yetkisiz erişim fiilinin bilişim ağları aracılığıyla gerçekleştirilmesi halinde uygulanacağı belirtilmiştir. Diğer bir farklılık ise Tasarıda düzenlenen yetkisiz erişim ve verinin ele geçirilmesi suçunun TCK'nin 243. maddesinde düzenlenen suçtan farklı olarak şikâyete bir suç olarak düzenlenmesi şeklinde karşımıza çıkmaktadır.

243. maddede “*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden...*” hükmüne yer verilmiş ve suçun maddi unsuru “*girme ve orada kalmaya devam etme*” olarak düzenlenmiştir. Tasarıda yetkisiz erişim suçunun düzenlendiği maddede “*bir bilişim sistemine giren veya orada kalmaya devam eden*” hükmünü içermekte iken. TBMM Genel Kurul görüşmeleri sırasında bu maddeye ilişkin değişiklik önergesinin kabulü sonucunda, madde halen yürürlükteki halini almıştır.

Tasarıdaki hüküm Fransız Ceza Kanunun 323-3¹⁵² ve İtalyan Ceza Kanunun 615 ter maddesi maddi unsur itibarıyla paralellik arz etmekte ve “*sisteme girme*” ve “*sistemde kalmaya devam etme*” seçimlik hareketleri oluşturmaktaydı Madde metninde yapılan değişikliklerle bu iki hareket birleştirilmiş. “*sisteme girme ve kalmaya devam etme*” şeklinde tanımlanmıştır.

Nitekim İtalyan Ceza Kanunun 615-ter maddesinde suçun maddi unsurunu birbirinden bağımsız iki hareket oluşturmakta olup suç seçimlik hareketli bir suç olarak düzenlenmiştir. Maddede öngörülen birinci olasılık “*bilişim*” ya da “*telematik*” sistemine hukuka aykırı olarak girilmesi, ikinci olasılık ise ilgili kişinin (sistemden dışarıda tutma hakkına sahip olan kişinin) açık ya da zımni rızası hilafına sistemde kalma şeklindedir. Birinci durumda failin hukuka aykırı olarak bir sisteme girmesi esas iken ikinci durumda failin sistemde kazara veya yanlışlıkla girmesi sonrasında sistemde kalması ya da sisteme rızai bir şekilde girmesi sonucunda,

¹⁵² Madde metni için bkz, <http://www.legifrance.gouv.fr/WAspad/UnCode?code=CPENALLL.rcv> . Fransız Ceza Kanunundaki ilgili düzenleme hakkında ayrıca bkz., **YAZICIOĞLU, Bilgisayar Suçları**, s.308 vd.

rızanın açık ya da zımnî olarak ortadan kalkmasına rağmen sistemde kalması söz konusudur¹⁵³.

Tasarıdaki düzenleme ile ilgili olarak yukarıda aktarılanlar geçerli olabilecek iken 243. maddedeki düzenleme için aynı şeyi söylemek mümkün değildir. Bu açıdan 243. maddede düzenlenen suçun Tasarıda öngörülen suçtan daha farklı bir yapıya sahip olduğunu görülmektedir. Meclis görüşmeleri sırasında kabul edilen değişiklik önergesinde “...hukuka aykırı olarak giren **veya** orada kalmaya devam eden...” ifadesinin “...hukuka aykırı olarak giren **ve** orada kalmaya devam eden.” şeklinde değiştirilmesi, bu suçun unsurunda ve niteliğinde değişikliğe yol açmıştır¹⁵⁴.

¹⁵³ Valerio **FALZETTI**, I Computer Crimes, 83 vd. <http://www.unicam.it/ssdici/falzetti.pdf..>

¹⁵⁴ Meclis görüşmelerinde bu hususa ilişkin olarak “*Biliyorsunuz bir de bilgisayar sistemin bozan hackerlar var, onlar size bir şey gönderdi, üzerine tıkladınız ve bir sisteme girdiniz. Hemen bunu suç haline getirirsek, çok geniş bir kapsama almış oluruz, suç kapsamını genişletmiş oluruz. Burada da – hazırladığımız taslakta- girme ve orada kalma şartını koyduk; çünkü bu bir kasıttır. Kazara girersiniz çıkarsınız, bu başka bir şey; ama, girdiniz, kaldınız, değiştirdiniz, bozdunuz, bu farklı bir şey. İşte tasarıda, buraya açıklık getirdik...*” denmiştir. TBMM Genel Kurul Tutanağı 22. Dönem 2. Yasama Yılı 121. Birleşim 16/Eylül /2004 Perşembe s. 23 http://www.tbmm.gov.tr/develop/owa/tutanak_ss.birlesim_baslangic?P4=12505&P5=B&page1=23&page2=23&web_user_id=2491460 (kontrol tarihi 30.11.2005)

İleri sürülen bu görüşten ,sisteme kazara girilmesi halinin madde kapsamında bir suç olduğu görüşünden hareketle maddede değişiklik yapıldığı sonucunu çıkarmak mümkündür. Öncelikli olarak belirtmek gerekirse, yukarıda İtalyan Ceza Kanunun 615-ter maddesi ile ilgili olarak belirtildiği üzere, sistemde kalma ya da kalmaya devam etme iki olasılık ile ilgili olarak karşımıza çıkmakta idi. Bunlardan birincisi sisteme hukuka uygun ya da rızaen girilmiş olması ve daha sonra sistemde rıza dışında kalınması halidir. İkinci olasılık ise sisteme yanlışlıkla, kazayla girilmiş olması durumunda sistemden çıkılmaması halini düzenlemektedir. Kazara sisteme girilmiş olması durumunda – yukarıdaki örnekte olduğu gibi- suçun manevî unsurunu oluşturan kast eksiktir. Bu açıdan kazara sisteme girme zaten taslaktaki düzenleme kapsamında değildi. Bu açıdan kazara girilmesi halinde de suçun işlenmiş sayılacağı gerekçesi yersizdir. Nitekim benzer bir düzenlemeye yer verilen İtalyan Ceza Kanununun 615 ter maddesinde de sistemde kalma ile ilgili olarak bunun hataen ya da rıza dışında olmak üzere iki şekilde gerçekleşebileceği, ifade edilmiş, özellikle sisteme hataen girilmesi durumunda bunun devam etmesi halinde yani sistemde kalınması halinde 615 ter maddesine göre cezalandırılacağı belirtilmiştir. **FALZETTI**, s.90 – 91.

b. Suçun Hukuki Konusu

i. Genel Olarak

Bilişim sistemlerine yetkisiz erişim suçuyla, verinin elde edilmesine ilişkin düzenlemelere paralel bir şekilde fakat bilişim söz konusu sistemlerin sahibi ya da kullanıcılarının ilgili sistem üzerinde tasarruf edebilmelerine ilişkin yetkinin korunması amaçlanmıştır. Bu tasarruf yetkisinin kapsamı ise genel olarak bir bilgisayar sistemine kimlerin erişim sağlayabileceğinin ya da diğer bir ifade ile girebileceğinin, sistem sahibi ya da sistem üzerinde hak sahibi olan diğer kişiler tarafından belirlenebilmesidir. Bu şekliyle dışa dönük bir nitelik taşıyan tasarruf yetkisinin görünümü; kimi düzenlemelerde kişinin malvarlığı üzerindeki tasarruf yetkisinin korunması ve dolayısıyla mameleki bir değer korunması, kimi düzenlemelerde ise özel hayatın gizliliğinin belirli bir yönünün korunması şeklinde ortaya çıkmıştır¹⁵⁵.

¹⁵⁵ Siberaç Sözleşmesinin Açıklayıcı Rapor'u incelendiğinde bilişim sistemlerine yetkisiz erişim suçunun hukuki konusu kapsamında çeşitli ülkelerde ortaya çıkan eğilimleri kapsayacak şekilde bir yaklaşımın sergilendiği sonucuna varmak mümkündür. Bu açıdan Siberaç Sözleşmesinde yer alan bilgisayar sistemlerine yetkisiz erişim suçu ile yukarıda sayılan hususları kapsayacak bir şekilde bilgisayar sistemlerinin korunduğu ifade edilmektedir. Sözleşmenin açıklayıcı raporunda bilgisayar sistemlerinin güvenliğinin korunması esastan hareketle geniş bir koruma alanının kapsama alınmak istendiği görülmektedir. Açıklayıcı raporda bu husus bir yandan gizli verinin ve sırrın ele geçirilmesinin önlenmesi olarak gizliliğin korunması şeklinde ifade edilmiştir. Diğer yandan, verinin ve sistemin bütünlüğünün korunması bakımından bunlara ilişkin bir tahribata ve bu tahribatın giderilmesine ilişkin yüksek bir maliyete yol açacağı, sistemin ödeme yapılmadan kullanılması sonucunu doğuracağı, bilgisayar aracılığıyla dolandırıcılık ve sahtekarlığı teşvik edeceği ifade belirtilerek hem mameleki değer olarak ortaya çıkan bir zarara işaret edilerek bu yönde bir koruma sağladığı hem de Sözleşmenin diğer maddelerinde yer alan suçların önlenmesine ilişkin bir ön koruma sağladığı vurgulanmıştır. Bkz., Convention on Cybercrime, Explanatory Report <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>, parag. 44. Türkçe çevirisi için bkz., <http://www.ivhp.org.tr/belgelik/siber.zip>. Siberaç Sözleşmesinde yer alan yetkisi erişim suçu hakkında bkz., SOKULLU-AKINCI, s. 14-16

ii. Mameleki Bir Değerin Korunması Açısından Siberaian

Malvarlığının ve dolayısıyla kişiye ait mameleki değerin korunmasına ilişkin yaklaşım ABD’de özellikle ABD’de federe devletlerde kendisini göstermektedir. Yukarıda belirtildiği üzere bu devletlerin ilgili düzenlemelerinde verinin kendisi eşya olarak kabul edilmekte ve dolayısıyla verinin ele geçirilmesi suçu da mameleki değerin korunmasına yönelik bir suç olarak düzenlenmiştir. Aynı yaklaşım yetkisiz erişim suçu bakımından da geçerliliğini korumaktadır. Bu husus bir yönden yetkisiz erişim suçunun özellikle Federe devletlerde ceza mevzuatları içerisinde düzenlendiği yerde göstermektedir. Diğer bir yönden yetkisiz erişim suçunun kıyasen incelendiği ve başkasının mülküne girilmesi olarak çevrilebilecek “*criminal trespass*” suçunun niteliği, yetkisiz erişim suçu ile de ABD ve özellikle Federe devletlerde yetkisiz erişim suçu ile mameleki değerin korunmak istendiği sonucuna götürmektedir¹⁵⁶.

Nitekim yetkisiz erişim suçu kapsamındaki fiiller ABD’de genel olarak başkasının mülküne girilmesi suçu kapsamında bu suç ile karşılaştırmalı olarak incelenmiştir¹⁵⁷. Başkasının hakkına tecavüz olarak Türkçe’ye çevrilebilen “trespass”

Carr ise Siberaian Sözleşmesinde de yer alan ve herhangi ek bir şarta yer vermeyen yetkisiz erişim suçuna ilişkin düzenlemenin, güvenlik önlemlerinin ihlali edilmesi durumunda ihlalin tespiti veya finansal ya da bir başka şekilde ortaya çıkan zararın tespitinde zaman ve para sarf edilmesine yol açacağı ve ayrıca güvenlik önlemlerinin geliştirilmesi ya da kullanıcıların tekrar eğitilmesi şeklindeki ekonomik nedenlere dayandırıldığını ifade etmektedir. Bkz., Indira **CARR, Draft Cyber Crime Convention**, s. 84. (Sciencedirect)

¹⁵⁶ Aynı şekilde sistematik olarak incelendiğinde Fransız Ceza Kanununun 323-1 maddesinde düzenlenen yetkisiz erişim suçunun da mameleki bir değeri korumaya yönelik olduğunu ifade etmek mümkündür.

¹⁵⁷ ABD ve buna bağlı eyaletlerde mülke tecavüz suçu asıl olarak kişinin kendi mülkü üzerindeki tasarruf yetkisinin korunmasına yönelik olarak düzenlenmiştir. Bu suç geleneksel olarak gelişen ve haksız fiil olarak tazmin yükümlülüğünden kaynaklanmaktadır. Önceki dönemlerde sadece bir haksız fiil olarak kabul edilen bu fiil daha sonraki dönemlerde suç haline getirilmiştir. Bu suç hakkında bkz., **Susan W. BRENNER, Is There A Thing as “Virtual Crime”, 4. Cal. Crim. Law. Rev. 1, parag. 18.** <http://www.boalt.org/CCLR/v4/v4brenner.htm>

Anglo-Saxon hukukunda hem gayrimenkullere izinsiz girmeyi hem de menkullere hukuka aykırı müdahaleleri kapsayan bir haksız fiildir. Bu gelişim içerisinde ABD ve ABD’ye bağlı federe devletlerde özellikle gayrimenkule izinsiz girme suç haline getirilmiştir. Bu suçun maddi unsuru ise başkasının taşınmazına hukuka aykırı olarak girilmesi ya da ilgili kişinin rızası hilafına gayrimenkulden çıkılmamasıdır.¹⁵⁸ Niteliği itibariyle bu suç ile genel olarak kişinin taşınmazı üzerindeki mülkiyet hakkından doğan tasarruf yetkisi korunmaktadır¹⁵⁹. Yetkisiz erişim suçu ise bu yaklaşım içerisinde genel olarak başkasının alanına girilmesi esassından hareketle, başkasına ait olan bir alana yetkisiz girme¹⁶⁰ olarak tanımlanabilen “*criminal trespass*” suçu kapsamında incelenmiştir.

Başkasının mülküne fiziksel bir girişin (özellikle gayrimenkule giriş bakımından) ya da müdahalenin arandığı bu suçun, fiziki anlamda bir girişin ya da müdahalenin olmadığı yetkisiz erişim fiillerini kapsamaması, yetkisiz erişim suçunun özel olarak düzenlenmesine neden olarak gösterilmektedir¹⁶¹. Bu gerekçeler esas

¹⁵⁸ Patty M. **DEGAETANO**, *Note: Intel Corp v. Hamidi: Private Property Keep Out – The Unworkable Definition of Injury for a Trespass to Chattels Claim in Cyberspace*, 40. Cal. W. L. Rev. (2003-2004), s. 357-358

¹⁵⁹ ABD’de Yüksek Mahkemenin bir kararında, polisin arama emri olmadan bir kişinin taşınmazına girmesine ilişkin olayda özel hayatın gizliliğine ilişkin makul bir beklentinin söz konusu olmadığı, aynı hakların korunmasının bu gibi durumlarda arama ve elkoyma yetkisine bir engel oluşturmadığı, taşınmaz üzerindeki aynı hakların korunmasına yönelik bir suç olan “*criminal trespass*” suçunun, genel olarak özel hayatın gizliliğinin korunmasına ilişkin hükmün yer aldığı söylenebilecek olan ABD Anayasasının Dördüncü Eki (Fourth Amendment) kapsamında korunan alanlardan çok ve bunların ötesinde, kişinin mülkiyet hakkının korunmasına yönelik bir düzenleme olduğu ifade edilmiştir. Bkz., *Oliver vs. United States*, 466 U.S. 170, bölüm 4, ayrıca dipnot 15., http://supct.law.cornell.edu/supct/search/display.html?terms=trespass&url=/supct/html/historics/USSC_CR_0466_0170_ZO.html (01.06.2006) . Adı geçen karar hakkında ayrıca bkz., Paul R. **STONE** – Henry **De La GARZA**, *Criminal Trespass and the Exclusionary Rule in Texas*, 24 St. Mary’s L. J, 1992, 1993, s. 454 vd. (Heinonline)

¹⁶⁰ **BRENNER**, *Virtual Crime* , parag. 18.

¹⁶¹ Mark D. **RASCH**, *Criminal Law and The Internet*, <http://swiss.csail.mit.edu/6095/articles/computer-crime/rasch-criminal-law.html>.

alınarak yetkisiz erişime ilişkin bazı Federe devletlerin ceza mevzuatlarında yapılan düzenlemelerde yetkisiz erişim suçu, genel olarak malvarlığı aleyhine işlenen suçlar arasında başkasının mülküne girilmesi (criminal trespass) suçu ile aynı bölümde düzenlenmiştir¹⁶².

Burada vurgulanan husus geleneksel “*criminal trespass*” suçu ile yetkisiz erişim suçunun korudukları hususun ya da amacının aynı olduğu, sorunun suçun unsurlarından kaynaklandığıdır. Bu açıdan *Olivenbaum*, genel olarak bilgisayar ile ilgili düzenlemelerin bilgisayarı esas alan teknoloji merkezli düzenlemeler olarak ortaya çıktığını ve gerçekte bu suçların var olan suçların yeni tekniklerle işlenmesi olduğunu ifade etmekte, devamında, bu tür özel düzenlemelerin yerine var olan suçlara ilişkin tanımların bu tür fiilleri de kapsayacak şekilde değiştirilmesi gerektiğini vurgulamaktadır. Yazar, yetkisiz erişim suçu ile ilgili olarak da bu suç ile geleneksel başkasının mülküne girilmesi suçunun aynı amaca yönelik olarak ortaya çıktığını, başkasının mülküne girilmesi suçunun unsurlarının tam olarak gerçekleşmediğinden bahisle buna ilişkin özel bir düzenleme yapılması yerine mülke tecavüz suçuna ilişkin tanımların, özellikle eşyanın tanım ve kapsamının, bu suçu kapsayacak şekilde değiştirilmesinin daha iyi bir çözüm yolu olduğunu ifade etmiştir¹⁶³. Aynı yönde *Brenner* de yetkisiz erişim (hacking) fiillerinin başkasının

Olivenbaum, s 578, ABD’de Federal düzeyde bir kanun olan “Computer Fraud and Abuse Act” Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Hakkında Kanuna yetkisiz erişim suçunun eklenmesi ile ilgili teklifin gerekçesinde de benzer yaklaşım sergilenmiştir. Nitekim yetkisiz erişim suçunun eklenmesi ile ilgili olarak gerekçesinde, yetkisiz erişim fiilinin başkasının mülküne tecavüz suçu ile benzerlik taşıdığı, bilgisayar içerisindeki enformasyonun araştırılması/karıştırılmasının başkasının evine giren kişinin ve orada kişisel kayıt ve belgeleri incelemesi ile aynı zarara yol açtığı ifade edilmiştir. Aktaran OLIVENBAUM, s. 641.

¹⁶² **BRENNER, Virtual Crime**, parag. 83.

¹⁶³ **OLIVENBAUM**, s.557-578, s.640-641; Yazar, bilgisayarla ilgili suçların, suçun maddi unsuru ya da suçta kullanılan araç olarak bilgisayarın esas alınarak düzenlendiğini, bu

mülküne girilmesi ile benzerlik taşıdığını, başkasının mülküne tecavüzde başkasına ait fiziksel bir alana tecavüzün, yetkisiz erişim fiillerinde de başkasına ait sanal bir alana tecavüzün söz konusu olduğunu belirtmiştir. Yazar devamında geleneksel başkasının mülküne tecavüz suçunun unsurlarının “hacking” fiillerini de kapsayacak şekilde yeniden düzenlenebileceğini ifade etmiştir¹⁶⁴.

Brenner’in belirttiği üzere, sanal bir alana giriş ya da *Olivenbaum* ve *Brenner*’in vurguladığı üzere, her iki fiilde de aynı zararın ortaya çıktığı tek farkın suçun maddi unsurunu oluşturan fiilin farklı olmasından kaynaklandığı görüşlerinden hareketle ve ayrıca Federe devletlerin ceza mevzuatları içerisinde yetkisiz erişimin düzenlendiği bölümler de esas alınarak, ABD ve özellikle Federe devletler bakımından yetkisiz erişim suçunun genel olarak malvarlığına yönelik bir suç olduğu sonucuna varılabilmektedir. Burada vurgulanan husus ise her iki suç ile ortaya çıkan zararın ve suçların amaçlarının ya da diğer bir ifade ile suçların hukuki konusunun aynı olduğu, sorunun fiziksel bir girişin yetkisiz erişim suçunda var olmamasından yani suçun maddi unsurunun gerçekleşmediğinden kaynaklandığıdır.

Burada özellikle vurgulanması gereken nokta *Brenner*’in belirttiği üzere sanal bir alanın varlığı noktasından hareket edilmiş olmasıdır. Gerçek ve sanal alan ayrımı

düzenlemelerde suç ile korunmak istenen hususun gözden kaçırıldığını ifade etmektedir. Bu doğrultuda yazar, “*criminal trespass*” suçu ile yetkisiz erişimin aynı amaca yönelik olarak ortaya çıktığını ve yetkisiz erişim suçu ile ilgili özel düzenleme yapılması yerine özellikle eşya tanımının bilgisayar verilerini de kapsayacak şekilde genişletilmesi suretiyle mülke tecavüz suçunun kapsamına sokulabileceğini ifade etmektedir. s. 640-641. Aksi görüş için bkz, Leslie **WHARTON**, *Comment: legislative Issues in Computer Crime*, 21 Harv. J. On Legis (1984), s.249.

¹⁶⁴ Yazar, *Olivenbaum* ile aynı yönde, ortaya çıkan zararın her iki fiilde de aynı nitelikte olduğunu bu açıdan alanın fiziksel bir alan ya da sanal bir alan olmasının bunlar arasında herhangi bir fark yaratmadığını ifade etmektedir. Bu açıdan ABD’de federe devletlerin bu yaklaşımı benimsediğini, fakat var olan başkasının mülküne tecavüz (*trespass*) suçunu değiştirmek yerine yeni suçların düzenlendiğini ancak her iki suçun birbirine benzerliği esas alınarak sisteme yetkisiz erişim suçlarının başkasının mülküne tecavüz suçu ile aynı yerde düzenlendiğini belirtmiştir. Bkz **BRENNER, Virtual Crime**, parag. 77 vd.

Avrupa Konseyi Sıbersu Szleşmesinde de yer almıřtır. Szleşmede de siber alan ya da sanal alan “*Enformasyon teknoloji alanındaki hızlı gelişmenin modern toplumun her bölümünde doğrudan etkiler doğurduğu, dünyanın herhangi bir yerinden herhangi bir kişinin erişim sağlayabileceği internet de dahil olmak üzere enformasyon super-otoyollarının ve ağlarının ortaya çıkışının bu gelişmeyi hızlandırdığı. Enformasyon ve iletişim servislerine bağlanması suretiyle kullanıcıların bir çeşit ortak alan yarattıkları ve bunun siber alan olarak adlandırıldığı...*” şeklinde ifade edilmektedir¹⁶⁵.

Bu durumda, gerçek alan ve sanal alan ayırımı içerisinde Szleşmenin açıklayıcı memorandumunda belirtilen ortak alan içerisinde, kişiye ait ya da kişinin tasarrufu altında olan bir alanın yetkisiz üçüncü kişilerin müdahalesinden korunması söz konusu olmaktadır. Bu yaklaşım ise genel olarak gerçek alan ve sanal alan ya da siber alan şeklinde ikili bir ayırıma dayanmaktadır.

iii. Özel Hayatın Gizliliğinin Korunması Kapsamında Siber Alan

Sanal alan gerçek alan ayırımı, yukarıda aktarıldığı şekliyle, İtalyan Ceza Kanununda bilişim alanında işlenen suçlara ilişkin düzenlemeler içerisinde yetkisiz erişim suçunda da bu suçun hukuki konusu bakımından etkisini göstermiştir.

Bilişim suçlarına yönelik olarak İtalyan yaklaşımı, bu alanda ortaya çıkan kötüye kullanımlara ilişkin düzenlemelerin İtalyan Ceza Kanunu içerisinde suçun hukuki konusu esas alınarak ilgili bölümlerde düzenleme yapılması şeklindedir. Bu yaklaşım içerisinde sisteme yetkisiz erişim suçu, Kanunun “*kişilere karşı suçlar*”

¹⁶⁵ Sıbersu Szleşmesi Açıklayıcı Raporu parag. 8.
<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

düzenleyen 12. bölümünde bireysel özgürlüklere karşı suçlar kapsamında “konut dokunulmazlığına karşı suçlar” arasında 615 ter maddesinde düzenlenmiştir. İtalyan Ceza Kanunun 615 ter maddesinde “bilişim” veya “telematik” sistemlerine hukuka aykırı girme veya hak sahibinin açık veya zımni rızası hilafına sistemde kalmaya devam etme fiilleri cezalandırılmaktadır¹⁶⁶.

Konut dokunulmazlığına karşı suçlar arasında düzenlenen yetkisiz erişim suçu ile ilgili olarak madde gerekçesinde, “bilişim” ve “telematik” sistemleri ile İtalyan Anayasasının 14. maddesince güvence altına alınan ve daha önemli hallerde İtalyan Ceza Kanunun 614. ve 615. maddeleri ile korunan ilgili kişiye ait saygı alanının (konutun) düşünsel olarak genişlediği ifade edilmiştir¹⁶⁷.

Bu gerekçe incelendiğinde, özel hayatın gizliliği kapsamında fiziksel bir alan olarak korunan konut yanında bilgisayar sistemlerinin kullanılmaya başlanması ile birlikte konutun düşünsel olarak genişlediği ifade edilmekle, düşünsel bir alanın varlığı da vurgulanmaktadır. Bu ikili ayırım içerisinde, sanal alan içerisinde kişinin tasarrufunda bulunan alan, ABD’de genel olarak malvarlığına ilişkin bir değer koruması olarak karşımıza çıkmakta iken, bu ikili ayırımı esas alan İtalya’da ise özel hayatın gizliliğinin korunması kapsamında konutun bir uzantısı olarak algılanmış ve yetkisiz erişim suçu, konut dokunulmazlığının elektronik ihlali olarak ifade edilmiştir¹⁶⁸.

¹⁶⁶ IPPOLITO, s. 398.

¹⁶⁷ Aktaran IPPOLITO, s. 398; FALZETTI, 83 vd. Federico Tavassi La GRECA, Hacking e Criminalità Informatica, s. 145, http://www.dvara.net/hk/hacking_e_criminalita_informatica.doc; Giovanni TONELLI, Il Delitto Di Accesso Abusivo A Sistemi Informatici O Telematici Con Particolare Riferimento Alla Tutela Dei Dati Personali, s. 22, <http://www.diritto.it/materiali/tecnologie/tesina.pdf>.

¹⁶⁸ IPPOLITO, s. 398.

Bunun yanında, İtalyan doktrinde bir görüş, sanal bir alanın kabulü halinde de yetkisiz erişim suçunun yukarıda belirtildiği şekliyle konut dokunulmazlığın elektronik ihlali olarak düzenlenemeyeceğini savunmaktadır. Buna göre, yetkisiz erişim suçunun hukuki konusunun belirli bir alan olduğu kabul edilse bile bunun başkasının mülküne girilmesi suçunun düzenlendiği 637. maddenin hukuki konusu ile paralellik arz edeceği ifade edilmiştir. Bu kapsamda 614. maddede düzenlenen konut dokunulmazlığının daha çok fiziksel bir alana işaret ettiği bilgisayar sistemlerinin bu anlamda bir alanı oluşturmadığı; bir alanın varlığı kabul edilse bile bunun 637. maddeye paralel bir şekilde, konutun korunması anlamında değil de, kişinin malvarlığı üzerindeki egemenlik hakkı ve bu kapsamda tasarruf yetkisinin korunması şeklinde olabileceği, ABD deki malvarlığının korunmasını esas alan yetkisiz erişim suçuna ilişkin düzenlemelere paralel bir şekilde dile getirilmiştir¹⁶⁹.

iv. Sırrın Korunması Kapsamında Verinin Gizliliğinin Dolaylı Olarak Korunması

Yetkisiz erişim suçunun hukuki konusunun belirli bir alan bakımından malvarlığının ve kişinin malvarlığı üzerindeki tasarruf yetkisinin korunması ya da özel hayatın gizliliği kapsamında konut dokunulmazlığının korunması olduğu görüşleri yanında, bu suçun hukuki konusu ile ilgili olarak ileri sürülen diğer bir görüş, yetkisiz erişim suçunun sırrın korunmasına yönelik olduğudur.

Özellikle İtalyan Ceza Kanununda yetkisiz erişim suçunun düzenlendiği yer ve hukuki konusuna ilişkin ileri sürülen eleştirilere göre, bilişim sistemleri yukarıda

¹⁶⁹

GRECA, s. 148 – 149, **TONELLI**, s. 29 – 30,

aktarıldığı üzere konut ve konutun devamı olan bir sanal alan yaratmamaktadır. Bu açıdan bilişim sistemlerine yetkisiz erişim suçu ile korunmak istenen husus bilişim sistemleri içerisinde bulunan veri hakkında yetkisiz üçüncü kişilerin bilgi sahibi edinememesi olup, bu husus konut dokunulmazlığının da dâhil olduğu özel hayatın gizliliğinin korunması bakımından başka bir yönü gündeme getirmektedir. Bu da özel hayatın gizliliğinin korunması kapsamında sırrın korunmasıdır. Bilişim sistemleri bakımından sırrın korunması bilişim sistemleri içerisindeki verilere erişimin korunması olarak ortaya çıkmakta ve söz konusu durum verinin gizliliğinin korunmasını gündeme getirmektedir. Bu nedenle bilişim sistemlerine yetkisiz erişim suçu ile bilişim sistemleri içerisindeki verilerin gizliliği, sırrın korunması kapsamında dolaylı olarak korunmaktadır¹⁷⁰.

Bu yaklaşım, sırrın korunması kapsamında verinin gizliliğinin korunması şeklinde ortaya çıkan, verinin ele geçirilmesine ilişkin suçlara hukuki konu bakımından paralellik arz etmektedir. Verinin ele geçirilmesine ilişkin suçlarda verinin gizliliği doğrudan bir koruma sağlarken bilişim sistemlerine yetkisiz erişime ilişkin düzenlemelerde bilişim sistemlerinin gizliliğinin korunması dolayısıyla bilişim sistemleri içerisindeki verinin gizliliği korunmakta ve bu haliyle verinin gizliliği bakımından sırrın korunması anlamında dolaylı bir koruma sağlanmaktadır.

v. Türk Ceza Kanunda Düzenlenen Yetkisiz Erişim Suçunun Hukuki Konusu

¹⁷⁰ Ayrıntılı bilgi için bkz., **FALZETTI**, s. 88. vd., **GRECA**, s. 153 vd., **TONELLI**, s. 31 vd., **IPPOLITO**, s. 395.

243. maddede düzenlenen yetkisiz erişim suçunun hukuki konusu ile ilgili olarak çeşitli görüşler ileri sürülmüştür. Bu görüşlerden bir kısmında, 244. maddede düzenlenen suçun hukuki konusunun özel hayatın gizliliğinin korunması olduğu ifade edilmiştir. *Kurt*, bilişim sistemine yetkisiz erişim suçu ile sistem sahibinin kişisel alanına girildiğini ifade etmiştir. Yazara göre; “*Bilişim sistemine girme ve orada kalmaya devam etme suçunda korunan hukuki yarar, özel hayatın gizliliği ve sırların masuniyeti olarak belirlenebilir. Bilişim sistemi ve içinde bulunan veriler, programlar sistem sahibinin özel alanı da bulunmaktadır. Bu suç ile bu alana girilmesi suretiyle güvenlik ve sükun duygusunun sarsılması önlenmeye çalışılmıştır. Bilişim sistemi sahibinin kişisel alanına girilmektedir. Hak sahibi izin vermedikçe bu alana girilmesi mümkün değildir. Anayasanın 20. maddesindeki 'özel hayatın gizliliği'ne ilişkin maddesine paralel bir hüküm olarak karşımıza çıkmaktadır*¹⁷¹.”

Yazarın bu görüşü incelendiğinde, yukarıda da belirtildiği üzere, bilişim sistemlerinin kullanılması ile birlikte, Amerikan hukukunda hakkı olmayan yere tecavüz ve İtalyan hukukunda konut dokunulmazlığının elektronik ihlali şeklinde somutlaşan, gerçek alanın yanında bir siber alanın var olduğu görüşü ile paralellik arz etmektedir.

Biçkin ise, 243. maddede düzenlenen suçun hukuki konusunun karma bir nitelik gösterdiğini ve devamında *Kurt* ile aynı yönde ilk olarak “*bireyin özel hayatının korunduğunu*” belirtmektedir. Yazar özellikle 2. fıkrada yer alan düzenlemeyi esas alarak “*malvarlığının*” da korunan hukuki menfaatler arasında

¹⁷¹ **KURT**, s. 148. Yazar devamında 243. maddede düzenlenen suçun hukuki konusunun kişisel veriler olduğunu ifade etmektedir. a.g.e., s. 150

olduğunu, çünkü bu fıkra da bedeli karşılığında yararlanılabilen sistemler hakkında ilgili suçun işlenmesi halinin düzenlendiğini vurgulamaktadır¹⁷².

TCK'nin 243 maddesinde düzenlenen yetkisiz erişim suçunun hukuki konusunun karma bir nitelik taşıdığı başka bir açıdan *Dülger* tarafından ifade edilmiştir. Yazar, yetkisiz erişimin engellenmesiyle sistemin malik ya da kullanıcıları olarak sistemden faydalanan kişilerin birçok sayıdaki farklı türden çıkarları koruma altına alındığını belirtmektedir. Bu kişilerin çıkarlarının, verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuksal değerler olabildiğini ifade etmiştir. Yazar, farklı türden çıkarlar olarak ifade ettiği bu değerlerin üstünde ve bu değerleri kapsayacak şekilde “*bilişim sisteminin güvenliği*”nin korunmasının asıl hukuki konuyu oluşturduğunu belirtmiştir¹⁷³. Aktarılan bu görüş ise, yukarıda belirtildiği üzere, Siber Suç sözleşmesinin 2. maddesinde düzenlenen yetkisiz erişim suçu ile ilgili olarak Sözleşmenin açıklayıcı raporundaki gerekçe ile paralellik arz etmektedir.

Farklı hukuki konulara yönelik bir suç olduğu bir an için kabul edilse bile, *Dülger*'in ifade ettiği gibi bütün bunları kapsayacak şekilde bilişim sisteminin güvenliğinin asıl hukuki konuyu oluşturduğundan bahsedilmesi söz konusu değildir. Yazarın bilişim sisteminin güvenliği olarak bahsettiği husus, yetkisiz kişilerin sisteme girmesi ve sistem içerisinde işlem yapmasının engellenmesidir. Bu da

¹⁷² İnci **BİÇKİN**, *Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları*, Yargıtay Dergisi, C. 32, S. 1-2, Ocak-Nisan 2006, s. 152.

¹⁷³ **DÜLGER**, s.214 . Aynı Yönde Necati **MERAN**, *Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında İşlenen Suçlar*, 1. B., Ankara, 2005, s.363; **Recep GÜLŞEN**, *İnternet ve Suç*, İnternet ve Toplum, Editör: Ahmet Tarcan, Ankara, 2005, s. 207.

öncelikli olarak sisteme girilmesinin ya da erişimin suç haline getirilmesi ile sağlanmak istenmektedir. Bu durumda bilişim sisteminin güvenliğinin korunması Yazar tarafından ifade edildiği şekliyle birden çok hukuki konunun korunmasına ilişkin araçtır. Bu nedenle kapsayıcı bir değer olarak bilişim sistemlerin güvenliğin korunmasından bahsedilmesi yerine, eğer varsa, farklı türden çıkarların korunmasına yönelik karma bir hukuki konuya sahip bir suçtan bahsedilmesi mümkün olabilecektir. Bilişim sistemlerinin güvenliğinin sağlanması ise, tercih edilen bir araç ya da yöntem olarak yetkisiz erişim ya da TCK'deki ifade ile hukuka aykırı girme ve orada kalmaya devam etme şeklinde somutlaşmaktadır.

Karağülmez ise, başka bir açıdan, genel olarak yetkisiz erişim olarak adlandırılan suçun 243. maddesinde düzenleniş biçimini esas alarak, bu suçun hukuki konusunun bilişim sisteminin güvenliği olduğu görüşünün tartışmalı hale geldiğini ifade etmektedir. Yazar, 243. maddede yer alan suçun maddi unsurunun sadece sisteme yetkisiz erişim olmadığı, bunun yanında sistemde kalmaya devam etme unsurunun da arandığından yola çıkarak, suçun unsurunun bu şekilde düzenlenişinin suçun hukuki konusunun belirlenmesinde de etkili olduğunu vurgulamaktadır. Bu açıdan bilişim sisteminin güvenliğinin korunmasına yönelik bir düzenlemede “*kalmaya devam etme*” şeklinde bir unsura yer verilmeyeceğini; aynı şekilde 2. fıkrada yer alan düzenlemenin de hukuki konunun bilişim sisteminin güvenliği olduğu düşüncesini zayıflattığını ifade etmektedir.

Yazar bu görüşten yola çıkarak ve yine 243. maddede düzenlenen suçta “*kalmaya devam etme*”nin suçun unsuru olmasını esas alarak bu suçun hukuki konusunun bilişim sistemini kullananların belirli bir süreden sonra rahatsız edilmemesi ve devamında suçun hedefi durumundaki sistem kullanıcılarının

(sahiplerinin) çıkarlarının zedelenmemesinin de hukuki konu kapsamında olduğu sonucuna varmaktadır¹⁷⁴.

Yazarın 243. maddenin birinci fıkrasında düzenlenen suçun unsurlarından yola çıkarak “*bilişim sisteminin güvenliği*”nin yetkisiz erişim suçunun, hukuki konusunu oluşturmadığı görüşüne ya da yukarıda ifade edildiği şekliyle güvenliğin korunmasının bir ya da yöntem olarak seçilmediğine katılmak mümkündür. Buna karşın Yazarın 243. maddede düzenlenen suçun hukuki konusuna ilişkin ileri sürdüğü sistem kullanıcılarının belirli bir süre sonrasında rahatsız edilmemesi ve ayrıca sistem kullanıcılarının ya da sahiplerinin çıkarlarının zedelenmemesi olduğu görüşü bu maddenin yorumlanması bakımından açıklıktan uzaktır. Nitekim “*sistem kullanıcıların rahatsız edilmemesi*”, hukuki konu kriterini esas alan ceza kanunları ve suçların dört başlık altında kural olarak hukuki konu kriteri esas alınarak düzenlendiği ifade edilen TCK açısından, kişiye ait hangi tür menfaati ihlal ettiği konusunda somut bir sonuca ulaştırmamaktadır. Aynı şekilde sistem kullanıcılarının çıkarlarının zedelenmemesi de hukuki konu kapsamında hangi tür çıkarların esas alındığını açıklamaktan uzak olup, bu açıdan da somut bir sonuca ulaşmayı engellemektedir.

TCK’nin 244. maddesinde suçun maddi unsuru olarak “*sisteme girme ve orada kalmaya devam etme*”, düzenlenmiştir. Bu düzenleme, ister konut dokunulmazlığının elektronik ihlali, isterse sırrın korunması ya da bilişim sisteminin güvenliğinin korunduğu kabul edilsin, söz konusu değerleri korumaya yönelik ve de bunları koruyabilecek nitelikte değildir. Özellikle, sırrın korunması esasan

¹⁷⁴ Ali **KARAGÜLMEZ**, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 1. B., Ankara , 2005, s. 167.

hareket edildiği düşüncesi, sırrın öğrenilmesi ile sır olarak saklanmasına ilişkin ilgili kişinin beklentisini ve bu yöndeki tasarrufunu ortadan kaldıracığından, bunun korunması sisteme girme ve kalmaya devam etme şeklinde bir düzenleme ile mümkün değildir; bu yönde bir koruma sağlamanın yolu sisteme girilmesinin başlı başına bir suç olması ile sağlanabilir. Aynı şekilde bu suçun unsurları bakımından bu yöndeki düzenleme yukarı da aktarıldığı şekliyle bilişim sisteminin güvenliğinin korunması amacına da hizmet etmemektedir; sisteme girilmesi ile güvenlik ihlal edilmiş olacaktır.

Yetkisiz erişim suçunun hukuki konusunun saptanmasında TBMM Genel Kurul görüşmelerinde 244. maddeye ilişkin değişiklik teklifi ve bu teklif hakkındaki görüşlerin bilinmesi önemlidir. Söz konusu değişiklik teklifine ilişkin görüşler maddenin hangi hukuki konuya yönelik olarak düzenlenmek istediğini göstermesi bakımından önemlidir.

Nitekim, 244. maddeye ilişkin TBMM Genel Kurulunda yapılan görüşmelerde suçun unsurlarına ilişkin bir değişiklik teklif edilmiş ve bu teklif kabul edilerek madde son şeklini almıştır. Suçun unsurlarında yapılması istenen değişikliğe ilişkin “... Burada da -hazırladığımız taslakta- girme ve orada kalma şerhini koyduk; çünkü, bu bir kasttır. Kazara girersiniz çıkarsınız, bu başka bir şey; ama girdiniz kaldınız, değiştirdiniz, bozdunuz, bu farklı bir şey. İşte biz tasarıda, buraya açıklık getirdik . Bağlantılı olarak 244'te de bir açıklık getiriyoruz¹⁷⁵.” gerekçesi ileri sürülmüştür.

Aynı değişiklik teklifinde 243. maddenin son fıkrasında düzenlenen ağırlatıcı nedenin varlığı halinde öngörülen cezanın miktarına ilişkin olarak şu görüş dile

¹⁷⁵ GÜNEY, s. 712.

getirilmiştir: “Çocuğunuz 16 yaşında; geldi, bilişim sistemine girdi ve istemeden bir değişikliğe ya da veri kaybına neden oldu. Biz, şu andaki tasarıda diyoruz ki, bu kişiyi iki yıldan dört yıla kadar mahkûm edelim; ama, bir sonraki maddede diyoruz ki, bozma niyeti olana, bozma amacıyla, veriyi değiştirme amacıyla, sistemin tamamına zarar verme amacıyla bu eylemi işleyene de bir yıldan üç yıla kadar ceza verelim; hazırlanan metin bu şekilde. Şimdi, bir şey düşünün; suçu işleyen kişi, hâkimin karşısına geçecek, bu işi bilmeyerek yaptıysa, daha az ceza almak için "hâkim bey, benim kastım vardı, bu işi bilerek, isteyerek yaptım" diyecek ve bunun karşılığında daha az bir ceza alıp kurtulacaktı. Fiilde dengesizlik var.”¹⁷⁶”

Her iki görüş incelendiğinde de 243. maddenin hukuki konusu ile ilgili olarak özel hayatın gizliliğinin ya da bu kapsamda sırrın korunmasına ilişkin tercihin esas alınmadığı görülmektedir. Bunun yerine bilişim sisteminin işleyişinin korunması açısından bilişim alanında işlenen suçların konusunu oluşturan hareketler arasında önem derecesine göre bir ayırım yapılmıştır. Bu açıdan bu fiiller içerisinde en hafifi sisteme girilmesi olarak kabul edilmektedir. Her ne kadar hatalı olarak suçun manevi unsuru kapsamında sadece girmenin suç sayılması çeşitli sakıncalara yol açacağı belirtilmişse de gerekçenin devamı incelendiğinde girmenin önem derecesi bakımından en alt sırada olduğu ve en önemli hususun sistemin bozulması olarak ifade edildiği görülmektedir.

Bilişim alanında suçlara ilişkin değişiklik teklifine ilişkin bu görüşler incelendiğinde, değişiklik tekliflerine hakim olan yaklaşımın bilişim sistemlerinin işleyişinin korunması isteği olduğu görülmektedir. Bu haliyle değişikliğe hakim olan yaklaşım, malvarlığına ilişkin bir değer korunması olup bu husus 243. ve 244.

¹⁷⁶ GÜNEY, s. 712.

maddelerde somutlaştırılmıştır. 243. ve 244. maddeler içerisinde en hafif cezanın yetkisiz erişim fiiline ve en ağır cezanın 244. maddenin birinci fıkrasında düzenlenen sisteme müdahaleye öngörülmesi bunu göstermektedir. 244. maddenin 3. ve 4. fıkralarında düzenlenen ağırlatıcı nedenlerin varlığı halinde cezanın artması da bu hususu destekler niteliktedir. Ayrıca değişikliğe ilişkin olarak, özellikle 243. maddenin son fıkrasına ilişkin Tasarıda yer alan hüküm bakımından dile getirilen eleştiri, yetkisiz erişim suçunun malvarlığının korunması merkezinde ele alındığını göstermektedir. Nitekim 243. maddenin son fıkrasında yer alan ağırlaştırıcı nedenin gerçekleşmesi halinde, faile, veriye müdahale suçunun kasten işlenmesi halinde verilecek cezaya göre daha fazla ceza verilmesini öngören Tasarıdaki hüküm, değişiklik teklifinin konusunu oluşturmuştur. Tasarıda ve Genel Kurul gündemine alınan metinde, yetkisiz erişim sonucunda verilerin yok olması ya da değişmesi halinde 244. maddenin son şeklinde olduğu gibi cezanın arttırılacağı öngörülmektedir. Fakat Genel Kurul görüşmelerine konu olan metinde, neticesi sebebiyle ağırlaşan suç olarak düzenlenen bu durumda, verilecek ceza veriye müdahaleye göre daha fazlaydı. Değişiklik teklifi gerekçesinde bu husus sisteme veya veriye kasten müdahale eden failin daha az ceza alacağı, fakat sisteme giren ve kasıtlı olmadan veriyi değiştiren veya yok eden failin ise daha çok ceza alacağı için eleştirilmiştir. Tek bir hukuki konu açısından yani sisteme yönelik zarar verici fiiller anlamında malvarlığının korunması açısından bakıldığında söz konusu eleştiri yerindedir. Fakat yetkisiz erişim suçu ile özel hayatın gizliliğinin korunmasının esas alınması durumunda bu eleştiri değerini kaybetmektedir. 244. maddenin son fıkrasında Tasarıda olduğu şekliyle veriye müdahaleden daha ağır cezanın verileceğinin düzenlenmesi ikinci bir hukuki konunun ihlali olarak

yorumlanabilecekti. Bu doğrultuda, özel hayatın gizliliğinin ya da sırrın korunması birinci hukuki konuyu oluştururken, bunun yanında sistem içerisinde veriye müdahale edilmiş olması diğer bir hukuki konuyu oluşturabilecekti. Bu durumda hem özel hayatın gizliliğinin ihlali hem de malvarlığına yönelik bir müdahale doğal olarak sadece malvarlığına yönelik bir müdahaleyi esas alan veriye müdahaleden daha ağır cezalandırılabilirdi. Değişiklik teklifinde bu hususun göz ardı edilerek sisteme yönelik zarar verici fiiller açısından değerlendirme yapması, malvarlığına ilişkin koruma sağlama amacının güdüldüğünü göstermektedir. 243. ve 244 maddelerin son şekli bu amacın maddeye yansıtıldığını da göstermektedir.

Karşılaştırmalı hukuk incelendiğinde de hukuki konuya ilişkin tercihin malvarlığının korunması olarak esas alınan yetkisiz erişim suçuna ilişkin düzenleme şekli bakımından TCK'ye benzer bir yaklaşımın egemen olduğu görülmektedir.

Yukarıda özellikle ABD'de federe devletlerde ve İtalya örneklerinde de incelendiği üzere, bilgisayar sistemlerine yetkisiz erişim suçu, genel olarak kişiye ait mameleki bir değer korunması ya da kişi hürriyetinin korunması merkezinde suçun hukuki konusunun seçimi ve bu yönde yapılan düzenlemeler, yetkisiz erişim suçunun ceza kanunları içerisinde düzenlendiği yer bakımından da etkisini göstermektedir. Suçunun hukuki konusunun mameleki bir değer olarak öngörülmesi durumunda, yetkisiz erişim suçu mameleki değerleri korumaya yönelik diğer suçlar arasında yer almakta¹⁷⁷, kişi hürriyetinin korunması esas alınarak yapılan düzenlemelerde ise yetkisiz erişim suçu İtalya örneğinde olduğu gibi kişi hürriyetinin korunmasına yönelik suçlar arasında yer almaktadır.

177 ABD'ye bağlı Federe devletler yanında Fransız Ceza Kanununda da bu ve bilişim sistemleri ile ilgili diğer suçlar “*Malvarlığına Karşı diğer Suçlar*” başlığı altında sistematik olarak malvarlığına karşı suçlar bölümünde düzenlenmiştir.

Her iki yaklaşım incelendiğinde, birinci bölümde genel olarak incelenen veri ve veri işleme faaliyetinin, birbirini tamamlayan farklı görünümüleri içerisinde belirli bir tercihi yansıttığı söylenebilir. Bu açıdan malvarlığına ilişkin değerin korunması esasından hareketle yapılan düzenlemeler bilgisayar sistemlerinin kötüye kullanılmasına ya da bilgisayar suçları olarak düzenlenen fiillerin işlenmesine ilişkin tarihsel sürece ve sosyo-ekonomik dönüşüm içerisinde bilgi ve enformasyonun başlı başına bir değer, bu kapsamda ekonomik bir değer, kazanması esasına vurgu yapmaktadır¹⁷⁸.

Kişî hürriyeti kapsamında genel olarak sırrın korunması ya da İtalyan örneğinde olduğu şekliyle konutun dokunulmazlığının elektronik ihlali bağlamında

178 Tarihsel olarak incelendiğinde bilgisayar sistemlerinin kötüye kullanılması birinci bölümde değinildiği üzere, hukuki düzenlemeleri iki farklı yönden etkilediği görülmektedir. 1960'lı yıllarda, bilişim suçlarından daha önceki bir dönemde tartışılmaya başlanan husus, özel hayatın gizliliği merkezinde dile getirilen kişisel verilerin korunmasıdır. Bunun yanında 1970'li yıllarda tartışılmaya başlanan husus ise bilgisayar suçları olarak karşımıza çıkmaktadır. Bu konudaki tartışmalar ise ekonomik çıkar amacıyla işlenen suçlar merkezinde yapılmıştır. Bu açıdan bilgisayar sistemlerinin kötüye kullanımına ilişkin tartışmalar özellikle ABD'de 1970'li yıllarda ilk olarak telefon hat ve frekanslarından bedelsiz yararlanılması fiillerini tanımlayan "phreaking" fiilinin örnek verilebileceği ve aşağıda incelenecek olan bilgisayar sistemleri aracılığıyla yarar sağlama fiilleri kapsamında ekonomik çıkar sağlamaya yönelik fiiller merkezinde tartışılmıştır. Bu tarihsel gelişim bilgisayar suçları olarak adlandırılan suçların ekonomik suçlar arasında incelenmesine ve hali hazırda ekonomik suçlar kapsamında değerlendirilmesine neden olmuştur. Bu açıdan yetkisiz erişim suçu da bu tür fiillerin engellenmesine yönelik bir suç olarak ekonomik suçlar arasında değerlendirilmiştir. bkz, **SIEBER**, , s. 27 vd., Jari **RAMAN**, Computer Crime, parag 2.2.1, http://www.ulapland.fi/home/oiffi/enlist/commentary/computer_crime.html#alav13 (kontrol tarihi 01.06.2006)

Bu yaklaşımın Avrupa Birliği tarafından da benimsendiği görülmektedir. bkz., COMMISSION OF THE EUROPEAN COMMUNITIES, COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime , s.13, http://eur-lex.europa.eu/LexUriServ/site/en/com/2000/com2000_0890en01.pdf. (kontrol tarihi 01.06.2006)

"Phreaking" hakkında bkz., Bryan **CLOUGH** – Paul **MUNGO**, **Veri Suçları ve Bilgisayar Yer altı Dünyası**, Çev. Emel Kurma, İletişim Yayınları, 1. B., 1999, s. 19 vd.

konutun korunması, tarihsel süreç içerisinde yetkisiz erişimin hukuki konusu bakımından yeni bir yaklaşım olarak ortaya çıkmaktadır. Özel hayatın gizliliğinin çeşitli yönleriyle korunmasına ilişkin değer ile malvarlığına ilişkin değer içerisinde yetkisiz erişim suçundan suçun hukuki konusu bakımından tercih, yetkisiz erişim suçunun ceza kanunları içerisinde düzenlendiği yeri de belirlemektedir.

Yetkisiz erişim suçunda tercih edilen hukuki konu, aynı zamanda bu suç için bilişim alanında diğer suçlara göre öngörülen cezanın miktarını da etkilemektedir. Bilişim suçlarının genel olarak malvarlığı aleyhine işlenen suçlar arasında düzenlendiği ve bu sistematikten hareketle mameleki bir değer korunduğunu ifade edebileceğimiz ceza kanunlarında, yetkisiz erişim suçunun basit şekli için öngörülen cezanın, sisteme ya da verilere zarar verme suçunun basit şekli için öngörülen cezadan genel olarak daha hafif olduğu ifade edilebilir.

Nitekim 243. maddenin esinlendiği Fransız Ceza Kanununda bunu görmek mümkündür. Adı geçen Kanunda yetkisiz erişim suçuna ilişkin 323-1. maddesi malvarlığına karşı suçlar arasında düzenlenmiştir. Suça öngörülen ceza aynı Kanunun 323-2. maddede düzenlenen sisteme müdahaleye ilişkin suçu ve de 323-3. maddede düzenlenen veriye müdahale suçunun cezasından daha hafiftir. Aynı yaklaşımı ABD’de federe devletlerin ceza mevzuatlarında benimsenmiştir.

Buna karşın, bilişim alanında suçların hukuki konusu bakımından ayırımı gidildiği ve özellikle yetkisiz erişim suçu bakımından bu suçun hukuki konusunun genel olarak özel hayatın gizliliği kapsamında değerlendirildiği düzenlemelerde, yetkisiz erişim suçunun basit şekline öngörülen ceza, sisteme ve verilere zarar verme suçuna öngörülen ceza ile miktarı itibarıyla paralellik arz etmektedir. Nitekim yetkisiz erişim suçunun özel hayatın gizliliği esas alınarak düzenlenen İtalyan Ceza

Kanunun 615-ter maddesinde yetkisiz erişim suçunun basit şeklinin cezası ile aynı Kanunda malvarlığına karşı suçlar içerisinde mala zarar verme suçunun düzenlendiği bölümde yer alan bilişim ya da telematik sistemine ya da verilere zarar verme suçuna öngörülen ceza ile, yukarı hadleri itibariyle, paralellik arz etmektedir. Alman Ceza Kanunu içerisinde de sırrın korunması kapsamında özel hayatın gizliliğinin korunmasına ilişkin suçların düzenlendiği bölümde yer alan, yetkisiz erişim fiillerine de uygulanabileceği ifade edilen¹⁷⁹ verinin ele geçirilmesinin düzenlendiği 202a maddesinde öngörülen ceza ise, mala zarar vermeye ilişkin suçların yer aldığı bölümde veriye müdahale suçunun düzenlendiği 303a maddesinde öngörülen cezadan daha ağırdır.

İtalyan Ceza Kanunun 615 ter maddesinin 3. fıkrasında, bilişim ya da telematik sistemlerine girilmesi ya da ilgili kişinin rızası dışında kalınması sonucunda sistemin ya da sistem içerisindeki verilerin tahrip olması ya da bunlara zarar verilmiş olması halinde verilecek cezanın arttırılacağı öngörülmüştür. 615 ter maddesinde yer alan yetkisiz erişim suçunun basit şeklinin cezası, üç yıla kadar hapis cezasıdır. Maddenin 3. fıkrasında öngörülen ağırlatıcı nedenin gerçekleşmesi halinde verilecek ceza, bir yıldan beş yıla kadar hapis cezasıdır. Aynı Kanunun 635 bis maddesinde, genel olarak sisteme ve verilere zarar verme mala zarar verme suçundan hemen sonra bu suça ilişkin özel bir düzenleme olarak ele alınmış ve düzenlenmiştir. 635 bis maddesinde düzenlenen fiilin gerçekleştirilmesi halinde fiil daha ağır bir suç oluşturmuyorsa verilecek ceza altı yıldan üç yıla kadar hapis cezasıdır. Bu açıdan bakıldığında İtalyan Ceza Kanunun 615 ter maddesinin 3. fıkrasında ağırlatıcı neden olarak düzenlenen husus, neticesi sebebiyle ağırlaşan suç olup burada iki farklı

179 SCHWARZENEGGER, , parag. 33 vd.

hukuki konunun ihlali suçı öngörülen cezanın 635bis maddesine göre daha ağır olması sonucunu doğurmaktadır. 3. fıkrada öngörülen halde, gerekçe esas alınırsa konut dokunulmazlığının ya da doktrinde yaygın görüş kabul edilirse sırrın masuniyetinin ihlali yanında, mala zarar verme kalıbında düzenlenen sisteme veriye zarar verilmesi merkezinde, malvarlığının korunmasına ilişkin değer de ihlal edilmektedir.

Buna karşın, bilişim alanında işlenen suçların malvarlığına karşı diğer suçlar başlığı altında düzenlendiği, Fransız Ceza Kanunun 323-1 maddesinde yetkisiz erişim suçunun cezası iki yıl hapis ve 3000 avro para cezası öngörülmüştür. Yetkisiz erişim fiili sonucunda sistemin işleyişinde değişime neden olur ya da sistem içerisindeki veriye erişilemez hale gelir veya veri değişirse, verilecek ceza arttırılmakta ve 3 yıl hapis 45000 avro para cezası öngörülmektedir. Bu halde verilecek ceza, aynı Kanunun 323-2 ve 323-3 maddelerinde düzenlenen sistem ve verilere müdahaleye ilişkin suçlar için öngörülen cezadan daha hafiftir¹⁸⁰. Sistematiik olarak malvarlığının korunması esasından hareketle düzenlenen bilişim alanında suçlar, Fransız Ceza Kanununda aynı hukuki konu içerisinde bu hukuki konuyu ihlale yönelik çeşitli fiilleri kapsamakta ve önem derecelerine göre düzenlenmektedir. İtalyan Ceza Kanununda olduğu şekliyle, yetkisiz erişim suçu bakımından özel hayatın gizliliğinin belirli bir yönünün korunması şeklinde bir tercih esas alınmamaktadır.

Her iki kanun açısından bakıldığında yetkisiz erişim suçuna öngörülen cezanın miktarının sisteme ve veriye müdahale suçuna öngörülen cezaya oranı,

180 Fransız Ceza Kanunun 323-2 ve 323-3 maddelerinde düzenlenen bu suçlar için öngörülen ceza 5 yıl hapis ve 7000 avro para cezasıdır. Kanunun ilgili maddeleri için bkz., <http://www.legifrance.gouv.fr/WAspad/UnCode?code=CPENALLL.rcv>

bunun yanında ve belki de bundan daha önemli olan, yine her iki kanun bakımından yetkisiz erişim fiili sonucunda sisteme ya da sistem içerisindeki veriye bir zarar verilmesi ya da bunların yok olması ya da bozulması halinde öngörülen cezanın miktarının, sisteme ve veriye müdahale suçuna öngörülen cezanın oranına göre gösterdiği farklılık bu suçun hukuki konusunun saptanmasında belirleyici bir etken olmaktadır.

İtalyan Ceza Kanununda olduğu şekliyle yetkisiz erişim suçunun özel hayatın gizliliğine ilişkin bir suç olarak düzenlenmesi, bu suçun hukuki konusunu malvarlığının korunması kapsamında mala zarar vermenin özel şekli olarak düzenlenen sisteme ve veriye müdahale suçundan farklılaştırmaktadır. Sisteme yetkisiz erişim sonucunda ağırlatıcı neden olarak karşımıza çıkan sisteme ya da veriye zarar verilmesi halinde verilecek ceza, birden fazla hukuki konunun ihlali dolayısıyla, 635bis maddesinde yer alan sisteme ve veriye kasten müdahale suçuna öngörülen cezadan daha ağır olmaktadır. Buna karşın Fransız Ceza Kanununda düzenlendiği şekliyle yetkisiz erişim suçunda, kasten sisteme giren bir kişinin bu fiili sonrasında bu fiille bağlantılı olarak sistem ya da veriye zarar verilmesi, sisteme ve veriye kasten müdahale suçlarına (323-2, 323-3) öngörülen cezaların, bu suçların aynı hukuki konuya sahip olması ve bu açıdan sisteme ve veriye müdahalenin kasıtlı olarak gerçekleşmemiş olması nedeniyle, daha azdır.

TCK'nin 243. maddesindeki düzenleme karşılaştırmalı hukuktan da örnek verildiği üzere malvarlığının korunmasına ilişkin bir düzenlemedir. Yukarıda açıklananlar doğrultusunda özetle, Türk Ceza Kanununda bilişim alanında işlenen suçlar içerisinde 243. maddede düzenlenen yetkisiz erişim suçunda bir zarar tehlikesinin esas alındığı görülmektedir. Bu haliyle de yetkisiz 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 korunmasıdır¹⁸¹. Bu haliyle de, sırrın korunması ya da konut dokunulmazlığı korunması şeklinde ortaya çıkan, özel hayatın gizliliğinin korunmasına ilişkin değerin ikinci plana itildiği görülmektedir.

c. Suçun Maddi Unsuru Olarak Bilişim Sisteminin Bütününe veya Bir Kısmina Girme ve Orada Kalmaya Devam Etme

Bu suç yaygın olarak “*illegal access*” “*yetkisiz veya hukuka aykırı erişim*”¹⁸² olarak adlandırılmakta ve suçun maddi unsuru sisteme erişim (access) olarak düzenlenmektedir. Nitekim Avrupa Konseyi’nin Siberaç Söleşmesi’nin İngilizce metninde de bu suç “*illegal access*” (yetkisiz/hukuka aykırı erişim) olarak adlandırılmaktadır. Aynı şekilde ABD ve İngiltere’de bu suç yetkisiz erişim olarak

181 Bir an için yukarıda aktarıldığı şekliyle bilişim sistemlerinin kullanılması ile birlikte bir siber alanın oluştuğı kabul edilse de, suçun hukuki konusunda mameleki bir değerin korunmasının esas alındığını söylemek mümkündür. Siber alanın varlığı kabul edilse de Türk Ceza Kanununda düzenlendiğı şekliyle, yetkisiz erişim suçunun hukuki konusu, sistem üzerindeki hak sahibinin bu hakkının kullanmasına ilişkin tasarruf yetkisinin sınırlandırılması anlamında, 765 Sayılı TCK’nin 520. maddesinde düzenlenen başkasının kapalı arazisine girilmesi suçuna paralellik arz etmektedir. Söz konusu suç incelendiğinde maddede yer alan şekilde başkasına ait kapalı bir alana girilmesi suçunda maddi bir zarar aranmamakta fakat bura da kişinin aynı haktan doğan tasarruf yetkisi bertaraf edilmektedir. 765 Sayılı TCK’de düzenlenen başkasının kapalı arazisine girilmesi suç hakkında bkz, DÖNMEZER, **Kişilere ve Mala Karşı Cürümler**, s. 575-576

182 “Access” teriminin Türkçe karşılığı olarak erişim terimi kullanılmaktadır. Bkz., TDK “**Bilgisayar Terimleri Karşılıklar Kılavuzu**” <http://tdk.org.tr/biliterim/>

adlandırılmakta ve bu suçla ilişkin düzenlemelerde suçun maddi unsuru sisteme erişim (access) olarak düzenlenmektedir.

Parker, Türkçeye erişim olarak çevrilen “*access*” teriminin ceza hukuku alanında karışıklıklara yol açabileceğini, bu terimin fiziksel bir alana erişilmesini ya da girilmesini çağrıştırdığını, fakat bilgisayara girişin bu açıdan imkânsız olduğunu belirtmektedir¹⁸³. Bilgisayarlar bakımından, bilgisayara sinyal gönderilmesi ve bunun sonucunda bilgisayarın, bu sinyale belirli bir programın çalışması ve de sıklıklı bir programın başlaması şeklinde, cevap vermesinin söz konusu olduğunu ifade etmektedir. Bu nedenle kullanılması gereken doğru terimlerin “*bilgisayara yaklaşılma (approach) ya da enformasyona girilmesi*” ve bilgisayarın “*kullanılması*” olduğunu ifade etmektedir¹⁸⁴.

Günümüzde yaygın olarak kullanılan Windows ve Unix tabanlı işletim sistemleri açısından değinilecek olursa, en az bir yönetici hesabı ve bunun yanında sistemin teknik olarak elverdiği sayıda oluşturulabilecek kullanıcı hesabı bulunmaktadır¹⁸⁵. Kullanıcılar kimi zamanlarda yönetici yetkilerine de sahip olabilmesine rağmen, özellikle çok kullanıcıli sistemler açısından genel olarak sınırlı yetkiye sahip olabilmektedir. Sistem içerisinde kullanıcıların yetkilerinin belirlenmesi genel olarak sistem içerisinde yer alan yönetici tarafından

¹⁸³ Aynı yönde, Mark D. **RASCH**, 11. Criminal Law and The Internet, <http://cla.org/RuhBook/chp11.htm> , Salvatore **RESTA**, I Computer Crimes Tra Informatica e Telematica, Cedam, 2000, s.100-101.

¹⁸⁴ Donn B. **PARKER**, Fighting Computer Crime, A New Framework For Protecting Infomation, 1998, s.82, Karagülmez de “girme ve “erişim” sözcüklerinin kullanımında, bilişim sisteminin kendine özgü yapısı bakımından farklılıklar bulunduğunu; girme sözcüğünün fiziki bir alanı anlattığını, elektronik yapıdaki bilişim sistemine ise, girmenin değil erişimin söz konusu olduğunu ifade etmiştir. **KARAGÜLMEZ**, s. 169

¹⁸⁵ Windows işletim sistemleri ve Unix tabanlı işletim sistemlerinde kullanıcı hesapları ve gruplar hakkında teknik açıklama için bkz., Davut **YILMAZ**, Hacking, Bilişim Korsanlığı ve Korunma Yöntemleri, İstanbul 2004, s. 76 vd.

gerçekleştirilmektedir¹⁸⁶. Bu açıdan yönetici sistem içerisindeki kullanıcıları belirli dizin, klasör ya da dosyalara erişim yani genel olarak verilere erişim bakımından sınırlandırabileceği gibi bununla birlikte belirli işlemlerin yapılması bakımından da sınırlandırabilir¹⁸⁷. Özellikle çok kullanıcıli sistemlerde kullanıcıların yetkilerinin belirlenmesi sistem kaynaklarına kimlerin ne şekilde erişebileceğinin önceden tespit edilmesi bakımından önem arz etmektedir.

Yönetici (administrator ya da root), bir bilgisayar sisteminde, sistemin teknik olarak elverdiği ölçüde her türlü yetkileri kullanabilir. Yönetici dışındaki kullanıcılar ise yönetici ile aynı yetkilere sahip olabileceği gibi bunun yanında daha sınırlı bir yetkilendirme söz konusu olabilir. Bu durum genel olarak yönetici ve diğer kullanıcıların ilgili sistem üzerindeki yetkileri olarak karşımıza çıkmaktadır. Bu yetkiler ise genel olarak iki grupta toplanabilir. Bunlardan birincisi genel olarak sisteme “log on¹⁸⁸ (oturum açma)” yetkisi diğeri ise kullanıcıların sistem içerisinde işlem yapma (kopyalama, silme vb.) yetkileri olarak karşımıza çıkmaktadır.

¹⁸⁶ Bu tür sistemler içerisinde kullanıcı ya da kullanıcı yetkilerinin yer aldığı gruplar işletim sistemi içerisinde yazılımın özelliğine bağlı olarak yöneticisinin müdahalesi olmadan yer almaktadır. Fakat bunlar üzerinde sistem yöneticisinin her türlü değişikliği yapabilmesi söz konusu olduğundan bunları yöneticinin yetkisi dahilinde görmek mümkündür. Kimi sistemlerde de kullanıcı hesabı açılması sistem yöneticisinin müdahalesi olmaksızın sistem aracılığıyla otomatik olarak gerçekleştirilebilmektedir. Bir e-posta hesabının açılması buna örnek olarak gösterilebilir.

¹⁸⁷ Yılmaz kişisel bilgisayarlarda yaygın olarak kullanılan Microsoft Windows Xp ve 2000 işletim sistemi açısından bu yetkileri kullanıcı “hakları” başlığı altında iki kategoriye ayırmaktadır. Yazara göre “log on hakları” ve yetkiler bu iki kategoriye oluşturmakta, log on hakları bilgisayara girmeye kimlerin hakkı olduğunu belirlemekte, yetkiler ise kullanıcıların neleri yapmaya yetkili olduğunu (kullanıcı ekleme/silme, sistem zamanını değiştirme vd.) belirlemektedir. **YILMAZ, Bilişim Korsanlığı**, s. 95; Unix tabanlı işletim sistemleri hakkında ayrıca bkz. s. 112 vd.

¹⁸⁸ Log on ya da log in olarak ifade edilen durum genel olarak bir bilgisayar sisteminde bir oturumun açılması işlemi ya da bu süreci ifade eden bir terimdir. Bu açıdan kişisel bilgisayarların çoğunda bu süreç oluşturulmamakta ve bilgisayarın açılmasına bağlı olarak bilgisayar kullanılmaya başlanmaktadır. Daha geniş çaplı sistemlerde ise bu süreç genel

Bu ayırım içerisinde oturum açma “log on” yetkisi, kimlerin sistemi kullanma yetkisi olduğunu göstermektedir. Bu açıdan bir sistemde kimlerin oturum açma yetkisinin olduğunu belirlenmesi kimlerin sistemde işlem yapabileceğinin tespiti anlamına gelmektedir. Bu yetki aynı zamanda diğer yetkilerin kullanılmasına ilişkin bir ön koşul olarak ortaya çıkar.

Söz konusu yetkiye sahip olan kullanıcının sistemde oturum açmasından sonraki konumu ise, sistem içerisindeki işlem yapma yetkileri gündeme getirir . Bu ise genel olarak sistem aracılığıyla ya da içerisinde var olan veri ve programlar üzerinde ya da bunlar aracılığıyla işlem yapılabilmesi yetkisi anlamına gelmektedir. Bu doğrultuda sistemde oturum açma yetkisi olan kullanıcıların sistemde hangi işlemleri yapabileceği kullanıcı hesabına ya da kullanıcı hesabının bağlı bulunduğu gruba göre sınırlandırılması mümkündür. Bu nedenle bir bilgisayar sisteminde işletim sisteminin elverdiği ölçüde değişik düzeyde işlem yapabilme yetkisine sahip olan kullanıcı hesaplarının oluşturulması mümkündür.

Yukarıda açıklanan hususlar doğrultusunda, hacking olarak da adlandırılan yetkisiz erişimde failin amacı kullanma yetkisi olmadığı bir sistem üzerinde hukuka aykırı olarak kullanma yetkisini sağlaması yani sistemde oturum açması olarak

olarak bir kullanıcı adı ve şifre aracılığıyla gerçekleştirilmektedir. Bkz., http://www.webopedia.com/TERM/l/log_on.html

Oturum açmanın kendisi de bilgisayara doğru komutların gönderilmesi sonucunda bilgisayarın buna cevap vermesi şeklinde oluşur. Kişisel bilgisayarlarda yaygın olarak bilgisayarın güç düğmesine B.ldığında yani çalıştırıldığında oturum açma süreci otomatik olarak gerçekleşmektedir. Bir e-posta sunucusunun hizmetinden yararlanılmasında olduğu gibi çok kullanıcı sistemler açısından, genel bir ifade ile erişim kodlarının (kullanıcı adı, şifre vs) girilmesi ve bunun sonucunda doğru erişim kodları olduğunun sistemde otomatik olarak kontrol edilmesi sonucunda oturum açılması şeklindedir.

özetlenebilir¹⁸⁹. Bu durum sistem içerisindeki yetkilerin elde edilmesi bakımından yönetici düzeyinde ya da kullanıcı düzeyinde erişim/hacking olarak adlandırılabilir¹⁹⁰. Bu şekliyle yetkisiz erişim, sistemi kullanmaya yetkili kullanıcılara ait erişim kodlarının (kullanıcı adı, şifre vb) ele geçirilmesi suretiyle gerçekleştirilebileceği¹⁹¹ gibi sistem açıklarından faydalanılması ya da sistemde açık yaratılması suretiyle de gerçekleştirilebilir¹⁹².

Sisteme yetkisiz erişim, başka bir bilgisayarın kullanılması suretiyle hedef bilgisayara iletişim araçları aracılığıyla erişilmesi suretiyle gerçekleştirilebileceği gibi, hedef doğrudan da gerçekleştirilebilir¹⁹³.

Yukarıda aktarılan hususlar göz önünde bulundurularak, teknik olarak oturum açma (log on) yetkisi olarak da adlandırılan ve kimlerin sistemde oturum açabileceğini belirleyen yetkinin ihlal edilerek sistemde oturum açmanın, TCK'nin

¹⁸⁹ Sistem içerisinde oturum açmanın sisteme erişim sağlama ya da madde metninde belirtildiği şekliyle sisteme girme olduğunun kabulü, port tarayıcı kullanımının başlı başına bu madde kapsamında olmadığı sonucuna götürür. Çünkü port tarayıcısının kullanılmasında sistem ile iletişim kurabilmek için sistemdeki hangi kapıların açık olduğunun saptanması amaçlanmakta bu haliyle sistemde oturum açma söz konusu olmamaktadır. Şartları varsa bu durumun teşebbüs kurumu içerisinde değerlendirilmesi mümkündür. Aksi görüş için bkz **KURT, Bilişim Suçları**, s. 156.

¹⁹⁰ Bu ayrım hakkında bkz., Eric J. **SINROD** - William P. **REILLY**, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara Computer & High. Tech. L. J. 177 (2000), s. 204 vd. Ayrıca bkz., **David L. CARTER**, **Computer Crime Categories:How Techno-Criminals Operate**, <http://www.lectlaw.com/files/cril4.htm> (kontrol 12.11.2005)

¹⁹¹ Bu ihtimalde kullanıcı ya da şifrenin ele geçirilmesi suçun gerçekleşmesi için yeterli olmamakta failin bu kodları kullanarak sistemde oturum açması gerekmektedir. İtalyan Ceza Kanununun 615-quater maddesinde bu tür erişim kodlarının yetkisiz 3. kişilerin eline geçmesinin engellenmesi amacıyla bunların yayılması ve dağıtılması. ayrı bir suç olarak düzenlenmiştir. Bkz., **FALZETTI**, s. 93 vd.

¹⁹² Aynı yönde Near Kumar **KATYAL**, *Criminal Law in Cyberspace*, 149 U. Pa. L. Rev.2000-2001, s. 1023.

Hacking teknikleri için genel olarak bkz, Wallace **WANG**, *Steal This Computer Book 3: What They Won't Tell You About the Internet*, San Francisco, 2003, s. 147 vd.

¹⁹³ Aynı yönde **DÜLGER**, s.217, **MERAN**, s. 365.

243. maddesinde belirtilen hukuka aykırı girmeyi oluşturduğunu söylemek mümkündür. Bu madde kapsamında, sisteme hukuka aykırı olarak elde edilen erişim kodlarından yararlanılması suretiyle girilmesi, sistemdeki açıklardan faydalanılarak ya da sistemde açıklar yaratılarak girilmesi arasında bir fark yoktur. Aynı şekilde sistemin tamamına ya da bir kısmına girilmesi bakımından bir farklılık yoktur.

Yukarıda sistemi kullanma ya da daha teknik bir ifade ile sistemde oturum açma yetkisi olmayan bir kişinin sisteme girmesi olasılığı incelenmiştir. Burada incelenmesi gereken diğer husus, bir genel olarak bilişim sisteminin bütününe ya da bir kısmına girmeye yetkili olan bir kişinin sisteme kendisine ait oturum açma yetkisinin ilişkilendirildiği kullanıcı hesabından başka bir hesap ile sisteme girmesi olasılığıdır.

Burada özellikle iki olasılık açısından değerlendirme yapılması gerekir. Bunlardan birincisi sistem içerisinde işlem yapma yetkisinin kapsamı diğeri ise maddede açıkça vurgulandığı üzere bilişim sistemi içerisinde sistemin belirli kısımlarına girişe ilişkin yetkilendirme olarak karşımıza çıkmaktadır.

Sistem içerisinde işlem yapma yetkisinin kapsamı¹⁹⁴ bakımından incelendiğinde sistem içerisinde işlem yapma bakımından farklı yetkilendirme söz konusu ise kural olarak sisteme girme yetkisine sahip bir kişinin başka bir kullanıcı hesabı kullanarak sisteme girmesi durumunda yetkisiz erişim gerçekleşir. Bu durumda sistem içerisinde sınırlı işlem yapma yetkisine sahip bir kullanıcının daha üst düzeyde işlem yapma yetkisine sahip bir kullanıcı hesabı aracılığıyla sisteme

¹⁹⁴ Sistem içerisinde işlem yapma yetkisi sistem içerisindeki veriler açısından değerlendirildiğinde genel olarak okuma, yazma ve çalıştırma olarak karşımıza çıkabilmektedir. İşlem yapma yetkisi bu açıdan sadece belirli bir veri bakımından sınırlandırılabilir gibi belirli bir izin ya da bölüm açısından da sınırlandırılabilir.

girmesi halinde hukuka aykırı bir girişten bahsedilir. Üst düzey işlem yapma yetkisine sahip bir kullanıcının ise alt düzeyde bir kullanıcı yetkisiyle sisteme girmesi işlem yapma yetkisi bakımından bir yetki aşımı söz konusu olmadığından kural olarak hukuka aykırılık teşkil etmeyecektir. Aynı düzeydeki kullanıcılar bakımından ise işlem yapma yetkisi bakımından bir farklılaştırma yapıp yapılmadığı sisteme girmenin hukuka aykırılığın tespitinde ölçüt teşkil eder.

Madde metni incelendiğinde sadece sistemin bütününe girişten bahsedilmemekte bunun yanında sistemin bir kısmına girilmesi hali de suç olarak öngörülmektedir. Burada belirli bir kısma girilmesinin sınırlandırılması ise yukarıda belirtildiği üzere, tek bir sistem içerisindeki yetkiler bakımından okuma, yazma ve çalıştırma yetkileri içerisinde en azından okuma yetkisinin de verilmemiş olması anlamına gelmektedir. Bu ise yukarı da belirtildiği üzere oturum açma yetkisi kapsamında düşünülebilir çünkü oturum açma yetkisi sistemde işlem yapma yetkisinin önkoşuludur. Sistem içerisindeki kısım ve bu kapsamda düşünülebilecek veri bakımından işlem yapma yetkilerinin kullanımı konusunda bunlar üzerinde en azından okuma yetkisinin bulunması şarttır.

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.

Burada önemli olan husus, sistemdeki kullanıcıların sistem içerisinde yetkilerinin belirli bir bölüm, veri bakımından sınırlandırılıp sınırlandırılmadığıdır.

Bu doğrultuda, sistemde oturum açmaya yetkisi olan bir kişinin aynı sistemde daha geniş işlem yapma yetkisine sahip bir kullanıcı olarak oturum açması, sistemde oturum açma yetkisine sahip olan bir kullanıcının aynı düzeyde yetkilere sahip diğer bir kullanıcının hesabıyla sistemde oturum açması ve son olarak üst düzey işlem yapma yetkisine sahip olan bir kişinin sınırlı işlem yetkisine sahip kullanıcılara ait bölümlere, verilere erişmesi olasılıkları incelenmelidir.

Birinci olasılık, özellikle çok kullanıcıli sistemlerde söz konusu olabilir. Bu tür sistemlerde yukarıda belirtildiği üzere en az bir tane yönetici yetkilerine sahip kullanıcı ve bunun yanında, sistemin teknik olarak elverdiği ölçüde kullanıcılar bulunabilmektedir. Burada tartışılması gereken husus, sınırlı yetkiye sahip olan bir kullanıcının yani sınırlı yetki ile oturum açma yetkisine sahip olan bir kullanıcının sistemde yönetici yetkilerine sahip olacak şekilde oturum açmasıdır.

Eğer sistem içerisinde sınırlı kullanıcılar için bölüm ya da verilere erişim bakımından bir sınırlandırma söz konusu ise, bu durumda sisteme girmeye yetkili kullanıcının, kendisine ait olmayan ve daha geniş yetkilere sahip bir kullanıcı hesabı aracılığıyla girmesi durumunda hukuka aykırı girmenin var olduğu söylenebilir. İkinci olasılıkta ise, sisteme girmeye yetkili bir kullanıcının aynı düzeyde yetkiye sahip başka bir kullanıcı hesabıyla sisteme girmesi söz konusudur ve bu olasılık da genelde çok kullanıcıli sistemler bakımından ortaya çıkar. Burada da ölçüt kullanıcılar arasında bölüm ve verilere erişim bakımından herhangi bir fark yaratılıp yaratılmadığıdır. Farklı kullanıcılar bakımından sisteme girilmesine ilişkin bölüm veya veri bakımından farklılık söz konusu ise bu durumda 243. madde kapsamında sisteme girmenin hukuka aykırılığından bahsedilebilecektir.

Son olasılığın ise özellikle sistem yöneticisinin sistem içerisindeki konumu açısından değerlendirilmesi gerekir. Sistem yöneticisi teknik olarak sistem içerisinde her dizin, klasör ya da veriye erişebilir ve sistemin teknik olarak elverdiği ölçüde her türlü işlemi yapabilir. Sistem yöneticisinin sistem içerisinde her türlü işlemi yapmaya yetkisinin olması ve bu yetkinin genel olarak sınırlı kullanıcılar tarafından sınırlandırılmaması kuraldır. Buna rağmen sınırlı kullanıcı tarafından sistem içerisinde üçüncü kişilerin girmesine kısıtlanmış bir bölüm, veri bulunması halinde, bunlara erişim ister sınırlı kullanıcı ister yönetici tarafından gerçekleştirilmiş olsun bu madde kapsamında hukuka aykırı girmeden bahsetmek mümkündür.

Bu olasılıklar göz önünde tutularak bir bilişim sistemi içerisinde yetkili kullanıcının kendisinin girmesi sınırlandırılmış olan bir bölüme girmesi, veriye erişmesi, maddede özellikle bilişim sisteminin bütünü ve bir kısmına girme şeklinde ayırım karşında hukuka aykırı girme kapsamında olduğu söylenebilir.

Bunun dışında başkasına ait herhangi bir kullanıcı hesabını kullanmadan sistem açıklarında yararlanılması gibi diğer yollarla sistem içerisinde girişin sınırlandırılmış olduğu bir bölüme girilmesi, yetkisiz erişimi oluşturur¹⁹⁵.

. 243. maddede düzenlenen suçun gerçekleşmesi için sadece sistemin bütününe ya da bir kısmına hukuka aykırı olarak girme yeterli olmamakta, sistemde kalınmaya devam edilmesi de gerekmektedir. Sisteme girme ve orada kalmaya devam etme, bir bütün olarak, 243. maddede düzenlenen yetkisiz erişim suçunun maddi unsurunu oluşturmaktadır.

¹⁹⁵ Bilişim ya da telematik sistemlerinin bütünü ya da bir kısmına girme şeklinde bir ayırım yapılmayan İtalyan Ceza Kanunun 615-ter maddesinin de bu gibi durumlarda uygulanabileceği, ifade edilmiştir. Bkz, **FALZETTI**, s. 90 .

Başta da belirtildiği üzere, suçun maddi unsurunun bu şekilde düzenlenmesi, suçun niteliğini de değiştirmiştir. Maddede yer alan suçun unsuru olarak “*girme ve orada kalmaya devam etme*”ye verilecek anlama göre, söz konusu suçun niteliği hakkında iki farklı düşüncenin ileri sürülmesi mümkündür. Özellikle “*kalmaya devam eden*” ifadesinin anlam ve kapsamı burada önemlidir.

Girme ve orada kalmaya devam etmenin birbirinden bağımsız iki farklı hareketi oluşturduğunun kabulü halinde, Kanunun 243. maddesinde düzenlenen yetkisiz erişim suçunun birden fazla hareketi gerektiren bir suç olduğu sonucuna varılır¹⁹⁶. Birden fazla hareketi gerektiren suçlarda olduğu şekliyle, bu maddede sadece sisteme girme yeterli olmamakta, sistemde kalmaya devam edilmesi suçun gerçekleştirilmesi için zorunlu olmaktadır. Bu durumda sisteme girme, yukarıda ifade edildiği şekliyle, sistemde oturum açmayı, sistemde kalmaya devam etme ise, sistemden çıkmama anlamına gelmektedir. Bu yaklaşımla sisteme girme icrai, sistemde kalmaya devam etme ihmali hareketi oluşturur.

Girme ve orada kalmaya devam etmenin birbirinden bağımsız iki farklı hareketi oluşturmadığının kabul edilmesi halinde ise, maddede düzenlenen suçun zorunlu mütemadi (kesintisiz) suç olduğu sonucuna varılır. Bu durumda sisteme girme sonrasında, sistemde kalmaya devam edilmesi şartı, suçun tamamlanmış sayılabilmesinin belirli bir sürenin aranması amacına hizmet eder. Sisteme girmenin aynı zamanda sistemde kalmaya başlanması anlamına geldiğinin ve kalmaya devam etmenin, kalmanın belirli süre devam etmesine yönelik olarak maddede yer aldığının

¹⁹⁶ Birden fazla hareketi gerektiren suçlar hakkında bkz., ÖNDER, **Ceza Hukuku Genel Hükümler**, s. 59 – 60.

kabulü¹⁹⁷, bu suçta temadının arandığı sonucuna götürür. Bu durumda maddede yer alan hüküm, mütemadi suça işaret eder.

Söz konusu suçun bu şekilde kaleme alınışından çeşitli sonuçlar ortaya çıkmaktadır. Bu doğrultuda sisteme hukuka uygun bir şekilde girilmesi sonrasında rızanın ortadan kalkması ya da diğer nedenlerle hukuka aykırılığın gerçekleşmesi durumunda failin sistemde kalmaya devam etmesi, girişin hukuka aykırı olması şartı arandığından, 243. madde kapsamında değildir¹⁹⁸. Bu husus 243. maddede düzenlenen suçun niteliği hakkında yukarı aktarılan her iki düşünce bakımından da geçerlidir.

Diğer bir husus yetkisiz erişim suçuna teşebbüs ile ilgilidir. Bu hususla ilgili olarak *Kurt*, Tasarıda iki ayrı hareketi kapsayan bir suç olarak düzenlenmek istenen yetkisiz erişim suçuna ilişkin olarak değişiklik gerekçesindeki yaklaşımla aynı yönde, “*Sistemde kalmaya devam etmek’ tanımlamasının suçun tamamlayıcı unsuru haline getirilmesi, kötü niyeti olmayıp da kısa süreliğine giriş yapan, araştırma amacı taşıyan, ya da yazdığı yazılımın başarısını test etmek isteyen kişilerin*

¹⁹⁷ *Karagülmez*, madde metninde yer alan “*orada kalmaya devam eden*” ifadesinin “*kalan*” ifadesinden daha geniş bir anlamı çağrıştırdığını ifade etmekte, “*kalmaya devam etme*”nin, “*kalma*” ya göre daha nitelikli olduğunu ve daha uzun süren bir temadiyi gündeme getirdiğini belirtmiş ve sonrasında kalmaya devam etme unsuru için yeterli süre araştırmasının her somut olayın özelliğine göre belirlenmesi gerektiğini savunmaktadır. **KARAGÜLMEZ**, s. 170.

Kurt ise, sisteme girdikten sonra orada kalmaya devam etmenin sisteme giren failin sistem içerisinde bir süre kalması (bu arada sistem içerisindeki verileri kontrol edebilir, veri akışını izleyebilir, veriler üzerinde oynama yapabilir veya sistemi bozmaya yönelik işlemler yapabilir, yahut da hiçbir şey yapmayabilir) şeklinde gerçekleşebileceğini belirtmiştir, **KURT**, s. 149.

Meran ise, bilişim sistemine girilip kalmaya devam edilmezse suçun oluşmayacağını belirtmekte ve burada hemen çıkmadan anlaşılması gerekenin olanaklı en kısa zaman olduğunu belirtmektedir. **MERAN**, s. 365

¹⁹⁸ Aksi yönde Engin **AKIN**, *Bilişim Suçu*, Yaklaşım, Yıl 14, Sayı 157, Ocak 2006, s. 268

yaptıkları sisteme girme eylemlerini de çok katı bir düzenleme ile münhasıran suç saymama düşüncesinden kaynaklanmaktadır.” görüşünü dile getirmiştir. Devamında, “Ancak, yine de bu düşüncelerle olsa dahi sadece sisteme girmeleri suça teşebbüs olarak değerlendirilecektir, Kanunun bu tarzda bu tür eylemleri aynı kefeye koymaması isabetli olmuştur.” demektedir¹⁹⁹.

Kurt tarafından, sistemde kalmaya devam etme niyeti olmayan, sadece sisteme girme niyeti olan bir kişinin yani sadece sisteme girme kastıyla hareket eden failin yetkisiz erişim suçuna teşebbüsten cezalandırabilmesinin mümkün oluşu görüşü, suçun niteliği ile ilgili yaklaşımlar açısından da değerlendirilmesi gerekir.

244. maddede düzenlenen suçun niteliğinin tespiti, teşebbüse elverişli olup olmadığının kabulü bakımından da önemlidir. Yukarıda ifade edildiği üzere, suçun birden fazla hareketli suç olarak kabulü halinde sadece girme, kalma devam etme hareketi de zorunlu olarak arandığından bu suça teşebbüs olarak kabul edilemez. Nitekim fazla hareketli suçlarda ilk hareketin yapılmış olması, ikinci hareket yapılmadıkça suça teşebbüs olarak kabul edilemez²⁰⁰. Sistemde kalmaya devam etme ise parçalara bölünemediğinden bu görüşün sonucu olarak yetkisiz erişim suçu teşebbüse müsait olmamaktadır.

Aynı şekilde, mütemadi suç olduğunun kabul edilmesi halinde de kastın, suçun unsuru olarak ortaya çıkan kalmaya devam etmeyi yani belirli bir süreyi de kapsamaması gerektiğinden teşebbüsten bahsedilemeyecektir. Buna karşın 244. maddenin 3 Söz konusu suçun mütemadi suç olarak kabul edilmesi halinde söz konusu suçun tamamlanma anından önce 765 Sayılı TCK'deki ifadesiyle eksik teşebbüse müsait olduğu sonucuna varılır. Bu husus, mütemadi suçun, ihlal edici durumun oluşturulduğu an değil söz konusu durumun bu

¹⁹⁹

KURT, s. 148.

²⁰⁰

ÖNDER, Genel Hükümler, s. 60

suçun varlığı için gerekli olduğu ölçüde devam ettirilmesi anında tamamlanmış olması özelliğine dayanmaktadır²⁰¹.

d. Suça Etki Eden Nedenler

Yetkisiz erişim suçunun düzenlendiği 243. maddenin 2. fıkrasında, fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, cezada indirim sebebi olarak öngörülmüş bunun yanında son fıkrada sistemin içerdiği verilerin değişmesi ve de yok olması hali ise ağırlatıcı neden olarak düzenlenmiştir.

i. Yetkisiz Erişim Suçunun Bedeli Karşılığı Yararlanılabilen Sistemler Hakkında İşlenmesi

Maddenin ikinci fıkrasında düzenlenen bedeli karşılığı yararlanabilen sistemlerin ne olduğu ve neden bu şekilde bir cezada indirim sebebinin öngörüldüğü hakkında herhangi bir gerekçeye yer verilmemiştir.

Dülger, bedeli karşılığı yararlanılabilen sistem ifadesinin genel olarak dört durumu kapsadığını ifade etmiştir. Yazara göre İnternet üzerinden ücret karşılığı hizmet veren web siteleri, “*internet kafe*” gibi yerlerde olduğu üzere belirli bir bedel karşılığı bilişim sisteminin kiralanması, bir kuruluş tarafından belli bir sistemin bedel karşılığında sunulması (örneğin sağlanan anlaşmayla kişilerin cep telefonlarına bilişim sistemi üzerinden reklam amaçlı mesaj çekilmesi) ve de belirli bir zaman ya da dönem sınırlaması ile İnternet bağlantı servisinin sağlanması bedeli karşılığı yararlanılabilen sistem kapsamındadır²⁰².

²⁰¹ TOROSLU, *Ceza Hukuku Genel Kısım*, s. 251.

²⁰² DÜLGER, s. 226-227; aynı yönde MERAN, s. 366.

Karag lmez ise maddede yer alan bu ifadenin yoruma a ık olduėunu ifade etmekte ve devamında belirli bir  cret karřılıėında hizmet veren web sayfalarının bu kapsamda d ř n lebileceėini belirtmektedir. Yazar, internet kafe ve benzeri yerlerde bedeli karřılıėında sistemin kullanılmasının bu kapsamda d ř n lemeyeceėini ifade ederek maddede sistemin kullanıldıėı mekanın deėil sistem i erisindeki elektronik yapıda sunulan  cretli hizmetleri vurguladıėını savunmaktadır. Yazara g re, belirli bir s re İnternet baėlantı servisinin saėlanması da bu fıkra kapsamında deėildir²⁰³.

Yazıcıoėlu ise, bu fıkrada d zenlenen hafifletici sebebi,  creti karřılıėı hizmet veren sistemlere girilmesi řeklinde yorumlamakta ve devamında ve bu d zenlemenin yetkisiz eriřim su unun uygulanmasının geniřliėinden doėacak sakıncaları gidermesi bakımından isabetli olduėunu ifade etmektedir²⁰⁴.

Bedeli karřılıėı yararlanılabilen sistemler ifadesi geniř bir anlama sahip olup belirgin olmaktan uzaktır. Bu a ıdan h k m geniř yorumlanarak *D lger*'in ifade ettiėi durumları kapsayacaėı gibi aynı řekilde dar yorumlanarak sadece biliřim sisteminin bir hizmetin sunumunda kullanılması durumunu kapsayacak řekilde dar da yorumlanabilir. Bu a ıdan fıkranın tekrar d zenlenmesi ve belirgin hale getirilmesi gerekmektedir.

Yetkisiz eriřim su unun T rk Ceza Kanununda sistem ve veriye m dahale kapsamında mala zarar verme fiillerine y nelik bir d zenleme olduėu bu fiillerin

²⁰³ **KARAG LMEZ**, s. 174-175.

²⁰⁴ Yılmaz **YAZICIOėLU**, *Yeni T rk Ceza Kanunundaki Biliřim Su larının Genel Deėerlendirilmesi*, Yeditepe Hukuk Fak ltesi Dergisi, C. 2, S. 2., 2005, s. 407.

gerçekleştirilmesi tehlikesinin esas alındığı göz önünde tutulacak olursa bu durumda bu tür bir ayırma gidilmesinin de belirli bir anlam ifade etmediği söylenebilir.

Her ne kadar gerekçede bu yönde bir açıklamaya yer verilmemiş olmasına rağmen, ikinci fıkra da öngörülen durumun bir indirim sebebi olarak düzenlenmesi, hükmün özellikle ücret karşılığı hizmet veren bir sisteme girilmesi hallerini kapsadığının kabul edilmesi durumunda, burada TCK'nin 163. maddesinin 1. fıkrasında düzenlenen otomatların kötüye kullanılması suçuna öngörülen ceza ile paralellik kurmak için bu tür bir indirim sebebine yer verildiği sonucuna varılabilir. 163. maddenin birinci fıkrasında düzenlenen suçun cezası iki aydan altı aya kadar hapis cezası olup 243. maddenin 2. fıkrasında ise bir yıla kadar hapis veya adli para cezası öngörülen yetkisiz erişim suçunun cezasının yarı oranına kadar indirileceği belirtilmiştir.

Nitekim bu hususa ilişkin TCK'nin 163. maddesinin 1. fıkrasında düzenlenen suçun bu tür sistemlerden bedelsiz yararlanmayı düzenlediği burada ise bu sistemlere sadece girme ve kalmanın düzenlendiği ifade edilmiştir²⁰⁵. Dülger ise burada “otomat”ların kastedilmediği, otomatlar aracılığıyla sunulan ve bedeli ödendiği takdirde hizmetten bedeli ödenmeden yararlanılmasının 163. maddede düzenlendiğini ifade etmiştir²⁰⁶.

²⁰⁵ Süheyl **DONAY** – Mahmut **KAŞIKCI**, En Son Değişikliklerle Açıklamalı ve Karşılaştırmalı Türk Ceza Kanunu, 1. B., İstanbul, 2005, s. 329.

²⁰⁶ **DÜLGER**, s. 226. Aynı yönde **KARAGÜLMEZ**, s. 173-174.

ii. Yetkisiz Eriřim Fiili Sonucunda Sistem İerisindeki Verinin Deęiřmesi ya da Yok Olması

244. maddenin son fıkrasında sisteme yetkisiz eriřim sonucunda sistem ierisindeki verinin deęiřmesi veya yok olması aęırlatıcı neden olarak dzenlenmiřtir. Bu fıkrada, TCK'nin 23. maddesinde dzenlendięi řekliyle, neticesi sebebiyle aęırlařan bir su sz konusu olup aęırlatıcı nedenin uygulanabilmesi iin failde verinin deęiřtirilmesi ya da yok edilmesi ynnde bir kastının olmaması gerekmektedir²⁰⁷. Bunun kasıtlı olarak iřlenmesi halinde 244. maddenin 2. fıkrasında yer alan hkm gndeme gelecektir²⁰⁸.

Biliřim sistemlerinde yer alan ve bunların iřleyiřini saęlayan ana yazılımlar olarak karřımıza ıkan iřletim sistemleri aısından deęerlendirildięinde, genellikle bu iřletim sistemlerinin her aılıřında ya da bu sistemlere girilmesinde gnlk kayıtları ieren veriler gibi birok veri sistemin iřleyiřine baęlı olarak deęiřebilmektedir. Bu tr deęiřiklikler sistemin olaęan alıřması iin zorunlu ya da iřlevsel olup bunlardaki deęiřiklik bu fıkra kapsamına girmemektedir.

Son fıkrada ngrlen aęırlatıcı nedenlerin uygulanması aısından birinci ya da ikinci fıkrada dzenlenen sistemler bakımından maddede zellikle cezanın miktarı bakımından bir fark yaratılmamıřtır. Fıkrada belirtilen durumun gerekleřmesi halinde verilecek ceza, yetkisiz eriřimin konusunun bedeli karřılıęı sistemler olup olmamasına bakılmaksızın altı aydan iki yıla kadar hapis cezasıdır.

²⁰⁷ YAZICIOęLU, *Biliřim Sularının Genel Deęerlendirilmesi*, s. 407-408.

²⁰⁸ Aynı ynde KARAGLMEZ, s. 177

IV. BİLİŞİM SİSTEMİNE VE VERİYE MÜDAHALE

A. Genel Olarak

Sosyo-ekonomik yapı içerisinde faaliyetlerin ağırlıklı olarak bilgisayar sistemleri aracılığıyla veri işleme şeklinde gerçekleştirilmeye başlanması ve bunun yoğunluğundaki artış, verinin gizliliğine ve içeriğine ilişkin koruma yanında verinin bütünlüğünün ve erişilebilirliğinin de korunmasını gündeme getirmiştir.

Verinin işlenmesi faaliyeti bilgisayar ortamında genel olarak bir veri grubunu oluşturan ve sistemin nasıl çalışması gerektiğine ve sistem içerisindeki verinin işlenmesine ilişkin komutları içeren programlar aracılığıyla gerçekleştirilebilmektedir. Programın kendisi genel olarak verinin düzenli ve öngörülen şekilde işlenmesini sağlayan bir veri grubunu oluşturmaktadır. Veri işleme süreci içerisinde merkezi bir işleve sahip programlara müdahale edilmesi ise her zaman için sistemin tamamen zarar görmesine yol açmamakla birlikte, veri işleme faaliyetinde aksamalara neden olabilmektedir. Bu açıdan veri işleme faaliyeti içerisinde bunların da müdahalelerden korunması önem arz etmektedir.

Verinin işlenmesi faaliyetinin ana unsurunu oluşturan bilgisayar sistemlerinin işleyişinin ve bütünlüğünün korunmasının önemi de bu sistemlerin kullanımının yaygınlaşması ve faaliyetlerin bilişim sistemlerine bağlı olarak yapılmasına paralel bir şekilde artmaktadır²⁰⁹. Günlük hayatın her alanında yer edinmesine ve birçok kritik ve önemli faaliyetlerin yerine getirilmesinde kullanılmasına bağlı olarak bu tür sistemlere saldırı da her geçen gün yaygınlaşmaktadır.

²⁰⁹

HEYMANN, s. 378

Günümüzde bilgisayar sistemlerinin işleyişine, veri ve programlara müdahale genel olarak bunlara doğrudan erişim yoluyla gerçekleştirilebileceği gibi bu amacı güden kötü amaçlı programların kullanılması da yaygın bir yöntemdir. Virüs²¹⁰, solucan²¹¹, mantık bombaları²¹², DOS saldırıları²¹³, Truva atı²¹⁴ yöntemleri günümüzde yaygın olarak kullanılan yöntemlere örnek gösterilebilir.

Bu tür bir müdahale olanağı, aynı zamanda çeşitli avantajları da beraberinde getirmiştir. Veri ve programlar esas alınarak yapılan müdahalenin fiziksel bir müdahaleye göre avantajlı yönleri müdahalenin konusu ile müdahale edenin aynı mekânda olması zorunluluğunun ortadan kalkmasıdır²¹⁵. Farklı mekânlarda olma ise

²¹⁰ Bilgisayar virüsü çalıştığı bilgisayara ve veriye çeşitli şekillerde zarar verebilen bir program ya da kötü amaçlı kod olarak tanımlanabilmektedir. Bu programlar (ya da kodlar) herhangi bir şekilde çalıştırılırsa, programlanma şekline göre bilgisayarınıza zarar vermeye başlar. Ayrıca, tüm virüs kodları (bilinen adıyla virüsler) bir sistemde aktif hale geçirildikten sonra çoğalma (bilgisayardaki diğer dosyalara yayılma, ağ üzerinden diğer bilgisayarlara bulaşma vb.) özelliğine sahiptir. Bkz., **PARKER**, s. 82 vd.

²¹¹ Solucan ise bilgisayar ağ ve sistemlerinde kendi kendini kopyalayarak çoğalabilen ve bilgisayar ve bilgisayar verilerine zarar verebilen program ya da kodlara verilen genel addır. Bu haliyle virüsün bir alt kategorisi olarak tanımlanabilmekle birlikte virüsten farklı olarak, bilgisayar kullanıcısının herhangi bir hareketi olmadan kendi kendini kopyalayabilmesi ve çoğalabilmesi sonucunda solucan adı verilmiştir. Bkz., *The Difference Between a Virus, Worm and Trojan Horse*

<http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>

²¹² Mantık bombası belirli gün ve saat gibi belirli koşullar oluştuğunda, genel olarak bilgisayar veri ve programlarına çeşitli şekillerde zarar vermek üzere kendiliğinden çalışabilen program ya da kötü amaçlı kod olarak tanımlanmaktadır. Bkz., **PARKER, Fighting Computer Crime**, s. 90. , Ayrıca bkz.,

http://www.webopedia.com/TERM/I/logic_bomb.html

²¹³ İngilizce “*denial of service*” teriminin kısaltması olan “*DOS*” saldırılarında sistemin işleyemez hale gelmesi ya da sisteme erişimin engellenmesini amaçlayan hareketlere verilen genel bir ad olarak tanımlanması mümkündür. **YILMAZ**, s. 319 vd.

²¹⁴ Truva atı ise adını Truva efsanesinden almış olup genel olarak başka bir programın içine yerleştirilmiş olan kötü amaçlı kod ya da program olarak tanımlanabilmektedir. Bu haliyle bilgisayar program ve verilerine zarar verme gibi bir çok amaçla kullanılabilir. **PARKER**, s. 89,

²¹⁵ **HEYMANN**, . 377; Michael **SUSSMANN**, *The Critical Challenges From International High-Tech and Computer-Related Crime*, 9 DukeJ. Comp. & Int’l (1998-1999) s. 451.

öncelikli olarak müdahale edenin yakalanma olasılığını azaltmaktadır. Bunun yanında bu tür bir müdahale fiziksel mekânın getirdiği sınırlamaları ortadan kaldırmakta ve bilgisayarlar aracılığıyla verilebilecek zararın miktarı fiziksel sınırlardan çok, ağın hızı ve failin amaçlarıyla sınırlı hale gelmektedir.²¹⁶ Özellikle İnternet de dâhil olmak üzere bilgisayar ağlarının gelişimi bu tür faaliyetlerin gerçekleştirilmesinde çok büyük olanaklar sağlamaktadır,

Yukarıda aktarılan bu hususlar sonucu, veri ve programlara ve ayrıca bilgisayar sistemlerinin işleyişine müdahalenin engellenmesi zorunluluğu ortaya çıkmış ve bunlara yönelik müdahaleler ceza mevzuatlarında düzenlenmeye başlanmıştır. Bu düzenlemelerde yeni ve önemli olan nokta, müdahalenin konusunun fiziki varlığı olmayan veri, program ya da genel olarak bilişim sistemlerinin yazılım unsuru olması ve sisteme yönelik müdahalelerin yazılım unsuruna yönelik olarak gerçekleştirilmesidir.

Nitekim Sibersuç Sözleşmesinde bu sorundan yola çıkılarak ve veri ve programa müdahale esas alınarak, veriye²¹⁷ müdahale 4. maddede, sisteme müdahale ise 5. maddede düzenlenmiştir. Sözleşmenin 4. maddesine göre veriye müdahale, bilgisayar verilerinin haksız bir şekilde kasten tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilmez kılınmasıdır. “Bilgisayar sistemlerine müdahale” ise Sözleşmenin 5. maddesinde bilgisayar verisi girişi yapmak, bilgisayar verisi göndermek, bilgisayar verilerini tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak suretiyle bilgisayar sistemlerinin işleyişini ciddi bir şekilde haksız ve kasten engellemek olarak tanımlanmıştır.

²¹⁶ **CHARNEY**, s. 940

²¹⁷ Sibersuç Sözleşmesinin 1. maddesinde bilgisayar verisi, bilgisayar programlarını kapsar bir şekilde tanımlanmıştır.

Sözleşmenin 4. maddesinde düzenlenmiş olan veriye müdahale fiilinin gerçekleşebilmesi bakımından verinin bilgisayar sistemi içerisinde veya herhangi bir veri taşıyıcısında bulunması arasında fark yaratılmamıştır²¹⁸. Sisteme müdahalede ise bilgisayar sisteminin fiziki bir zarar görmesi aranmamış işleyişinin ciddi bir şekilde engellenmesi esas alınmıştır. Sisteme müdahalede genel olarak sistemdeki verilere müdahale edilmesi ya da sisteme veri gönderilmesi suretiyle müdahale esas alınmış ve bu haliyle bilişim sisteminin fiziki varlığını oluşturan donanımına yönelik fiziksel müdahale kapsam dışı bırakılmıştır.

Bilgisayar sistemlerinin yaygın olarak kullanılması ile birlikte yukarıda aktarılan şekliyle veri ve bilgisayar sistemlerine yönelik müdahaleler, Sibersuç Sözleşmesinin hazırlanmasından önce de birçok ülkenin ceza mevzuatlarında düzenlenmiştir. Bu konuda ortaya çıkan ilk düzenleme, ABD’de Federal Kanunun 1030(a)(5)(A) maddesinde üç grup halinde düzenlenen bilgisayar sistemine ve veriye müdahale suçu yer almaktadır. Bu maddede bilgisayara müdahale kapsamında 3 farklı fiil düzenlenmiştir. Bu fiiller, bilgisayara program, enformasyon, kod ya da komut iletilmesi suretiyle hedef bilgisayara kasıtlı olarak zarar verilmesi, bilgisayara yetkisiz olarak erişilmesi sonucunda taksirli bir şekilde zarar verilmesi ve son olarak bilgisayara yetkisiz olarak erişilmesi sonucunda kusursuz olarak zarar verilmesidir²¹⁹.

²¹⁸ Bkz., Explanatory Report, parag, 60, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>. Sözleşmenin 4. maddesinin ikinci fıkrasında taraf devletlerin bu suçun oluşabilmesi için ciddi bir zararın varlığı şartını koyabilecekleri ifade edilmiştir. Carr bu hükümden yola çıkarak taraf devletlerin çoğunun zararı ekonomik açıdan para ve zaman kaybı olarak tanımlayabildiklerini ifade etmiş ve bu maddenin de yetkisiz erişim de olduğu şekliyle ekonomik çıkarın gözetildiğini bu açıdan bireyin korunmasının ikinci plana itildiğini ifade etmiştir., **CARR**, s. 85.

²¹⁹ John M. **CONLEY** – Robert M. **BRYAN**, *A Survey of Computer Crime Legislation in the United States*, Information & Communication Technology Law, Vol. 8, No. 1, s. 38;

Alman Ceza Kanununda ise veri ve bilgisayara müdahale filleri malvarlığı aleyhine işlenen suçlar bölümünde düzenlenmiştir. Adı geçen Kanunun 303. maddesinde mala zarar verme suçu düzenlenirken, 303a maddesinde “*verinin değiştirilmesi*” suçu, 303b maddesinde ise “*bilgisayar sabotajı suçu*” düzenlenmiştir. 303a maddesinde verinin hukuka aykırı olarak silinmesi, erişilmez kılınması, kullanılmaz hale getirilmesi veya değiştirilmesi cezalandırılmaktadır. 303b maddede belirtilen nitelikteki veri işleme sürecine 303a maddesinde belirtilen şekilde müdahale edilmesi veya veri işleme sisteminin veya veri taşıyıcısının tahrip edilmesi, zarar verilmesi kullanılmaz hale getirilmesi, çıkarılması ya da değiştirilmesi cezalandırılmaktadır.

İtalyan Ceza Kanununda ise Alman Ceza Kanunuyla aynı yönde veri ve bilgisayar sistemlerine müdahale malvarlığı aleyhine suçlar bölümünde mala zarar verme suçundan sonra gelmek üzere 635bis maddesinde düzenlenmiştir. 635bis maddesinde genel olarak başkasına ait enformatik ya da telematik sistemlerinin²²⁰, programlarının, enformasyon ya da verilerin tahrip edilmesi, bozulması tamamen

Scott **CHARNEY** – Kent **ALEXANDER**, *Computer Crime*, 45 Emory L.J. (1996), s. 952; *The Computer Crime and Intellectual Property Section United States Department Of Justice, The National Information Infrastructure Protection Act of 1996, (legislative analysis)*, http://www.usdoj.gov/criminal/cybercrime/1030_anal.html (kontrol tarihi 02.08.2005); Sheri A. **DILLON** – Douglas E. **GRONE** – Todd **HAYWARD**, *Computer Crimes*, American Criminal Law Review, Vol. 34, 1997, s. 414- 415

²²⁰ İtalyan Ceza Kanununda bilgisayar terimi yerine enformatik ve telematik sistemler terimi kullanılmıştır. “Enformatik terimi enformasyon kelimesinin otomatik kelimesiyle birleşmesinden ortaya çıkmaktadır. Bu haliyle elektronik hesaplama makineleri yardımıyla enformasyonun otomatik olarak temsil edilmesi, iletilmesi, dönüştürülmesi ve hesaplanmasını ifade etmektedir. Enformatik araçlarının iletişim kuracak şekilde birbirne bağlanması ise telematik terimini ortaya çıkarmaktadır. Her iki terimin bir araya gelmesi ise ‘telekomünikasyon ve enformatik’ terimini ortaya çıkarmaktadır.” Bkz **RESTA**, s. 7.

veya kısmen kullanılmaz hale getirilmesi daha ağır bir ceza gerektiren suç oluşturulmaması halinde cezalandırılmaktadır²²¹.

Fransız Ceza Kanununda da, son haliyle, veri ve bilgisayar sistemine müdahale malvarlığı aleyhine suçlar bölümünde yer almaktadır. Kanunun 323–2. maddesinde otomatik veri işleme sisteminin işleyişinin engellenmesi veya işleyişine müdahale edilmesi, 323–3. maddesinde ise hileli bir şekilde otomatik veri işleme sistemine veri sokulması veya hileli bir şekilde sistemin içerdiği verilerin erişilmez kılınması ve değiştirilmesi cezalandırılmaktadır²²².

B. Türk Ceza Kanununda Bilişim Sistemi ve Veriye Müdahale

1. Genel Olarak

Türkiye’de ise, bilişim sistemi ve veriye müdahaleye yönelik ilk düzenleme 1991 yılında 3756 sayılı Kanunla TCK’ye eklenen 525/b maddesinin 1. fıkrasıdır. Sz konusu maddeye göre, “*Başkasına zarar vermek veya kendisine veya başkasına zarar yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir.*”, Bu düzenleme genel olarak

²²¹ Bkz., Giancarlo Taddei **ELMI, The Law on Computer Crime in Italy, Information & Communications Technology, Oct97, Vol. 6, Issue 3. (EBSCOHOST)**

²²² Kanunun İngilizce çevirisi için bkz, http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm

“bilgisayar ve içeriğini tahrip²²³”, “bilgisayar ortamına karşı müdahale fiilleri²²⁴”, “bilgisayar programlarına zarar verme²²⁵”, “bilgisayar sistemlerine yönelik “nası ızrar suçu²²⁶” başlıkları altında incelenmiştir.

525/b 1. fıkrasında yer alan düzenleme ile ilgili olarak *Dönmezer* şu görüşü dile getirmiştir: “*Bilgisayarın dokunulmaz olması gereği ve sistemin uygun şekilde işlev görmesi ve içeriğinin aynı suretle hizmet görmesidir. Böylece aslında başta malikin veya sistemi kullananın yararı korunmaktadır*²²⁷.” *Yazıcıoğlu* da bu suç ile kişilerin sistem ve içerisindeki unsurlar bakımından sahip oldukları mülkiyet hakkının koruma altına alındığı görüşündedir²²⁸. *Önder* suçun koruduğu yararın tartışmalı olduğunu bazı yazarların bu suç tipi ile bilgisayarda mevcut veriler ile ilgili olan kişinin yararının korunduğunu, bazı yazarların ise mevcut verilerin ülke ekonomisinde ve idarede gerçekleştirildiği fonksiyon gereği, bu suçun ekonomik yaşama karşı işlenmiş bir suç olduğunu ifade ettiklerini ifade etmiştir²²⁹. *Ersoy* ise, bu suç ile kişinin malvarlığının korunduğunu belirtmiştir²³⁰.

Suçun maddi unsuru, sistemin, verilerin ya da diğer herhangi bir unsurun kısmen ya da tamamen tahrip edilmesi, değiştirilmesi ya da silinmesi; sistemin işlemesine engel olan ya da yanlış bir biçimde işlemesini sağlama şeklindeydi. Bu suç tipi ile ilgili olarak maddede belirtilen hareketlerin bilgisayar sistemlerinin hem

²²³ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 622.

²²⁴ **ERSOY**, s. 177.

²²⁵ **ÖNDER**, s. 508.

²²⁶ **YAZICIOĞLU, Bilgisayar Suçları**, s. 259,

²²⁷ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 622

²²⁸ **YAZICIOĞLU, Bilgisayar Suçları**, s. 260.

²²⁹ **ÖNDER**, s. 508.

²³⁰ **ERSOY**, s. 166 – 167.

yazılım hem de donanımına yönelik fiilleri kapsadığı ileri sürülmüştür²³¹. Buna karşın *Ersoy*, 1. fıkra sistemin fiziksel kısmına yönelik fiillerin cezalandırılma kapsamına girmesinin düşünülmediği, sadece elektro-manyetik ortamına yönelik fiiller cezalandırılmak istendiğini belirtmiştir²³². Yazar, “*tahrip*”in bilgisayarın elektro-manyetik ortamına yöneldiği ölçüde bu suçun kapsamına girebileceğini belirtmiştir²³³. Aynı yönde *Önder* de bu fıkra hükmü ile genel olarak, bilgisayar program ve verilerine yani yazılım yönüne yönelik fiillerin cezalandırıldığını belirtmiştir²³⁴.

525/b 1. fıkrasında bu suçun “*başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla*”, yani manevi unsur bakımından suçun özel kast ile işlenebileceği öngörülmekteydi²³⁵. *Önder*, bu suç tipinin klasik mala zarar verme suçunu oluşturduğunu, “*başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak*” amacıyla bu suçun işlenmesinin anlamının açıklanmasının da zor olduğunu belirtmiştir. Yazar devamında, “*Bizim anladığımıza göre fıkra, bilgisayar sistemine sahip olan kişinin bu sistemden herhangi bir kişinin*

²³¹ **YAZICIOĞLU, Bilgisayar Suçları**, s. 261

²³² **ERSOY**, s.177. “*Kullanılan terim ve deyimlerin, bilgisayar dili anlamlarında değerlendirildiğinde fiziksel kısımlara ilişkin fiilleri de kapsayacak şekilde anlaşılabilmesi, Kanun Koyucunun bilgisayar ortamını koruma yönündeki gerçek amacını unutturmamalıdır... ‘Tahrip’ fiilleri de fiziksel kısımlara değil bilgisayarın elektro-manyetik ortamına yöneldiği ölçüde bu kapsama girecektir. Örneğin bir monitörün tahribi sistemin fiziksel bir parçasının tahribi olarak Ceza Kanunun 516. maddesi hükmünde öngörülen suçu oluştururken, içinde bulunan verileri ortadan kaldırmak için bir “sabit disk”i (hard disc) tahrip etmek fiili 525/b-1 fıkrasındaki suç sayılmaktadır.*” a.g.m., s. 177. Aynı yönde **DÜLGER**, s. 150.

²³³ Yazara göre örneğin bir monitörün tahribi sistemin fiziksel bir parçasının tahribi olarak TCK’nin 516. maddesi hükmünde öngörülen suçu oluştururken, içinde bulunan verileri ortadan kaldırmak için “sabit disk”i (hard disc) tahrip etmek fiili 525/b-1 hükmüne göre bilgisayar ortamına müdahale teşkil edecektir. **ERSOY**, s.177.

²³⁴ **ÖNDER**, s. 508.

²³⁵ **ERSOY**, s. 177, **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 623.

müdahalesi olmadan yararlanabilme imkânının engellenmiş olmasıdır. Bu imkânın ortadan kaldırılması, failde şu ya da bu kast olmadan da gerçekleşebilir. Failde, başkasına veya kendisine yarar maksadı olmadan fakat kasten bilgisayar verilerinin tahribi halinde bu suç oluşmayacak mıdır ?” görüşünü dile getirmiştir²³⁶. Ersoy da bu fıkra kapsamında “program değiştirme” fiilinde “başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak” amacının tartışılabileceğini; program tahribi, silinmesi veya değiştirilmesi gibi bir sonuç doğuran hareketin zarar vermesi veya yarar sağlaması kaçınılmaz olduğuna göre, ayrıca bir de özel kastın aranmasının gereksiz olduğu görüşünü dile getirmiştir²³⁷. Yazıcıoğlu ise, maddede öngörülen özel kastın, bu suçun taksirle işlenemeyeceğinin vurgulanması amacıyla yer aldığını ifade etmiştir²³⁸.

Yukarıda kısaca değinilen TCK’nin 525/b maddesi, TCK’nin yürürlüğe girmesi ile birlikte 1 Haziran 2005 tarihinde yürürlükten kalkmıştır. 5237 Sayılı TCK’nin 244. maddesinde, sisteme ve veriye müdahale iki fıkra halinde düzenlenmiş, maddenin birinci fıkrasında sistemin işleyişine müdahale ikinci fıkroda ise sistem içerisindeki veriye yönelik fiiller düzenlenmiştir. 765 Sayılı TCK’nin 525b maddesinden farklı olarak sisteme ve veriye müdahale fiilleri için farklı cezalar öngörülmüştür. Bu açıdan sistemin işleyişinin engellenmesi ve bozulması daha ağır cezayı gerektiren fiiller olarak ele alınmıştır. Ayrıca maddenin üçüncü fıkrasında birinci ve ikinci fıkroda düzenlenen fiillerin banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali ağırlatıcı neden olarak düzenlenmiştir. Aynı şekilde aşağıda inceleneceği üzere bilişim sistemi

²³⁶ ÖNDER, s. 508.

²³⁷ ERSOY, s. 181.

²³⁸ YAZICIOĞLU, *Bilgisayar Suçları* s. 265

aracılığıyla yarar sağlama fiillerine ilişkin 765 Sayılı TCK'nin 525b/ 2. fıkrasında yer alan suç unsurları itibariyle belirginleştirilerek 244. maddenin son fıkrasında yeniden düzenlenmiştir. Her iki Kanunda yer alan bilgisayara aracılığıyla yarar sağlamaya ilişkin suçlara aşağıda ayrıca değinilecektir.

2. Sisteme ve Veriye Müdahale Suçunun Hukuki Konusu

a. Genel Olarak

Yukarıda verinin gizliliği ile ilgili olarak, ilgili kişinin tasarruf yetkisinin dışa dönük bir nitelik taşıdığı ve bu açıdan ister malvarlığı isterse sırrın korunması kapsamında düzenlensin, verinin yetkisiz kişilerin eline geçmesinin önlenmesinin amaçlandığı ifade edilmişti. Veriye müdahalede ise Sözleşmenin 4. maddesinde düzenlenen veriye müdahale ile ilgili olarak Sözleşmenin açıklayıcı raporunda, maddi varlığı olan şeylere yönelik zarar verme girişimlerine korumaya benzer bir şekilde bilgisayar veri ve programlarına yönelik fiillerin korunmak istendiği, bu açıdan verinin bütünlüğü ve düzgün bir şekilde çalışması ve kullanımının korunmasının amaçlandığı belirtilmektedir²³⁹. Veriye müdahale bakımından ilgili kişinin veri üzerinde, veriye yönelik olarak üçüncü kişiler tarafından gerçekleştirilecek müdahalelerden uzak bir şekilde tasarrufta bulunabilmesi sağlanmak istenmektedir. İlgili kişinin tasarruf yetkisi verinin elde edilmesinde üçüncü kişilerin verinin içeriğini öğrenmesinin ya da veriyi kullanmasının önüne geçilmesi şeklinde dışa dönük olarak korunmakta iken; veriye müdahalede, veriyi

²³⁹ Bkz., Sözleşme açıklayıcı rapor, parag. 60
<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

elinde bulunduran kişinin veri üzerinde tasarruf yetkisinin, veriye müdahale edilerek ve bu şekilde zarar verilerek hukuka aykırı bir biçimde sınırlandırılması ya da ortadan kaldırılması anlamında içe dönük olarak korunmaktadır.

Bilişim sistemine yönelik müdahaleler genel olarak veri ya da programlara müdahale açısından ele alınmakta, bu haliyle ilgili kişinin sistem üzerinde sistemin işleyişi bakımından tasarruf yetkisinin korunması veriye paralel bir şekilde ortaya çıkmaktadır. Nitekim Sibersuç Sözleşmesinin açıklayıcı raporunda bu husus, sistemi kullanan kişilerin ya da sistem operatörlerinin sistemin sorunsuz bir şekilde işlemesindeki çıkarlarının korunduğu şeklinde ifade edilmiştir²⁴⁰.

Tasarruf yetkisinin görünümü, yukarıda aktarıldığı üzere, verinin elde edilmesi ya da yetkisiz erişim suçlarında olduğu gibi, özel hayatın gizliliğinin ya da malvarlığının korunması şeklinde çeşitli ülke mevzuatları bakımından hukuki konuya ilişkin farklı tercihlerin konusunu oluşturmamaktadır. Bu açıdan verinin elde edilmesi ve yetkisiz erişime ilişkin düzenlemelerde suçun hukuki konusu bakımından yapılan tercihe ilişkin çeşitli ülkelerin ceza mevzuatlarında ortaya çıkan farklılık sisteme ve veriye müdahale bakımından etkisini kaybetmektedir. Veri ve sistem üzerinde ortaya çıkan tasarruf yetkisi suçun hukuki konusu kapsamında mameleki varlıkların korunması kapsamında ele alınmaktadır ve bu kapsamda kişiye ait mameleki varlıkların korunması söz konusudur.

Nitekim verinin ele geçirilmesi suçunun sırrın korunması kapsamında düzenlendiği Alman Ceza Kanununda, verinin ele geçirilmesi malvarlığına karşı suçlar arasında mala zarar verme suçundan sonra düzenlendiği ve sistematik olarak

²⁴⁰ Bkz. Sözleşme açıklayıcı rapor parag. 65
<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

malvarlığının korunmasına işaret edildiği görülmektedir. Benzer bir şekilde yetkisiz erişim suçunun konut dokunulmazlığının korunması paralelinde düzenlenen İtalyan Ceza Kanununda aynı yaklaşım sergilenmektedir. Adı geçen Kanunda sistem ve veriye zarar verilmesi suçu, malvarlığına karşı suçlar arasında mala zarar verme suçun düzenlendiği 635 maddesinden hemen sonra 635bis maddesinde düzenlenmiştir. Hukuki konu kriterine göre suçların sınıflandırıldığı İtalyan Ceza Kanunu bakımından da sistematik bir yaklaşımla sistem ve veriye müdahalenin malvarlığının korunması kapsamında ele alındığını söylemek mümkündür.

Fransız Ceza Kanununda da her ne kadar sistem ve veriye müdahale mala zarar vermeye ilişkin suçlar arasında düzenlememekte ise de adı geçen Kanunda veri ve sisteme zarar verme malvarlığına karşı diğer suçlar başlığı altında düzenlenmiştir.

Bilişim sistemine ve veriye müdahale suçları yukarıda belirtildiği üzere genel olarak malvarlığına karşı suçlar arasında düzenlenmekte, hukuki konu esas alınarak yapılan düzenlemelerde ise mala zarar verme suçu ile aynı bölümde yer almaktadır. Özellikle hukuki konu bakımından esas alınan bu düzenleme tarzı, bu suçların hukuki konusunun tespitinde önem arz etmekte aynı zamanda bu suçların düzenlenmesinde klasik mala zarar verme suçunun kapsamı bakımından tartışmaları da beraberinde getirmektedir. Mameleki varlığın korunması içerisinde sistem ve veriye müdahale edilmesi açısından suçların hukuki konusunun tespiti ise bu fiillerin ayrı bir suç olarak düzenlenmesine ilişkin nedenlerle bağlantılı bir biçimde ortaya çıkmaktadır.

b. Suçun Hukuki Konusu Açısından Mala Zarar Verme Suçu Karşısında Sisteme Ve Veriye Müdahale

Klasik mala zarar verme suçunun düzenlenmesinde tarihsel süreç esas alındığında taşınır ya da taşınmaz malın fiziki yapısı ya da diğer bir ifade ile maddi varlığı esas alınarak bunlara yönelik zarar verici fiillerin engellenmesi amaçlanmaktadır. Mala zarar verme suçunun ceza kanunları içerisinde düzenlenmesinde ise genel olarak bu suçun seçimlik hareketli bir suç olarak ele alınması yoluna gidilmiş ve bu yönde mala zarar verme suçunun maddi unsuru belirlenmiştir. Bu açıdan 765 Sayılı TCK'de da Kanunun 516. maddesinde düzenlenen mala zarar verme suçunun maddi unsurunu oluşturan hareketler, taşınır ya da taşınmaz malın yıkılması, yok edilmesi, bozulması ve ayrıca zarar verilmesi şeklinde karşımıza çıkmaktadır. TCK'de ise mala zarar verme suçu Kanunun 152. maddesinde düzenlenmiş olup suçun maddi unsurunu oluşturan hareketler taşınır ya da taşınmaz malın kısmen ya da tamamen yıkılması, tahrip edilmesi, yok edilmesi, bozulması, kullanılmaz hale getirilmesi ve de kirletilmesi olarak karşımıza çıkmaktadır.

Bilişim sistemlerinin yaygınlaşması bu kapsamda veri işleme faaliyetinin artması ile birlikte, bunlara yönelik, veri ya da programları hedef alan müdahalelerin önlenmesi ve bu tür fiillerin cezalandırılabilirliği sorunu ortaya çıkmıştır. Geleneksel mala zarar verme suçunda yukarıda aktarıldığı şekliyle öngörülen hareketler taşınır ya da taşınmaz malda genel olarak fiziksel bir zarar ararken, bilişim sistemlerine yönelik sistemin yazılım unsuruna müdahale bilişim sistemi bakımından her zaman için fiziksel bir değişikliğe yol açmamaktadır.

Sisteme müdahale bakımından ortaya çıkan sorun, sistemin yazılım ve donanım unsurlarından oluşması karşısında, sistemin fiziki yapısı yani donanımına yönelik olmayan yani yazılım unsuruna yönelik müdahaleler sonucunda sistemin fonksiyonlarını yerine getirememesinin mala zarar verme suçu kapsamında değerlendirilip değerlendirilemeyeceğidir. Bu durumda, suçun unsurlarını oluşturan hareketler ve hareketler sonucunda sistemin fiziki yapısında bir değişiklik olmadan sistemin işleyişine müdahale edilmiş olması bakımından soruna yaklaşmak gereklidir.

Bilişim sistemine yönelik müdahalelerde genel olarak sorun, sisteme müdahale teşkil edebilecek fiillerin mala zarar verme suçunu oluşturup oluşturmadığıdır. Bu tür müdahalelerde sistemin maddi varlığı ya da fiziki yapısında bir değişiklik olmamasına karşın sistemin fonksiyonlarını yerine getirememesi söz konusu olmaktadır. Bu haliyle mala zarar verme suçu açısından çözümlenmesi gereken husus, mala zarar verme suçunun unsurlarının bu tür fiilleri kapsayıp kapsamadığı noktasında toplanmaktadır. Sorunun bu noktada toplanması ise, diğer bir husus hakkında, yani bu tür fiillerin cezalandırılması ise korunmak istenen değerini yani bu suçun hukuki konusu bakımından bir çözüme ulaştırabilmektedir. Bu açıdan sorunun suçun maddi unsuru bakımından ortaya çıkması ve bunun çözümü için yeni bir suça yer verilmesi, mala zarar verme suçunun hukuki konusu ile bu suçun hukuki konusunun aynı olduğunu göstermektedir.

Nitekim sisteme müdahale bakımından yukarıda örnek olarak verilen ceza kanunlarında hukuki konu açısından bu yaklaşımın sergilendiği ve sisteme müdahaleye ilişkin ya veriye müdahale ile birlikte ya da veriye müdahaleden

bağımsız bir suç şeklinde malvarlığının korunması merkezinde özel düzenlemelerin yapıldığı görülmektedir.

Verinin bütünlüğüne yönelik müdahalelerde ise sorun, yukarıda belirtildiği şekliyle mala zarar verme suçunun unsurları bakımından ortaya çıkmakla birlikte sorunun diğer bir yönü maddi varlığı olmayan verinin, genel olarak maddi varlığı olan taşınır ve taşınmaz malın esas alınarak düzenlendiği mala zarar verme suçunun konusunu oluşturup oluşturmadığıdır²⁴¹. Bu açıdan bu son söylenen husus maddi varlığı olmayan verinin, verinin ele geçirilmesi suçunda da bahsedildiği üzere, mal olarak kabul edilip edilmemesi ile bağlantılıdır.

Verinin mal/eşya olarak kabul edilemeyeceğine ilişkin sorun ise, veriye müdahaleye yönelik fiillerin cezalandırılmasında iki farklı yaklaşımın esas alınmasına yol açmıştır. Birinci yaklaşım genel olarak ekonomik değer taşıyan verinin mal/ eşya olarak kabul edilmesi şeklinde olup bu haliyle genel olarak kıta Avrupasında ve Türk Ceza Hukukunda mala zarar verme suçunun konusunun maddi varlığı olan taşınır veya taşınmaz mal olması şartından uzaklaşmaktadır²⁴². Diğer yaklaşım ise veriye müdahalenin verinin saklandığı diğer bir ifade ile bulunduğu mala yönelik bir zarar verme fiili olduğudur. Burada verinin saklandığı maddi mal esas alınarak veriye müdahale ile verinin saklandığı malın işlevine müdahale edilmiş oluşu bu haliyle de mala zarar verme suçunun kapsamında olduğudur²⁴³.

²⁴¹ **SIEBER**, s. 77.

²⁴² Enformasyonun bilişim sistemleri içerisinde temsil edici işlevi olan veriye müdahale özellikle verinin müdahalelerden korunması isteği ise öncelikli olarak, yukarıda ifade edildiği üzere günümüzde yaygın olarak enformasyon ya da bilişim toplumu olarak ifade edilen dönüşüm içerisinde verinin içerdiği enformasyonun başlı başına bir ekonomik değer olarak ortaya çıktığı görüşüne işaret etmekte ve ekonomik değere sahip veri saklandığı aygıtın işlevinden bağımsız olarak bir değer ifade etmektedir.

²⁴³ **SIEBER**, s.77

Yukarıda verinin ele geçirilmesi ile ilgili bölümde belirtildiği üzere ABD’de özellikle federe devletlerin ceza mevzuatlarında genel olarak ekonomik değeri olan veri, mal olarak kabul edilmiş ve veriye müdahale de verinin mal olarak kabul edilmesi merkezinde düzenlenmiştir. Bu doğrultuda sisteme ve veriye müdahale mala zarar verme kapsamında ele alınmış bunlara müdahale malvarlığına karşı suçlar olarak düzenlenmiştir²⁴⁴.

İkinci yaklaşımda ise verinin kendisi mala zarar verme suçu kapsamında suçun konusunu oluşturabilecek bir mal olarak kabul edilmemektedir. Burada veriye yönelik müdahale doğrudan mala zarar verme olarak kabul edilmemiş, sorun verinin saklandığı mal esas alınarak ele alınmıştır. Bu yaklaşıma göre veriye müdahale verinin saklandığı mal, içerdigi veri ile birlikte bir işleve sahip olup veriye müdahale sonucunda bu işleve zarar verilmekte bu haliyle mala zarar verme söz konusu olmaktadır. Bu durumda veriye müdahaleye ilişkin özel düzenleme yapılması bu duruma ilişkin bir açıklık getirilmesi amacını taşımaktadır²⁴⁵. Aynı yaklaşım, sisteme

²⁴⁴ Örnek olarak Bkz Iowa Code @ 716A.4 (1989), Kanunda bilgisayara zarar verme başlığı altında hem bilgisayar sistemlerine hem de veriye müdahale bir arada düzenlenmiş olup, bu suça öngörülen ceza Kanunun ilgili maddelerinde düzenlendiği şekliyle ortaya çıkan ekonomik zararın ağırlına göre değişmektedir. <http://nsi.org/Library/Compsec/computerlaw/Iowa.txt> . New York eyaletinde ise veriye müdahale suçunda 1000 doları aşan bir zararın meydana gelmesi halinde fail veriye müdahale suçundan dolayı cezalandırılmaktadır. <http://nsi.org/Library/Compsec/computerlaw/Newyork.txt>

Ayrıca bkz Delaware 11 Del. C. @ 935. Kanunda veriye müdahale suçu hem kasıt hem de taksirle işlenebilen bir suç olarak düzenlenmiştir. <http://nsi.org/Library/Compsec/computerlaw/Delaware.txt>

²⁴⁵ Aktaran **SIEBER**, s. 91-92 Yazar yukarıda aktarılan görüşün birçok ülkede B.n görüş olarak ortaya çıktığını ifade etmektedir. Yazara göre burada sorun veriye, iletilmesi sırasında müdahale edilmesi halinde ortaya çıkmaktadır. Yazar devamında aralarında yukarıda örnek olarak verilen İtalya, Almanya ve Fransa’nın da bulunduğu birçok ülkenin veriye müdahaleye yönelik fiillere açıklık getirilmesi amacıyla ceza mevzuatları içerisinde düzenleme yaptıklarını ifade etmektedir. Bu düzenlemeler genel olarak klasik mala zarar verme suçuna ek yapılması, her türlü bilgisayar sistemlerinde saklanan veri yanında her türlü dokümanın korunmasına ilişkin düzenleme yapılması, verinin bütünlüğünün korunmasına ilişkin özel düzenleme yapılması şeklinde ortaya çıkmıştır. Yazar bu ülkeler arasında

müdahale bakımından geçerli olup, her ne kadar sistemin yazılım unsuruna yönelik müdahale söz konusu olsa da burada sistemin işlevini yerine getirememesi söz konusu olduğundan, mala zarar verme suçunun oluştuğu söylenebilir.

Yukarıda aktarılan hususlar topluca değerlendirildiğinde, sistem ve veriye müdahaleye ilişkin suç ya da suçların, genel olarak mala zarar verme suçuna ilişkin hükümlerin özellikle sistemin yazılım yönüne ve veriye müdahale bakımından uygulanabilir olup olmadığı noktasında ortaya çıkan tartışmalar ve söz konusu soruna açıklık getirme isteği noktasından hareketle ortaya çıktığı görülmektedir. Bu haliyle de sisteme ve veriye müdahale genel olarak mala zarar verme kapsamında değerlendirilmektedir. Söz konusu fiillerin mala zarar verme kapsamında değerlendirilmiş olması bu fiillerin esas alındığı suçların hukuki konusu bakımından da bir işleve sahiptir.

Bu açıdan değerlendirildiğinde, ister ABD de federe devletlerde kabul edildiği şekliyle veri mal olarak kabul edilsin isterse verinin saklandığı malın işlevi ya da sistemin işleyişi esas alınarak soruna yaklaşılsın, mala zarar verme kapsamındaki fiiller söz konusu olmakta bu haliyle de malvarlığının korunması amaçlanmaktadır. Sisteme ve veriye müdahale fiillerine ilişkin suç, mala zarar verme suçu ile aynı hukuki konuya sahiptir.

ABD'yi de belirtmesine rağmen federe devletlerin ceza mevzuatlarında verinin mal olarak kabul edilmesi karşısında bu ifadenin verinin açıkça mal olarak kabul edilmediği Federal düzeydeki düzenleme açısından geçerli olduğu kanaatindeyiz.

c. Türk Ceza Kanununda Düzenlenen Bilişim Sistemine ve Veriye Müdahale Suçunun Hukuki Konusu

Yukarıda sisteme ve veriye müdahalenin hukuki konusu tartışılırken bu fiillerin ayrıca suç olarak düzenlenmesinin nedenlerinden hareket edilmiş, bu kapsamda mala zarar verme suçunun unsurunda ve kapsamında ortaya çıkan tartışmalar bu suçun hukuki konusunun saptanmasında esas alındığı belirtilmişti.

Sisteme ve veriye zarar verme suçuna ilişkin, mala zarar verme suçundan ayrı özel bir düzenlemenin yapılmasına ilişkin gerekçeler incelendiğinde, Türk Ceza Hukuku bakımından da sisteme ve veriye zarar verme suçunun mala zarar verme suçu ile birlikte değerlendirildiği görülmektedir.

Nitekim, 765 Sayılı TCK'nin 525/b 1. fıkrasında yer alan sisteme ve veriye zarar verme suçu ile ilgili olarak *Dönmezer*, bu maddede düzenlenen fiiller ile sisteme ve içeriğine karşı mala zarar verme fiillerinin işlendiğini ifade etmiştir²⁴⁶. *Önder* de bu suçun klasik mala zarar verme suçunu oluşturduğunu belirtmiştir. *Yazıcıoğlu* da bu suçun klasik mala zarar verme suçunun özel bir şekli olduğunu, bu suçun sistem ve içeriğini esas alan mala zarar verme fiillerini kapsadığını ifade etmiştir²⁴⁷.

²⁴⁶ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler** s. 622.

²⁴⁷ **YAZICIOĞLU, Bilgisayar Suçları** s. 258

Buna karşın 765 Sayılı TCK'nin 516. maddesinde düzenlenmiş olan mala zarar verme suçunda suçun konusunu sadece somut mal niteliği taşıyan nesnelerin oluşturduğu, veriye ve sisteme zarar verme suçunda ise suçun konusunu içinde veri bulunması şartıyla bilişim sisteminin mal olarak nitelenen donanım kısmı kadar klasik anlamda mal olarak nitelendirilemeyecek veri kısmının da oluşturduğu ifade edilmiş ve bu açıdan her iki maddenin birbirinden tamamen farklı iki suç tipini içerdiği *Dülger* tarafından ifade edilmiştir. Yazar devamında mala zarar verme suçu ile sisteme ve veriye müdahale suçunun

TCK'nin gerekçesi incelendiğinde de sisteme ve veriye yönelik müdahale fiillerinin mala zarar verme suçuna göre özel bir düzenlemeye tabi tutulduğunun belirtildiği görülmektedir. Nitekim sisteme ve veriye müdahale ile ilgili olarak madde gerekçesinde “...sistemlere yöneltilen ızzar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkıada seçimlik hareketli bir suç meydana getirilmiştir.” denmektedir²⁴⁸.

TCK'nin 244. maddesinin 1. ve ikinci fıkıalarında düzenlenen “sistem ve veriye müdahale” suçunun da mala zarar verme suçu ile bağlantılı olarak incelendiği ve sisteme ve veriye zarar verme fiillerinin ayrıca özel olarak düzenlendiği yazarlarca da kabul edilmektedir²⁴⁹.

birbirinden tamamen farkı iki suç tipini düzenlediğini ve birbirleri arasında yasaların uygulanmasına ilişkin olarak özel hüküm- genel hüküm ya da önceki-sonraki hüküm ilişkisi bulunmamaktadır. **DÜLGER**, s. 160,

Yazarın gerekçesi incelendiğinde, yukarıda aktarıldığı üzere, mala zarar verme kapsamında sistem ve veriye müdahalenin neden ayrı bir suç haline getirildiğine ilişkin tartışmaları yansıttığı görülmektedir. Bu açıdan maddi varlığı olmayan verinin hukuken mal olarak kabul edilmesi ya da verinin saklandığı aygıtın işlevinin kaybetmesi noktasından hareketle ve bu ikinci yaklaşıma bağlantılı olarak bu kapsamda mala zarar verme suçuna ilişkin düzenlemelerde ortaya çıkabilecek sorunlara açıklık getirmek amacıyla düzenlenen sistem ve veriye müdahale klasik mala zarar verme suçunun bu tür fiilleri kapsayıp kapsamadığına ilişkin sorunun çözümü olarak karşımıza çıkmaktadır. Bu nedenle yazarın mala zarar verme suçu ile sisteme ve veriye müdahaleye ilişkin suçları birbiriyle ilişkisi olmayan ve birbirinden tamamen bağımsız suçlar olduğu görüşüne katılmamaktayız. Bu kapsamda mala zarar verme ve sistem ve veriye müdahale suçu birbirini tamamlayan suçlardır.

²⁴⁸ Madde gerekçesi için bkz, maddegerekce-1. doc <http://www.ceza-bb.adalet.gov.tr/> .

Madde gerekçesi incelendiğinde bu gerekçenin 244. maddenin Meclis Genel Kuruluna sunulan tasarıdaki düzenlemesine yönelik olduğu görülmektedir. Gerekçede 244. maddenin 1. fıkrasında sisteme ve veriye müdahale fiillerinin düzenlendiği belirtilmekte ise de Meclis görüşmeleri sırasında bu madde değişmiş ve sisteme müdahale ve de veriye müdahale iki ayrı fıkrada düzenlenmiştir.

²⁴⁹ Durmuş **TEZCAN** – Mustafa Ruhan **ERDEM** – Murat **ÖNOK**, 5237 Sayılı Türk Ceza Kanunu'na Göre Teorik ve Pratik Ceza Özel Hukuku, Seçkin Yayınevi, 3. B., 2006, s.447. Yazarlar sisteme ve veriye müdahale fiillerinin mala zarar verme suçuna ilişkin özel bir düzenleme olduğunu ifade ederken verinin mala zarar verme anlamında mal kavramına

Yukarıda aktarılan bu görüşler kapsamında 765 Sayılı TCK'nin 525/b 1. fıkrasında yer alan düzenleme ile ilgili olarak *Dönmezer* şu düşünceleri ileri sürmektedir: “*Bilgisayarın dokunulmaz olması gereği ve sistemin uygun şekilde işlev görmesi ve içeriğinin aynı suretle hizmet görmesidir. Böylece aslında başta malikin veya sistemi kullananın yararı korunmaktadır*²⁵⁰. *Yazıcıoğlu* da bu suç ile, kişilerin sistem ve içerisindeki unsurlar bakımından sahip oldukları mülkiyet hakkının koruma altına alındığı görüşündedir²⁵¹. *Önder* suçun koruduğu yararın tartışmalı olduğunu bazı yazarların bu suç tipi ile bilgisayarda mevcut veriler ile ilgili olan kişinin yararının korunduğunu, bazı yazarların ise mevcut verilerin ülke ekonomisinde ve idarede gerçekleştirildiği fonksiyon gereği, bu suçun ekonomik yaşama karşı işlenmiş bir suç olduğunu ifade ettiklerini ifade etmiştir²⁵². *Ersoy* ise bu suç ile kişinin malvarlığının korunduğunu belirtmiştir²⁵³.

TCK'nin 244. maddesinin 1. ve 2. fıkralarında düzenlenen sistem ve veriye müdahale suçuna ilişkin olarak *Kurt*, mülkiyet hakkının koruma altına alındığını bu kapsamda sistem ve sistem içerisinde yer alan verinin dokunulmazlığının korunan hukuki yarar olduğunu belirtmiştir²⁵⁴. *Karagülmez* ise bu yönde, hukuki konusun madde gerekçesinde belirtildiği şekliyle sisteme ve veriye yöneltilen ızzar fiilleri ile

girip girmediğinden hareketle bu hususun buna ilişkin özel düzenleme yapılması yoluyla veriye ilişkin ortaya çıkan boşluğun giderildiğini ifade etmektedirler.

TCK'nin 244. maddesinde düzenlenen sisteme ve veriye zarar verme suçunun mala zarar verme suçunun özel bir şekli olduğu hakkında ayrıca bkz, İnci **BİÇKİN**, *Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları*, Yargıtay Dergisi, C. 32, Ocak – Nisan 2006, S. 1-2, s. 153, **KARAGÜLMEZ**, s. 187, **KURT**, s. 161.

²⁵⁰ **DÖNMEZER**, *Kişilere ve Mala Karşı Cürümler*, a.g.e., s. 622

²⁵¹ **YAZICIOĞLU**, *Bilgisayar Suçları*, s. 260.

²⁵² **ÖNDER**, s. 508.

²⁵³ **ERSOY**, s. 166 – 167.

²⁵⁴ **KURT**, s. 161-162

bağlantılı olduğunu ifade etmekte ve bu kapsamda hem bilişim sisteminin hem de sistem içerisinde yer alan veriler ve diğer unsurların zarar görmemesinin amaçlandığını belirtmektedir. Bu açıdan yazarın da hukuki konunun mülkiyet olduğunu belirttiğini söylemek mümkündür²⁵⁵.

Dölger ise, bilişim sisteminin veri ve yazılımlardan oluşan soyut unsurları yanında donanım unsurunun da koruma altına alınması karşısında, suçun hukuki konusunun karma bir nitelik gösterdiğini belirtmiştir. Yazara göre; suçun hukuki konusunun bilişim sistemi ve bilişim sisteminin içerdği veriler üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanılmasındaki çıkardır²⁵⁶. Yazarın ifade ettiği sistemin yazılım unsurunu oluşturan veri ve programlar bakımından genel olarak kişinin sistem içerisindeki veriye ulaşması ve kullanılmasındaki yarar, yukarı da belirtildiği şekliyle ya verinin mal olarak kabul edilmesi ya da sistemin veri ile birlikte işlevi esas alınması suretiyle malvarlığına karşı suç olarak düzenlenmektedir. Bu açıdan karma bir hukuki konuya sahip olduğunu ifade ettiği sisteme ve veriye müdahale, tek bir hukuki konuya indirgenmektedir.

Aktarılan bu hususlar incelendiğinde TCK ve 765 Sayılı TCK bakımından da sistem ve veriye müdahalenin genel olarak mala zarar verme suçu kapsamında değerlendirildiği ve genel olarak 765 Sayılı Kanunun 525/b 1. fıkrasında ve TCK'nin 244 1 ve 2. fıkralarında düzenlenen sistem ve veriye müdahalenin mala zarar vermenin özel bir şekli olarak genel kabul gördüğü görülmektedir.

²⁵⁵ **KARAGÜLMEZ**, s. 187.

²⁵⁶ **DÜLGER**, , s 231; Aynı yönde **MERAN**, s. 370.

Sisteme ve veriye müdahalenin mala zarar verme suçunun özel şekli olduğu kabulü aynı zamanda Türk Ceza Hukukunda da sisteme ve veriye müdahalenin hukuki konusu ile mala zarar vermenin hukuki konusunun birbirine paralel olduğu sonucuna götürebilmektedir.

Bütün bu söylenenler topluca değerlendirildiğinde, 244. maddenin 1. ve 2. fıkralarında düzenlenen sistem ve veriye müdahale suçunun, yukarıda aktarıldığı üzere, klasik mala zarar verme suçunun bilişim sistemleri içerisinde sistemin yazılım yönünü oluşturan veri ve programlara yönelik müdahaleleri kapsayıp kapsamadığına ilişkin tartışmalara bir açıklık getirilmesi amacıyla düzenlenen bir suç olduğunu kabul ile bu suçun hukuki konusunun mala zarar verme suçunun hukuki konusuyla örtüşmektedir.

3. Suçun Maddi Unsuru

a. Sistemin İşleyişini Engelleme ve Bozma

i. Genel Olarak

Sistemin işleyişini engelleme ve bozma TCK'nin 244. maddesinin 1. fıkrasında, “*Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*” şeklinde düzenlenmiştir²⁵⁷. 244. maddenin birinci fıkrasında suçun unsurunu oluşturan seçimlik hareketler “*bilişim sisteminin işleyişinin engellenmesi*” ve “*sistemin işleyişinin bozulması*”dır. Maddede

²⁵⁷ Tasarının 20. maddesinde ise, “**sistemin çalışmasına müdahâle**” adı altında benzer bir suça yer verilmektedir. 20. maddeye göre, “*Bir bilişim ağı üzerinden hukuka aykırı olarak bir bilişim sisteminin çalışmasını veya işleyişini tamamen veya kısmen engelleyen, erişilmez kılan veya bozan kişiye iki yıldan beş yıla kadar hapis ve adli para cezası verilir.*”

yer aldığı şekliyle bilişim sisteminin işleyişi genel olarak veri işleme faaliyeti anlamına gelmekte olup bu haliyle fıkrada veri işleme faaliyetinin engellenmesi ya da bozulması düzenlenmiştir.

Kanunda engellenmenin ve bozmanın tanımına yer verilmemiştir. Türk Dil Kurumu Sözlüğünde engellemek, “*bir şeyin gerçekleşmesini veya yapılmasını önlemek*”; bozmak ise, “*bir şeyi kendisinden beklenen işi yapamayacak duruma getirmek*” olarak tanımlanmaktadır. Bu kapsamda bilişim sisteminin işleyişinin engellenmesi sistem aracılığıyla veri işleme faaliyetinin gerçekleştirilmesinin engellenmesi²⁵⁸, bilişim sisteminin bozulması ise sistemin veri işleme faaliyetini yapamayacak hale getirilmesi olarak tanımlanabilir.

Nitekim yazarlar tarafından, sistemin işleyişinin engellenmesinin sistemin çeşitli yönleriyle sürekli ya da geçici olarak iş görmesinin engellenmesi anlamına geldiği, sisteme her türlü müdahalenin bu kapsamda değerlendirilmesi gerektiği ifade edilmiştir²⁵⁹. Sistemin tamamen çalışamaz hale gelmesi²⁶⁰, sistemin olağan

²⁵⁸ 765 Sayılı TCK’nin 525/b maddesinde bu hareket bilişim sisteminin işlemesine engel olmak şeklinde yer almaktaydı. *Önder*, bilişim sisteminin işlemesine engel olmanın, bilgilerin, yapılan ilavelerle usulüne uygun bir biçimde değerlendirilebilmesine engel olmak ve amacını gerçekleştirememek anlamına geldiğini belirtmiştir. **ÖNDER**, s. 509

Dönmezer ise işlemesine engel olmanın çeşitli yollarla sistemin daimi ya da geçici olarak durdurulması anlamına geldiğini belirtmiştir. **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 623; Aynı yönde **YAZICIOĞLU, Bilgisayar Suçları**, s. 262.

²⁵⁹ **MERAN**, s. 371; Aynı yönde **DÜLGER**, s. 234., **KARAGÜLMEZ**, s. 188

Kurt bilişim sisteminin engellenmesi halinde sistemin bozulmasının söz konusu olmayıp normalde yerine getirdiği fonksiyonları ifa etmesinin engellendiğini ifade etmektedir. **KURT**, s. 164.

²⁶⁰ **KURT**, s. 164. Yazar bilişim sisteminin işleyişinin engellenmesinde de bazen çalışamaz hale gelmenin söz konusu olduğunu, fakat bu durumun arızı nedenlerden kaynaklandığını, ancak bozulmada tamamen devre dışı kalmanın söz konusu olduğunu belirtmiştir.

koşullarda yapması gereken işlevlerin değişikliğe uğratılması²⁶¹, haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılmasının²⁶² sistemin işleyişini bozma anlamına geleceği ifade edilmiştir²⁶³.

ii. Mala Zarar Verme Suçu Kapsamında Sistemin İşleyişinin

Engellenmesi ve Bozulması

244. maddenin 1. fıkrası incelendiğinde Sibera suç sözleşmesinden farklı olarak, sisteme müdahalenin sistemin yazılımına yönelik olarak sisteme veri gönderilmesi, yerleştirilmesi gibi hareketlerle gerçekleştirileceğine ilişkin bir düzenlemeye yer verilmediği görülmektedir. Burada tespit edilmesi gereken, sistemin yazılımına veri aracılığıyla müdahale halinin mi yoksa her türlü müdahalenin mi bu kapsamda değerlendirilmesi gerektiğidir.

Bu hususun tespiti, 244. maddenin 1. fıkrasının yazılıma yönelik fiiller yanında, maddi varlığı yani donanımına yönelik, mala zarar verme suçunun

²⁶¹ **MERAN**, s. 371.

²⁶² **KARAGÜLMEZ**, s. 188. Yazar sistemin işleyişinin kısmen ya da tamamen bozulmasının kısmen veya tamamen sistemin işleyişine engel olma anlamına geldiğini bu nedenle fıkra da bozma hareketine yer verilmeyebileceğini ifade etmiştir, a.g.e., s. 189

²⁶³ Sistemin işleyişinin engellenmesi açısından kimi yazarlarca sistemin elektriğinin kesilmesi durumunda da sistemin işleyişinin engel olma kapsamında değerlendirilebileceği ifade edilmiştir. Bkz., **YAZICIOĞLU, Bilgisayar Suçları**, s. 263. **MERAN**, s. 371.

Mala zarar verme suçunda belirtildiği şekliyle mala zarar verilmiş olması nedeniyle başkasına zarar verme söz konusu olmakta, bu açıdan elektriğin kesilmesi suretiyle makinelerin işlemesinin engellenmesi örneğinde olduğu gibi doğrudan mala yönelik olmayan filer mala zarar verme kapsamında değerlendirilmemektedir. Bkz., **TOROSLU; Ceza Hukuku Özel Kısım**, s. 156.

Aynı şeyi sistemin işleyişinin engellenmesi bakımından da söylemek mümkündür. Bu açıdan doğrudan sisteme müdahale teşkil etmeyen bir hareket yukarıda belirtildiği şekliyle elektriğin kesilmesi sistemin işleyişine engel olma kapsamında değerlendirilmemelidir.

konusunu oluşturabilecek fiilleri de kapsayan özel bir suç mu olduğu; yoksa bu fıkranın sadece sistemin yazılım unsuruna yönelik fiillerin esas alınarak mala zarar verme suçunu tamamlayan bir suç olarak düzenlendiğinin tespiti bakımından önem arz etmektedir.

Yukarıda belirtildiği üzere, sisteme müdahale, sistemin özellikle yazılım kısmına müdahale teşkil eden fiillerin cezalandırılabilmesine ilişkin mala zarar verme suçunun unsurlarına açıklık getirilmesi amacıyla çeşitli ülke kanunlarında düzenlenmeye başlanmıştır. Sisteme müdahalenin bu kapsamda düzenlenmesi ise öncelikli olarak yazılıma müdahalenin esas alınması suretiyle sisteme müdahale fiillerinin düzenlenmesi sonucuna götürmüş olup Sibera suç Sözleşmesinin 5. maddesinde de bu husus somutlaştırılmıştır.

244. maddede ise, sadece sistemin işleyişinin engellenmesi veya bozulmasından bahsedilmiş olup bunun sistemin yazılımına veri aracılığıyla müdahale edilerek gerçekleştirileceğine ilişkin açık bir hükme yer verilmemiştir. Madde ile ilgili yaygın kabul, sisteme veri yoluyla müdahale yanında sistemin işleyişini engelleyen ya da bozan her türlü müdahalenin de bu madde kapsamında değerlendirilmesi yönündedir²⁶⁴. Bunun yanında 244. maddenin 1. fıkrasının sadece donanıma yönelik müdahaleleri kapsadığı görüşü de ileri sürülmüştür²⁶⁵.

²⁶⁴ Bkz, **KURT**, s. 164-166, **KARAGÜLMEZ**, s. 188, **DÜLGER**, s. 234-235, **MERAN**, s. 371, **BİÇKİN**, s. 153-154; **AKINCI**, s. 242

²⁶⁵ Yılmaz **YAZICIOĞLU**, *Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi*, Yeditepe Hukuk Fakültesi Dergisi, C. 2, S. 2, 2005, 408–409.

Yazar Türk Ceza Kanununun 2001 Tasarısının sisteme ve veriye müdahaleyi düzenleyen 347. maddesinin gerekçesinde yer alan “ fiiller, aracın fizik varlığını ve işlemlerini sağlayan bütün diğer unsurları kapsamaktadır” ifadesinden hareketle sistemin fiziki varlığını oluşturan donanımının 244. maddenin 1. fıkrası ile koruma altına alındığını belirtmektedir. Devamında ise donanımın korunması bakımından fiziki müdahalenin ya da veri yoluyla müdahalenin bu fıkra kapsamında olduğunu belirtmektedir.

Bu fıkra kapsamında hangi tür fiillerin düzenlendiğinin belirlenmesi, TCK'de sisteme müdahalenin mala zarar verme suçu karşısındaki konumunun saptanması bakımından önemlidir. Eğer bu fıkranın yazılıma yönelik veri aracılığıyla gerçekleştirilen fiilleri kapsadığı kabul edilecek olursa, mala zarar verme suçu bakımından 244. maddenin birinci fıkrasında, suçun konusunun sistemin yazılım yönünün esas alındığı sonucuna varılabilecektir. Fakat bu fıkranın donanıma ve yazılıma yönelik fiilleri bir bütün olarak kapsadığı ya da donanıma yönelik fiilleri kapsadığı kabul edilecek olursa, mala zarar verme suçuna göre bilişim sistemini bir bütün olarak konu edinen özel hüküm olduğu sonucuna varılabilecektir²⁶⁶.

²⁶⁶ Nitekim bilgisayar programlarına ve veriye müdahalenin özel olarak düzenlendiği İngiltere'de bu konuya, müdahale sonucunda ortaya çıkan değişikliğin fiziksel sonuç doğurup doğurmamasından hareketle açıklık getirilmiştir. Bilişim suçları ile ilgili özel kanunun (Computer Misuse Act) yer aldığı İngiltere'de ise suçun konusunu bilgisayar programları ve veriler oluşturmakta olup kanunda mala zarar verme suçu ile farklılık yaratılmıştır. Bu kanun bakımından fiilin bilgisayar programı ve veriye müdahale suçu kapsamında olması için fiziksel bir değişiklik meydana gelmemesi gerekir. Fiziksek bir değişikliğin söz konusu olması halinde suç mala zarar vermeye ilişkin suçların düzenlendiği 1971 tarihli Kanun kapsamındadır (Criminal Damage Act) Bkz, **LLOYD**, s. 246 vd. Ayrıca bkz., Steve **SHACKELFORD**, *Computer-Related Crime: An International Problem in Need of an International Solution*, 27 Tex. Int'l L.J. 1992, s. 492, David **BAINBRIDGE**, *Introduction to Computer Law*, third edition, 1996, s. 258. vd.

İtalyan Ceza Kanununda ise bu sorunun çözümüne farklı bir açıdan yaklaşmış olup 635/bis maddesi ile bilişim sistemi ver veriye yönelik her türlü müdahale özel bir suç haline getirilmiştir. Bu düzenlemede dikkat edilmesi gereken nokta mala zarar verme suçunun maddi unsurunu oluşturan hareketlerin bilişim sistemlerine ve veriye müdahale bakımından aynen tekrar edilmesidir. Maddenin bilişim sistemi ve veri esas alınarak Kanunun 635. maddesinde düzenlenen mala zarar verme suçunun maddi unsurunu oluşturan hareketleri aynen tekrar etmesi karşısında TCK'nin 244. maddesinin özellikle 1. fıkrasının uygulanması bakımından ortaya çıkan sorunun İtalyan Ceza Kanunu bakımından çözümlendiği söylenebilir.

Alman Ceza Kanununda ise veriye müdahale 303a maddesinde, suçun unsurları veriye müdahaleyi esas alacak şekilde düzenlenmiştir. 303b maddesinde ise bilgisayar sabotajı başlığı altında maddede sayılan amaçlara yönelik veri işleme faaliyetlerine, veri işleme sistemlerine ve veri taşıyıcılarına yönelik zarar verici fiillerin gerçekleştirilmesi ve 330a maddesinde belirtilen şekliyle müdahale edilmesi özel olarak düzenlenmiştir. Maddede veri işleme faaliyetine müdahale esas alınmış olup bunun veriye müdahale edilmesi yoluyla veya sisteme ya da veri taşıyıcısına müdahale edilmesi yoluyla gerçekleştirilebileceği açıkça düzenlenmiştir. Maddedeki ifadesiyle veri işleme sistemine ya da veri taşıyıcısına

244. maddenin 1. fıkrasında yer alan düzenlemenin mala zarar verme suçunu tamamlayıcı nitelikte bir düzenleme olduğu kabul edilecek olursa geleneksel olarak taşınır ya da taşınmaz malın maddi varlığına yönelik hareketleri kapsayan mala zarar verme suçu ile sisteme müdahale bir bütün halinde uygulanabilecektir. Bu kapsamda yazılıma yönelik hareketler sonucunda sistemin işleyişinin engellenmesi ya da bozulması halinde 244. maddenin 1. fıkrası, sistemin tahrip edilmesi, yok edilmesi gibi donanımına yönelik fiilleri kapsayan maddi varlığına yönelik fiillerde ise TCK. nun 151. maddesi uygulama alanı bulacaktır. Bu durumda sorun cezaların miktarında ve 3. fıkra düzenleneni ağırlatıcı nedenlerin uygulanmasında ortaya çıkmaktadır.

244. maddenin 1. fıkrasının 151. maddeye göre, hem donanımına hem de yazılıma ya da sadece donanımına yönelik fiilleri düzenleyen, özel bir suç olduğu kabul edilecek olursa, bu durumda mala zarar verme suçunun maddi unsurunu oluşturan hareketlerin bilişim sisteminin maddi unsurunu oluşturan donanımına yönelik gerçekleştirilmesi durumunda nasıl bir çözüme varılması gerektiği sorun olarak karşımıza çıkmaktadır. Bu durumda sorun, mala zarar verme suçunun düzenlendiği 151. maddenin bilişim sistemleri bakımından uygulanıp uygulanamayacağı şeklinde karşımıza çıkmaktadır.

Fıkra bilişim sisteminin işleyişinden bahsedilmesinin belirli bir anlam ifade ettiğinin kabulü gerekmektedir. Bunlardan birincisi henüz özel ya da genel amaca yönelik bir faaliyete özgülenmeyen bir bilişim sisteminin bu madde kapsamında olmadığıdır. İkincisi ise, girişte kısaca değinilen fakat burada tekrar değinilmesi

yönelik zarar verici fiiller fiziksel bir zararı kapsamaktadır. Aktaran. **SCHWARZENEGGER**, parag. 7 vd.

gereken sistemin işleyişinin ne anlama geldiğidir. Yukarıda bunun veri işleme faaliyeti olduğu kısaca ifade edilmiştir.

Bilişim sistemleri ve özellikle bilgisayar sistemleri esas alındığında bunların karakteristik özelliklerini donanım yani fiziksel yapıdan çok yazılım unsuru belirlemektedir. Bu açıdan bir aygıt olarak bilgisayar sistemlerini diğer aygıtlardan ayıran unsur yazılım kapsamında belirli komutlar aracılığıyla veri işleme faaliyetini yapabilmesi ya da daha genel bir ifade ile işlem yapabilmesidir. Bu açıdan bir veri grubu olarak da adlandırılabilen programlar aracılığıyla verinin işlenmesi ve de saklanması yani yazılım unsuru diğer sadece donanıma bağlı çalışan aygıtlardan farkını ortaya koymaktadır. Veri işleme faaliyeti olarak adlandırılan bu süreç ise kanunda bilişim sisteminin işleyişi olarak formüle edilmiştir.

Bilişim suçları içerisinde sisteme müdahalenin ayrı olarak düzenlenmesinin nedeni ise, veriye müdahale edilmesi suretiyle sistemin işleyişine müdahale edilebilmesidir. Bilişim sisteminin işleyişinden, yazılıma bağlı veri işleme faaliyeti olarak anlaşıldığına göre 244. maddenin birinci fıkrasında bilişim sisteminin işleyişine müdahale edilmesi düzenlenmesinin, bilişim sisteminin yazılım yönüne yani veri işleme faaliyetine işaret ettiği sonucuna götürebilmektedir. Bu kapsamda sisteme yönelik fiziki müdahaleler yoluyla değil, sistemin yazılımına ve veriye müdahale ya da yazılımda değişiklik yapılması nedeniyle işleyişinin engellenmesi ya da bozulması halinin bu fıkra düzenlenmek istendiği söylenebilir²⁶⁷.

²⁶⁷ *Kurt* da bir yandan sistemin maddi varlığını oluşturan donanıma yönelik fiziksel saldırıları da bu madde kapsamında olduğunu ifade ederken burada hareketin amacının sistemin işleyişine yönelik olması gerektiğini belirtmiştir. Yazarı bu ifadesinden sistemin işleyişine engel olmayan fiziksel saldırıları bu madde kapsamında değerlendirmede sonucuna çıkarılabilmektedir. **KURT**, s. 165.

Bununla bağlantılı olarak maddede sadece sistemin işleyişinin engellenmesi ya da bozulmasına yer verilmesi, maddenin sisteme yönelik fiziksel müdahaleyi kapsam dışı bıraktığı sonucuna götürmektedir.

Bu açıdan incelendiğinde, bilişim sistemi açısından, sistemin işleyişinin engellenmesi, bilişim sistemi olarak bilgisayarın çalışma yöntemi esas alınarak, çalışma yöntemine yani veri işleme faaliyetine müdahale edilmesi yoluyla sistemin çalışmasının engellenmesi olarak karşımıza çıkmaktadır. Bunu daha somutlaştıracak olursak, bir bilgisayar sistemi kendi içinde işlemleri kapasitesine göre sıraya koyarak gerçekleştirir. Bir bilgisayar sisteminin işlem yapabilme sonuçlandırma hızı onun donanımsal yapısı ile bağlantılıdır. Bir sistemin belirli bir sürede yapabileceği işlem miktarını, yani sistemin işlem kapasitesinin zorlanması ise bir süre sonra sistemin işlem yapamaz hale gelmesi ile sonuçlanır. Bu durumda, sistemin donanım ya da yazılımında bir bozukluk meydana gelmemesine rağmen kapasitesi üzerinde işlem talep edilmesi nedeniyle çalışamaz hale gelmektedir. Yani sistemin donanım ve yazılımı ile birlikte bütünlüğü ve gördüğü işlev bakımından bir bozukluk meydana gelmemekte fakat sistem belirli bir süre çalışmamaktadır.

Bu kapsamda değerlendirilebilecek müdahale yöntemleri birbirinden farklı olmalarına rağmen şu örnekle konuyu açıklamak mümkündür. Bir web sayfasına erişim genel olarak o web sayfasının barındırıldığı sunucu bilgisayara bağlantı kurulması ve sunucuda bulunan web sayfasının içeriğinin yer aldığı verinin

Buna benzer bir görüş de 525/b 1. fıkrada yer alan “tahrip” etme ile ilgili olarak özellikle maddede geçen diğer unsurları kapsamında değerlendirilen yazı vs gibi aygıtların sisteme bağlantılı olarak fonksiyon görmesi halinde bunlara yönelik tahririn bu fıkra kapsamında olduğu ifade edilmiştir. Bağlı olmaması halinde mala zarar verme suçunun işlenmiş olacağı çünkü bu durumda verileri otomatik işleme tabi tutulmasında işlev görmediği vurgulanmıştır. Bkz, **AKINCI**, s. 238 – 239.

kopyalanması anlamına gelmektedir. Web sayfasının yer aldığı sunucunun ise belirli bir zaman diliminde ancak belirli sayıda bağlantıyı sağlayabilecek ve veri kopyalamasına izin verebilecek bir kapasiteye sahiptir. Birim zamandaki işlem kapasitesinin aşılmasını sağlayacak şekilde sisteme bağlantı kurulması ve veri kopyalanmasına ilişkin bilgisayar aracılığıyla gönderilen talep, yani veri iletilmesi, sistemin gönderilen taleplere cevap verememesi sonucunu doğurabilmektedir. Bu durum ise belirli bir zaman diliminde sistemin öngörülen hizmeti verememesi, örnekte olduğu gibi, web sayfasına erişilememesi sonucunu doğurmaktadır.

Yukarıda verilen örnek dışında, sistem içerisindeki veriye müdahale edilmesi, veri yerleştirilmesi yoluyla da bu sistemin işleyişinin engellenmesi mümkün olmakla birlikte bu örnekte olduğu şekliyle sistem içerisindeki verinin ya da genel olarak yazılımın değiştirilmesi, yok edilmesi gibi durumlar gerçekleşmeden ya da sistem bozulmadan da sistemin çalışmaması söz konusu olabilmektedir²⁶⁸. Nitekim bu hususu da kapsamı amacıyla Sibersuç Sözleşmesinde diğer hareketler yanında sistemin veri iletilmesi (transmitting) yoluyla işleyişinin engellenmesi de sisteme müdahalenin düzenlendiği 5. maddede yer almıştır.

Yukarıda aktarılan hususlar doğrultusunda, Sibersuç Sözleşmesinin 5. maddesinde olduğu şekliyle bir düzenlemeye yer verilmemiş olmasına rağmen, 244. maddenin 1. fıkrasında, fiziksel müdahaleleri kapsam dışı bırakacak şekilde, veriye ya da yazılıma müdahale yoluyla gerçekleştirilen fiillerin esas alındığı soncuna varmak mümkündür.

²⁶⁸ Bu konu hakkında ayrıntılı olarak bakınız, **YILMAZ, Bilişim Korsanlığı**, s. 319 vd., **SINROD**, s. 189 vd., **YAZICIOĞLU, Bilgisayar Suçları**, s. 158, **KURT**, s. 68-69.

Bilişim sisteminin işleyişinin bozulması ise, bu kapsamda sistemin yazılımını oluşturan işletim sistemi ya da diğer programlar gibi sistem içerisinde veri işleme faaliyetini ya da genel olarak işlem yapabilmesini sağlayan unsurlarına müdahale edilmesi sonucu, bunların işlem yapabilme kabiliyetinin tamamen ya da kısmen ortadan kaldırılması anlamındadır.

Bilindiği üzere bir aygıtın fonksiyonunu yerine getirememesi bozulma kapsamında değerlendirilmekte²⁶⁹ ve bu haliyle mala zarar verme suçunun kapsamında değerlendirilebilmektedir. Bir bilişim sistemi ele alındığında sistemin iki farklı şekilde bozulması söz konusu olabilmektedir. Bu açıdan bir bilgisayarın işlemcisine, anakartına, sabit diski gibi donanımına ait unsurlara zarar verilmesi sonucu sistemin kullanılmasının önüne geçilebilmesi mümkündür. Bütün bu fiiller ise mala zarar verme suçu kapsamındadır.

Bunun yanında bilişim sisteminin ve bu kapsamda ortaya çıkan bilgisayar sistemlerinin donanım yanında yazılım unsuru ile birlikte çalışması bunlara yönelik fiiller ile de sistemin bozulması, yani tamamen ya da kısmen kullanılmasının önüne geçilmesi mümkün hale gelmiştir. Bu durumda sistemin donanımında herhangi bir değişiklik meydana gelmemekle birlikte yazılım unsurunun bozulması nedeniyle sistem çalışmamaktadır.

Aslında burada, sistemin işleyişinin bozulmasına ilişkin bir hükmün yer almamış olması durumunda da sistemin işleyişinin bozulmasının mala zarar verme suçu kapsamında bozma olarak değerlendirilmesi mümkün olabilecektir. Çünkü bozma, sistemin fonksiyonu yerine getirememesi olarak anlaşıldığında bunun fiziksel bir müdahale ya da yazılıma müdahale yoluyla gerçekleştirilmesi arasında bir fark

²⁶⁹ ÖNDER, s. 464.

yoktur. Her ikisinde de özgülendiği amaç için kullanılamaması hali ortaya çıkmaktadır.

Bu durumda, sistemin donanımında diğer bir ifadeyle maddi varlığında ve bütünlüğünde bir değişiklik olmasından ve bozulmasından bağımsız olarak sistemin çalışmaması durumunda, sistemin bozulmuş sayılıp sayılmayacağına ilişkin ortaya çıkabilecek tereddüdün giderilmesi amacıyla bu hükme yer verildiğini söylemek mümkündür. Bunun sonucunda maddede ayrıca bilişim sisteminin işleyişinin bozulmasına yer verilmesi, bu madde ile fiziksel müdahalelerden çok yazılım ve veriye müdahale yoluyla sistemin bozulmasına ilişkin bir düzenleme yapıldığı sonucuna götürmektedir²⁷⁰.

Bu açıdan değerlendirildiğinde maddede donanımı da kapsayacak şekilde “*bilişim sisteminin bozulması*” ya da “*bilişim sisteminin engellenmesi*” şeklinde bir düzenlemenin yer almaması, sistemin işleyişine yani veri işleme faaliyetine yönelik fiillerin düzenlenmesi ve bu hareketlerin kapsamı esas alındığında bu fıkra ile sadece sistemin yazılım yönüne yönelik fiillerin esas alındığı sonucuna varmak mümkündür. Bu durumda bilişim sistemine ya da maddede belirtildiği şekliyle sistemin işleyişine yönelik fiziksel müdahaleler mala zarar verme suçu kapsamında değerlendirilebilecektir. Bozma dışında suçun unsurunu oluşturan hareketler bakımından 244. maddenin 1. fıkrası ile 151. madde arasında farklılık yaratılması bu açıdan birbirinden farklı hareketleri düzenlemesi de aynı sonuca götürebilmektedir.

²⁷⁰ “Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı”nın “Sistemin çalışmasına müdahale” başlıklı 20.maddesinde sistemin işleyişine müdahalenin bilişim ağları aracılığıyla gerçekleştirilebileceği düzenlenerek bu hususa dolaylı olarak yer verilmiştir. Madde metni şu şekildedir: “**MADDE 20-** (1) Bir bilişim ağı üzerinden hukuka aykırı olarak bir bilişim sisteminin çalışmasını veya işleyişini tamamen veya kısmen engelleyen, erişilmez kılan veya bozan kişiye iki yıldan beş yıla kadar hapis ve adli para cezası verilir”

Yukarıda açıklandığı üzere 244. fıkranın 1. fıkrasında sistemin işleyişinin bozulmasından bahsedilmesi, sistemin donanımın bütünlüğünün bozulmadan yazılımına müdahale nedeniyle kullanılamamasına işaret etmekte ve bu haliyle aslında bir tekrardan öteye gitmemektedir. İster donanımına zarar verilmesi ister yazılımına müdahale edilmesi sonucu sistemin çalışamaz hale gelmesi mala zarar verme suçunun maddi unsurunu oluşturan seçimlik harekelerden bozma olarak değerlendirilebilecektir.

244. maddenin birinci fıkrasında düzenlenen fiillerin, yazılım unsuruna yönelik müdahalelerin veri aracılığıyla gerçekleştirilmesi şeklinde olduğunun kabulü, 2. fıkra da düzenlenen veriye müdahale ile sisteme müdahale arasındaki ilişkinin ise genel olarak geçitli suç şeklinde olması sonucunu doğurmaktadır²⁷¹. Aynı gerekçe bu suçun mala zarar verme suçuna göre, sadece yazılım unsurunu kapsayan, özel bir norm olması sonucuna götürmektedir.

b. Bilişim Sistemi İçerisindeki Verileri Bozma, Yok Etme, Değiştirme, Verileri Başka Bir Yere Gönderme

i. Genel Olarak

765 Sayılı TCK'nin 525b/1. maddesinden farklı olarak bilişim sistemi içerisindeki veriye müdahale TCK'nin 244. maddesinin ikinci fıkrasında ayrıca düzenlenmiş ve sisteme müdahaleye göre daha az ceza öngörülmüştür. 244. maddenin 2. fıkrasında, *“Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren*

²⁷¹Geçitli suç hakkında bkz., Sulhi DÖNMEZER – Sahir ERMAN, Nazari ve Tatbiki Ceza Hukuku, Genel Kısım, C. I, 12. B., İstanbul, 1997, s. 404 vd.

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 verilmiştir²⁷².

Maddede yer alan seçimlik hareketlerden ilki, bilişim sistemi içerisindeki “verinin yok edilmesi”dir. Bilişim sistemi içerisindeki verinin yok edilmesi, verinin varlığına son verilmesi, ortadan kaldırılması, hak sahibinin tekrar elde edemeyeceği ya da büyük güçlükler sonucu elde edebileceği şekilde tasarrufundan çıkarılması²⁷³ verinin yok edilmesi olarak tanımlanabilir²⁷⁴.

244. maddenin 2. fıkrasında, 765 Sayılı TCK’nin 525/b maddesinde olduğu şekliyle verinin silinmesinden bahsedilmemiş, verinin yok edilmesi esas alınmıştır. Bu açıdan bilişim sistemi içerisindeki verinin silinmesinin yok etme kapsamında olup olmadığının tartışılması gerekmektedir. Nitekim verinin silinmesi teknik olarak silinen veriye her zaman için ulaşılamaması anlamına gelmemekte, sadece olağan yollardan o veriye ulaşılması imkânının ortadan kaldırılması anlamına gelmektedir. *Yazıcıoğlu*, silmenin mevcut kayıtların bulunduğu yerden yok edilmesinin kastedildiğini belirterek silme ve yok etmenin aynı anlamda olduğunu vurgulamıştır. Yazar, maddi anlamda bir yok etmekten bahsedilemeyeceğini, sadece silinen unsura

²⁷² Tasarının “**Veriler veya programların bütünlüğüne müdahâle**” adı altında 19. maddesinde ise, “*Bir bilişim ağı aracılığıyla; bir bilişim sisteminde bulunan verileri veya programları hukuka aykırı olarak bozan, silen, değiştiren, yok eden, erişilmez kılan veya sisteme veri veya program yerleştiren veya ekleyen veya veri veya programlara zarar veren kimseye iki yıldan beş yıla kadar hapis ve adli para cezası verilir.*” şeklinde veri ve programa müdahale suçuna yer verilmek istendiği görülmektedir. Tasarının gerekçesinde 19. maddede düzenlenen suçun bilişim ağı ile gerçekleştirilen fiiller bakımından uygulanabileceği bunun dışında TCK’nin 244. maddesinin 2. fıkrasının uygulanacağı belirtilmiştir.

²⁷³ **TOROSLU, Ceza Hukuku Özel Kısım** s. 157.

²⁷⁴ *Kurt* ise verinin yok edilmesinin veriye bir daha ulaşılamaması anlamına geldiğini belirterek daha dar bir anlam yüklemektedir. **KURT**, s. 168.

ulaşabilmek bakımından gereken normal bağın kaldırılması, bilgilerin tanınamaz hale gelmesinin söz konusu olduğunu bu açıdan silmek anlamının şeklen anlaşılması gerektiğini ifade etmiştir. *Önder* de bu yönde, silmenin mecazi ve mantıki anlamda olduğunu, bir programa ulaşabilmek için aradaki mevcut bağın koparılması anlamına geldiğini ifade etmiştir²⁷⁵.

Verinin silinmesine ilişkin yukarıdaki aktarılanlar ile aynı yönde görüş dile getiren *Dülger*, 244. maddenin 1. fıkrasında yer alan verileri yok etmenin verinin silinmesi anlamına geldiğini bu açıdan verinin yok edilmesinin mantıksal silme eylemi olduğunu vurgulamıştır²⁷⁶.

Buna karşın *Kurt*, verinin yok edilmesinin veriye bir daha ulaşılabilmesi 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 etmektedir²⁷⁷.

Bu aktarılanlar doğrultusunda, verinin yok edilmesinin, verinin varlığına son verilmesi, ortadan kaldırılması ve verinin tamamen ya da büyük güçlüklerle elde edebilecek şekilde tasarrufundan çıkartılması olarak tanımlandığında, verinin silinmesi de verinin yok edilmesi olarak değerlendirilir. Verinin teknik olarak tekrar edilebilmesi olanağı ya da olasılığının varlığı verinin silinmesinin verinin yok edilmesi kapsamı dışında tutulabilmesine ilişkin gerekçe olarak gösterilemez²⁷⁸.

²⁷⁵ **ÖNDER**, s. 509

²⁷⁶ **DÜLGER**, s. 236. Aynı yönde **MERAN**, s. 372.

²⁷⁷ **KURT**, s. 168.

²⁷⁸ Fakat hâlihazırdaki işletim sistemlerinde yer alan ve verinin yanlışlıkla ortadan kaldırılmasının engellenmesine ve veriye tekrar ulaşılabilmesine olanak sağlamak üzere, ara

Mala zarar verme suçunda olduğu gibi verinin tekrar elde edilebilmesine ilişkin emek ve masraf söz konusudur.

Maddede yer alan diğer bir seçimlik hareket bilişim sisteminin içindeki “*verinin bozulması*”dır. Verinin bozulması verinin içeriğine ya da yapısına müdahale suretiyle verinin kısmen ya da tamamen kullanılamayacak hale gelmesi olarak tanımlanabilir²⁷⁹. Burada özellikle verinin içeriğine müdahalenin var olan verinin içerdiği bilgi ya da enformasyona olumsuz müdahaleyi kapsadığını belirtmek gerekir²⁸⁰. Verinin yok edilmesinden farklı olarak burada verinin tasarruf alanından çıkartılmaması ya da ortadan kaldırılmaması söz konusudur²⁸¹.

Sistem içerisindeki veriye ve veri grubunu oluşturan programa virüs vb kötü amaçlı kodların eklenmesi bu anlamda veriyi bozma değil, verinin değiştirilmesi olarak değerlendirilmelidir²⁸². Çünkü bu halde virüs gibi kötü amaçlı kodların öngörülen şekilde çalışmasından önceki bir aşamada var olan bir veriye eklenmesi söz konusu olup bu aşamada veri tamamen ya da kısmen kullanılamaz hale gelmemiştir.

bir aşama olarak tanımlanabilecek geri dönüşüm kutusuna gönderilmesi ya da geçici klasörlere gönderilmesi hallerinde ya da verinin sistem içerisinde başka bir yere gönderilmesi ve bu şekilde saklanması hallerinde verinin yok edildiğinden söz edileceği tartışmalıdır. *Dülger* bu gibi hallerde de verinin yok edildiğinden bahsedilebileceğini belirtmekte burada veriye ulaşılamamasının bir şekilde engellendiğinden bahsetmektedir. **DÜLGER**, s. 236. Bu olasılığın veriye erişimin engellenmesi hareketi kapsamında geçici bir engellenmenin erişilmez kılma kapsamında olup olmadığının tespiti ile mümkündür.

²⁷⁹ Aynı yönde **MERAN**, s. 372, **KURT**, s. 167.

²⁸⁰ Sözleşme açıklayıcı Rapor, parag. 61.

²⁸¹ *Kurt* ise verinin bozulması ile verinin yok edilmesi arasındaki farkı verinin bozulması durumunda tamir edilebilmesinin mümkün olduğu, yok edilmesi durumunda ise tamir edilebilecek bir unsurun kalmadığı noktasından hareketle açıklamıştır **KURT**, s. 168.

²⁸² Siberaşlar Sözleşmesi Açıklayıcı Rapor, parag. 61..

Bu açıklama doğrultusunda madde metninde yer alan verinin değiştirilmesi ise var olan verinin kullanılmasını engellemeyen fakat verinin içeriğinin ya da kendisinin orijinallliğini ortadan kaldıran her türlü değişiklik olarak tanımlanabilir²⁸³. Bu açıdan kötü amaçlı kodların veriye yerleştirilmesi bu kapsamda değerlendirilebilmektedir.

“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 koparılmaktadır²⁸⁴. Sisteme DOS saldırıları ile bunun gerçekleştirilmesi de mümkün olmakla birlikte²⁸⁵, 244. maddenin düzenlenişi bakımından, DOS saldırılarının sistemin işleyişine yönelik bir saldırı niteliğinde olması nedeniyle, sistemin işleyişinin engellenmesi ve kimi durumlarda da işleyişinin bozulması söz konusu olacağından burada sisteme yönelik saldırılar sonucunda veriye erişilememesi halinin 1. fıkra kapsamında olduğunu söylemek mümkündür. Veriye erişilmesi bakımından erişimin engellenmesinin geçici ya da daimi olması arasında bir fark yoktur.

244. maddenin 2. fıkrasında düzenlenen hareketlerin sonuncusu ise “*sistem içerisindeki verinin başka bir yere gönderilmesi*”dir. Verinin başka bir yere gönderilmesinin, verinin transferi, verinin kopyalanması olduğu ve kopyalandığı

²⁸³ **KURT**, s. 168. Yazar kısmen ya da tamamen değiştirme arasında fark olmadığını belirtmekle birlikte değiştirme orijinal verinin kullanılamaz hale gelmesi anlamına geldiğinde verinin değiştirilmesinden değil bozulmasından bahsedilebilecektir. Bu nedenle özellikle tamamen değiştirilme halinde veri içeriği bakımından kullanılamaz hale geleceğinden verinin içeriği bakımından bir bozulmanın söz konusu olduğunu söylemek mümkündür

²⁸⁴ **MERAN**, s. 372.

²⁸⁵ **SCHWARZENEGGER**, s. 3.

yerin önemsiz olduğu, ifade edilmiştir²⁸⁶. Bilişim sistemi içerisindeki verilerin bilişim sistemi dışında bulunan başka bir bilişim sistemine ya da veri taşıma aracına aktarılması, kaydedilmesi ya da kopyalanması verinin başka bir yere gönderilmesi olarak kabul edilmektedir²⁸⁷.

Bilişim sistemi içerisindeki verilerin başka bir yere gönderilmesi hükmü TBMM'ye 15.05. 2003 tarihinde sunulan Tasarının sistem ve veriye müdahaleyi düzenleyen 347. maddesinde yer almamaktadır. TBMM Adalet Komisyonu tarafından bu madde değiştirilmiş ve maddeye eklenmiştir.

Yukarıda, kimi ülkelerin ceza mevzuatları içerisinde ve 765. s. TCK'nin 525/a maddesinde düzenlenen verinin ele geçirilmesi suçunun, TCK'de düzenlenmediği bunun yerine yetkisiz erişim suçuna yer verildiği ifade edilmişti. 244. maddenin 2. fıkrasında yer alan verinin başka bir yere gönderilmesinin Bu şekilde anlaşılması TCK'de da verinin ele geçirilmesi suçuna yer verildiği sonucuna götürmektedir.

Madde bir bütün olarak incelendiğinde sisteme ve veriye müdahale fiillerini düzenlediği görülmektedir. Sisteme ve veriye müdahale fiilleri bakımından ise, sistem ya da verinin ilgili kişinin isteği doğrultusunda işlemesi ya da kullanılmasını engelleyici fiiller genel olarak düzenlenmiştir. Nitekim bizim de katıldığımız görüşe göre; sistemin işleyişi ve veri bakımından mala zarar verme suçuna ilişkin özel bir düzenleme olarak madde kaleme alınmıştır. Burada sorun, verinin başka bir yere gönderilmesi fiilinin, maddenin düzenleniş amacı ve mala zarar verme suçuna ilişkin özel bir düzenleme olan, sisteme ve veriye müdahaleye uygunluğudur.

²⁸⁶ **KURT**, s. 170. Aynı yönde **MERAN**s. 372.

²⁸⁷ **DÜLGER**, s. 238

Yukarıda aktarıldığı üzere verinin başka bir yere gönderilmesi verinin kopyalanması olarak kabul edilmiştir. Verinin kopyalanması verinin çoğaltılması anlamına gelmektedir. Verinin çoğaltılması ise verinin kendisine, verinin kullanımı ya da erişebilirliği açısından herhangi bir etkide bulunacak bir hareket değildir. 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.

Verinin başka bir yere gönderilmesinin, verinin aslının ortadan kaldırılması olarak anlamak da bu madde bakımından geçerli değildir. Verinin aslının ortadan kaldırılması 2. fıkra düzenlenen hareketler bakımından verinin yok edilmesi kapsamında düşünülmesi her halde mümkündür.

Her ne kadar düzenleniş biçiminden, verinin kopyalanması ya da transfer edilmesi verinin başka bir yere gönderilmesi olarak anlaşılabilecek olsa da, bu olasılığın maddenin amacına uygun olarak dar yorumlanması gerekmektedir.

Bu durumda, verinin başka bir yere gönderilmesinin sistem içerisindeki verinin yer değiştirilmesi şeklinde dar yorumlanması yoluyla sisteme ve veriye müdahale bakımından anlam kazandırılabilmesi mümkündür.

Nitekim yukarıda belirtildiği üzere, veriye erişimin engellenmesi de bu madde kapsamına alınmış ve verinin içeriğinin bütünlüğü bozulmamasına rağmen veriye geçici ya da sürekli olarak kullanım imkânının engellenmesi, verinin erişilmez kılınması olarak 244. maddenin 2. fıkrasında düzenlenmiştir.

Bu kapsamda verinin başka bir yere gönderilmesinin yine verinin bütünlüğünü bozmayan fakat sistem içerisindeki veriye erişimi zorlaştıran bir hareket

olarak dar yorumlanabilmesi, bu haliyle de veriye erişimin engellenmesi kapsamına girebilecek bir olasılığın maddede ayrıca düzenlendiği sonucuna varılabilmesi mümkündür. Bu şekildeki dar yorum maddenin düzenleniş amacı ve düzenlemenin kapsamı ile bağdaşabilmektedir.

Her ne kadar verinin başka yere gönderilmesi ifadesi bu şekilde dar yorumlanabilecek olsa da bunun verinin transfer edilmesi olarak verinin ele geçirilmesi şeklinde yorumlanabilmesi karşısında, maddede değişiklik yapılarak ya bu ifadenin maddeden çıkartılması ve de maddenin bütünlüğünün sağlanması gerekmekte ya da 765. s TCK’de olduğu gibi verinin ele geçirilmesi düzenlenmek isteniyorsa, bunun ayrı bir maddede ele alınması gerekmektedir.

ii. Müdahalenin Konusu Olarak Bilişim Sistemi İçerisindeki Veri

244. maddesinin 2. fıkrasında düzenlenen veriye müdahale fiilleri bakımından tartışılması gereken diğer bir nokta, verinin disket vb. saklama aygıtlarında olması durumunda söz konusu suçların gerçekleşmiş sayılıp sayılamayacağıdır. Nitekim İngiltere’nin Bilgisayarın Kötüye Kullanılması Hakkında Kanunu (Computer Misuse Act 1990) bakımından bu sorun gündeme getirilmiş ve verinin bilgisayar içerisinde olmaması durumunda, veriye müdahale suçunun gerçekleşmeyeceği belirtilmiştir²⁸⁸. Alman Ceza Kanunun verinin ele geçirilmesine ilişkin 202a ve veriye müdahaleye ilişkin 303a maddesinde suçun unsurları arasında

²⁸⁸

LLOYD, s. 248.

verinin bilgisayar ya da bilişim sistemi içerisinde bulunmasına yer verilmemiştir. Siberaç Sözleşmesinin 4.maddesinde de veriye müdahale düzenlenmiş olup maddede verinin bilişim sistemi ya da Sözleşmede ifade edildiği şekliyle bilgisayar sistemi içerisinde bulunması şartı yer almamaktadır.

Birinci bölümde belirtildiği üzere, bilişim sisteminin genel amaçlı olması hususunun kabulü karşısında sadece veri saklama işlevine sahip olan bir aygıtın bu kapsamda düşünülmesi tartışılır bir durum olarak karşımıza çıkmaktadır. Nitekim söz konusu düzenleme 765 Sayılı TCK'nin 525/b 1. fıkrasında yer alan düzenlemeden farklı bir şekilde kaleme alınmıştır²⁸⁹. 765 Sayılı TCK'nin 525/b maddesindeki düzenlemede veriye müdahale bakımından verinin bilgileri otomatik işleme tabi tutan sistemde olması unsuruna yer verilmemesine rağmen, doktrinde, veri saklama aygıtlarında verilere söz konusu aygıtlarında bilgileri otomatik işleme tabi tutan sisteme dahil olduğu ve bu tür saklama aygıtlarında bulunan veriye müdahalenin de 525/b 1. fıkra düzenlenmiş suç oluşturacağı ifade edilmiştir²⁹⁰. Verinin ele geçirilmesi suçunun düzenlendiği 525a maddesinde, bilgileri otomatik işleme tabi tutmuş sistemden verinin ele geçirilmesi bakımından, kimi yazarlarca aynı görüş dile getirilmiştir²⁹¹. Buna karşın verinin ele geçirilmesi bakımından verinin saklama aygıtında olması halinde 525a 1. fıkra düzenlenmiş suç konusunu oluşturmayacağı da ifade edilmiştir²⁹².

²⁸⁹ 765 Sayılı TCK'nin 525b/1. maddesinde “...bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri... tahrip eden, veya değiştiren...” şeklinde bir hükme yer verilmiştir.

²⁹⁰ YAZICIOĞLU, *Bilgisayar Suçları*, s. 261.

²⁹¹ YAZICIOĞLU, *Bilgisayar Suçları*, s. 237; DÜLGER, s. 123.

²⁹² YENİDÜNYA – DEĞİRMENCİ, s. 261.

Maddede bilişim sistemindeki veriden bahsedilmesi karşısında, saklama aygıtında bulunan veriye müdahale bakımından, bilişim sisteminin verilen anlam ve kapsamı, veri saklama aygıtında bulunan verinin TCK'nin 244. maddesinde düzenlenen suçun konusunu oluşturup oluşturmadığı bakımından önemlidir. Veri saklama aygıtının genel amaçlı bir aygıt olmaması ve sadece veri saklama işlevine sahip olması karşısında sisteme bağlı olmayan bir aygıttaki veriye müdahalenin bu madde kapsamında düşünülmesi kanaatimizce olanaklı değildir.

4. Suça Etki Eden Nedenler

244. maddenin 3. ve 4. fıkralarında suça etki eden nedenler açısından iki ağırlatıcı nedene yer verildiği görülmektedir. Bunlardan birincisi, 244. maddenin 1. ve 2 fıkrasında düzenlenen fiillerin bir kamu kurum ya da kuruluşuna ya da banka veya kredi kurumuna ait bilişim sistemi üzerinde işlenmesidir²⁹³. Türk Ceza Hukukunda sistem ve veriye müdahale suçunun da yer aldığı bilişim suçlarının tarihsel gelişimi bakımından hukuki konularına göre ilgili bölümlerde düzenlenmemesi ve diğer suçlar ile bağlantısının tam olarak kurulamaması, bu tür eklemelerin yapılmasına yol açmaktadır. Nitekim bu suç, malvarlığına karşı suçlara arasında mala zarar verme suçu ile birlikte ya da mala zarar verme suçun özel şekli olarak düzenlenmiş olsaydı, mala zarar verme suçlarına ilişkin ağırlatıcı nedenlerle

²⁹³ Bkz, **KARAGÜLMEZ**, s. 192-193. *Dülger* ise bu ağırlatıcı nedenin maddede yer almasının nedenini kişisel bilgisayarlara müdahale sonucu ortaya çıkan zarar ile bu tür kurum ya da kuruluşların sistemlerine müdahale sonucu ortaya çıkan zarar arasında büyük fark olmasına dayandırmaktadır. **DÜLGER**, s. 243.

bağlantısının kurulması kolaylaşacak ve bu tür ek düzenlemelere gidilmesi önlenebilecekti.

Son fıkrada yer alan hüküm ise, genel olarak bilişim ya da bilgisayar sistemleri aracılığıyla yarar sağlama fiillerinin cezalandırılmasına yönelik bir düzenlemedir ve bu husus aşağıda ayrıca incelenecektir.

V. BİLİŞİM SİSTEMLERİ ARACILIĞIYLA YARAR SAĞLAMA

A. Genel Olarak

Bilişim sistemlerinin yaygın olarak kullanılması, ekonomik değerlerin gerçek değişimi yanında, ekonomik değerın bilgisayar sistemleri içerisinde veri olarak temsil edilmesi olanağı sonucunda, bu tür veriler üzerinde bilgisayar sistemleri aracılığıyla işlem yapılması suretiyle ekonomik değerin temsili değişimini olanaklı kılmıştır. Bu temsili değişim olanağı, aynı zamanda ekonomik değerin temsil edildiğı verilere ya da bu verileri barındıran bilişim sistemlerine müdahale aracılığıyla hukuka aykırı olarak ekonomik değerin elde edilmesi olanağını beraberinde getirmiştir²⁹⁴. Bu husus, Sibersuç Sözleşmesinde de yer verilen bilgisayar aracılığıyla

²⁹⁴ Ticari faaliyet gösteren sektörler ve özellikle bankacılık ve finans sektörleri bilgisayar sistemlerini en önce kullanan sektörlerdir. Parasal işlemlerin bilgisayar sistemleri aracılığıyla yapılması bu sektörlerde bilgisayar sistemlerine müdahale yoluyla çıkar sağlanması olanağını da beraberinde getirmiştir. Bilişim sistemleri aracılığıyla yarar sağlama suçunu kapsayan yeni suç tiplerinin ülke mevzuatlarına girmesinde ticari faaliyet gösteren sektörlerin bu sistemleri en erken ve yoğun olarak kullanması tarihsel neden olarak da gösterilebilir. Günümüzde ise ekonomik faaliyetlerin birçoğunun bilişim ya da bilgisayar sistemleri aracılığıyla yapılması ve özellikle İnternetin devreye girmesi bilişim ya da bilgisayar sistemlerine müdahale yoluyla haksız çıkar sağlanması olanaklarını arttırmaktadır. Bkz, **LLOYD**, s. 208.

dolandırıcılık suçu ile ilgili olarak Sözleşmenin açıklayıcı raporunda, teknolojik gelişim sonucu olarak kredi kartı dolandırıcılığı da dâhil olmak üzere dolandırıcılık fiilleri gibi ekonomik suçların işlenme olanaklarının hızla çoğaldığı ve bilgisayar sistemlerinde temsil edilen ya da yönetilen ekonomik değerlerin, geleneksel olarak cezai müeyyideler ile korunan malvarlığına yönelik ihlallere benzer şekilde manipülasyonların hedefi olduğu şeklinde ifade edilmiştir²⁹⁵. Bunun sonucu olarak, bilgisayar aracılığıyla para ya da diğer ekonomik değerlerin elde edilmesine yönelik bu tür fiillerin etkin olarak cezalandırılabilmesi amacıyla, söz konusu fiillere özgü düzenleme yapılması yoluna gidilmiştir. Bu açıdan, “*bilgisayar sistemi kullanarak yarar sağlamak*²⁹⁶”, “*yarar sağlama suçu*²⁹⁷”, “*bilgisayar marifetiyle dolandırıcılık*” olarak da adlandırılan bilişim sistemleri aracılığıyla yarar sağlama genel olarak malvarlığı kapsamında değerlendirilebilecek bir değer, bilişim ya bilgisayar sistemlerine müdahale edilmesi suretiyle hukuka aykırı olarak ele geçirilmesi fiillerini kapsayan bir terim olarak karşımıza çıkmaktadır.

Bilişim sistemi aracılığıyla yarar sağlama suçunu oluşturabilecek fiiller, genel olarak iki başlık altında toplanabilir. Bunlar verilere veya programlara müdahale aracılığıyla işlenen yarar sağlama halleridir. Verilere müdahale yoluyla yarar sağlama, bilgisayar sistemi içerisinde yer alan verilerin değiştirilmesi, erişilmez kılınması, silinmesi veya sisteme yeni verilerin eklenmesi şeklinde ortaya çıkmaktadır. Programlara müdahale yoluyla yarar sağlama ise bilgisayar sistemleri içerisinde var olan bir programa müdahale edilmesi ya da yeni bir program

²⁹⁵ Sözleşme Açıklayıcı Rapor, parag. 86,

²⁹⁶ **ÖNDER**, s. 509

²⁹⁷ **ERSOY**, s. 1177

eklenmesi suretiyle gerçekleştirilebilir²⁹⁸. Programlara müdahale yoluyla dolandırıcılık suçuna “salam tekniği” adı verilen yöntemi örnek göstermek mümkündür. Bu yöntemde hedef banka hesap ya da hesaplarından çok küçük miktarda paranın failin belirlediği hesaba aktarılması söz konusudur. Bu yöntemin başarısı yeterli miktarda hesaba ulaşılabilmesine ve hedef hesaplardan transfer edilen küçük miktardaki meblağların transfer edildiğinin hesap sahibi ya da diğer ilgili kişiler tarafından fark edilmemesine bağlıdır. Bilgisayar sistemi içerisindeki programlara müdahale edilmesi suretiyle ya da yeni bir program eklenmesi suretiyle bu yöntemin gerçekleştirilmesi mümkündür²⁹⁹.

Bilişim sistemleri aracılığıyla yarar sağlama, ya doğrudan bir faydanın sağlanması ya da dolaylı bir faydanın sağlanması amacına yönelik olabilir. Doğrudan faydanın sağlanmasına bir banka hesabından başka bir hesaba hukuka aykırı olarak para transfer edilmesini, dolaylı faydanın sağlanmasına ise ücreti karşılığı yararlanılabilen bir hizmetten başkasına ait şifreleri ele geçirerek yararlanılması ve böylece bedelin üçüncü kişiye ödettirilmesini örnek olarak göstermek mümkündür³⁰⁰.

Yukarıda aktarıldığı şekliyle, veri, program ve sisteme diğer müdahaleler yoluyla yarar sağlanması, genel olarak dolandırıcılık suçu çerçevesinde ele alınmış ancak bu suçun unsurlarının söz konusu fiilleri kapsayamamasından hareketle ayrı bir suç olarak düzenlenmiştir. Buna rağmen, bilişim sistemi aracılığıyla yarar sağlamaya ilişkin iki farklı nedenin ileri sürüldüğü görülmektedir. Aşağıda bunlara kısaca değinilecektir.

²⁹⁸ Ayrıntılı bilgi için bkz., **BAINBRIDGE**, s. 24 vd.

²⁹⁹ Salam tekniği ve diğer yöntemler için bkz., **PARKER**, s.126 vd. Ayrıca bkz., **YAZICIOĞLU**, *Bilgisayar Suçları*, s. 155; **BAINBRIDGE**, s.237; **LLOYD**, s. 208 vd; **SCHJOLBERG**, *Computer-Related Offences*, s. 14 vd.

³⁰⁰ **LLOYD**, s. 214 vd.

B. Bilişim Sistemleri Aracılığıyla Yarar Sağlamanın Ayır Bir Suç Olarak Düzenlenmesinin Nedenleri

1. Genel Olarak

Mameleki değerleri koruyan bir suç olarak ortaya çıkan bilişim sistemleri aracılığıyla yarar sağlama suçunun, ceza kanunlarında yer alan hırsızlık, dolandırıcılık gibi suçlardan ayrı olarak düzenlenmesine gerekçe olarak genellikle iki neden öne sürülmektedir. İlk gerekçe, özellikle bilişim sistemi aracılığıyla hileli ya aldatici hareketler yapılarak haksız çıkar sağlanmasında, hileli ya da aldatici hareketlerin kişiye karşı yapılmadığı, bilgisayar sistemi içerisinde yapıldığı bu nedenle hileli hareketin kişiye karşı yapılmasını öngören klasik dolandırıcılık suçunun unsurlarının bu tür fiilleri kapsamadığı yönündedir³⁰¹. İkinci gerekçe ise, ceza kanunlarında yer alan güveni kötüye kullanma, hırsızlık ve dolandırıcılık suçlarında elde edilecek şeylerin cisminin olması, yerine göre bir mal olması, bilgisayar bakımından ise durumun farklı bulunması olarak ifade edilmektedir³⁰².

³⁰¹ Bkz. **SIEBER**, s.97; **YAZICIOĞLU**, **Bilgisayar Suçları**, s. 268; **Hatice AKINCI – A. Emre ALIÇ – Cüneyd ER**, *Türk Ceza Kanunu ve Bilişim Suçları*, İnternet ve Hukuk, Der. Yeşim M. Atamer, s. 1. B., İstanbul, 2004, s.188; **Stein SCHJOLBERG**, Computer-Related Offences, s. 13, <http://www.cybercrimelaw.net/documents/Strasbourg.pdf>; **SCHJOLBERG** Harmonizing National Legal Approaches on Cybercrime, s. 15. Amerikan hukuku bakımından da bilgisayarla ilgili hileli fiiller yoluyla yarar sağlanmasında bu tür fiillerin halihazırda ceza mevzuatı içerisinde yer alan dolandırıcılık, sahtekarlık ya da zimmet gibi suçlar kapsamında değerlendirilebileceği fakat kimi durumlarda ise bunun mümkün olmadığı ifade edilmiştir. **WHARTON**, s. 244 vd.

³⁰² **DÖNMEZER**, **Kişilere ve Mala Karşı Cürümler**, s.618-619. Aynı yönde **DÜLGER**, **Bilişim Suçları**, s. 161. Ayrıca bkz., **SIEBER**, s.97,.

Yazıcıoğlu’da bu hususla ilgili olarak, “*Esasta Ceza Kanununda yer alan hırsızlık, dolandırıcılık, inancı kötüye kullanma gibi suçların oluşması için elde edilmesi gereken şeylerin taşınabilir ve cismi bulunan bir mal olması gereğinin ortaya çıkardığı sakıncalar bu suçun meydana getirilmesi ile bertaraf edilmektedir. Zira bilgisayarlarda yer alan bilgi ne fizik bir varlık içermekte, ne de taşınabilir bir mal bulunduğundan, bu cihazla işlenen fiilleri Ceza Kanunundaki mal aleyhine suçların konusu kabul edilmek mümkün olmamaktadır. Bu*

2. Kişiyeye Karşı Hileli Bir Hareketin Olmaması

Bilişim sistemlerinin yaygın olarak kullanılması sonucunda ekonomik değeerlerin bilişim sistemi içerisinde veri olarak temsil edilmesi ve temsili değışim yoluyla ekonomik değeerlerin el değıştirebilmesi olanağı, temsil edici veriye ve veri işleme faaliyetine, hukuka aykırı müdahalelerle ekonomik değeerlerin elde edilmesi olanağını ortaya çıkarmıştır. Bu doğrultuda bilişim sistemi aracılığıyla yarar sağlama, veri ya da programlara bu kapsamda bilişim sistemine çeşitli müdahaleler yapılması yoluyla malvarlığı kapsamında bir yarar sağlanması durumunu kapsamaktadır. Bu tür fiillerin gerçekleştirilmesi sonucunda ekonomik bir değeerin elde edilebilmesi nedeniyle malvarlığında haksız bir artışın sağlanabilmesi ve malvarlığına ilişkin zarar verilebilmesi olanağı ise bu tür fiillerin ayrı bir suç olarak düzenlenmesi sonucunu doğurmuştur.

Bu tür fiillerin ayrı bir suç olarak düzenlenmesinin nedeni veri, program ya da sisteme müdahale olarak ortaya çıkan hileli hareketlerin kişiyeye karşı yapılmadan malvarlığına ilişkin bir değeerin elde edebilir olmasıdır. Yukarıda aktarıldığı şekliyle, dolandırıcılık suçunda söz konusu olan kişiyeye karşı hileli hareketlerin gerçekleştirilmesi ve bu yolla bir kişinin aldatılması ya da hataya düşürülmesinin söz konusu olmaması, bunun yerini bilişim sisteminin işleyişine ya da veriye teknik bir müdahalenin alması, bilişim sistemi aracılığıyla yarar sağlamaya yönelik fiillerin ayrı bir suç olarak düzenlenmesine yol açmıştır.

sebeple, gerek bilgisayar marifetiyle işlenen, özellikle dolandırıcılık eylemleri marifetiyle elde edilmek istenen haksız kazançlar bu hükmle karşılanmak istemektedir.” demektedir. YAZICIOĞLU, Bilgisayar Suçları, s. 267. Ayrıca bkz., YAZICIOĞLU, Bilişim Suçlarının Genel Değerlendirilmesi, s. 398.

Yukarıda örnek olarak verilene salam tekniğine dönecek olursak, programa müdahale yoluyla yarar sağlama olarak nitelendirilebilen salam tekniği, hedef banka hesaplarından ilgili kişilerin rızası dışında belirli bir miktar paranın belirli bir hesaba aktarılması şeklinde oluşabilmektedir. Aslında burada gerçek bir para transferi söz konusu olmayıp, verinin içerdiği parasal bilgilerde değişiklik yapılması ve faile ait banka hesabındaki alacak miktarının arttırılması söz konusudur.

Bu tür bir fiilin, failin sahte bir talimat ile bankaya giderek banka çalışanına bu talimatın gösterilmesi suretiyle gerçekleştirilmiş olması durumunda her halde dolandırıcılık suçuna vücut verebilmektedir. Çünkü burada sahte talimat hileyi oluşturmakta ve bu hile ile banka çalışanına para transferine ilişkin işlem yaptırılabilir.

Aynı sonucu doğuran hileli hareketin yukarıda örnekte olduğu şekliyle sisteme müdahale yoluyla gerçekleştirilmesi halinde ise, hilenin kişiye karşı yapılması ve kişinin bu şekilde aldatılması söz konusu olmadığından dolandırıcılık suçu kapsamında değerlendirilmesi mümkün olmamaktadır.

Bu ve buna benzer şekillerde ortaya çıkan sorunların giderilmesi amacıyla çeşitli ülke ceza mevzuatları içerisinde bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlama fiillerini kapsayacak şekilde düzenlemeler yapılması yoluna gidilmiştir. Bu tür düzenlemelerin odak noktası, bilişim sistemi aracılığıyla yarar sağlama fiillerinde kişiye karşı bir hile yapılması sonucunda kişinin aldatılmasının söz konusu olmaması nedeniyle, kişiye karşı hileli hareketin yapılması, unsurunun yerini bilişim sisteminin işleyişine veya veriye müdahale edilmiş olması, unsurunun almış olmasıdır. Nitekim Alman ve İtalyan Ceza Kanunlarında yer alan ve bilgisayar

aracılığı ile dolandırıcılık suçu olarak adlandırılan suçları buna örnek olarak vermek mümkündür.

İtalyan Ceza Kanunu incelendiğinde söz konusu suçun klasik dolandırıcılık suçundan sonra gelmek üzere Kanunun 640 ter maddesinde düzenlendiği görülmektedir. 640 ter maddesinde, dolandırıcılığa ilişkin diğer unsurlar korunmuş, hile ve desise ile kişinin hataya düşürülmesi unsuru yerine genel olarak veri işleme faaliyetine ya da verinin kendisine müdahale edilmesi suçun unsuru haline getirilmiştir. İtalyan Ceza Kanunundaki bu düzenlemede sistemin işleyişine müdahale dolandırıcılık suçunun unsurunu oluşturan bir kişinin hileli hareketler sonucunda hataya düşürülmesinin yerini aldığı ifade edilmiştir³⁰³.

Alman Ceza Kanununda benzer bir yaklaşım sergilenmiş,, Kanunun dolandırıcılık suçunun düzenlendiği 263. maddesinden sonra gelmek üzere, 263a maddesinde, failin kendisine veya üçüncü kişiye hukuka aykırı yarar sağlaması amacıyla veriye ve veri işleme faaliyetine müdahale etmesi suç olarak düzenlenmiştir. Bu kanunda 263. maddede düzenlenen dolandırıcılık suçunun unsurunu oluşturan hileli hareketlerle kişinin hataya düşürülmesi ya da var olan hatadan yararlanılması şartı bilgisayar dolandırıcılığı bakımından aranmamıştır.

Bu açıdan incelendiğinde, bilişim sistemleri aracılığıyla yarar sağlama fiilleri, dolandırıcılık suçunun teknolojik görünümünü oluşturmakta ve bu durum klasik dolandırıcılık suçunun unsurlarının bu tür fiillere uygulanması bakımından sorunları da beraberinde getirmektedir. Dolandırıcılık suçu bakımından ortaya çıkan sorun ise,

³⁰³ Bkz, Felicia **BONANO**, La frode informatica, s. 10 <http://www.computerlaw.it/public/bonannofrodeinfo.pdf>.

veri ve veri işleme faaliyetine yönelik hileli hareketlerin kişiye karşı yapılmaması şeklinde karşımıza çıkmaktadır. Söz konusu sorunun çözümü ise, ceza mevzuatları içerisinde dolandırıcılık suçunun yanında bilgisayar dolandırıcılığı olarak adlandırılan suçun düzenlenmesi şeklinde olmuştur.

Kişiye karşı hileli hareketlerin olmaması, Türk Ceza Hukukunda başka bir suç bakımından da dile getirilmiştir. Nitekim karşılıksız yararlanma suçu, tartışmaya konu olan başka bir suçtur. 765 Sayılı TCK'nin 521b maddesinde düzenlenmiş olan otomatların kötüye kullanılmasında da dolandırıcılık suçunun otomatlara karşı işlenebilmesinin mümkün olmadığı çünkü burada bir kişinin hile ve desise ile kandırılmasından ve hataya düşürülmesinden bahsedilemeyeceği, teknik anlamda aldatılmış olmasının söz konusu olmayacağı ifade edilmiştir³⁰⁴.

1997 Öntasarısının 218. maddesinde ve 12.05. 2003 tarihinde TBMM'ye sunulan Türk Ceza Kanunu Tasarısında da (223. m.) yer verilmiş olan bu suçun, Öntasarıda ve de Tasarıda yer alan gerekçesi incelendiğinde, bilişim sistemleri aracılığıyla yarar sağlama bakımından da gündeme geldiği görülmektedir. Söz konusu suça ilişkin olarak gerekçedeki örnek bu açıdan önemlidir. Nitekim Öntasarıdaki gerekçede, otomatik cihazlardan birtakım hileli usullerle faydalanmanın çağımızda sık sık görülen bir suç şekli olduğu, hileli hareketlerin elektronik cihazlara karşı da yöneltilebileceği ifade edilmiş ve devamında “*Mesela bir bankanın elektronik cihazlarını programlamakla görevli yükümlü memuru, yanıltıcı bilgileri alete vermek suretiyle belirli bir hesapta mevcut olmayan bir paranın bulunduğu yolunda ilgili memura bilgi verilmesini ve bu suretle bu hesaptan para*

³⁰⁴ Bkz., Mustafa Ruhan **ERDEM**, Türk Hukukunda Karşılıksız Yararlanma Suçları, Ankara, 1996, s. 99 vd; **ÖNDER, Şahıslara ve Mala Karşı Cürümler**, s. 485 vd;

*çekmek isteyen kimseye ödeme yapılmasını veya başka bir şubeye ya da bankaya havale gönderilmesini sağlayabilir*³⁰⁵.” örneği verilmiştir. Aynı gerekçeye Tasarıda da yer verilmiştir. TCK’de de bu suç 163. maddede düzenlenmiş Kanunun gerekçesinde ise yukarıda verilen örnek yer almamıştır³⁰⁶.

Otomatların kötüye kullanılmasının dolandırıcılık suçunu oluşturmayacağına, bu nedenle ayrı bir düzenleme yapıldığına ilişkin gerekçenin, bilişim sistemleri aracılığıyla yarar sağlama ile ilgili gerekçeyle paralel olduğu görülmektedir. Her iki suçun düzenlenmesinde gerekçe, yukarıda belirtildiği üzere, kişiye karşı bir hilenin ve kişinin aldatılmasının söz konusu olmadığıdır. Bu açıdan Öntasarı ve de Tasarıda yer alan örnek, kişiye karşı hilenin söz konusu olmaması bakımından kısmen geçerlidir³⁰⁷. Aynı zamanda bu örnek genel olarak bilgisayar aracılığı ile yarar sağlamanın dolandırıcılığın özel şekli olarak düzenlenmesinde, gerekçe olarak ileri sürülmektedir.

Bu husus, TCK’nin hazırlık çalışmaları sırasında da başka bir suç kalıbı içinde düşünülmesine rağmen, bilişim sistemi kullanılarak yarar sağlamada

³⁰⁵ Türk Ceza Kanunu Öntasarısı, (1997) T.C. Adalet Bakanlığı Yayın İşleri Daire Başkanlığı, Özel Seri: 3, s 252.

³⁰⁶ TCK madde gerekçelerinde bu suç ile ilgili olarak “...*Otomatlar aracılığı ile satışa sunulan hizmetlerden, otomatın teknik işleyişini devre dışı bırakan müdahalelerle, bedeli ödenmeksizin yararlanılması durumunda, ortada bir taşınabilir mal bulunmadığı için, hırsızlık suçu oluşmayacaktır. Örneğin, toplu taşıma sistemlerinde yolcuların geçişlerini kontrol eden otomatlara müdahale edilmek suretiyle ücret ödenmeksizin yolculuk yapılması durumunda, karşılıksız yararlanma suçunun oluştuğunu kabul etmek gerekir. Burada, bir hilenin varlığından söz edilemez. Çünkü bu durumda herhangi bir kişi aldatılmamaktadır. Yapılan müdahale ile bir otomatın teknik işleyişinin devre dışı bırakılması durumunda, bir hilenin varlığından söz edilemez. Çünkü, dolandırıcılık suçu açısından hilenin varlığı için muhatabın mutlaka insan olması gerekir.*” denmektedir. Gerekçe için bkz., Güney, s. 477

³⁰⁷ Örnekte, programa müdahale sonrasında memura bilgi verilmesi ve bu şekilde para çekilmesi ya da havale gönderilmesini sağlamaktan bahsedilmektedir. Bu açıdan bu örnek bir kişiyi aldatacak nitelikte hileli hareketlerin olması karşısında yani memurun hesabın ve hesapta paranın varlığı konusunda aldatılması bakımında dolandırıcılık suçu kapsamında değerlendirilebilmektedir.

dolandırıcılık suçunun oluşabilmesi bakımından kişiye karşı hileli hareketlerin söz konusu olmadığı dolaylı olarak dile getirilmiştir.

3. Bilişim Sistemleri Aracılığıyla Yarar Sağlama Suçu Olarak Eşya Kapsamında Değerlendirilemeyen Verinin Elde Edilmesi

Yukarıda belirtildiği üzere, ceza kanunlarında yer alan hırsızlık, dolandırıcılık, güveni kötüye kullanma gibi suçlarda elde edilecek şeyin cisminin olması, bilişim sistemleri aracılığıyla yarar sağlama durumunda ise, belirli bir şeyin elde edilmesinden çok verinin ele geçirilmesinin söz konusu olduğu, bu nedenle buna ilişkin özel bir düzenlemeye ihtiyaç duyulduğu kimi yazarlarca ifade edilmiştir. Bu husus, özellikle klasik dolandırıcılık suçu kapsamında ele alınmış ve aktarılan bu gerekçe nedeniyle de klasik dolandırıcılık suçunun unsurlarının gerçekleşmediği ifade edilmiştir. Aşağıda görüleceği üzere bu hususlar, 765 Sayılı TCK'nin 525/b maddesinin düzenleniş gerekçesi olarak da ileri sürülmüştür.

Söz konusu gerekçe, *Sieber'in* de ifade ettiği üzere, geleneksel ceza kanunlarının görülebilir ya da elle tutulabilir eşya üzerine genel olarak inşa edildiği, fakat sosyo-ekonomik dönüşüm sonucu, görülemeyen ya da elle tutulamayan değerlerin ve özellikle bilgi ve enformasyonun öneminin arttığı ve bunun klasik olarak eşyanın korunmasına ilişkin hükümlerle korunamayacağı genel yaklaşımı ile paralellik arz etmektedir³⁰⁸.

³⁰⁸ **SIEBER**, s.39. Yazar, enformasyonun ve diğer görülemeyen şeylerin korunmasının geleneksel ceza kanunlarında var olduğunu fakat 20. yy'ın ortalarına kadar B.n bir rol oynamadığını belirtmektedir. a.g.e., s.39, dipnot 16.

Aynı şekilde, yukarıda incelenen, verinin ele geçirilmesi ve veriye müdahale bakımından verinin eşya olarak kabul edilmemesi karşısında bunların ele geçirilmesinin hırsızlık suçu kapsamında değerlendirilip değerlendirilemeyeceği hususu ile yakından ilgilidir. Nitekim, verinin ele geçirilmesi konusunda da incelendiği üzere, klasik hırsızlık suçu kapsamında değerlendirilemeyen verinin ele geçirilmesine ilişkin, ABD’de federe devletlerde, veri mal/eşya kapsamına sokulmuş ve veri hırsızlığı olarak adlandırdığımız suç ceza mevzuatı içerisine girmiştir. Verinin mal/eşya kapsamında değerlendirilemeyeceği ve bu nedenle hırsızlık suçunun konusunu oluşturamayacağına ilişkin soruna çözüm bu şekilde getirilmek istenmiştir. Verinin eşya/mal olarak kabul edilmediği ülkelerde ise, bu sorun verinin sır kapsamında korunması suretiyle çözüme kavuşturulmak istenmiştir. 765 Sayılı TCK bakımından da sorun 525/a maddesinin düzenlenmesi suretiyle giderilmeye çalışılmıştır³⁰⁹.

Bu doğrultuda incelendiğinde, verinin eşya/mal olmaması karşısında bunların ele geçirilmesinin klasik hırsızlık suçunu oluşturmayacağı, bu nedenle bilişim sistemi aracılığıyla yarar sağlama suçuna yer verildiği gerekçesi gerçeği yansıtmamaktadır. Söz konusu sorun, genel olarak veri hırsızlığı ya da verinin ele geçirilmesi şeklindeki suçlar ile çözümlenmeye çalışılmıştır.

Yetkili kullanıcının bilgisayar sistemlerinin kaynaklarını ve bu sistemler aracılığıyla sunulan hizmetleri kişisel çıkarı amacıyla kullanması durumu ise, güveni kötüye kullanma suçu ile ilişkili bir suç olarak düzenlenmek istenmiştir. Bu husus,

³⁰⁹ Aynı yönde AKINCI, s. 245.

yetkisi olmayan bir kişinin bilgisayarın ve bilgisayarın sunduğu hizmetlerinin³¹⁰ kişisel amaçla kullanılması suçların düzenlenmesine yol açmıştır³¹¹.

Verinin eşya/mal olmaması, dolandırıcılık suçunda elde edilecek şeyin cisminin bulunması gerektiği gerekçesi de dolandırıcılık suçunun unsurları incelendiğinde, 765 Sayılı TCK ve TCK bakımından gerçeği yansıtmamaktadır.

Bilindiği üzere dolandırıcılık suçu, hile ve desise yapılması suretiyle kişinin rızasının sağlanması sonucunda suçun pasif süjesinin ya da üçüncü bir kişinin malvarlığında azalma failin ya da üçüncü bir kişinin malvarlığında çoğalma fiillerini kapsamaktadır. Kanun koyucu bu suç için suçun pasif süjesi ya da üçüncü kişiye yönelik bir zararın, failin ya da üçüncü kişi lehine de bir yararın oluşması şartını aramıştır.

Malvarlığına ilişkin zarar ve yarar ise, belirli bir malın el değiştirmesini de kapsayan fakat bundan daha geniş bir kavram olarak karşımıza çıkmaktadır. Nitekim doktrinde malvarlığına ilişkin her türlü tasarrufun dolandırıcılık suçu kapsamında yararı oluşturabileceği ifade edilmiş; yararın kapsamı, kimi yazarlar tarafından sadece ekonomik değerlerin oluşturduğu³¹², kimi yazarlar tarafından ise ekonomik

³¹⁰ Örnek olarak bkz, Alaska Kanunu Bölüm 11.46.200
<http://nsi.org/Library/Compsec/computerlaw/Alaska.txt>

³¹¹ WHARTON, 251 vd.

Önder, tarafından, 525/b 2. maddesine ilişkin olarak verdiği “ Benzer bir olay Amerika’da meydana gelmiş, bir bilgisayarda çalışan 17 mühendis yaptıkları özel anlaşmalarla bilgisayardan, dışarıya özel hizmet vererek yarar sağlamışlardır.” örneği bu kapsamda değerlendirmek mümkündür. ÖNDER, s. 510

³¹² DÖNMEZER, Kişilere ve Mala Karşı Cürümler, s. 467; TEZCAN, Teorik ve Pratik Ceza Özel Hukuku, s. 476-477.

değer yanında manevi bir değerinde bu söz konusu yararı oluşturabileceği vurgulanmıştır³¹³.

Toroslu, dolandırıcılık suçundan bahsedilebilmesi için, zorunlu olan malvarlığına ilişkin tasarrufun konusunun, malvarlığının herhangi bir unsuru olabileceğini, taşınır mallar ve taşınmaz mallar yanında her türlü hakların ve şahsi hizmetlerin malvarlığına ilişkin tasarrufun konusunu oluşturabileceğini belirtmiştir³¹⁴. Bu açıdan dolandırıcılık suçunda belirli bir malın elde edilmesinden çok malvarlığı kapsamında bir yararın elde edilmesi ve bir zararın meydana gelmesi söz konusu olmaktadır³¹⁵.

Malvarlığında bir artış olarak alacak hakkının doğması ya da bu hakkın terki örneklerinde olduğu üzere, yararın sağlanması, zorunlu olarak bir malın el değiştirmesi anlamına gelmemektedir³¹⁶.

Hal böyle olunca, bilgisayar aracılığıyla yarar sağlama suçunun düzenlenmesine ilişkin, dolandırıcılık suçunun unsuru olarak malın elde edilmesinin zorunlu olarak aranmadığı, 765 Sayılı TCK ve TCK bakımından, verinin eşya olarak

³¹³ **TOROSLU, Ceza Hukuku Özel Kısım**, s. 183; **ÖNDER**, s. 379; Doğan **SOYASLAN**, Ceza Hukuku Özel Hükümler, Gözden Geçirilmiş 5. B., Ankara, 2005, s. 345. *Erem* yarar kavramının geniş anlama sahip olduğunu, herhangi bir şeyin, hukuki sonuç doğurmaya elverişli bir belgenin, şahsi hizmet ya da bir şeyin sadece kullanılmasın suçun unsuru olan yarar kapsamına gireceğini ifade etmiştir. Faruk **EREM**, Dolandırıcılık, Ankara Üniversitesi Hukuk Fakültesi Yayınları: 101, Ankara, 1956, 17.

³¹⁴ **TOROSLU, Ceza Hukuku Özel Kısım**, s. 180.

³¹⁵ **TEZCAN, Teorik ve Pratik Ceza Özel Hukuku**, s. 478-479

³¹⁶ Bunu bir örnek ile de açıklayacak olursak, İnternet Bankacılığı adı verilen bankacılık hizmeti, bir sistemde, başkasının şifre vs kullanılarak bağlanması suretiyle, kişiye ait hesaptan kişinin kendi hesabına para transferinde bulunması durumunda, failin o an için bu işlem ile taşınır bir malı elde etmesi söz konusu olmamaktadır. Fakat failin kendi mevduat hesabındaki miktarı arttırmış olması, bankaya karşı bir alacak hakkı doğurmaktadır.

kabul edilmemesi sonucunda, elde edilmesinin dolandırıcılık suçları kapsamında değerlendirilemeyeceği yönündeki gerekçe yerinde değildir.

Sisteme ve veriye birtakım hileli fiiller ile müdahale sonucunda yarar sağlanmasında özellikle kıta Avrupası bakımından sorun, ekonomik yarar sağlama amacıyla sisteme ve veriye çeşitli müdahaleleri içeren hareketler sonucunda yarar sağlanmasının, klasik dolandırıcılık suçu kapsamında değerlendirilip değerlendirilemeyeceği noktasında ortaya çıkmaktadır. Sorun ve sonucunda yeni bir suçun düzenlenmesindeki neden, kişiye karşı hile ya da desise içeren bir hareketin olmaması merkezinde toplanmaktadır.

C. Türk Ceza Hukukunda Bilişim Sistemleri Aracılığıyla Yarar Sağlama

Suç

1. Genel Olarak

Türk Ceza Hukukunda, bilişim sistemleri aracılığıyla yarar sağlamaya ilişkin düzenlemede, suçun düzenlendiği yer ve suçun unsurları bakımından, Alman ve İtalyan Ceza Kanunlarında tercih edilen yöntemden farklı bir yöntemin benimsendiği görülmektedir. Bu kapsamda, 765 Sayılı TCK'nin 525/b 2. fıkrasında yer alan, *“Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye...”* hükmü ile, değişik adlar altında incelenmekle birlikte, bilişim aracılığıyla yarar sağlama fiilinin düzenlendiği ifade edilmiştir. Bu açıdan, 765 Sayılı TCK'de bilişim sistemi aracılığıyla yarar sağlama, dolandırıcılık suçu esas alınarak bir zarar suçu olarak düzenlenmemiş aynı zamanda

kişiy e karşı hileli hareketin yerine, sisteme ve veriye müdahale edilmesi şeklinde teknik hile olarak adlandırılacak hareketlerin yer aldığı bir suç olarak düzenlenmemiştir. Bunun yerine bilişim sistemi kullanılması suretiyle her türlü hukuka aykırı yarar elde edilmesi suç olara düzenlenmiştir³¹⁷.

TCK’de ise, 765. S. TCK’nin 525/b 2. fıkrasındaki düzenlemeden farklı bir yöntem tercih edilerek, 244. maddenin son fıkrasında, “*Yukarıda fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması...*” şeklinde, 244. maddede yer alan sisteme ve veriye müdahale suçunun ağırlatıcı nedeni olarak düzenlenmiştir. 765 Sayılı TCK’den farklı olarak, TCK’nin 152. maddesinde bilişim sisteminin kullanılması suretiyle hırsızlık fiili, hırsızlık suçunun ağırlatıcı nedeni, aynı şekilde TCK’nin 158. maddesinde, bilişim sistemlerinin kullanılması suretiyle dolandırıcılık fiili, dolandırıcılık suçunun ağırlatıcı nedeni olarak düzenlenmiştir.

³¹⁷ Girişte belirtildiği üzere bilişim suçlarına ilişkin düzenlemelerde Fransız Ceza Kanunu örnek alınmıştır. Bu durum özellikle bilgisayar aracılığıyla yarar sağlama suçı bakımından suçun unsurlarına ilişkin klasik dolandırıcılık suçundan farklı bir düzenleme yapılmasına yol açmıştır. Bilindiği üzere hem 765 Sayılı TCK’nin 503. maddesinde hem de TCK’nin 157. maddesinde düzenlenen dolandırıcılık suçı bakımından suçun tamamlanabilmesi için sadece yararın gerçekleşmiş olması yetmemekte bunun yanında zararın da gerçekleşmiş olması gerekmektedir. Hal böyle iken, özellikle eski Fransız Ceza Kanununda düzenlendiği haliyle, dolandırıcılık suçunda zararın gerçekleşmiş olma şartı suçun unsurları arasında sayılmamıştır. Bu açıdan dolandırıcılık suçunun malvarlığı üzerindeki teslim ile tamamlanmış sayılacağı ifade edilmiştir. Bunun sonucunda zararın oluşması suçun unsurunu oluşturmamaktadır. Bu konuda bkz., Sami **SELÇUK**, Dolandırıcılık, 1. B., 1982, s. 81. vd. Ayrıca bkz., **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 469-470. *Dönmezer*, yeni Fransız Ceza Kanunun 313-1. maddesinde düzenlenen dolandırıcılık suçunda zarar görülmesinin suçun unsuru olarak düzenlendiğini belirtmiştir. a.g.e., s 470.

Bu nedenle 765 Sayılı TCK’nin 525b/2. maddesinde düzenlenen bilgisayar aracılığıyla yarar sağlama suçunda, suçun unsuru arasında zararın oluşmasının aranmamasının, bu maddenin eski Fransız Ceza Kanununda dolandırıcılık suçı ile uyumlu bir şekilde düzenlenen bilgisayar aracılığıyla yarar sağlamaya ilişkin maddenin 765 Sayılı TCK’ye aktarılmasından kaynaklandığını söylemek mümkündür.

Ayrıca, 765 Sayılı TCK'nin 525/b maddesinin bu Kanuna eklenmesinden sonra, 525/b 2. fıkra kapsamında olduğu belirtilen ve bu haliyle de yargı kararlarına konu olan banka ve kredi kartlarının kötüye kullanımı, TCK'nin 245. maddesinde özel olarak düzenlenmiştir.

Yukarıda aktarıldığı şekliyle bilişim sistemleri aracılığıyla yarar sağlamaya ilişkin hükümlerin, özellikle 525/b maddesinin 2. fıkrasının, uygulama içerisinde ortaya çıkan sorunlar kapsamında şekillendirilmiş olması ve ayrıca “*Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı*”nın 23. maddesinde³¹⁸ benzer bir düzenlemeye yer verilmek istenmesi nedeniyle, öncelikli olarak 765. s. TCK'nin 525/b 2. fıkrasının incelenmesi gerekmektedir.

2. Bilgileri Otomatik İşleme Tabi Tutmuş Sistemi Kullanarak

Hukuka Aykırı Yarar Sağlama (765 Sayılı TCK 525b/2)

a. Genel Olarak

Yukarıda belirtildiği üzere bilişim sistemleri aracılığıyla hukuka yarar sağlama fiillerinin, Türk Ceza Hukukunda ilk olarak 765 Sayılı TCK'nin 525/b 2. fıkrasında düzenlendiği yazarlarca ifade edilmiştir.

Dönmezer, bu fıkra düzenleneni suçun konulmasındaki temel nedeninin, hırsızlık dolandırıcılık gibi suçların oluşması için alınacak ve elde edilecek şeylerin

³¹⁸ Tasarının ilgili 23. maddesi şu şekildedir: **MADDE 23** – “(1) *Bilişim ağı aracılığı ile kendisi veya başkası lehine haksız yarar sağlayan kimseye, fiilin başka bir suç oluşturmaması hâlinde, iki yıldan beş yıla kadar hapis ve bin günden ikibin güne kadar adli para cezası verilir.*”

cisminin ve yerine göre bir mal olması, bilgisayar bakımından ise durumun farklı olmasından kaynaklandığını belirtmiştir³¹⁹. Aynı şekilde *Yazıcıoğlu Dönmezer*'in ifade ettiği hususları tekrar etmiş ve devamında “*Zira bilgisayarlarda yer alan bilgi ne fizik bir varlık içermekte, ne de taşınabilir bir mal bulunduğundan, bu cihazla işlenen fiilleri Ceza Kanunundaki mal aleyhine suçların konusu kabul edebilmek mümkün olmamaktadır. Bu sebeple, gerek bilgisayar marifetiyle işlenen, özellikle dolandırıcılık eylemleri marifetiyle elde edilmek istenen haksız kazançlar bu hükümle karşılanmak istenmektedir.*” ifadesine yer vermiştir³²⁰.

Bunun yanında, sisteme yanlış veri girilmesi gibi teknik hilelerin kullanılması ile sistemin istenildiği gibi çalıştırılmasının bilgisayar dolandırıcılığını oluşturduğu; sistemin kullanılması ile hukuka aykırı yarar sağlanmasında ise özel olarak sistemin istenildiği gibi çalıştırılması değil, sistem aracılığıyla bir kişiyi hataya düşürerek yarar sağlamanın bilgisayar marifetiyle dolandırıcılık suçunu oluşturduğu, şeklinde bir ayırım yazarlarca yapılmıştır. Buna göre birinci durum, 765 Sayılı TCK'nin 525/b 1. maddesinde suçu oluştururken, ikinci durum ise aynı maddenin 2. fıkrasında düzenlenen suçu oluşturmaktadır³²¹.

Dönmezer, sistemi kendi normal işleyişi içinde bırakmayarak ve böylece sistemi oluşturan unsurları etkileyerek netice almanın maddede suçun maddi unsuru olarak düzenlendiğini; kendisi veya başkası için ekonomik yarar sağlamanın³²² suçun neticesini oluşturduğunu; haksız yarar sağlama özel kastının var olması

³¹⁹ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 617-618, **DÜLGER**, s. 163.

³²⁰ **YAZICIOĞLU, Bilgisayar Suçları**, s. 267

³²¹ **AKINCI**, s. 244-245.

³²² *Ersoy* ise yarar sağlamanın geniş bir kavram olduğunu, maddi, manevi, kültürel her türlü hakların bu madde kapsamında değerlendirildiğini ifade etmiştir. **ERSOY**, s.178.

gerektiğini belirtmiştir³²³. *Yazıcıoğlu*, 765 Sayılı TCK'nin 525b/ 2. fıkrasında serbest hareketli bir suçun düzenlendiğini ifade etmiştir³²⁴

Dikkat edilecek olursa, 765 Sayılı TCK'nin 525/b 2 .fıkrasında yer alan suçun gerekçesi, yukarıda aktarıldığı gibi, bilişim sistemleri aracılığıyla yarar sağlamada elde edilen şeyin mal olarak kabul edilmemesi şeklinde ifade edilmektedir.

Yazarların belirttiğinin aksine sorun, bilişim sistemi aracılığıyla yarar sağlamada elde edilen şeyin niteliğinde yatmamakta, özel olarak dolandırıcılık suçunun unsurlarında ortaya çıkmaktadır. Bu açıdan incelendiğinde, bu maddenin genel bir düzenleme olarak suçun unsurunun birçok fiili kapsayıcı şekilde kaleme alınması bu suçun uygulanma alanını genişletmiş ve aşağıda görüleceği gibi banka kartı ile para çekilmesi şeklinde ortaya çıkan ve hırsızlık suçu kapsamına giren fiillerin bu suç kapsamında değerlendirilmesine yol açmıştır. Bu nedenle, suçun düzenlenmesine yönelik olarak ileri sürülen gerekçeler, suçun düzenlemesine ilişkin sorunlara ve nedenlere işaret etmekten çok suçun kapsamında ortaya çıkan sorunlara işaret etmektedir.

Nitekim *Ersoy*, konuyu bu açıdan ele almıştır. Yazar, yarar sağlamak kavramını ekonomik yararlar dışındaki yararları da kapsayacak şekilde yorumlamış ve yarar sağlamanın bu şekilde geniş bir anlama sahip olması karşısında özellikle hırsızlık, dolandırıcılık, güveni kötüye kullanma gibi “maddi çıkar” sağlama fiillerinin bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde nasıl bir çözüme ulaşılacağını sorgulamıştır. Yazar 525/b maddesinde yer alan düzenlemenin

³²³ **DÖNMEZER, Kişilere ve Mala Karşı Cürümler**, s. 618. Aynı yönde **YAZICIOĞLU, Bilgisayar Suçları**, s. 271-273, **DÜLGER**, s. 166 vd.

³²⁴ **YAZICIOĞLU, Bilgisayar Suçları**, s. 271. Aynı yönde **DÜLGER**, s. 166.

hırsızlık, dolandırıcılık ve de güveni kötüye kullanmaya göre özel bir düzenleme olduğunu bu sebeple söz konusu maddenin uygulanması gerektiği sonucuna varmıştır³²⁵.

Ünver de suçun kapsamına ilişkin soruna işaret etmiş ve söz konusu maddenin hırsızlık, dolandırıcılık, güveni kötüye kullanma gibi birçok suçu kapsayan bir düzenleme olduğunu, bu şekliyle her türlü haksız eylemi cezalandıran genel bir hüküm olduğundan belirginlik ve kanunilik ilkesine aykırılık itirazların ileri sürülebileceğini ifade etmiştir³²⁶.

525b/2. fıkrasında düzenlenen suça ilişkin aşağıda ayrıca değinilecek olan Yargıtay kararları incelendiğinde, düzenlemenin, bir bütün olarak sadece malvarlığına karşı işlenen diğer suçların kapsamına girmeyen fiillere ilişkin olarak ortaya çıkan bir eksikliği gidermeye yönelik bir sonuç doğurmadığı görülmektedir. Söz konusu madde daha çok daha önce hırsızlık dolandırıcılık ya da emniyeti suiistimal olarak nitelendirilebilecek fiilleri kapsayan bir sonuç doğurmuştur.

5237 Sayılı TCK'nin 244. maddesinin son fıkrasında ve 245. madde düzenlenen suçların, 765 Sayılı TCK'nin 525b/2. maddesinin Türk Ceza Hukukunda özellikle uygulamada ortaya çıkardığı sorunlar esas alınarak düzenlenmesi ve ayrıca Tasarıda da 765 Sayılı TCK'nin 525b 2. fıkrasındaki suça benzer bir düzenlemeye yer verilmesi sebebiyle, 765 Sayılı TCK'nin 525b/ 2. maddesinin uygulamadaki görünümünün değerlendirilmesi gerekmektedir. Aşağıda

³²⁵ **ERSOY**, s. 178-179.

³²⁶ Yener **ÜNVER**, *Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi*, İHFM, C. LIX, S. 1-2, 2001, s. 98-99. Aynı yönde **DÜLGER**, s. 166-167. Aksi yönde **DÖNMEZER**, *Kişilere ve Mala Karşı Cürümler*, s. 618.

765 Sayılı TCK'nin 525b/2. maddesine ilişkin Yargıtay kararları bu nedenle ayrıntılı olarak incelenecektir.

b. Haksız Olarak Ele Geçirilen Banka Kartı Kullanılması Suretiyle “ATM”lerden Para Çekilmesi

765 Sayılı TCK'nin yürürlükte bulunduğu dönemde bilişim suçları bakımından en çok uygulama alanı bulan hüküm, 525/b 2. maddesidir. Yargıtay kararları incelendiğinde, 525/b 2. fıkrasının, 765 Sayılı TCK'de bilişim sistemlerinin kullanılmasıyla ortaya çıkan boşluğu doldurmadan çok, özellikle banka ve kredi kartlarının kullanılması suretiyle haksız yarar sağlama fiillerine yönelik olarak gündeme geldiği görülmektedir. Söz konusu fiiller bakımından, malvarlığına karşı diğer suçlar ile söz konusu suçun kapsamına ilişkin tartışmalara neden olan bir işleve bürünmüştür.

Nitekim kısaca “atm” olarak da adlandırılan otomatik para çekme makinelerinden başkasına ait kart ile para çekilmesi fiilinin 765 Sayılı TCK'nin 493/2. maddesindeki suçu mu yoksa 765 Sayılı TCK'nin 525/b 2. fıkarda düzenlenen suçu mu oluşturduğu yargı kararlarında tartışma konusu olmuştur.

Yargıtay 6. CD, kararlarında, bu tür fiillerin 765 Sayılı TCK'nin 493/2. maddesinde düzenlenen suçu oluşturduğunu³²⁷, bu fiillerin işlenmesinde banka

³²⁷ “ Müştekinin bankomat kartını ele geçiren sanığın, müşterinin bankadaki hesabından bu kart ile para çekmekten ibaret eyleminin, bankomat kartının alet olarak kullanılması karşısında, TCY'nın 493/2. maddesindeki suçu oluşturduğu gözetilmeden aynı yasanın 524/b-2. maddesi ile uygulama yapılması...” Yargıtay **6. CD E. 1998/3880 K. 1998/4044 T. 22.4.1998** <http://www.kazanci.com.tr/kho2/ibb/files/6cd-1998-3880.htm>

kartının alet olduğunu ifade etmiştir. 6 CD, bu yöndeki kararlarında, otomatik para çekme makinelerinden para çekilmesi fiilini, hırsızlık olarak nitelendirmiş, banka kartının kullanılmasını, 765 Sayılı TCK'nin 493. maddesinin 2. fıkrasında düzenlenen anahtar veya diğer aletler kavramına dahil olduğunu ifade etmiştir.

Yargıtay Ceza Genel Kurulu ise, 2000 yılında verdiği bir kararında, banka kartı ile “atm” den para çekilmesi fiili ile ilgili olarak banka kartının anahtar ya da sair alet kavramına dahil olup olmadığı ve de bilişim sisteminin kullanılmış olup olmadığını tartışmıştır.

Kararda banka kartının anahtar veya sair alet olup olmadığı ve bilişim sisteminin kullanılıp kullanılmadığına ilişkin olarak şu görüş ortaya çıkmıştır: *“TCY.sının geleneksel, nitelikli hırsızlık suçuna ilişkin 493/2. maddesinde taklit anahtar, sair alet veya sahibinin terk ettiği veya kaybettiği anahtarı elde ederek yahut haksız yere elde bulundurulmuş asıl anahtarla bir kilidin açılması suretiyle hırsızlık suçunun işlenmesi yaptırım altına alınmış, sair aletin ne olduğu hususunda bir tanımlamada bulunulmamıştır. Ancak, uygulama ve öğretide bir kilidi açan her türlü aletin (görünüşü ve özelliği ne olursa olsun) sair alet olarak değerlendirilmesi gerektiği kabul edilmektedir. Kısaca ATM olarak da adlandırılan Automated Teller Machine sisteminin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura gereksinim vardır, bunlardan birincisi kart diğeri ise kullanıcı şifresidir. Bu*

“Müştekiye ait kredi kartını ele geçiren sanığın, bu kartı kullanarak 2 gün ara ile ATM'den para çekmekten ibaret eyleminin, kredi kartının alet olarak kullanılması karşısında, TCK'nin 493/2, 80. maddelerindeki suçu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek aynı yasanın 525/b-2. maddesi ile uygulama yapılması...” Yargıtay **6. CD E. 1998/10848 K. 1998/10939 T. 26.11.1998** <http://www.kazanci.com.tr/kho2/ibb/files/6cd-1998-10848.htm>

iki araca sahip olmadan, bir bilgi işlem biriminin parçası olan ve ana sisteme bağlı bulunan ATM makinelerini kullanma olanağı yoktur. Belirtilen karta ve şifreye sahip olan kişi, kartı makineye takıp şifreyi de yazdıktan sonra işlem sürecini başlatabilir. Ancak, kartı elinde bulunduran kişinin makine vasıtasıyla sisteme verdiği komutların yerine getirilebilmesi için ana kumanda merkezinin de bu komutları onaylaması gerekmektedir. Örneğin nakit para çekilmek istendiğinde hesapta para yoksa veya günlük çekme limiti dolmuş yada herhangi bir nedenle hesap ana merkez tarafından kullanıma kapatılmışsa işlem, komut onaylanmayacağından yapılamaz. Bu olgu da gösteriyor ki ATM makineleri bir bilgi işlem sisteminin ünitesidir. Yine, sistemi harekete geçirmede kullanılan kartların geleneksel hırsızlık suçları bakımından "sair alet" olarak kabul edilmesi de olanaklı değildir. Gelişen teknoloji ürünü olsalar da bu kartlar şifre olmadan kullanılamazlar, diğer bir söylemle sistemi tek başına harekete geçiremezler. Sistem harekete geçirilemeden bundan bir yarar sağlanması da söz konusu edilemez. Burada bilgisayar sistemini harekete geçirebilen kartlar ile belirli bir yere girilmesi için kullanılan diğer kartların, fonksiyonları itibariyle yek diğerine benzemediği de belirtilmelidir. Ayrıca anahtar benzeri sair bir aletten söz edebilmek için mantiken bir kilidin de bulunması gereklidir. Bu bakımdan da ATM makinelerinde kullanılan kartları sair alet olarak saymaya olanak yoktur.”

Bütün bu gerekçeler doğrultusunda, Yargıtay CGK, 6. CD kararlarından farklı olarak, haksız bir şekilde ele geçirilmiş banka kartı ile “atm”lerden para çekilmesi fiilinin 765 Sayılı TCK’nin 493/2. maddesinde düzenlenen suç değil aynı Kanunun 525/b 2. maddesindeki suç oluşturduğu sonucuna varmıştır³²⁸.

³²⁸ **YARGITAY CGK E. 2000/6-62 K. 2000/72 T. 11.4.2000**
<http://www.kazanci.com.tr/kho2/ibb/files/cgk-2000-6-62.htm> Kararda bu fiilin 765 Sayılı TCK’nin 493/2. maddesinde belirtilen suç oluşturduğu farklı gerekçelerle dile

Banka kartının, anahtar ya da sair alet kapsamında olduğuna ilişkin tartışma bir yana bırakılarak bu karar incelendiğinde, öncelikli olarak haksız bir şekilde ele geçirilen banka kartı ile “atm”den para çekme fiilinin hırsızlık suçunu oluşturup oluşturmadığına ilişkin bir tartışmaya yer verilmeden, fiilin bilişim sisteminin kullanılması suretiyle gerçekleştirildiği tartışmasına yer verildiği görülmektedir. Bu kapsamda, Ceza Genel Kurulu kararında, bilişim sisteminin kullanıldığı sonucuna varılmış ve bu nedenle fiilin 525/b 2. maddesindeki suçu oluşturduğu ifade edilmiştir. Bu tartışma yapılırken, fiilde hırsızlık suçunun unsurlarının gerçekleşip

getirilmiştir. Bu doğrultuda “Her ne kadar bilişim suçlarının tanım ve tarifi üzerinde ulusal ve uluslar arası hukuk alanlarında çok farklı ve değişik düşünceler ileri sürülmüş, bu suçları geleneksel suçlardan ayıracak kriterler bakımından dahi görüş birliğine ulaşılmamışsa da, enformatik sistemin kötüye kullanılması olarak adlandırılan ve bir bilgisayar sisteminin kullanılmasını zorunlu kılan bilişim suçlarının ancak enformatik teknoloji hakkında bilgi sahibi olan kişiler tarafından işlenebileceği kabul edilmelidir. Bu itibarla bilişim suçundan bahsedebilmek için sisteme yanlış veriler yükleyerek yada bilgi işlem sürecinin aşamalarından birine müdahale edilerek sistemin yönlendirilmesi gerekmektedir. ATM'lerin kullanılmasında ise, bilgi işlem sürecinin aşamalarından birine müdahale edilmeden, başkalarının sahip olduğu ve bilgi işlem sürecini başlatmayı sağlayan bir kart ve şifreden yararlanılarak basit bir manipülasyonla eylem gerçekleştirilmektedir, bu nedenle ATM'lere yönelik eylemleri bilişim suçu kapsamında değerlendirme olanağı bulunmamaktadır. Kısaca, sanığın haksız olarak elinde bulundurduğu kart ve şifre ile ATM makinesinden para çekme eylemi, teknolojik bilgi kullanılmayı gerektiren bir hareket değildir. Somut olayda bir mal varlığına yönelik eylemde kart sair alet olarak kullanılmış olduğundan bu eylem TCY'nın 493/2nci maddesinde düzenlenen hırsızlık suçunu oluşturmaktadır.” görüşü dile getirilmiştir. Diğer yandan bu gerekçe ile aynı görüşlere yer verilmesine rağmen fiilin hem 765 Sayılı TCK 493/2. hem de 525/b 2. maddelerine aykırılık oluşturduğu Kanunun 79. maddesi gereği 493/2. maddesinin uygulanması zorunlu olduğu ifade edilmiştir. Bunların yanında bu fiilin teknolojik bilgiye gerektirmeyen basit bir işlem olması nedeniyle 525/b 2. fıkrasına girmeyeceği ifade de diğer bir karşıoy gerekçesini oluşturmuştur.

Söz konusu kararlardan sonra haksız olarak ele geçirilen banka kartı ile “atm”lerden para çekilmesi fiili 765 Sayılı TCK'nin 525/b 2. fıkrasındaki suçu oluşturduğu yönünde içtihat birliğinin sağlandığı görülmektedir. **Örnek olarak bkz., YARGITAY 10 CD E. 2004/14311 K. 2004/10906 T. 2.11.2004**, <http://www.kazanci.com.tr/kho2/ibb/files/10cd-2004-14311.htm> ; **YARGITAY 11. CD E. 2003/2671, K. 2004/3755, T. 29.4.2004**, <http://www.kazanci.com.tr/kho2/ibb/files/11cd-2003-2671.htm> ; **YARGITAY 6. CD, E. 2003/4492, K. 2003/6558, T. 8.10.2003**, <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2003-4492.htm> Bu kararda kredi kartının çalınmasının hırsızlık bunun sonrasında “atm”den para çekilmesi ise 525/b 2. maddesindeki suçu oluşturduğu sonucuna varılmıştır. Aynı yönde **YARGITAY 6. CD, E. 2002/23728, K. 2004/3131, T. 18.3.2004**, <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2002-23728.htm>

gerçekleşmediğine ilişkin herhangi bir tartışmaya yer verilmemiş ve bu yönde bir sonuca varılmamıştır. Kararda, her iki suç kapsamına girecek olan fiil, 525/b 2. maddesindeki özel düzenleme nedeniyle bu madde kapsamında değerlendirilmiştir.

Bu açıdan incelendiğinde, hırsızlık suçu kapsamında değerlendirilemeyecek fiillerin cezalandırılması gerekçesiyle düzenlendiği belirtilen 525/b 2. fıkrasının, aslında hırsızlık suçu kapsamında olan bir fiili, sadece bilişim sisteminin kullanılmış olması nedeniyle kapsamına alması sonucunun ortaya çıktığı görülmektedir. Söz konusu madde olmasa da haksız bir şekilde ele geçirilmiş olan bir banka kartı ile “atm”den para çekilmesi hırsızlık suçu olarak değerlendirilebilmesi mümkündür. Banka kartının anahtar veya sair alet olup olmadığına ilişkin tartışma ise burada sadece ağırlatıcı nedenin uygulanıp uygulanmaması bakımından önemli olacak, suçun oluşumunu etkilemeyecektir. 525/b 2. fıkra geniş bir düzenlemeye yer verilmesi ve banka kartı ile para çekilmesi fiillerinin bu suç kapsamında değerlendirilmesi, Yargıtay CGK kararında da yer aldığı şekliyle, bilişim sisteminin kullanılıp kullanılmadığının belirlenmesine ilişkin ek bir yük getirmekten başka bir işlev taşımamıştır³²⁹.

³²⁹ Özellikle “atm”lerden banka kartı ile para çekilmesi fiilleri bakımından MAHMUTOĞLU bu fiilde kişiye karşı hilenin söz konusu olmadığını bu nedenle burada 765 Sayılı TCK’nin 525/b kapsamında bir bilişim suçu olduğunu ifade etmiştir. Fatih S. MAHMUTOĞLU, Ekonomik Suçlar Bağlamında Kredi Hukukundan Kaynaklanan Suç ve İdari Suçlar, 1. B., Ankara, 2003, s. 278.

Sadece para çekme fiili açısından düşünüldüğünde yukarıda belirtildiği üzere ve 6 CD’nin önceki tarihli kararlarında da yer aldığı üzere hırsızlık suçunu oluşturacağı şüphesizdir. Bu fiile ilgili kişinin rızası olmadan taşınır bir malın alınması açısından bakıldığında fiilin hırsızlık olarak nitelendirilmesi mümkün olacaktır. Burada hilenin söz konusu olup olmadığı ya da bir kişiye karşı hilenin yapılmış olup olmadığına ilişkin tartışma tali bir nitelik taşımaktadır.

Buna karşın Bayraktar, “bu tür fiillerde mağdurun mevduatından para alınması olgusu hırsızlığı akla getirebilmekte ise de ‘zilyetliği altındaki’ malın alınması kuşku yaratabilmektedir.” demiştir. Bu tür fiillerde başkasının zilyetliği altındaki malın alınmasının söz konusu olması karşısında, paranın banka kartının sahibinin zilyetliği altında

525/b 2. maddesindeki bu suçun unsurları bakımından kapsamının geniş tutulması, sadece banka kartları ile para çekilmesine ilişkin hırsızlık suçu olarak nitelendirilebilecek bir fiilin, bu madde kapsamına girmesine yol açmamış, aynı zamanda yine banka kartının kullanılması şekliyle ortaya çıkan fakat emniyeti suiistimal olarak değerlendirilebilecek bir fiilde de 525b/2. fıkrasının uygulanması sonucunu doğurmuştur. Yargıtay 11. Ceza Dairesinin 2001 yılında verdiği bir kararda, iptal ettirilmesi için sanığa verilen banka kredi kartıyla sanığın değişik tarihlerde nakit para çekmesi fiilinin 525/b 2. maddesine girdiğinden bahisle söz konusu fiilin emniyeti suiistimal suçunu oluşturduğu yönündeki yerel mahkeme kararını hukuka aykırı bulmuştur³³⁰. Söz konusu fiil incelendiğinde, kartın sahibi tarafından iptal ettirilmesi için teslim edilmesine rağmen kullanılması emniyeti suiistimal olarak değerlendirilebilmesi mümkündür. Burada, banka kartı ile, yukarıda Ceza Genel Kurulu kararında belirtildiği şekliyle, bilişim sisteminin kullanılmış olması suçun niteliğini değiştirmiştir. Bu açıdan da 525/b maddesinin emniyeti suiistimal suçunu oluşturacak bu tür fiilleri sadece bilişim sistemi kullanılmış olması nedeniyle kapsadığı görülmektedir.

olması ya da üçüncü bir kişinin zilyetliği altında olması (banka kartı ile para çekilmesine ilişkin fiillerde banka mevduatındaki paranın kime ait olduğu ya da banka ile mevduat sahibi arasındaki söz konusu mevduat nedeniyle var olan hukuki ilişkiye girilmeksizin) şeklindeki bir fark suçun hırsızlık olarak nitelendirilmesinde etkiye sahip değildir. Bu açıdan, banka kartı ile para çekilmesine ilişkin fiillerin hırsızlık suçunu oluşturabilmesi mümkün olup bu nedenle yazarın görüşüne katılmamaktayız. Bkz., Köksal **BAYRAKTAR**, *Banka Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları*, Prof. Dr. Kemal Oğuzman Anısına Armağan, İstanbul, 2000, s. 198.

³³⁰ **YARGITAY 11. CD, E. 2001/8765, K . 2001/9224, T. 10. 10. 2001**, <http://www.kazanci.com.tr/kho2/ibb/files/11cd-2001-8765.htm>

**c. Kişiyeye Karşı Hileli Hareketler Yapılması ve Bilişim Sistemi
Kullanılması Sonucunda Yarar Sağlanması**

Haksız bir şekilde elde edilen banka kartı ile para çekilmesi fiillerinin, “*bilişim sisteminin kullanıldığı*” gerekçesiyle 765 Sayılı TCK’nin 525/b maddesindeki suç oluşturduğunu çeşitli Yargıtay kararlarında ifade etmekle birlikte, özellikle kartın ve şifresinin ele geçirilmesinde kişiyeye karşı hileli hareketler yapılması söz konusu olduğunda, bu tür fiiller Yargıtayın bazı kararlarında dolandırıcılık bazı kararlarında bilgisayar aracılığıyla yarar sağlama olarak nitelendirilmiştir.

Yargıtay CGK.nun 2001 yılında verdiği bir kararda, “*Y... Bankasının ...şubesindeki ATM’nin, kart konulan bölümüne önceden kağıt yerleştiren sanığın, işlem yapmak isteyen şikayetçinin kartının sıkışmasını sağlayıp, böylelikle sistemle iletişimi ve işleme geçilmesini engellediği, yardımcı olmak bahanesiyle Kredi Kartları Merkezini arıyor izlenimi verip önceden anlaştığı arkadaşını cep telefonu ile arayarak şikayetçi ile görüşmesini sağladığı, kartını geri alabilmek, olmazsa kartın kullanımını iptal ettirebilmek umuduyla görüşen şikayetçiye banka görevlisi gibi davranan arkadaşının yaptırdığı şifre kodlama işlemi sırasında şikayetçinin şifresini öğrendiği, onun ayrılmasından sonra da kredi kartını yuvadan çıkartıp Y... Bankasının anlaşmalı olduğu P...’ın iki ayrı şubesindeki ATM’lerinden farklı*

tarihlerde toplam altıyüz milyon lira nakit kredi çektiği”ne ilişkin fiilin 765 Sayılı TCK’nin 525/b ikinci fıkrasında düzenlenen suçı oluşturduğu sonucuna varmıştır³³¹.

Buna karşın, Yargıtay 11 CD.nin 2002 yılında verdiği kararda ise, “*Sanığın ATM cihazında önceden hazırladığı tertibatla bankamatik kartının makinasında sıkışmasını sağlayıp banka görevlisi ile telefonla görüştüğü izlenimini de uyandırarak yaptığı hile ile şikayetçiden bankamatik kartını ve şifresini ele geçirdiği ve para çektiği anlaşılmaya göre; sanığın şikayetçiye ait bankamatik kartını ve şifresini hile ve desise yaparak öğrenmesi telefon ve bankayı vasıta kılarak şikayetçinin zararına, kendi yararına haksız menfaat sağlaması nedenleriyle eylemin TCK. nun 504/3. maddesine uygun dolandırıcılık suçunu oluşturduğu gözetilmeden suçun nitelemesinde yanılığa düşülerek yazılı şekilde aynı yasanın 525/b-2 maddesindeki bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak suçundan mahkumiyetine karar verilmesi” hukuka aykırı bulunmuş ve bozma nedeni sayılmıştır³³².*

³³¹ **YARGITAY CGK, E. 2001/6-30 K. 2001/57 T. 10.4.2001,** <http://www.kazanci.com.tr/kho2/ibb/files/cgk-2001-6-30.htm>

³³² **YARGITAY 11. CD, E. 2002/11700, K. 2003/7599, T. 10.11.2003,** <http://www.kazanci.com.tr/kho2/ibb/files/11cd-2002-11700.htm>. Aynı yönde “...Bir bankanın ATM makinesinin kredi kartı giriş bölümüne, kartın geri alınışını engellemek amacıyla yapışkan kağıt koyan sanığın, bu makinede işlem yapmak isteyen şikayetçinin kartını geri alamaması üzerine, sanık ile haklarındaki karar temyiz edilmeyen sanıkların yardım etmek amacıyla yanına gelip şifresini sordukları, şikayetçinin söylemeyip kartı makinenin içine iteklediği, bankanın kapalı olması nedeniyle açılmasını beklemek amacıyla kendi işyerine gittiği, bir süre sonra kredi kartını çıkaran sanıkların kart üzerindeki bilgileri öğrenerek şikayetçiye telefon edip kendilerini banka görevlisi gibi tanıtıp, hesap ile ilgili bazı bilgileri söylemek suretiyle güveni sağladıktan sonra iptal edeceklerinden bahisle şifresini sorup öğrendikleri, bu suretle elde ettikleri kart ve şifreyi kullanarak para çekip havale yaptıkları olayda; sanığın, şikayetçiye ait şifreyi hile ve desise yaparak öğrenmesi, telefon ve bankayı vasıta kılarak şikayetçinin zararına, kendi yararına haksız menfaat sağlaması nedeniyle eylemin dolandırıcılık suçunu oluşturduğu ve TCY.nın 504/3. maddesine uygun bulunduğu gözetilmeden, yasal ve yeterli gerekçe gösterilmeden yazılı şekilde hırsızlık suçundan mahkumiyet hükmü kurulması...” hukuka aykırı bulunmuştur.

Bu kararlar incelendiğinde, her ne kadar Yargıtay CGK tarafından bu tür fiillerin 525b/2. maddesi kapsamında olduğu ifade edilmiş olsa da, sonraki kararlarda bu fiillerin dolandırıcılık suçu kapsamında değerlendirildiği görülmektedir. Bu açıdan Yargıtay Ceza Genel Kurulunun yukarıda aktarılan kararının, aksine Daire kararlarında kişiye karşı hile yapılması sonucunda kartın ve şifrenin ele geçirilmesi ve sonrasında para çekilmesi fiilinde, bilişim sistemi olarak kabul edilen “atm”lerin kullanılması, suçun niteliğinde dikkate alınmamıştır. Daire kararlarında, kişiye karşı hileli hareketler yapılması sonucunda kişinin aldatılması suretiyle kartın ele geçirilmesi ve sonrasında para çekilmesinde, bir bütün olarak dolandırıcılık suçunun unsurlarının olduğu ve bankanın aracı kılınması suretiyle dolandırıcılık suçunun gerçekleştiği kanaatine varılmıştır³³³.

Yargıtay 11. CD, E. 2002/5633, K. 2002/5659, T. 11.6.2002, <http://www.kazanci.com.tr/kho2/ibb/files/11cd-2002-5633.htm> .

³³³ Aynı yönde “...Bir bankanın ATM makinesinin kredi kartı giriş bölümüne, kartın geri alınışını engellemek amacıyla yapışkan kağıt koyan sanığın, bu makinede işlem yapmak isteyen şikayetçinin kartını geri alamaması üzerine, sanık ile haklarındaki karar temyiz edilmeyen sanıkların yardım etmek amacıyla yanına gelip şifresini sordukları, şikayetçinin söylemeyip kartı makinenin içine iteklediği, bankanın kapalı olması nedeniyle açılmasını beklemek amacıyla kendi işyerine gittiği, bir süre sonra kredi kartını çıkaran sanıkların kart üzerindeki bilgileri öğrenerek şikayetçiye telefon edip kendilerini banka görevlisi gibi tanıtır, hesap ile ilgili bazı bilgileri söylemek suretiyle güveni sağladıktan sonra iptal edeceklerinden bahisle şifresini sorup öğrendikleri, bu suretle elde ettikleri kart ve şifreyi kullanarak para çekip havale yaptıkları olayda; sanığın, şikayetçiye ait şifreyi hile ve desise yaparak öğrenmesi, telefon ve bankayı vasıta kılarak şikayetçinin zararına, kendi yarına haksız menfaat sağlaması nedeniyle eylemin dolandırıcılık suçunu oluşturduğu ve TCY.nın 504/3. maddesine uygun bulunduğu gözetilmeden, yasal ve yeterli gerekçe gösterilmeden yazılı şekilde hırsızlık suçundan mahkumiyet hükmü kurulması...” Yargıtay 11. CD, E. 2002/5633, K. 2002/5659, T. 11.6.2002, <http://www.kazanci.com.tr/kho2/ibb/files/11cd-2002-5633.htm> .

Buna karşın Yargıtay bir yönüyle dolandırıcılık suçu kapsamında değerlendirilebilecek olan bir fiili, olayda kredi kartı ile pos makinesi kullanılmış olması nedeniyle 765 Sayılı TCK’nin 525b/2. maddesindeki suçu oluşturduğu sonucuna varmıştır. Kararda “Sanığın, müdahile ait benzin istasyonunda akşam saat 18’den başlayarak sabah 08 saatine kadar çalışmakta olduğu, işyerine ait muhtelif tarihlerde peşin mal satışlarından elde ettiği paraları mal edindiği, bu suretle müdahile karşı emniyeti suistimal suçunu işlediği, ayrıca

Aynı şekilde Yargıtay, kredi kartının bankadan alımı sırasında, bankaya yönelik birtakım hileli hareketler yapılması suretiyle aldatılması ve bu şekilde kartın temin edilmesi sonrasında, elde edilen kredi kartı ile para çekilmesini veya kullanılmasını bir bütün olarak dolandırıcılık suçu olarak değerlendirmektedir³³⁴.

Daha önceden hileli hareketler yapılması sonucunda kişinin kendi hesabına para gönderilmesi ve sonrasında banka kartı kullanarak para çekilmesi fiili de

bu suçtan dolayı takibata uğramamak için mağdurlar ... 'ın kredi kartları ile bu işyerinden yaptıkları alışverişlerinde, kredi kartlarını, habersizce ikinci kez bilgileri otomatik işleme tabi tutmuş bir sistem olan post cihazından geçirip slip harcama makbuzlarına sonraki yaptığı peşin satışlardan tahsil ettiği paraları mal edindiği miktarları yazıp imzalarını taklit etmek suretiyle bankadaki hesaplarından müdahil tarafa ödemeler yapılmasını sağlamak suretiyle yararlandığı toplanan deliller ve oluştan anlaşılmasına göre sanığın TCK'nin 510, 80 ve 525/b maddesinin 2. bendi, 80. maddelerine uyan iki ayrı fiilden dolayı ayrı ayrı mahkumiyeti yerine dolandırıcılık suçu esas alınarak delil yetersizliğinden bahisle beraatine karar verilmesi” hukuka aykırı bulunmuştur. YARGITAY 6 CD, E. 2002/4342, K. 2002/5394, T. 6.6.2002, <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2002-4342.htm>,

Sahte kredi kartlarının pos makinaları ya da imprinter adlı cihazlardan geçirilerek slip üretilmesi ve bunun sonucunda ilgili meblağın bankadan tahsil edilmesi fiili Yargıtay Ceza Kurulu’nun 2001 yılındaki bir kararında dolandırıcılık suçu kapsamında değerlendirilmiştir. YARGITAY CGK, E. 2001/6-106, K. 2001/111, T. 29.05.2001, <http://www.kazanci.com.tr/kho2/ibb/files/cgk-2001-6-106.htm>.

Benzer bir şekilde haksız olarak ele geçirilen kredi kartının kullanılarak benzin satılmadığı halde satılmış gibi gösterip belge düzenlenmesi ve karşılığının bankadan alınması fiilinin de dolandırıcılık suçu kapsamında olduğu karara bağlanmıştır. YARGITAY 6. CD, 2001/14625, K. 2001/14804, T. 3.12.2001, <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2001-14625.htm>

³³⁴ “...Sanığın V... Bank Ezine Şubesi'ne başvurarak "Kredi Kartı Başvuru Formu ve Üyelik Sözleşmesi" düzenlediği, bu belgeye yakınının imzasını da müşterek ve müteselsil borçlu sıfatı ile sahte olarak attığı ve aldığı kredi kartı ile bankadan para çektiğinin iddia edilmesi karşısında; sübutu halinde eyleminin TCK'nun 79.maddesi aracılığıyla aynı yasanın 504/1, 80. ve 522. maddelerine uyan suçu oluşturup oluşturmadığına ilişkin delilleri takdir ve tartışmanın üst dereceli Ağır Ceza Mahkemesine ait olduğu gözetilerek görevsizlik kararı verilmesi gerekirken, duruşmaya devamla yazılı şekilde hüküm kurulması...” YARGITAY 6 CD E. 2002/4134, K. 2002/5800, T. 6.5.2002, <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2002-4134.htm> . Aynı yönde “...Sahte belgeler kullanarak katılan banka tarafından kredi açılmasını sağlayıp kredi kartı alarak bu kartla alışveriş yapıp para çekmek suretiyle haksız çıkar sağlayan sanığın eylemi TCK'nun 504/1. maddesine uyan suçu oluşturduğu halde 503/ilk, 80. maddeleri ile hüküm kurulması...” YARGITAY 6 CD, E. 2002/18128, K. 2003/8030, T. 3.11.2003, <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2002-18128.htm>,

dolandırıcılık suçu kapsamında değerlendirilmiştir. Yargıtay 6. CD.nin 1996 yılında verdiği bir kararında, “*Saniğin, kamu kurumundan sayılan Bankası ile özel banka niteliğindeki Bankası'nın muhtelif şubelerindeki banka görevlilerini hile ve desiseler yaparak hataya düşürüp, daha önce hayali isimlerle açtırdığı hesaplara havale yoluyla para aktarılmasını sağlayarak, karşılığını vezneye yatırmadan, sahibi olduğu bankamatik kartı ile çekmek suretiyle gerçekleştirdiği dolandırıcılık eylemlerinin, TCK'nin 504/7, 80 ve 503/1-80. maddelerine uyan suçları oluşturduğu gözetilmeden, aynı Yasanın 525/b-son maddesi ile yazılı şekilde uygulama yapılması*” bozma nedeni saymıştır³³⁵.

Yargıtay kararlarında bir bilişim sistemi olarak kabul edilen “atm”lerin kullanılması suretiyle para çekilmesine ilişkin söz konusu olayda, banka görevlilerine karşı hileli hareketler sonucunda, daha önce açtırdığı hayali hesaplara karşılığının yatırılmadan para aktarılması fiilini esas alan Yargıtay, dolandırıcılık suçunun olduğu sonucuna varmıştır. Fiil sonucunda paranın “atm”den çekilmiş olması yani bilişim sisteminin kullanılmış olması, fiilin hukuki niteliğini etkileyici bir unsur olarak görülmemiştir.

Kartın elde edilmesine ya da kartla para çekilmesinden önce kişiye karşı hileli hareketlerin yapılması ve sonuçta bir kişinin aldatılması şeklinde ortaya çıkan fiillerde, Yargıtay, bu tür fiillerin hukuki niteliği bakımından, kimi zamanlar dolandırıcılık suçunu oluşturduğu, kimi zamanlarda ise 525b/2. maddesindeki suçu oluşturduğu sonucuna ulaşmış, bu haliyle de birbirinden farklı kararlar vermiştir. Bu açıdan, Yargıtay kararlarında, 525b/ 2. maddesinin uygulanması bakımından,

³³⁵ **YARGITAY 6 CD, E. 1996/11031, K. 1996/10933, T. 11.11.1996,** <http://www.kazanci.com.tr/kho2/ibb/files/6cd-1996-11031.htm>

özellikle kişiye karşı hileli hareketler söz konusu olduğunda, birbirinden farklı sonuçlara varıldığı görülmektedir.

Yukarıda aktarılan kararların konusunu oluşturan fiillerde de 765 Sayılı TCK'nin 525b/2. maddesinin Kanuna eklenmesine ilişkin olarak yazarların belirttiğinin aksine, maddede düzenlenen suç, dolandırıcılık suçu kapsamında olmayan fiillerin cezalandırılmasına yönelik olmaktan öte, kimi durumlarda, dolandırıcılık suçu olarak nitelendirilebilecek fiillere uygulanan bir hüküm olarak karşımıza çıkmaktadır.

d. Kişiyeye Karşı Hile Yapılmaksızın Bilişim Sistemi Kullanılmak Suretiyle Yarar Sağlanması

Yukarıda genel olarak hırsızlık veya dolandırıcılık suçları kapsamında değerlendirilebilecek fiillerde bilişim sisteminin kullanılmasında Yargıtay'ın yaklaşımı incelenmiştir. Bunun yanında, yukarıda aktarıldığı şekliyle genel olarak dolandırıcılık suçunda zorunlu olan hileli hareketlerin kişiye karşı yöneltilmiş olması unsurunun bilgisayar aracılığıyla yarar sağlama durumunda söz konusu olmadığına ilişkin gerekçenin geçerli olup olmadığının ve bu tür fiillere uygulamada nasıl yaklaşıldığının saptanması gerekmektedir.

Yargıtay bir kararında, *“... Bankası İzmir otomasyon bölge merkezinde şef olarak görev yapan sanığın, icra ettiğı görev nedeniyle sık sık gidip personeli ile yakınlık kurduğı aynı bankanın İzmir Şubesine gidip müdür şifresini öğrendiğı ve memur E.K.'un bilgisayarının başında bulunmadığı bir sırada O'nun şifresiyle H.Ö. adına sıfır bakiyeli vadeli hesap açarak aynı gün şube mudilerinden İ.A.'nın*

hesabını 8 milyar lira düşürüp H.Ö. adına açtığı hesabı, aynı miktarda yükseltmek suretiyle gerçekleştirdiği eylemin TCK'nin 525/b-2. maddesindeki bilgileri otomatik işleme tabi tutmuş bir sistemin kullanarak hukuka aykırı yarar sağlamak suçunu oluşturduğu, icrai hareketlerin tamamlanmaması nedeniyle suçun eksik kalkışma aşamasında kaldığı gözetilmeden, suçun nitelendirilmesinde yanılığa düşülerek TCK'nin 504/7. maddesi uyarınca mahkumiyetine hükmolunması”nı hukuka aykırı bulmuştur³³⁶.

Buna karşın, Yargıtay benzer bir fiilde, failin sıfatını esas alarak banka çalışanı olan ve kendi bilgisayar şifresi ile her türlü işlem yapabilen banka çalışanının, bilişim sistemini kullanarak virman, tahsil ve tediye işlemleri yapması ve bu şekilde başka kişilerin hesaplarına para aktararak bu kişiler aracılığıyla para çekmesi eyleminin zimmet suçunu oluşturduğu sonucuna varmıştır.³³⁷ Bu kararda da bilişim sisteminin kullanılmış olması ve bunun sonucunda yarar sağlanmış olmasına rağmen fiil bu hususlar tali görülerek 525/b 2. madde kapsamında değerlendirilmemiştir.

³³⁶

YARGITAY 6. CD, E. 2002/20630 ,K. 2002/14552, T. 19.12.2002,

<http://www.kazanci.com.tr/kho2/ibb/files/6cd-2002-20630.htm> .

³³⁷

“...Sanığın, mudiler Ali, Ebubekir, Zarif, Mustafa ve M. Ali'nin hesaplarına bir şekilde öğrendiği müdür konumundaki bilgisayar şifresini kullanarak faiz tahakkuk ettirip daha sonra düzenlediği tahsil ve tediye fişleriyle tahakkuk ettirdiği 5.877.000.000 lirayı şubedeki diğer mudilerin hesaplarına aktarıp onlara veznedenden çektiler temellük etmesinin nitelikli dolandırıcılık olarak kabulünde bir isabetsizlik yoksa da, 4.6.1999 günlü müfettiş raporunun, 51. sahifesinde vurgulandığı gibi, kendi bilgisayar şifresi ile virman, tahsil ve tediye işlemleri yapabilen, bu nedenle bankanın paralarının muhafazasından sorumlu olduğu anlaşılan sanığın, adı geçen mudiler dışındaki 60 mudinin hesaplarına faiz tahakkuku yapmadan sadece tahsil ve tediye fişleri düzenleyerek bu mudilerin hesaplarındaki 2.362.650.000 lirayı bankada diğer mudilerin hesaplarına aktarıp ve onların vasıtasıyla veaneden alarak maledinmesi eyleminin müteselsil basit zimmet niteliğinde olduğunun gözetilmemesi...” YARGITAY 5. CD, E. 2001/536, K. 2001/5749, T. 11.10.2001, <http://www.kazanci.com.tr/kho2/ibb/files/5cd-2001-5749.htm>

Benzer bir fiilin konu edinildiği fakat paranın bir kısmının nakit olarak çekildiği başka bir kararda ise Yargıtay, “*Sanık ...'nın, müdür yardımcısı ..'nın başka bir amaçla verdiği şifreyi haksız olarak kullanmak suretiyle, mevduat sahiplerinin hesaplarında vade başı ve vade sonu bilgileri ile faiz oranlarını değiştirerek, oluşturduğu faiz farkını, Nazmiye adına açtığı menkul hesabı ile Sabri adına açılan vadesiz hesaba ve kendi adına açtığı vadesiz tasarruf ve menkul hesaba aktarmak, bir kısmını da nakden çekmek suretiyle inceleme tarihi itibarıyla 162.344.868.691 lirayı haksız olarak mal edindiği..*” fiilin bir bütün olarak dolandırıcılık suçunu oluşturduğu sonucuna varmıştır³³⁸.

Başka bir kararında ise Yargıtay, bankanın bilişim sistemine girilerek usulsüz hesap açılması fiili ile ilgili olarak “*...Hizmetli olarak çalıştığı bankanın bilgisayar sistemine girerek usulüne uygun açılmış bir maaş kredi limitli bankomat hesabının kredi limitini yükseltmek ve ayrıca kendi adına usulsüz olarak bankomat 7/24 hesabı açmak suretiyle haksız yarar sağladığı oluşa uygun olarak kabul edilen sanığın eyleminin TCK'nin 525/b maddesinin 1. fıkrasındaki suça uygun bulunduğu gözetilmeden, aynı maddenin 2. fıkrasıyla hüküm kurulması*”nı hukuka aykırı bulmuştur³³⁹.

Yargıtay 6 CD 2001 yılında verdiği bir kararda ise “*Herhangi bir kişiyle gerek doğrudan, gerekse dolaylı olarak muhatap olmadan, çalıntı kredi kartlarını sözleşme gereği iş yerinde bulundurduğu pos cihazından geçirip bilgileri otomatik*

³³⁸ . YARGITAY CGK E. 2002/11-329, K. 2003/29, T. 11.3.2003,
<http://www.kazanci.com.tr/kho2/ibb/files/cgk-2002-11-329.htm> .

³³⁹ YARGITAY 11. CD, E1997/5052, K. 1997/6536, T. 2.12.1997,
<http://www.kazanci.com.tr/kho2/ibb/files/11cd-1997-5052.htm>.

işleme tabi tutulmuş off-line sisteminden yararlanarak kredi kartı hesaplarından, kendi hesabına para aktaran sanığın eyleminin TCK'nin 525/b-2. maddesinde yazılı suçu oluşturduğu” sonucuna varmıştır³⁴⁰.

Aktarılan ilk dört kararda, usulsüz hesap açılması ya da bu hesaba başka hesaplardan para aktarılmasında herhangi bir kişiye yönelik hile ya da desise söz konusu değildir. Bu fiiller bilgisayar sisteminin şifresinin çeşitli şekillerde elde edilmesi suretiyle ya da bu olmadan bankanın bilgisayar sistemine girilmesi suretiyle usulsüz hesaplar açılması veya diğer hesaplardan para çekilmesi şekillerinde oluşmuştur. Bu açıdan bakıldığında, bu aşamada herhangi bir kişinin, hileli hareket kapsamında değerlendirilebilecek bu hareketlerin muhatabı olması söz konusu değildir. Son kararda ise herhangi bir kişiyle doğrudan ve dolaylı olarak muhatap olunmaması ve bu şekilde kartın pos cihazından geçirilmesi sonucu sistemin kullanılması hileli hareket olarak karşımıza çıkmaktadır.

Bu kararlara konu olan fiillerin hepsinde doğrudan ya da dolaylı bir şekilde bilişim sisteminin kullanılması söz konusu olmakta bu kapsamda yarar sağlamaya yönelik fiiller sistem içerisine yeni veri yerleştirilmesi ya da var olan verilerin değiştirilmesi şeklindedir.

Yukarıdaki kararlarda yararın sağlanıp sağlanmadığı ya da yararın sağlanma anı bakımından farklı sonuçlara varıldığı görülmektedir. Birinci kararda icra hareketlerinin tamamlanmaması dolayısıyla teşebbüs aşamasında kaldığı, ikinci kararda bir miktar paranın nakden çekilmesi esas alınarak yararın sağlandığı, üçüncü

³⁴⁰ **YARGITAY 6. CD, E. 2001/7716, K. 2001/8463, T. 21.5.2001,** <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2001-7716.htm>.

kararda ise birinci karardan farklı olarak usulsüz hesap açılması ve hesap üzerinde değişiklik yapılması ile yarar sağlandığı sonucuna varılmıştır. Son kararda ise kartın pos cihazından geçirilmesi sonucunda bilişim sisteminin kullanılması suretiyle kişinin kartın bağlı bulunduğu hesaptan kendi hesabına para aktarması ile yararın sağlandığı sonucuna varılmıştır.

Buna karşın bir bilişim sistemi kullanılarak hileli bir davranış sonucunda bedel ödemeksizin bir hizmetten yararlanılması 765 Sayılı TCK'nin 525b/1. maddesi kapsamında değerlendirilmiştir. Yargıtaya göre, pornografik yayın yapan Web sayfasının şifresinin çözülüp yeni bir şifre oluşturmak suretiyle bundan yarar sağlanması fiili, TCK'nin 525/b 1.fıkrasında düzenlenen suçu oluşturmaktadır³⁴¹.

Bu doğrultuda, kişiye karşı bir hile yapılmadan bilişim sisteminin kullanılması suretiyle sistem içerisine yeni veri yerleştirilmesi ya da verinin değiştirilmesi sonucu yarar sağlanması, Yargıtay kararlarında kimi durumlarda dolandırıcılık suçunun olduğu, kimi durumlarda ise 765 Sayılı TCK'nin 525/b 1. maddesi ya da 525b/ 2. fıkrasında düzenlenen suçun olduğu sonucuna varılmıştır; failin sıfatının esas alındığı durumda ise zimmet suçunun olduğuna karar verilmiştir.

Kişiye karşı hilenin yapılmamış olup, kişinin aldatılmaması açısından değerlendirildiğinde, yukarıda bilişim sistemi kullanılması suretiyle gerçekleştirilen fiillerin TCK'nin 525/b maddesinde değerlendirilmesi yerinde olmakla birlikte³⁴² bu

³⁴¹ **YARGITAY 6. CD, E. 2002/16699, K. 2003/6727, T. 13.10.2003,** <http://www.kazanci.com.tr/kho2/ibb/files/6cd-2002-6727.htm>.

³⁴² Bu açıdan yukarıda aktarılan, YARGITAY CGK E. 2002/11-329 no.lu kararına konu olan fiilin, kararda açıklık olmamakla birlikte, kişiye karşı hileli hareketlerin

maddenin kendi içinde de çeşitli sorunlara yol açtığı görülmektedir. Bu sorunun kaynağı ise 525b/1. maddede düzenlenen suçta suçun yarar sağlamak amacıyla ya da zarar vermek amacıyla işlenebileceğine ilişkin özel kastın yer alması ve ayrıca 1. fıkra da düzenlenen suçun cezasının (2 yıldan 6 yıla kadar hapis ve para cezası) 2. fıkra da düzenlenen suçun cezasından (1 yıldan beş yıla kadar hapis ve para cezası) ağır olmasıdır. Bu açıdan incelendiğinde yarar sağlamak amacıyla maddenin 1. fıkrasında belirtilen suçun işlenmesi halinde verilecek ceza bilişim sisteminin kullanılması suretiyle yarar sağlanması halinde verilecek cezadan daha ağır olduğu görülmektedir.

Yukarıda aktarıldığı üzere, her ne kadar maddenin birinci fıkrasının sisteme yönelik zarar verme fiillerini kapsadığı ikinci fıkra da ise sistem aracılığıyla yarar sağlama fiillerinin düzenlendiği doktrinde yaygın olarak belirtilmiş ise de maddenin düzenlenişi itibarıyla daha farklı anlama sahip olduğu görülmektedir.

Bilgisayar aracılığıyla yarar sağlama açısından her iki madde birlikte incelendiğinde sisteme ve veriye zarar verme fiilleri yanında yarar sağlamaya yönelik fiillerin de birinci fıkra kapsamında düzenlendiği bu açıdan bilgisayar aracılığıyla yarar sağlamayı düzenleyen tek suçun 2. fıkra da düzenlenen suç olmadığı söylenebilirdi. Bu açıdan kanun koyucunun yarar sağlamaya yönelik fiiller açısından ikili bir ayırıma gittiği görülecekti. Her iki fıkra da yer alan suçlar bu açıdan suçun unsurunu oluşturan hareketler ve sonucunda yararın sağlanmasının şart olup olmadığı noktasında birbirinden ayrılmaktadır.

gerçekleştirilmemesi nedeniyle dolandırıcılık suçu kapsamında değerlendirilmesi yerinde değildir.

Nitekim 765 Sayılı TCK'nin birinci fıkrasında yer alan suçun maddi unsurunu oluşturan hareketler seçimlik olarak düzenlenmiş ve hareketlerin yarar sağlamak için gerçekleştirilmiş olması halinde yararın sağlanmış olmasına bakılmaksızın bu yöndeki bir fiilin bu fıkra da belirtilen suçu oluşturması öngörülmüştür. İkinci fıkra da ise bilgisayarın kullanılması ve sonuçta yararın sağlanması suç olarak düzenlenmiştir.

Yukarıda usulsüz olarak hesap açılması ve başka hesaplardan para aktarılmasına ilişkin kararlar bu doğrultuda incelendiğinde, bu fiillerde sistemdeki verinin yarar sağlamak için değiştirilmesinin söz konusu olması karşısında yararın sağlanmış olup olmamasına bakılmaksızın birinci fıkra kapsamında düşünülmesi mümkündür. Bu haliyle de bir kişiye yönelik hileli hareketler gerçekleştirilmeden yarar sağlanmasına yönelik fiillerin, maddede sayılan hareketlerle gerçekleştirilmesi halinde bu fıkra kapsamına girmesi mümkündür.

Bu açıdan incelendiğinde, bilişim sistemi ile yarar sağlamaya ilişkin 525b/ 2. maddesinde düzenlenen suçun yukarıda belirtildiği gibi ağırlıklı olarak suçun kapsamına ilişkin sorunları gündeme getirdiği görülmektedir. Banka kartı ile “atm”den para çekilmesi şeklinde gerçekleşen fiillerin, klasik hırsızlık suçu olarak değerlendirilebilecek olması ve bunun Yargıtay'ın çeşitli kararlarında ve Yargıtay CGK.nun kararında karşıoy gerekçelerinde dile getirilmesine rağmen, sırf bilişim sisteminin kullanılması olarak nitelendirilen “atm”lerin kullanılmış olması nedeniyle, bilgisayar aracılığıyla yarar sağlama olarak değerlendirildiği görülmektedir.

Banka veya kredi kartlarının ve şifrelerinin elde edilmesine ilişkin süreçte bir kişiye karşı hileli hareketlerin gerçekleştirilmesi ve kişinin aldatılması ve sonrasında

elde edilen kredi kartları ile “atm”lerden para çekilmesinde ise Yargıtay kimi zamanlarda dolandırıcılık suçunun kimi zamanlarda da bilgisayar aracılığıyla yarar sağlama suçunun mevcut olduğu sonucuna varmıştır. Banka veya kredi kartlarının elde edilmesi ve kullanılmasına ilişkin süreçte, bir kısım hileli hareketlerin yapılması durumunda Yargıtay birbirinden farklı sonuçlara varabilmektedir.

Yargıtayın yukarıda aktarılan kararları değerlendirildiğinde, 765 Sayılı TCK’nin uygulanmasında, maddenin kapsamını özellikle dolandırıcılık fiilleri bakımından kimi kararlarında dar tuttuğu görülmektedir. Banka kartı ile para çekilmesi bakımından, fiilin sırf bilişim sisteminin kullanılması suretiyle gerçekleştirilmesi, suçun niteliğinde değişiklik için bir neden olarak görülmüştür. Buna karşın, banka kartının hile ve desise ile elde edilmesi veya kişiye karşı hile yapılarak banka hesabına para aktarılması sonucunda, paranın “atm”lerden çekilmesi durumlarında, bilişim sisteminin kullanılmış olması suçun niteliğini değiştiren bir unsur olarak kabul edilmeyerek, bu tür fiillerin dolandırıcılık suçunu oluşturduğu sonucuna da varıldığı görülmektedir. Bu konuda Yargıtayın farklı yönde kararlı mevcuttur.

Yargıtaya göre, hesap açılmasına ve hesaba para transfer edilmesine ya da kartın ele geçirilmesine ilişkin olarak kişiye yönelik hileli hareketlerin varlığı ve bu hareketler sonrasında bilişim sistemi kullanılarak paranın çekilmiş yani yararın sağlanmış olması, fiillerinde, herhangi bir aşamada bilişim sisteminin kullanılmış olması, sırf bu nedenle 765 Sayılı TCK’nin 525b/2. maddesindeki suça vücut vermesine yeterli görülmemektedir.

Topluca bir deęerlendirme yapıldığında, TCK'nin 525/b 2. maddesinde , yazarların ifade ettięi üzere, dolandırıcılık, hırsızlık, güveni kötüye kullanma gibi suçlar bakımından bilişim sistemlerinin ve verinin söz konusu olması nedeniyle bu gibi suçların unsurlarının gerçekleşmemesi gerekçesiyle düzenlendięi ifade edilen bilgisayar aracılığıyla yarar sağlama suçunun, yukarıda aktarılan fiiller bakımından geçerlilięinin olmadıęını göstermektedir. 525b/2. maddesinin uygulamada görünümü çoęunlukla hırsızlık, dolandırıcılık ya da güveni kötüye kullanma olarak nitelendirilebilecek fiillerin bilişim sisteminin kullanılması nedeniyle 525b/2. maddesindeki suçu oluřturduęu şeklinde olup burada da malvarlıęının korunmasına iliřkin geleneksel suçların kapsamında olmayan fiillerden çok, özel düzenleme sebebiyle 525b/2. maddesinin uygulandıęı durumlar olarak karřımıza çıkmaktadır.

Sonuç olarak, 525/b maddesinin iki durumda aęırlıklı olarak uygulama alanı bulduęu bunlardan birincisinin haksız olarak ele geçirilen banka kartı ile para çekilmesi dięeri ise usulsüz hesap açılması ve hesaba para aktarılması olduęu görölmektedir. Banka kartı ile para çekilmesi hırsızlık suçu olarak da düşünöleceęinden, bu fıkranın sadece ikinci duruma yani kiřiye karřı hile yapılmadan yarar sağlanması şeklinde dolandırıcılık suçu olarak vasıflandırılmayacak fiiller bakımından bir işleve sahip olduęunu söylemek mümkündür.

Haksız olarak elde edilen banka kartları ile para çekilmesinin hırsızlık, hileli hareketler ile banka veya kredi kartlarının elde edilmesi sonucunda bunlarla para çekilmesi veya kullanılması fiillerinin, dolandırıcılık suçu olarak deęerlendirilebilmesi karřısında, maddenin yürürlükte bulunduęu dönemdeki

uygulamada edinilen tecrübe de göstermektedir ki, sorun kişiye karşı hileli hareketler gerçekleştirilmeden sadece sisteme ve veriye müdahale yoluyla hukuka aykırı yarar sağlanmasının nasıl cezalandırılacağıdır. Bu sorunun çözümü için geleneksel suçlar kapsamında cezalandırılabilen kimi fiilleri de bünyesine alan bir suçun düzenlenmesi ise sorunu çözmekten çok kapsam ve uygulama sorunlarını beraberinde getirmiştir. Bu durum ise banka ve kredi kartları bakımından, eskiden hırsızlık ya da dolandırıcılık suçu olarak kabul edilen fiillerin yeni ve ayrı bir suç olarak düzenlenmesi sonucunu doğurmuştur.

Bu nedenle, sadece sistemin kullanılmasını konu edinen bir düzenleme yerine özellikle malvarlığına yönelik olarak ortaya çıkan bu suç bakımından hâlihazırdaki suçlarla çözülemeyen sorunun tespiti ve buna yönelik bir düzenlemenin yapılması gerekmektedir. Bilişim alanında işlenen diğer suçlar bakımından da geçerli olan bu yaklaşım bilgisayar aracılığıyla yarar sağlamada ise kişiye karşı hile yapıp kişinin hataya düşürülmesi söz konusu olmadan sistemin işleyişine ve bu kapsamda veri ve veri işleme faaliyetine hileli müdahaleler ile yarar sağlamanın cezalandırılabilirliği sorunu olarak karşımıza çıkmaktadır. Aşağıda TCK'nin bilişim alanında işlenen suçlar içerisinde 244. maddenin son fıkrası ve getirdiği diğer yeni suç tipleri ve diğer yenilikler, bu soruna getirdiği çözüm açısından değerlendirilecektir.

3. Türk Ceza Kanununda Bilişim Sistemleri Aracılığıyla Yarar Sağlama

a. Genel Olarak

765 Sayılı TCK’de bilişim sistemi aracılığıyla yarar sağlama, yukarıda belirtildiği üzere genel olarak Kanunun 525b maddesinde birinci fıkrada yarar sağlamak için sisteme ve veriye müdahale ve sistemin kullanılması suretiyle yarar sağlama şeklinde iki fıkra halinde yer almakta idi. TCK’de ise, 244. maddenin son fıkrasında bilişim sistemi aracılığıyla haksız yarar sağlamaya ilişkin bir düzenlemeye yer verilmiştir. 244. maddenin son fıkrasında *“Yukarıda fıkroda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız çıkar sağlamanın başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur”* hükmü yer almaktadır.

Bunun yanında Kanunda, banka ve kredi kartlarının hukuka aykırı kullanımına ilişkin 245. maddeyi bilişim alanında işlenen suçlar arasında düzenlenmiştir. Aynı şekilde Kanunda hırsızlık suçunun ve dolandırıcılık suçunun bilişim sistemleri aracılığıyla işlenmesi halini ağırlatıcı neden olarak Kanunun 142 ve 157. maddelerinde düzenlemiştir³⁴³.

TCK’de yer alan bu hükümler, 765 Sayılı TCK’nin 525/b 2. maddesinin uygulamada ortaya çıkardığı sorunlardan etkilenilerek kaleme alınmıştır. Bu nedenle, bilişim sistemlerinin kullanılmasının hırsızlık ve dolandırıcılık suçunun ağırlatıcı

³⁴³ *Dülger*,r 765 Sayılı TCK’nin 525b/ 2. fıkrasında düzenlenen suçun bu açıdan dört parçaya bölündüğünü ifade etmiştir. **DÜLGER**, s. 244

nedeni olarak öngörülmesi ve son olarak 245. maddede düzenlenen banka ve kredi kartlarının kötüye kullanımına ilişkin suçların, 765 Sayılı TCK'nin 525b/2. maddesinin, yukarıda incelendiği şekliyle özellikle diğer suçlar ile içtimaina ilişkin uygulamada ortaya çıkardığı sorunların giderilmesi amacıyla yönelik olarak düzenlendiğini söylemek mümkündür.

Burada da bilişim sistemleri aracılığıyla yarar sağlamanın dolandırıcılığın özel bir şekli olarak kabul edilmesine ve bu şekilde düzenlenmesine ilişkin soruna getirilen çözümün TCK'deki görünümünün ne olduğu açısından inceleme yapılacaktır. Bu nedenle bilişim sistemlerinin işleyişine ve veriye müdahale edilerek, kişiye karşı herhangi bir hileli hareketin yapılması ve kişinin aldatılması söz konusu olmadan yarar sağlamanın yukarıda aktarılan suçlar bakımından görünümü, incelemenin kapsamını oluşturmaktadır.

b. Suçun Kapsamı

i. Maddi Unsur Açısından

TCK'nin 244. maddesinin son fıkrasında 244. maddenin birinci fıkrasında düzenlenen fiillerin işlenmesi suretiyle failin kendisi veya başkasının yararına haksız çıkar sağlaması düzenlenmiştir. Yukarıda 244. maddenin birinci ve ikinci fıkrasında düzenlenen fiillere ilişkin ayrıntılı açıklamalara yer verildiğinden burada yarıca değinilmeyecektir.

Suçun maddi unsurunun 244. maddenin 1. ve 2. fıkrasında yer alan fiillerin gerçekleştirilmesi suretiyle yarar sağlanması³⁴⁴ olarak düzenlenmesi sonucunda 765

³⁴⁴ 244. maddenin son fıkrasında kendisi veya başkası yararına haksız çıkar sağlanmasından bahsedilmiştir. Bu hüküm 765 Sayılı TCK'nin 525/b 2. maddesinde yer alan “ yarar sağlanmasından” farklı bir şekilde kaleme alınmış olsa da TDK sözlüğünde yararın çıkar ile

Sayı 525/b TCK'nin maddesine göre suçun unsurlarının daha belirgin hale getirilmek istendiği görülmektedir. 244. maddenin 1. ve 2. fıkralarında yer alan hareketlerin gerçekleştirilmesi suretiyle yarar sağlanması esas alınması suretiyle suçun maddi unsuru bakımından kapsamının 765 Sayılı TCK'deki düzenlemeye göre daraltıldığı görülmektedir. Nitekim 244. maddenin son fıkrası incelendiğinde suçun işlenebilmesi için ya 244/1. maddede yer aldığı şekliyle sistemin işleyişinin engellenmesi veya bozulması ya da aynı maddenin 2. fıkrasında belirtildiği şekliyle bilişim sistemi içerisindeki verilerin bozulması, yok edilmesi, değiştirilmesi, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi gerekmektedir.

244. maddenin son fıkrası incelendiğinde, 765 Sayılı TCK'nin yarar sağlama amacıyla sisteme ve veriye müdahaleyi düzenleyen 525b 1. fıkrası ile aynı maddenin 2. fıkrasının unsurlarının, bir araya getirilmesi şeklinde olduğu görülmektedir. Sisteme ve veriye müdahaleye ilişkin hareketler suçun unsuru arasına alınmış ve bu haliyle 525b/ 1. fıkraya yakın bir düzenlemeye yer verilmiş; 525b 2. fıkranın unsuru olarak ortaya çıkan bilişim sisteminin kullanımı şeklinde geniş bir unsurdan vazgeçilmiş, fakat yarar sağlama unsuruna yer verilerek 765 Sayılı TCK'nin 525/b 1. maddesinde yer alan yarar sağlama amacıyla sisteme müdahale edilmesi unsurundan uzaklaştırılmıştır. Bu haliyle 765 Sayılı TCK'deki bilgisayar aracılığıyla yarar sağlamaya ilişkin geniş kapsamlı bir düzenlemeden vazgeçilmiştir.

Bu şekliyle, suçun unsurları bakımından belirginlik sağlanarak, özellikle 765 Sayılı TCK'nin 525b/2. maddesinde düzenlenen suçun uygulamada sorunlara yol açacağı yönündeki görüşler karşılanmaya çalışılmak istenmiştir.

eş anlamlı olarak kullanılması karşısında bu iki ifadenin özü itibarıyla birbiri ile aynı olduğu sonucuna varmak mümkündür. Yarar ve çıkar kelimelerinin anlamları için bkz. "Güncel Türkçe Sözlük" <http://www.tdk.gov.tr/>

ii. Düzenleme Şekli Açısından

244. maddenin son fıkrası incelendiğinde, fiilin başka bir suç oluşturmaması halinde söz konusu maddenin uygulanacağı hükmünün, madde metninde yer aldığı görülmektedir. Bu hükme göre, fiil, TCK ve diğer özel kanunlarda yer alan başka bir suçu oluşturuyorsa, bu madde kapsamında değerlendirilmeyecek ve ilgili maddelerde düzenlenen suçlara göre hüküm kurulacaktır.

Maddede, “*başka bir suçu oluşturmaması*” hükmüne yer verilmiş iken, madde gerekçesinde, “*Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.*” İfadesine yer verilmiştir³⁴⁵. Hüküm ile gerekçe arasında bir çelişkinin var olduğu açıkça görülmektedir. Maddede yer alan ifadeden fiilin daha ağır cezayı gerektirip gerektirmediğine bakılmaksızın başka bir suçu oluşturmaması halinde ilgili suçun uygulanacağı sonucu çıkartılmakta iken, gerekçe bunu daraltmakta ve ilgili suçun daha ağır ceza gerektirmesi şartını öngörmektedir. Bu itibarla gerekçe ile hüküm çelişmektedir ve de gerekçenin bağlayıcı olmaması karşısında gerekçeye itibar edilmemesi gerekir.

244. maddenin son fıkrasındaki hüküm ile 765 Sayılı TCK’nin 525b/ 2. maddesinde düzenlenen suça ilişkin olarak, Yargıtay kararlarında kimi yönlerden daraltılmakla birlikte söz konusu suçun kapsamının geniş olduğu yönünde ileri sürülen görüşlerin belirli bir yönden karşılanmak istendiği görülmektedir. Nitekim bu madde ile özellikle 765 Sayılı TCK’nin 525b/2. fıkrasının kapsamına ilişkin

³⁴⁵ Gerekçe için bkz., <http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc>.

sorunların ve de bu yöndeki eleştirilerin bu maddede dikkate alındığı ifade edilmiştir³⁴⁶. Bu açıdan 244. maddenin son fıkrası, suçların içtimaı bakımından ortaya çıkabilecek sorunların giderilebilmesine yönelik bir şekilde kaleme alınmak istenmiştir.

Bu haliyle, 244. maddenin son fıkrasında, başka bir suç oluşturmaması hükmüne yer verilmesi karşısında, *İçel*'in ifade ettiği şekliyle, yardımcı bir norm olarak düzenlendiği³⁴⁷ sonucuna varmak mümkündür.

Bilişim sisteminin işleyişine müdahale etmek suretiyle kişiye karşı herhangi bir hilenin ve bir kişinin hataya düşürülmesi ya da TCK'deki ifadeyle aldatılması söz konusu olmadan yarar sağlanmasına ilişkin olarak, dolandırıcılık suçunun

³⁴⁶ DÜLGER, s. 244.

³⁴⁷ *İçel* fiil ile ceza normları arasındaki ilişki yönünden fikri içtima yanında gerçekleşmesi mümkün olan diğer bir durumun, çeşitli normların aynı fiille ilgili görünmelerine rağmen, aslında bunlardan yalnız birinin uygulanabilmesi anlamında görünüşte içtima olarak ortaya çıktığını belirtmektedir. Yazar görünüşte içtimanın çeşitlerini “özel norm – genel norm”, “tüketen – tüketilen norm”, “asal – yardımcı norm ”, ilişkisi açısından üç grupta incelemektedir. Kayıhan İÇEL, *Suçların İçtimaı*, İstanbul 1972, s. 167 vd. Aynı yönde, DEMİRBAŞ, *Ceza Hukuku Genel Hükümler*, s. 445 vd. Ayrıca bkz., Veli Özer ÖZBEK, *Yeni Türk Ceza Kanununun Anlamı*, C. 1, Ankara, 2006, s. 506 vd.

İçel'e göre bir norm, açık ya da zımni bir şekilde, başka bir normun gerisine çekilirse, bu norma yardımcı norm ismi verilir ve böylece normun sonralığı ilkesi söz konusu olur, Bu nitelikteki normları sözü geçen ilke gereğince, aynı konuyu düzenlemiş normların tümü veya sadece kendilerinden daha ağır ceza ihtiva eden normlar karşısında ikinci planda kalırlar ve yalnız diğer normlar uygulanır, İÇEL, *Suçların İçtimaı*, s. 175.

Görünüşte içtimanın bir çeşidi olarak *İçel* tarafından incelenen asal – yardımcı norm ilişkisi için yazar, “Yardımcı normun sonralığı ilkesinin kapsamına giren içtima hallerinde, yardımcı normların ihtiva ettiği suçlar ile asal normların düzenlendiği suçlara bir arada bulunmaktadır. Ancak bu bir arada bulunuş görünüştedir: gerçekte fiile uygun asal normun metninde açık bir şekilde gösterilmiştir veya kanunun esas fikri (ratio legis), normlar arasındaki ilişkiler ve normun ihtiva ettiği suçun özellikleri aracılığı ile, söz konusu normun, yardımcı bir norm olduğu ve böylece asal normların kapsamına girmeyen hallerde uygulanabileceği sonucuna varılır” ifadesine yer vermiştir. İÇEL, *Suçların İçtimaı*, s. 209.

Buna karşın Toroslu, “özel normun önceliği ilkesinin” görünüşte normlar çatışmasına ilişkin sorunların çözümünde yeterli olacağını vurgulamıştır. TOROSLU, *Ceza Hukuku Genel Kısım*, s. 84.

unsurlarının gerçekleşmediği merkezinde, suçun unsurlarına ilişkin sorun bilişim sistemi aracılığıyla yarar sağlama suçunda gündeme gelmektedir. Türk Ceza Hukukunda bu sorun yerine , suçta kullanılan araç ya da suçun maddi konusu olarak bilişim sistemin varlığı noktasında, hukuki olmaktan çok teknik bir açıdan soruna yaklaşılması, 765 Sayılı TCK'nin 525b/2. maddesinde düzenlendiği şekliyle uygulama alanı geniş olan bir suçun düzenlenmesi sonucuna götürmüştür. Aynı yöndeki yaklaşımın devam ettirilmesi ve 765 Sayılı TCK'nin 525b/2. maddesine ilişkin sorunların da gündeme gelmesi, kanun koyucu tarafından 244. maddenin son fıkrasında düzenlenen hükmün yardımcı norm niteliğinde düzenlenmesi sonucuna götürmüştür.

Bilişim sistemi ve veriye müdahale edilmesi sonucunda yarar sağlamada sorunun, dolandırıcılık suçu bakımından hile ve kişinin aldatılmasına ilişkin suçun unsurlarının gerçekleşmediği şeklinde tespit edilmesi halinde, bu durumda soruna ilişkin çözüm, Alman ve İtalyan Ceza Kanunlarında yer aldığı gibi klasik dolandırıcılık suçunun özel bir şeklinin, dolandırıcılık suçunun düzenlendiği yerde, bilişim sistemleri aracılığıyla dolandırıcılık veya bilgisayar dolandırıcılığı olarak adlandırılan özel bir suçun düzenlenmesi şeklinde olabilecekti. Bunun yerine, 765 Sayılı TCK'de 525b/ 2. maddesindeki suça, TCK'de ise, 244. maddesinin son fıkrasında yer alan suça yer verilmesi, soruna, Türk Ceza Hukukunda farklı bir açıdan bakıldığını göstermesi bakımından önemlidir. Gerekçede hırsızlık, dolandırıcılık, emniyeti suiistimal ve zimmet suçunun unsurlarının gerçekleşmediğinden bahisle bu suçun düzenlendiğinin belirtilmesi de bu durumu destekler niteliktedir.

c. Bilişim Sistemleri Aracılığıyla Yarar Sağlama Suçunun Kapsamının Daraltılmasından Çıkan Sonuçlar

244. maddenin son fıkrasında düzenlenen suçun 244. maddenin 1. ve 2. fıkralarından yer alan seçimlik hareketlerin gerçekleştirilmesi suretiyle işlenebilmesi ve 244. maddenin son fıkrasının yardımcı norm olarak düzenlenmesi sonucunda, bilişim sistemleri aracılığıyla yarar sağlama suçunun uygulama alanının saptanması gerekmektedir. Aşağıda, 765 Sayılı TCK'nin 525b 2. fıkrasının uygulanması ile ilgili olarak Yargıtay kararlarında en çok tartışılan hırsızlık ve dolandırıcılık suçları açısından konu incelenecektir.

i. Hırsızlık Suçu Karşısında Bilişim Sistemi Aracılığıyla Yarar Sağlama

TCK'nin 244. maddesinin son fıkrasında, fiilin başka bir suçu oluşturmaması hükmüne yer verilmesi ve bu şekilde maddenin yardımcı norm olarak düzenlenmesi sonucunda, yararın konusunun taşınır bir malın elde edilmesi açısından, 244. maddenin son fıkrasında düzenlenen suçun hırsızlık suçu karşısında, asal norm – yardımcı norm ilişkisi açısından incelemek mümkündür. 244. maddenin son fıkrasında düzenlenen bilgisayar aracılığıyla yarar sağlama suçunun, bir yardımcı norm olarak düzenlenmesi karşısında, bilişim sistemine 244. maddenin son fıkrasında düzenlendiği şekliyle bir müdahalenin söz konusu olması ve bunun sonucunda bir taşınır mal elde edilmesi halinde fiilin, hırsızlık suçunu mu yoksa 244. maddenin son fıkrasında düzenlenen suçu mu oluşturacağının tartışılması gerekmektedir. 244. maddenin son fıkrasında yer alan suçun, taşınır bir malın elde edilmesi durumunu da kapsayan dolandırıcılık suçunun özel bir şekli olarak

düzenlenmemesi bu tartışmanın yapılmasını gerektirmektedir. Bu sorunun çözümünde, Türk Ceza Hukukunda otomatların kötüye kullanılmasına ilişkin olarak taşınır bir malın elde edilmiş olması durumunda, fiilin hırsızlık suçunu oluşturup oluşturmayacağına ilişkin tartışmalar önem arz etmektedir.

Bilindiği üzere, otomatların kötüye kullanılmasına ilişkin mal ve hizmet otomatları ayırımı açısından özellikle mal otomatlarından çeşitli müdahalelerle malın bedeli ödenmeksizin alınması durumunda hırsızlık suçu mu yoksa karşılıksız yararlanma suçunun mu oluşacağı tartışılmıştır. 765 Sayılı TCK'nin 521b maddesi ile ilgili olarak mal sahibinin otomat içerisindeki mal üzerinde egemenlik yetkisinin devam ettiği, bedelin ödenmesi halinde malın alınması yönünde mal sahibinin iradesinin devam ettiği ve egemenlik yetkisinin otomatın mekanizmasının harekete geçirilmesi ve malın bulunduğu yerden alınması suretiyle ihlal edilmiş olacağı ifade edilmiştir. Ayrıca, maddede fiilin daha ağır bir suçu oluşturmadığı takdirde bu madde uyarınca cezalandırılacağına ilişkin hükmün de yer alması karşısında mal otomatlarından bedelsiz olarak malın alınmasının hırsızlık suçu kapsamında değerlendirileceği sonucuna varılmıştır³⁴⁸.

Otomatlar ile sunulan hizmetler bakımından, bedelsiz yararlanmak için otomata yapılan her türlü manipülasyonun hile olarak kabul edilebileceği fakat hilenin kişiye karşı yapılmamış olduğundan kişinin hataya düşürülmesinin ya da TCK'deki ifadesiyle aldatılmasının söz konusu olmaması nedeniyle, dolandırıcılık suçu kapsamında değerlendirilemeyeceği bu nedenle bunlara ilişkin otomatların kötüye kullanılması şeklinde bir suça yer verildiğine ilişkin gerekçe, yararın konusunu bir taşınır malın oluşturması durumunda geçerliliğini kaybetmektedir.

³⁴⁸

ERDEM, s. 101 vd.; SOYASLAN, s. 379

Burada soruna mal sahibinin rızası dışında onun egemenlik alanında bulunan malın bulunduğu yerden alınması şeklinde gerçekleştiği noktasından yaklaşmış ve ayrıca 765 Sayılı TCK'nin 521b maddesindeki düzenleme nedeniyle otomatlardan bedeli ödenmek suretiyle elde edilebilen taşınır bir malın otomata müdahale edilmesi suretiyle bulunduğu yerden alınmasının hırsızlık suçunu oluşturacağı ifade edilmiştir.

Otomatlara müdahale edilerek bedeli ödenmeden taşınır bir malın alınmasının hırsızlık suçunu oluşturacağına ilişkin yukarıdaki gerekçelerin, sisteme ve veriye müdahale edilmesi suretiyle elde edilen yararın taşınır malın bulunduğu yerden alınması şeklinde gerçekleşen fiiller bakımından da geçerlidir.

244. maddenin son fıkrasında belirtilen şekillerde sisteme veya veriye müdahale edilmesi sonucunda taşınır bir malın yerinden alınması söz konusu olması halinde de hırsızlık suçu söz konusu olabilecektir. Burada da faydalanmak için bulunduğu bir yerden malın alınması söz konusudur. Malın üzerinde tasarrufun nasıl yapılacağına ilişkin mal sahibinin iradesi devam etmekte ve bu açıdan mal bulunduğu yerden alınmakla, mal sahibinin egemenlik alanından çıkartılmaktadır. Bu haliyle, TCK'nin 142. maddesinde hırsızlık suçunun ağırlatıcı nedeni olarak bilişim sistemlerinin kullanılmasının düzenlenmiş olması karşısında, nitelikli hırsızlık suçunun oluşabileceğini söylemek mümkündür.

Yararın sağlandığı anın saptanması, fiilin hangi suçu oluşturduğunun belirlenmesi bakımından ayrıca önem arz etmektedir. Taşınır malın elde edilmesinden önce herhangi bir yararın sağlandığı söylenemiyor ise bu durumda

hırsızlık suçunun gerçekleştiği sonucuna varılabilecektir³⁴⁹. Yararın sağlanması malın bulunduğu yerden alınmasından önceki bir aşamada gerçekleşmiş olup, malın elde edilmesi tali bir durum olarak ortaya çıkıyorsa, fiil 244/son madde kapsamında değerlendirilebilecektir.

ii. Dolandırıcılık Suçu Karşısında Bilişim Sistemi Aracılığıyla

Yarar Sağlama

Türk Ceza Kanununda, 765 Sayılı TCK'de olduğu şekliyle, bilişim sistemi ya da bilgisayar aracılığıyla yarar sağlamaya ilişkin her türlü ihtimali kapsayabilecek nitelikte bir düzenlemeye yer verilmemiştir. Bunun yerine yukarıda belirtildiği gibi sistem ve müdahaleyi esas alan ve bu şekilde yarar sağlanmasını kapsayan fiillere ilişkin yardımcı norm olarak suçun düzenlenmesi yoluna gidilmiştir.

Bilişim sistemi ya da bilgisayar aracılığıyla yarar sağlama, dolandırıcılık suçuna göre özel bir düzenleme olarak öngörüldüğünde “*yarar sağlama*” taşınır malın da içinde bulunduğu klasik dolandırıcılık suçunda yarar olarak kabul edilen, malvarlığına ilişkin her türlü artışı kapsayabilmektedir. Nitekim İtalyan Ceza Kanununda bu suç dolandırıcılığın özel bir şekli olarak düzenlenmiş ve sisteme ya da veriye müdahale edilmiş olması durumunda bir kişinin hataya düşürülmüş olması ve malvarlığında artışı sağlayan işlemin bir kişi tarafından yapılmış olması dikkate alınmayıp suç bilgisayar dolandırıcılığı olarak kabul edilmiştir.

İtalyan doktrininde de bilgisayar dolandırıcılığı olarak düzenlenen 640bis maddesinin niteliği ve uygulama alanı tartışma konusu olmuştur. İtalyan

³⁴⁹ Bu nedenle bir bankanın bilişim sistemine müdahale edilmesi suretiyle bankaya ait “atm”den, banka ya da kredi kartı kullanmadan para çekilmesi fiilinin hırsızlık suçunu oluşturacağını söylemek mümkündür.

Yargıtayının da kabul ettiği görüşe göre; bu suç dolandırıcılık suçunun özel bir şekli olup, bir kişinin hataya düşürülmüş olması zorunluluğu kaldırılmıştır. Diğer bir görüşe göre, bu suç dolandırıcılık suçunun unsurlarının hiçbir şekilde gerçekleşmediği durumları kapsamaktadır. Birinci görüşe göre, sistem ya da veriye müdahale, dolandırıcılık suçunda yer alan kişiye karşı hile yapılması sonucu kişinin hataya düşürülmesi şartının aranmasını ortadan kaldıran bir unsur olup, maddede belirtilen bir müdahalenin varlığı halinde, başka bir şeye bakılmaksızın fiilin 640bis maddesinde düzenlenen bilgisayar dolandırıcılığı suçunu oluşturacağı ifade edilmiştir. Buna karşın ikinci görüşe göre, failin ya da üçüncü bir kişinin malvarlığında meydana gelen kazandırıcı işlemin bir kişi tarafından yapılması halinde bu işlemin yapılmasına yol açan sisteme ve veriye müdahale, kişiye karşı kişinin hataya düşürülmesine yönelik bir davranışı oluşturacağı ve bu durumda, fiilin klasik dolandırıcılık suçu olarak nitelendirilebileceği belirtilmiştir. Buna karşın failin ya da üçüncü bir kişinin malvarlığında meydana gelen artışın doğrudan sisteme ve veriye müdahale edilmesi sonucunda gerçekleştirilmesi söz konusu ise, bu durumda İtalyan Ceza Kanunun 640bis maddesinde düzenlenen, bilgisayar dolandırıcılığının söz konusu olacağı ifade edilmiştir³⁵⁰.

244. maddenin son fıkrasında yer alan suçun yardımcı norm olarak düzenlenmiş olması ve dolandırıcılık suçunun özel bir şekli olarak düşünülmemesi karşısında bu suçun unsurlarının ve klasik dolandırıcılık suçuna göre sınırının belirlenmesi gerekmektedir. Bu açıdan İtalyan Ceza Kanununda yer alan bilgisayar aracılığıyla dolandırıcılık suçu hakkında ileri sürülen ikinci görüşün, 244.maddenin

³⁵⁰ Aktaran, Felicia BONANO, **La frode informatica**, s. 9 vd., <http://www.computerlaw.it/public/bonannofrodeinfo.pdf>

son fıkrasındaki düzenlenen yararın sağlanmasına ilişkin işlemin gerçekleştirilmesi açısından geçerli olacağını söylemek mümkündür. Bu durumda yararın kapsamını oluşturan kazandırıcı işlemin bir kişi tarafından mı yapıldığı yoksa sisteme ve veriye müdahale sonucunda yararın doğrudan müdahale sonucunda mı sağlandığının saptanması gerekmektedir.

Sisteme ve veriye müdahalenin yapılmış olması sonrasında, doğrudan bir yarar sağlanmıyor ve yararın sağlanmasına ilişkin işlem bir kişi tarafından gerçekleştiriliyor ise, bu durumda klasik dolandırıcılık suçu kapsamında değerlendirilmesi gerektiğini söylemek mümkündür. Bu durumda sisteme ve veriye müdahale teşkil eden hareketler kişinin aldatılmasına yönelik hileli hareketler kapsamında değerlendirilebilmektedir. Dolandırıcılık suçu bakımından yarar yanında zararın oluşması şartı, suçun teşebbüs aşamasında kalması ya da tamamlanmış olması bakımından önem arz etmektedir.

Bunun dışında, bir sisteme ya da sistem içerisindeki veriye müdahale teşkil etmeyen fakat bir bilişim sisteminin kullanılması sonucunda yarar sağlama hallerini kapsayan fiillerin, klasik dolandırıcılık suçu kapsamında değerlendirilmesi mümkündür. Bir bankanın müşterileri hakkında bilgi güncellemesi yapacağı gerekçesiyle ve ilgili bilgilerin gönderilmesine ilişkin e-postaların gönderilmesi sonucu³⁵¹ ya da İnternet üzerinden alışveriş imkanı sağlayan bir sitenin taklit edilmesi sonucunda, buradan alışveriş yapılabileceğine ilişkin hileli hareketlerle kişileri aldatıp yarar sağlama hallerinin dolandırıcılık suçu kapsamında

³⁵¹ Örnek için bkz, **KARAGÜLMEZ**, s. 194

değerlendirilmesi gerektiğini söylemek mümkündür³⁵². Bu olasılıkta da yarar yanında bir zararın oluşması dolandırıcılık suçunun teşebbüs aşamasında kalması ya da tamamlanmış olması bakımından önem arz etmektedir.

Yukarıda aktarılan her iki ihtimalde, TCK'nin 157. maddesinin f bendinde, bilişim sistemleri aracılığıyla fiili gerçekleştirilmesinin ağırlatıcı neden olarak düzenlenmesi karşısında, nitelikli dolandırıcılık suçunun söz konusu olabileceği sonucuna varmak mümkündür.

iii. Banka ve Kredi Kartlarının Kötüye Kullanılması

Bilişim suçlarına ilişkin olarak ceza mevzuatlarında yer verilen suçlar incelendiğinde, söz konusu suçlar ile hali hazırda ceza mevzuatlarında yer alan suçlar bakımından özellikle suçun unsurlarında ortaya çıkan sorunlar nedeniyle cezalandırılmayan ya da cezalandırılmasında çeşitli sorunlara yol açan fiiller düzenlendiği görülmektedir. Fakat bilişim alanında suçlara ilişkin 765 Sayılı TCK'deki suçlar, suçun unsurlarının geniş tutulması nedeniyle halihazırda Kanunda yer alan diğer suçlar kapsamında değerlendirilebilen birçok fiil bakımından da uygulanabilir bir nitelik kazanmıştı. Yukarıda da incelendiği üzere bu durumun en belirgin şekilde ortaya çıktığı suç, 525b/2. maddesinde düzenlenen bilgisayar aracılığıyla yarar sağlama suçudur. Yine yukarıda incelendiği üzere bu suçun unsurunun birçok fiili kapsayacak şekilde düzenlenmesi, özellikle malvarlığına karşı işlenen diğer suçlar kapsamında değerlendirilebilecek birçok fiilin bu madde

³⁵² Hırsızlık ve de dolandırıcılık suçunun 244. maddenin son fıkrası kapsamında uygulanabilirliği hakkında yukarıda açıklanan hususlardan yola çıkarak *Yazıcıoğlu*'nun hırsızlık suçunun uygulanabilmesinin mümkün olmadığı, dolandırıcılık suçu bakımından ise, hilenin sisteme yapılmış olmasında kişinin rolünün bir araç teşkil etmekten öteye gidemeyeceği şeklindeki görüşlerine katılmamaktayız. **YAZICIOĞLU, Bilişim Suçlarının Genel Değerlendirilmesi**, s. 398-399

kapsamına girmesine ilişkin tartışmaları da beraberinde getirmiş Yargıtay kararlarında da bu husus etkisini göstermiştir.

Bu kapsamda, özellikle banka ve kredi kartlarının hukuka aykırı kullanılması suretiyle yarar sağlanması fiilleri de bu gelişmeden etkilenmiş ve bu kartların ağırlıklı olarak bilişim sistemine dayalı olarak kullanılabilmesi, banka ve kredi kartlarının kullanılması suretiyle yarar sağlama fiillerinin de 765 Sayılı TCK'nin 525b/ 2. maddesi kapsamında olduğuna ilişkin yargı kararlarına da yansıyan bir eğilimin ortaya çıkmasına neden olmuştur.

Bunun sonucunda, öncelikli olarak haksız olarak ele geçirilen banka kartları ile “atm”lerden para çekilmesi fiillerinin, “atm”lerin bir bilişim sistemi olması ve bu kartlarla bilişim sisteminin kullanıldığı kabulü sonucunda, 525b/ 2. maddesinde düzenlenen bilgisayar aracılığıyla yarar sağlama suçunu oluşturduğu sonucuna varılmıştır. Devamında banka veya kredi kartının hile ile ele geçirilmesi sonucunda kullanılmasına ilişkin fiillerin bu madde kapsamında değerlendirilip değerlendirilemeyeceği tartışılmış, bu hususa ilişkin olarak Yargıtay birbirinden farklı kararlar vermiştir. Bunun ötesinde kredi kartlarının pos makinelerinde kullanılması suretiyle yarar sağlanmasına ilişkin birtakım fiiller de bu suç kapsamında değerlendirilmek istenmiştir.

TCK'de ise bilişim alanında işlenen suçlar yeniden düzenlenmiş ve yukarıda belirtildiği üzere, 245. maddenin son fıkrasında düzenlenen bilişim sistemi aracılığıyla yarar sağlama suçunun unsurlarının, 765 Sayılı TCK'nin 525b/2. fıkrasına göre daha belirgin hale getirilmesi ve yardımcı norm olarak düzenlenmesi nedeniyle uygulanma alanı daraltılmıştır. Ayrıca, TCK'de banka ve kredi kartlarının

hukuka aykırı kullanılması suretiyle yarar sağlanmasına ilişkin bir takım fiiller, 245. maddede ayrıca düzenlenmiştir³⁵³.

Madde gerekçesinde ise, bu tür fiillerin ayrı bir suç olarak düzenlenmesine ilişkin, *“Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmeleri uygun görülmüştür.”* denmiştir³⁵⁴. Bu gerekçe incelendiğinde, kredi kartlarının hukuka aykırı kullanılarak yarar sağlanması fiillerinde sorunun, ağırlıklı olarak malvarlığına karşı suçlar içerisinde hangisine vücut verdiği noktasında toplandığı ifade edilerek, 765 Sayılı TCK’nin 525b/2. fıkrasının ortaya çıkardığı sorunun göz

³⁵³ 245. madde incelendiğinde banka ve kredi kartlarının kötüye kullanımı ile ilgili olarak 3 farklı fiilin düzenleme konusu yapıldığı görülmektedir. 245. maddenin birinci fıkrasında hukuka aykırı olarak ele geçirilen ya da elde bulundurulmuş kartın ilgili kişinin rızası dışında kullanılarak yarar sağlanması, ikinci fıkrasında başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, satın alınması veya kabul edilmesi, üçüncü fıkrada ise sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartının kullanılması suretiyle yarar sağlanması fiilleri düzenlenmiş bulunmaktadır. Fiilin üçüncü fıkraya göre cezalandırılabilmesi için daha ağır bir cezayı gerektiren bir suç oluşturulması gerektiği belirtilmiştir. 245. madde hakkında ayrıntılı olarak bkz., **KURT**, s. 176 vd; **MERAN, Suçları** s. 378 vd; s. 195 vd.

Bunun yanında 5464 s. Banka ve Kredi Kartları Kanununda da kredi kartlarının kötüye kullanımı ile ilişkili suçlara yer verildiği görülmektedir. Kanunun *“Sahte belge düzenlenmesi”* başlıklı 36. maddesinde *“Gerçeğe aykırı olarak harcama belgesi, nakit ödeme belgesi ya da alacak belgesi düzenlemek veya bu belgelerde ne surette olursa olsun tahrifat yapmak suretiyle kendisine veya başkasına yarar sağlayanlar, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılırlar.”* hükmüne yer verilmiştir. Aynı Kanunun *“Gerçeğe aykırı beyan, sözleşme ve eki belgelerde sahtecilik”* başlıklı 37. maddesinde ise, *“Banka kartı veya kredi kartını kaybettiği ya da çaldığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar bir yıldan üç yıla kadar hapis ve ikibin güne kadar adli para cezası ile cezalandırılırlar. ..Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler.”* hükümlerine yer verilmiştir.

³⁵⁴ Aynı yönde **DÖNMEZER, Kişilere ve Mala Karşı Cürümler** s. 630, **YAZICIOĞLU**, s. 411, Ayrıca bkz., Yılmaz **YAZICIOĞLU, Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı**, Uluslararası İnternet Hukuku Sempozyumu, 21-22 Mayıs 2001, İzmir, Dokuz Eylül Üniversitesi Yayını, 2002, s. 469.

ardı edildiđi görlmektedir. Bu soruna, deđinilmemesi ise, bir yandan dzenleme yerine iliřkin soru iřaretlerini beraberinde getirirken, diđer bir yandan aslında bu tr fiillerin ađırlıklı olarak malvarlıđına karřı suęlar kapsamında deđerlendirilmesine iliřkin bir geręeđin tespiti bakımından dikkate deđerdir.

Banka ve kredi kartlarının ktye kullanılmasına iliřkin fiiller, madde gerekęesinde de belirtildiđi zere, duruma gre aslında genel olarak hırsızlık, dolandırıcılık ya da gveni ktye kullanma gibi malvarlıđına karřı suęlar ve evrakta sahtecilik suęları arasında deđerlendirilebilecek fiillerdir. Fakat gerekęede belirtilenin aksine sayılan bu suęlardan hangisinin bu tr fiillere uygulanacađına iliřkin uygulamada bir sorun ortaya çıkmamıř, bunun aksine, bu suęlar kapsamında deđerlendirilen fiillerin, sırf biliřim sistemi kullanılmıř olması nedeniyle 765 Sayılı TCK'nin 525b/2. maddesinin kapsamına sokulmasına iliřkin ęeřitli sorunlar gndeme gelmiřtir. Uygulamada sorunların 525b/2 . maddesinin uygulanabilirliđine iliřkin olması ise, 245. maddenin biliřim alanında iřlenen suęlar arasında dzenlenmesine yol aęmıřtır.

Yukarıda incelendiđi zere, banka ve kredi kartlarının hukuka aykırı kullanımında, 765 Sayılı TCK'nin yrrlkte olduđu dnemde sorun, bu tr fiillerin 765 Sayılı TCK'nin 525b/2. maddesinde dzenlenen suęu oluřturup oluřturmadıđıdır. Bu nedenle sorunun kaynađını 765 Sayılı TCK'nin 525b/2. maddesidir. Biliřim sistemi aracılıđıyla yarar sađlamaya iliřkin 244. maddenin son fıkrasının yardımcı norm olarak dzenlenmesi karřısında, banka ve kredi kartlarının hukuka aykırı kullanımına iliřkin fiillere, malvarlıđına karřı suęlar ve ayrıca evrakta sahtecilik suęlarına iliřkin hkmlerin 245. madde olmasa da uygulanması mmknd.

Madde gerekçesinde bu sorun göz ardı edilerek, malvarlığına karşı suçların ve ayrıca evrakta sahtecilik suçlarının bu tür fiillere uygulanmasında içtihat farklılığına gidildiği ifade edilmektedir. Madde gerekçesi ile suçun düzenlendiği yer arasında da uyumsuzluk söz konusudur.

Madde gerekçesinde de ifade edildiği üzere, banka ve kredi kartlarının hukuka aykırı kullanımına ilişkin fiiller ağırlıklı olarak malvarlığına karşı hali hazırda TCK içerisinde düzenlenen suçları oluşturmaktadır. Buna karşın TCK’de, bilişim alanında suçlar arasında 245. maddede söz konusu suç düzenlenmiştir. Suçun düzenleniş yeri bakımından ortaya çıkan bu tercih esas alınarak, sırf bu nedenden dolayı, banka ve kredi kartlarının hukuka aykırı kullanımına ilişkin fiillerin bilişim alanında işlenen suçlar arasında incelenmesi zorunluluğu da doğmamaktadır. Maddenin düzenleniş biçiminden ve kapsamından dolayı da ayrı bir çalışmanın konusunu oluşturabilecek birçok sorunu beraberinde getirmesi nedeniyle, burada incelenmeyecektir.

Sonuç olarak, 244. maddenin son fıkrasında yer alan suçun kapsamı karşısında TCK. bakımından kredi kartlarının hukuka aykırı kullanılması suretiyle yarar sağlanmasına ilişkin 245. maddede düzenlenen fiiller bir bilişim sistemi kullanılarak ya da 244. maddede belirtilen şekilde sisteme ve veriye müdahale edilerek gerçekleştirilmesine bakılmaksızın 245. madde kapsamında değerlendirilebilecektir³⁵⁵.

³⁵⁵ 245. maddenin kaleme alınış şeklinden bu kartların kullanılması suretiyle yarar sağlamaya ilişkin bir sorunun özellikle 1. fıkra bakımından hala devam ettiği söylenebilecekti. Nitekim maddede özellikle fiilen bir kartın esas alınarak kullanılmasından bahsedilmektedir. *Kurt*’un da belirttiği üzere bu madde lafzından hareketle kart numarasının kullanılmasının bu madde kapsamında olmadığını söylemek mümkündür. Bu durum ise özellikle İnternetin yaygınlaşması ile gelişen elektronik ticaret kapsamında yaygın ödeme

aracı olarak kredi kartının hukuka aykırı kullanılmasına ilişkin birçok fiili madde kapsamında bırakmaktadır. Özellikle elektronik ticarete kartın üzerinde bulunan ilgili bilgilerin kullanılması söz konusu olup kartın fiilen kullanılması ya da elde bulundurulması gerekmemektedir. Bu tür durumlarda sadece başkasına ait kart numarasının elde edilerek kullanılması halinde ise maddenin lafzından hareketle 245. maddenin uygulanamayacağı dile getirilebilecektir. Bu sorunun özellikle kredi kartı bakımından 5464 s. Kanunla giderildiği görülmektedir. Nitekim 5464 s. Banka ve Kredi Kartları Kanunun 3. maddesinin d bendine göre banka kartı, mevduat hesabı veya özel cari hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kart, e bendine göre kredi kartı ise, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan B.lı kartı veya fiziki varlığı bulunmayan kart numarası anlamına gelmektedir. Bu açıdan 245. madde yer alan kredi kartının 5464 s. Kanunda tanımlanan kartı ifade ettiği kabul edilecek olursa bu durumda fiilen bir kartın kullanılması yanında kart üzerindeki bilgilerin kullanılması da 245. madde kapsamında değerlendirilebilecektir. Bkz., **KURT**, s. 187.

ÜÇÜNCÜ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI

I. GENEL OLARAK KİŞİSEL VERİLERİN KORUNMASI

Bilişim teknolojisinin gelişmesi ve kullanımının yaygınlaşması genel olarak temel hak ve hürriyetlerin korunmasını, özel olarak da özel hayatın gizliliği kapsamında değerlendirilen kişisel verilerin korunması sorununu da beraberinde getirmiştir. 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 verilerin bilişim sistemleri aracılığıyla işlenmesi karşısında temel hak ve hürriyetlerin ve özellikle özel yaşamın gizliliğinin korunmasıdır³⁵⁶.

Kişisel verilerin işlenmesi karşısında temel hak ve hürriyetlerin ve özellikle özel hayatın korunması 1970’li yıllardan itibaren yoğun olarak tartışılmaya başlanmış ve kişisel verilerin korunmasına, işlenmesine ilişkin düzenlemeler ortaya

³⁵⁶ Aynı yönde, Durmuş **TEZCAN**, *Bilgisayar Karşısında Özel Hayatın Korunması*, Anayasa Dergisi, Cilt 8, 1991, s. 385. <http://www.anayasa.gov.tr/eskisite/anyarg8/dtezcan.pdf>

çıkmiştir³⁵⁷. Kişisel verilerin korunması uluslararası düzeyde de ele alınmıştır. nitekim Avrupa Konseyi 1974, 1975 yıllarında iki karar çıkarmıştır³⁵⁸. Ardından 1981’de “*Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme*” imzaya açılmış ve adı geçen sözleşme 1.10.1985 tarihinde yürürlüğe girmiştir³⁵⁹. OECD tarafından 1980 yılında, kişisel verilerin işlenmesine ilişkin bağlayıcı olmayan ilkeler³⁶⁰, Birleşmiş Milletler tarafından da 1990 yılında kişisel verilerin işlenmesine ilişkin tavsiye kararı yayımlanmıştır³⁶¹. Avrupa Birliğinde ise, Avrupa Parlamentosu ve Konsey 1995

³⁵⁷ 1973 tarihli İsveç Veri Koruma Kanunu kişisel verilerin korunmasına ilişkin ülke düzeyinde ilk düzenlemedir. Bu tarihten önce Almanya Hessen Eyaleti, Kişisel Veri Koruma Kanununu yürürlüğe koymuştur (1971). Kişisel verilerin korunmasına ilişkin ülke mevzuatları hakkında ayrıntılı bilgi için bkz., http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/National_laws/NATIONALLAWS-EN.asp#TopOfPage (kontrol tarihi 28.05.2005).

³⁵⁸ “**Resolution (74) 29 on the protection of individuals vis-à-vis electronic data banks in the public sector**”; “**Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector**”, http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/2CM.asp#TopOfPage (kontrol tarihi 28.05.2005)

³⁵⁹ “**Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**” (ECT no. 108) Sözleşmenin İngilizce metni için bkz., <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (kontrol tarihi 28.05.2005); Türkçe resmi çevirisi için bkz., “**Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme**” <http://www.uhdigm.adalet.gov.tr/kisiverkorun.htm> (kontrol tarihi 28.05.2005). Bundan sonra “**Sözleşme**” olarak anılacaktır.

³⁶⁰ İngilizce tam metin için bkz., “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” <http://www1.oecd.org/publications/e-book/9302011E.PDF> (kontrol tarihi 28.05.2005). Bundan sonra “**OECD İlkeleri**” olarak anılacaktır.

³⁶¹ İngilizce tam metni için bkz., “**United Nations, Guidelines Concerning Computerized Personal Data Files**”, www.datenschutz-berlin.de/gesetze/internat/aen.htm (kontrol tarihi 28.05.2005). Bundan sonra “**BM İlkeleri**” olarak anılacaktır.

yılında “*Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Tür Verilerin Serbest Dolaşımı Yönergesi*³⁶²”ni kabul etmiştir³⁶³.

Türkiye’de ise kişisel verilerin korunmasına ilişkin özel bir düzenleme bulunmamaktadır. “*Kişisel Verilerin Korunması Kanunu Tasarısı*” halen Başbakanlıkta olup henüz yasalaşmamıştır. TCK’de ise, “*Özel Hayata ve Hayatın Gizli Alanı Karşı Suçlar*” başlıklı 9. bölümünde, 135 vd. maddelerde kişisel verilerin korunmasına ilişkin suçlara yer verilmiştir.

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 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. Nitekim Öntasarıda da bu yaklaşım esas alınarak suçların düzenlendiği görülmektedir. Aynı yaklaşım

³⁶² İngilizce tam metni için bkz., “DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm (kontrol tarihi 28.05.2005). Bundan sonra “*Yönerge*” olarak anılacaktır.

³⁶³ Yukarıda aktarılan kişisel verilerin korunmasına ilişkin genel düzenlemeler olup, Avrupa Konseyi ve Avrupa Birliği içerisinde kişisel verilerin korunmasına ilişkin özel düzenlemeler de bulunmaktadır. Avrupa Konseyi içerisinde kişisel verilerin korunmasına ilişkin tavsiye kararları için bkz., http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/2CM.asp#TopOfPage (kontrol tarihi 28.05.2005).

12.05. 2003 tarihinde TBMM'ye sunulan Türk Ceza Kanunu Tasarısının 197. vd. maddelerine de hakimdir. 5237 S. TCK'de ise, bu hususlar suçun unsurları arasından genel olarak çıkartılmıştır.

Kişisel verilerin korunması, özel hayatın gizliliğinin korunmasının bir yönü olarak bir çok hukuk dalını ilgilendiren bir konudur. Bu haliyle devlet- birey, bireyler arası ilişkileri çeşitli yönleriyle etkilemesi nedeniyle hem kamu hukuku hem de özel hukuk bakımından etkileri söz konusudur. Söz konusu karmaşıklık bir çok ülkede kişisel verilerin işlenmesine ilişkin usul ve esasların özel bir Kanunla düzenlenmesi sonucunu doğurmaktadır. Kişisel verilerin korunmasına ilişkin suçlar da kişisel verilerin işlenmesine ilişkin usul ve esaslara uymama olarak ifade edilen çeşitli fiillerin, suç olarak düzenlenmesi şeklindedir.

Bu nedenlerle TCK'de yer alan kişisel verilerin korunmasına ilişkin suçların daha iyi anlaşılabilmesi bakımından aşağıda kişisel verilerin korunmasının amacı olarak özel hayatın bir yönünü oluşturan veri mahremiyetine değinilecektir. TCK'de yer alan kişisel verilerin korunmasına ilişkin suçlar da, kişisel verilerin işlenmesinde usul ve esasların 135. vd. maddelerindeki görünümü açısından incelenecektir.

II. KİŞİSEL VERİLERİN KORUNMASININ AMACI – VERİ/ENFORMASYON MAHREMİYETİ

“Kişi hakkında kişinin bilinmesini ya da bilinebilmesini sağlayan her türlü bilgi ve enformasyonu içeren veriler” olarak tanımlanan kişisel veriler, kişinin kendisi ve yaşantısı hakkında bilgi veya enformasyon içermesi ya da bunları elde etme aracı olarak kullanılması nedeniyle özel hayat ile yakından ilişkili olup, özel

hayat kapsamındadır. Kişisel verilerin korunmasına ilişkin düzenlemeler ise, gelişen bilişim teknolojileri sonucunda kişilere ait verilerin işleme 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 taşımaktadır³⁶⁴. Nitekim kişisel verilerin korunmasına ilişkin Sözleşmenin konu ve amaç başlıklı 1. maddesinde “*Bu Sözleşmenin amacı her Akit Devlet ülkesinde, uyruğu veya ikametgâhı ne olursa olsun tüm gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin, otomatik bilgi işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır.*” ifadesine yer verilmiştir. Aynı şekilde Yönergenin 1. maddesinde, Yönergenin amacının kişisel verilerin işlenmesi karşısında kişilerin temel hak ve özgürlüklerinin ve özellikle özel hayatın gizliliğinin korunması olduğu açıkça belirtilmektedir.

Özel hayatın gizliliğine ilişkin olarak ayrıntılı bir incelemeye girmeksizin özel hayatın gizliliğini, birbiriyle ilişkili 4 başlık altında incelemek mümkündür. Bu açıdan özel hayatın gizliliği, kişinin üstünün, özel kâğıtlarının ve eşyasının dokunulmazlığı, konut dokunulmazlığı gibi hususları içeren “*bölgesel mahremiyet*”; kişinin mektuplarının, telefon görüşmelerinin, e-posta ve diğer iletişim olanaklarını içeren “*haberleşmenin gizliği*”; kişinin vücut bütünlüğüne yönelik genetik testi, uyuşturucu testi gibi müdahaleleri içeren “*vücut bütünlüğüne ilişkin mahremiyet*”;

³⁶⁴ J. Colin **BENNET**, *Regulating Privacy: Data Protection and Public Policy in Europe and United States*, Cornell University Press , Ithaca and London 1992, s.vii; *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments*, <http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf>, s. 8 (kontrol tarihi 13.03.05); Priscilla M. **REGAN**, *Legislating Privacy. Techonology, Social Vaules, and Public Policy*, The University of North Carolina Press 1995, s. 69–70.

son olarak kişisel verilerin toplanması ve kullanılması ve genel olarak işlenmesi sürecini kapsayan “*veri mahremiyeti*” başlıkları altında toplanabilir³⁶⁵.

Özel hayatın gizliliğinin korunmasının bir yönü olarak karşımıza çıkan kişisel verilerin korunması ise, özel hayatın gizliliğinin korunması kapsamında “veri ya da enformasyon mahremiyeti”ne karşılık gelmektedir³⁶⁶. Enformasyon mahremiyetine ilişkin tartışmalar, genel olarak kişi hakkındaki enformasyonun işlenmesi süreciyle bağlantılı olarak 20 yüzyılın ikinci yarısından itibaren ortaya çıkan sosyo-ekonomik dönüşüm içerisinde, bilişim teknolojilerinin ve özellikle bilgisayarların etkin olarak kullanılmaya başlanmasıyla birlikte ortaya çıkmıştır. Veri mahremiyeti bu süreç içerisinde kişi hakkındaki bilgi ya da enformasyonun toplanması, kullanılması ve iletilmesi, genel olarak bilgisayarlar aracılığıyla işleme sürecini kapsayan ve “*veri gözetimi*” olarak adlandırılan bu duruma tepki olarak karşımıza çıkmaktadır³⁶⁷.

Özel hayatın gizliliğinin bozulması ya da özel hayatın gizliliğine müdahale³⁶⁸ olarak gözetim, *Westin’e* göre, *fiziksel gözetim*, *psikolojik gözetim* ve *veri gözetimi* şeklinde üç başlık altında toplanabilir. Yazar “*fiziksel gözetim*”i kişinin bulunduğu

³⁶⁵ **Privacy and Human Rights 2002**, s.3

³⁶⁶ James MICHAEL, *Privacy and Human Rights: an International and Comparative Study, with Special Reference to Development in Information Technology*, Unesco 1994, s. 3; Simone FISCHER-HÜBNER, *Privacy and Security at Risk in the Global Information Society*, Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Edit. Douglas THOMAS - Brian D. LOADER, Routledge 2000, s. 174; **Privacy and Human Rights 2002**, s.3.

³⁶⁷ George B. TRUBOW, *Protecting Informational Privacy in the Information Society*, 10 N. Ill. U. L. Rev. 1989-1990, s. 521.; LLOYD, s.39 vd.

³⁶⁸ *Westin* özel hayatın gizliliğinin “*kişinin kendisinin açığa vurması*”, “*merak*” ve “*gözetim*” yoluyla bozulabileceğini; *Gross*, ise özel hayatın gizliliğinin o toplum içinde yer alan otorite veya toplum içinde yaşayan diğer kişiler tarafından yapılan müdahaleler yoluyla bozulabileceğini belirtmektedir. Ayrıntılı bilgi için bkz., Alan F. WESTIN, *Privacy and Freedom*, New York 1970, s. 52 vd; Hyman GROSS, *Privacy-Its Legal Protection*, New York 1964, s. 1. Özel hayatın gizliliğinin bozulması hakkında ayrıca bkz. Oya ARASLI, *Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi*, yayımlanmamış doçentlik tezi, Ankara, 1979 s. 11 vd.

yerin hareketlerinin konuşmalarının ya da özel yazışmalarının kişinin bilgisi veya rızası dışında optik ya da akustik araçlarla gözetlenmesi; “*psikolojik gözetim*”i, yazılı ya da sözlü testlerin ya da araçların veya maddelerin kullanılması suretiyle kişiden isteyerek vermediği bilgileri ya da enformasyonu elde etme veya kişinin kendisinin özel hayatı ve kişiliği bakımından önemli olabilecek hususları farkında olmadan açığa çıkarma; “*veri gözetimi*” ise veri işleme makineleri aracılığıyla kişi veya gruplar hakkında bilginin ya da enformasyonun toplanması, değişimi ve kullanımı olarak tanımlamaktadır³⁶⁹.

1960’lı yıllardan başlayarak veri kaydetme faaliyetinde ortaya çıkan artış ve veri işleme sürecinde bilgisayarların etkin olarak kullanılması³⁷⁰, gözetimin bir parçasını oluşturan ve yeni bir olgu olmayan³⁷¹ veri gözetimini arttıran iki etkindir. Bu iki etken, asıl olarak sosyo-ekonomik dönüşüm içerisinde modern organizasyonların yönetim ve etkin karar alma süreçlerinde ve devletlerin faaliyetlerinin artması sonucu bu faaliyetlerin rasyonel bir şekilde yürütülmesinde kişisel verilere artan ihtiyaç ile bağlantılıdır³⁷².

³⁶⁹ **WESTIN**, s.52, 68 vd.; Aynı yönde, **LLOYD**, s. 39 vd. Özel hayatın gizliliğine yönelik bir tehdit olarak “gözetim” ve bilişim sistemlerinin gözetim aracı olarak kullanılması hakkında ayrıca bkz., Arthur R. **MILLER**, *The Assault on Privacy: Computerrs, Data Banks and Dossiers*, The University of Michigan Pres, 2. B. 1971, s. 38 vd.,

³⁷⁰ **REGAN**, s. 68.

³⁷¹ Modern toplumlarda gözetim ve gözetimin gelişimi hakkında bkz., David **LYON**, *Elektronik Göz: Gözetim Toplumunun Yükselişi*, Çev. Dilek Hattatoğlu, Sarmal Yayınevi, 1. B. 1997, s. 39 vd.

³⁷² **REGAN**, s 68. Ayrıca bkz. **WESTIN**, s. 158 vd.; Willis H. **WARE**, *Privacy and Information Technology-The Years Ahead*, Computers and Privacy in the Next Decade, Edit. Lance J. Hoffman, Academic Press 1980, s. 9 vd.; James B. **RULE** – Douglas **McADAM** – Linda **STEARNS** – David **UGLOW**, *Preserving Individual Autonomy in an Information-Oriented Society*, Computers and Privacy in the Next Decade, Edit. Lance J. Hoffman, Academic Press 1980, s. 65 vd.

Yukarıda belirtilen nedenlerle, bilgisayar sistemlerinin yaygınlaşması ve büyük miktarda verileri çok hızlı bir şekilde işleme ve iletme kapasitelerinin kişisel verilerin oluşturulması, saklanması ve kullanılmasında başta gelen araç olması³⁷³ ve bunun sonucunda veri gözetiminin bilgisayar merkezli bir yapıya bürünerek artması, özel hayatın gizliliğinin korunmasına ilişkin kolaylığı ortadan kaldırmıştır³⁷⁴.

³⁷³ Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973: Transmittal Letter and Foreword <http://aspe.os.dhhs.gov/datacncl/1973privacy/foreword.htm>

Veri madenciliği (data mining) adı verilen uygulama, bilgisayar sistemleri aracılığıyla kişisel verilerin elde edilmesinde ve işlenmesinde önemli bir örnek oluşturmaktadır. Belirli bir veri tabanı içerisinde birbiriyle ilgili verileri daha önceden bilinmeyen bağlantıların çeşitli yazılımlar kullanmak suretiyle ortaya çıkarılması faaliyeti olarak tanımlanabilecek veri madenciliği, bilgisayarlar aracılığıyla kişisel verilerin işlenmesinde etkin olarak kullanılmaktadır. Veri madenciliği genel olarak dört aşamayı içerir. *Birinci aşamada* veri bankalarından ve diğer veri tabanlarından toplanan verilerin hatalı, eksik ve ilgisiz olanları ayrıştırılır ve ayrıştırılan bu veri tek bir veri ambarında (data warehouse) toplanır. *İkinci aşamada* önceden belirli olan strateji çerçevesinde veri ambarından örnek veriler seçilir ki bu strateji çerçevesinde seçilen örnek veriler öngörülen hedef ile ilgilidir. *Üçüncü aşama* veri madenciliği teknolojisinin seçilmiş olan veriye uygulanmasıdır. *Dördüncü aşama* ise veri madenciliği teknolojisi sonucu ortaya çıkan sonuçların analizidir. Bu açıdan veri madenciliği uygulamalarının, veri madenciliği programının belirli bir organizasyonun kendi verileri üzerinde analiz yapma ve “spyware” adı verilen programların kullanıcılarının bilgisayarlarına yüklenmesi suretiyle, kullanıcının faaliyetlerinin kaydedilmesi ve bunların, programı kullanan organizasyona, özellikle kullanıcıya hedeflenen reklamların gönderilmesi amacıyla, iletilmesi olarak iki yaygın kullanım şekli vardır. Veri madenciliği günümüzde, müşteri profili çıkartılması, kredi risk analizleri gibi faaliyetlerde etkin olarak kullanılmaktadır. Bkz. “Data Mining”, <http://www.twocrows.com/glossary.htm#anchor314309> (kontrol tarihi 28.03.2005); http://www.webopedia.com/TERM/D/data_mining.html (kontrol tarihi 28.03.2005); Nordine MELAB, *Data Mining: A Key Contribution to E-business*, Information & Communications Technology Law, Vol. 10, No. 3, 2001, s. 310 vd; Vagelis PAPAKONSTANTINO, *A Data Protection Approach to Data Matching Operations Among Public Bodies*, International Journal of Law and Information Technology, Vol. 9, No. 1, s. 42 vd.

³⁷⁴ Buna ilişkin olarak Miller, daha önceki dönemlerde özel hayatın gizliliğinin korunmasının şu nedenlere daha kolay olduğunu ifade etmektedir; 1. kişi hakkında çok büyük miktarda enformasyonun geleneksel olarak toplanmaması ve dolayısıyla üçüncü kişiler tarafından elde edilebilir olmaması. 2. Varolan enformasyonun genel olarak merkezi olmayan bir şekilde tutulması ve genellikle dağınık olması; nispeten yüzeysel bir karakterde olması ve sıklıkla kullanılabilir olarak görülmemesi; hâlihazırdaki enformasyona erişimin çok kolay sağlanamaması. 3. Kişilerin çok devingen toplum içerisinde olması nedeniyle takip edilememesi. 4. Birçok kişinin hâlihazırdaki verilerin ortaya çıkardığı enformasyonu yorumlayamaması ve sonuç çıkaramaması.. MILLER, s. 26

Schwartz da kişisel verilerin korunması açısından İnternet boyutuna değinmekte ve İnternetin kişisel verilerin işleme sürecini kişilere ilişkin bilgilerin niteliği, miktarı ve

Miller, bilişim sistemleri merkezli veri gözetiminin artmasının özel hayatın gizliliğinin korunmasını iki açıdan zayıflatıldığını belirtmektedir. Bunlardan birincisi, kişisel verilerin bilişim sistemleri aracılığıyla işlenmesi sonucu, kişinin kendisiyle ilgili verinin kişinin rıza gösterdiğinden çok daha fazla kişiye yayılması nedeniyle kişinin kendisiyle ilgili verilere kimlerin erişebileceğini kontrol imkânının ortadan kalkmasıdır. Diğer ise, işleme süreci içerisinde (toplama, kullanım, iletim) ortaya çıkan hatalar sonucu -verinin içeriğinin doğruluğunun ortadan kalkması gibi durumlarda- kişinin kendisine ait kişisel verinin doğrulunu kontrol edememesidir³⁷⁵.

erişilebilirliğini etkileyerek, kişiye ait özel alanın sınırlarını daraltarak ki bunu anonimlik olarak adlandırmakta ve kimlerin kişisel verileri işlediğine, işleme koşullarına ilişkin bilinebilirliği ve kesinliği ortadan kaldırarak bu süreci önemli bir etkilediğini ifade etmektedir. Ayrıntılı bilgi için bkz, Paul M. **SCHWARTZ**, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev., 1999.1643 vd

³⁷⁵ Ayrıntılı bilgi için bkz., **MILLER**,. 26 vd.;

“Records, Computers and the Rights of Citizens (1973)” raporunda ise bilgisayar sistemlerinin kullanılmasını kayıt tutulmasının kişisel veri işleminde ortaya çıkardığı potansiyel tehlikenin genel olarak, 1) veri işleme kapasitesini önemli ölçüde genişletme, 2) tek bir organizasyon ya da farklı organizasyonlar arasında sınırlar aşarak kişisel verilere erişimi kolaylaştırma, 3) veri sağlayan kişiler ve nihai uzak kullanıcılarla irtibatı olan ve teknik bir işleve sahip yeni bir uzman grubun ortaya çıkması nedenlerinden etkilendiği belirtilmektedir. Bkz. Records, Computers and the Rights of Citizens (1973) II. Latent Effects of Computer Based Record Keeping, <http://aspe.os.dhhs.gov/datacncl/1973privacy/c2.htm> (kontrol tarihi 06.02.2005)

Tosun da, kişilerin özel hayatına ilişkin bilgilerin bilgisayarlarda depo edilmesi ve istenildiği zaman çok kısa bir sürede bir kişiyi ilgilendiren bütün bilgilerin bu makinelerden alınması olanağının doğduğunu ve bu makinelerin kullanılması sayesinde çok kısa zamanda, çeşitli görsel ve işitsel araçlarla elde edilmiş belgelerin hemen ortaya çıkarılması ve özel hayatın gizliliğinin ihlal edilmesi olanağının olduğunu belirtmiştir. Öztekin **TOSUN**, *Özel Hayatın Gizliliği*, Değişen Toplum ve Ceza Hukuku Karşısında TCK’nın 50. Yılı ve Geleceği Sempozyumu, İstanbul 1977, s. 379-380.

Danışman ise, özel hayatın gizliliğinin korunmasının iki görünümü – araştırma ve açığa vurma- bakımından, bilgisayarların bilgileri stoklama kapasitesi nedeniyle yalnızca tek bir kişi değil birçok kişi hakkında çok ve çeşitli veriler stok edebilmesi sayesinde araştırma açısından tehlike yarattığını; bilgisayarlarda toplanan bilgilerin amaç dışı kullanımlarının ise açığa vurma açısından tehlike yarattığını ifade etmiştir. Ahmet **DANIŞMAN**, Ceza Hukuku Açısından Özel Hayatın Korunması, Konya 1991, s. 40 – 41.

Bu gelişme, özel hayatın gizliliğinin tanımı ve kapsamı konusunda yeni tartışmaları beraberinde getirmiştir³⁷⁶. Nitekim bu döneme kadar, özel hayatın gizliliği, genel olarak bireyin toplum içerisinde konumu açısından “müdahale edilmezlik ve “sınırlı erişim³⁷⁷” olarak ele alınarak, “yalnız kalma hakkı”, ya da “kamuyu ilgilendirmeyen konularda kişinin, kamuya haksız ya da istenmeyen ifşalardan uzak tutulması” şeklinde tanımlanmıştır³⁷⁸. Bu dönem içerisinde özel hayatın gizliliğine ilişkin olarak, kişisel verileri de kapsayacak ve kişiye veri işleme sürecinde tasarruf edebilme imkânı sağlayacak şekilde bir yetki, iktidar ya da istem olarak kontrol merkezli³⁷⁹ tanımlar yapılmıştır. Bu şekliyle özel hayatın gizliliği, “Birey, grup ve kurumların kendileri hakkındaki enformasyonun diğerleri tarafından ne zaman nasıl ve hangi boyutlarda iletilebileceğinin kendileri tarafından belirlenebilmesi” ya da kısaca, “bir kişinin kendi hakkındaki enformasyonu kontrol hakkı.” olarak tanımlanmaktadır³⁸⁰. Anayasa Mahkemesinin 1987 tarihli bir

³⁷⁶ REGAN, s.26.

³⁷⁷ ARASLI, s.7; Lee A. BYGRAVE, *The Place of Privacy In Data Protection Law*, *University of New South Wales Law Journal*, 2001, vol. 24, no. 1, <http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html> (kontrol tarihi 6.02.2005), parag. 7-12.

³⁷⁸ Samuel D. WARREN -Louis D BRANDEIS, *The Right to Privacy*, *Harvard Law Review*, Vol 4 1890, s. 193- 195, 213-215.; Samuel H. HOFSTADTER– George HOROWITZ, *The Right of Privacy*, New York 1964, s. 1. Ergun ÖZSUNAY, *Gerçek Kişilerin Hukuki Durumu*, 4. B., İstanbul 1979, s. 128

³⁷⁹ BYGRAVE, *The Place of Privacy*, parag. 7.

³⁸⁰ WESTIN, s. 1. Aynı yönde, MILLER, , s.40; Rochelle C. DREYFUSS – David W. LEEBRON, W., *Foreword: Privacy and Information Technology*, *Ann. Surv. Am.L.* 1986, s. 495; MICHAEL, s.3.

Parker, kişi hakkındaki enformasyonun kontrolü hususunun özel hayatın gizliliğini tam olarak karşılamadığını belirtmekte ve bunun yerine özel hayatın gizliliğini, yine kontrol merkezli biçimde, “bize ait çeşitli bölümlere ilişkin olarak kimlerin ve ne zaman bu bölümleri algılayacağını kontrol etme” şeklinde tanımlamaktadır. Richard B. PARKER, *A Definition of Privacy*, 27 *Rutgers L. Rev.* 1973-1974, s. 279 vd.

Aynı yönde Araslı da özel hayatın gizliliğini, “özel yaşamını düzenlemek, ve bu yaşamı kimlerin, ne zaman, nasıl ve ne ölçüde algılayabileceğine ve bu yaşama müdahale

kararında da, “Özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Orada cereyan edenlerin yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini istemek hakkı, kişinin temel haklarından biridir.” diyerek özel hayatın gizliliğini bu yönde tanımlamıştır³⁸¹.

Özel hayatın gizliliğinin müdahale edilmezlik ve sınırlı erişim doğrultusundaki tanımlarında özel hayatın gizliliğine ilişkin klasik ihlaller esas alınmıştır. Özel hayatın gizliliğini kişiye tanınmış bir iktidar, istem ya da yetki olarak esas alan kontrol merkezli tanımlar³⁸² ise bilişim sistemlerinin yaygınlaştığı ve kişisel verilerin işlenmesinde etkin olarak kullanılmaya başlandığı döneme rastlamaktadır. Bu açıdan, daha önceki tanımlar sadece müdahale edilmemeyi talep etme gibi daha çok pasif bir yaklaşım öngörürken, kontrol merkezli tanımlar kişinin aktif katılımını sağlamaya yönelmiştir. Kontrol merkezli bu tanımlar içerisinde asıl belirleyici rol kişiye verilmekte ve özel hayata ilişkin kişinin tasarruf edebilme imkânı ön plana çıkmaktadır. Avrupa Konseyinin Parlamenterler Meclisi’nin 1998 tarihli kararında da, 1970 tarihli 428 no.lu kararında³⁸³ “ *kişinin kendi hayatını en az müdahaleyle yaşaması hakkı*” olarak tanımlanan özel hayatın gizliliği tanımına, yeni iletişim teknolojilerinin kişisel verilerin saklanması ve kullanılmasını olanaklı

edebileceğine karar vermek ve başkalarının da bu karara saygı göstermesini istemek konusunda kişiye, hukuk kurallarınca tanınmış bir yetki” şeklinde kontrol merkezli olarak tanımlamaktadır. ARASLI, s. 44.

³⁸¹ 31.3.1987 T, 1986/24 E., 1987/8 K. No.lu Anayasa Mahkemesi Kararı, <http://www.anayasa.gov.tr/eskisite/KARARLAR/IPTALITIRAZ/K1987/K1987-08.htm>

³⁸² ARASLI, s.8, BYGRAVE, *The Place of Privacy*, parag. 7

³⁸³ Resolution 428 (1970); *containing a declaration on mass communication media and human rights*

<http://assembly.coe.int//Main.asp?link=http://assembly.coe.int/Documents/AdoptedText/TA70/ERES428.htm>

kılması sonucu “kişinin kendisi hakkındaki verileri kontrol hakkı”nın eklenmesi gerektiği belirtilmiştir³⁸⁴.

Özel hayatın gizliliğini kontrol merkezli olarak ele alan tanımlar, Alman Anayasa Mahkemesi’nin 1983 tarihli kararında açıkça vurgulanan, kişinin kendisi hakkındaki enformasyon üzerindeki tayin etme hakkı ile paralellik arz etmektedir.³⁸⁵. Kişinin kendisi hakkındaki bilgi/enformasyon üzerindeki tayin hakkı (self-determinasyon) Alman Anayasa Mahkemesinin, kişisel verilerin işlenmesine ilişkin hükümleri içeren nüfus sayımı kanunu Anayasaya aykırı bulduğu 1983 tarihli kararında şu şekilde ifade edilmiştir:

“Eğer bir kimse kendisi hakkında belirli alanlarda hangi enformasyonun toplumsal çevresinde bilindiğini yeterli kesinlikte öngöremiyorsa ve iletme ihtimali olan tarafları yeterince tahmin edemiyorsa, herhangi bir baskı ya da etki altında kalmadan hür bir şekilde planlama ya da karar verme hürriyetinden alıkonulmuş demektir. Enformasyona ilişkin self-determinasyon hakkı, vatandaşların bundan sonra kendileri hakkında kimlerin ne zaman ve hangi nedenle ne bildiklerini bilemeyecekleri bir duruma olanak veren toplumsal ve yasal düzeni engeller. Eğer bir kişinin, ayrıkçı davranışlarının sistemli bir şekilde enformasyon olarak saklanıyor, bu husus uygulanıyor ya da

³⁸⁴ Resolution no: 1165 (1998); Right to Privacy, <http://assembly.coe.int/Main.asp?link=http%3A%2F%2Fassembly.coe.int%2FDocuments%2FAdoptedText%2Fta98%2FERES1165.htm>

³⁸⁵ **BYGRAVE**, parag. 7. Enformasyon üzerindeki tayin hakkının kişisel veriler üzerinde kontrol hakkı olarak ele alınmadığı ve bireyin kendisiyle ilgili verileri üzerinde mutlak bir hak tanımadığı; bunun yerine kişisel özerkliğin sağlanması amacıyla veri işlemeye ilişkin düzenlemeler yapmaya zorunlu kıldığı hakkında bkz., Paul **SCHWARTZ**, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 Am J. Comp L. 1989, s. 690.

intikal ettiriliyor yönünde şüphesi varsa, o kişi bu tür bir davranışla ilgiyi üzerine çekmemeye gayret edecektir. Sivil girişime ya da toplantıya katılımın kaydedildiği ve bu yüzden kişisel bir risk oluşabileceği gözüyle bakıyorsa, muhtemel olarak bu haklarının kullanımından vazgeçecektir. Bu durum sadece kendi gelişmesine zarar vermeyecek aynı zamanda toplumun menfaatlerine de zarar verecektir. Çünkü self-determinasyon vatandaşlarının hareket ve katılımına dayalı olan özgür demokratik toplumun temel işlevsel koşuludur³⁸⁶.”

Özel hayatın gizliliğini, kişisel verileri ve bu doğrultuda kişisel verilerin korunmasını kapsayacak şekilde yapılan bu tanımlarla paralel olarak, kişisel verilerin özel hayat kapsamında olduğu ve işleme sürecinin özel hayatın gizliliğini koruyacak şekilde düzenlenmesi gerektiği dile getirilmiştir. Nitekim BM Kişisel ve Siyasal Haklar Uluslararası Sözleşmesinin özel hayatı düzenleyen ilgili 17. maddesi ile ilgili olarak, Birleşmiş Milletler İnsan Hakları Komitesi söz konusu maddenin

³⁸⁶

65 BverfGE 15 Kasım 1983 tarihli karar, aktaran **MICHAEL**, s. 4.

Alman Anayasa Mahkemesi bu kararında özel hayatın gizliliğinden çok Alman Anayasasının 1. ve 2. maddelerinde yer alan insan onuru ve kişinin maddi ve manevi varlığını geliştirme hakkına dayanmıştır. Bkz., **LLOYD**, s.145. Karar hakkında inceleme için ayrıca bkz., Paul **SCHWARTZ**, s. 686 vd.

Avrupa İnsan Hakları Mahkemesi eski başkanı *Rolv Ryssdal*, AİHS'in özel hayatın gizliliğini düzenleyen 8. maddesinin yorumunun, kişinin kendisi hakkındaki enformasyon üzerindeki kendisinin tayin etme hakkına yönelmiş bir şekilde geliştiğini ifade etmiştir. Aktaran, Samuli **SIMOJOKI**, Location-based Services and General Privacy and Data Protection Principles: Report of the NAVI Regulatory Framework-project, http://www.vtt.fi/virtual/navi/cd/Privacy_Principles.pdf, s.13. (kontrol tarihi 12.03.05)

AİHM ise, *Van Kuck v. Germany* kararında özel hayatın gizliliği kapsamında 8. maddenin kişiye self –determinasyon hakkını içerdiği yönünde Mahkemenin bir karar vermediğini fakat kişisel özerkliğin 8. maddenin yorumunda temel bir ilke olduğunu belirtmiştir. Karar için bkz., <http://cmiskp.echr.coe.int/tkp197/portallhbk.asp?sessionId=8731656&skin=hudoc-en&action=request&poll=3>. Ayrıca bkz., *Pretty v. the United Kingdom*, <http://cmiskp.echr.coe.int/tkp197/portallhbk.asp?sessionId=8731662&skin=hudoc-en&action=request&poll=3>

hem kamu hem de özel sektör içerisinde kişisel verilerin korunmasına ilişkin düzenlemelerin yapılmasını zorunlu kıldığını belirtmektedir. Komite, Sözleşmenin 17. maddesinin, kamu ve özel sektörler bakımından kişisel verilerin korunmasının garanti altına alınmasına ilişkin yasal düzenlemeler yapılmasını zorunlu kıldığını ifade etmiş ve devamında şu görüşü dile getirmiştir.

“Bilgisayarlar, veri bankaları ve diğer araçlar ile kişisel verilerin toplanması ve elde tutulması, ister kamu otoriteleri ister özel kişi ya da gruplar tarafından olsun kanunla düzenlenmelidir. Devletler tarafından kişilerin özel hayatına ilişkin enformasyonun, bunları almak işlemek ve kullanmak için yetkilendirilmeyen kişilerin ellerine geçmesini ve Sözleşmeyle uyumayan amaçlar için hiçbir zaman kullanılmamasını sağlayacak etkili önlemlerin kanunla alınması gerekir. Özel hayatın en etkili biçimde korunmasına sahip olması için bireylerin, kişisel verilerin otomatik veri dosyalarında ve hangi amaçlarla saklanıp saklanmadığını ve eğer saklanıyorsa hangi kişisel verilerin otomatik veri dosyalarında saklandığını ve ne amaçla saklandığını anlaşılır bir şekilde tespit etme hakkına sahip olması gerekir. Her bireyin ayrıca hangi kamu otoriteleri ya da özel bireylerin veya grupların kendi dosyalarını kontrol ya da kontrol edebiliyor olduğunu tespit edebilme olanağına sahip olması gerekir. Eğer böyle dosyalar doğru olmayan kişisel veri içeriyor ya da kanunun

*hükümlerine aykırı olarak toplanmış ya da işlenmiş ise, her birey düzeltmeyi veya yok etmeyi talep etme hakkına sahip olmalıdır*³⁸⁷.”

Avrupa İnsan Hakları Mahkemesi de AİHS'in 8. maddesinde düzenlenen özel hayatın gizliliğine ilişkin genel bir tanım vermemesine rağmen, özel hayatı geniş yorumlamakta ve kişisel verilerin korunmasını da özel hayat kapsamında değerlendirmektedir³⁸⁸. Nitekim Mahkeme, *Leander v. İsveç* kararında, başvuru hakkında güvenlik soruşturması yapılması suretiyle enformasyon toplanmasının ve bunların doğruluğuna ilişkin olarak başvurucuya itiraz hakkı verilmemesinin özel hayatın gizliliğine müdahale oluşturduğuna karar vermiştir³⁸⁹.

M.G v. İngiltere kararında Mahkeme, davacının sosyal hizmetlerde tutulan ve davacı hakkında bilgi içeren kayıtlara erişiminin engellenmesini, Kişisel Veri Koruma Kanununun yürürlüğe girdiği 1998 yılına kadar, erişim yönünde yapılan başvuruların engellenmesi açısından, AİHS'in 8. maddesine aykırı bulmuştur. Mahkeme, gerekçesinde davacının sosyal hizmetlerde kayıtlı olan kendisi hakkındaki

³⁸⁷ Bkz., General Comment 1, 23.3.1998 **U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994)** <http://www1.umn.edu/humanrts/gencomm/hrcom16.htm>, ayrıca bkz., 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.252

³⁸⁸ Durmuş **TEZCAN** - M. Ruhan **ERDEM** - Oğuz **SANCAKDAR**, Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'nin İnsan Hakları Sorunu, Seçkin Yayıncılık 2. B., Ankara 2004, s. 385.

³⁸⁹ **Leander v. Sweden**, <http://cmiskp.echr.coe.int/tkp197/viewhbkm.asp?sessionId=8200265&skin=hudoc-en&action=html&table=1132746FF1FE2A468ACBCD1763D4D8149&key=104&highlight=Leander>

Leander kararında Mahkeme, başvuru hakkında güvenlik soruşturması yapılması ve elde edilen bilgilerin doğruluğuna karşı başvurucuya itiraz hakkı verilmemesinin özel yaşama saygı hakkına müdahale oluşturduğuna karar vermiştir. Kararın devamında ise Mahkeme, iç hukukta yasaya 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. Ayrıca Bkz, **TEZCAN**, **Avrupa İnsan Hakları Sözleşmesi**, s. 387.

bilgilere erişiminin sağlanması yönünde devletin pozitif bir yükümlülüğünün bulunduğunu ve bu yükümlülüğün yerine getirilmediğini belirtmiştir³⁹⁰

Amann v. İsviçre kararında ise, bireyin özel hayatı ile ilgili olarak enformasyon toplanmasının AİHS'in 8. maddesi kapsamında olduğunu; özel hayat teriminin dar yorumlanmaması gerektiği ve özel hayatın diğer insanlarla ilişki kurma ve geliştirme hakkını da kapsadığını; iş ve mesleki faaliyetleri bunun dışında tutmayı haklı kılan bir nedenin olmadığını; özel hayatın geniş yorumunun ise Avrupa Konseyinin kişisel verilerin korunmasına ilişkin Sözleşmesinde yer alan kişinin bilinmesini ya bilinebilmesini sağlayan her türlü enformasyona karşılık geldiğini belirtmiştir³⁹¹.

Rotaru v. Romania kararında, Romanya vatandaşı Rotaru, üniversitede öğrenci olduğu dönemde, “*Romanya Lejyoner Hareketi*”ne üye olduğu yönündeki gizli servis tarafından kendisi hakkında tutulan kaydın yanlış olduğu ve silinmesi gerektiği yönündeki, Romanya yetkili organlarına başvurusunun reddedilmesi ile ilgili olarak bu durumun AİHM'e AİHS'in 8. ve diğer maddelerine aykırılık oluşturduğu iddiasıyla başvurmuştur. Taraf devlet, başvuru hakkında toplanan enformasyonun özel hayatı ile ilgili olmadığı fakat kamusal hayatı ile ilgili olduğu

³⁹⁰

M. G. v. United Kingdom,
<http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=M.G.&sessionId=8200151&skin=hudoc-en>

³⁹¹

Amann v. Switzerland,
<http://cmiskp.echr.coe.int/tkp197/viewhbkm.asp?sessionId=8200275&skin=hudoc-en&action=html&table=1132746FF1FE2A468ACBCD1763D4D8149&key=1078&highlight=Amann>

AİHM eski başkanı Rolv Ryssdall da Sözleşmede yer alan ilkeleri Strazburg organlarının görmezden gelemeyeceğini, bu sözleşmede yer alan temel ilkelerin AİHS'in 8. maddesinin otomatik işleme bağlamında sektörel uygulamasını oluşturduğunu ve bu nedenle 8. maddenin yorumunda yardımcı olacağını ifade etmiştir. Aktaran **BYGRAVE, Data Protection**, s. 256.

ve bu nedenle AİHS'in 8. maddesinin uygulanamayacağı itirazında bulunmuştur. Buna karşın Mahkeme, *Amann* kararındaki görüşünü tekrar etmiş ve bunun da ötesine geçerek, kişinin kamusal hayatına ilişkin enformasyonun sistematik olarak toplandığı ve saklandığı durumlarda özel hayat kapsamında olduğunu, bunun kişinin çok uzak geçmişi hakkında olması durumunda da geçerli olduğunu ifade etmiştir. Devamında, *Leander* kararıyla aynı yönde, kişi hakkında enformasyon toplanmasının ve bunların doğruluğuna karşı başvurucuya itiraz hakkı verilmemesinin özel hayatın gizliliğine müdahale oluşturduğuna karar vermiştir³⁹².

Yukarıda aktarılanlar doğrultusunda kısaca belirtmek gerekirse, AİHM tarafından da özel hayat kapsamında değerlendirilmeye başlanan kişisel verilerin korunması, enformasyon mahremiyetinin korunması amacına hizmet etmekte ve özel hayatın gizliliğinin korunmasının bir yönünü oluşturmaktadır. Bu hususa ilişkin son olarak söylenecek diğer bir husus da kişisel verilerin korunmasının ayrı temel bir hak olarak ele alınmaya başlandığıdır. Nitekim “*Avrupa İçin Bir Anayasa Oluşturan Antlaşma*”da kişisel verilerin korunması özel hayatın gizliliğinin düzenlendiği II. 67. maddesinden sonra gelmek üzere ayrı bir maddede düzenlenmiştir³⁹³. İtalyan Veri Koruma Kanununda da kişisel verilerin korunması “*kişisel verilerin korunması hakkı*” olarak düzenlenmiştir (Bkz 1/1.m., 2/1. m.).

³⁹²

Rotaru v. Romania,

<http://cmiskp.echr.coe.int/tkp197/viewhbk.asp?sessionId=8200279&skin=hudoc-en&action=html&table=1132746FF1FE2A468ACBCD1763D4D8149&key=1167&highlight=rotaru>

³⁹³ “Kişisel Verilerin Korunması” Madde II- 68: 1. Herkes, kendisiyle ilgili kişisel verilerin korunması hakkına sahiptir... 2. Bu tür veriler, belirli amaçlar için ve ilgili kişinin rızasının alınması esasına veya yasa tarafından belirlenen başka bir meşru esasa göre, adil bir şekilde işlemiden geçirilmelidir. Herkes, kendisi hakkında toplanmış bilgilere erişme ve bu bilgilerin düzeltilmesini sağlama hakkına sahiptir.” Bkz., *Avrupa İçin Bir Anayasa Oluşturan Antlaşma*, Ankara Barosu, 2005., s. 71

III. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN SUÇLAR

A. Genel Olarak

Bilindiği üzere 765 Sayılı TCK’de özel hayatın gizliliği kapsamında değerlendirilen konut dokunulmazlığı ile haberleşmenin gizliliğine ilişkin suçlar yer almaktaydı³⁹⁴. 765 Sayılı TCK’nin 193. vd. maddelerinde yer alan “*mesken masuniyeti aleyhine cürümler*”, 195. vd. maddelerinde yer alan genel olarak haberleşmenin gizliliğini korumaya yönelik olarak karşımıza çıkan “*Sırrın Masuniyeti Aleyhine Cürümler*” 765 Sayılı TCK’de özel hayatın gizliliğinin korunmasına ilişkin suçlar olarak düzenlenmekteydi.

TCK’de ise hem özel hayatın gizliliği genel olarak, hem de özel hayatın gizliliğinin çeşitli yönleri ayrıca özel olarak düzenlenmiştir. 5237 Sayılı Türk Ceza Kanununda Özel hayatın gizliliğine ilişkin suçlar genel olarak “*Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*” başlıklı 9. 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. Gerek doktrinde özel hayatın gizliliği kapsamında değerlendirilen ve gerekse Anayasanın 20. vd maddelerinde özel hayatın gizliliği kapsamında düzenlenen konut dokunulmazlığını

³⁹⁴ DANIŞMAN, s. 106.

ihlal suçu ise TCK'de “*Hürriyete Karşı Suçlar*” başlığını taşıyan yedinci bölümde, 116. maddede düzenlenmiştir.

765 Sayılı TCK'den farklı olarak TCK'de, ayrıca kişisel verilerin korunmasına ilişkin kimi suçlara yer verilmiştir. Nitekim Kanunun 135. maddesinde “*kişisel verilerin kaydedilmesi*” 136. maddesinde “*verileri hukuka aykırı olarak verme veya ele geçirme*”, 138. maddesinde ise “*verileri yok etmeme*” suçları düzenlenmiştir. 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 öngörülmüştür³⁹⁵.

TCK'nin 135. vd. maddelerinde düzenlenen suçların manevi unsur bakımından ortak özelliği, İtalya ve Almanya'da kişisel verilerin korunmasına ilişkin suçlardan farklı olarak, genel kast ile işlenebilen suçlar olarak düzenlenmiştir. Bu haliyle kişisel verilerin korunmasına ilişkin TCK'de yer alan suçların manevi unsur bakımından da Fransız Ceza Kanununda yer alan kişisel verilerin korunmasına ilişkin suçlar ile aynı yönde düzenlendiği görülmektedir.

Söz konusu suçlar incelendiğinde 135 ve 136. maddelerde düzenlenen suçların faili bakımından herhangi bir nitelik aranmadığı görülmektedir. 138.

³⁹⁵ “Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı”nın 29. maddesinde de ağırlatıcı sebebe yer verilmiş olup madde şu şekilde düzenlenmiştir: “**MADDE 29- (1)** *Kişisel verilerin kaydedilmesi ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarının bilişim ağı üzerinden işlenmesi hâlinde, Türk Ceza Kanunu hükümlerine göre verilecek ceza yarı oranda artırılır.*”

Bkz., <http://www.kgm.adalet.gov.tr/gorus/bilisim.htm> (10.08.2006)

maddede düzenlenen verilerin yok edilmemesi suçu bakımından ise sadece verileri yok etme yükümlülüğü olan kişiler suçun faili olabilirler. Bu açıdan 138. madde düzenlenen verileri yok etmeme suçu mahsus suç olarak düzenlenmiştir. Başka bir yönden farklılık ise 135 ve 136. maddede yer alan suçların maddi unsurlarını oluşturan hareketlerin icrai bir nitelik taşıması 138. maddede ise ihmali bir hareketin esas alınmasıdır.

135. vd. maddelerinde düzenlenen suçlar bakımından Türk Ceza Kanunu Tasarısında sadece otomatik işlemenin³⁹⁶ düzenlendiği ve bu hususun maddelerde

³⁹⁶ Kişisel verilerin korunmasının genel olarak bilişim sistemlerinin kullanımının bir etkisi olarak özel hayatın gizliliğinin ihlali olarak ortaya çıkması, kişisel verilerin korunmasına ilişkin düzenlemelerin otomatik işlem olarak da adlandırılabilen olan özellikle bilişim sistemleri aracılığıyla işlenmesine odaklanmasına neden olmuştur. Nitekim Kişisel verilerin korunmasına ilişkin Sözleşmede de bunun görmek mümkündür. Sözleşmenin kapsamının asıl olarak otomatik kişisel veri dosyaları ve bunların otomatik olarak işlenmesi olduğu Sözleşmenin 3. maddesinde belirtilmiştir. Aynı maddenin “e” bendinde ise taraf devletlerin kişisel verilerin otomatik olmayan yöntemlerle işlenmesini de düzenleyebilecekleri ifade edilmiştir. Yönergede de asıl olarak kişilerin otomatik olarak işlenmesi esas alınmıştır. Kişisel verinin otomatik olmayan yöntemlerle işlenmesi ise kural olarak Yönerge kapsamında olmamakla birlikte, kişisel verilerin, bu tür verilere erişimin kolaylaştırılmasını sağlayacak şekilde, herhangi bir sisteme göre düzenlenmesi halinde Yönerge kapsamında olduğu ifade edilmiştir. Yönerge hakkında bkz., Nilgün BAŞALP, Kişisel Verilerin Korunması ve Saklanması, Ankara 2004, s. 32 – 33.

Verinin otomatik olmayan yöntemlerle sistematik olarak işlenmesi anlamına gelen Tasarının 199. maddesinde düzenlenen fişliklerin, kişisel verilerin işlenmesine ilişkin suçlar kapsamında olacağına ilişkin hüküm, Tasarıda otomatik olmayan yöntemlerle kişisel verilerin işlenmesinin de söz konusu suçlar kapsamında olacağını ifade etmesi bakımından bir anlama sahipti.

“*Kişisel Verilerin Korunması Hakkında Kanun Tasarısı*”nın 3. maddesinin c bendinde kişisel verilerin işlenmesi, “*Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlandırılması amacıyla işaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem ya da işlemler bütünü*,” olarak tanımlanmış ve her türlü işleme şekli Kanunun uygulanma alanına sokulmuştur. Buna karşın Tasarının kapsam başlıklı 2. maddesinde ise Kanunun, sadece kişisel verilerin belirli bir veri kütüğüne bağlı olarak işlenmesi durumunda uygulanacağı öngörülmüştür. Tasarının 3/(e) maddesinde ise “*veri kütüğü sistemi*”, “*gerçek ve tüzel kişilere ilişkin belirli kriterlere göre kişisel verilere ulaşmasını kolaylaştıracak şekilde yapılandırılmış herhangi bir kişisel veri grubu*” olarak tanımlanmaktadır.

bilişim sistemine yerleştirme, işleme şekillerinde ifade edildiği görülmektedir. TCK’de ise, 135. maddede düzenlenen kişisel verinin kaydedilmesi suçu bakımından bu şart aranmamıştır. 138. maddede düzenlenen verinin yok edilmesi 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.

Türk Ceza Kanunun 135 vd. maddelerindeki suçlar incelendiğinde, genel olarak kişisel verilerin işlenmesine ilişkin ilkeler olarak ifade edilen, hem ulusal hem de uluslar arası düzenlemelerde çeşitli şekillerde yer verilen kişisel verilerin işlenmesine ilişkin usul ve esasları esas alındığı görülmektedir. Aşağıda inceleneceği üzere, “*veri işleyenin sorumluluk ve yükümlülükleri*” başlığı altında değerlendirilen kişisel verilerin korunmasına ilişkin ilkelerin çeşitli görünümlerinin 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. Söz konusu suçların anlaşılabilirliği bakımından kişisel verilerin işlenmesine ilişkin ilkeler olarak da adlandırılan kişisel verilerin işlenmesine ilişkin usul ve esasların bilinmesi gereklidir.

Bu hususlar doğrultusunda öncelikli olarak TCK'nin 135 vd. maddelerinde düzenlenen suçların hukuki konusu olarak ortaya çıkan özel hayatın gizliliğine, özellikle kişisel verilerin korunması bakımından özel hayatın gizliliğine ilişkin olarak Anayasada yer alan sınırlandırma nedenleri ve temel hak ve hürriyetlerin sınırlandırılmasına ilişkin rejim açısından, kısaca değinilecektir.

Kişisel verilerin işlenmesine ilişkin suçların, kişisel verilerin işlenmesine ilişkin usul ve esaslara bağlantılı olarak düzenlenmesi nedeniyle de bu konuya yer verilecek ve söz konusu suçların ağırlıklı olarak ilişkili olduğu, dürüst ve hukuka uygun toplama ve işleme ilkesiyle amaçla bağlılık ilkesine ayrıca değinilecektir.

Bunun yanında, TCK'de düzenlenen suçlar bakımından kişisel verinin anlam ve kapsamına değinilecek ve son olarak TCK'de yer alan kişisel verilerin korunmasına ilişkin suçlar özellikle suçun şekilleniş biçimi itibariyle, ağırlıklı olarak suçun maddi unsuru açısından incelenecektir.

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

TCK'nin 135. vd. maddelerinde düzenlenen kişisel verilerin korunmasına ilişkin suçlar, 765 Sayılı TCK'de yer almayan ve TCK'nin getirdiği yeniliklerden biridir. Yukarıda da belirtildiği üzere 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^{397 398}.

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 sınırlandırılması anlamına gelmekte ve bu açıdan söz konusu usul ve esaslar özel hayatın gizliliğinin meşru olarak sınırlandırılması anlamına gelmektedir.

Kişisel verilerin korunmasının 1970’li yıllardan itibaren özel hayatın gizliliği kapsamında özel hayatın gizliliğinin bir yönü olarak tartışıldığı ve genel olarak özel hayatın gizliliği kapsamında veri/enformasyon mahremiyetine karşılık geldiği gerçeği karşısında, bu yönde bir ihlal özel hayatın gizliliğinin ihlali anlamını taşır. Kişisel verilerin korunmasına ilişkin kanunlar ise, kişisel verilerin işleme usul ve esaslarını, işlenmesine ilişkin yasakları ve sınırlamaları düzenlemesi açısından, özellikle kişisel verilerin işlenmesine izin veya yetki veren normlar olarak özel hayatın gizliliğinin

³⁹⁷ Aynı yönde bkz., **TOSUN**, , s. 379 - 380

³⁹⁸ 1997 tarihli Türk Ceza Kanunu Öntasarının ve sonrasında TBMM’ye sunulan Türk Ceza Kanunu Tasarının gerekçesinde, kişilik hakkının korunmasına ilişkin kuralların yetersiz kalması dolayısıyla Avrupa Konseyinin 1970’li yıllarda elektronik bilgi bankalarında işlenen veriler ile ilgili olarak 1973 ve 1974 yıllarında iki tavsiye kararını kabul ettiği devamında Avrupa Konseyinin, Türkiye’nin de imzaladığı, “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması*”na ilişkin 108 sayılı Sözleşmeyi imzaya açtığı hususuna işaret edilmiştir. Devamında Sözleşme ile getirilen yükümlülüklerin yerine getirilmesi amacıyla taraf devletlerin yasa hazırladıklarını ve meydana gelebilecek çeşitli hukuka aykırılıkları suç haline getirdikleri ve bu bağlamda Yeni Fransız Ceza Kanununda yapılan düzenlemeye paralel bir şekilde kişisel verilerin yerleştirilmesi ve işlenmesi suçuna yer verildiği ifade edilmiştir. 1997 tarihli Türk Ceza Kanunu Öntasarının ve gerekçesinin tam metni için bkz., Türk Ceza Kanunu Öntasarısı (1997) T.C: Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, Özel Seri:3. TBMM’ne sunulan Tasarının gerekçesi için bkz. **GÜNEY**, s. 197 vd.

sınırlandırılması sonucunu doğurur. Bu nedenle, kişisel verilerin işlenmesine ilişkin genel ya da özel kanunların özel hayatın gizliliğinin sınırlandırılmasına ilişkin Anayasada öngörülen normlara uygun olması gerekmektedir. Türk hukuka bakımından söz konusu durum, Anayasanın temel hak ve hürriyetlerin sınırlandırılmasına ilişkin rejiminin gündeme gelmesine yol açmaktadır. 1982 Anayasasının temel hak ve hürriyetlere ilişkin sınırlandırma rejiminin 2001 yılında yapılan değişiklikle yeniden düzenlenmesi, kişisel verilerin işlenmesine ilişkin düzenlemelerin Anayasaya uygunluğu açısından değerlendirilmesinin önemini arttırmaktadır.

Anayasa Mahkemesinin 1996/68 E. 1991/1 K., 6. 1.1999 T. no.lu kararında³⁹⁹ kişisel verilerin Anayasa'nın 20. maddesinde düzenlenen özel hayatın gizliliği ile doğrudan ilişkili olduğu teyit edilmiştir. Bu karar doğrultusunda kişisel verilerin işlenmesine ilişkin düzenlemelerin, Anayasada yer alan özel hayatın gizliliğinin sınırlandırılmasına ilişkin usul ve esaslara uyması gerekmektedir. Halihazırda mevzuat içerisinde kişisel verilerin işlenmesine ilişkin olarak ilgili mevzuatın konusu ve amacı kapsamında kişisel verilerin toplanması ve işlenmesini öngören bir çok normun bulunması karşısında, bunların tek tek incelenmesi yerine söz konusu karar ve bu karardan çıkan sonuçlar üzerinden Anayasanın 20. maddesinde düzenlenen özel hayatın gizliliğinin sınırlandırılmasına ilişkin kapsam ve sorunlara kişisel verilerin korunması açısından değinilecektir. Konu bu şekilde sınırlandırılmasına rağmen aşağıda görüleceği üzere sorun kişisel verilerin işlenmesini aşan boyutlara sahiptir.

³⁹⁹ Anayasa Mahkemesi Kararı, 1996/68 E. 1991/1 K. 6. 1.1999 T <http://www.anayasa.gov.tr/eskisite/KARARLAR/IPTALITIRAZ/K1999/K1999-01.htm>

Söz konusu kararın konusu, 4178 S. Kanunun 10. maddesiyle 1774 S. Kimlik Bildirme Kanununa eklenen Ek-1 maddesinin Anayasaya aykırılığına ilişkin olup madde şu şekildedir: *“Bu Kanunun uygulanması sırasında genel kolluk kuvvetlerine ait karakollara, il merkezlerinden de sorgulanabilen bilgisayar terminalleri konulur. Bunun için gerekli giderler İçişleri Bakanlığı bütçesine konulacak ödenekten karşılanır.”*

Adı geçen kararın konusunu oluşturan 4178 S. Kanunun 10. maddesine ilişkin iptal isteminin gerekçesinde, kişilerin bir bilgi toplama saklama, işleme ve değiştirme tekeli olan idareye karşı korunması gerektiği, Anayasanın temel hakların sınırlandırılmasının sınırı olarak öngördüğü *“demokratik toplum düzeninin gerekleri”*nin bunu zorunlu kıldığı, getirilen bu düzenlemede buna ilişkin hiçbir güvencenin yer almadığı ifade edilmiştir. Devamında, iptali istenen madde ile Anayasanın 20 maddesinde düzenlenen özel hayatın gizliliği hakkının sınırlandırıldığı, maddede bilginin niteliği ve toplanma amacı belirtilmediği için, düzenlemenin adli soruşturma ve kovuşturma istisnası içinde değerlendirilmesinin de mümkün olmadığı, çünkü, güvenlik kuvvetlerinin yakaladıkları şüphelilerin kimliklerine ilişkin bilgileri depolayabilecekleri gibi, herhangi bir suç kovuşturmasıyla ilgili salt gözlemlerine ve değerlendirmelerine yönelik bilgileri depolayabilecekleri ifade edilmiştir. Kişisel verilerin korunmasına ilişkin olarak Avrupa Konseyinin Sözleşmesine gönderme yapılarak değerlendirme yapılmış ve iptali istenen hükmün, genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanması yetkisini tanıdığı, fakat bu yetkinin Anayasal haklara getireceği sınırlamayı sınırlamadığı ve bu nedenle demokratik toplum düzeninin gerekleriyle bağdaşmadığı belirtilmiştir. Sonuç olarak, 4178 sayılı Yasa’nın 10. maddesinin, özel

hayatın gizliliğini düzenleyen Anayasanın 20. maddesine; temel hak ve hürriyetlerin demokratik toplum düzeninin gereklerine aykırı olarak sınırlanamayacağını düzenleyen 13. maddesine ve Türkiye Cumhuriyeti'nin demokratik hukuk devleti olduğunu düzenleyen 2. maddesine aykırı olduğu ifade edilmiştir .

Anayasa Mahkemesinin iptal isteminin reddi kararının gerekçesinde ise, ilgili yasa maddesi ile Bakanlar Kurulunca belirlenecek konaklama tesislerinin bilgisayarlarındaki bilgilerin, her konuda yararlanılmak için değil, sadece 1774 sayılı Yasa'nın uygulanmasını sağlamak amacıyla genel kolluk kuvvetlerinin bilgisayarlarına aktarılacağı ifade edilmiştir. Bu nedenle 1774 sayılı yasanın genel gerekçesinde yer bulan amacından⁴⁰⁰ hareketle dava konusu kuralın, kamu düzeni, genel asayiş ve kamu yararını sağlama amacına yönelik olması ve demokratik toplum düzeninin gereklerine de aykırı bir yönü bulunmaması nedeniyle, Anayasa'nın 2. 13. ve 20. maddelerine aykırı olmadığı sonucuna varılmıştır.

Yukarıda aktarılan Anayasa Mahkemesi Kararı özellikle iki açıdan önem arz etmektedir. İlk olarak Mahkeme, iptal isteminin gerekçesinde kişisel verilerin işlenmesine ilişkin düzenlemelerle bağlantı kurulmuş olan 1774 sayılı Kanun gereğince kişiye ilişkin bilgilerin toplanmasını, iptal isteminin gerekçesinde olduğu

⁴⁰⁰ 1774 sayılı Kimlik Bildirme Yasası'nın amacı, genel gerekçesinde şöyle açıklanmaktadır: “Milli güvenlik, kamu düzeni, kamu, toplum ve kişi yararı yönünden ülkemizdeki nüfus yerleşimi ve hareketlerinin; yabancıların geliş gidişlerinin, kaldıkları ve çalıştıkları yerler itibarıyla tesbiti ve izlenmesi zorunluluğu vardır... Vatandaşın seyahat, dilediği yerde oturma ve dilediği alanda çalışma hürriyeti Anayasa ile sağlanmış temel haklardan olmakla beraber kamu güvenliğini ve düzenini sağlamakla görevli Devlet örgütlerinin bu konuda bazı bilgilere sahip olması gerektiği ve bunun büyük önemi çok açık bir gerçektir. Esasen bu bilgilerin toplanmasını sağlamak maksadıyla Anayasa'ya uygun olarak alınacak kanuni tedbirlerin yukarıda sözü edilen temel hakların özü ile doğrudan doğruya bir ilgisi de bulunmamaktadır... Demokratik idare tarzına sahip Batı memleketlerinde de çeşitli şekillerde uygulandığı bilinen kimlik bildirme sisteminin tesisi ile elde edilecek bilgiler, kolluk hizmetlerinin yürütülmesinde büyük faydalar sağlayacağı gibi, kamu hizmetlerini ifa eden diğer kuruluşlar için de gerektiğinde yararlanılacak değerli bir kaynak olacaktır.”

gibi Anayasanın 20. maddesi kapsamında ele almış ve değerlendirmiştir. Buradan Anayasa Mahkemesinin de kişisel verilerin kaydedilmesini genel olarak özel hayatın gizliliği kapsamında değerlendirdiği sonucuna varmak mümkündür. Kararda yer alan diğer önemli husus, Mahkemenin, kişisel verilerin toplanmasının düzenlendiği 1774 sayılı Kanunun amacının belirtildiği genel gerekçesine gönderme yaparak, söz konusu maddeyi, Anayasanın 13. maddesinde yer alan genel sınırlandırma sebeplerini göz önüne alarak “*kamu düzeni*”, “*genel asayiş*” ve “*kamu yararı*”nı sağlama amacına yönelik olması nedeniyle iptal etmemiş olmasıdır. Buradan çıkarılacak sonuç ise kişisel verilerin toplanmasının ve işlenmesinin özel hayatın gizliliği kapsamında değerlendirildiği ve Anayasada özel hayatın gizliliğine yönelik sınırlandırma rejimine tabi olması gerektiğidir.

Anayasada temel hak ve hürriyetlerin sınırlandırma rejimi 2001 yılında tamamen değiştirilmiştir. Temel hak ve hürriyetlerin sınırlandırılması usul ve esaslarını düzenleyen 13. madde değiştirilmiş ve bu maddede yer alan genel sınırlandırma sebepleri kaldırılmıştır⁴⁰¹. 2001 yılında yapılan değişiklik sonrasında 13. maddeye göre, “*temel hak ve hürriyetler ilgili maddesinde belirtilen sınırlama sebeplerine bağlı olarak kanunla sınırlandırılabilir. Sınırlandırma ilgili temel hak ve hürriyetlerin özüne dokunamaz*”⁴⁰².

⁴⁰¹ 2001 yılı Anaya Değişikli öncesinde 1982 Anayasasına göre temel hak ve hürriyetlerinin sınırlandırılmasına ilişkin genel sınırlandırma nedenleri hakkında bkz, Yılmaz **ALİEFENDİOĞLU**, *2001 Anayasa Değişikliklerinin Temel Hak ve Özgürlüklerin Sınırlandırılmasında Getirdiği Yeni Boyut*, Anayasa Yargısı Dergisi C.19, 2002, s. 152. <http://www.anayasa.gov.tr/eskisine/anyarg19/aliefendioglu.pdf> Ayrıca bkz, H. Tahsin **FENDOĞLU**, *2001 Anayasa Değişikliği Bağlamında Temel Hak ve Özgürlüklerin Sınırlanması AY. Md 13*, Anayasa Yargısı Dergisi, C. 19, 2002 s. 122 vd. <http://www.anayasa.gov.tr/eskisine/anyarg19/fendoglu.pdf>

⁴⁰² 2001 yılı değişikliği sonrasında Anayasanın 13. maddesinin kapsamı ve içeriği hakkında bkz., **ALİEFENDİOĞLU**, s. 54 vd. **FENDOĞLU**, s. 130 vd.

Özel hayatın gizliliğini düzenleyen Anayasanın 20. maddesi de 4709 sayılı Kanunun 5. maddesi ile değiştirilmiştir. Bu değişiklikte birlikte An. 20. maddesinin 1. fıkrasında “*Herkes, özel hayatına ve aile hayatına saygı gösterilmesi isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*” hükmüne yer verilmiştir. 1. fıkra da yer alan “*Adli soruşturma ve kovuşturmaların getirdiği istisnalar saklıdır*” hükmü yapılan değişiklikte madde metninden çıkartılmıştır⁴⁰³.

Bu açıdan Anayasanın 20/1.maddede yapılan değişiklik Anayasanın 13. maddesinde yapılan değişiklikte birlikte değerlendirildiğinde, özel hayatın ve aile hayatının gizliliğine ilişkin anayasal bir sınırlama nedeninin olmadığı sonucuna varılabilir. Şöyle ki;

Anayasanın 20/2. maddesinde yer alan “*milli güvenlik, kamu düzeni, suçun işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması*” sınırlama nedenleri olarak karşımıza çıkmaktadır. Fakat 2. fıkra da belirtilen bu sınırlama nedenleri, 1. fıkra da düzenlenmiş bulunan özel hayatın gizliliğine yönelik sınırlama nedenleri olmayıp, bu sınırlama nedenleri, özel hayatın gizliliği kapsamında olan, bir kimsenin üstünün, özel kâğıtlarının ve eşyalarının aranması ve bunlara el konulmasına ilişkindir. Özel hayatın gizliliğinin görünümüleri olarak kabul edilen konut dokunulmazlığını ve haberleşme hürriyetini

⁴⁰³ 2001 değişikliği sonrasında Anayasanın 20. maddesi şu şekildedir: “*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Mülga cümle: 3.10.2001-4709/5 md.)...(Değişik: 3.10.2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.*”

düzenleyen 21. ve 22. maddelerinde bunlara ilişkin sınırlama nedenleri adı geçen maddelerde ayrıca belirtilmiştir⁴⁰⁴.

Anayasanın 13. maddesinde yapılan bu değişiklik sonrasında, düzenlendiği maddede hiçbir sınırlandırma sebepleri bulunmayan temel hak ve hürriyetlerin sınırlandırılıp sınırlandıramayacağı sorunun gündeme gelmiştir. Doktrinde sınırlama nedeni bulunmayan temel hak ve hürriyetlere ilişkin her hak ve hürriyetin genel bir norm alanı olduğu, bu alan dışında kalan hususlara ilişkin düzenleme temel hak ve hürriyeti sınırlamayacağı belirtilmiştir⁴⁰⁵. Ayrıca sınırlama sebebi bulunmayan temel hak ve hürriyetlerin, pratik uyum ilkesi gereği, başka bir hak ve hürriyetle çatıştığı durumlarda sınırlandırılabilmesi ve bu şekilde temel hak ve hürriyetler arasında denge kurulacağı ifade edilmiştir⁴⁰⁶.

Yukarıda aktarılan Anayasa Mahkemesi kararı doğrultusunda, kişisel verilerin toplanmasının özel hayatın gizliliği kapsamında ve bu hakkın norm alanı içerisinde olduğunu söylemek mümkündür. Bunun sonucunda kişisel verilerin toplanmasına ya da genel bir ifade ile işlenmesine ilişkin bir düzenleme Anayasanın 20. maddesinin 1. fıkrasında düzenlenen özel hayatın gizliliği kapsamında değerlendirilebilecektir. Anayasanın 20. maddesinde sınırlandırma sebeplerinin

⁴⁰⁴ Anayasanın 20. maddesinin 2. fıkrasında belirtilen sınırlama sebeplerinin birinci fıkra için de geçerli olduğu hakkında bkz, **ALİEFENDOĞLU**, s. 118.

⁴⁰⁵ **FAZIL SAĞLAM**, Temel Hakların Sınırlandırılması ve Özü, Ankara, 1982, s. 47 vd., s. 129 vd. **FAZIL SAĞLAM**, 2001 Yılı Anayasa Değişikliğinin Yaratabileceği Bazı Sorunlar ve Bunların Çözüm Olanakları, Anayasa Yargısı Dergisi, C.19, 2002, s. 4, <http://www.anayasa.gov.tr/eskisite/anyarg19/fsaglam.pdf> . Aynı yönde Mehmet **SAĞLAM**, Ekim 2001 tarihinde Yapılan Anayasa Değişiklikleri Sonrasında Düzenledikleri Maddede Hiçbir Sınırlama Nedenine Yer Verilmemiş Olan Temel Hak ve Özgürlüklerin Sınırı Sorunu, **Anayasa Yargısı Dergisi**, C.19, 2002, s. 255 vd.

⁴⁰⁶ **SAĞLAM**, Temel Hakların Sınırlandırılması ve Özü, s. 39 vd., s. 136 -137. **SAĞLAM**, 2001 Yılı Anayasa Değişikliği, s.4. Aynı yönde **SAĞLAM**, **Anayasa Değişiklikleri**, s. 258- 259

sadece 2. fıkrada belirtilen hususlar bakımından geçerli olması karşısında, özel hayatın gizliliğinin sınırlandırılmasına ve dolayısıyla kişisel verilerin toplanması ya da genel olarak işlenmesine ilişkin genel sınırlandırma sebebinin bulunmadığı sonucuna varmak mümkündür. Bu nedenle kişisel verilerin toplanmasına ve genel olarak işlenmesine ilişkin bir kanunda, söz konusu kararda olduğu üzere “*kamu düzeni*”, “*genel asayiş*” ve “*kamu yararı*”nı sağlama amacına yönelik olması gibi Anayasanın 13. maddesinde 2001 değişikliği öncesinde yer alan genel sınırlandırma nedenlerine bağlı olarak kişisel verilerin toplanmasına ve işlenmesine izin verilmesinin Anayasanın 13. ve 20. maddelerine aykırı olacağını söylemek mümkündür. Aynı şekilde özel hayatın gizliliği kapsamında değerlendirilen fakat Anayasanın 20. maddesinin 2. fıkrasına girmeyen bir husus hakkında da 2. fıkrada öngörülen sınırlandırma sebeplerine dayanılması Anayasaya aykırılık oluşturabilecektir.

Söz konusu durum halihazırda kişisel veri olarak nitelendirilebilecek bilgilerin toplanmasına ilişkin bir çok kanun bakımından sorun yaratmakla birlikte, tek tek bu kanunların ilgili hükümlerinin incelenmesi yerine kişisel verilerin işlenmesine ilişkin usul ve esasların genel olarak düzenlenmeye çalışıldığı ve halen Başbakanlıkta bulunan “*Kişisel Verilerin Korunması Hakkında Kanun Tasarısı*”nın ilgili maddeleri üzerinden değerlendirme yapılması, bu sorunun kapsamının somut olarak gösterilmesi bakımından yeterli olabilecektir.

Söz konusu Tasarıda, Kanunun kapsamının sadece “*veri kütüğüne*”⁴⁰⁷ bağlı olarak kişisel veri işlenmesi hallerini kapsayacağı, 2. maddede düzenlenmiştir.

⁴⁰⁷ Tasarının 3/(e) maddesinde veri kütüğü sistemi “*gerçek ve tüzel kişilere ilişkin belirli bir kritere göre kişisel verilere ulaşımı kolaylaştıracak şekilde yapılandırılmış herhangi bir kişisel veri grubu*” olarak tanımlanmaktadır.

Tasarının “*Hukuka uygunluk nedenleri*” başlıklı 6. maddesinde kişisel verilerin işlenmesinde hukuka uygunluk nedenleri öngörülmektedir⁴⁰⁸. Tasarının “*İstisnalar*” başlıklı 22 maddesinde ise genel olarak, “*milli güvenliğin korunması*”, “*milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbarî faaliyetlerin yürütülmesi*”; “*kamu düzeninin korunması*”, “*suçun önlenmesi için gerekli olması*”, “*suç veya meslek ahlak kurallarını ihlâl eden eylemlerin soruşturulması veya kovuşturulması*”; “*bütçe, vergi ve mâli konulara ilişkin olarak devletin önemli ekonomik veya malî çıkarlarının gerektirmesi*” hallerinde 6. maddeninde de dâhil olduğu birçok maddenin uygulanmayacağı öngörülmektedir⁴⁰⁹. 6. madde açısından incelendiğinde 22. maddede sayılan bu haller Tasarıda yer alan diğer hukuka uygunluk nedenleri olarak karşımıza çıkmaktadır.

⁴⁰⁸ **MADDE 6:** “(1) Kişisel veriler ancak ilgili kişinin açık rızasıyla işlenebilir. (2) Kanunlarda öngörülen yükümlülüklerin yerine getirilmesi dışında, ilgili kişinin bir itirazda bulunması hâlinde veri işlenemez. (3) Aşağıdaki hâllerde de hukuka uygunluk sebeplerinin bulunduğu kabul edilir: a) Kanunun öngördüğü bir zorunluluk dolayısıyla, kamu yararına veya resmi olarak verilmiş bir görevin yerine getirilmesi amacıyla veri işlenmesi, b) Kişisel verilerin, ilgili kişinin rızasını açıklayamayacak durumda olması hâlinde kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak amacıyla işlenmesi, c) Bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesi, ç) İlgili kişiler tarafından açıklanmış olması veya açık sicillerde mevcut bilgiler olması sebebiyle herkesçe bilinen kişisel verilerin işlenmesi.

d) Veri kütüğü sahibinin kendi haklı çıkarları için, ilgili kişinin temel hak ve özgürlükleri ile meşru çıkarlarına zarar vermediği sürece, veri işleminin zorunlu olması”

⁴⁰⁹ “**İstisnalar**” **MADDE 22:** “(1) Bu Kanunun 6, 11, 16, 17 ve 19 uncu maddeleri aşağıda sayılan haller bakımından uygulanmaz: a) Milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbarî faaliyetlerin yürütülmesi, b) Kamu düzeninin korunması, c) Suçun önlenmesi için gerekli olması, suç veya meslek ahlak kurallarını ihlâl eden eylemlerin soruşturulması veya kovuşturulması, ç) Bütçe, vergi ve mâli konulara ilişkin olarak devletin önemli ekonomik veya malî çıkarlarının gerektirmesi, d) (b), (c) ve (ç) bentlerinde belirtilen konularda, resmî mercilerin izleme, denetleme veya düzenleme görevlerinin gerektirmesi. (2) Bu Kanunun 12 nci maddesinde belirtilen haklar, kişisel verilerin özellikle belli bir kişiye ilişkin tedbir veya karar alınmasına yönelik kullanılmadığı ve ilgili kişinin özel yaşamının gizliliğinin ihlâl edilmesi riskinin bulunmadığı hallerde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, bilimsel araştırma veya istatistik oluşturma amaçları ile sınırlanabilir.”

Burada örnek olarak vermek gerekirse, özellikle kişisel verilerin işlenebilmesine ilişkin hukuka uygunluk nedenleri olarak karşımıza çıkan ve 6. maddede yer alan “*kamu yararı*” ve ayrıca 22. maddede yer alan “*milli güvenlik*”, “*kamu düzeni*”, 2001 değişikliği öncesinde Anayasada genel sınırlama nedenlerinin düzenlendiği 13. maddede yer alan temel hak ve hürriyetlerin sınırlandırma nedenleri oluşturmaktaydı. Yukarıda belirtildiği üzere 2001 Anayasa değişikliği sonrasında söz konusu genel sınırlandırma sebepleri kaldırılmıştır. Son haliyle Anayasanın 20. maddesinde kişinin üstü ve özel kağıtları ve eşyasının aranması ve ayrıca bunlara el konulmasına ilişkin nedenler arasında “*milli güvenlik*”, “*kamu düzeni*” nedenleri yer almaktadır. Yukarıda belirtildiği üzere, Anayasanın 20. maddesinin 2. fıkrasında düzenlenen sınırlandırma nedenleri, 1. fıkra düzenlendiği şekliyle genel olarak özel hayatın gizliliği ile ilgili olmayıp sadece ikinci fıkra düzenlenenen kişinin üstünün ve özel kağıtları ve eşyasının aranması durumuna hasredilmiştir.

Anayasada 20. maddenin birinci fıkrasına ilişkin herhangi bir sınırlama nedeni öngörülmemiş olması karşısında, Tasarının 6. ve 22. maddesinde öngörülen hukuka uygunluk nedenlerinin, özel hayatın gizliliği kapsamında değerlendirilen kişisel verilerin korunması bakımından, normlar hiyerarşisi içerisinde Anayasaya uygun bir sınırlandırma olduğu tartışmalı olup Anayasanın genel olarak temel hak ve hürriyetlerinin sınırlandırılmasına ilişkin rejimi ve 20. maddesi karşısında Anayasaya aykırılık teşkil edebileceğini söylemek mümkündür.

Kişisel verilerin korunması hakkındaki Tasarıya ilişkin yukarıda aktarılan örnek kapsamında dile getirilen Anayasanın 20. maddesine ilişkin sorunun halihazırda yürürlükte bulunan birçok kanun bakımından da söylemek mümkündür.

Kişisel verilerin de yer aldığı birçok hususu bünyesinde barındıran özel hayatın gizliliğine ilişkin *Sağlam* tarafından dile getirildiği üzere, pratik uyuşum ilkesi çerçevesinde sınırlandırılması halleri hariç Anayasanın 20. maddesinin birinci fıkrasında sınırlandırma nedeni bulunmamaktadır. Kişisel verilerin işlenmesine ilişkin düzenlemelerde, Anayasanın 20. maddesinin birinci fıkrasında yer alan ve hiçbir sınırlandırma nedenine yer verilmeyen düzenlemeye uyulması zorunludur.

Aynı şekilde, kişisel verilerin korunmasına ilişkin suçlar arasında düzenlenen 135. maddenin ikinci fıkrasında yer alan hükümle ilgili olarak “... özellikle suçlulukla mücadele bağlamında, suç ve suçluların ortaya çıkartılmasını sağlamak amacıyla belli ölçüde izin verilebilir...” gerekçesinin Anayasanın 13. ve 20. maddeleri karşısında yeniden değerlendirilmesi gerekmektedir⁴¹⁰.

C. Kişisel Verilerin İşlenmesine İlişkin Usul ve Esaslar – Kişisel Verilerin Korunmasına İlişkin İlkeler

1.Genel Olarak

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

⁴¹⁰ Gerekçe için bkz., GÜNEY, s. 415.

yani veri/enformasyon mahremiyetinin ve dolayısıyla özel hayatın gizliliğinin korunması isteğidir⁴¹¹.

Kişisel verilerin işlenmesine ilişkin düzenlemeler incelendiğinde, hangi tür kişisel verilerin ne şekilde işleneceğinin belirlenmesi yerine, kişisel verilerin korunmasına ilişkin ilkeler olarak adlandırılan kişisel verilerin işlenmesindeki usul ve esasların asıl olarak düzenlendiği söylenebilir. Bu açıdan söz konusu usul ve esaslar ya da ilkeler, genel olarak usule ilişkin koruyucu tedbirlerdir⁴¹². Bunun yanında, hassas veriler olarak adlandırılan bazı nitelikteki kişisel verilerin ise, verinin içeriği esas alınarak, ya işlenmesi yasaklanmakta ya da işlenmesine izin verilmekle birlikte daha katı koruyucu tedbirlerin alınması öngörülmektedir.

Bu açıdan kişisel verilerin işlenmesine ilişkin düzenlemelerin kapsam ve içeriğini oluşturan kişisel verilerin işlenmesine ilişkin ilkeler, genel olarak, “1. kişisel verileri dürüst ve hukuka uygun bir şekilde toplama ve işleme (*dürüst toplama ilkesi* - *dürüst ve hukuka uygun toplama ve işleme*); 2. kişisel verilerin toplanmasının, verinin toplanma amaç(lar)ının gerçekleştirilmesi için gerekli olduğu miktarla sınırlı tutulması (*asgarilik ilkesi*); 3. kişisel veriler önceden belirlenmiş ve hukuka uygun amaçlarla toplama, işleme ve bu amaçlarla bağdaşmayan şekillerde işlememe (*amaçla bağlılık ilkesi*); 4. belirlenen amaçlar dışında bir amaç için kişisel verilerin

⁴¹¹ PHR 2004’te kişisel verilerin işlenmesine ilişkin düzenlemelerin nedenleri 3 grupta toplanmıştır. Raporu göre, “1. eski otoriter rejimler altında meydana gelen özel hayata yönelik ihlalleri bertaraf etme; (özellikle orta Avrupa güney Amerika ve Güney Afrika’da), 2. Elektronik ticareti destekleme (özellikle Asya ülkeleri); 3. Avrupa Birliğine katılma isteği olan ülkelerin (özellikle doğu ve orta Avrupa ülkeleri) Sözleşme ve Yönerge doğrultusunda ve diğer ülkelerin Yönerge hükümleri nedeniyle özellikle ticaretin etkilenmesinden sakınmak amacıyla düzenleme yapması,” verilerin işlenmesine ilişkin düzenlemelerin yapılmasının nedenleri olarak gösterilmektedir.

Privacy and Human Rights 2004, An International Survey of Privacy Laws and Developments (PHR2004) <http://www.privacyinternational.org/> (kontrol tarihi 28.03.2004).

⁴¹² BENNET, s.98

kullanımının sadece veri sahibinin rızasının veya yasal bir yetkinin varlığı durumunda mümkün olması (*kullanımın sınırlandırılması ilkesi*); 5. kişisel verilerin doğru, tam ve işleme amaçları ile ilgili olması ; 6. kişisel verilerin istenmeyen ya da yetkili olmayan ifşalardan, yok edilmeden veya değiştirilmeden korumak için gerekli güvenlik önlemleri alınması (*korum - /güvenlik ilkesi*); 7. veri öznelerinin, diğerleri tarafından elde tutulan verileri hakkında bilgilendirilmesi, bunlara erişimleri sağlanması ve yanlış veya yanıltıcı olması durumunda düzeltme olanağına sahip olması (*bireysel katılım ilkesi*); 8. başkaları hakkındaki verileri işlemekle sorumlu olan kişilerin, yukarıda sayılan hususlara uyma yönünde sorumlu tutulması (*sorumluluk ilkesi*)” olarak sekiz başlık altında toplamak mümkündür⁴¹³.

Kabaca dile getirilecek olursa, kişisel verilerin hukuka uygun bir şekilde işlendiğinden bahsedilebilmesi için öngörülen bu usul ve esaslara ya da ilkelere uygun davranılması gerekmektedir. Bu usul ve esaslara uyulmaması halinde ortada bir kötüye kullanım olduğu ve özel hayatın gizliliğinin bir yönünü oluşturan veri mahremiyetinin ihlal edildiği kabul edilebilecektir.

Yukarıda aktarılan ilkelerin çeşitli yönleriyle ele alındığı ve genel olarak kişisel verilerin işlenmesi usul ve esaslarının gösterildiği, kişisel verilerin korunması başlığı altında toplanabilecek kanunlar hali hazırda bir çok ülkenin mevzuatına girmiş bulunmaktadır⁴¹⁴. Kişisel verilerin korunmasına ilişkin suçlar incelendiğinde genel olarak kişisel verilerin işlenmesine ilişkin usul ve esaslara aykırı fiillerin çeşitli

⁴¹³ **BYGRAVE, Data Protection** s.3; Raymond **WACKS, Personal Information: Privacy and the Law**, Clarendon Press, Oxford 1989., s. 210

⁴¹⁴ Çeşitli ülkelerin kişisel verilerin korunmasına ilişkin mevzuat hakkında bkz., http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/NATIONALLAWS-EN.asp#TopOfPage

yönleriyle ele alındığı görülmektedir. Bu açıdan kişisel verilerin korunmasına ilişkin suçlar kişisel verilerin işlenme usul ve esaslarına aykırı fiilleri oluşturmaktadır.

Nitekim İtalya ve Almanya’da kişisel verilerin korunmasına ilişkin usul ve esasların yer aldığı kanunlarda aynı zamanda kişisel verilerin korunmasına ilişkin suçlara da yer verilmiştir⁴¹⁵. Buna karşın Fransa’da kişisel verilerin korunmasına ilişkin suçlar, kişisel verilerin korunmasına ilişkin kanun yerine Fransız Ceza Kanununda düzenlenmiştir.

Ülkemizde ise halen kişisel verilerin korunmasına yönelik olarak kişisel verilerin işlenmesine ilişkin usul ve esasların yer aldığı özel bir düzenleme yer almamakla birlikte kişisel verilerin korunmasına ilişkin suçlara TCK’nin 135 vd. maddelerinde yer verilmiştir. Türk Ceza Kanununda Kişisel verilerin korunmasına ilişkin suçların düzenlenmesinde, Fransız Ceza Kanununda takip edilen yöntemin tercih edildiği görülmektedir. Yöntemsel olarak bu tercihin yanında kişisel verilerin korunmasına ilişkin suçlar bakımından da Fransız Ceza Kanununda yer alan suçlardan esinlenildiği anlaşılmaktadır. Fransa’da her ne kadar kişisel verilerin korunmasına ilişkin suçlar Fransız Ceza Kanununda yer alsa da, kişisel verilerin korunmasına ilişkin kanunda kişisel verilerin işlenmesine ilişkin usul ve esasların ayrıntılı olarak düzenlendiği görülmektedir. Kişisel verilerin korunmasına ilişkin suçlar ise genel olarak kişisel verilerin korunmasına ilişkin kanunda yer alan usul ve

⁴¹⁵ İtalyan Kişisel Veri Koruma Kanunun İngilizce çevirisi için bkz., http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/Italy%20DataProtectionCode-2003.pdf

Almanya’da Kişisel verilerin korunması hakkında Federal Kanunun İngilizce çevirisi için bkz., http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf

esaslara uymamanın yaptırımı olarak çeşitli şekillerde Fransız Ceza Kanunu içerisinde yer almaktadır⁴¹⁶. Nitekim bu husus Fransa’da kişisel verilerin korunmasına ilişkin Kanunun 50. maddesinde, Kanunda yer alan hükümlerin ihlaline ilişkin suçların Fransız Ceza Kanunun 226-16-226-24 maddelerinde düzenlendiği belirtilerek açıkça ifade edilmiştir⁴¹⁷.

Tarihsel olarak, kişisel verilerin korunmasına ilişkin suçların kişisel verilerin işlenmesine ilişkin usul ve esaslara bağlantılıdır. TCK’de yer alan kişisel verilerin korunmasına ilişkin suçların esinlendiği Fransız Ceza Kanunundaki suçlar da kişisel verilerin korunmasına ilişkin Kanunun hükümlerinin ihlal olarak Fransız Ceza Kanununda yer almaktadır. Bu nedenlerle TCK’de yer alan suçların anlaşılması bakımından kişisel verilerin işlenmesine ilişkin usul ve esasların incelenmesi gerekmektedir. Aşağıda veri işleyenin sorumluluk ve yükümlülüklerine ilişkin olarak gündeme gelen dürüst ve hukuka uygun toplama ve işleme ilkesi ve amaçla bağlılık ilkesine değinilecektir.

2. Veri İşleyenin Sorumluluk ve Yükümlülükleri

a. Genel Olarak

Kişisel verilerin hukuka uygun ve dürüst bir şekilde toplanması ve işlenmesi; amaçla bağlılık olarak da adlandırılan, belirli ve önceden belirtilmiş amaçlar için kullanılması, belirlenen amaçlarla bağdaşan şekilde kullanılması; belirlenen

⁴¹⁶ Fransız Ceza Kanunun İngilizce çevirisi için bkz., http://www.legifrance.org/html/codes_traduits/code_penal_textan.htm

⁴¹⁷ Kanunun İngilizce çevirisi için bkz., “Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties”, <http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf>

amaçlarla uygunluk göstermeyen kişisel verilerin toplanmaması ve işlenmemesi, belirlenen amaçlar için gerekli olduğu süreden daha fazla saklanmaması⁴¹⁸; kişisel verilerin işlenmesine ilişkin usul ve esaslara göre işlenmemesi durumunda veri işleyicisinin bu durumdan sorumlu tutulması hususları bu başlık altında toplanabilir. Bunlardan başka *Bennet*'in güvenlik ilkesi olarak adlandırdığı, veri işleyen tarafından verilerin hukuka aykırı olarak üçüncü kişilerin eline geçmesini önleyici tedbirlerin alınması⁴¹⁹ da bu başlık altında düşünülebilir.

b. Dürüst ve Hukuka Uygun Toplama ve İşleme

Kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan birinci ilke kişisel verilerin hukuka uygun ve dürüst bir şekilde toplanması ve işlenmesidir. Dürüst ve hukuka uygun işleme ilkesine ilişkin olarak Sözleşmede, kişisel verilerin dürüst ve hukuki yollardan elde edilmesi ve işlenmesi gerektiği (m.5/a), OECD ilkelerinde dürüst ve hukuki yollardan elde edilmesi, uygun olduğu durumlarda, veri öznesine bilgi verilmesi veya veri öznesinin rızasının alınması gerektiği⁴²⁰ (m. 7), Yönergede ise, kişisel verilerin dürüst ve hukuka uygun bir şekilde işlenmesi (processs) gerektiği, (m. 6/1(a)) hükümlerine yer verilmiştir.

⁴¹⁸ **CATE**, s.46

⁴¹⁹ **BENNET**, s. 110.

⁴²⁰ OECD ilkelerine ilişkin açıklayıcı memorandumda bazı durumlarda, veri öznesinin bilgisi ya da rızası pratik nedenlerle mümkün olmayabileceği ve maddede geçen “uygun olduğu durumlarda” ibaresi veri öznesinin bilgi veya rızasının önemli görülmediği durumları ifade etmek amacıyla kullanıldığı belirtilmektedir. Açıklayıcı memorandumda ceza soruşturması sırasında kişisel veri toplanması ya da posta listesi güncellenmesi gibi durumlar örnek olarak verilmiştir. **Bkz Ocdaçıklayıcı not**, s. 41.

Dürüst ve hukuka uygun işleme, dürüst toplama, dürüst ve hukuka uygun toplama ve işleme⁴²¹ gibi farklı şekillerde ifade edilse de, kişisel verilerin işlenmesi sürecinin tamamını kapsayan temel bir ilke olarak karşımıza çıkmakla birlikte, bu ilkeye ilişkin Sözleşme ve OECD ilklerinde başkaca bir hükme yer verilmemiş ve bu hususların tespiti devletlere bırakılmıştır. Yönergenin 7. maddesinde ise hangi hallerde kişisel verilerin işlenebileceği ayrıca düzenlemiştir. Yönergenin meşru işleme halleri olarak ifade edilen 7. maddesine göre kişisel veriler genel olarak, “*veri öznesinin rızasının olması*”, “*kamu yararı veya yasal bir yetkinin kullanılması*” ve son olarak “*menfaatlerin dengelenmesi*” (Türl Medeni Kanununun 24 maddesinde ifade edilen şekliyle üstün çıkarın bulunması) olarak özetlenebilecek üç halde işlenebilir⁴²².

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.

⁴²¹ Sözleşme 5/a m.

⁴²² **KORFF**, s. 73 vd.

Madde incelendiğinde kişisel verilerin işlenmesinde asıl olan veri öznesinin kuşkuya yer vermeyecek şekilde açık rızasının varlığıdır (7/a). Yönergenin 7.maddesine göre, veri öznesinin rızasının aranmadığı diğer durumlar ise, zorunlu olması koşuluyla, veri öznesi ile yapılmış bir sözleşmenin ifası veya bir sözleşmenin yapılması (7/b); yasal bir yükümlülüğün yerine getirilmesi (7/c); veri öznesinin hayati bir yararının korunması (7/d); verinin ifşa edildiği üçüncü kişinin veya veri kontrolörüne tanınan yasal bir yetkinin kullanılması ya da kamu yararı nedeniyle bir görevin yerine getirilmesidir (7/e). Meşru menfaat nedeniyle kişisel veri işleyebilmesi ise, veri öznesinin rızasının ve zorunlu olma koşulunun aranmadığı, diğer bir hukuka uygun işleme durumudur (7/f). Bu son durumda kişisel verilerin işlenmesi, meşru çıkarın, veri öznesinin Yönergenin 1. maddesinde belirtilen temel hak ve hürriyetlerinden (özellikle özel hayatın gizliliğinin) üstün olmaması şartına bağlıdır. Ayrıntılı bilgi için bkz., **LLOYD**, s.119 vd.; **KORFF**, s. 73 vd.

Yukarıda belirtildiği üzere 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 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 bir kişilik hakkına saldırı olarak da değerlendirilebilmektedir.

Bilindiği üzere, temel hak ve hürriyetler özel hukuk alanında genel olarak kişilik hakkı kapsamında olup özel hayatın gizliliği de kişilik hakkının bir parçası olarak korunmaktadır⁴²³. Yukarıda da belirtildiği üzere, kişisel verilerin korunması

⁴²³ Ahmet **KILIÇOĞLU**, Şeref, Haysiyet ve Özel Yaşama B.n Yoluyla Saldırılarından Hukuksal Sorumluluk, Gözden Geçirilmiş 2. B., Ankara 1993, s.5; Ayrıca bkz., Ergun **ÖZSUNAY**, Gerçek Kişilerin Hukuki Durumu, 4. B., İstanbul 1979, s. 126 vd.; Bilge **ÖZTAN**, Medenî Hukukun Temel Kavramları, Turhan Kitabevi Yayınları 10 B., Ankara

genel olarak veri mahremiyetini sağlamaya yönelik olup, bu haliyle özel hayatın gizliliğinin bir yönünü oluşturmaktadır. Kişisel verilerin işlenmesinde de TMK’de de, kişilik hakkının korunmasına ilişkin kurallara uyulması zorunludur. Nitekim, TMK’nin 24/2. maddesinde, kişilik haklarına müdahalenin hangi hallerde hukuka uygun sayılacağı belirtilmektedir. Adı geçen maddeye göre “zarar görenin rızası”, “üstün nitelikte özel veya kamusal bir yararın varlığı”, “kanunun verdiği yetkiye dayanılarak kişilik hakkına yapılan saldırı”, kişilik hakkına müdahaleyi hukuka uygun kılar⁴²⁴.

Bu söylenenler doğrultusunda, özel hayatın gizliliği kapsamında ele alınan kişisel verilerin, TMK’nin 24. maddesinde belirtilen hukuka uygunluk koşullarına uygun bir şekilde işlenmesi durumunda, hukuka uygun bir şekilde işlemeyen bahsedilebilecektir. TMK’nin 24. maddesinde belirtilen şartların oluşmaması durumunda özel hayatın gizliliğine hukuka aykırı bir müdahale söz konusu olacaktır. Bu açıdan TCK ve özel kanunlarda bu yönde bir müdahaleye izin veren ya da yetkilendiren bir normun bulunmaması halinde kişisel verilerin işlenmesi, hukuka aykırıdır⁴²⁵.

2002, s. 254 vd.; Aydın **ZEVKLİLER**, Medeni Hukuk:Giriş ve Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku, Savaş Yayınları, 3. B. Ocak 1992, s. 395 vd.

Kılıçoğlu, “Kişilik hakkı, genel anlamda, kişisel varlıklar üzerinde söz konusu olan şahsa bağlı bir mutlak haktır. Yaşam, sağlık, özgürlükler, şeref ve haysiyeti özel yaşam, isim, resim, his yaşamı gibi kişisel varlıklar üzerindeki haklar kişilik hakkını ifade eder.”demekte; Öztan da kişilik hakkı yerine kişilik hakları ifadesini kullanmakta ve “Kişilik hakları, insana insan olması nedeniyle ve onun korunması için tanınan haklar topluluğudur. Öğretide ağır basan görüşe göre, kişilik hakları, kişinin kişi olması nedeniyle sahip olduğu hak ve fiil ehliyetinin yanında, kişinin hayatı sağlığı, bedenî bütünlüğü, şeref ve haysiyeti, itibarı, sırları, adı ve diğer değerleri üzerindeki hakların tamamını kapsar.” görüşünü dile getirmektedir. **KILIÇOĞLU**, s. 4.; **ÖZTAN**, s.251. Genel olarak kişilik hakkı ve kapsamı için ayrıca bkz., **ZEVKLİLER**, , s. 373 vd.

⁴²⁴ **ÖZTAN**, s. 261.

⁴²⁵ Aynı yönde, **BAŞALP**, s.10.

Yukarıda, kişisel verilerin işlenmesinde hukuka uygunluk boyutuna kısaca değinilmiş olmakla birlikte, dürüst ve hukuka uygun işleme, aynı zamanda TMK.nun 2. maddesinde düzenlenen dürüstlük kuralı ile bağlantılıdır. *Edis*, doğruluk ve güven ilkesi ya da objektif hüsünüyet olarak da adlandırılan dürüstlük kuralını, “*orta zekâlı, normal, makul kimselerin, toplum içerisinde karşılıklı güvene, ahlaka ve dürüstlüğe dayalı davranışları sonunda meydana gelmiş ve toplum ihtiyaçları ile iş hayatının gereklerine cevap veren, -bu nedenle de- herkesçe bilinen kurallar bütünü*” olarak tanımlamaktadır⁴²⁶. Zevkliler ise, dürüstlük kuralının, toplum içinde kişilerin birbirleriyle olan ilişkilerinde nasıl davranmaları gerektiğini

Alman Veri Kanununun § 4 (1). maddesinde de göre kişisel verilerin bu veya diğer yasal düzenlemelerin izin verdiği ya da zorunlu kıldığı hallerde veya veri öznesinin rızasının bulunduğu hallerde kullanılabileceği veya işlenebileceği hükmüne yer verilmiştir Alman Veri Koruma Kanunun (**Bundesdatenschutzgesetz- BDSG**) İngilizce çevirisi için bkz http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf. (kontrol tarihi 12.05.2006)

İtalyan Veri Koruma Kanununda işleme terimi, toplamada dâhil bütün süreci kapsayacak şekilde geniş anlamda kullanılmakta ve adı geçen kanunun 11/1(a) maddesinde kişisel verilerin dürüst ve hukuka uygun bir şekilde işlenebileceğinden bahsedilmektedir. Kanunun İngilizce çevirisi için bkz.,

<http://www.garanteprivacy.it/garante/document?ID=1219452&DOWNLOAD=true> (kontrol tarihi 12.06.2006)

⁴²⁶ Seyfullah **EDİS**, *Medenî Hukuka Giriş ve Başlangıç Hükümleri*, 6. B., Ankara 1997, s. 291; Aynı yönde **ÖZTAN**, s.159.

“Tarihi çıkış noktası göz önünde tutulduğu zaman MK. m. 2. f. 1’de ‘güven düşüncesi’nin hakim olduğu görülür. Nitekim sözleşmeden doğan ilişkilerde taraflardan herbiri, verilen söze bağlı (sadık) kalınacağı, bir başka deyişle ‘ahde vefa’ gösterileceği bir karşı taraf da bu söze güvenebileceği inancı içerisinde olacağından taraflar arasında bir ‘bir karşılıklı güven ilişkisi’ kurulur. Bunun sonucu olarak da her hukuki ilişkide ilgililerin, birbirinden beklemeye haklı oldukları hususlarda yanıtılmamaları gerekir.” Bkz., **EDİS**, s. 290.

gösterdiğini ve hatta kişilere dürüstlük kuralının gösterdiği bir biçimde davranma yükümlülüğünü yüklediğini ifade etmektedir⁴²⁷.

TMK'nin 2. maddesinde ifadesini bulan dürüstlük kuralı genel olarak, hakların kullanılmasında, hukuki işlemde veya kanunda bir düzenlemenin yapılmadığı durumlarda, işlemin tamamlanmasında ve kanundaki boşluğun doldurulmasında veya hukuki işlemin ve kanundaki bir yorumunda göz önünde tutulur⁴²⁸. Bu açıdan bir hakkın kullanılmasında ya da borcun yerine getirilmesinde veya kanunun yorumlanmasında ya da tamamlanmasında, hakkın amacına uygun olarak kullanılması ya da kanunun, amacına uygun olarak yorumlanması veya tamamlanması gerekir⁴²⁹. Dürüstlük kuralı hukuki işlemler alanında ise, hukuki işlemin öncesi ve sonrasında, tarafların birbirinden beklemeye haklı oldukları hususlarda yanıltılmamaları olarak şeklinde yorumlanmaktadır⁴³⁰. Kısaca aktarılan bu hususlar birlikte değerlendirildiğinde dürüstlük kuralı kapsamında “*amaca uygun davranma*” ve “*yanıltılmama*” iki önemli unsur olarak karşımıza çıkmaktadır.

Kişisel verilerin korunmasına ilişkin düzenlemelerde yer alan dürüst toplama ve işleme ilkeli ile ilgili olarak, kişisel verilerin kişinin nasıl kullanıldığının anlaşılamayacağı tarzda kullanılamaması şeklinde yorumlanması gerektiği, bu ilkeye yer verilmeyen bir durumda kişisel verinin kullanımının sınırlandırılmayacağı dile

⁴²⁷ **ZEVLİLER**, s.135.

⁴²⁸ **ÖZTAN**, s. 161. Aynı Yönde **ZEVLİLER**, s. 135, Turgut **AKINTÜRK**, Medeni Hukuk, 4. B., Savaş Yayınları Ankara 1991, s. 92. Dürüstlük kuralının uygulanma alanı ile ilgili ayrıntılı bilgi için ayrıca bkz., **EDİS**, 301 vd.

⁴²⁹ **ZEVLİLER**, s. 135 vd. **EDİS**, s. 304 vd.

⁴³⁰ **ÖZTAN**, s. 161. **EDİS**, s. 290.

getirilmiştir⁴³¹. Nitekim *Lloyd*, dürüst olma kriterinin subjektif bir anlam taşıdığını belirtmekle birlikte, İngiliz Veri Koruma Kanununun (1998) ilgili maddesinde bu hususun, kendisinden kişisel veri toplanan kişinin, kişisel verilerin hangi amaç ya da amaçlar için kullanılacağı, konusunda aldatılmaması ya da yanıltılmaması şeklinde ifade edildiğini belirtmekte ve ayrıca bu ilkenin yorumunda amaca uygun işlemeye de işaret etmektedir⁴³². Avrupa Konseyi Bakanlar Komitesinin 1973 tarihli tavsiye kararının açıklayıcı notunda da dürüst işleme ilkesine uyulup uyulmadığının saptanmasında aşağıda incelenecek olan amaçla bağlılığın belirleyici kriter olduğu ifade edilmiştir⁴³³.

Yukarıda söylenenler topluca değerlendirildiğinde, dürüst toplama ve işleme, TMK'nin 2. maddesinde yerini bulan dürüstlük kuralı ile bağlantılıdır. Kişisel verilerin dürüst olarak toplanması ve işlenmesi ilkesi, genel olarak işleme süreci içerisinde kişinin toplama ve işleme amacı hususunda yanıltılmaması ve amaçla bağdaşmayan ya da kişilerin anlayamayacağı bir amaç için işlenmemesi hususlarını kapsamaktadır. Aktarılan bu hususlar ise dürüstlük kuralının temelini oluşturan amaca uygun davranma ve yanıltmama ile örtüşmektedir. Nitekim aşağıda da inceleneceği üzere, dürüstlük kuralının bir parçasını oluşturan amaca uygun davranma, kişisel verilerin korunmasına ilişkin düzenlemelerde kişisel verilerin

⁴³¹ Bkz. *The Privacy Principles of the Information Infrastructure Task Force*, aktaran CATE, s. 189 vd.

Yönergede yer alan hükümlerle ilgili olarak Avrupa Birliği'ne üye ülkelerin mevzuatlarının karşılaştırmalı olarak incelenmesi için bkz., KORFF, s. 62

⁴³² LLOYD, s.110-111

⁴³³ Bkz., **Avrupa Konseyi, Resolution (74) 29** on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, **Explanatory Memorandum, parag. 16.**, [http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20\(74\)%2029.asp#TopOfPage](http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20(74)%2029.asp#TopOfPage) (kontrol tarihi 13.03.2005)

işlenmesinin kapsam ve sınırlarının belirlenmesi açısından merkezi bir konuma sahiptir. Ancak belirli amaç ya da amaçlar için kişisel verilerin işlenmesine izin verilebilir ve işleme amacı konusunda veri öznesinin veya üçüncü kişilerin yanıltılmaması esastır. Bu açıdan dürüst toplama ve işleme ilkesinin, hakkın kötüye kullanılması yasağı olarak da adlandırılan ve TMK'nin 2. maddesinde düzenlenen dürüstlük kuralının kişisel verilerin işlenmesi alanındaki görünümü olduğu sonucuna varmak mümkündür.

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.

Nitekim Anayasanın 13. maddesinde temel hak ve hürriyetlerin sınırlandırılması, TMK'nin 24. maddesinde ise buna paralel olarak kişilik hakkının korunması ve bunlara yönelik bir müdahalenin hukuka uygunluk koşulları belirtilmektedir. Kişisel verilerin korunmasına ilişkin bir düzenlemenin hem Anayasaya uygun olması hem de Yönergede olduğu gibi TMK'nin 24. maddesi ile örtüşmesi zorunludur. Dürüst ve hukuka uygun toplama ve işleme aynı zamanda bütün hukuk düzeni açısından geçerli bir kural olarak karşımıza çıkan hakkın kötüye

kullanılması yasağı veya TMK'nin 2. maddesindeki ifadesiyle dürüstlük kuralını da kapsamaktadır⁴³⁴.

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 zaman dürüstlük hukuka uygun toplama ve işleme ilkesine uyulup uyulmadığının saptanmasında belirleyici kıstas olarak karşımıza çıkmaktadır⁴³⁵.

c. Amaçla Bağlılık

Kişisel veriler önceden belirlenmiş ve hukuka uygun amaç ya da amaçlar için toplanması ve bu amaçlarla bağdaşmayan şekillerde işlenmemesi olarak özetlenebilecek olan amaçla bağlılık, kişisel verilerin dürüst ve hukuka uygun olarak işlenip işlenmediğinin somut bir durumda gerçekleşip gerçekleşmediğinin tespiti bakımından önem taşır⁴³⁶. 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.

⁴³⁴ Wacks da her ne kadar kişisel verilerin işlenmesine ilişkin ilkelerde dürüstlük kuralına açık bir atıf yapılmamasına rağmen Dürüst ve hukuka uygun işleme ilkesinin dürüstlük kuralını da içerdiğini belirtmektedir. Bkz., **WACKS**, s. 211 vd.

⁴³⁵ Bkz., **Avrupa Konseyi, Resolution (74) 29** on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, **Explanatory Memorandum, parag. 16.**, [http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20\(74\)%2029.asp#TopOfPage](http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20(74)%2029.asp#TopOfPage)

⁴³⁶ Bkz., **Avrupa Konseyi, Resolution (74) 29** on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, **Explanatory Memorandum, parag. 16.**, [http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20\(74\)%2029.asp#TopOfPage](http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Resolution%20(74)%2029.asp#TopOfPage)

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 halihazırda bilinmeyen amaç ya da amaçlar için kişisel veriler işlenemez⁴³⁷. Aynı şekilde, kişisel veri ancak toplanma anında belirtilmiş amaç doğrultusunda amaca uygun bir şekilde işlenebilir; belli olan bu amaçla ilgisiz amaçlar için işlenemez⁴³⁸. Diğer ilkelerle birlikte bu ilke aracılığıyla kişisel verilerin çok amaçlı kullanılmasının sınırlandırılması sağlanmak istenmekte⁴³⁹ ve kişisel verilerin işlenmesinde keyfiliğin önlenmesi amacına hizmet etmektedir.

Bu ilkeye ilişkin BM ilkelerinin⁴⁴⁰ 3. maddesinde kişisel verinin kullanım amacının belirli ve meşru olması ve genel olarak kamunun ve ayrıca hakkında kişisel verilerin toplandığı kişinin bilgisine sunulması gerektiği belirtilmektedir. OECD ilkelerinin 9. maddesine göre, kişisel verilerin hangi amaç için işleneceği en geç

⁴³⁷ **Simitis, SPIROS** *Reviewing Privacy In an Information Society*, U.Pa. L. Rev, 1986-1987, s. 740.; Bennett, J. Colin, **Regulating Privacy**, s.108.

⁴³⁸ **BENNET**, s. 108 Sözleşmenin açıklayıcı raporunda amaçla bağlılık ilkesinin 5. maddenin (c) bendinde toplanan kişisel verinin niteliği (doğru, tam ve işleme amacı ile ilgili olması) ilkesiyle birlikte kişisel verilerin belirli olmayan amaçlar için saklanması önüne geçilmesi amacıyla öngörüldüğü belirtilmektedir. Bkz. **Explanatory Report: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (ETS No. 108), <http://conventions.coe.int/Treaty/en/Reports/Html/108.htm> pr. 42

⁴³⁹ **SPIROS**, s. 740; **BENNET**, , s.108.

⁴⁴⁰ “**Guideline for the Regulation of Computerized Personal Data Files**” Adopted by General Assembly resolution 45/95 of 14 December 1990. <http://www.unhchr.ch/html/menu3/b/71.htm>

kişisel veri toplanmaya başlandığı anda belirlenmiş olmalıdır⁴⁴¹. Sözleşmenin 5. maddesinin (b) bendinde bu husus, kişisel veriler “*belli ve meşru amaçlar için saklanmalı ve bu amaca aykırı şekilde kullanılmamalıdır*” şeklinde dile getirilmiştir⁴⁴². Yönergenin 6/1 (b) maddesine göre de kişisel verileri açık ve meşru amaçlar için toplanabilir, bundan başka, bu amaçlarla bağdaşmayacak bir şekilde işlenmez.

Amaçla bağlılık ilkesi, kişisel verilerin rızaya bağlı olarak işlenmesi durumunda rızanın varlığı ve kapsamının belirlenmesi bakımından önemlidir⁴⁴³. Yukarıda belirtildiği üzere 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 bir inceleme yapılması ve toplanma ve işlenmeye başlandığı andaki amaç ya da amaçların belirlenmesi gerekmektedir⁴⁴⁴.

Amacın belli olması yasal bir zorunluluk ya da yetkiye dayanması halinde de önemlidir. Bu tür bir zorunluluk ya da yetkinin kullanılması açısından bu zorunluluk

⁴⁴¹ OECD ilkeleri açıklayıcı raporunda keyfi olarak yeni amaçlar için kullanılamayacağı ve yapılacak değişikliğin orijinal amaçla uygunluk göstermesi gerektiği dile getirilmektedir. Bkz. Açıklayıcı rapor <http://www1.oecd.org/publications/e-book/9302011E.PDF> s.41-42.

⁴⁴² Sözleşmenin bu maddesi, kişisel verilerin toplanma amaçlarının ne olacağı bakımından bir tanım yapılmamıştır; bu ifade ile önceden belirlenmemiş ya da açıklanmamış amaçlar için kişisel verilerin toplanmasına sınır getirilmesi amaçlanmıştır. Bkz. **MICHAEL**, s. 38

⁴⁴³ Bkz., *The Privacy Principles of the Information Infrastructure Task Force*, aktaran **CATE**, s. 189 vd.

⁴⁴⁴ **LLOYD**, s. 130.

ya da yetkinin öngördüğü amaç dışında kişisel verinin toplanması ve işlenmesi kural olarak mümkün değildir.

Genel kural, kişisel verilerin toplanma anında belli olan amaç ya da amaçlar dışında, yasal bir yetki veya zorunluluğun ya da kişinin rızasının olmadan işlenmemesidir⁴⁴⁵. Toplama ve işleme amacı dışında, kişisel verilerin bilimsel ve istatistikî⁴⁴⁶ ve tarihsel amaçlar için işlenmesine izin verilmekte ve bu durum amaç dışı işleme sayılmamaktadır⁴⁴⁷.

Özetle, amaçla bağlılık kişisel verilerin çok işlevli kullanılmasını sınırlandırma⁴⁴⁸ ve kişisel verilerin işlenmesinde keyfiliğin önlenmesi amacıyla getirilmiş bir ilkedir. Kişisel verilerin toplanma miktarının (asgarilik ilkesi)⁴⁴⁹ ve somut bir durumda kişisel verinin meşru işleme sınırlarının tayini (kullanımının sınırlandırılması ilkesi)⁴⁵⁰; toplanan kişisel verinin niteliği (doğru, tam ve işlenme amacı ile ilgili olması)⁴⁵¹ bakımından merkezi bir konuma sahiptir. Ayrıca, kişisel

⁴⁴⁵ Bkz., OECD ilkeleri, 10. m.

⁴⁴⁶ *Dreyfuss ve Leebon* kişilere ilişkin bilgilerin kişilerin kimliği ile bağlantı kurulabilmesi imkanının özel hayatın gizliliğinin ihlali bakımından belirleyici olduğunu ve belirtilen bu bağlantının kurulabilmesinin önlenmesinin ise özel hayatın gizliliğinin korunması bakımından önemli olduğunu vurgulamaktadırlar. Yazarlar devamında aktarılan bu nedenden dolayı istatistiksel amaçlarla kişisel verilerin kişinin kim olduğuna ilişkin bağlantı kurulmadan toplanmasının özel hayatın gizliliğinin ihlali olarak kabul edilmediğini belirtmektedirler. Bkz., **DREYFUSS – LEEBRON, Privacy and Information Technology**, s.498, 12. dipnot; Aynı yönde, *Erem* de bilişim sistemleri aracılığıyla kişisel verilerin toplanmasının sır dokunulmazlığının daralmasına yol açacağını, bu alanda özel hayata saygıya dikkat edilmesi gerektiğini ve bu nedenlerle toplamanın saklamanın ve açıklamanın bazı hukuki sorunları getireceği bu açıdan koruyucu tedbirleri gerektireceğini ve devamında kişiye bağlı tutulmayan bilgilerde bu sorunun oluşmadığını belirtmektedir. Faruk **EREM**, “*Kamu Hukuku Açısından Siberetik*”, AÜHF Dergisi, C. XXXI, Sayı 1-4, 1974, s. 5-6.

⁴⁴⁷ Bkz., Yönerge 6/1 (b) m., İtalyan Veri Koruma Kanunu 97. m. vd.

⁴⁴⁸ **SPIROS**, a.g.e., 740.

⁴⁴⁹ OECD 9. m., Sözleşme 5/c m., Yönerge 6/1 (c) m.

⁴⁵⁰ OECD 9. m. Sözleşme 5/b Yönerge 6/1 (b) maddeleri;

⁴⁵¹ OECD 8. m., Sözleşme 5/c m., 5/d m., Yönerge 6/1 (c), (d) maddeleri

verilerin amacın gerçekleştirilmesi sonunda imha edilmesi ya da anonim haline getirilmesi yükümlülüğü⁴⁵² bakımından da amaca bağlılık ilkesi önemlidir⁴⁵³.

D. Kişisel Verilerin Korunmasına İlişkin Suçlar Bakımından Kişisel Veri

TCK'nin 135 vd. maddelerinde düzenlenen suçlar bakımından kişisel veri tanımı yapılmamıştır. Sözleşmenin 2/(a) maddesinde ise kişisel veri, *“kim olduğu belirli olan ya kim olduğu tespit edilebilen bireylerle ilgili enformasyon”* olarak tanımlanmaktadır⁴⁵⁴. Yönergenin 2/(a) maddesine 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*

⁴⁵² Sözleşme 5/e, Yönerge 6/1 (e) maddeleri; Anonim hale getirme verinin, içerdiği enformasyon ya da bilgi kullanılarak kişinin tespit ya da teşhis edilememesi, kişinin kim olduğunun anlaşılamamasını sağlamaya yönelik işlemlerin yapılmasını kapsamaktadır. Bu husus kişisel verilerin korunmasına ilişkin düzenlemelerde bir adım daha ilerletilerek sadece kullanım sonrası değil kullanım sırasında da zorunlu değilse verinin anonim haline getirilmesinin gerektiği şeklinde de karşımıza çıkmaktadır. Bu konu hakkında genel olarak bkz., Ian **WALDEN**, *Anonymising Personal Data*, International Journal of Law and Information Technology, Vol. 10, No.2, s. 224 vd.

⁴⁵³ Adı geçen ilkeler hakkında bkz, Bkz., Olga **ESTADELLA YUSTE**, Report: *The Relevance of the Data Protection Principles Set Out in the Convention 108 and Its Additional Protocol*, European Conference on Data Protection on Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Present and Future, Warsaw 2001, s. 42-44 [http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Events/Conf\(Warsaw2001\)ProceedingsE.pdf](http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Events/Conf(Warsaw2001)ProceedingsE.pdf) (kontrol tarihi 15.04.05); **BENNET**, s. 103-108.

⁴⁵⁴ Sözleşmenin Türkçe resmi çevirisinde kişisel veri *“Kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder”* şeklindedir. Bkz., **“Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme”** <http://www.uhdigm.adalet.gov.tr/kisiverkorun.htm>

faktörlere bağılı olarak doğrudan ya da dolaylı olarak tespit edilen veya edilebilen kişi” şeklinde tanımlanmıştır. Kişisel verilerin bu şekildeki geniş tanımları, kişi hakkında herhangi bir bilgi ve enformasyon yanında, kişiyle ilgili ses ve görüntüleri de kapsamaktadır⁴⁵⁵.

135. maddenin gerekçesinde ise kişisel veri, “*gerçek kişiyle ilgili her türlü bilgi*” olarak tanımlanmaktadır⁴⁵⁶. Gerekçenin devamında, “*Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış veriş yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında*

⁴⁵⁵ Bkz., **Douwe KORFF**, EC Study on Implementation of Data Protection Directive: comparative summary of national laws, s. 15 vd. http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

Bu açıdan isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim ve ses, parmak izleri, genetik bilgileri gibi veya dolaylı olarak da kişiyi belirlenebilir kılan kriterlerin kombinasyonu (yaş, meslek, medeni durum, adres, vb.) olan veriler de kişisel verilerdir. Aktaran, **BAŞALP**, s. 33-34; Aynı yönde **DÜLGER**, s. 270.

⁴⁵⁶ Buna karşın halen Başbakanlıkta bulunan “Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı”nın 3. maddesinin a bendinde kişisel veri “belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler” olarak tanımlanmaktadır. Bu açıdan kişisel veri tanımının gerekçede belirtildiği şekliyle sadece gerçek kişiler hakkında bilgi olarak sınırlandırma yapılmamış tüzel kişiler hakkındaki her türlü bilgi de kişisel veri kapsamına alınmıştır. Tasarıdaki bu geniş aslında kişisel verilerin korunmasına ilişkin kanunların uygulanma alanı bakımından ortaya sadece gerçek kişiler hakkındaki verilerin kişisel verilerin korunmasına ilişkin kanunun kapsamında olması ya da gerçek veya tüzel kişiler arasında bir ayırıma gidilmeksizin bunlar hakkındaki verilerin kanunun kapsamında olmasına ilişkin iki yaklaşım içerisinde bir tercihi ifade ettiği söylenebilir. Nitekim Almanya’da kişisel verilerin korunmasına ilişkin kanunun uygulama alanı sadece gerçek kişiler hakkındaki verileri kapsamakta iken İtalya’da kişisel verilerin korunmasına ilişkin kanun uygulama alanı hem gerçek hem de tüzel kişiler hakkındaki verileri kapsamaktadır. “*Kişisel Verilerin Korunması Kanunu Tasarısı*” için bkz., <http://www.kgm.adalet.gov.tr/kisiselveriler.htm>

Almanya, İtalya, Fransa ve diğer ülkelerin kişisel verilerin kapsamı hakkında bkz., http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/NATIONALLAWS-EN.asp#TopOfPage

kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler.” ifadesine yer verilmiştir⁴⁵⁷.

Gerekçe incelendiğinde, kişiyle ilgili kayda geçirilmiş bilgi ve enformasyonun kişisel veri kapsamında değerlendirildiği⁴⁵⁸, kişiyle ilgili ses ve görüntülerin kişisel veri kapsamında değerlendirilmediği sonucuna varılabilmesi mümkündür. Bu açıdan gerekçede yer alan tanım Sözleşme ve Yönergede yer alan kişisel veri tanımı ve kapsamına göre dar bir anlam taşımaktadır.

E. Kişisel Verilerin Kaydedilmesi Suçu

1. Genel Olarak

TCK'nin kişisel verilerin korunmasına ilişkin ilk suç kişisel verilerin hukuka aykırı olarak kaydedilmesi suçudur. TCK'nin kişisel verilerin hukuka aykırı olarak kaydedilmesine ilişkin olarak 135. maddesinde “(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.” hükmüne yer verilmiştir.

⁴⁵⁷ Gerekçe için bkz, GÜNEY, , s. 415.

⁴⁵⁸ Aynı yönde SOYASLAN, s. 273.

Türk Ceza Kanunu Tasarıda bu suç “*kanuna aykırı olarak kişisel verileri toplamak*” başlığı altında 193. maddede düzenlenmişti. TCK’nin 135. maddesinde ise Tasarının 197. maddesinin birinci fıkrasında yer alan “*Rızaları olmaksızın veya kanunların öngördüğü şekil ve usullere uyulmaksızın kişisel verileri bilişim sistemlerine yerleştiren veya işleyen kimseye altı aydan üç yıla kadar hapis cezası verilir.*” son fıkrasında yer alan “*3. Kanunun öngördüğü hâller dışında, kişilerin âhlakî niteliklerini, siyasal, felsefî veya dinsel görüşlerin, veya ırkî kökenlerini veya sendikal bağlantılarını veya cinsel yaşamlarını veya sağlık durumlarını kişisel veri olarak sisteme yerleştiren veya işleyen kimseye bir yıldan iki yıla kadar hapis cezası verilir*” hükümleri esas alınarak kişisel verilerin hukuka aykırı kaydetme suçu düzenlenmişti⁴⁵⁹.

Türk Ceza Kanunu Tasarının birinci fıkrası incelendiğinde, suçun maddi unsurunun seçimlik hareketli bir suç olarak düzenlenmek istendiği görülmektedir. Kişisel verinin kaydedilmesi yanında kişisel verinin işlenmesine de Tasarının 197. maddesinin birinci fıkrasında yer verilmek istenmiştir. Bu haliyle Tasarıda, kişisel verilerin işlenmesine ilişkin ilkeler kapsamında hem kişisel verinin hukuka aykırı olarak toplanması hem de bütün süreci kapsayan kişisel verinin hukuka aykırı olarak

⁴⁵⁹ Tasarının 193. maddesinin tam metni şu şekildedir. “Madde 197: “*Rızaları olmaksızın veya kanunların öngördüğü şekil ve usullere uyulmaksızın kişisel verileri bilişim sistemlerine yerleştiren veya işleyen kimseye altı aydan üç yıla kadar hapis cezası verilir... Veriler, hileli veya kanun dışı yollarla elde edildiğinde verilecek ceza üçte biri oranında arttırılır... 2. Kanuna uygun olarak bilişim sistemlerine yerleştirilmek veya işlenmekle beraber muhafazaları için gerekli güvenlik tedbirlerinin alınmaması nedeni ile kişisel verilerin başkalarının ellerine geçmesine veya bozulmasına veya zarar görmesine neden olan kimse hakkında bir yıldan dört yıla kadar hapis cezası verilir... Fiil taksirle işlendiğinde ellimilyon liradan ikiyüzmilyon liraya kadar ağır para cezası verilir. 3. Kanunun öngördüğü hâller dışında, kişilerin âhlakî niteliklerini, siyasal, felsefî veya dinsel görüşlerin, veya ırkî kökenlerini veya sendikal bağlantılarını veya cinsel yaşamlarını veya sağlık durumlarını kişisel veri olarak sisteme yerleştiren veya işleyen kimseye bir yıldan iki yıla kadar hapis cezası verilir.*”

işlenmesi suç haline getirilmek istenmekteydi.. TCK'nin 135. maddesinde ise kişisel verinin işlenmesine ilişkin ilkeler kapsamında yukarıda aktarılan dürüst ve hukuka uygun toplama ve işleme ilkesi içerisinde, kişisel verinin toplanmasının, esas alındığı görülmektedir.

2. Dürüst ve Hukuka Uygun Toplama – Amaçla Bağlılık İlkesi Karşısında Kişisel Verinin Hukuka Aykırı Olarak Kaydedilmesi

135. maddede düzenlenen suçun maddi unsuru, kişisel verilerin kaydedilmesidir. Kanunda kaydetmenin ne anlama geldiğine ilişkin bir tanıma yer verilmemiştir. TDK sözlüğüne göre “*kaydetme*” genel olarak yazmak, bazı önemli noktaları tespit etmek; herhangi bir şeyi bir yere mal etmek, bir şeyin tarih, numara veya adını bir deftere geçirmek; hatırlamak için yazmak, not etmek; sesi veya resmi manyetik bant üzerine geçirmek; bilişim açısından ise, elektronik veya sayısal araçlarda bilgiyi korumaya almak anlamlarını taşımaktadır. Öntasarının ve TCK Tasarısının 193. ve 197. maddelerinde ise, kişisel verilerin bilişim sistemine yerleştirilmesi veya işlenmesi suç olarak düzenlenmek istenmişti. Aynı şekilde Öntasarının 195., TCK Tasarısının 199. maddelerinde ise bu suçun her türlü fişliklere yerleştirilmiş kişisel veriler hakkında da işleneceği hükme bağlanmıştı. Tasarının gerekçesinde ise fişlik ile ilgili olarak, otomatik olmayan her türlü yöntemle yani elle veya daktilo ile yazılmış fişlerin bu hususa tahsis edilmiş dolaplara yerleştirilmesi ve işlenmesi halinde de bu suçun oluşabileceği belirtilmişti.

Öntasarının ve Tasarının gerekçelerinde, bu suçlarla Sözleşmenin ilgili maddelerine işlerlik kazandırılmak istendiği belirtilmiştir. Nitekim Sözleşmenin

“uygulama alanı” başlıklı 3. maddesinin 1. fıkrasında “*Taraf Devletler, bu Sözleşmeyi Kamu ve Özel Sektörde, kişisel nitelikteki verilerin otomatik işleme tabi tutulması konusunda ve otomatik fişiyeler hakkında uygulamayı taahhüt ederler*” hükmüne yer verilmiş 3. maddenin 2 fıkrasının (c) bendinde ise devletin istemesi halinde sözleşmeyi otomatik işlemeye tabi olmayan fişliklere de uygulayabileceği ifade edilmiştir⁴⁶⁰. Sözleşmenin 2. maddesinde “*otomatik fişiye*”, “*otomatik işleme konu teşkil eden verilerin tümü olarak tanımlanırken*”, “*otomatik işlem*” ya da kullandığımız ifade ile “*otomatik işleme*”, “*tamamı veya bir kısmı otomatik yöntemlerle gerçekleştirilen verilerin kaydı, bu verilere biyolojik ve/veya aritmetik*

⁴⁶⁰ Sözleşmenin uygulanma alanının bu şekilde belirlenmesinin nedeni, yukarıda ayrıntılı olarak açıklanan bilişim sistemleri ve özellikle bilgisayarların kişisel veri işleme faaliyetlerinde yoğun olarak kullanılmasında yatmaktadır. Yukarıda aktardığımız üzere gözetimin bilgisayarlar aracılığıyla yapılmaya başlanması, bilgisayarların üstün işleme ve saklama kapasiteleri sayesinde önceki dönemlerde önemsiz olarak görülen kişisel verilerin toplanması, saklanması gibi faaliyetleri, temel hak ve hürriyetleri ve özellikle özel hayatın gizliliğini tehdit eden boyutlara ulaştırmıştır. Bunun sonucu olarak da Sözleşme ve diğer düzenlemelerin öncelikli hedefi, otomatik işleme yoluyla, daha genel bir ifade ile bilgisayarlar aracılığıyla kişisel verilerin toplanması ve işlenmesi olmuştur.

Nitekim Yönergenin girişinin 15. paragrafında kişisel verilerin işlenmesine ilişkin olarak sadece otomatik işleme ya da belirli bir sorgulama esasına dayanarak kişiye ait verilere hızlı erişimin sağlandığı dosyalama sistemleri aracılığıyla işlenmesi bu sistemlerde bulundurulması ya da dosyalama sistemlerinde bulundurma niyetinin olması hallerini Yönergenin kapsadığı belirtilmektedir. Buna paralel olarak Yönergenin kapsam başlıklı 3. maddesinde Yönergenin kişisel verilerin tamamen veya kısmen otomatik olarak işlenmesi ve ayrıca otomatik işleme dışında bir dosyalama sisteminin parçası ya da bunun parçasını oluşturması niyetiyle işlenmesi hallerinde uygulanabileceği belirtilmiştir. Yönerge hakkında bkz., **BAŞALP**, s. 32 – 33

Kişisel Verilerin Korunması Hakkında Kanun Tasarısı’nın 3. maddesinin “c” bendinde kişisel verilerin işlenmesi, “*Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem ya da işlemler bütünü,*” olarak tanımlanmakta ve her türlü işleme şekli Kanunun uygulanma alanına sokulmak istenmektedir.

*işlemlerin uygulanışı, verilerin değiştirilmesi, silinmesi, çıkarılması veya dağıtılması” olarak tanımlanmıştır*⁴⁶¹.

Aktarılan bu hususlar doğrultusunda Sözleşmede asıl olarak “*otomatik fişiye*” ve kişisel verilerin otomatik işlenmesi düzenlenmiş olup otomatik olarak işlenmeyen kişisel veri dosyaları ile ilgili olarak Sözleşme hükümlerinin uygulanması taraf devletlerin ihtiyarındadır. “*Otomatik fişiye ve otomatik işleme*” Öntasarı ve Tasarıda bilişim sistemine yerleştirme ve işleme, otomatik olmayan kişisel veri dosyaları ise fişlik olarak yer almıştır. Bu açıdan hem otomatik hem de fişliklerle ilgili olarak kaydetme ve işleme fiilleri, Öntasarı ve Tasarıda düzenlenen bu suç kapsamındadır. Bu açıdan Öntasarıda ve Tasarıda yer alan suçun herhangi bir şekilde kayıt ya da işleme yerine bilişim sistemine ve fişliklere kaydetme ve bilişim sistemleri ile veya fişliklere bağlı olarak işleme şeklinde gerçekleşebileceği sonucuna varmak mümkündür.

Öntasarı ve Tasarıda yer alan bu düzenleme, TBMM Adalet Komisyonu çalışmaları sırasında değiştirilmiş ve TCK’nin 135. maddesinde kişisel verilerin bilişim sistemine veya Tasarıdaki ifadeyle fişliğe yerleştirilmesi unsurlarına yer verilmemiştir. Adalet Komisyonunda kişisel verilerin kaydedilmesi suçunda yapılan değişiklikle ilgili olarak gerekçesinde, bu suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmediği belirtilmektedir⁴⁶². Madde metni incelendiğinde de sadece kişisel verinin kaydından bahsedilmekte fakat Tasarıdaki gibi bilişim sistemine yerleştirme şeklinde bir unsura

⁴⁶¹ Sözleşmenin resmi Türkçe çevirisinde veri (data) bilgi, otomatik işleme (automatic processing) ise Sözleşmenin 2.maddesinde otomatik işlem 3. maddesinin 2. fıkrasının (c) bendinde ise bilgi işlem olarak çevrilmiştir.

⁴⁶² Maddenin gerekçesi içi bkz., GÜNEY, s. 415.

yer verilmediği görülmektedir. Bu açıdan söz konusu madde uyarınca kişisel verinin, bilişim sistemine ya da bir dosyalama sistemine ya da Tasarıdaki ifadeyle fişliğe bağlı olmadan herhangi bir şekilde kaydı veya bilişim sistemine kaydı arasında fark yoktur; kişisel verinin kaydı bir bilişim sistemine veri olarak kaydedilmesi, yazılı hale getirilmesi ya da diğer şekillerde kaydı suretiyle olabilecektir⁴⁶³.

Genel olarak her türlü kişisel verinin hukuka aykırı olarak kaydı, 135. maddede düzenlenen suç oluşturur. Bunun yanında 135. maddenin ikinci fıkrasında ikili bir ayırıma gidilmiş “*kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine*”, “*hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına*” ilişkin bilgilerin kişisel veri olarak kaydedilmesi durumunda 135. maddenin birinci fıkrasına göre cezalandırılacağı belirtilmiştir⁴⁶⁴.

Bu düzenleme, Tasarının 197. maddesinin 3. fıkrasında yer almakla birlikte, Tasarının 197. maddesinin 1. fıkrasında kişilerin rızası olmaksızın veya kanunların öngördüğü şekil ve usullere uyulmaksızın kişisel verilerin kaydedilmesi ya da

⁴⁶³ Aynı yönde bkz., **DÜLGER**, s. 271.

⁴⁶⁴ Kişisel verilerin işlenmesine ilişkin ulusal ve uluslar arası düzenlenmeler incelendiğinde kişisel verilerin işlenmesine ilişkin usul ve esaslar gösterilmekte, bu açıdan genel olarak kişisel verilerin işlenmesinde ilgili verilerin niteliği bakımından kural olarak bir ayırım yapılmamaktadır. Hassas veriler olarak adlandırılan veriler ise kuralın istisnası olarak karşımıza çıkmaktadır. Nitekim Sözleşmenin 6. maddesinde, özel kategorideki veriler başlığı altında, kişilerin etnik kökenlerini, politik görüşlerini ya da dini ya da diğer inançlarını ortaya çıkaran kişisel verilerin ve aynı zamanda sağlık ve cinsel yaşamlarına ilişkin verilerin iç hukukta ek güvenceler sağlanmadığı sürece otomatik olarak işlenmeyebileceği düzenlenmiştir. Maddeye göre kişilerin ceza mahkumiyetlerine ilişkin verilere de aynı hüküm uygulanacaktır.

Hassas veriler olarak adlandırılan bu tür verilerin işlenmesi Yönergenin 8. maddesinde yer almış ve birinci fıkraya göre maddede gösterilen istisnai durumlar dışında bu tür verilerin işlenmesi kural olarak yasaklanmıştır. Yönerge hakkında bkz., **BAŞALP**, s. 42 vd.

işlenmesi düzenlenmişti⁴⁶⁵. İlgili 3. fıkra ise kanunun öngördüğü haller dışında söz konusu verilerin kaydedilmesi ya da işlenmesi şeklinde düzenlenmişti. Özellikle TCK'nin 26. maddesinde düzenlenen ilgilinin rızasına ilişkin *“kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere”* rızanın geçerli olabileceğine ilişkin hüküm bakımından, Tasarının 197. maddesinde özellikle 3. fıkra düzenlen fiiller bakımından ilgilinin rızasının geçerli olmadığını ifade edebilmesi bakımından bir anlama sahip olabildi.

135. maddede ise bu yönde bir düzenlemeye yer verilmemiştir. Madde gerekçesinden, kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine ilişkin veriler bakımından mutlak bir yasak getirilmek istendiği anlaşılmaktadır⁴⁶⁶. İkinci fıkra düzenlen diğer hususlar bakımından ise gerekçede *“Ancak, bunlardan kişilerin ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kayda alınmasına kanunlarda özellikle suçlulukla mücadele bağlamında, suç ve suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde izin verilebilir. Bu durumlarda söz konusu suç oluşmayacaktır.”* ifadesine yer verildiği görülmektedir. Fıkranın düzenleniş biçiminden 135. maddesinin 2. fıkrasında yer verilen *“hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına”* ilişkin

⁴⁶⁵ Maddenin Fransız Ceza Kanunda bu yönde bir hüküm bulunmakla birlikte söz konusu atfın Kişisel Verilerin Korunmasına ilişkin Kanuna yapıldığının söylemek mümkündür. Kişisel verilerin korunmasına ilişkin suçlar Fransız Ceza Kanunun 226-16 vd. maddelerinde düzenlenmiştir. İngilizce çevirisi için bkz., http://www.legifrance.gouv.fr/html/codes/traduits/code_penal/textan.htm. Kişisel Verilerin Korunmasına ilişkin kanun 50. maddesinde bu husus açıkça belirtilmektedir. İngilizce çevirisi için bkz, **Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties**

<http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf> .

⁴⁶⁶ Aynı yönde, **DEĞİRMENCİ, Bilişim Suçları**, s. 202.

bilgilerin kişisel veri olarak kaydedilmesi durumunda kanun koyucunun birinci fıkradaki genel kurala döndüğü görülmektedir

Aslında burada sorun, maddenin kaynağını oluşturan Fransız Ceza Kanununda yer alan kişisel verilerin korunmasına ilişkin suçların eksik norm⁴⁶⁷ olarak düzenlenmesi ve özellikle kişisel verilerin korunmasına ilişkin kanunun varlığı karşısında, söz konusu kanunda gösterilen usul ve esaslara uyulmamasının müeyyide altına alınmasından dolayı ortaya çıkmıştır.

TCK'nin 135. maddesinde düzenlenen suç bakımından ise Fransız hukukunda olduğu şekliyle eksik norm olarak bağlantı kurulabilecek kişisel verilerin korunmasına ilişkin genel bir düzenleme bulunmamaktadır. Bu nedenle maddede yer alan hukuka aykırı olarak kaydetmenin yorumlanması gerekmektedir. Maddede gösterildiği şekliyle hukuka aykırılık, kimi yazarlarca hukuka özel aykırılık halini oluşturmaktadır⁴⁶⁸. Buna karşın bu tür bir hükmün özel hukuka uygunluk nedenlerine işaret ettiği kimi yazarlarca ifade edilmektedir⁴⁶⁹.

⁴⁶⁷ Eksik norm hakkında bkz, Zeki **HAFIZOĞULLARI**, Ceza Normu, Normatif Bir Yapı Olarak Ceza Hukuku Düzeni, 2. B., Ankara, 1996, s. 280.

⁴⁶⁸ *Dönmezer - Erman*, Ceza Kanununun bazı maddelerinde hukuka aykırılık unsurunun ayrıca gösterilmesinin sebepsiz olamayacağını, hukuka aykırılığın manevi unsur yani kusurluluğun kapsamına alındığını, bu durumlarda failin maddede belirtilen şekilde hareket ettiğini bilmesinin ve hareket etmeyi istemesinin de aranmış olduğunu ifade etmektedir. Yazara göre, özel hukuka aykırılık hallerinde hakim – diğer bütün suçlarda olduğu gibi – hukuka aykırılığın varlığını aramakla yetinmeyecek, ayrıca failin bu özel aykırılığı bilip bilmediğini ve böylece hareket etmeyi isteyip istemediğini, kusurluluğun bunu da kapsayıp kapsamadığını araştıracaktır, ve bu işte bu bakımdandır ki, hukuka özel aykırılık konusu önemli olacaktır. Sulhi **DÖNMEZER** – Sahir **ERMAN**, Nazari ve Tatbiki Ceza Hukuku, Genel Kısım, C. 2, 10 B., İstanbul, 1994. s. 20. Aynı yönde, Kayıhan **İÇEL** – İzzet **ÖZGENÇ** – Adem **SÖZÜER** – Fatih S. **MAHMUTOĞLU** – Yener **ÜNVER**, Suç Teorisi, İstanbul, 1999, s. 118; Timur **DEMİRBAŞ**, Ceza Hukuku Genel Hükümler, 3. B., Ankara, 2005, s. 239; Nur **CENTEL** – Hamide **ZAFER** – Özlem **ÇAKMUT**, Türk Ceza Hukukuna Giriş, 3. B., İstanbul, 2005, s. 298.

Hukuka özel aykırılık hakkında ileri sürülen çeşitli görüşler için bkz., Tuğrul **KATOĞLU**, Ceza Hukukunda Hukuka Aykırılık, Ankara, 2003, s. 122 vd. Yazar, hukuka özel aykırılık olarak adlandırılan durumların tümünün, mahiyet itibarıyla aynı olmadığını

Maddenin yorumunda ve uygulanmasında 1. fıkra da yer alan hüküm ve 2. fıkra da düzenlenen, hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kişisel veri olarak kaydedilmesi hükmü bakımından, hukuka özel aykırılığın var olduğu kabul edilecek olursa, sorun manevi unsur içerisinde çözümlenecek; özel hukuka uygunluk nedeni olduğu kabul edilirse hukuka uygunluk nedenlerine ilişkin genel kurallar burada da geçerli olacaktır. 2. fıkra da düzenlenen diğer hususlar bakımından ise, hali hazırda, sadece TCK'nin 24. vd. maddelerinde düzenlenen genel hukuka uygunluk nedenlerinin geçerli olduğu sonucuna varmak mümkündür.

Hukuka uygunluk sebepleri açısından, yukarıda kısaca “*amaca uygun davranma*” ve “*yanıltılmama*” olarak ifade ettiğimiz dürüstlük kuralı ise rızaya bağlı olarak kişisel veri kaydında hangi tür kişisel verinin kaydedildiği ve kayıt amaç ya da amaçları ile ilgili olarak kişinin yanıltılmaması anlamına gelmektedir.⁴⁷⁰ Diğer hukuka uygunluk nedenlerinde ise dürüstlük kuralı, öngörülen amaç doğrultusunda bu amaca uygun ve yeterli miktarda kişisel verinin kaydedilmesi; amaca uygun olmayan ya da amacın gerçekleşmesine elverişli olmayan kişisel verinin kaydedilmemesi, özetle keyfi davranmama olarak karşımıza çıkmaktadır.

belirtmekte, ve yerine göre özel kast, özel hukuka uygunluk nedeni, ya da fiilin özel bir biçimi, olarak ortaya çıkan bu özel durumların tek bir başlık altında toplanmasının farklı görüşlerin ortaya çıkmasına neden olduğunu belirtmektedir. Bu nedenle yazara göre, bu tür özel durumların her birinin farklı doğalarına göre incelenmesi gerekli olup, hukuka genel aykırılık ve hukuka özel aykırılık ayrımının kabul edilebilir bir ayırım olduğunu söylemek güçtür. a.g.e., 125 – 126.

⁴⁶⁹ Zeki **HAFIZOĞULLARI**, Ceza Hukuku Genel Hükümler, s. 208 <http://www.baskent.edu.tr/~zekih/uygulamaci/ucezagenel.htm> (kontrol tarihi 15.07.2006)

⁴⁷⁰ Nitekim geçerli bir rızadan bahsedilebilmesi için, hukukun genel ilkeleri gereği rızaya ilişkin irade şiddet, hata hile gibi iradeyi bozan nedenlerle sakatlanmamış olmalıdır. Bkz., **TOROSLU**, **Ceza Hukuku, Genel Kısım**, s. 167; Aynı yönde, Timur **DEMİRBAŞ**, Ceza Hukuku Genel Hükümler, Seçkin Yayınevi, 2. B., Ankara 2005, s.247.

135. maddede, sadece kişisel verilerin hukuka aykırı olarak kaydedilmesi suçuna yer verilmiştir. Bu haliyle Öntasarı ve Tasarıda yer alan seçimlik hareketlerden, kişisel verilerin korunmasına ilişkin bütün süreci kapsayan bir ilke olarak ifade edilebilen kişisel verilerin işlenmesi, madde metninden çıkar. Bu durumda sorun hukuka uygun bir şekilde toplanan kişisel verinin hukuka aykırı bir amaç için kullanılmasının 135. maddedeki suçu oluşturup oluşturamayacağı noktasında toplanmaktadır. Daha da somutlaştırılacak olursa sorun, belirli bir amaç doğrultusunda işlenmek için ilgili kişinin bu amaç doğrultusunda gösterdiği rızasıyla toplanan verinin bu amaçlar dışında kullanılması durumunda bu kullanımın 135. madde kapsamında olup olmadığıdır. Bu ise genel olarak kişisel verilerin işlenmesine ilişkin ilkeler arasında yer alan ve amaçla bağlılık olarak yukarıda ifade edilen ilkenin suç olarak düzenlenip düzenlenmediğinin belirlenmesi anlamına gelmektedir.

İster ilgili kişinin rızasına, ister kanunun verdiği yetkiye ya da diğer hukuka uygunluk sebebine dayanılarak kişisel verilerin toplanmasında, toplanma anındaki amacın belirlenmesi önem arz etmektedir. Bu açıdan, ilgili kişinin rızası dışında ya da rıza gösterdiği amaç dışında kişisel verilerin toplanması ya da yetkinin kaynağı olan kanunda öngörülen amaç dışında kişisel verilerin 135. maddede düzenlenen suçu oluşturur. Fakat hukuka uygun olarak toplanmış kişisel verinin, öngörülen amaç yanında diğer amaç ya da amaçlar için işlenmesi durumunda ise, maddeden hukuka aykırı işlemenin çıkarılması karşısında, aynı şeyi söylemek mümkün değildir.

Bu durumda yukarıda veri işleyenin sorumluluk ve yükümlülükleri başlığı altında incelenen amaçla bağlılık ilkesinin, meşru amaç dışında meşru olamayan

ikincil bir amaç işlemeyi sınırlandırmaya yönelik işlevi 135. maddede dikkate alınmamıştır⁴⁷¹.

Özetle kişisel verilerin kaydedilmesi suçunda toplanma anında hukuka uygun olması yeterli olup bu haliyle bu suç, hukuka uygun toplama sonrasında kişisel verinin toplanma amacı dışında kullanımının engellenmesi amacına hizmet etmemektedir. Bu açıdan maddenin *“bu tür bilgilerin amacı dışında kullanılmasından... dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler”⁴⁷²* yönündeki gerekçesi kişisel verilerin işlenmesine ilişkin bir gerçeği yansıtmakla birlikte, 135. maddede düzenlenen suç ile örtüşmemektedir.

Son olarak değinilmesi gereken bir husus da, veri ile ilgili kişi arasındaki bağlantının ortadan kaldırılması suretiyle kaydedilmesi durumunda, kişisel verinin kaydı suçundan bahsedilemeyeceğidir. Kişisel verilerin anonim hale getirilmesi ya da anonim olarak kaydı olarak adlandırılan bu gibi durumlarda doğrudan ya da dolaylı olarak veri ile ilgili arasında bağlantı kurulamaması gerekir. Aynı şekilde, alenileşmiş olup genel olarak erişilebilir bir kişisel verinin kaydedilmesinin suç oluşturmayacağını söylemek mümkündür. Kişisel verilerin amacının özel hayatın gizliliğinin korunması olduğunda bu tür durumlarda, hukuka uygun bir şekilde alenileşen kişisel veriye ilişkin, ilgili kişinin gizli kalması konusunda makul bir beklentisinin varlığından bahsedilemeyecektir. Burada sorun kişisel verinin diğer verilerle birleştirilerek işlenmesinde çıkmaktadır.

⁴⁷¹ “*Kişisel Verilerin Korunması Hakkında Kanun Tasarısı*”nın 50. maddesinde ise, hukuka aykırı olarak kişisel verilerin işlenmesinin TCK’nin 135. maddesine göre cezalandırılacağı öngörülmektedir.

⁴⁷² Bkz. TCK madde gerekçeleri, <http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerkekce.doc>

F. Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme

Kişisel verilerin korunmasına ilişkin TCK'nin 136. maddesinde yer alan diğer bir suç *“Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.”* şeklindedir.

Söz konusu suçun da Tasarıdan çeşitli değişikliklerle yapılmak suretiyle TCK'ye aktarıldığı görülmektedir. Tasarının 198. maddesinin 1. fıkrasında, *“Kişisel verileri yetkisiz kişilere veren, ifşa eden, çeşitli özel maksatlarla kullanan ile ele geçirenle iki yıldan beş yıla kadar hapis cezası verilir”* şeklinde bir suça yer verilmek istenmişti.

Maddede kişinin kendisi hakkındaki verileri kontrol edebilmesi bakımından, ilgili kişi hakkındaki verinin, sadece rıza gösterdiği ya da hukuken kişisel veri işlemeye yetkili kişilerin elinde bulunması ve yetkisiz üçüncü kişilerin eline geçmesinin önlenmesi için kişisel verinin başkasına verilmesi, yayılması ve ele geçirilmesi şeklinde seçimlik hareketli bir suç olarak düzenlenmiştir. TCK'nin 136. maddesinde düzenlenen suç, genel olarak hangi tür verilerin, kimler tarafından ne şekilde kaydedilebileceğine ilişkin bir koruma sağlarken, bu maddede düzenlenen suç, kişisel verinin yetkisiz üçüncü kişilerin eline geçmesinin önlenmesi ya da kişisel verinin içeriğinin genel olarak öğrenilmesinin engellenmesi açısından, kişisel verilerin işlenmesi süreci içerisinde, kişi bakımından bir koruma getirmektedir. Aynı şekilde, kişisel verilerin korunması genel olarak kişinin kendisi hakkındaki verileri kontrol hakkı olarak tanımlandığında, ilgili kişinin kendisi ile ilgili verileri kimlerin

işlediğini bilebilmesi veya öngörebilmesi bakımından 136. maddede düzenlenen suç önem taşımaktadır.

Maddede yer alan seçimlik hareketlerden, kişisel verinin başkasına verilmesi ve yayılması, bir yönüyle kişisel veri işlemeye yetkili olan kişilere yönelik verinin işlenmesine ilişkin bir iç sınırı oluşturmaktadır. Kişisel veri işlemeye yetkisi olan kişilerin hukuka uygun olarak kişisel verileri kaydetmesi halinde de söz konusu veriler üzerindeki tasarrufu, verinin üçüncü kişilere verilmesi ya da verilerin içeriğinin birçok kişi tarafından öğrenebilecek şekilde başkalarının bilgisine sunması⁴⁷³ yani yayması bakımından sınırlandırılmaktadır. Bu haliyle, kişisel verilerin kullanımının sınırlandırılması ve istenmeyen ya da yetkili olmayan ifşalardan korunması istenmektedir.

Maddede düzenlenen suçun maddi unsurunu oluşturan seçimlik hareketlerden bir diğeri, verinin yetkisiz üçüncü kişiler tarafından ele geçirilmesidir. Bu hüküm bakımından, kişisel verilerin yetkisiz üçüncü kişiler tarafından elde edilmesinin engellenmesine yönelik bir işleve sahiptir. 135. maddede genel olarak kişisel verilerin toplanmasından bahsedilmesi karşısında, bu maddede düzenlenen kişisel verinin ele geçirilmesi, kaydedilmiş olan kişisel verinin hukuka aykırı olarak elde edilmesi anlamına gelmektedir.

⁴⁷³

SOYASLAN, s. 272.

G. Verileri Yok Etmeme

Kişisel verilerin korunmasına ilişkin olarak TCK’de yer alan üçüncü suç kişisel verilerin yok edilmemesidir. Verileri yok etmeme başlığını taşıyan 138. maddeye göre *“Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.”* İhmal suretiyle işlenebilen bir suç olarak 138. maddede düzenlen suçun, Tasarının 198. maddesinin ikinci fıkrasından aynen alındığı görülmektedir.

Kişisel verilerin kaydedilmesinin ve işlenmesinin kişisel verilerin korunmasına ilişkin hükümlerle ayrıntılı olarak düzenlenmesi ve bu açıdan kişisel verilerin işlenmesi, özel hayatın gizliliğinin sınırlandırılması anlamında istisnai bir durum olması, beraberinde kişisel veriye ihtiyaç duyulmadığı durumlarda verinin yok edilmesi ya da ilgili kişiyle olan doğrudan ya da dolaylı bağlantısının ortadan kaldırılmasını gündeme getirmektedir.

Bireysel ve toplumsal olarak belirli bir ihtiyaca hizmet etmesi nedeniyle kişisel verilerin işlenmesi meşru kabul edilirken, bireysel ya da toplumsal ihtiyacın ortadan kalkması durumunda kişisel verinin işlenmesine ilişkin meşruiyet de ortadan kalkmaktadır. Kişisel verinin işlenmesine ilişkin meşruiyetin ortadan kalktığı durumlarda ise, özel hayatın gizliliği kapsamında genel kurala dönülmekte ve ilgili kişi hakkında bilgi ya da enformasyon içeren verinin üçüncü kişiler tarafından bilinmesi zorunluluğu ya da ihtiyacı ortadan kalkmaktadır.

Kişisel verinin yok edilmesi yukarıda belirtildiği üzere, verinin tamamen ortadan kaldırılması anlamına gelebileceği gibi bunun yanında verinin içerdiği bilgi ya da enformasyon ile ilgili kişinin arasındaki bağlantının ortadan kaldırılması şeklinde de gerçekleştirilebilir. Bu ikinci husus özellikle bilimsel ve istatistikî amaçlarla kişisel verinin işlenmesinde önem arz etmektedir. Saklama zorunluluğunun ortadan kalkması sonrasında, bu tür faaliyetler için verinin gerekli olduğunda kullanılabilmesi açısından verinin yok edilmesi tamamen ortadan kaldırma yanında ilgili kişi ile bağlantısının kurulamayacak hale getirilmesi olarak anlaşılmalıdır. Bu son durumda, verinin ilgili kişi ile doğrudan ya da dolaylı bir biçimde irtibat sağlanamayacak hale getirilmesi sonucunda kişisel verilerin korunmasına ilişkin düzenlemelerin amacını oluşturan veri/enformasyon mahremiyeti kapsamında özel hayatın gizliliğinin korunmasına ilişkin bir beklenti söz konusu olmamaktadır. Bu durumda verinin içerdiği bilgi ya da veri herhangi bir konu hakkında genel bir bilgi olarak kalmakta ve ancak istatistiki ya da bilimsel bir anlam taşıyabilmektedir.

Amaçla bağlılık ilkesine ilişkin açıklamalarda belirtildiği üzere, kişisel verilerin işlenmesinde özellikle keyfiliğin önlenmesine ilişkin olarak işleme amacının ortadan kalktığı ya da ilgili amacın gerçekleşmesi sonucunda, kişisel veriye ihtiyacın kalmaması halinde kişisel verinin yok edilmesi önem arz etmektedir. Bu haliyle de ikincil işleme ya da amaç dışı işlemenin önüne geçilmesi anlamında kişisel verinin yok edilmesi keyfililiğin önlenmesi bakımından önemlidir.

TCK'nin 138. maddesinde, amacın ortadan kalkması ya da amacın gerçekleştirilmesi sonucunda kişisel verilerin yok edilmesi hususuna yer verilmemiş,

bunun yerine kanunların belirlediği sürelerin geçmiş olması sonucunda verinin yok edilmemesi esas alınmış ve ihmali bir suç olarak düzenlenmiştir⁴⁷⁴.

Madde metninde TCK'nin 135. ve 136. maddelerinden farklı olarak kişisel verilerin sistemden yok edilmesi öngörülmüştür. Kişisel verilerin kaydına ilişkin açıklamalarda belirtildiği üzere Türk Ceza Kanunu Tasarısında kişisel verilerin korunmasına ilişkin suçlar bakımından bilişim sisteminin kullanımı esas alınarak suçlar düzenlenmişti. Bu haliyle asıl olarak kişisel verilerin korunmasına ilişkin suçlarda otomatik işleme esas alınması sonucun Tasarının 198. maddesinin ikinci fıkrasında verileri yok etmeme suçu, verinin kaydedildiği sistemden yok edilmeme olarak düzenlenmişti.

TCK'de ise, kişisel verilerin korunmasına ilişkin 135. 136. maddelerinde sadece otomatik işleme esas alınmamıştır. Verilerin yok edilmesi suçu bakımından ise bu unsurun korunduğu görülmektedir. Kişisel verilerin korunmasına ilişkin suçlar yönünden TCK'de otomatik ya da otomatik olmayan işleme bakımından önceki maddelerde bir farklılık görülmemesi, bu maddede düzenlenen suçta ise, sistemden yok edilmemesi şeklinde, genel olarak otomatik işlemeyi esas alması, maddeler arasında bir çelişkiye yol açmaktadır. 135. ve 136. maddelerden otomatik işleme unsurunun çıkartılması karşısında, 138. maddesinde düzenlenen suçun 135. 136. maddeler suçlarla uyumlu hale getirilmesi gerekir. Bu nedenle kişisel verinin yok edilmesi açısından sistemde bulunması şartı maddeden çıkartılmalıdır.

⁴⁷⁴ SOYASLAN, , s. 275.

SONUÇ ve DEĞERLENDİRME

20 yüzyılın ikinci yarısından itibaren bilişim ve özellikle bilgisayar sistemlerinin kullanılmaya başlanması ve kullanımının yaygınlaşması, bu dönem içerisinde ortaya çıkan sosyo – ekonomik dönüşümün altyapısı olarak dönüşümün dinamikleri içerisinde, toplumsal kurumları çeşitli yönleriyle etkilemiş olup bu etkinin boyutları ve derinliği giderek artmaktadır. Bilişim toplumu, bilgi toplumu, enformasyon toplumu olarak adlandırılan dönüşümün ana karakteri bilginin ya da enformasyonun kendisinin önemli hale gelmesidir. Bilginin ya da enformasyonun işlenme sürecini etkin kılan teknik altyapı ise bilişim ve özellikle bilgisayar sistemleridir.

Toplumsal bir kurum olan hukuk sistemleri de çeşitli yönleriyle bu gelişimden etkilenmektedir. Bilişim suçları olarak adlandırılan suç tiplerini ise bu gelişimin maddi ceza hukukuna etkisi olarak tanımlamak mümkündür.

Söz konusu etkinin görünümleri olarak TCK'nin 243 vd. maddelerinde düzenlenen bilişim alanında suçlar ve 135 vd. maddelerinde düzenlenen kişisel verilerin korunmasına ilişkin suçlar; incelemenin iki boyutunu oluşturmuştur. Her iki grup düzenleme, dönemin dinamiklerin etkisi ile ceza mevzuatlarında yer almaya başlamıştır. Bilişim alanında suçlar genel olarak bilginin ya da enformasyonun korunması ve ayrıca bilişim sistemlerinin korunmasına yönelik olarak ceza mevzuatlarında yer edinmiştir. Kişisel verilerin korunması ise, dönem içerisinde kişiyle ilgili bilgi ve enformasyonun işlenme miktarının artmasına bağlı olarak gündeme gelmiştir.

Bilişim suçlarının hâlihazırdaki suçlardan kategorik olarak farklı suçları kapsamaması, bunun yerine bilişim sistemlerinin sosyo-ekonomik dönüşüm içerisinde ceza hukukuna etkisi olarak karşımıza çıkması, bu suçların incelenmesinde çeşitli sorunları da beraberinde getirmektedir. Bilişim sistemlerinin kullanımının yaygınlaşması ile birlikte ortaya çıkan sorunların topluca değerlendirilmeye çalışılması; sosyo-ekonomik dönüşüm içerisinde bilişim sistemlerinin kullanımının etkisinin, suçun konusu ve suçta kullanılan araç olarak bilişim sistemleri merkezinde tartışılmasına yol açmaktadır. Bunun sonucunda bir fiilin suç olarak düzenlenmesine ilişkin genel ya da özel amacın ne olması gerektiğine ya da bilişim suçları adı altında yer verilen suçların düzenlenmesinde amacının ne olduğuna ilişkin yapılması gereken asıl tartışmaları ikinci plana itilmektedir. Bu ise, özellikle suçun hukuki konusu olarak karşımıza çıkmaktadır.

Suçun hukuki konusu bakımından incelendiğinde, TCK'nin 243 vd. ve ayrıca 135 vd. maddelerinde düzenlenen suçlar yeni bir hukuki konuya işaret etmemektedir. Bu doğrultuda incelendiğinde özellikle bilişim alanında suçlara yönelik olarak kanun koyucunun, TCK'nin özel kısmının sistemine uymayan bir şekilde düzenleme yaptığı görülmektedir.

Nitekim 243 vd. maddelerde düzenlenen suçlar açısından tartışılan sorun, yeni bir hukuki konudan çok, hâlihazırdaki suçların hukuki konularına yönelik yeni ihlal yöntemleri karşısında özellikle suçun maddi unsurlarında ortaya çıkan sorunların giderilmesi merkezindedir. Bu sorunun çözümü, yaygın olarak bilişim suçları adı altında incelenen kimi suçların ceza mevzuatları içerisinde yer edinmesi şeklindedir. İncelendiği üzere söz konusu suçlar TCK'de, genel olarak kişiye ait değerlerin korunması açısından, mameleki değerlerin korunmasına yönelik olarak

düzenlenmiştir. Buna karşın, söz konusu suçlar Kanunda topluma karşı suçlar arasında yer almıştır. Söz konusu suçların, bir bütün olarak kişiye ait mameleki değerlerin çeşitli yönleriyle korunmasına yönelik olarak düzenlenmesi karşısında, topluma karşı suçlar arasında yer verilmesi kanaatimizce TCK'nin sistematığına uymamaktadır.

Bilişim alanında suçların topluma karşı suçlar arasında düzenlenmesinin yarattığı ilk büyük sorun, genel olarak malvarlığına karşı suçlar bakımından geçerli olan ilgili kişinin rızasının bilişim alanında suçlar bakımından geçerli olup olmadığı noktasında toplanmaktadır. Kanunun sistematığı esas alındığında, bu soruya olumlu bir cevap vermek mümkün değildir. Burada sorun, bilişim alanında işlenen suçlar bakımından kanunun sistematığından uzaklaşılması ve bunların düzenleniş itibarıyla kişiye karşı suç olarak kabul edilmesi ile çözümlenebilecektir.

Bilişim alanında suçların düzenlenme yeri, özellikle mameleki değerlerin çeşitli yönleriyle korunduğu malvarlığına karşı suçlardan bir kısmı için öngörülen cezasızlık ya da cezada indirim sebeplerinin uygulanıp uygulanamayacağı noktasında da önemlidir. Bilindiği üzere 5237 Sayılı TCK'nin 167. maddesinde “*şahsî cezasızlık sebebi veya cezada indirim yapılmasını gerektiren şahsî sebepler*”, 168.maddede ise cezada indirim sebebi olarak “*etkin pişmanlık*” halleri düzenlenmiştir. Bunun yanında malvarlığına karşı suçlar bakımından cezanın ortadan kaldırılması ve de cezada özel indirim sebeplerine de yer verilmiştir (Örnek olarak bkz., TCK 145.m. , 147. m.).

Bu doğrultuda, Kanunda bilişim alanında işlenen suçlar için malvarlığına ilişkin suçlarda olduğu gibi cezasızlık ya da cezada indirim sebeplerinin öngörülmemesi, korunan hukuki değer yönünden ortak özelliğe sahip suçlar

bakımından, sırf suçta kullanılan aracın bilişim sistemi olması nedeniyle, farklılık yaratılması sonucunu doğurmaktadır. Sorun malvarlığına karşı suçlar bakımından öngörülen genel ve özel cezasızlık ve cezada indirim sebeplerinin bilişim alanında işlenen suçlar bakımından uygulanıp uygulanamayacağıdır. 765 Sayılı TCK'nin yürürlükte olduğu dönemde; 525/b maddesi kapsamında değerlendirilen banka kartı ile para çekme fiiline ilişkin, 525b/2. maddesinden hüküm kurulan Yargıtay kararlarında, 522. maddeyi uygulanmayacağıının belirtilmesi karşısında aynı sonuca TCK'nin 243 vd. bakımından da varılabilmesi mümkündür⁴⁷⁵.

243. vd. maddelerinde yer alan suçlara ilişkin hâlihazırdaki hükümler, kendi içlerinde de çeşitli sorunları taşımaktadır. Ayrıca, TCK'de yer alan diğer suçlarla birlikte değerlendirildiğinde, söz konusu suçların düzenlenme yeri ve şekli, çeşitli sorunlar doğurmaktadır.

Türk Ceza Kanunu Tasarısında seçimlik hareketli bir suç olarak düzenlenen yetkisiz erişim suçu bakımından, suçun unsurlarında değişiklik yapılmıştır. Bu şekliyle, ister malvarlığını korumaya yönelik olduğu isterse de özel hayatın gizliliğinin korunmasına yönelik ya da sistemin gizliliğini korumaya yönelik olduğu kabul edilsin, suçun unsurları bakımından kapsamın daraltılması, yetkisiz erişim suçunu, bu değerlerin korunmasına ilişkin yeterli bir işleve sahip olmaktan uzaklaştırmıştır. Söz konusu suç bakımından, Sibersuç Sözleşmesi'ndeki hüküm ya maddi unsur açısından benzerlik taşıyan İtalyan ve Fransız Ceza Kanunlarındaki

⁴⁷⁵ Yargıtay, 10. CD, E. 2004/14311 K. 2004/10906 T. 2.11.2004, <http://www.kazanci.com.tr/kho2/ibb/files/10cd-2004-14311.htm>

Yargıtay 6. CD, E. 2002/23728, K. 2004/3131, T. 18.3.2004
<http://www.kazanci.com.tr/kho2/ibb/files/6cd-2002-23728.htm>

düzenlemelere paralel bir düzenlemeye yer verilmesi, suçun maddi unsurunda ortaya çıkan sorunun giderilmesinde yararlı olabilecektir.

TCK'de bilişim alanında suçlar başlığı altında yer verilen diğer bir suç grubu 244. maddenin 1. ve 2. fıkrasında düzenlenen sisteme ve veriye müdahaledir. Bilişim sistemine ve veriye müdahale, klasik mala zarar verme suçunun bilişim sistemine ve veriye yönelik fiiller bakımından uygulanabilir olup olmadığı tartışması sonucu ceza mevzuatlarında yer almıştır. Bunun sonucu olarak iki yaklaşım esas alınmış, ya ABD'de -özellikle federe devletlerde- olduğu şekliyle veri, hukuken eşya olarak kabul edilmiş ve bu şekliyle sisteme ve veriye müdahale düzenlenmiş ya da veri, eşya olarak kabul edilmemekle birlikte bu fiillerin verinin saklandığı aygıtın ya da sistemin fonksiyonuna müdahale olduğu kabul edilerek bunlara ilişkin özel düzenleme yapılması yoluna gidilmiştir. Her iki yaklaşımda da sisteme ve veriye müdahale, malvarlığını korumaya yönelik bir suç olarak düzenlenmiştir. Bu şekliyle de sisteme ve veriye müdahalenin hukuki konusu, mala zarar verme suçunun hukuki konusu ile örtüşmektedir.

Aktarılan nedenlerle, 244. maddenin 1. ve 2. fıkrasında düzenlenen suçun mala zarar verme suçunun düzenlendiği yerde düzenlemesi gerekir. Bu yönde bir tercih, hem TCK'nin sistemine hem de bu suçun düzenlenmesindeki amaca uygun düşer. Sisteme ve veriye müdahale bakımından, Sibersuç Sözleşmesindeki hükümler ve ayrıca suçun unsurlarında kısmen farklı yaklaşımların egemen olduğu Alman ve İtalyan Ceza Kanunlarındaki düzenlemeler esas alınabilir.

Bu yönde bir tercihin yapılmaması, çeşitli sorunlara yol açmaktadır. Öncelikli olarak belirtmek gerekirse; mala zarar vermenin şikâyeteye bağlı bir suç olarak düzenlendiği TCK'de 244. maddenin birinci ve ikinci fıkrasında yer alan sisteme ve

veriye müdahaleye ilişkin hükümlerde şikâyet şartının aranmaması, düzenleme gerekçesinin ötesinde bir sonuç doğmasına yol açmaktadır. Sisteme ve veriye müdahale re'sen kovuşturulabilirken, mala zarar verme suçunda şikâyet şartı gündeme gelmektedir. Bu sorun, kimi yazarların belirttiği şekliyle, 244. maddenin özellikle birinci fıkrasındaki hükmün sistemin fiziki yapısına yönelik hareketleri de kapsadığının kabulü halinde daha da derinleşmektedir.

244. maddenin birinci fıkrasında düzenlenen bilişim sisteminin işleyişinin engellenmesi ve bozulmasında, suçun unsurlarını oluşturan hareketlere belirginlik kazandırılmaması, özellikle bilişim sistemleri bakımından mala zarar verme kapsamında ortaya çıkan soruna ilişkin çözümün ötesinde bir kapsama sahip olabilecek şekilde yorumlanmaya elverişlidir. Her ne kadar, bu suçların ortaya çıkış nedeni ve amacı göz önünde bulundurularak, bu fıkra ve ayrıca ikinci fıkra düzenlenen hareketlerin fiziki müdahaleleri esas almayan, yazılıma yönelik müdahaleleri kapsar şekilde yorumlanması gerektiği yukarıda ifade edilmiş ise de, uygulamada ortaya çıkabilecek sorunların giderilmesi bakımından, özellikle birinci fıkranın yeniden düzenlenmesi gerekmektedir.

İkinci fıkra ise, sistem içerisindeki verinin başka bir yere gönderilmesi hareketine yer verilmekte ve bu da sistem içerisindeki veriye müdahale bakımından fıkranın düzenleniş amacıyla bağdaşmayan yorumlara neden olabilmektedir. Verinin başka bir yere gönderilmesinin, sistem içerisinde verinin yerinin değiştirilmesi olarak dar yorumlanması halinde bilişim sisteminin içindeki veriye müdahale bakımından kısmen anlam kazanmakla birlikte, madde metninden çıkartılması, maddenin düzenleniş amacına daha uygundur.

Bilişim alanında suçlar arasında TCK’de düzenlenen diğer bir suç, Kanunun 244. maddesinin son fıkrasında yer alan, bilişim sistemi aracılığıyla yarar sağlamadır. Bilişim sistemi aracılığıyla yarar sağlama, genel olarak klasik dolandırıcılık suçunun unsurlarında ortaya çıkan sorunların giderilmesi ve bu tür fiiller sonucunda yarar sağlanması hallerinin cezalandırılması amacıyla ceza mevzuatları içerisinde suç olarak düzenlenmeye başlanmıştır. 244. maddede ise bir anlamda bu suç, mala zarar verme suçunun özel şekli olarak düzenlenen sisteme ve veriye müdahalenin ağırlatıcı nedeni olarak ele alınmıştır.

765 s. TCK’nin 525b/ 2. fıkrasına göre, unsurlarda belirginlik kazandırılmaya çalışılması ve yardımcı norm olarak düzenlenmesi suretiyle son fıkranın uygulama alanı 525b/2. maddeye göre daraltılmış olsa da, unsurlar bakımından 244. maddenin birinci ve ikinci fıkrasının esas alınması kendi içinde sorunlara neden olabilmektedir. Bu durum, 244. maddenin 1. ve 2. fıkrasındaki fiillerin fiziki müdahale yoluyla da işlenebileceğine ilişkin görüş kabul edilecek olursa, çok daha belirgin hale gelecektir. Bu görüş kabul edildiğinde, bilişim sistemine fiziki bir müdahalenin hile kapsamında değerlendirilmesi sonucunu doğurmaktadır. Bu ise, son fıkrada düzenlenen fiilin tarihsel gelişim itibarıyla işaret ettiği soruna ve bu kapsamda düzenlenmesindeki amaca ters düşmektedir.

Başta da belirtildiği üzere, sorun, bir kişiye karşı hileli hareketlerin ve dolayısıyla kişinin aldatılmasının söz konusu olmadan yarar sağlanabilmesidir. Bu açıdan, 244.maddenin son fıkrasında yer alan suçun yeniden ele alınması ve Alman ve İtalyan Ceza Kanunlarında yer alan şekliyle, dolandırıcılık suçunun özel bir şekli olarak tekrar düzenlenmesi gerekmektedir. Kişiye karşı hile yapılarak kişinin aldatılmasının söz konusu olmadığı bu suçta, sistem içerisindeki verilere ve

programlara müdahale edilmesi, Alman ve İtalyan Ceza Kanunlarındaki bilgisayar aracılığıyla yarar sağlama suçlarında olduğu gibi dolandırıcılık suçunun unsurunu oluşturan hileli hareketlerle bir kişinin aldatılmasının yerine geçebilecektir. Bu tür bir düzenleme yapılırken de bilişim sistemi aracılığıyla yarar sağlamada; suçun unsuru olarak sadece yarar sağlama kabul edilmemeli, zararın meydana gelmesinin suçun unsuru olarak düzenlendiği TCK'nin 157. maddesinde yer alan dolandırıcılık suçuyla, bu yönden de uyum sağlanmalıdır.

Kanunda, bilişim sistemlerinin kullanımının ikinci büyük etkisi olarak karşımıza çıkan kişisel verilerin korunmasına ilişkin suçlarda ise farklı bir yöntem tercih edilmiştir. Bilişim alanında suçlardan farklı olarak bu suçlar, suçların hukuki konusuna göre ilgili bölümde düzenlenerek, TCK'nin sistemi açısından, yerinde bir tercih yapılmıştır. Söz konusu suçlar bakımından öncelikli olarak ortaya çıkan sorun, hangi hallerde hukuka uygun bir işlemenin var olduğudur. Bu sorun asıl olarak Anayasanın 20. maddesinde düzenlenen özel hayatın gizliliğine ilişkin olarak, maddenin 1. fıkrasında sınırlandırma sebebine yer verilmemesinden kaynaklanmaktadır. Kişisel verilerin işlenmesi genel olarak özel hayatın gizliliğine bir müdahale ve dolayısıyla özel hayatın gizliliğinin sınırlandırılması olarak kabul edildiğinde, herhangi bir sınırlandırma nedenine yer verilmeyen Anayasanın 20. maddesinin birinci fıkrası ve temel hak ve hürriyetlerin sınırlandırılmasına ilişkin Anayasanın 13. maddesi karşısında, kişisel verilerin işlenmesine izin ya da yetki veren normların Anayasaya aykırılığı gündeme gelmektedir.

Ortaya çıkan diğer bir sorun ise, TCK'nin 135 vd. maddelerinde düzenlenen suçlar bakımından kişisel verinin çok kapsamlı olması ve hâlihazırda kişisel verilerin işlenmesi usul ve esaslarının yer aldığı özel bir kanunun bulunmamasıdır. Kişisel

verilerin işlenmesine ilişkin çeşitli kanunlardaki dağınık hükümler bir yana bırakılacak olursa, kişisel verilerin işleme usul ve esaslarının belirlendiği özel bir kanunun mevcut olmaması, bir yandan bu söz konusu hükümlerin uygulanabilmesinde sorunlara ve belirsizliğe yol açmaktadır.

Her iki suç grubunda, kanun koyucu tarafından çözümün, sistematik olarak farklı şekillerde öngörülmesi ise diğer bir soruna işaret etmektedir. Bu da sosyo-ekonomik dönüşüm içerisinde anlam kazanan bilişim sistemlerini kullanımının genel olarak hukuka ve özel olarak ceza hukukuna etkisi bakımından sorunun yeterince tartışılmamış olmasıdır. Bilişim suçları açısından 5237 Sayılı TCK incelendiğinde, Kanunun, yapımı aşamasında ve bilişim sistemlerinin ceza hukukuna etkilerinin ne olduğu ve ortaya çıkardığı sorunların niteliksel ya da niceliksel mi olduğuna ilişkin yeterli bir tartışma yapılmadığı ve TCK'nin hazırlanmasında söz konusu maddelere kaynaklık eden kanun ya da kanunlardan adapte edilmeye çalışıldığı görülmektedir. *“Bilişim alanında suçlar”* açısından bu husus daha açık bir şekilde kendisini hissettirmektedir.

TCK' nin sistemi bakımından, bilişim sistemlerinin kullanımının ceza hukukuna etkisi olarak karşımıza çıkan kişisel verilerin korunmasına ilişkin suçlardaki isabetli tercih ise, bu konuda yeterince incelemenin yapıldığının bir göstergesi olmaktan uzaktır. Söz konusu tercih, maddelerin esinlenildiği kaynak kanun ya da kanunlardaki tercihin aynen aktarılması şeklinde olup ve bu haliyle konunun derinlemesine incelendiğine ilişkin bir bulgu oluşturamamaktadır.

Başta da belirtildiği üzere, bilişim sistemlerinin kullanımının ceza hukukuna etkisi olarak bilişim suçları, homojen bir niteliğe sahip suç kategorisi olarak ele alınamayacak niteliktedir. Bilişim sistemlerinin kullanımlarının yaygınlaşmasına

paralel olarak hukukta etkileri her geçen gün itibariyle artmaktadır. Bu husus bilişim suçları kapsamında değerlendirilen suçların kapsamının artmasında da kendisini göstermektedir. Bu açıdan kategorik olarak yeni ve bağımsız bir suç ya da suçların var olduğunu söylemek bir yandan sorunu kendi içinde çıkmazlara sokarken bir yandan da çözüm için öngörülen suçların, ihtiyaca cevap verememesi ya da amacını aşan uygulamalara yol açmasına neden olmaktadır.

Sonuç olarak, 765 S. TCK' nin 525a vd. maddelerinde düzenlenen bilişim suçlarına ilişkin olarak *Ersoy* tarafından yapılan değerlendirmenin, özellikle 243.madde ve devamında düzenlenen bilişim suçları açısından ve bunun ötesinde Türk Ceza Hukukunda bilişim sistemlerinin kullanımının etkisinin algılanma düzeyi bakımından da geçerli olduğunu söylemek mümkündür. Yazara göre; “ *Bilişim alanında ortaya çıkan hukuki koruma ihtiyacının genel olarak ele alınıp bu çerçevede cezaî korumanın ne olduğunu saptamak gerekirken böyle yapılmamış ve bir yabancı tasaridan yararlanılarak Ceza Kanununa ‘Bilişim Alanında Suçlar’ başlıklı dört maddelik bir ‘Bab’ eklenmiştir... Bu maddelerde getirilen hükümlerin yeterince isabetli oldukları ve sisteme tutarlı hale getirildikleri söylenemez. Bu bakımdan, Ceza Kanununa yapılan ekleme, bilgisayar çağının ortaya çıkardığı hukukî düzenleme ihtiyacının göstermesi bakımından olumlu sayılabilmesine karşın, yetersiz ve sınırlı bir çaba olarak kalmıştır... Bu konudaki hukukî düzenlemelerin, elbette yabancı ülkelerdeki örneklerden yararlanılarak ancak Ülkemiz ortamının özellikleri de göz önünde tutularak yeniden ve daha genel çerçevede ele alınması,*

ciddî çalışmalarla değerlendirilmesi ve tüm hukuk sistemimiz içinde tutarlı hükümler bütünü olarak oluşturulması zorunludur...” ⁴⁷⁶

Bilişim sistemlerinin kullanımının ceza hukukunda etkisi bakımından Türk Ceza Hukukunda, maddi ceza hukukuna etkilerine ilişkin özellikle sorunlara yaklaşımın ne şekilde olduğunun değerlendirildiği bu incelemenin kapsamı dışında bırakılan bir düzenleme de *Ersoy*’un yukarıda aktarılan görüşlerini teyit eder niteliktedir. Nitekim 5271 Sayılı CMK’nin 154. maddesinde “*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*” düzenlenmiş olup maddenin ikinci fıkrasında “*Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşamaması 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.*” hükmüne yer verilmiştir. Özellikle delil elde etme açısından bakıldığında bir bilgisayarın her açılışında, işletim sisteminin özelliğine göre, delil niteliği taşıyabilecek büyük miktarda veri değişebilmektedir; açılış ya da şifre girme komutu olarak bilinen bir komutun, bilgisayarın bütün bilgilerini geri dönülemeyecek hale sokacak şekilde kodlanması mümkündür. Aynı maddenin birinci fıkrasında ise, maddede öngörüldüğü şekliyle arama “*Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması*” şartına bağlanmıştır. Söz konusu hükümlerin bir bütün olarak, kimi durumlarda, aslında tamamen delilleri yok

⁴⁷⁶ **ERSOY**, s. 183.

etmeye yönelik olduğunu bilmek⁴⁷⁷, *Ersoy'un* genel olarak ifade ettiđi üzere, daha derin ve kapsamlı bir çalışma yapılmasının zorunluluđunu ortaya koymaktadır.

⁴⁷⁷ Bkz., Eoghan **CASEY**, Digital Evidence and Computer Crime, Forensic Science Computers and the Internet, 3. Edition, 2001, s. 54 vd.

KAYNAKÇA*

- AKGÜL**, Mustafa (der.) Türkiye İnternetinin ve İnternet Kurulunun Kısa Tarihi, <http://kurul.ubak.gov.tr/dok20.htm>. (kontrol tarihi 03.06. 2006)
- AKIN**, Engin *Bilişim Suçu*, Yaklaşım, Yıl 14, Sayı 157, Ocak 2006, s. 266 – 270.
- AKINCI**, Hatice–
ALIÇ, A. Emre – **ER**, Cüneyd *Türk Ceza Kanunu ve Bilişim Suçları* ,İnternet ve Hukuk, Der. Yeşim M. Atamer, Baskı, İstanbul, 2004, s. 157-275.
- AKINTÜRK**, Turgut *Medeni Hukuk*, 4. Basım, Savaş Yayınları Ankara 1991.
- ALİEFENDİOĞLU** Yılmaz *2001 Anayasa Değişikliklerinin Temel Hak ve Özgürlüklerin Sınırlandırılmasında Getirdiği Yeni Boyut*, Anayasa Yargısı Dergisi C.19, 2002, s. 141 – 176,
<http://www.anayasa.gov.tr/eskisite/anyarg19/aliefendioglu.pdf>.
- ANDREANO**, Frank P. *The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem*, 27 Am. J. Crim L. 1999-2000, pp. 81-103. (Heinonline)

* Heinonline, Heinonline veri tabanından alınmış makaleleri ifade eder (www.heinonline.org). Ebrary, Ebrary veri tabanından alınmış kitapları ifade eder (www.ebrary.com) . Sciencedirect, Science Direct veri tabanından alınmış makaleleri ifade eder (www.sciencedirect.com)

- ARASLI, Oya** Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi, yayımlanmamış doçentlik tezi, Ankara 1979.
- ARTUK Mehmet Emin – GÖKÇEN,**
Ahmet – **YENİDÜNYA,** Ahmet Caner 5327 Sayılı TCK'ya Göre Hazırlanmış Ceza Hukuku Genel Hükümler 1, 2. baskı, Ankara, 2006.
- AYDIN, Emin D.** Bilişim Terimleri Sözlüğü, 1. Baskı, 1992.
- BAINBRIDGE, David:** Introduction to Computer Law, 3. Edition, 1996.
- BAŞALP, Nilgün** *Kişisel Verilerin Korunması ve İnternet, İnternet ve Hukuk, Derleyen Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004. s. 5 – 36.*
- BAŞALP, Nilgün** *Kişisel Verilerin Korunması ve Saklanması, Ankara, 2004.*
- BAYRAKTAR, Köksal** *Banka Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları, Bilgi Toplumunda Hukuk, Prof. Dr. Kemal Oğuzman Anısına Armağan, İstanbul, 2000, s. 195 – 203.*
- BENIGNER, James A.** The Control Revolution: Technological and Economic Origins of Infomation Society, Harvard University Press, 1986.

- BENNET, J. Colin** Regulating Privacy: Data Protection and Public Policy in Europe and United States, Cornell University Press , Ithaca and London, 1992.
- BENSON, Carl –JABLON, Andrew V. – KAPLAN, Pal J. – ROSENTHAL, Mara Elena** *Computer Crimes*, 34 Am. Crim. L. Rev. 1997, pp., 409 – 443. (Heinonline)
- BİÇKİN, İnci** *Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları*, Yargıtay Dergisi, C. 32, Ocak – Nisan 2006, s. 145 – 168.
- BONANO, Felicia** La frode informatica,
<http://www.computerlaw.it/public/bonannofrodeinfo.pdf> . (kontrol tarihi 13.01.2006)
- BOZKURT, Veysel** Endüstriyel – Post-Endüstriyel Dönüşüm, İstanbul, 2005.
- BRANSCOMB, Anne W.** *Rogue Computer Programs and Computer Rouges: Tailoring the Punishment to Fit the Crime*, 16. Rutgers Computer & Tech. L. J. 1990, pp., 1 – 61.
- BRENNER, Susan W.** *Is There A Thing as “Virtual Crime”*, 4. Cal. Crim. Law. Rev. 1,
<http://www.boalt.org/CCLR/v4/v4brenner.htm>.
(kontrol tarihi 10.10.2006)

- BYGRAVE, Lee A.** *The Place of Privacy In Data Protection Law, University of New South Wales Law Journal, 2001, Vol. 24, no. 1, <http://www.austlii.edu.au/au/journals/UNSWLJ/2001/6.html> (kontrol tarihi 10.10.2006)*
- BYGRAVE, Lee A.** *Data Protection Pursuant to the Right to Privacy in Human Right Treaties, International Journal of Law and Information Technology, Vol. 6, No. 3, pp. 247-284, http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf. (kontrol tarihi 09.01. 2006)*
- CARR, Indira** *Draft Cyber Crime Convention, Criminalization and the Council of Europe (Draft) Convention on Cyber-Crime, Computer Law & Security Report Vol.18, no. 2, 2002, pp. 83 – 90. (Sciencedirect)*
- CARTER, David L.** *Computer Crime Categories:How Techno-Criminals Operate, <http://www.lectlaw.com/files/cr14.htm>. (kontrol tarihi 12.11.2005)*
- CASEY, Eoghan** *Digital Evidence and Computer Crime, Forensic Science Computers and the Internet, 3. ed., 2001.*
- CASTELLS, Manuel** *Gerçek Sanallık Kültürü, Çev. Kemal Akay, İnternet: Üçünü Devrim?, Cogito, Sayı 30, 2002, s. 212- 214.*

- CASTELLS, Manuel** The Rise of The Network Society: The Information Age, Economy, Society and Culture, Vol I, 2. Edition, Oxford, 2000.
- CASTELLS, Manuel** Informational City: Information Technology, Economic Restructuring and The Urban-Regional Process, Oxford, Blackwell, 1989.
- CATE, Fred** Privacy in the Information Age, Booking Institutions Press, Washington, D.C., 1997.
- CENTEL, Nur – ZAFER, Hamide – ÇAKMUT Özlem** Türk Ceza Hukukuna Giriş, 3. Bası, İstanbul, 2005.
- CHARNEY, Scott – ALEXANDER, Kent** *Computer Crime*, 45 EMORY L. J. 1996, pp. 931 – 957. (Heinonline)
- CLOUGH, Bryan – MUNGO, Paul** Veri Suçları ve Bilgisayar Yer altı Dünyası, Çev. Emel Kurma, İletişim Yayınları, 1. baskı, 1999.
- CONLEY, M. John – BRYAN, M Robert** *A Survey of Computer Crime Legislation in the United States*, Information & Communication Technology Law, Vol. 8, No. 1, 1999, pp. 35 – 57.
- ÇELEBİCAN, Özcan** Roma Eşya Hukuku, 2. Basım, Ankara, 2005.

- ÇOBAN, Hasan** Bilgi Toplumuna Geçiş, Gelecekte Kaçılmaz, İstanbul, 1997.
- DANIŞMAN, Ahmet** Ceza Hukuku Açısından Özel Hayatın Korunması, Konya, 1991.
- DEGAETANO, Patty M.** *Note: Intel Corp v. Hamidi: Private Property Keep Out –The Unworkable Definition of Injury for a Trespass to Chattels Claim in Cyberspace* 40 Cal. W. L. Rev. 2003-2004, pp. 355 – 382. (Heinonline)
- DEĞİRMENCİ, Olgun** *2004 Türk Ceza Kanunun Bilişim Suçları Bakımından Değerlendirilmesi*, Türkiye Barolar Birliği Dergisi, S. 58, 2005, s. 195 – 208.
- DEMİR, Önder** *İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu*, Uluslararası İnternet Hukuku Sempozyumu, İzmir 2002, s. 481 – 484.
- DEMİRBAŞ, Timur** Ceza Hukuku Genel Hükümler, 3. Bası, Ankara, 2005.
- DILLON, Sheri A. – GROENE, Douglas E. – HAYWARD Todd** *Computer Crimes*, 35 Am. Crim. L. Rev. 1997-1998, pp., 503-547 (Heinonline)

DITZION, Robert –**GEDDES**,

Elizabeth – **RHODES**, Mary

Computer Crimes, 40 Am. Crim. L. Rev. 2003,
pp. 285-336. (Heinonline)

DONAY, Süheyl –

KAŞIKÇI, Mahmut

En Son Değişikliklerle Açıklamalı ve
Karşılaştırılmalı Türk Ceza Kanunu, 1. Baskı,
İstanbul, 2005.

DÖNMEZER, Sulhi

Ceza Hukuku Dersleri, İstanbul, 2003.

DÖNMEZER, Sulhi

Kişilere ve Mala Karşı Cürümler, 16. Bası,
İstanbul 2001.

DÖNMEZER, Sulhi –
ERMAN, Sahir

Nazari ve Tatbiki Ceza Hukuku, Genel Kısım, C.
I, 12. B., İstanbul, 1997.

DÖNMEZER, Sulhi –

ERMAN Sahir

Nazari ve Tatbiki Ceza Hukuku, Genel Kısım, C.
2, 10 Baskı, İstanbul, 1994.

DREYFUSS, Rochelle C. –

LEEBRON, David W.

Foreword: Privacy and Information Technology,
Ann. Surv. Am. L. 1986, pp. 495 – 510.
(Heinonline)

DÜLGER, Murat Volkan

Bilişim Suçları, 1. Baskı, Ankara, 2004.

- EDİS**, Seyfullah Medenî Hukuka Giriş ve Başlangıç Hükümleri, 6. Basım, Ankara 1997.
- ELMI**, Giancarlo Taddei *The Law on Computer Crime in Italy*, Information & Communications Technology, Vol. 6, Issue 3, 1997, (EBSCOHOST)
- ERDEM**, Mustafa Ruhan Türk Hukukunda Karşılıksız Yararlanma Suçları, 1996.
- EREM**, Faruk – **TOROSLU**, Nevzat Türk Ceza Hukuku Özel Hükümler, Savaş Yayınevi, 9. Baskı, Ankara, 2003.
- EREM**, Faruk *Kamu Hukuku Açısından Siberetik*, AÜHF Dergisi, C. XXXI, Sayı 1-4, 1974, s. 1 – 7.
- EREM**, Faruk Dolandırıcılık, Ankara Üniversitesi Hukuk Fakültesi Yayınları: 101, Ankara, 1956.
- EREM**, Faruk: *Bilgisayar Suçları ve Türk Ceza Kanunu*, Yargıtay Dergisi, C. 17, S. 4, Ekim 1991, s. 437 – 444.
- ERKAN**, Hüsnü Bilgi Toplumu ve Ekonomik Gelişme, Türkiye İş Bankası Kültür Yayınları, 4. Baskı, 1998.
- ERMAN**, R. Barış *Alman Hukukunda İnternette Kaynaklanan Ceza Sorumluluğu* İHFM, C. LIX, S. 1-2, 2001, s. 202 -225.

- ERSOY, Yüksel** Ceza hukuku Genel Hükümler, Ankara, 2002.
- ERSOY, Yüksel** *Genel Hukuki Koruma Çerçevesinde Bilgisayar Suçları*, Prof. Dr. Yılmaz Günal’a Armağan, Ank. Ün. SBFD, C. 49, Haziran-Aralık 1994, No. 3-4, Ankara, 1995, s. 149 – 183.
- ESTADELLA YUSTE, Olga** Report: *The Relevance of the Data Protection Principles Set Out in the Convention 108 and Its Additional Protocol*, European Conference on Data Protection on Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Present and Future, Warsaw 2001, [http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Events/Conf\(Warsaw2001\)ProceedingsE.pdf](http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Events/Conf(Warsaw2001)ProceedingsE.pdf) (kontrol tarihi 15.04.05);
- FALZETTI, Valerio** I Computer Crimes, 83 vd. <http://www.unicam.it/ssdici/falzetti.pdf>. (kontrol tarihi 13.10.2005)
- FENDOĞLU, H. Tahsin** *2001 Anayasa Değişikliği Bağlamında Temel Hak ve Özgürlüklerin Sınırlanması*, Anayasa Yargısı Dergisi, C. 19, 2002 s. 178 – 214, <http://www.anayasa.gov.tr/eskisite/anyarg19/fendoğlu.pdf>.
- FISCHER-HÜBNER, Simone** *Privacy and Security at Risk in the Global Information Society, Cybercrime: Law Enforcement, Security and Surveillance in the*

- Information Age, Edit. Douglas Thomas - Brian D. Loader, Routledge 2000, pp. 173 – 192.
- FLORIDI**, Luciano
Philosophy and Computing: An Introduction, Routledge, 1999. (Ebrary)
- FOURMAN**, Michael
Informatics,
<http://www.inf.ed.ac.uk/publications/online/0139.pdf>. (kontrol tarihi 08.09.2006)
- GÖLCÜKLÜ**, Feyyaz –
GÖZÜBÜYÜK, A. Şeref
Avrupa İnsan Hakları Sözleşmesi ve Uygulaması, 1. Baskı, Ankara, 1994.
- GRAHAM**, Gordon
The Internet: A Philosophical Inquiry, Routledge, 1999. (Ebrary)
- GROSS**, Hyman
Privacy-Its Legal Protection, New York, 1964.
- GÜLŞEN**, Recep
İnternet ve Suç, İnternet ve Toplum, Editör: Ahmet Tarcan, Ankara, 2005, s. 200 – 256.
- GÜNEY** Niyazi – **ÖZDEMİR**, Kenan – **BALO**, Yusuf S.
Yeni Türk Ceza Kanunu, 1. Baskı, 2004.
- HAFIZOĞULLARI**, Zeki
Ceza Hukuku Genel Hükümler,
<http://www.baskent.edu.tr/~zekih/uygulamaci/ucezagenel.htm> (kontrol tarihi 15.07.2006)

- HAFIZOĞULLARI, Zeki** Ceza Normu, Normatif Bir Yapı Olarak Ceza Hukuku Düzeni, 2. baskı, Ankara , 1996.
- HAFIZOĞULLARI, Zeki** *Türk Ceza Hukuku'nun Seksen Yılı, Cumhuriyetim Kuruluşundan Bugüne Türk Hukukunun Seksen Yıllık Gelişimi*, Ankara Üniversitesi Hukuk Fakültesi Yayınları No: 538, 30-31 Ekim 2003, Sempozyum, s. 165 – 210.
- HEADRICK, Daniel R.** Enformasyon Çağı, Akıl ve Devrim Çağında Bilgi Teknolojileri 1700 – 1850, Çev. Zülal Kılıç, 1. Basım, İstanbul, 2002.
- HÉBERT, Monique –**
PILON, Marilyn Computer Crime, [http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/BP/bp87-e.htm#\(25\)txt](http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/BP/bp87-e.htm#(25)txt).
- HEYMANN, Stephen P.** *Legislating Computer Crime*, 34. Harv. J. on Legis. (1997), pp. 373 – 391. (Heinonline)
- HOFSTADTER, Samuel H.–**
HOROWITZ, George The Right of Privacy, New York 1964.
- IFRAH, Georges** Rakamların Evrensel Tarihi -IX-, *Bilgisayar Ne Sayar*, Çev. Kurtuluş Dinçer, 2 Basım, 2002.

- IPPOLITO**, Carlo Sarzana di S. *Biliřim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalyadaki Durum*, İHFM, C: LV, S. 3, 1997, Çev. Vesile Sonay Daragenli. s. 389-405
- İÇEL**, Kayıhan – **ÖZGENÇ**, İzzet – **SÖZÜER**, Adem – **MAHMUTOĞLU**, Fatih S.– **ÜNVER**, Yener *Suç Teorisi*, İstanbul, 1999.
- İÇEL**, Kayıhan – **ÜNVER**, Yener *Kitle Haberleşme Hukuku*, Yenilenmiş 6. Bası, İstanbul, 2005.
- İÇEL**, Kayıhan *Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında “Avrupa Siber Suç Politikasının Ana İlkeleri”*, İHFM, C. LIX, S. 1-2, 2001, s. 3- 9.
- JOHNSON**, Maggie *Background and History*, <http://cse.stanford.edu/class/cs103a/h2Background.pdf>.
- KANGAL** Zeynel *Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu*, İHFM, C. LIX, S. 1-2, 2001, s. 227 – 240.
- KARAGÜLMEZ**, Ali *Biliřim Suçları ve Soruşturma-Kovuşturma Evreleri*, 1. baskı, Ankara , 2005.
- KESKİN**, Serap *Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İliřkin Hükümlerin*

Değerlendirilmesi, İHFM, C. LIX, S. 1-2, s. 155 – 180.

HAFNER, Katie –

LYON, Matthew

İnternet Tarihi: Sihirbazların Gecelediği Yer, Çev. Sinem Yazıcıoğlu, 1. Baskı, İstanbul, 2000.

KATOĞLU, Tuğrul

Ceza Hukukunda Hukuka Aykırılık, Ankara, 2003.

KATYAL Near Kumar

Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 2000-2001, pp. 1003 – 1114.(Heinonline)

KILIÇOĞLU, Ahmet

Şeref, Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılarından Hukuksal Sorumluluk, Gözden Geçirilmiş 2. Baskı, Ankara 1993.

BUDEN, Kit – PALMER, Creole –

LYDE, Barlow – GILBERT

Cybercrime – A new Breed of Criminal, Computer Law & Security Report Vol. 19, no. 3, 2003, pp. 222-227. (Sciencedirect)

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, C. III, s. 785 – 816.

KORFF, Douwe

Ec Study On Implementation Of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49): *Comparative Summary of National*

Laws,

http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf (kontrol tarihi 01.02.2005).

KÖKSAL, Aydın

Bilişim Toplumu,
kurultay.tbd.org.tr/kurultay20/Bildiriler/Aydin_K
oksalsal/bildiri.pdf. (kontrol tarihi 30.02.06)

KURT, Levent

Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim
Suçları ve Türk Ceza Kanunundaki Uygulaması,
Seçkin Yayınevi, 1. Baskı, Ankara, 2005.

La GRECA, Federico Tavassi

Hacking e Criminalità Informatica,
http://www.dvara.net/hk/hacking_e_criminalita_informatica.doc. (kontrol tarihi 15. 10. 2005)

LEINER, Barry M. – CERF, Vinton G. –

CLARK, David D. – KAHN, Robert E. –

KLEINROCK, Leonard – LYNCH,

Daniel C. – **POSTEL, Jon – ROBERTS,**

Larry G. – **WOLFF, Stephen**

A Brief History of the Internet,
<http://www.isoc.org/internet/history/brief.shtml>.

LLOYD, Ian J.

Information Technology Law, 3. Edition
Butterworths, London, Edinburg, Dublin, 2000.

- LYON, David** Elektronik Göz: Gözetim Toplumunun Yükselişi, Çev. Dilek Hattatoğlu, Sarmal Yayınevi, 1. Baskı 1997.
- MACODRUM, Dona – NASHERI, Hedieh –O’HEARN, Timothy J.** *Spies in Suits: New Crimes of the Information Age from the United States and Canadian Perspectives*, Information & Communications Technology Law, Vol. 10, No. 2, 2001, pp. 139 – 166.
- MAHMUTOĞLU, F. Selami.** Ekonomik Suçlar Bağlamında Kredi Hukukundan Kaynaklanan Suç ve İdari Suçlar, 1. Baskı, Ankara, 2003.
- MAHMUTOĞLU, F. Selami** *Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Cezai Sorumluluğu*, İHFM, C. LIX, S. 1-2, 2001, s. 39 – 49.
- MAHONEY, Michael S.** *The History of Computing in the History of Technology*, Annals of the History of Computing, Volume 10, Number, 2, 1988, <http://web.mit.edu/STS.035/www/PDFs/mahoney.pdf>
- MALKOÇ, İsmail** Açıklamalı Türk Ceza Kanunu, C. 4, Ankara, 2002.

- MELAB**, Nordine *Data Mining: A Key Contribution to E-business, Information & Communications Technology Law*, Vol. 10, No. 3, 2001, pp. 309 – 318.
- MENNELLY**, Lisa A. *Prosecuting Computer-Related Crime in the United States, Canada, and England: New Laws for Old Offenses*, 8 B. C. Int'l & Comp. L. Rev. 1985, pp. 551-573.
- MERAN**, Necati *Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında İşlenen Suçlar*, Seçkin Yayınevi, 1. Baskı, Ankara, 2005.
- MICHAEL**, James *Privacy and Human Rights: an International and Comparative Study, with Special Reference to Development in Information Technology*, Unesco 1994.
- MILLER**, Arthur R. *The Assault on Privacy: Computerrs, Data Banks and Dossiers*, The University of Michigan Pres, 2. Edition, 1971.
- MULGAN**, Geoffrey J. *Communication and Control: Networks and the New Economies of Communication*, 1991.
- NICHOLSON**, Laura J. – **SHEBAR**, Tom F. – **WEINBERG** Meredith R. *Computer Crimes*, 27 Am. Crim. L. Rev. (2000), pp. 207 – 259.

- OLIVENBAUM, Joseph M.** <CTRL> <ALT> <DEL>: *Rethinking Federal Computer Crime Legislation*, 27 Seton Hall L. Rev., 1996-1997, pp. 574 – 642.
- ÖNDER, Ayhan** Ceza Hukuku Genel Hükümler, C. II-III, İstanbul, 1992.
- ÖNDER, Ayhan** Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul, 1994.
- ÖZBEK, Veli Özer:** *İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 4, S. 1, 2002, s. 101 – 158.
- ÖZBEK, Veli Özer** Yeni Türk Ceza Kanununun Anlamı, C. 1, Ankara, 2006.
- ÖZSUNAY, Ergun** Gerçek Kişilerin Hukuki Durumu, 4. baskı, İstanbul 1979.
- ÖZTAN, Bilge** Medenî Hukukun Temel Kavramları, Turhan Kitabevi Yayınları, 2002.
- PAPAKONSTANTINOU, Vagelis** *A Data Protection Approach to Data Matching Operations Among Public Bodies*, International Journal of Law and Information Technology, Vol. 9, No. 1, pp. 39-64.

- PARKER, Donn B.** Fighting Computer Crime, A New Framework For Protecting Information, 1998.
- PARKER, Richard B.** *A Definition of Privacy*, 27 Rutgers L. Rev. 1973-1974, pp. 275 – 296. (Heinonline)
- RAMAN, Jari** Computer Crime,
http://www.ulapland.fi/home/oiffi/enlist/commentary/computer_crime.html#alav13. (kontrol tarihi 08.03.2006)
- RASCH, Mark D.** 11. Criminal Law and The Internet,
<http://cla.org/RuhBook/chp11.htm>. (kontrol tarihi 03.04.2006)
- REGAN, Priscilla M.** Legislating Privacy. Technology, Social Values, and Public Policy, The University of North Carolina Press 1995.
- RESTA, Salvatore** Computer Crimes Tra Informatica e Telematica, Cedam, 2000.
- RULE, James B. – McADAM, Douglas – STEARNS, Linda – UGLOW, David** *Preserving Individual Autonomy in an Information-Oriented Society*, Computers and Privacy in the Next Decade, Edit. Lance J. Hoffman, Academic Press 1980.

SAĞLAM, Fazıl

2001 Yılı Anayasa Değişikliğinin Yaratabileceği Bazı Sorunlar ve Bunların Çözüm Olanakları, Anayasa Yargısı Dergisi, C.19, 2002, <http://www.anayasa.gov.tr/eskisine/anyarg19/fsaglam.pdf> .

SAĞLAM, Fazıl

Temel Hakların Sınırlandırılması ve Özü, Ankara, 1982.

SAĞLAM, Mehmet

Ekim 2001 tarihinde Yapılan Anayasa Değişiklikleri Sonrasında Düzenledikleri Maddede Hiçbir Sınırlama Nedenine Yer Verilmemiş Olan Temel Hak ve Özgürlüklerin Sınırı Sorunu, Anayasa Yargısı Dergisi, C.19, 2002, s. 233 – 272.

SAXBY, Stephen

The Age of Information : The Past Development and Future Significance of Computing and Communications, London : Macmillan, 1990.

SCHJOLBERG, Stein

Computer-Related Offences,
<http://www.cybercrimelaw.net/documents/Strasbourg.pdf>. (kontrol tarihi 04.05.2006)

SCHØLBERG, Stein –

HUBBARD, Amanda M.

Harmonizing National Legal Approaches on Cybercrime, International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva, 28, June – 1 July 2005, Documnet: CYB/04, 10 June 2005,

http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf. (kontrol tarihi 20.03.2006)

SCHWARTZ , Paul

The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 Am J. Comp L. 1989, pp. 675 – 701.

SCHWARTZ, Paul M.

Privacy and Democracy in Cyberspace, 52 Vand. L. Rev., 1999, pp. 1609 – 1702.

SCHWARZENEGGER, Christian

Computer crimes in Cyberspace: A Comparative Analysis of Criminal Law in Germany, Switzerland and Northern Europe, <http://www.rwi.unizh.ch/schwarzenegger/unterlagen/pdf/ComputerCrimeCyberSpace2002.pdf>. (04.12.2005)

SELÇUK, Sami

Dolandırıcılık, 1. Basım, 1982.

SHACKELFORD, Steve

Computer-Related Crime: An International Problem in Need of an International Solution, 27 Tex. Int'l L.J. (1992), pp. 479 – 505. (Heinonline)

- SIEBER, Ulrich** Legal Aspects of Computer – Related Crime, in the Information Society, - COMCRİME-Study -, 1998,
<http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc>. (kontrol tarihi 08.08.2006)
- SIMOJOKI, Samuli** Location-based Services and General Privacy and Data Protection Principles: Report of the NAVI Regulatory Framework –project,
http://www.vtt.fi/virtual/navi/cd/Privacy_Principles.pdf. (kontrol tarihi 12.03.05)
- SINAR, Hasan** İnternet ve Ceza Hukuku, 1. Baskı, İstanbul, 2001.
- SINROD, Eric J. –
REILLY, William P.** *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara Computer & High. Tech. L. J. (2000), pp. 177 – 232.
- SİRMEN, Lale** Eşya Hukuku Dersleri, Ankara, 1995.
- SOKULLU-AKINCI, Füsün** *Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi*, İHFM, C. LIX, S. 1-2, 2001, s. 11-38.

- SOYASLAN, Doğan** Ceza Hukuku Özel Hükümler, Gözden Geçirilmiş 5. Baskı, Ankara, 2005.
- SPIROS Simitis** *Reviewing Privacy In an Information Society*, 135 U. Pa. L. Rev, (1986-1987), s. 707 - 746
- STONE, Paul R. – De La GARZA, Henry** *Criminal Trespass and the Exclusionary Rule in Texas*, 24 St. Mary's L. J, (1992 – 1993), pp. 443 - 461 (Heinonline)
- STRATTON, John** *Siberalan ve Kültürün Küreselleşmesi*, İnternet: Üçünü Devrim?, Cogito, Sayı 30, 2002, s. 81 -84.
- SUSSMANN, Michael** *The Critical Challenges From International High-Tech and Computer-Related Crime*, 9 Duke J. Comp. & Int'l (1998-1999) pp. 451 – 489. (Heinonline)
- ŞAYLAN, Gencay** Değişim ve Küreselleşme ve Devletin Yeni İşlevi, 2. Baskı, 2003.
- TEZCAN, Durmuş – ERDEM, M. Ruhan – SANCAKDAR, Oğuz** Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'nin İnsan Hakları Sorunu, 2. Baskı Ankara, 2004.

TEZCAN, Durmuş – ERDEM,

Mustafa Ruhan – **ÖNOK, Murat**

5237 Sayılı Türk Ceza Kanunu’na Göre Teorik ve Pratik Ceza Özel Hukuku, Seçkin Yayınevi, 3. Baskı, 2006.

TEZCAN, Durmuş

Bilgisayar Karşısında Özel Hayatın Korunması, Anayasa Dergisi, Cilt 8, 1991, s. 385 – 392 .
<http://www.anayasa.gov.tr/eskisite/anyarg8/dtezc an.pdf>.

THOMAS, Douglas –

LOADER, Brian D.

Cybercrime in the Information Age, , Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Ed. Douglas Thomas & Brian D. Loader, Routledge 2003, pp. 1 – 16.

THOMAS, Douglas

Criminality in The Electronic Frontier: Corporality and Judicial Construction of the Hacker, Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Ed. Douglas Thomas & Brian D. Loader, Routledge, 2003, pp. 17 – 35.

TİMİSİ, Nilüfer

Yeni İletişim Teknolojileri ve Demokrasi, 2003.

TONELLI, Giovanni

Il Delitto Di Accesso Abusivo A Sistemi Informatici O Telematici Con Particolare Riferimento Alla Tutela Dei Dati Personali,
<http://www.diritto.it/materiali/tecnologie/tesina.pdf> (kontrol tarihi 15.07.2006)

- TOPALOĞLU, Mustafa** Bilişim Hukuku, 1. Baskı, 2005.
- TOROSLU, Nevzat** Ceza Hukuku Genel Kısım, 8. Baskı, Ankara, 2005.
- TOROSLU, Nevzat** Cürümlerin Tasnifi Bakımından Suçun Hukuki Konusu, Ankara Üniversitesi Yayınları No:273, Ankara 1970.
- TOROSLU, Nevzat** Ceza Hukuku Özel Kısım, 1. Baskı, Ankara, 2005.
- TOSUN, Öztekin** *Özel Hayatın Gizliliğini İhlâl Suçları* Değişen Toplum ve Ceza Hukuk Karşısında TCK'nın 50 Yılı ve Geleceği Sempozyumu, İstanbul, 1977, s. 371 – 437.
- TRUBOW, George B.** *Protecting Informational Privacy in the Information Society*, 10 N. Ill. U. L. Rev. (1989-1990), pp. 521 – 542.
- ÜNVER, Yener** Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer, Ankara, 2003.
- ÜNVER Yener** *Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi*, İHFM, C. LIX, S. 1-2, 2001, s. 51- 146.

- VANDEVELDE, Kenneth J.** *The New Property of Nineteenth Century: The Development of Modern Concept of Property*, 29 Buff. L. Rev. 1980, pp. 325 – 367.
- WACKS, Raymond** *Personal Information: Privacy and the Law*, Clarendon Press, Oxford 1989.
- WALDEN, Ian** *Anonymising Personal Data*, International Journal of Law and Information Technology, Vol. 10, No.2, pp. 224-237.
- WALL, David S.** *Cybercrimes and Internet*, Crime and the Internet, Edit: David S. Wall, Routledge, 2003, pp. 1 – 17 (Ebrary)
- WALLACE, Wang** *Steal This Computer Book 3: What They Won't Tell You About the Internet*, San Francisco, 2003. (Ebrary)
- WARE, Willis H.** *Privacy and Information Technology-The Years Ahead*, Computers and Privacy in the Next Decade, Edit. Lance J. Hoffman, Academic Press 1980, pp. 9 – 22.
- WARREN, Samuel D. –**
BRANDEIS, Louis D. *The Right to Privacy*, 4. Har. L Rev, 1890 – 1891, pp. 193 – 220.

- WASIK, Martin** *Following in American Footsteps? Following Computer Crime Developments in Great Britain and Canada*, 14 N. Ky. L. Rev. 1997-1998, pp. 249-262. (Heinonline)
- WESTIN, Alan F** *Privacy and Freedom*, New York. 1970.
- WHARTON, Leslie** *Comment: legislative Issues in Computer Crime*, 21 Harv. J. On Legis 1984, pp. 239 – 254. (Heinonline)
- WOLF, Jonathan B.** *War Games Meets The Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money*, 28 Am. J. Crim. L. (1995), pp. 95 – 117. (Heinonline)
- YAZICIOĞLU, Yılmaz** *Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı*, Uluslararası İnternet Hukuku Sempozyumu, 21-22 Mayıs 2001, İzmir, Dokuz Eylül Üniversitesi Yayını, 2002, s. 451-470.
- YAZICIOĞLU, Yılmaz** *Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları İle*. 1. Baskı 1997.
- YAZICIOĞLU Yılmaz** *Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi*, Yeditepe Hukuk Fakültesi Dergisi, C. 2, S. 2, 2005, s. 393 – 412.

YENİDÜNYA, A.Caner –

DEĞİRMENCİ, Olgun

Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, 1. Baskı, 2003.

YILMAZ, Halit

İdarenin Görsel – İşitsel İletişim Alanındaki İşlevi, Ankara, 2006.

YILMAZ, Davut

Hacking, Bilişim Korsanlığı ve Korunma Yöntemleri, İstanbul, 2004.

ZEVKLİLER, Aydın

Medeni Hukuk:Giriş ve Başlangıç Hükümleri, Kişiler Hukuku, Aile Hukuku, Savaş Yayınları, 3. Basım. 1992.

The Knowledge-Based Economy, Paris, OECD.
OCDE/GD(96)102. OECD,
<http://www.oecd.org/dataoecd/51/8/1913021.pdf>.
(kontrol tarihi 05.01.2006)

OECD Guidelines on the Protection of Privacy
and Transborder Flows of Personal Data,
www1.oecd.org/publications/e-
book/9302011E.PDF. (kontrol tarihi 01.06.2005)

An Overview Of Computational Science, “3 A
Brief History of Computer Technology”
http://www.ipp.mpg.de/de/for/bereiche/stellarator/Comp_sci/CompScience/csep/csep1.phy.orml.gov/ov/node8.html#SECTION00030000000000000000. (kontrol tarihi 03.02.3006)

Türk Ceza Kanunu Öntasarısı, Adalet
Bakanlığı Yayın İşleri Daire Başkanlığı, Özel
Seri: 3.

Privacy and Human Rights 2002: An l Survey of
Privacy Laws and Developments,
<http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf>. (kontrol tarihi 13.03.05)

Privacy and Human Rights 2004 An
International Survey of Privacy Laws and
Developments (PHR2004)
<http://www.privacyinternational.org/> (kontrol
tarihi 28.03.2004)

Türkiye Bilişim Şûrası, Ankara, 2002.

An Overview Of Computational Science, “3.2
First Generation Electronic Computers (1937-
1953)”
http://www.ipp.mpg.de/de/for/bereiche/stellarator/Comp_sci/CompScience/csep/csep1.phy.ornl.gov/ov/node10.html#SECTION00032000000000000000. (13.04.2006)

Bilgisayar Aşkımız 60 Yaşında, Bilişim, Yıl 35,
S. 93, s. 20 -23.

The Journey InsideSM: History of Computers
http://www97.intel.com/discover/images/tji/TJI_Intro_back.pdf. (kontrol tarihi 10.11.2006)

Timeline of Computing History
http://www.computer.org/portal/cms_docs_computer/computer/timeline/timeline.pdf. (kontrol tarihi 08.07.2006)

Records, Computers and the Rights of Citizens,
Report of the Secretary's Advisory Committee
on Automated Personal Data Systems, 1973:
Transmittal Letter and Foreword
<http://aspe.os.dhhs.gov/datacncl/1973privacy/foreword.htm>. (kontrol tarihi 10. 10. 2006)

Avrupa İçin Bir Anaysa Oluşturan Antlaşma,
Ankara Barosu, 2005.

The Computer Crime and Intellectual Property
Section United States Department of Justice:
The National Information Infrastructure
Protection Act of 1996: Legislative Analysis,
http://www.usdoj.gov/criminal/cybercrime/1030_anal.html. (kontrol tarihi 02.08.2005)

Creating a Safer Information Society by
Improving the Security of Information
Infrastructures and Combating Computer-related
Crime,

http://eur-lex.europa.eu/LexUriServ/site/en/com/2000/com2000_0890en01.pdf. (kontrol tarihi 01.06.2006)

Güncel Türkçe Sözlük, <http://www.tdk.gov.tr>

Bilgisayar Terimleri Karşılıklar Kılavuzu
<http://www.tdk.gov.tr/bilterim>

The Difference Between a Virus, Worm and Trojan Horse,
<http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>.

Logic Bomb
http://www.webopedia.com/TERM/l/logic_bomb.html.

Convention on Cybercrime, Explanatory Report
<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Infotmatique, <http://www.techno-science.net/?onglet=glossaire&definition=162>.

Informatics,
<http://en.wikipedia.org/wiki/Informatics>

Bilişim,
<http://tr.wikipedia.org/wiki/Bili%C5%9Fim>