FATİH SULTAN MEHMET VAKIF ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU PROGRAMI

TÜRK CEZA HUKUKUNDA BİLİŞİM SUÇLARI (TCK. M. 243-244 VE 245)

YÜKSEK LİSANS TEZİ

NECMETTİN YAZICI

İSTANBUL, 2021

FATİH SULTAN MEHMET VAKIF ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU PROGRAMI

TÜRK CEZA HUKUKUNDA BİLİŞİM SUÇLARI (TCK. M. 243-244 VE 245)

YÜKSEK LİSANS TEZİ

NECMETTİN YAZICI
(180151007)

Danışman
(Prof. Dr. Murat Balcı)

İSTANBUL, 2021

FATİH SULTAN MEHMET VAKIF ÜNİVERSİTESİ
TEZ ONAY FORMU

30/06/2021

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Kamu Hukuku Anabilim Dalı'nda 180151007 numaralı Necmettin YAZICI'nın hazırladığı "Türk Ceza Hukukunda Bilişim Suçları (TCK. M. 243-244 ve 245" konulu Yüksek Lisans tezi ile ilgili Tez Savunma Sınavı, 30/06/2021 Çarşamba günü saat 14:00 'da yapılmış, sorulara alınan cevaplar sonunda adayın tezinin **KABULÜNE** karar verilmiştir.

Düzeltme verilmesi halinde:
Adı geçen öğrencinin Tez Savunma Sınavı tarihinde, saat : da yapılacaktır.

Tez Adı Değişikliği Yapılması Halinde: Tez adının ……
……..
şeklinde değiştirilmesi uygundur.

Jüri Üyesi	Tarih	İmza
(Danışman) Prof. Dr. Murat BALCI	30/06/2021	**KABUL**
Doç. Dr. Hüseyin AYDIN	30/06/2021	**KABUL**
Dr. Öğ. Üyesi Kerim ÇAKIR	30/ 06/2021	**KABUL**

BEYAN/ ETİK BİLDİRİM

Bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, tezin herhangi bir kısmının bağlı olduğum üniversite veya bir başka üniversitedeki başka bir çalışma olarak sunulmadığını beyan ederim.

NECMETTİN YAZICI

TÜRK CEZA HUKUKUNDA BİLİŞİM SUÇLARI (TCK. M. 243-244 VE 245)

Necmettin Yazıcı

ÖZET

Bilişim sistemleri ile birlikte toplumların ve devletlerin bilişim sistemlerini kullanması sonucunda hukuksal sorunlar ve reform ihtiyaçları ortaya çıkmaktadır. Bilişim hukukunun ortaya çıkmasıyla birlikte bilişim suçlarının önüne geçilmesi adına ulusal ve uluslararası hukukta bir takım düzenlemeler yapılmaya başlanmıştır.

Bu çalışmanın birinci bölümünde bilişim kavramı, sistemleri ve suç çeşitleri incelenmiştir. Çalışmanın devamında 5237 Türk Ceza Kanunu ile düzenlenen *"Bilişim Alanında Suçlar"* bölümü, Türk hukukundaki düzenlemeler, yargı kararları ve uluslararası kuruluşların ve devletlerin bilişim hukuku alanında ortaya koyduğu hukuksal reformların incelenmesi ışığında detaylı bir şekilde ele alınmıştır.

Anahtar Kelimeler:

Bilişim, Bilişim Sistemleri, Bilişim Suçları, Hukuksal Düzenlemeler, Türk Ceza Kanunu.

CYBER CRİMES ON TURKİSH PENAL CODE
(TPC. ART. 243-244 AND 245)

Necmettin Yazıcı

ABSTRACT

Along with the information systems, legal problems and reform needs arise as a result of the use of information systems by societies and states. With the emergence of the IT law, a number of regulations have been made in national and international law in order to prevent cyber crimes.

In the first part of this study, the concept of informatics, systems and crime types are examined. In the subsequent of the study, the "Crimes in the Field of Informatics" section, which is regulated by the 5237 Turkish Penal Code, was discussed in detail in the light of the regulations in Turkish law, judicial decisions and the examination of the legal reforms which put forward by international organizations and states in the field of IT law.

Key Words:

Informatics, Information Systems, Cyber Crimes, Legal Arrangements, Turkish Penal Code

ÖNSÖZ

Bilişim sistemlerinin gelişmesi ve bilişim teknolojilerin kullanılmasının yaygınlaşması ile birlikte bilişim suçlarının her geçen gün arttığı bir teknoloji çağı yaşanmaktadır. Teknolojinin her alanı kucaklaması ile bilişim sistemlerinin tanınması ve korunması, adaletin her alanda tecil etmesi adına önem taşımaktadır. *"Fiat iustitia nec pereat mundus"* ilkesi gereği dünya değişse bile adaletin gerçekleşmesi esastır. Bilişim alanında işlenen suçların gerçek dünyada işlenen suçlardan herhangi bir farkı yoktur. Değişen dünyanın bir zorunluluğu ve artık ayrılmaz bir parçası olan bilişim sistemleri kullanıcıları için hayati bir önem taşıdığı gibi büyük bir konfor ve fayda alanı sunmaktadır. Ancak aynı doğrultuda oluşan suç unsurları nedeniyle kullanılacıların temel hak ve özgürlüklerine gölge düşürecek hukuki problemler hızla artış göstermektedir. İşte bu nedenle bilişim suçlarının derinlemesine incelenmesi ve kullanıcıların haklarının doğru ve eksiksiz bir şekilde savunulması adına bilişim alanında hukuksal çalışmalara her geçen gün artan ihtiyaç hali hasıl olmuştur.

İşbu çalışmayla hızla yayılan ve insanlığın ortak sorunu haline gelen bilişim suçlarının kavramları, tarihi, evrensel hukuk reformları ve Türk Hukuku'ndaki yerinin incelenmesi üzerine çalışılmıştır.

Lisans ve lisansüstü eğitim dönemim ve meslek hayatım boyunca desteği, rehberliği ve güveni ile her zaman yanımda olan saygıdeğer hocam, Sayın Prof. Dr. Murat Balcı'ya, çalışma sürecinde fikirleri ve tavsiyeleri ile ışık tutan Muhammed Talha Kaan, Akif Emre Aktaş ve Samandağ Cumhuriyet Savcısı Muhammed Nesih Gözcü'ye, her koşulda yardım ve inancını esirgemeyen değerli eşim Zeynep Rabia Yazıcı'ya ve maddi manevi desteklerini her zaman hissettiğim kıymetli aileme teşekkürlerimi arz ederim.

İÇİNDEKİLER

ÖZET ..... **iv**

ABSTRACT ..... **v**

ÖNSÖZ ..... **vi**

KISALTMALAR ..... **xi**

GİRİŞ **1**

BİRİNCİ BÖLÜM **4**

1. BİLİŞİM SİSTEMLERİ VE BİLİŞİM HUKUKU İLE İLGİLİ GENEL KAVRAMLAR VE AÇIKLAMALAR **4**

1.1. GENEL BİLGİLER **4**

1.2. BİLİŞİM KAVRAMI ve TEMEL KAVRAMLAR **6**

1.2.1. Bilişim Kavramı **6**

1.2.2. Temel Kavramlar **8**

1.2.2.1. Bilgisayar 9

1.2.2.2. İnternet 10

1.2.2.3. Bilgisayar Programı 12

1.2.2.4. Bilgisayar Verisi 12

1.2.2.5. IP Adresi 13

1.2.2.6. Donanım 14

1.2.2.7. Yazılım 14

1.2.2.8. Bulut Bilişim 14

1.3. BİLİŞİM SİSTEMLERİNİN GELİŞİMİ **15**

1.4. BİLİŞİM SUÇLARININ TANIMI **17**

İKİNCİ BÖLÜM **20**

2. BİLİŞİM SUÇLARININ TASNİFİ, BİLİŞİM HUKUKUNUN ÖNEMİ ve HUKUKSAL DÜZENLEMELER **20**

2.1. BİLİŞİM SUÇLARININ TASNİFİ **20**

2.1.1. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin Getirdiği Tasnif 20
2.1.2. Avrupa Birliği ve Birleşmiş Milletler Komisyonu Ortak Raporu'nun Getirdiği Tasnifler 21
2.1.3. Avrupa Ekonomik Topluluğunun Getirdiği Tasnifler 23
2.1.4. Birleşmiş Milletler 'in Getirdiği Tasnifler 23
2.1.5. 5237 Sayılı Türk Ceza Kanunu'nda Geçen Tasnifler 24
2.2. BİLİŞİM HUKUKUNUN ÖNEMİ 25
2.3. HUKUKSAL DÜZENLEMELER 25
2.3.1. Ulusal Düzenlemeler 25
2.3.1.1. 765 Sayılı (Eski) Türk Ceza Kanunundaki Düzenlemeler 27
2.3.1.2. 5237 Sayılı Türk Ceza Kanunundaki Düzenlemeler 30
2.3.1.3. Fikir ve Sanat Eserleri Kanunu 33
2.3.1.4. Elektronik İmza Kanunu 34
2.3.1.5. İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 36
2.3.1.6. Tüketicinin Korunması Hakkında Kanun 38
2.3.1.7. 7258 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkındaki Kanun 38
2.3.2. Uluslararası Düzenlemeler 41
2.3.2.1. Fransa 44
2.3.2.2. Almanya 45
2.3.2.3. İngiltere 46
2.3.2.4. İtalya 47
2.3.2.5. Amerika Birleşik Devletleri 48
2.3.2.6. Japonya 50
ÜÇÜNCÜ BÖLÜM 52
3. 5237 SAYILI TÜRK CEZA KANUNU MADDE 243,244 ve 245'in İNCELENMESİ 52
3.1. BİLİŞİM SİSTEMİNE GİRME VEYA SİSTEMDE KALMA SUÇU (M.243) **..... 52**
3.1.1. Genel Olarak 52
3.1.2. Korunan Hukuki Yarar 53

3.1.3. Suçun Maddi Unsurları 55
3.1.3.1. Fail 55
3.1.3.2. Mağdur 55
3.1.3.3. Suçun Konusu 56
3.1.3.4. Hareket 57
3.1.3.5. Netice 64
3.1.4. Suçun Manevi Unsurları 65
3.1.5. Hukuka Aykırılık 65
3.1.6. Kusurluluk 66
3.1.7. Suçun Özel Görünüş Biçimleri 67
3.1.7.1. Teşebbüs 67
3.1.7.2. İştirak 68
3.1.7.3. İçtima 68
3.1.8. Yaptırım 70
3.2. BİLİŞİM SİSTEMİNİN ENGELLENMESİ VEYA BOZULMASI SUÇU İLE VERİLERİN YOK EDİLMESİ VEYA DEĞİŞTİRİLMESİ SUÇU (M.244) **71**
3.2.1. Genel Olarak 71
3.2.2. Korunan Hukuki Yarar 72
3.2.3. Suçun Maddi Unsurları 74
3.2.3.1. Fail 74
3.2.3.2. Mağdur 74
3.2.3.3. Suçun Konusu 74
3.2.3.4. Hareket 75
3.2.3.5. Netice 77
3.2.4. Hukuka Aykırılık 78
3.2.5. Kusurluluk 78
3.2.6. Suçun Özel Görünüş Biçimleri 79
3.2.6.1. Teşebbüs 79
3.2.6.2. İştirak 79
3.2.6.3. İçtima 79
3.2.7. Yaptırım 80

3.3. BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI SUÇU (M.245) **81**
3.3.1. Genel Olarak **81**
3.3.2. Şahsi Cezasızlık Sebepleri ve Cezayı Kaldıran veya Azaltan Şahsi Sebepler **83**
3.3.3. Korunan Hukuki Yarar **84**
3.3.4. Suçun Maddi Unsurları **85**
3.3.4.1. Fail 85
3.3.4.2. Mağdur 86
3.3.4.3. Suçun Konusu 87
3.3.4.4. Hareket 88
3.3.4.5. Netice 89
3.3.5. Hukuka Aykırılık **89**
3.3.6. Kusurluluk **90**
3.3.7. Suçun Özel Görünüş Biçimleri **90**
3.3.7.1. Teşebbüs 90
3.3.7.2. İştirak 92
3.3.7.3. İçtima 93
3.3.8. Yaptırım **100**
SONUÇ **102**
KAYNAKÇA **107**

KISALTMALAR

a.g.e.	Adı geçen eser
ABD	Amerika Birleşik Devletleri
ACK	Alman Ceza Kanunu
ASSS	Avrupa Siber Suç Sözleşmesi
ATM	Bankamatik (Automatic Teller Machine)
BM	Birleşmiş Milletler
C.	Cilt
CCIPS	Computer Crime and Intekkectual Prooerty Section
CFAA	Computer Fraud and Abuse Act
CMA	Computer Misuse Art
çev.	Çeviren
E.	Esas
EİK	Elektronik imza Kanunu
FCK	Fransız Ceza Kanunu
FSEK	Fikir ve Sanat Eserleri Kanunu
H.D.	Hukuk Dairesi
IP	Internet Protocol Address
K.:	Karar
md.	Madde
ODTÜ	Orta Doğu Teknik Üniversitesi
s.	Sayfa/sayfalar
TBB	Türkiye Barolar Birliği
TC	Türkiye Cumhuriyeti
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
vb.	Ve benzeri
VPN	Sanal Özel Ağ (Virtual Private Network)

GİRİŞ

Bilinen tarihten itibaren insanlık hep bir arayış içerisinde olmuştur. Bu arayışlar tarihten bu yana genellikle aynı doğrultularda yönlenmiştir. Yaşam ve yaşamaya yönelik ihtiyaçlarını giderme adına hayatta kalma arzusu, birlikte yaşama güdüsü ve toplum olmanın gereği devlet ve adalet arayışı ile eğlenme ve hayattan keyif bulma dürtüsü insanlığın ve toplumların gelişimini etkileyen en temel faktörler olmuştur. Bu arayışlar neticesinde insanlık tarihinde icatlar bulunmuş, çağlar değişmiş, savaşlar ve devrimler ile tarihe yön verilmiştir.

Kuşkusuz insanlık tarihinin gelişimi incelendiğinde, gelişim ve değişim çizgisinin en büyük kırılmaları çağımızda yaşanmıştır. Bu kırılma tarihteki kırılmalara nazaran o kadar sert ve hızlı olmuştur ki çağımıza "Bilişim Çağı" ya da "Teknoloji Çağı" denmektedir. Dolayısıyla bilişim ve teknoloji alanında yaşanan gelişmeler ve bu alanların hayatı kapsayıcı bir rol edinmesiyle birlikte bu çağdaki nesiller "Teknoloji Nesli" olarak anılmaya başlamıştır. Bunun en büyük sebebi, neredeyse kırk yıl önce hayatımıza giren ve hayatımızın büyük bir alanını işgal eden bilişim ve teknolojinin gelmiş olduğu seviyedir.

Çok daha basit amaçlar için üretilmiş olan bilgisayarlarından, iletişimin kolaylaşması adına icat edilmiş olan cep telefonlarına bilişim sistemleri ve aletlerinin gelmiş olduğu nokta bir kuşak öncesinde dahi tahmin edilemeyecek bir seviyededir. Bililişim sistemleri artık kişilerin hayatındaki özel veye kurumsal olarak yapabileceği tüm işlemleri neredeyse bir tuş ile insanlığın önüne serebilmektedir. Resmi devlet işlerinden ticari işlere, özel ilişkilerden mesleki faaliyetlere tüm iş ve işlemler, geliştirilen bilişim metodları ile bu alanında icra edilebilmektedir.

Belirtilen seviyede büyüyen ve hayatın her alanını kapsayan bu sistemlerin insanlığa faydalarının gelişimine paralel olarak tahrip edebileceği alanlar da büyümektedir. Nasıl ki klasik hayatında gerçekleştirdiği iş veya işlemlerde kişiler kişisel haklarının ve hukukunun devlet ve adalet sistemleri aracılığıyla korunmasını istiyor ve ihtiyaç duyuyorsa, artık hayatların ikame edildiği bilişim alanında da bu güvencelerin verilmesi ve bu güvencelerin bilişim alanlarının gelişimiyle birlikte güncelliğini koruması elzem hale gelmiştir. Öyle ki, nasıl insanlık ihtiyaçlarını karşılamak arayışı doğrultusunda teknolojinin bu seviyeye gelmesini istemişse ve sağlamışsa, toplumlar içerisinde huzurla yaşamak ve haklarını aramak için de hukuk ve adalet sistemlerinin bu doğrultuda gelişmesine ve güncellenmesine ihtiyaç duymaktadır. Böylece bilişim suçlarının düzenlenmediği hukuk sistemleri artık hayatın olağan akışına uygun olmayan ve adalete olan güvenin kaybedileceği sistemler olacaktır.

Bilişim suçlarının işlenme alanı olan bilişim sistemlerinin sınırsızlığı, herhangi bir ulusal norma bağlı kalmadan yeryüzünün her yerinde bilişim suçlarının işlenebilir olması ve herhangi bir kitlenin değil de tüm insanlığın bu suçların hedefi olabileceği hukuk sistemleri açısından oldukça güç ve değişime açık bir alan oluşturmaktadır. Bilişim sistemlerinin gelişmesiyle birlikte devletler ve uluslararası kuruluşlar bu yönde adımlar atmış ve hukuksal reformlar hukuk tarihinde yer almaya başlamıştır.

Bu çalışmada da, bilişim suçlarının Türk Ceza Kanunu'nun içerisinde düzenlenmesi ve detaylı incelenmesi yapılacaktır. Çalışmanın daha kapsayıcı ve anlaşılabilir olması adına birinci bölümde bilişim sistemleri ve bilişim hukuku ile ilgili temel kavramlar bilişim sistemlerinin tarihi ile birlikte incelenecektir. Bu bölümde bilişime yönelik tüm kavramların ve bilişim sistemlerinin gelişimi, ulusal ve uluslararası hukuklar incelenerek ele alınacaktır.

İkinci bölümde ise bilişim suçlarının tasnifi, işlenme şekilleri ve bilişim suçlarına yönelik hazırlanan ulusal ve uluslararası düzenlenemeler işlenecektir. Bilişim suçlarına yönelik getirilen çeşitli tasnifler ve bilişim suçlarının işlenme şekillerinin incelenmesi ile bu suçların ceza hukuku açısından önemi değerlendirilmeye çalışılacaktır. Bölümün sonunda ise bilişim suçlarına yönelik mukayeseli hukukta yapılan düzenlemeler detaylı bir şekilde incelenerek, hukukumuzda bilişim suçlarına yönelik yapılan reformlar ele alınacaktır.

Çalışmanın son bölümünde ise Türk Ceza Kanunu'nda bilişim suçlarına yönelik doğrudan düzenlenmiş olan 243., 244. Ve 245. Maddeler Ceza hukuku ve bilişim sistemleri açısından tüm unsurlarıyla ele alınacaktır.

BİRİNCİ BÖLÜM

1. BİLİŞİM SİSTEMLERİ VE BİLİŞİM HUKUKU İLE İLGİLİ GENEL KAVRAMLAR VE AÇIKLAMALAR

1.1. GENEL BİLGİLER

İnsanlığın var olmasıyla birlikte insanoğlunun toplu yaşama gayesi ve ihtiyacı da var olmuştur. Bu gaye ve ihtiyacın neticesinde, çeşitli zorunluluklar meydana gelmiştir. Bilişim sistemlerinin başlangıç noktası olarak, insanlığın ilk ihtiyaçlarından ötürü ortaya koyduğu icatlar değerlendirmeye alınabilmektedir. Şüphesiz ki insanoğlunun doğasından gelen ilk büyük icatlarından bir tanesi, oluşturduğu hukuk sistemidir. Yazının olmadığı, devlet sistemlerinin kurulmadığı topluluklarda bile içgüdüsel olarak tesis edilen ilk sistem hukuk sistemidir. Öyle ki insanlar, birlikte yaşamanın gerekliliği olarak ve bireysel ve toplumsal ihtiyaçlarının giderilmesi adına eşitlik ve adalet arayışı içinde olmuşlardır.

Hukuk kurallarının sistematik halde toplumlar açısından ilk ortaya çıkışı 17. yüzyıl gibi gözükse de milattan sonra 527-565 yıllarında Doğu Roma İmparatoru'nun klasik roma hukukçularının eserleri ile o zamana kadar çıkartılmış hukuki düzenlemeleri bir araya getirip toplattığı "Corpus Iuris Civilis" bilinmektedir. Bu dokümanla, dönemin Roma Hukuku'na dair bilgiler edinmekteyiz. Bu bilgiler ışığında, bu dönemden öncesinde dahi hukuki bilgi ve belgeleri ve hukuk sitemlerinin var olduğu apaçık bir şekilde anlaşılmaktadır.

İnsanoğlunun doğası gereği ortaya çıkardığı hukuk sistemleri, toplumların gelişmesi ve kalabalıklaşmasıyla birlikte uyumlu halde değişmiş ve sistematik hale gelmiştir. Çağlar ilerledikçe, devlet sistemleriyle tümleşik hale gelen hukuk ve adalet kavramları, insan davranışlarını, devlet sistemlerini ve zamanla artık ticaret işlerinden aile kuramına, doğadan hayvan haklarına kadar geliştirilmiş ve düzenleme alanını

genişletmiştir. Zamanla, hukuk düzenleri daha sistematik hale gelmiş hukuki yapılar ve kurumlar ortaya çıkmıştır.

Hukuk, her dönemde insanların ihtiyaçları ve devletlerin sistemlerine göre değişim göstermiş temelde olan adalet arayışının sonuçları toplumlar üzerinde çok farklı tezahürler ile ortaya çıkabilmiştir. Bu değişikliklerin ana sebebi, toplumların ve inançlarının getirileri ile farklılıkları olsa da çağların değişimi ile duyulan ihtiyaçların şekillenmesi, farklılaşması ve yaygınlaşmasıdır. Nihayet, hukuk sistemlerinin insanla ve toplumla birlikte değişmesi, gelişmesi ve uyum sağlaması, ortaya çıkış sebebi gereği zorunlu hale gelmiştir.

Devletler ve toplumlar tarihi incelendiğinde bilimin gelişimi doğrultusunda icatlar ve buluşlar ile birlikte toplumların ihtiyaçlarının ve haklarının değiştiği, bununla birlikte yeni sistemlere ihtiyaç duyulduğu görülmektedir. Muhakkak ki insanlık tarihinin en büyük kırılmalarını yaşadığı dönemlerden bir tanesi de teknolojinin gelişmesi ve icatların hızlı bir şekilde değişmesidir. Her ne kadar toplumlarda hakkın öz manası kendisini korumuş olsa da, bu mananın çevresinde tesis edilen sistemler ve koruma yöntemleri gelişen ve değişen dünya düzenleri ile birlikte kapsayıcılığını artırmak zorunda kalmıştır. Hukukun temel koruma alanları olan ekonomik, sosyal, siyasal alanlar, teknoloji ile değişime uğramış ve teknolojiden bağımsız düzenlenemeyecek hale gelmiştir. Hukukun kapsama alanına giren hakların korunmasında delil niteliği taşıyan bilgi ve belgelerin de artık teknolojik ve bilişim alanlarında incelenmesi 2000'lerden sonra zorunlu hale gelmiştir. Teknolojiyle birlikte toplumların bu alandaki hukuki düzenlemeler üzerine eğilimleri ve bu düzenlemelerin kaçınılmazlığı değişime ayak uyduran toplumların huzur ve adalet tesisi için farklılıklar ortaya koymuştur.

1.2. BİLİŞİM KAVRAMI ve TEMEL KAVRAMLAR

1.2.1. Bilişim Kavramı

Temel olarak Bilişim hakkında doktrinde net bir tanım ile karşılaşılmaması ile birlikte birçok farklı tanım karşımıza çıkmaktadır. Bilişim kavramının tanımları incelenmeye başlandığında ilk olarak Türk Dil Kurumu'nun 1981 tarihli Bilişim Terimleri Sözlüğü 'ne bakılacak olursa, bilişim; "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, .Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararını gözeterek inceleyen uygulamalı bilim dalı. "* [1] Tanımıyla karşılaşılmaktadır.

Bilişim sözcüğünün kökenine bakıldığında ise, Fransızca informatique, İngilizcede informatics olarak karşımıza çıkmış, dilimize bilişim kavramı ile geçiş yapmıştır. Bilişim kavramı, bilgi ile matematik kavramlarının birleşiminden oluşmuştur.[2]

Bilişim kavramına doktrinde getirilen tanımlara bakılacak olursa, Dr. Metin Turan bilişimi: *"Genel olarak elektronik olmak üzere, dijital, sanal vb. ortamlarda veri ya da bilgilerin belirli biçimlerde, belirli mantıklarla ya da sistematik, belirli düzenlerde ve sıralarda otomatik olarak (tam ve kısmen) işlenmesidir*." [3] olarak belirtmiştir. Yine, bilişim: "Bilginin makinelerce işlenmesi ve aktarılmasının bilimi, tekniği ve uygulaması" [4] olarak da tanımlanmaktadır.

Diğer bir tanıma göre bilişim: *"İnsanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla*

---

[1] Aydın Ünsal, **"Bilişim Terimleri Sözlüğü"**, Türk Dil Kurumu Yayınları, Ankara, Ankara Üniversitesi Basımevi, 1981, s. 28

[2] Ali Parlar, **"Türk Ceza Hukukunda Dolandırıcılık Suçları"**, 2. Baskı, Bilge Yayınevi, Ankara, 2015, s.172

[3] Metin Turan, **"Bilişim Hukuku",** Seçkin Yayınevi, 4. Baskı, s.47

[4] Heinrich Müller ve Frank Weichert, **"Vorkurs Informatik Der Einstieg ins Informatikstudium",** Springer Fachmedien, s.1, (Aktaran) Turan, s. 46

düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir."[5]

Başka bir tanımda ise bilişim: *"Bilginin ve iletişim yapısı ve özellikleri, bilginin aktarılması, organize edilmesi, saklanması, tekrar elde 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 teknolojileri temel alan bilgi sistemleri, şebekeleri, süreçleri ve etkinlikleri"* [6] şeklinde açıklanmaktadır.

Bir diğer tanımlamaya göre ise bilişim: *"Bilgisayar, çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, Mouse, klavye, kulaklık, yazıcı vb) iletişim altyapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan veri saklama ve iletmeye yönelik sistemi ifade eder."*[7] denmektedir.

Türk Ceza Kanunu, Bilişim kavramının açıklaması ile ilgili incelendiğinde iki yönden ele alınmalıdır. 765 sayılı Eski Türk Ceza Kanunu'nda bilişim sistemleri ile ilgili açıkça bir tanım bulunmamaktadır. Ancak 525. maddede yüzeysel bir tanımlama yapılmaktadır. Bu tanımlamaya göre bilişim sistemi: *" Bilgileri otomatik olarak işleme tabi tutmuş bir sistem" olarak geçmektedir. 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'na göre ise 243. maddede bilişim sistemi: "Verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işlemlere tabi tutma olanağı veren manyetik sistemler"* olarak tanımlanmaktadır.

Yargıtay Kararları incelendiğinde ise Bilişim ile ilgili tanımlamalar ile karşılaşmaktayız. Örneğin, Yargıtay Ceza Genel Kurulu 2006/E-136 E., 2007/150 K. Numaralı kararında: "*Bilişim sözcüğü ise, bilginin otomasyona tabi tutulması sonucunda işlenmesini, başka deyişle, verinin saklanması, organize edilmesi,*

---

5 Murat Volkan Dülger; **"Bilişim Suçları ve İnternet İletişim Hukuku"**, Ankara, Seçkin Yayınevi, 6. Baskı, Eylül 2015, s. 75

6 D. Emin AYDIN, **"Bilişim Suçları ve Hukukuna Giriş",** Doruk Yayınevi, s. 3

7 Murat Volkan DÜLGER; Gözde MODOĞLU, **"Bilişim Suçları, Soruşturma Ve Kovuşturma Yöntemleri İle İnternet Ve İletişim Hukuku Uygulama Rehberi",** s. 25, (Çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2564591 Erişim Tarihi:30.04.2021

değerlendirilmesi, nakledilmesi, çoğaltılmasını da kapsamaktadır." bu tanımlamalardan bir tanesidir.

Özetle, bilişim hakkında doktrinde birçok tanımla karşılaşsak da tanımlamalarının temelinde özellikle karşımıza çıkan birtakım kavramlar vardır. Bu kavramlar; bilgi, bilgisayar, iletişim, veri, verilerin işlenmesi, verilerin korunması, verilerin saklanması, verilerin hesaplanması, verilerin aktarılmasıdır. Bilişim denince akla gelen en önemli terimlerin ortak noktası ise bilgisayar ve teknoloji olarak karşımıza çıkmaktadır. Çağımızın en önemli kavramları olan bu terimlerle birlikte, bilgi çağından bilişim ve teknoloji çağına geçişi de görülebilmektedir. Bilişim çağı olarak adlandırılabilen günümüzde ise bilişim sistemlerinin ve bilişim hukukunun önemi ve gerekliliği ortaya çıkmaktadır. Bilişim sistemleri ve teknolojileri ile oluşan bilişim alanında ve bu alanın insan hayatının neredeyse tümünü kapsadığı çağımızda, bu değişim ve gelişimin hukuk kuralları ile birlikte büyümesi ve hukuk kuralları çerçevesinde düzenlenmesi, bu alanın hukukun kapsamına giren bir alan olarak belirlenmesi ve bu kapsamda değerlendirilip analiz edilmesi hak ve adalet kavramlarının her zaman ve her yerde olma prensibine göre önemlilik göstermektedir. Öyle ki, bilişim alanında işlenen suçların önüne geçilmesi, engellenmesi veya bir müeyyide ile caydırıcılığa kavuşturulması, sadece elektronik alanda oluşturulan kurallar ile sağlanamayacaktır. Toplumlar nezdinde böyle bir öneme sahip olan bilişim alanında işlenebilecek suçların karşısında, yasal tanımlamalar getirilmesi gelişen teknoloji ve bilişim alanında artık zorunluluk olarak kabul edilmektedir.

1.2.2. Temel Kavramlar

Bilişim kavramının incelenmesiyle, birçok elektronik kavram ile karşılaşılmaktadır. Bu kavramların tanımı bilişim kavramının ve bilişim suçlarının anlaşılmasında önemli bir rol oynamaktadır. Zikredilen bilişim sistemlerinin kullanılması ve bilişim suçlarının işlenmesinde temel rol oynayan bu kavramlardan bazıları aşağıda zikredilmiştir.

1.2.2.1. Bilgisayar

Bilgisayar, kelime manası olarak hesaplama yapan, hesaplayıcı, otomatik hesaplayıcı manasını taşımaktadır. Türk Dil Kurumu'nda bilgisayar: *"Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin."*[8] Olarak tanımlanmaktadır.

Bir diğer tanıma göre bilgisayar: *"Belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen masaüstü, dizüstü bilgisayarlar, cep telefonu ve benzeri tüm elektronik araçları ifade ederi. Bilgisayarın elektronik kısmına donanım (Hardware), program kısmına ise yazılım (Software) denir."*[9] Olarak tanımlanmaktadır.

Bilgisayar, modern bilgisayarın babası olarak anılan Charles Babbage tarafından 1833 yılında tasarlanarak insanların hayatında yer edinmeye başladı. Babbage, ürettiği bu icadını 1870 yılına kadar geliştirdi. Aslında bu icat, günümüz bilgisayarlarının temeli olan abaküsün makine haliydi. Toplama ve çıkarma gibi basit işlemler yapan bu makine, 1944-1945 yıllarında günümüz bilgisayarlarının atası olan dijital haline kavuştu. 1944'te IBM firmasıyla birlikte çalışan Harvard Üniversitesi'nden Howard Hattaway Aiken'in tasarladığı MARK-IC ve Pensilvanya Üniversitesi'nden John Presper Eckert ve John William Mauchly'nin tasarladığı ENIAC adı verilen bu dijital bilgisayarların boyutu insandan büyük, ağırlığı tonlar ile hesaplanacak kadar fazla, maliyeti yüz binlerce doları bulabilecek kadar uçuk kalıyordu. 1965 yılına gelindiğinde ise dijital bilgisayarların modernleşme süreci başladı. Zamanla kişisel bilgisayarlar üretilmeye başlandı ve günümüzde hayatın her alanının vaz geçilmez zorunluluğu halini aldı.

Ticaret, Kamusal İşlem, Bilgi Depolama, Hukuki İşlemler gibi birçok alanda artık kullanılmaya başlayan bilgisayar, her geçen gün gelişimine devam etmektedir.

---

[8] Türk Dil Kurumu Sözlüğü, (Çevrimiçi), https://sozluk.gov.tr/ Erişim Tarihi: 23.03.2021

[9] Murat Volkan DÜLGER; Gözde MODOĞLU, a.g.e., s. 25

Bu gelişimle birlikte suç işleme ağının ve yöntemlerinin gelişimi de kaçınılmaz olmaktadır. Bilişim ağında işlenen suçların büyük bir kısmı, her ne kadar alternatifi artmış olsa da bilgisayar kaynaklı gerçekleşmektedir. Bilgisayar ile işlenebilen bilişim suçlarının herhangi bir ulusal sınırının olmaması ve günümüzdeki internet ağının derinliği ile takibinin zorlaşması bu yöntemin kullanılmasını artırmaktadır. Zamanla bilişim kavramı ile bilgisayar kavramı aynı manada kullanılmakta olup birbirlerinin yerini almaktadırlar. Bilişim kavramı başlığında da değinildiği gibi, Bilgisayar kavramı bilişim alanının alt başlığı olarak değerlendirilmeli, özellikle çağımızda bilişim araçlarının çeşitlenmesiyle muadil sayısının çok arttığı ve bu nedenle bilgisayar kavramının bilişim kavramından ayrılması gerektiği görülmektedir. Bilişim alanı; bilgisayar, internet, telefon, pos cihazı vb. araçları kapsamaktadır.

Bilgisayar, temelde donanım, yazılım, internet ve veri gibi unsurlardan oluşmaktadır. Bu unsurlara aşağıda değinilecektir. Bilgisayar, bu unsurlarıyla birlikte bilişim suçlarında hatta tüm suçlarda delil olarak değerlendirilebilmektedir. Günümüzde en fazla değerlendirilen adli bilişim yöntemi Bilgisayarlardır. Suçun tespitinde, aydınlatılmasında, failin veya mağdurun suç sürecindeki hareketlerinin tespit ve tayininde en önemli delillerin, bilgisayarların incelenmesi ile ortaya çıktığı görülmektedir.

1.2.2.2. İnternet

İnternet kavramı, kelime anlamı olarak ağlar arası demektir. İnter (arasında) ve net (ağ) kavramlarının birleşimiyle oluşmaktadır. İnternet tanımlanacak olursa, dünya üzerinde yer alan milyonlarca bilgisayar veya bilişim araçlarının, herhangi bir sınırlamaya tabi olmadan birbirine bağlanmasını sağlayan ağ yapısı olarak belirtmek mümkün olacaktır.[10] İnternetin ortaya çıkışı gelişimiyle birlikte hayatın her alanında

[10] Hasan Sınar, **"İnternet ve Ceza Hukuku"**, 2001, İstanbul, Beta Yayınevi, s.21

kendine yer tutan internet, erişilebilir bilgiye ulaşmanın yolları arasında [11]en hızlı ve tercih edilen aracı yöntem olmuştur.

Toplumların ve devletlerin temel yaşam standartlarını baştan aşağıya değiştiren ve çağın en önemli kavramlarından birisi olan "internet" kavramının tarihine bakıldığında, ilk olarak "ARPANET" tabiri ile karşılaşılacaktır. 1969 yılında, Amerikan Federal Hükümeti Savunma Bakanlığı'nın Savunma İleri Düzey Araştırma Projeleri Kurumu askeri alandaki projeleri desteklemek adına bir ağ çalışması başlattı. Çalışmayla birlikte, zamanla bilgisayarlar arasında bir ağ bağlantısı kuruldu ve bu yolla iletişim sağlanmaya başladı. Ve insanlık bilgisayar ağları kavramı ile tanıştı. 1972 yılında E-Posta dönemi başladı. 20. yüzyılın sonunda artık internet, günümüz modern halini almıştı ve evlerde kişisel bilgisayarlar aracılığıyla kullanılmaya başlanmıştı. Bugün internet kullanan insan sayısı 2 milyarın üzerine ulaşmış bulunmakta.

Türkiye'de ise internet kullanımına 12 Nisan 1993 yılında TUBİTAK, ODTÜ ve EGE Üniversitelerinin öncülüğüyle başlandı. Tüm dünya gibi Türkiye'de de hız kesmeden internet kullanımı yayıldı ve günümüzde, Türkiye İstatistik Kurumunun Ocak 2020 tarihinde yayınladığı son rapora göre internet kullanan bireylerin oranı %79,0 'a ulaştı. Bu rapora göre: "*İnternet kullanım oranı 2020 yılında 16-74 yaş grubundaki bireylerde %79,0 oldu. Bu oran, bir önceki yıl %75,3'tü. İnternet kullanım oranı cinsiyete göre incelendiğinde, bu oranın erkeklerde %84,7, kadınlarda %73,3 olduğu görüldü."* [12]

İnternete evden erişim imkânı ise yine aynı rapora göre %90,7'yi buldu. Bu oran sadece bir önceki yılda %88,3'tü. Bu verilere bakıldığında Türkiye'deki internet kullanımının vardığı ciddi oran göz önüne alınarak bilişim hukuku alanında ulusal düzenlemelerin yapılmasının ve uluslararası düzenlemelerin takip edilmesinin önemi ortaya çıkmaktadır.

---

[11] Ali Nizam, Gökhan Cabiroğlu, **"Yönetici ve Son Kullanıcılar İçin Bilişim",** Mayıs 2014, İstanbul Fatih Sultan Mehmet Vakıf Üniversitesi Yayınları, s.18

[12] Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2020, (Çevrimiçi), https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679 Erişim Tarihi: 20.02.2021

1.2.2.3. Bilgisayar Programı

İnsanların kullanması için tasarlanan bilgisayarlar, komut zincirleri ile çalışmaktadır. İnsanlar, istedikleri işlevleri yerine getirmeleri için bilgisayarlara komutlar vermektedir. İşte bu kod ağına program denmektedir. Bilgisayar cihazına işlevini kazandıran ve insanların kullanımına sunan kod zincirleridir. Bilgisayar programı kavramının bir diğer tanımlarından birisi de 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda geçmektedir. Bilgisayar programları tabirinin kanunlarda ilk düzenlenmesi 1995 yılında olmuştur. Avrupa Birliği uyum görüşmeleri ile yapılan değişiklikler sonucunda, bilgisayar programı kavramının 5846 sayılı Fikir ve Sanat Eserleri Kanunu'ndaki son düzenlemesi Tanımlar bölümünde Madde 1/B'de geçmektedir; "*Bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgisini ve bu emir dizgisinin oluşum ve gelişimini sağlayacak hazırlık çalışmalarını…*"

1.2.2.4. Bilgisayar Verisi

Bilgisayar Verisi, kelime anlamı olarak Bilgisayara girilen ilk bilgi olarak tanımlanmaktadır. Her türlü bilgilerin bilgisayarın komut işleyebileceği hale gelmesi ile veri oluşmaktadır. Bilgisayar ile bu veriler üzerinden işleme, saklama, değiştirme gibi işlemler yapılabilmektedir. Avrupa Konseyi Siber Suç Sözleşmesinin 1. Maddesi'nde belirtilen tanımlamalarda ise bilgisayar verisi: *"Bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsepti ifade edecektir."*[13] Şeklinde düzenlenmiştir. Bilgisayar verileri, kişiler veya kurumlar

[13] Avrupa Siber Suç Sözleşmesi, (Çevrimiçi), https://polis.osce.org/file/11326/download?token=1NGQndqh Erişim Tarihi: 20.02.2021

açısından mahrem bilgilerden veya kamusal sırlardan oluşabilecektir. Özellikle kişisel veriler alanındaki hak ihlallerinin önüne geçilmesi adına uluslararası alanda birçok hukuksal ve teknolojik reformlarda bulunulmuştur. Türkiye'de ise 6698 sayılı Kişisel Verileri Koruma Kanunu ile birlikte kişiler ve kurumların bu verileri koruma huşundaki bilinci ve hassasiyeti artmıştır. [14]

1.2.2.5. IP Adresi

Bilişim teknolojilerinin ve bilgisayar kavramının, hukuku ilgilendiren en önemli alt kavramlarından bir tanesi de IP adresidir. IP Adresi, bilgisayara atanan anal adrese denir. Her bilgisayarın bir adresi yani kimliği vardır. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkındaki Yönetmelik, IP Adresine bir tanım getirmektedir: "*IP Adresi: Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adresi ifade eder*."[15]

Bilişim suçlarındaki en önemli delil unsurlarından birisi olan IP Adresi, suçu ve failin yerini ve kimliğini tespit etmekte büyük ön em taşımaktadır. Başka bir tanıma göre "*İnternete bağlanan her bilgisayara internet servis sağlayıcı tarafından IP adresi atanır ve internetteki diğer bilgisayarlar bu bilgisayara verilen IP adres ile ulaşırlar*."[16] Fakat bu noktada adreslerin failler ile ilişkisinin tespiti de hukuki açıdan ciddi önem taşımaktadır. Bilişim suçu türlerinden bir tanesi de IP Adresi hırsızlığıdır. Failler, IP adreslerini çalma, değiştirme vb. suçlar işleyebilecekken, Başkasının IP Adresini izinsiz ve yetkisiz kullanarak da suç işleyebileceklerdir.

---

[14] Fahrettin Özdemirci, Zeynep Akdoğan, **"Bilgi Sistemleri ve Bilişim Yönetimi, Beklentiler ve Yeni Yaklaşımlar"**, Ankara, 2017, Ankara Üniversitesi Basımevi, s.153

[15] 30 Kasım 2007 Resmî Gazete Yayın Tarihli, 26716 yayın sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik https://www.resmigazete.gov.tr/eskiler/2007/11/20071130-6.htm

[16] Murat Volkan DÜLGER; Gözde MODOĞLU, a.g.e., s. 25

1.2.2.6. Donanım

Donanım (hardware) bilgisayar dendiğinde akla gelen ilk kavramlardan bir tanesidir. Öyle ki donanım, bilgisayarı oluşturan bölümlere denmektedir. Bahsedilen bölümler, bilgisayarı bilgisayar yapan elle tutulabilir fiziki, maddi ve elektronik parçalardır. Donanım kavramı da kendi içerisinde iki gruba ayrılmaktadır; Dahili donanım ve Harici Donanım. Dahili yani iç donanım ürünleri ekran kartı, RAM, İşlemci gibi ürünlerdir. Harici yani dış donanım ürünleri ise ekran, Mouse (fare), klavye gibi ürünlerdir.

1.2.2.7. Yazılım

Bilgisayar donanımlarının çalışması, Yazılım ile sağlanabilecektir. Öyle ki donanım kavramının ayrılmaz parçası Yazılım kavramıdır. Yazılım, donanımların verilen komutları gerçekleştirebilmesi için geliştirilmiş kodlara denmektedir. Türk Dil Kurumu, yazılım kavramını *"Bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlar, yordamlar, programlama dilleri ve belgelemelerin tümü"* diye açıklamaktadır.

1.2.2.8. Bulut Bilişim

Bulut bilişim, bilişim sistemi kullanıcılarının sisteme yönelik taleplerine ve ihtiyaçlarına göre artırılıp azaltılabilen bilişim kaynaklarını ifade eder.[17] Bu sistem ile kullanıcılar bilişim sistemlerinde depoladıklarını kaynaklarını internet vasıtası işleyerek her zaman ve her yerden bu kaynaklara erişebileceklerdir. Böylece sistem kullanıcıları hem kaynak ve depolama tasarrufu yapabilecek hem de kaynaklarına daha

[17] Armağan Ebru Bozkurt Yüksel, **Bulut Bilişimde Kişisel Verilerin Korunması (Personel Data Protection in Cloud Computing)**, Ankara, 2016, Yetkin Yayınları, s. 23

hızlı ulaşabileceklerdir. Kullanıcılar, çeşitli sağlayıcılar vasıtası ile bu hizmetten satın alma veya kiralama yöntemi ile faydalanabileceklerdir. Sistemin en temel ve bilinen özellikleri çevre dostu ve çalışma garantisinin yanında, erişilebilirliği, cihaz veya konumlardan bağımsız oluşu, esnekliği, ölçeklenebilirliği, sürekli bakımda ve gelişimde oluşu ve ekonomik açıdan uygun olması olarak akla gelebilecektir.[18]

1.3. BİLİŞİM SİSTEMLERİNİN GELİŞİMİ

İnternet, artık insanoğlunun hayatın her alanında yer almaktadır. Sosyal platformların yanı sıra, insanlık ekonomik, siyasal, hukuksal vb. birçok alanda teknoloji ile iç içedir. İnsanlığın en başlarında var olan kişisel haklarını koruma ve adalet ihtiyacı, her halde bugün bilişim alanında da ortaya çıkmaktadır. Haklarının korunmasında ve adalet arayışında insanlar için en önemli hukuki kaynaklardan birisi yazılı belgelerdi. Değişen dünyada artık, bu belgelerin büyük bir kısmı bilişim alanında ortaya çıkmaktadır. Bu çerçevede, hukuki düzenlemeler ve yasama faaliyetleri teknolojik ve bilişim alanlarını takip etmek ve gerisinde kalmamak mecburiyetindedir. Bireyler, uluslararası şirketlerin yanı sıra, devletlerin dahi birçok temel sistemini entegre ettiği bilişim sahası, kaçınılmaz olarak hukuk sistemlerinin artık en büyük ilgi alanını oluşturmaktadır.

Bilişim alanlarındaki belgeler ve bu belgelerin geçerliliği, ifadeler, söylemler ve ihlaller ile birlikte haklara tecavüz gibi birçok belge ve davranış, hukuki anlamda bir zemine ihtiyaç duymaktadır. Toplumların ve devletlerin bu gelişmeler ışığında günümüzdeki en büyük ihtiyaçlarından bir tanesi de bilişim hukukuna dair düzenlemelerdir. Elektronik ortamda yapılan işlemlerin hukuksal zemin kazanması, bu alanla ilgili olacak hukuki düzenlemeler ile sağlanacaktır.

Başta Avrupa Birliği olmak üzere, birçok ülkede teknolojik alandaki gelişmeler toplumları hayati yönden etkilemektedir. Bilişim teknolojilerinin iletişim alanı olarak

[18] Murat Topaloğlu, Harun Özkişi, Egemen Tekkanat, **"Bulut Bilişim"**, 2017, Ankara, Seçkin Yayıncılık, s. 21

kullanıldığı dünyada, bilgi alışverişiyle birlikte her türlü iletişim yöntemi olarak kullanılmaktadır. Devletlere yük olan ve toplumların yaşamsal fonksiyonlarını yerine getirmesinde tıkanıklığa sebep olan birçok işlem artık neredeyse tamamen elektronik ortama taşınmıştır. Bu gelişmeler üzerine devletlerin sistemlerini bilişim alanlarına entegre etmeleri ve bu alanlarda devlet hizmeti verdikleri de görülmektedir. Bu hizmetler, elbette ki peşinde hukuki düzenlemeler ihtiyacı ile gelmektedir. Ülkemizde bilişim teknolojileri alanındaki gelişmeler incelemeye alınacak olursa, ilk başta 2000'li yılların başında hizmete giren e-devlet uygulaması ele alınmalıdır. E-devlet, devlet tarafından vatandaşlara sunulan hizmetlerin bilişim ortamlarında sunulması olarak tanımlanabilecektir.[19] Kamu kurumlarında bürokrasiden ve devlet anlayışından kaynaklı birçok tıkanıklık ve zaman kaybı, bu uygulama ile ortadan kalkmaktadır. Özellikle günümüzde, kişilerin her türlü kamusal bilgisini içerisinde barındıran ve bu alanlarda işlem yapma hakkı tanıyan e-devlet uygulaması, devlet hizmetlerinin elektronik ortamda gerçeklik bulmuş halidir. Türkiye İstatistik Kurumu'nun 2020 yılında yayınladığı Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması raporuna göre e-devlet kullanım oranı açıklanmıştır: *"Kişisel amaçla kamu kurum ya da kuruluşları ile iletişime geçmek veya kamu hizmetlerinden yararlanmak için 2019 yılı Nisan ayı ile 2020 yılı mart ayını kapsayan on iki aylık dönemde İnterneti kullanan bireylerin 16-74 yaş grubu bireyler içerisindeki oranı %51,5 oldu. Bu oran önceki yılın aynı döneminde %51,2 idi. E-devlet hizmetlerini kullanım amaçları arasında, kamu kuruluşlarına ait web sitelerinden bilgi edinme %48,7 ile ilk sırayı aldı"* Elektronik ortamda sağlanan bu hizmetle ve bu hizmetin belirtilen oranlarda yayılması ile birlikte, kişilerin verilerinin güvenliği açısından da oluşturulması gereken birçok hukuki düzenleme ortaya çıkmaktadır. 3 Eylül 2016 tarihli ve 20820 sayılı Resmî Gazetede yayınlanan E-devlet Hizmetlerinin Yürütülmesine İlişkin Usul ve Esaslar Hakkındaki Yönetmelik'te geçen, 5. Maddenin f fıkrasında; "Kişisel verilerin korunması ve mahremiyet prensibinin de dikkate alınarak, temel hak ve özgürlüklere riayet edilmesi" maddesiyle, Kamu kurum ve Kuruluşlarına e-devlet hizmetlerinin hayata geçirilmesi ve hizmete sunulmasına ilişkin riayet edilmesi gereken bir ilke

[19] Murat Akçakaya, **"E-Devlet Anlayışı ve Türk Kamu Yönetiminde E-Devlet Uygulamaları"**, Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2017, sayı 3, s. 11 (Çevrimiçi)

yükümlülüğü getirmiştir. Bu hükümden de anlaşıldığı üzere, bilişim teknolojileri alanında gerçekleşen değişikliklere uyum sağlarken, bir yandan da kişilerin ve devletlerin de hak ve yükümlülükleri hukuki düzenlemeler ile güvence altına alınmalıdır ve alınmaktadır da. Öyle ki bu suçların meydana gelmesindeki en temel unsur, hukuk ihlallerinin olmasıdır. Ve hukuk ihlali suçunun işlenmesinde kullanılan kaynağın bilişim sistemleri olması, bilişim suçlarının hukuksal açıdan düzenlenmesinin gerekliliğini tekrardan ortaya çıkarmaktadır.

1.4. BİLİŞİM SUÇLARININ TANIMI

Bilişim sistemlerinin incelenmesi ile çağımızda bilişim alanının kapsamı ve etki alanı ile bu alandaki suç ihtimallerinin hukukun korunması açısından önemi incelendikten sonra, bu suçların tanımları, tasnifleri ve düzenlenmeleri gereklilik göstermektedir.

Doktrinde bilişim suçlarına yönelik geliştirilen tanımlamalarda farklı ölçütlerden yola çıkılarak birçok tanım ortaya çıkmıştır. Bilişim alanının ve bu alandaki suçların yeniliği ve sürekli gelişme içerisinde olmasından dolayı kesin sınırlamalar içerisinde ortak bir tanıma ulaşılamamıştır.[20] Tanımlamanın içeriğiyle birlikte tanımı adlandırma konusunda da ortak bir noktaya ulaşılamamıştır.

Bilişim suçları, bilişim alanının gelişmesiyle birlikte ortaya çıkmış, bilişim teknolojileri geliştikçe ve değiştikçe ortaya çıkan suç tipleri ve suçların işleniş şekilleri de değişim göstermiştir. Bilişim tarihinde bu suçlara ilk olarak internet suçları, siber suçlar ya da bilgisayar suçları diye isimler verilse de bu kavramlar zamanla yetersiz kalmıştır. Bilişim suçları tanımını kullanmak ise ise tüm bu kavramları kapsayıcı olduğundan dolayı isabetli olacaktır.[21]

---

[20] Ö. Umut Eker, **"Türk Ceza Hukuku'nda Bilişim Suçları"**, TBB Dergisi, sayı 62, 2006, s.104

[21] Mehmet Emin Artuk, Ahmet Gökçen, Caner Yenidünya, **" Ceza Hukuku Özal Hükümler"**, 15. Baskı, Adalet Yayınevi, 2015, Ankara, s.859

Bu suçlara karşı mücadele için hukuk sistemleri düzenlenmiş, geliştirilmiş ve suçların değişim hızına ayak uydurmak için sürekli güncellenme ihtiyacı duyulmuştur. Bilişim sistemlerinin kamusal ve özel alan dahil olmak üzere hayatın her alanında kullanılması sebebiyle sistemlerin işleyişinin ve veri güvenliğinin ceza hukuku vasıtası ile korunmaya alınması zamanla zorunlu olmuştur. Özellikle Bilişim hukuku alanında hak ve adaletin tesisi ve korunması amacıyla, ceza hukuku normları en önemli esasları oluşturmaktadır.[22] Bilişim alanı her geçen dakika gelişebildiği ve genişleyebildiği gibi, kişilerin kullanım alanı ve erişim kapsamı da bu doğrultuda evirilmektedir. Bilişim alanının bu gelişimiyle birlikte, bilişim alanında kullanılan araçlar da değişim gösterebilmektedir. Örneğin; 2000'li yılların başında bilişim denilince akla ilk gelen sistemler bilgisayar ve internet iken, günümüzde mobil telefonlar ile uluslararası ekonomik ve sosyal işlemler gerçekleştirilebilmektedir. Böylece çok kısıtlı alanda işlenebilecek olan bilişim suçları, artık sosyal medya, dijital sistemler, online bankacılık, bulut sistemleri vb. alanlarla yayılabilme imkânı bulmuştur. Genel itibariyle, görülen üzere bilişim suçları, elektronik ortamlarda, elektronik araçlar ile, bu ortamlara yönelik ya da bu ortamlar vasıtasıyla işlenen suçlardır.

21. Yüzyılda ilk akla gelen teknolojik alet bilgisayar olarak ortaya çıkmıştır. İnsanlar, zaman geçtikçe devlet işlemlerinden aile ilişkilerine kadar birçok işlemini bilgisayar aracılığı ile elektronik ortama taşımıştır. Belirtilen dönemlerde bilişim suçlarının tanımı bilgisayar ile sınırlı kalabilmiştir. Bilgisayar suçları gibi getirilen başlıklar ile bilişim araçlarının yalnızca bu suçlar için tanımlamalarda başlık olarak kullanılması dar ve isabetsiz olacaktır. Örneğin, bilgisayar ile bilişim suçlarının kapsamına girmeyen ve bilişim sistemleri kullanılmadan işlenebilecek suçlar olabilecektir.[23] Günümüze gelindiğine bilişim suçları çok daha geniş kapsamda değerlendirilmeli ve tanımlanmalıdır.

Değerlendirilen bilgiler ışığında, bilişim suçları, elektronik veya bilişim teknolojileri ortamlarında, elektronik donanımlar vasıta olarak kullanılarak

---

[22] Mahmut Koca, İlhan Üzülmez, **"Türk Ceza Hukuku Özel Hükümler"**, 4. Baskı, Adalet Yayınevi, Ankara, 2017, s.803

[23] Hüseyin Koçak, Ali Nazmi Dandin, **"Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri"**, Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi / C.: 19, Sayı: 1, Haziran 2017, s.145 (Çevrimiçi)

gerçekleştirilen hukuka aykırı eylemlerdir. Öncelikle, bilişim sistemlerine hukuka uygun veya hukuka aykırı bir şekilde giriş sağlanmaktadır. Öyle ki bilişim suçundan bahsedebilmek için suçun ortaya çıktığı zeminin bilişim alanı olması gerekmektedir. Bu alana giriş hukuka uygun olsa da hukuka aykırı bir suç işlenebilecektir. Bilişim alanına giriş yapıldıktan sonra, yine bilişim sistemleri vasıtasıyla, bilişim alanındaki sistemlere veya verilere kendi ya da 3. Kişi menfaatine müdahale etme, değiştirme, izinsiz kullanma, çalma, silme, yok etmek şekliyle suç işlenebilecektir. Bilişim suçları sayılan suçlar ile sınırlı kalması mümkün değildir. Suçun zemin olan bilişim alanı her gün zaman ve mekân sınırı olmaksızın geliştikçe ve genişledikçe, suç türleri de değişip genişleyebilecektir. Böylelikle suçlu ve mağdur sayısı artmakta, fail ve delil tespiti ise zorlaşmaktadır. Suç, yurt içinde işlenebildiği gibi, tespit edilemeyen konumlarla ve sahte kimliklerle ortaya çıkabilmekte veya delil niteliğinde olan verilerin tespit edilmesi mümkün olamayacak şekilde değiştirebilmekte veya silinebilmektedir. Bu durum da yargı mensuplarının mevcut suçu ispatlamalarının önünde büyük bir engel oluşturmaktadır. Bu tarz hukuka aykırı durumlar, hukuk sistemlerinin her kademesinde ve her konumunda bilişim teknolojilerine hâkim yapıların ve kişilerin olmasını zorunlu hale getirmekte, bilişim ürünlerinde ilkel veya eski ürünler yerine son teknolojinin takip edilmesini ihtiyaç haline getirmektedir.

İKİNCİ BÖLÜM

2. BİLİŞİM SUÇLARININ TASNİFİ, BİLİŞİM HUKUKUNUN ÖNEMİ ve HUKUKSAL DÜZENLEMELER

2.1. BİLİŞİM SUÇLARININ TASNİFİ

Bilişim suçlarının genel tanımında bilişim alanının sürekli güncellenmesi ve gelişmesinden ötürü birçok farklılıklar ortaya çıkmaktadır. Bilişim alanının genişlemesi ile kapsamı sürekli genişleyen bilişim suçlarının sınıflandırılması da bu değişikliklerle birlikte net bir tanıma oturamamış, doktrindeki görüşler bilişim suçlarının sınıflandırılmasında ortak bir noktada buluşamamıştır. Fakat tam manasıyla bir tanım birlikteliği olmasa da anlam olarak benzerlik gösteren tasniflere rastlamak mümkün olacaktır.

2.1.1. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin Getirdiği Tasnif

Bilişim suçlarına getirilen tasnifler incelemeye alındığında, ilk olarak Avrupa Konseyi Siber Suçlar Sözleşmesi'ne bakılabilecektir. Sözleşmenin 1. Kısmı olan Maddi Ceza Hukuku düzenlemesiyle birlikte ilgili tasnifler ele alınmıştır. [24]Sözleşme'nin bilişim suçlarıyla ilgili sınıflandırılması beş başlık üzerinden düzenlenmiştir. *"Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulunmasına Yönelik Suçlar"* getirilen tasnife göre ilk suç çeşididir. Sözleşme, bu suçları yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı olarak saymıştır.

"Bilgisayarlarla ilişkili suçlar" ikinci başlık olarak düzenlenmiştir. Bu başlık altında suçun bilgisayar aracılığıyla işlenmiş olması ele alınmıştır. Maddenin

[24] Cahit Aliusta, Recep Benzer, a.g.e., s.38

içeriğinde, bilgisayarlarla ilişkili sahtecilik ve bilgisayarlarla ilişkili sahtekarlık fiilleri düzenlenmiştir.

Bir sonraki başlık ile *"İçerikle İlişkili Suçlar"* düzenlenmiştir. Bu başlıkla bilişim alanında işlenen suçun içeriğinin düzenlenmesi amaçlanmıştır. Bu suç başlığıyla içerikle ilişkili suçlar ve çocuk pornografisinin engellenmesi amaçlanmıştır.

Bilişim suçlarının ASSS metninde sınıflandırılmasının dördüncü başlığında ise *"Telif Haklarının Ve Benzer Hakların İhlaline İlişkin Suçlar"* düzenlenmiştir.

Ayrıca, sözleşme ile sayılan suçlara ilişkin teşebbüste bulunmak ve yardım ve yataklık etmek de suç kapsamında düzenlenmiştir. Sözleşme, taraf devletlere kendi mevzuatlarında bu suçlara teşebbüs edilmesini veya yardım ve yataklık edilmesinin de suç kapsamında düzenlenmesi ve yaptırım uygulanması yükümlülüğü getirmiştir.

2.1.2. Avrupa Birliği ve Birleşmiş Milletler Komisyonu Ortak Raporu'nun Getirdiği Tasnifler

Avrupa Birliği ve Birleşmiş Milletlerin ortak yayınladığı 11.06.1999 tarihli Bilişim Raporu'na göre, bilişim suçları altıya ayrılmaktadır.[25] Bunlardan birincisi *"Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme"* suçudur. Bu suç sınıfı ile başka bir kişinin veya kurumun bilgisayar sistemine veya servisine, bu suçun icrası için kullanılan yasal olmayan programlar ile izinsiz ve yetkisiz bir şekilde erişilmesi tanımlanmıştır. Türk Ceza Kanunu'nun 243. Maddesinde düzenlenen *"Bilişim Sistemine Girme veya Orada Kalma Suçu"* ile bu sınıfta belirtilen suç hakkında yasal düzenleme yapılmıştır.

Raporda düzenlenen bilişim suçlarının sınıflarından ikincisi ise *"Bilgisayarların Sabote Edilmesi"* suçudur. Bu sınıflandırma ile bilgisayarlara izinsiz ve yetkisiz erişim ile gerçekleştirilen bir suç başlığı düzenlenmiştir. Bilgisayarlara izinsiz ve yetkisiz erişim sonrası bilgisayarlarda var olan verilerin sabote edilmesi,

[25] Ebru Altunok, Ali Fatih Vural, "BİLİŞİM SUÇLARI", Çevrimiçi, s.76 (Çevrimiçi)

bilinçli ve kasıtlı olarak zarar verilmesi veya imha edilmesi suç olarak düzenlenmiştir. Türk Ceza Kanunu yine bu suça 244. Maddesinin 2. Fıkrasında değinmiştir.

Bilişim Raporunun üçüncü suç başlığı "*Bilgisayar Kullanarak Dolandırıcılık Suçudur."* Günümüzde en çok kullanılan suç yöntemlerinden birisi olan bilişim yoluyla dolandırıcılık yapma suçu tanımlanmıştır. Öyle ki, kredi kartı bilgilerinin elde edilmesi, izinsiz ve yetkisiz kullanılması, kopyalanması, hesap bilgilerine erişilmesi ve izinsiz hesap hareketlerinin gerçekleştirilmesi, sahte hesaplar ve yollar ile dolandırıcılık faaliyetinin yürütülerek kendisine veya başkasına haksız kazanç elde edilmesi bu suça verilebilecek örnekler olacaktır.

Raporun dördüncü başlığında *"Bilgisayar Kullanarak Sahtecilik Suçu"* düzenlenmiştir. Yine günümüzde en çok karşılaşılan suçlardan birisi olan bu alanda en sık rastlanılan örneklerden bir tanesi de telefon veya mail gibi çeşitli bilişim araçları kullanılarak kişilere sahte belge veya söylemler ile ulaşılması ve sonrasında kişilerden bu sahte bilgi veya belgelere dayandırılarak kendisi veya başkası menfaatine haksız kazanç veya özel bilgi elde edilmesidir. Sahte telefon aramaları veya mesajları, karşılıksız atılan e-postalar, devlet kurumları veya özel bankalar adına açılmış sahte sosyal medya hesapları, emniyet adına yapılan sahte telefon aramaları en çok karşılaşılan suç örnekleri olmuştur.

Raporun beşinci başlığında ise *"Kanun Tarafından Korunan Bir Yazılımın İzin Alınmadan Kullanılması"* suçu düzenlenmiştir. Bu başlık ile de kanun tarafından korunma altına alınmış olan yasal bir yazılımın, yazılımın mülkiyetini elinde bulunduran kişinin izni olmadan çalınması, çoğaltılması ve satılması suçu düzenlenmiştir.

Raporun altıncı ve son suç sınıfında ise *"Yasaya Aykırı Yayınlar"* ele alınmaktadır. Bu başlıkta ise, yasal olmayan bir yayın ile bilişim araçları vasıtasıyla yayın yapılması düzenlenmiştir. Kanunlar ile düzenlenmesi veya yayınlanması yasaklanmış yayınların gizli yollar veya yasaya aykırı sistemler ile yayına sokulması suç olarak kabul edilmiştir. Bu suça örnek verilecek olunursa, yasadışı bahis siteleri ele alınabilir.

2.1.3. Avrupa Ekonomik Topluluğunun Getirdiği Tasnifler

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun 1983 yılında Bilişim suçlarına yönelik getirdiği tanımlama ve sınıflandırma, bu alandaki en fazla kabul gören ve doktrinde yer verilen tanımlamadır.[26] Paris'te yapılan toplantıda komisyonun açıkladığı üzere bilişim suçları: *"Bilgileri, otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"* olarak tanımlanmıştır.[27] Topluluğun getirdiği tasnife göre ise suçlar bilgisayardaki verilere girilmesi, bozulması silinmesi ve yok edilmesi suçu, bilgisayar sistemlerine sahtekarlık amacıyla girilmesi suçu, bilgisayar sistemlerinin engellenmesi suçu, maddi kazanç amacıyla bilgisayar sahibinin haklarına zarar verme suçu ve bilgisayar sistemlerine hukuka aykırı şekilde müdahale etme suçu olarak beşe ayrılmaktadır.[28]

2.1.4. Birleşmiş Milletler 'in Getirdiği Tasnifler

BM, 2000 yılında Brüksel'de yaptığı onuncu kongresinde bilişim suçlarını gündeme almış, suçlara yönelik tanımlama getirmiştir. Birleşmiş Milletlerin tanımlamasına göre bilgisayarlarda ve bilgisayar ağlarında gerçekleşen haksız eylemler veya bilgisayar ağlarına karşı düzenlenen tüm saldırı ve işlemlere bilişim suçu denmektedir. Bu suçlar dar anlamda siber suçlar ve geniş anlamda bilişim suçları olarak kendi içerisinde kategorilere ayrılmaktadır. Tanımdan anlaşıldığı üzere, bilgisayar ve ağlarına yönelik gerçekleştirilen her türlü eylem, bilişim suçu kapsamına girmektedir. Bilişim suçları, dar anlamıyla bilişim sistemlerinin güvenliğine yönelik

---

[26] Mesut ORTA, **"Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)",** Yetkin Yayınları, Ankara, 2015, s. 85

[27] Cahit Aliusta, Recep Benzer, a.g.e., s.36

[28] Ebru Altunok, Ali Fatih Vural, a.g.e., s.77

saldırı suçlarını konu edinirken, geniş anlamıyla ise bilişim sistemlerinde gerçekleşen her türlü hukuka aykırı eylemlere denmektedir.[29]

2.1.5. 5237 Sayılı Türk Ceza Kanunu'nda Geçen Tasnifler

765 sayılı Eski Türk Ceza Kanunu ile 1991 yılında bilişim suçları tabiri ilk defa Türk Hukuku'nda düzenlenmiştir. 5237 sayılı yeni Türk Ceza Kanunu ile birlikte Siber suçlar daha geniş kapsamda düzenlenmiş ve yeni tasnifler getirilmiştir. Bu düzenlemeler ile Türk Ceza Kanunu, bilişim suçları ile ilgili yapılan hukuksal düzenlemeler arasında önemli bir yere sahip olmuştur. Bunun önemli bir sebebi olarak, uluslararası düzenlemelerde de pek rastlanmayan, bilişim alanında suçlar bölümünün bu kanunda münhasır bir başlık ile tesis edilmiş olmasıdır.[30]

Türk Ceza Kanunu'nda bilişim suçları çeşitli şekillerde sınıflandırılmaktadır. Fakat, genel kabul gören görüşe göre bilişim suçları, doğrudan bilişim suçları ve dolaylı bilişim suçları olarak ikiye ayrılmaktadır. Doğrudan bilişim suçları ile gerçek bilişim suçları kastedilirken, dolaylı bilişim suçları ile ise bilişim bağlantılı suçlar tanımlanmıştır. Türk Ceza Kanunu'nda düzenlenen, Doğrudan bilişim suçları başlığı altına giren suçlar, TCK madde 243 ile düzenlenen Bilişim Sistemine Girme Suçu, TCK madde 244 ile düzenlenen Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, TCK madde 245 ile düzenlenen Banka veya kredi kartlarının kötüye kullanılması suçudur. Dolaylı bilişim suçları yani bilişim bağlantılı suçlar ise TCK ile düzenlenmiş suçların bilişim yoluyla işlenmesi ile ortaya çıkan suçları kapsamaktadır. Bu suçlar, TCK madde 142/2-e ile düzenlenen nitelikli hırsızlık, madde 135 ile düzenlenen Kişisel verilerin kaydedilmesi, madde 226 ile düzenlenen müstehcenlik suçları ile örneklendirilebilecektir.

---

[29] B. Zakir Avşar, Gürsel Öngören, **"Bilişim Hukuku",** İstanbul, Türkiye Bankalar Birliği Yayınları, 2010, s.124

[30] Metin Turan, a.g.e., s.67

2.2. BİLİŞİM HUKUKUNUN ÖNEMİ

İnternet kullanmanın, teknolojik aletlerin, bilişim icatlarının hayatımızın her alanında olduğu ve artık bir lüks olmak halinden çıkarak herhangi bir yaş veya sosyal sınıf farkı ayırt etmeksizin herkesin kullandığı ve hayati önem taşıyan bilgilerini paylaştığı, sakladığı, öğrendiği bir çağ yaşanmaktadır. Bu alandaki hızlı gelişmeler pek çok fayda ve kolaylık sağladığı gibi birçok zarar ve sorunu da ortaya çıkarmaktadır.[31] Bilişim sistemlerinin özel hayatın veya kamusal alanın her alanına hâkim olduğu bu çağda, bu sistemlerin güvenliği ve gizliliği, özel hayatın ve kişisel verilerin dokunulmazlığı, kamusal alanın ihlal edilemezliği ve güvenliği son derece önem arz etmektedir. Kişiler veya devletler, bu gizliliği ve güvenilirliği haliyle beklemektedir. Bu sistemlerin gizliliği ve güvenilirliği açısından, bilişim sistemleri kadar bilişim alanında gerçekleştirilecek olan yasal düzenlemeler ile mümkün olacaktır.

2.3. HUKUKSAL DÜZENLEMELER

2.3.1. Ulusal Düzenlemeler

Elektronik alanda gerçekleştirilen faaliyetlerin çeşitliliği günden düne artarken, bu hıza ayak uydurmak için birçok konuda hukuki düzenlemeler ülkemizde ortaya çıkmaktadır. Bu hukuki düzenlemelere bir sonraki bölümde detaylı bir şekilde değinilecek olsa da bu düzenlemelerin hukuktaki yeri ve önemine kısaca değinmek gerekmektedir.

Bilişim alanında ulusal düzeyde birçok suç işlenmekte ve kişilerin hakları ihlal edilmektedir. Toplumun ve devletin bilişim alanında yaptığı çalışmalar ile birlikte, kişilerin devlet işlerini dahil elektronik ortamda düzenlediği ve veri girdiği bir çağ

[31] Ahmet Efe, **"Bilişim Hukuku Alanındaki Sorunlar ve Risklerin Mevzuat Boyutuyla Analiz ve Çözümlemesi"**, Türkiye Noterler Birliği Hukuk Dergisi, 2016, sayı 1, s.175 (Çevrimiçi)

yaşanmaktadır. Geçmiş yıllarda günlerce süren kamusal işlemler, elektronik ortamda dakikalar içerisinde halledilebilecek şekilde düzenlenmiştir. Bu elektronik ve teknolojik atılımlarla birlikte yaşam kalitesi ve zaman kazancı yaşanıyor olsa da özellikle kamusal işlerde kişilerin kullandığı veriler, ticari faaliyetler, maddi veriler, kredi kartı bilgileri, şifreleri, TC. Kimlik numaraları, vergi numaraları gibi özel nitelikteki kişisel verilerin hepsi elektronik ortama girilmektedir.

Kişisel verilerin bu düzeyde toplandığı elektronik ortamda, verilerin takibi, gizliliği ve korunması genişleyen bilişim alanıyla birlikte her geçen gün daha da zorlaşmaktadır. Kişilerin yazılı ve somut bir şekilde teslim ettiği veriler, günümüz çağında artık bulut sistemleri gibi sanal ortamlarda saklanmaktadır. Bu hizmetler ile birlikte toplanılan bu verilen korunması, bu verilerin tespiti ve incelenmesi de yükümlülüğü beraberinde getirmektedir. Bilişim alanında işlenen suçların temelinde delil olarak ortaya çıkan unsurlar genellikle bu veriler olmaktadır. Verilerin tespitinin ve incelenmesinin önemi gibi, verilerin kim tarafından işlendiği, girildiği veya kim tarafından hukuka aykırı şekilde ele geçirildiğinin tespiti de önemli olacaktır. Zikredilen unsurlar göz önüne alındığında, getirilecek hukuki düzenlemeler ile işlenebilecek suçların çerçeve içine alınarak caydırıcılık oluşturulması kadar, oluşabilecek suçların aydınlatılmasında da çözüm üretici tedbir ve düzenlemelerin yürürlüğe girmesi gerekmektedir.

Elektronik alandaki değişimler ve teknolojinin getirdiği yeni alanlar ile birlikte, yasal düzenlemelerin sayısı gittikçe artmakta, kişisel verilerin korunması ve verilerin delil olarak değerlendirilmesindeki güçlüğün kalkması adına farklı uygulamalara gidilmektedir. Örneğin; 23.01.2004 tarihli ve 5070 sayılı elektronik imza kanunu, bahsedilen ihtiyaçlardan birisi üzerine ortaya çıkmıştır. Elektronik imza, elektronik ortamda düzenlenen dokümanlarda el ile atılan imzanın doğurduğu hukuki sonuçları ortaya çıkarmaktadır.[32] Getirilen bu yöntem ile, kişilerin el ile imzaladığı belgelerin tespiti ve delili gibi, elektronik sistemlerde hazırlanan belgeler kişiler el ile imza atmış gibi sayılmaktadır. Böylece yazılı alanda geçerli olan hukuk normları, elektronik alana da uygulanabilecektir. Ayrıca benzer bir düzenleme, 03.02.2021 tarihli ve 31384 sayılı

[32] İnci Biçkin, **"Elektronik İmza Ve Elektronik İmza İle İlgili Yasal Düzenlemeler"**, TBB Dergisi, 2006, sayı 63, s.110 (Çevrimiçi)

Resmî Gazete ’de yayınlanan Teknoloji Geliştirme Bölgeleri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile karşımıza çıkmaktadır. 7263 sayılı kanunun 14. Maddesiyle 5070 sayılı Elektronik İmza Kanunu’na ek getirilmiştir: “*Elektronik Mühür, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve mühür sahibinin bilgilerini doğrulama amacıyla kullanılan veridir. Elektronik mühür sahibi; Elektronik mührü oluşturan kamu kurum ve kuruluşları, kamu idareleri, kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları, kamu ve özel hukuk tüzel kişileri ve noterliklerdir. Elektronik Mühür, elektronik belgenin veya verinin mühür sahibi tarafından oluşturulduğunu, belgenin veya verinin kaynağını ve bütünlüğünü garanti eden delil kaydıdır. Elektronik Mühür, resmi mühür dahil her türlü fiziki mühür ile aynı hukuki niteliğe haizdir. Elektronik mühür oluştura amacı ile ilgili mühür sahibinin rızası veya talebi dışında; mühür oluşturma verisi veya mühür oluşturma amacını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen mühür oluşturma araçlarını kullanarak izinsiz elektronik mühür oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adli para cezasıyla cezalandırılırlar. Suçun elektronik sertifika hizmet sağlayıcısı çalışanları işlenmesi halinde; bu cezalar yarısına kadar artırılır. Kanunlarda yer alan elektronik imzaya ilişkin hükümler, kıyasen elektronik hüküm hakkında da uygulanır.”.* İlgili madde ile, 5070 sayılı kanuna yeni bir madde eklenmiştir. Bu madde eklenmesinin sebebi, Bilişim alanında yaşanan değişim ve gelişime paralel olarak yapılmış, elektronik mühür ile fiziki mühür hukuken aynı sonuca bağlanmıştır. Eklenilen maddede, mühürlerin hükmü ile birlikte müeyyideler de belirtilmiş, elektronik alandaki bu değişimlerin hukuka uygunluğunun sağlanması amaçlanmıştır.

2.3.1.1. 765 Sayılı (Eski) Türk Ceza Kanunundaki Düzenlemeler

Bilişim sistemleri ve bilişim suçlarına yönelik kavramlar Türk Hukuk sisteminde ilk olarak 1990’lı yıllarla düzenlenmeye başlamıştır. Türkiye’de de bilişim suçları, münhasır bir yasal düzenleme ile değil, Türk Ceza Hukuku’na yapılan ilaveler

ile kanuna girmiştir. Eski Türk Ceza Kanunu olan 765 sayılı kanuna 6.6.1991 tarihiyle bilişim suçları ayrı bir bab ilave edilmesiyle girmiştir.

765 sayılı eski TCK'ya yapılan eklemeler "Bilişim Alanında Suçlar" adıyla düzenlenmiştir. 765 sayılı TCK'ya 525/a, 525/b, 525/c ve 525/d maddelerinden oluşan bir bab eklenmiştir. Düzenlenen bu hükümler Fransız Ceza Kanunu'ndan esinlenerek hazırlanmış ve kanunda yerini almıştı. Dülger' göre *"Bu düzenleme TCK'nın genel düzenleme mantığı olan "suçla korunan hukuksal değer" kavramına göre değil bilgisayar ortak kavramına göre yapılmıştır."*[33]

525/a ile verilerin ele geçirilmesi, verilere zarar verilmesi ve verilerin çoğaltılması suçu cezaya bağlanmıştır. Madde metni; *"Bilgileri otomatik olarak işleme tabi tutulmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve birmilyon liradan onbeşmilyon liraya*[34] *kadar ağır para cezası verilir. Bilgileri otomatik işleme tabi tutulmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir."*[35] Şekliyle düzenlenmiştir.

765 sayılı Eski Türk Ceza Kanunu'na 525/b ile yapılan ekleme, bilişim sistemlerindeki verilere kendisi veya başkası adına yarar sağlamak amacıyla kısmen veya tamamen zarar verme suçu düzenlenmiştir. Madde metni; "*Başkasına zarar vermek veya kendisine veya başkasına 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 işlenmesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beş milyon liradan ellimilyon liraya kadar ağır para cezası verilir. Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmi milyon liraya kadar ağır para cezası verilir." Şekliyle düzenlenmiştir.*

---

33 Dülger, a.g.e., 2015, s. 237

34 Miktar eski Türk Lirası cinsinden belirtilmiştir.

35 6.6.1991 kabul tarihli, 14.6.1991 Resmi Gazete yayın tarihli, 20901 yayım sayılı, 3756 sayılı "765 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun"

525/c ile sahte belge oluşturmak için tahrif suçu düzenlenmiştir. Madde; *"Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir."* Düzenlemesi içermektedir. Hukuk alanında delil olarak kullanılmak kastı ile düzenlenen suç oluşacaktır. Maddede belirtilen bu özel kast ile işlenebilecek iki suç düzenlenmiştir. Birincisi sahte belgenin düzenlenmesi amacıyla verilerin yerleştirilmesi, ikincisi ise oluşturulan belgelerin kasten kullanılmasıdır.

525/d ile getirilen son düzenlemede ise, 525/a ve 525/b maddelerinde düzenlenen hükümleri ihlal eden kişilerin cezalara ek olarak mesleklerinden veya hizmetlerinde ihraç edilmesi düzenlenmiştir.

1990'lı yılların henüz başında Türk hukuk sisteminde bilişim sistemlerine yönelik yapılan bu değişiklikler, Türkiye'de henüz internetin ve bilişim sistemlerinin daha yeni tanınmaya başladığı bir döneme denk geliyordu. Yukarıda da detayıyla bahsedildiği gibi Türkiye'de ilk internet kullanımı 1993 yılında gerçekleşmişken bilişim sistemleriyle ilgili yasal düzenlemeler 1991 yılında hazırlanmış ve yürürlüğe girmiştir.

Türk Hukukunun bilişim kavramıyla tanışması ve bilişime yönelik düzenlemeleri 1951 tarihli 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 1995 yılında yapılan değişikliklerle bilgisayar programlarına yönelik tanım ve kavramları muhtevasına dahil etmesiyle devam etmiştir. 7.6.1995 tarihli ve 4110 sayılı 5846 sayılı *"Fikir ve Sanat Eserleri Kanunu'nun Bazı Maddelerinin Değiştirilmesine İlişkin Kanun"* ile getirilen değişiklikle bilgisayar programları da *"eser"* kapsamında değerlendirilerek, bilgisayar programlarına yönelik gerçekleştirilecek hukuka aykırı fiiller de suç kabul edilmiştir.[36] Artık bilişim yazılımlarının eser olarak kabul edilmesi, yapılan bu değişiklik ile Türk Hukuku'na girmiştir. Böylece, eserlere yönelik yapılabilecek hak ihlallerinde saldırganlar nasıl cezalandırılıyorsa, bilişim

yazılımlarına ve bilişim verilerine yönelik yapılacak her türlü saldırı da müeyyide altına alınmıştır.

2.3.1.2. 5237 Sayılı Türk Ceza Kanunundaki Düzenlemeler

Türkiye'de yaşanan siyasi gelişmeler, hukuk alanındaki gelişmeleri ve değişiklikleri de engellemiş, yenilenmesi planlanan ve bu doğrultuda çalışmalar yapılan Yeni Türk Ceza Kanunu'nun da yürürlüğe girmesini ileri bir tarihe atmıştır. 1997 yılında tasarısı hazırlanan 5237 sayılı Türk Ceza Kanunu, birçok değişikliğe uğrayarak 26.9.2004 tarihinde kabul edilmiştir. 2004 yılında kabul edilen kanun, 344. Madde[37] gereğince 1.4.2005 tarihinde yürürlüğe girmiştir.

TCK oluşturulurken modern ceza hukukunun ilkelerinin gözetilmeye çalışıldığı ve öncelikle 765 sayılı ETCK'nın öncelikle devleti koruyan yapısından vazgeçilerek kişilerin korunmasının öne çıkarıldığı, bunun vurgulanması için de tasarının ikinci kitabını oluşturan özel kısımda, kişilere karşı işlenen suçlardan başlanarak suç tiplerinin düzenlendiği, böylelikle Batı Avrupa'da yürürlükte olan modern ceza yasalarına sistematik açıdan uyum sağlanmaya çalışıldığı belirtilmektedir. [38] Bu gelişmeler eşliğinde düzenlenen yeni TCK ile, bilişim sistemleri ile birlikte kişilerin haklarını korunmasına yönelik daha geniş ve kapsayıcı düzenlemeler hazırlanmıştır.

5237 sayılı Türk Ceza Kanunu iki kitaptan oluşmuştur. İlk kitap ceza hukukuna dair genel ilkeleri düzenlerken, ikinci kitap suç tipleri ve yaptırımları düzenlemektedir. İkinci kitap dört bölüme ayrılmaktadır. Bunlar, insanlığa karşı suçlar, topluma karşı suçlar, millete ve devlete karşı suçlar ile son hükümlerdir. Bilişim suçları ise, ikinci kitabın üçüncü bölümü olan topluma karşı suçlar kısmında "Bilişim Alanında Suçlar"

---

[37] 26.9.2004 kabul tarihli, 12.10.2004 Resmi Gazete yayın tarihli, 25611 yayım sayılı, 5237 sayılı Türk Ceza Kanunu'nun 344. Maddesi: *"(1) Bu Kanunun; a) "İmar kirliliğine neden olma" başlıklı 184 üncü maddesi yayımı tarihinde, b) "Çevrenin kasten kirletilmesi" başlıklı 181 inci maddesinin birinci fıkrası ile "Çevrenin taksirle kirletilmesi" başlıklı 182 nci maddesinin birinci fıkrası yayımı tarihinden itibaren iki yıl sonra, c) Diğer hükümleri 1 Hazir an 2005 tarihinde, (1) Yürürlüğe girer."*

[38] Dülger, a.g.e., 2015, s. 332

başlığıyla düzenlenmiştir. Bu bölüm haricinde de TCK'nın çeşitli bölümlerinde bilişime yönelik suçlar düzenlenmiştir.

Bilişim Alanında suçlar bölümüyle dört madde düzenlenmiştir. Bu bölümde bilişim sistemlerine yönelik olan hükümler 243, 244, 245 ve 246 numaralı maddelerde düzenlenmiştir. Maddelerin Ceza Hukuku bakımından detaylı incelenmesi son bölümde olacaktır.

243. Madde ile bilişim sistemine girme suçu, 244. madde ile Sistemi engelleme, bozma verileri yok etme veya değiştirme suçu, 245. maddede ise Banka veya kredi kartlarının kötüye kullanılması düzenlenmiştir. 246. Madde ile ise Tüzel kişiler hakkında güvenlik tedbiri uygulanmasına yönelik düzenlemeler yer almıştır.

5237 sayılı Türk Ceza Kanunu'nda bilişim suçları çeşitli bölümlerde yine ele alınarak, bilişim hukukuna yönelik hukuki düzenlemeler gerçekleştirilmiştir. 132. Madde ve devamı ile düzenlenen *"Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar"* bölümü ile *kişisel verilerin kaydedilmesi suçu* (m.135); *kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu* (m. 136); *verilerin yok edilmemesi suçu* (m.138) başlıkları bilişim suçları kapsamında değerlendirilebilecektir. [39] Avrupa Birliği Veri Koruma Kanunu'na göre kişisel veri, gerçek kişiler ile ilgili her türlü bilgiyi ifade etmektedir.[40]

TCK madde 135, hukuka aykırı olarak kişisel verileri kaydeden kişilere yönelik düzenlenen yaptırımları hükme bağlamıştır. Maddeye göre*: "(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir*[41]*. (2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."*[42]

---

39 Dülger, a.g.e., 2015, s. 338

40 Türkay Henkoğlu, **"Bilgi Güvenliği ve Kişisel Verilerin Korunması"**, 2015, Ankara, Yetkin Yayınevi, S.75

41 21/2/2014 tarihli ve 6526 sayılı kanunun 3 üncü maddesiyle bu fıkrada yer alan "altı aydan" ibaresi "bir yıldan" şeklinde değiştirilmiştir.

42 24/3/2016 tarihli ve 6698 sayılı Kanunun 30 uncu maddesiyle, bu fıkrada yer alan "Kişilerin" ibaresi "Kişisel verinin, kişilerin" şeklinde; "bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır" ibaresi "olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır" şeklinde değiştirilmiştir.

Madde 136 ile ise kişisel verilerin hukuka aykırı olarak bir başkasına verme veya ele geçirme suçlarına yönelik hükümler düzenlenmiştir. Maddeye göre: *"(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır. (4)* [43]*(2) (Ek:17/10/2019-7188/17 md.) Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır."*

Madde 138 ise, verileri yok etme suçunu ve müeyyidelerini ele almıştır. Maddeye göre: *"(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.*[44]*(2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.*

Belirtilen maddeler haricinde Türk Ceza Kanunu'nda 124. Maddesinde *"haberleşmenin engellenmesi suçu"*, 125. Maddesinde *"hakaret suçu"*, 132. Maddesinde *"haberleşmenin gizliliğinin ihlal suçu",* 133. Maddesinde *"kişiler arasındaki konuşmaların dinlenmesi veya kayda alınması suçu",* 134. Maddesinde *"özel hayatın gizliliğini ihlâl suçu",* 142. Maddesinde *"bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık suçu",* 158. Maddesinde *"bilişim sistemlerinin kullanılmasıyla dolandırıcılık suçu",* 226. Maddesiyle *"müstehcenlik*" suçu ve 186. Maddesiyle *"ses ve görüntülerin kayda alınması suçu"* düzenlenmiştir. Bu suçlar doğrudan bilişim suçları olarak değerlendirilmese de bilişim sistemleri kullanılarak suçun icrası gerçekleşebileceği için dolaylı yoldan bilişim suçları olarak sayılabilecektir. Böylece, yukarıda sayılan bölümler haricinde düzenlenen bu maddelerin de bilişim hukukuna yönelik maddeler olabileceği kabul edilebilecektir.

[43] 21/2/2014 tarihli ve 6526 sayılı kanunun 4 üncü maddesiyle bu fıkrada yer alan "bir yıldan" ibaresi "iki yıldan" şeklinde değiştirilmiştir.

[44] 21/2/2014 tarihli ve 6526 sayılı kanunun 5 inci maddesiyle bu fıkrada yer alan "altı aydan bir yıla kadar hapis" ibaresi "bir yıldan iki yıla kadar hapis" şeklinde değiştirilmiştir.

2.3.1.3. Fikir ve Sanat Eserleri Kanunu

Fikir ve sanat eseri, 1951 tarihli 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda tanımlar bölümünde 1/B maddesinde tanımlanmıştır. Maddeye göre eser: *"Sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsullerini…"* ifade eder.

7.6.1995 tarihli yapılan değişiklikle Fikir ve Sanat Eserleri Kanunu'na bilişim suçlarına yönelik eklemeler yapılmıştır. Bu değişiklikler kapsamında kanuna eklenen *"Bir bilgisayar programının uyarlanması, düzenlenmesi veya herhangi bir değişim yapılması;.."* ifadesi ile bilgisayar kavramı FSEK'e dahil olmuştur. Böylece 71., 72. Ve 73. Maddelerinde düzenlenen suç tipleri ile bilişim yazılımları da tanımlanmıştır.[45]

Yapılan eklemeler ile değiştirilen 71. Maddeye *"Manevi haklara tecavüz",* 72. Maddeye *"Mali Haklara tecavüz"* ve 73. Maddede bağlantılı suçlar düzenlenmiştir.

Teknolojinin ve bilişim sistemlerinin gelişmesi ile bilişim suçlarının da işlenme şekilleri değişmiş, mevcut düzenlenen hukuk normları yetersiz haline gelmiştir. Bilişim hukuku alanında yapılan hukuki düzenlemeler artık yeterli kalmamakta ve düzenlenen hukuk normlarının güncellenmesi ve genişletilmesi gerekmektedir. Bu bağlamda Fikir ve Sanat Eserleri Kanunu'nda da zamanla değişikliklere ve eklemelere gidilmiştir.

23.1.2008 tarihinde 5728 sayılı yasa ile FSEK'te 71.,72. Ve 73. Maddeler yeniden düzenlenmiştir. 73. Madde ilga edilmiş, 71., 72. Ve 73. Maddede yer alan suçlar birleştirilmiştir. [46]

---

[45] Dülger, a.g.e., 2015, s. 749

[46] 5/12/1951 kabul tarihli, 12.12.1951 Resmi Gazete yayım tarihli, 2393 yayım sayılı, 5846 sayılı FSEK madde 71 – (Değişik: 23/1/2008-5728/138.md.)'de Manevi, mali veya bağlantılı haklara tecavüz olarak değiştirilmiştir. Maddeye göre:
"Bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek: 1. Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur. 2. Başkasına ait esere, kendi eseri olarak ad koyan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hâlinde, hapis cezasının üst sınırı beş yıl olup, adlî para cezasına hükmolunamaz. 3. Bir eserden kaynak göstermeksizin iktibasta bulunan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. 4. Hak sahibi kişilerin izni olmaksızın,

72. Madde ile ise yeni bir düzenleme getirilmiş, Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri düzenlenmiştir.[47]

2.3.1.4. Elektronik İmza Kanunu

Bilişim teknolojilerinin geldiği nokta ile birlikte son yıllarda kişilerin alışverişlerde kullandığı yöntemlerin ciddi bir oranının sanal ticaret ile yapılması ile birlikte tüketicilerin haklarının korunması ve yapılacak olan ticaretlerde doğabilecek hukuksuzlukların önüne geçilebilmesi adına alternatif çözüm yollarına gidilmiştir. Bu yollardan bir tanesi de Türkiye'de de uygulanan elektronik imza yönetimidir. Dülger elektronik imza ile ilgili gelişmeleri şu şekilde özetlemiştir: *"Hız ve sınır tanımayan teknolojinin insanlığa hediyesi olan veri iletişim ağlarının bulunması ve yaygınlaşmasından sonra, bu ağların dünya çapında gelişen ticarette kullanılması ve elektronik ticaret kavramının ortaya çıkmasıyla birbirlerinden çok uzakta olan kişilerin yaptıkları sözleşmeleri ya da söz verimleri onaylamak için sanal alanda kullanabilecek veri halinde bulunan bir araca ihtiyaç duyulmuş ve kısa zaman içinde "elektronik imza" isimli ürün gelişmiştir."*[48]

---

alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır. 5. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır. 6. Bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu Kanunun ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına hükmolunur. Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir."

[47] FSEK madde 72 – (Değişik:23/1/2008-5728/139 md.)'ye göre:
"Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır."

[48] Dülger, a.g.e., 2015, s. 771

15.1.2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu (EİK) 25. maddesi[49] gereğince kanun yayımlandığı tarihten altı ay sonra 23.7.2004 tarihinde yürürlüğe girmiştir.[50] Elektronik imza kanunu ile birlikte klasik ticaret anlaşmalarının aksine alışveriş yaparken birbirinden uzakta ve hazır bulunmaya kişilerin sözleşmelerini yapabilmeleri ve tıpkı klasik sözleşmeler hazırlanırken ortaya çıkan güvence unsurunun sanal ortamda da kişiler arasında oluşması sağlanmıştır. Ayrıca, elektronik imza kanunu ile E-devlet ve UYAP gibi platformlarının altyapıları hazırlanmış, kişilerin ve kurumların resmi işlemlerinin bilişim sistemlerinde yapılabilmesi sağlanmıştır.

Elektronik İmza Kanunu ile birtakım suçlar düzenlenmiştir. "Denetim ve Ceza Hükümleri" başlıklı üçüncü bölümde 16., 17. Ve 18. Maddede bu suçlara yer verilmiştir.

5070 sayılı EİK'in 16. Maddesinde imza oluşturma verilerinin izinsiz kullanımı düzenlenmiştir. Maddeye göre: *"Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."* Düzenlenen suç ile kişilerin elektronik ortamda yapacağı ticaretlerde ve oluşturacağı resmî belgelerde güven duygusunun ve elektronik imzaya kişiler tarafından duyulan güvenin korunması amaçlanmıştır. Dolayısıyla, kişilerin sanal ortamda yapacağı işlemlerde de klasik imzaya duyulan güvenin elektronik imza ile sağlanması ve bilişim ortamlarının gelişimiyle birlikte klasik işlemlerde yer alan hukuk kurallarının sanal işlemlerde de geçerli olması amaçlanmıştır. Öyle ki, bilişim sistemlerinin geldiği noktada artık sanal veya sanal olmayan tabirlerinin bir önemi kalmamış, düzenlemelerin artık tüm platformlarda aynı mahiyete uygun bir şekilde kapsayıcılıkla yapılma hissi ortaya çıkmıştır.

---

49 E.İ.K. Madde 25'e göre *"Bu Kanun yayımı tarihinden altı ay sonra yürürlüğe girer."*

50 Karagülmez, a.g.e., s. 167

EİK'nın 17. Maddesine getirilen değişiklikle birlikte Elektronik Sertifikalarda Sahtekârlık Suçu düzenlenmiştir. İlgili maddeye göre: *"Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."* [51]Düzenlenen bu suç ile de elektronik sertifikalarda sahtekarlık engellenmeye çalışılmıştır. Sahte elektronik sertifikaların oluşturulması veya mevcut sertifikaların değiştirilmesi veya yetkisiz bir şekilde elektronik sertifikaların kullanılması suçun unsurlarını oluşturmaktadır. Suçun ağırlaştırıcı nedenleri de madde ile düzenlenmiştir.

Elektronik İmza Kanunu'nun 18. Maddesi ile de ilgili kanunda düzenlenen 10.,11.,12.,13. Ve 15. Maddelerine aykırı hareket edilmesi haline Telekomünikasyon Kurulu tarafından verilecek idari para cezaları düzenlenmiştir.

2.3.1.5. İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

23/5/2007 tarihli 5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele hakkında kanun internet sistemleri ile ilgili yasalaşan ilk özel yasal düzenlemedir. Kanun, internet sistemlerinde içerik sağlayıcıların yükümlülüklerini ve sorumluluklarını düzenlemiştir. Kanunun 1. Maddesine göre: *"Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir."*[52]

---

[52] 4.5.2007 kabul tarihli, 23.5.2007 Resmî Gazete yayın tarihli, 26530 yayın sayılı, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5651 sayılı kanun kapsamında, 8. Maddede bazı suçlar sayılmış ve bu suçların oluştuğu hususunda yeterli şüphe bulunmasıyla uygulanılacak tedbirler düzenlenmiştir. Kanun ile sayılan bu suçlar, Türk Ceza Kanunu'nda, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da, 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun'da düzenlenen birtakım suçlardır. Maddeye göre sayılan bu suçların oluştuğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilir.

Kanunun 8. Maddesinde yer alan suçlar sayılmıştır. Yalnızca sayılan suçların oluştuğu hususunda yeterli şüphe oluşursa düzenlenen madde hükümleri uygulanır. Kanun maddesine göre: *"a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan; 1) İntihara yönlendirme (madde 84), 2) Çocukların cinsel istismarı (madde 103, birinci fıkra), 3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190), 4) Sağlık için tehlikeli madde temini (madde 194), 5) Müstehcenlik (madde 226), 6) Fuhuş (madde 227), 7) Kumar oynanması için yer ve imkân sağlama (madde 228), suçları. b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar. c) (Ek:25/3/2020-7226/32 md.) 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar."*[53] Sayılmıştır.

Sayılan suçların işlenmesi hakkında yeterli şüphe oluştuğunda ise bilişim sistemlerinde meydana gelebilecek hukuka aykırı hallerin önüne geçilmesi amaçlanmıştır. Kanun ile düzenlenen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, soruşturma evresinde hâkim ve kovuşturma evresinde mahkeme kararı ile verilebilecektir. Gecikmesinde sakınca bulunan hallerde ise Cumhuriyet savcısı karar verebilecektir.

2.3.1.6. Tüketicinin Korunması Hakkında Kanun

2013 tarihli 6502 sayılı Tüketicinin Korunması Hakkında Kanun, tüketicilerin tüm platformlarda gerçekleştireceği ticari işlerde ekonomik haklarını koruyan, zararlarını tazmin etmeleri için kanuni imkanlar oluşturan, tüketiciyi hakları konusunda aydınlatan ve kendilerini ticari konularda geliştirici hususları düzenlemiştir. Kanun'un 1. Maddesine göre: *"Bu Kanunun amacı; kamu yararına uygun olarak tüketicinin sağlık ve güvenliği ile ekonomik çıkarlarını koruyucu, zararlarını tazmin edici, çevresel tehlikelerden korunmasını sağlayıcı, tüketiciyi aydınlatıcı ve bilinçlendirici önlemleri almak, tüketicilerin kendilerini koruyucu girişimlerini özendirmek ve bu konulardaki politikaların oluşturulmasında gönüllü örgütlenmeleri teşvik etmeye ilişkin hususları düzenlemektir."*[54] Böylece 6502 saylı kanun, tüketicilerin ticari işlemlerinde gerçekleştirdiği her türlü tüketici işlemlerini ve tüketici uygulamalarını kapsamaktadır.

Tüketicinin korunması hakkında kanunun 3. Maddesi tanımlar bölümünü düzenlemektedir. 2003 yılında yapılan değişiklik ile kanunun 3. Maddesindeki "mal" tanımına elektronik mallar eklenmiştir. Maddeye göre: *"Mal: Alışverişe konu olan; taşınır eşya, konut veya tatil amaçlı taşınmaz mallar ile elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri her türlü gayri maddi malları,… ifade eder."*[55] Değişiklikle eklenen tanımdaki "elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri her türlü gayri maddi mallar" ifadesi ile bilişim sistemleri kanuna dahil olmuştur.

2.3.1.7. 7258 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkındaki Kanun

1959 tarihli 7258 sayılı Futbol ve diğer spor müsabakalarında bahis ve şans oyunları düzenlemesi hakkında kanunda 2 Ağustos 2013 tarihli 6495 sayılı Resmî

[54] 7.11.2013 kabul tarihli, 28.11.2013 Resmî Gazete yayın sayılı, 28835 kabul sayılı, 6502 sayılı Tüketicinin Korunması Hakkındaki Kanun

Gazete 'de yayınlanan "Bazı Kanun ve Kanun Hükmünde Kararnamelerde değişiklik Yapılmasına dair Kanun" ile getirilen değişikliklerle internet üzerinde yapılan bahis oyunları konusunda düzenleme getirilmiştir. İlgili düzenlemenin 5. maddesine göre: *"Yurt dışında oynatılan spor müsabakalarına dayalı sabit ihtimalli veya müşterek bahis ya da şans oyunlarının internet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkân sağlayan kişiler, dört yıldan altı yıla kadar hapis cezasıyla cezalandırılır."*[56] Böylece yapılan bu değişiklik ile yurtdışı bahis sitelerine Türkiye üzerinden erişim sağlanmasına imkân tanımak suç sayılmıştır.

İnsanlık, bilişim sistemleri ile işlenebilen suçlarla ilk tanıştığında bu suçlar yalnızca ulus sınırları içerisinde sınırlı kalmaktaydı, fakat internetin ortaya çıkışı ve yayılması ile birlikte bilişim suçlarının sınırı ortadan kalkmış ve uluslararası bir boyut kazanmıştır. Bilişimin ve internetin sınırlarının olmadığı bu çağda, her geçen gün gelişen teknolojiyle birlikte devletlerin ve hukuk sistemlerinin bu alanda gelişmesi ve güncellenmesi kaçınılmaz olmuştur. Klasik suçlardan farklı olarak, bilişim suçlarının aynı anda birden fazla ülkede işlenebilir olması bilişim suçlarının ulusal sınırlarını ortadan kaldırmaktadır. Ceza suçlarının engellenmesine yönelik hazırlanan hukuksal düzenlemeler, düzenlendikleri ülkelerin sınırları ile sınırlı iken bilişim alanının sınırsız olmasıyla birlikte bilişim suçlarının işlenmesi ve bu suçların kovuşturulması ve faillerinin cezalandırılması açısından da ulusal sınırlar yeterli olamayacaktır.[57] Böylece sınırsız bir ağa sahip olan internet ile işlenebilen bu suçlar için artık suçun işlendiği ülkenin hukuk sistemleri ile sınırlı kalınması mümkün değildir. Böylece bir bilişim suçunun işlendiği yer ile sınırlı kalması uluslararası bilişim teknolojilerinin sınırsız olmasından dolayı hukukun korunması açısından artık mümkün olmayacaktır.

---

[56] 12.7.2013 kabul tarihli, 2.8.2013 Resmî Gazete yayın tarihli, 28726 yayın sayılı, 6495 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun

[57] Fisun Sokullu Akıncı, **"Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler Ve İnternette Çocuk Pornografisi"**, İstanbul, c.lıx s.1-2, 2001, s.12, (Çevrimiçi), https://dergipark.org.tr/tr/download/article-file/95989 Erişim Tarihi:30.04.2021

Uluslararası işlenen suçlar ve oluşan suçluluk, globalleşme ile gelen bir zorunluluktur.[58]

Bilişim teknolojilerinin uluslararası seviyede gelişmesi ile birlikte bilişim suçlarının globalleşmesi de kaçınılmaz olmaktadır. Her devlet, bilişim suçlarına yönelik hukuki düzenlemeler ortaya koysa da bilişim suçlarının çeşitliliği ve yaygınlığı ile birlikte bu düzenlemeler yeterli seviyeye ulaşamamakta ve bilişim suçlarının failleri yapılan düzenlemeler ile kendilerine kalan boşlukları suç işleme adına tespit ederek doldurmaktadır. Bir devletin hukuk sistemlerinde bilişim sistemleri ile işlenebilecek bir suçun düzenlenmiş olması ve o suçun işlenmesine yönelik erişim kısıtlamalarının getirilmesi, o devlette yer alan suçluların başka bir ulusal ağa bağlanarak yine kendi devlet sınırları içerisinde o suçun işlemesine engel olmayacaktır. Devletlerin hukuk sistemleri arasında oluşan bu farklılıklar, bilişim suçlarının önüne geçilmesinde en büyük engellerden bir tanesidir. Öyle ki, bir devletin milletine hâkim olan inanç sisteminden veya geleneklerinden dolayı yasaklamış olduğu bir suç, başka bir devlette hayatın olağan akışına uygun olabilecektir. Özellikle, çağımızda gelinen noktada internet sitelerine hâkim olan sanal bahis siteleri Türkiye'de her ne kadar kısıtlanmış olsa da farklı ülkelerin vpn ağlarına bağlanılarak bu suçun işlenmesi kaçınılmaz olmaktadır. Spor faaliyetleri üzerinden yasa dışı bahis oynatan online siteler günden güne daha fazla kitleye ulaşmaktadır.[59] Bu suç gibi, bir devletin kendi hukuk sisteminde düzenleme getirdiği bilişim suçlarının işlenmesinin önüne geçilebilmesi için, ulusal düzenlemeler ile birlikte uluslararası düzenlemeler ile hukuk sistemlerinin sesi suçlulara karşı ortak çıkmalıdır. Böylece hukuk sistemlerinde oluşturulacak uluslararası bir hukuk gücü, bilişim suçlarının işlenmesinin önünde daha sağlam durabilecektir.

Bilişim suçlarını faillerinin belirtilen şekilde ülke sınırlarından muaf olarak bu suçları işleyebilmesi ile yeni tartışmalar ve kavramlar ortaya çıkmıştır. Artık devlet sınırlarının bir öneminin olmadığı, devletler üstü bir siber devlet oluştuğunu ve bu

---

58 Hans-Jörg Albrect, **"Ululslararası Suçluluk, Şiddet Ekonomisi Ve İnsan Hakları; Ceza Hukukunun Cevapları",** Ord. Prof. Dr. Sulhi Dönmezler Armağanı, C.I, Çev. Yener Ünver, Ankara, AAM-TCHD Yayını, 2008, s.468(Aktaran) Dülger, 2015, a.g.e.,

59 Murat Balcı, **"Yasadışı Kumar ve Bahisle Hukuksal Mücadele",** Yeşilay Dergisi, 2021, sayı 1049, s. 20

devletin herhangi bir sınırlamaya tabi olmadığını ve artık vatandaşların devletlerinin değil, artık bu siber alanın vatandaşı olduğu fikri benimsenmeye başlamıştır. Buna göre, bilişim suçları toprak sınırına dayanmadan, herhangi bir sansüre maruz kalmadan ve yargısal yetkileri yetersiz kılarak işlenebilmektedir. Artık kişiler, sanal aleme geçince ulusal vatandaşlık kimliğini bırakıp internet vatandaşlığına geçmektedir.[60]

Belirtilen gaye ile bilişim kavramının insanlık terimlerine girdiği günden bu yana bilişim suçlarının artmasıyla birlikte ulusal ve uluslararası hukuksal çalışmaların ve düzenlemelerin yapıldığı görülmektedir. İşlenmiş suçlarla ilgili veri ve analizlere bakıldığında da bilişim suçlarının diğer suç tiplerine göre daha çok işlendiği ve son yıllarda katlanarak arttığı ortaya çıkmaktadır. Bilişim suçlarını düzenleyen ilk kanun tasarısı, senatör Ribikoff tarafından 1977 yılındaki ABD kongresine hazırlanmıştır.[61] Bu verilen kanun tasarısı teklifi kabul edilmemiş olsa da bilişim suçlarının tanınması adına ilk önemli girişim olarak kabul edilmektedir. Zamanla, devletlerin bilişim alanındaki çalışmaları ve teknolojik gelişmeler ile birlikte yapılan hukuksal çalışmaların sayısı artmıştır. Bilişim suçları Birleşmiş Milletler'in ve Avrupa Konseyi'nin bu alandaki çalışmaları ile birlikte, artık dünya devletlerinin gündemine girmiş, internetin yayılma hızıyla birlikte de hukuksal düzenlemelerin önemi devletler tarafından anlaşılmıştır.

2.3.2. Uluslararası Düzenlemeler

Bu değişim ve gelişimlerle birlikte bilişim teknolojilerindeki hukuki düzenlemelerin zorunluluğu ortaya çıkmakla birlikte, devletler ve hukuk sistemleri kanunlar ile toplumların ve devletlerin haklarını hukuki koruma altına alarak değişime ayak uydurmaktadır. Devletlerin, vatandaşlarını korumak ve kamu güvenliği ve düzenini sağlamak amacıyla enerji, gıda, iletişim gibi alanlarda düzenlemeler yaptığı

---

60 Dülger, a.g.e., 2015, s.192.

61 Ali Karagülmez**, "Bilişim Suçları Ve Soruşturma – Kovuşturma Evreleri"** 3. Baskı, Ankara, Seçkin Yayıncılık, 2011, s. 87

gibi bilişim alanlarında da hukuki düzenlemeler arayışı başlamıştır.[62] Tüm Dünya'da herkesin aynı anda ulaşabildiği, herhangi bir devlet veya hukuk sistemi sınırı veya ayrımı olmaksızın iletişime geçtiği, ticaret yaptığı, bilgi paylaştığı vb. durumların ortaya çıktığı esas alınırsa, ulusal düzenlemelerin yanında uluslararası düzenlemeler de kaçınılmaz olacaktır.

Ulusal ve Uluslararası alanda bilişim suçları alanında 1990'lı yıllardan itibaren çalışmalar devam etmektedir. Bilişim teknolojileri alanındaki denetim ve yaptırımların, bu alandaki teknolojik gelişmelerden çok daha sonra ortaya çıkması ve bu gelişime ayak uyduramaması sebebi ile, siber ortamların yaygınlaşmasıyla hızla artan uluslararası iletişim ve etkileşimlerde hukuka aykırı fiiller ortaya çıkmıştır. Bu fiiller ile, hakları ihlal edilen ve çeşitli zararları ortaya çıkan mağdurlar ile birlikte, siber suçlar ve suçlular da ortaya çıkmaktadır. Bu hukuk ihlallerinin sonucunda ortaya çıkan durumlara karşı düzenlenmesi gereken caydırıcı hukuki hükümlerin, uluslararası alanda oluşturulması ve bu hükümlerin hızla geliştirilmesi gerekmektedir.

Uluslararası alanda bilişim teknolojilerinin evrenselliği ve sınırsızlığına dair getirilen birçok hukuksal düzenleme vardır. Bu düzenlemelerin başında ise uluslararası hukukta bilişim suçlarını ilk düzenleyen sözleşme olan Avrupa Konseyi Siber Suç Sözleşmesi gelmektedir. Dünya çapında gerçekleşen bilişim suçlarına karşı ülkelerin ortak ve aynı kararlılıkla mücadele edebilmesi adına atılan en önemli adımlardan birisi olarak kabul görmektedir. 23.11.2001 kabul tarihli Avrupa Siber Suç Sözleşmesi Budapeşte'de bu tarihte devletlerin imzasına açılmıştır ve 01.07.2004 tarihinde yürürlüğe girmiştir.[63] Her ne kadar Avrupa Konseyi nezdinde akdedilmiş olsa da Siber Suç Sözleşmesine Avrupa ülkesi olmayan Japonya, Güney Afrika, Amerika Birleşik Devletleri ve Kanada müzakere aşamasına dahil edilmiştir. [64]Sözleşmenin yürürlüğe girmesi ile taraf devletler, iç hukuklarında bu sözleşmeye dair düzenlemeler yapma yükümlülüğü altına girmiştir. Avrupa Siber Suç

---

62 Bülent Kent, **"Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu"**, Ankara Sosyal Bilimler Üniversitesi Bilişim Hukuku Dergisi, Haziran, Sayı 1, 2020, s.6 (Çevrimiçi)

63 Cahit Aliusta, Recep Benzer, **"Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci"**, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C. 4, No:2, 2018, s.37 (Çevrimiçi)

64 Merve Erdem, Gürkan Özocak, **"Siber Güvenliğin Sağlanmasında Uluslararası Hukukun Ve Türk Hukukunun Rolü",** 04.06.2018, s.156 (Çevrimiçi)

Sözleşmesi'ne Türkiye, 10.11.2010 tarihinde imza atmış ve 22.04.2014 tarih ve 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onay vermiştir.

Bilişim suçlarının uluslararası düzenlemelerinde Avrupa Konseyi Siber Suç Sözleşmesi ve Ek Protokolü yanında, Avrupa Konseyi Çocukların Cinsel Suiistimal ve Cinsel İstismara Karşı Korunması Sözleşmesi, Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması, Batı Afrika Devletleri Ekonomik Topluluğu Siber Suçla Mücadele Direktifi Taslağı, Arap Devletleri Ligi Bilgi Teknolojilerine Karşı Saldırılarla Mücadele Anlaşması zikredilebilecektir.

Bilişim suçlarının uluslararası hukuktaki düzenlemelerinden bir tanesi de elektronik alanda yer alan unutulma hakkına dair düzenlemelerdi. Unutulma hakkı, bireyin hakkında özellik arz ederek geçmişte hukuka uygun bir şekilde cereyan eden hakkındaki doğru bilginin değişmesi ve ortadan kalkmasıyla birlikte güncelliğini kaybetmesi ve yayılmasının artık rızası dışında olup menfaatine aykırı olması sebebiyle kaldırılmasını talep etmesi ve mağduriyetini giderebilmesidir. Unutulma Hakkı, elektronik ortamda tam manasıyla ve unsurlarıyla birlikte Google İspanya kararı ile doğmakta ve tanınmaktadır. Karara konu olan İspanyol bir avukatın 1998 yılında sosyal güvenlik borçları nedeniyle mallarının haczedilmesi ve La Vanguardia gazetesi tarafından bu olayın yayınlanmasıdır.[65] İlgili avukat, bu borçları ödemiş olsa dahi internet üzerinden ismi Google'da aratıldığında bu haberler ilk olarak karşısına çıkmakta, hayatını ve yaptığı işi olumsuz etkilemektedir. Avrupa Birliği Adalet Divanı avukatın yaptığı itirazlar neticesinde bu bilgilerin elektronik ortamda yayınlamasının hukuka aykırılık oluşturacağına karar vermiş ve yayınların kaldırılmasına hükmetmiştir. İlgili karardan sonra Google bu tarz hak ihlallerinin önüne geçmek için bir başvuru linki oluşturmuş, günümüze kadar 100.000'in üstüne başvuru almıştır. Böylece bilişim alanında işlenebilecek bir suç hakkında yapılan yasal düzenlemeler ile yaptırımlar getirilmiş ve kişilerin haklarının korunması sağlanmıştır.

Bilişim suçlarının her geçen gün yaygınlaşması ve çeşitliliği ile, ülkelerin bu suçlara karşı ortak ve güncel düzenlemeler ile iş birliği yapması hukuk ve adaletin

---

[65] Hasan Elmalıca, **"Bilişim Çağının Ortaya Çıkardığı Temel Birİnsan Hakkı Olarak Unutulma Hakkı"**, Ankara Üni. Hukuk Fak. Dergisi, sayı 65, 2016, s. 1613 (Çevrimiçi)

tesisi için zorunlu hale gelmiştir. Suçlara karşı mücadelede, yaşanılabilecek zorluklara karşı ülkelerin hukuk normlarında uyum sağlanması, ortak farkındalıkla hareket etmesi ve birlikte adım atılması gerekmektedir. Ülkelerin bu hukuk dayanışması, bilişim sistemlerinin gelişme ve değişme hızı göz önüne alınarak hızlı ve güncel olmalıdır.

2.3.2.1. Fransa

Avrupa ülkelerinde bilişim hukuku ile ilgili yasal düzenlemeler yapan ilk ülkelerden bir tanesi Fransa'dır. Bilişim hukukuyla ilgili doğrudan bir düzenleme olarak görülmese de kişisel bilgilerin korunması doğrultusunda 1978 yılında çıkartılmış olan Bilgi Koruma Kanunu (Data Protection Law) ve oluşturulan Bilgi İşlem ve Özgürlükler Komisyonu (National Commission on Data Processing and Liberties) bu alandaki ilk adımlar olarak kabul edilmektedir.

Bilişim suçlarıyla ilgili önceleri klasik suçlarla ilgili düzenlemeler esas alınarak hukuki uygulamalar geliştirilmiş olsa da bilişim suçlarının önlenmesine yönelik ilk hukuki düzenlemelerden bir tanesi 1988 yılında Fransa kanunlarında yer almıştır. 5 Ocak 1988 tarihinde bilişim suçlarına ilişkin ilk müstakil düzenleme olan "Rêlative 'A La Fraude İnformatiqu" isimli Kanun ile Fransız Ceza Kanunu'nda bir düzenleme yapılmıştır.[66] Fransız Ceza Kanunu'nda ilk kez düzenlenen bilişim suçları düzenlemeleri ile Suça Teşebbüs ve iştirak, hukuka aykırı bir şekilde bilgisayara girme veya sistemde haksız yere kalma, bilişim sistemlerindeki verilere hasar verme, değiştirme, yok etme, bilişim sistemin işleyişini engelleme veya bozma, bilgisayar bilgilerinde sahte değişiklikler yapma, sahte bir şekilde düzenlenmiş belgeyi hukuka aykırı bir şekilde suç niyeti ile kullanma şeklinde beş tür bilişim suçu düzenlenmiştir.[67]

1 Mart 1993 tarihli Yeni FCK'da ise eski kanun ile aynı düzenlemeler korunmuştur.

Fransa, bilişim suçlarının büyük bir artış gösterdiği ülkelerden bir tanesidir. 1999 yılında, 1997 ve 1998 yılları arasında Fransa sınırları içerisinde bilişim suçlarıyla

---

66 Karagülmez, a.g.e., s. 119

67 Levent Kurt, **"Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması"**, Seçkin Yayıncılık, Ankara 2005 (Aktaran) Karagülmez, s. 119.

ilgili dava sayısında %33,49 oranında artış gerçekleşmiş ve bilişim sistemlerine karşı yirmi binden fazla saldırı düzenlenmiştir. [68]

2.3.2.2. Almanya

Bilişim sistemleri tarihinde bilinen uluslararası seviyedeki ilk korsan saldırı, 1989 yılında Almanya'da ABD'ye karşı gerçekleştirilmiştir. Sovyetler Birliği soğuk savaş döneminde ABD Savunma Bakanlığı'nın dosyalarına erişebilmek için bilişim sistemlerinde diğer ülkelere göre daha ileri seviyelerde olan Almanya'daki hackerleri kullanarak 1986 yılında "Cuckoo's Egg" (Guguk Kuşu Yumurtası) olarak bilinen bilişim saldırılarını gerçekleştirmiştir.[69]

Bilişim suçlarının ortaya çıkmasıyla birlikte, en çok suçun işlendiği ülkelerden birisi Almanya olmuştur. Ülkedeki ileri teknoloji kullanımı ve bilişim suçlarının ilk ortaya çıktığı zamanlardaki suç olanakları bu verilerde en önemli etken olarak görülmektedir. Almanya'da emniyet güçleri tarafında 2003'te yapılan bir araştırma sonucunda Almanya ekonomisi ülkede işlenen bilişim suçları sebebiyle 9 milyar Euro zarar görmüştür.[70]

Almanya'da da bilişim suçları, münhasır düzenlenen bir yasa ile değil, Ceza hukukunun içerisinde düzenlenmiştir. Yine Ceza hukuku dışında yer alan hukuki düzenlemeler ile bilişim suçlarına yönelik düzenlemelere yer verilmiştir. Almanya'da 13 Temmuz 1997 yılında bilişim sistemlerine yönelik suçları düzenleyen Teleservisler kanunu yürürlüğe girmiştir.[71] Bu yasa ile internet ortamında işlenebilecek suçlara yaptırım getirilmiş ve bilişim alanında hukuksal bir düzenleme yapılmıştır.

---

[68] Nichole, Atqill, **"Senior Legal Specialist Western Law Division Law Library Of Congess",** April, 2002, s.1,6 (Aktaran) Karagülmez, S. 122.

[69] Onur Şehitoğlu, **"Bilgisayar ve Ağ Üzerinden İşlenen Siber Suçlarla Mücadelenin Hukuksal Ve Güvenlik Boyutu",** Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2004, S.147 (Aktaran) Karagülmez, S. 123.

[70] Şehitoğlu, a.g.e., s. 147

[71] Rüya Şamlı, **"Türk ve Dünya Hukukunda Bilişim Suçları, Akademik Bilişim"** 10 - XII. Akademik Bilişim Konferansı Bildirileri, 2010 s.66. (Çevrimiçi) https://ab.org.tr/ab10/kitap/samli_AB10.pdf Erişim Tarihi:30.04.2021

2.3.2.3. İngiltere

1997 yılına kadar İngiltere üzerinde bilişim alanında gerçekleştirilen çalışmaları İngiliz bilim insanı Hollinger dört döneme ayırır.[72] İlk periyot 1946-1976 yılları arasıdır. Bu periyotta suçu keşfetme dönemi telefon ile işlenen suçlar ile başlar. İkinci periyot olan suça dönüşme süreci ise 1977'den 1988'e kadar devam eder. Üçüncü periyot 1989 yılından 1993 yılına kadar süren bilişim korsanlarının (hacker) profesyonelleşme sürecidir. Bu periyotta artık bilişim suçluları tam manasıyla hukuka karşı zafer dönemini yaşamışlarıdır. Son dönem ise 1993 yılı sonrası dönemdir. Bu dönem artık denetim dönemi olacaktır.

İngiltere'de bilişim suçlarının hukuk sistemlerine girişi ise 29 Haziran 1990 yılında müstakil bir şekilde düzenlenen "Computer Misuse Act" (CMA) adlı kanun ile gerçekleşmiştir.[73] İngiltere, bilişim suçlarının ilk işlendiği ve bu suçların işlenmesini engellemeye yönelik ilk hukuki düzenlemelerin yapıldığı ülkeler arasında sayılmaktadır.

CMA, 18 kısımdan oluşan "Computer Misuse Offences", "Jurisdiction" ve "Miscellaneous and General" başlıklı üç bölüm olarak düzenlenmiştir. [74]

CMA'da düzenlenen 3 maddede 3 farklı bilişim suçu çeşidi vardır. Bunlardan birincisi, yetkisiz erişim suçudur. Suçun oluşması için yetkisiz bir erişimin gerçekleşmesi, CMA'da yeterli olarak kabul edilmiştir.

CMA'nın 2. Maddesinde ise başka bir suçun işlenmesini kolaylaştırmak amacıyla suç işlemek düzenlenmiştir. Yani, bilişim suçunu işlemek gibi, başkası tarafından gerçekleştirilecek bilişim suçunun işlenmesine bilerek ve isteyerek yardımcı olmak ve suçun işlenmesini kolaylaştırmak da suç olarak düzenlenmiş ve cezai yaptırımlara bağlanmıştır.

CMA'nın 3. Maddesinde ise Yetkisiz Değiştirme – Müdahale suç tipi düzenlenmiştir. Bu suç tipine göre, bir bilişim sistemine izinsiz ve yetkisiz erişim

---

72 Murat Volkan Dülger, **"Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması",** Türkiye Adalet Akademisi Dergisi, Yıl:8, Sayı:31, Temmuz 2017, S. 151. (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/981531 Erişim Tarihi:30.04.2021

73 Karagülmez, s. 113

74 Yazıcıoğlu s. 194, Karagülmez, s. 115

sağlanması ve bilişim sisteminin içeriğinin değiştirilmesi, bilişim sisteminin bütünlüğünün bozulması, bilişim sistemindeki verilere izinsiz bir şekilde müdahale edilmesi, değiştirilmesi, çalınması veya erişiminin engellenmesi bilişim suçunu oluşturmaktadır.

İngiltere hukuk sisteminin bilişim hukuku adına münhasır bir hukuki düzenleme yapması bilişim suçlarının engellenmesi adına olumlu gözükmektedir. Fakat CMA hukuksal tartışmalara da sebebiyet vermiştir.

Kabul edildiği tarihten sonra bilişim sistemlerinin gelişmesi ve bilişim suçlarındaki çeşitliliğin artması ile CMA'nın artık bileşim sistemlerindeki tüm suç tiplerini karşılamadığı ve artık güncellenmesinin ve genişletilmesinin gerektiği İngiltere'de tartışılmaktadır. [75] CMA'nın başarısı, kapsayıcılığı ve güncelliği konusunda yapılan eleştiriler, CMA'nın bilişim suçlarıyla mücadele ederken başarılı olup olmadığı yönünde devam etmektedir.

2.3.2.4. İtalya

İtalya'da bilişim suçlarına yönelik hukuki tartışmalar 1990'lardan önce başlamıştır. Bir görüşe göre İtalya hukukunun eksiksiz olduğu ve kapsayıcılığı benimsenirken başka bir görüşe göre ise bilişim suçlarına yönelik yeni hukuksal düzenlemelere gidilmesi kaçınılmaz olmuştur. Yapılan tartışmalar neticesinde ise bilişim hukukunun kaçınılmaz olduğu artık kabul edilmiştir.

İtalya'da hakimler, akademisyenler ve bilişim alanında önde gelen isimlerden oluşan komisyon 1989 yılında Adalet Bakanlığı bünyesinde kurulmuş ve bilişim hukukuna yönelik çalışmalar gerçekleştirmiştir. Bu çalışmalar sonucunda hazırlanan kanun tasarı, 23 Aralık 1993 tarihli 547 sayılı Kanun metniyle İtalya hukukunda yürürlüğe girmiştir.[76] Kabul edilen bu yasayla birlikte İtalyan Ceza Kanunu'nda birtakım değişikliklere ve eklemelere gidilmiştir.

---

75 Karagülmez, a.g.e., s. 116.

76 Karagülmez a.g.e., s. 109.

Yapılan değişiklikler ve eklemelerle birçok bilişim suçunun yasalara girdiği görülmektedir. Örneğin, İtayla Ceza Kanunu madde 420 ile, kamusal yararı bulunan sistemlere zarar verme veya bu sistemleri yok etme suçu düzenlenmiştir.

Madde 392'de eşyaya zarar verme suçu düzenlenmiştir. 1993 tarihli değişiklikler ile birlikte maddedeki eşya tanımına bilişim sistemlerini de kapsayıcı hale gelmiş ve bilişim sistemlerine saldırı suç olarak düzenlenmiştir.

Yine aynı değişiklikler ile 491. Madde 'de düzenlenen sahtecilik suçlarına, bilişim belgeleri tanımı da eklenmiştir.

1993'te yapılan değişiklikler ile ayrıca yetkisiz erişim ve müdahaleler, bilişim sistemlerine müdahale etme, bozma, zarar verme ve çalışmasını engelleme, bilişim haberleşmelerinin engellenmesi, dinlenmesi ve araya girilmesi, bilişim verilerinin tahrip edilmesi, bilişim sistemleri aracılığıyla dolandırıcılık yapma, çocukları pornografide kullanma gibi suçlar düzenlenmiştir.

2.3.2.5. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri, teknolojideki ileri atılımları sonucunda internetin dünyaya yayıldığı ve en çok kullanıldığı ülkelerden bir tanesidir. Öyle ki ülke ile ilgili olarak internet ve bilgisayar kavramlarının doğduğu yer demek abartı olmayacaktır. Bununla birlikte bilişim sektörü de diğer devletlere göre hızla ilerlemiş, en önemli ve büyük bilişim şirketleri bu ülkede doğmuştur. Apple, Google, Microsoft, Amazon ve E-Bay gibi dünya devi şirketlerin hepsi Amerika menşeilidir. Bilişim sistemlerindeki önde gelen bu çalışmalar ve bilişim sistemlerinin doğduğu yer denilebilecek kadar bu alanda öncü olan Amerika Birleşik Devletleri'nde bilişim suçlarının hızlıca artması ve büyük etkilere sebep olması bilişim hukuku alanındaki çalışmalara olan ihtiyacı arttırmıştır.[77] Sayılan şirketler gibi nice dünya devi markaların Amerika menşeili olması, Amerika'ya ayrıca bu şirketlerin güvenliğini sağlama yükümlülüğü de getirmiş ve bu yönde yapılacak düzenlemelere teşvik etmiştir.

[77] Dülger, a.g.e., 2015, s. 213.

Amerika Birleşik Devletleri, bilişim hukukuna yönelik hukuki düzenlemeleri ile bu alandaki ilk yasa düzenlemelerinin merkezi olmuştur. 08.02.1996 tarihli "İletişim Ahlakı Yasası" bilişim sistemleri ve internete yönelik suçlara karşı oluşturulan ilk hukuksal düzenlemedir.[78] Ayrıca, bilgisayar suçlarıyla ilgili olarak da 1984 yılında "Bilgisayar Sahtekarlığı ve Bilgisayarları kötüye kullanma Kanunu" yürürlüğe girmiştir. Avrupa Konseyi üyesi olmayan bir devlet olmasına rağmen ABD Avrupa Siber Suç Sözleşmesi'ne taraf olmuştur.[79]

Amerika Birleşik Devletleri'nde, bilişim hukuku alanında hem federal hem de federe devletler tarafından kanuni düzenlemeler yapılmıştır. Federal devlet tarafından bilişim alanında düzenlenen ilk kanun olan CFAA (Computer Fraud and Abuse Act) yürürlüğe girdiğinde 47 federe devlet bilişim hukukuna yönelik düzenlemeleri hukuk sistemlerine entegre etmişti. [80]

CFAA, yani Bilgisayar sahtekarlığı ve bilgisayarların kötüye kullanılması yasası) 1984 yılında yürürlüğe girmiştir ve bilişim alanında Amerika Birleşik Devletleri'nde federal düzeyde düzenlenen en önemli ve ilk hukuk düzenlemesi olmuştur.

CFAA ile bir takım temel bilişim sorunları düzenlenmiş ve bilişim suçlarının önüne geçilmesi hedeflenmiştir. Bunlar, Amerika Birleşik Devletleri'nin kamusal ya da özel bilgilerinin izinsiz ve yetkisiz erişilerek ABD'nin zararına kullanılmasını engellemek, bilişim sistemlerine suç işlemek kastıyla izinsiz ve yetkisiz müdahalelerde bulunmak, hükümetin bilişim sistemlerine erişmek, erişimi engellemek ve veri hırsızlığı yapmaktır. İlerleyen yıllarda CFAA'da değişiklikler yapılarak getirilen hukuki düzenlemeler genişletilmiş ve kapsayıcılığı artırılmıştır.

Amerika Birleşik Devletleri, CFAA haricinde devam eden yıllarda bilişim hukuku alanında yasal düzenlemeler hazırlamaya devam etmiştir. 1992 tarihli Elektronik Haberleşme Gizlilik Kanunu (Electronic Communications Privacy Act),

---

78 Fatih. S. Mahmutoğlu, **"Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu",** S.41 (Çevrimiçi) Https://Dergipark.Org.Tr/Tr/Download/Article-File/95993 Erişim Tarihi: 30.04.2021

79 Dülger, a.g.e., 2015, s. 213

80 Burak Cesur Akgöz, a.g.e., s.205

1996 yılında yürürlüğe giren İletişim Ahlak Yasası (Communications Decency Act) ve Çocuk pornografisinin önlenmesi yasası (Children Pornografy Prevention Act), 1997 yılında yürürlüğe giren İnternette Kumarın Önlenmesi Kanunu (Internet Gambling Prohibiton Act) bunlardan bazılarıdır.

Amerika Birleşik Devletleri çıkardığı yasalarla birlikte, sürekli güncellenen bilişim sistemlerinin ve suç çeşitlerinin takibi amacıyla Adalet Bakanlığı'na bağlı bir birim olan CCIPS'i (Computer Crime And Intellectual Property Section) oluşturmuştur., 1991 yılı ile birlitke18 savcı yalnızca Bilgisayar Suç Birimi çalışma alanıyla CCIPS'de faaliyet yürütmektedir.[81] CCIPs,'in takip ettiği üç önemli amaç vardır: *"Bilgisayar ve fikri mülkiyet suçlarından caydırmak ve bu suçları engellemek, soruşturma aşamasında elektronik kanıtların toplanmasına yardım etmek ve hukuki tavsiyelerde bulunmak, Amerika Birleşik Devletleri'nin dünyadaki savcılarına ve soruşturmacılarına yardımda bulunmak*"[82]

2.3.2.6. Japonya

Japonya, 1980'li yılların sonunda bilişim alanında hukuksal düzenlemeler yapmaya başlayan ülkelerden bir tanesidir. Avrupa ülkelerinde görüldüğü gibi Japonya'da da bilişim suçları münhasır bir düzenleme olarak değil, ceza kanununda yapılan güncellemeler ve eklemeler ile yasalaşmış ve yürürlüğe girmiştir.

Dünya'da teknoloji denince ilk akla gelen ülkelerden biri olan Japonya'nın, bu başarıyla birlikte bilişim hukukunda ilk reformları yapmış olması kaçınılmaz olmuştur. Japonya, 22.06.1987 tarihli "Ceza Hukuku Alanında Bazı Hükümlerde Değişiklik Yapılmasına İlişkin Kanun" ile birlikte bilişim suçlarına yönelik düzenlemeleri ceza kanunu aracılığıyla yürürlüğe sokmuştur. 2000 yılında yürürlüğe giren Bilgisayara yetkisiz erişim kanunu (Unauthorized Computer Access Law) ile de

---

81 Karagülmez, a.g.e., s.95

82 Computer Crıme And Intellectual Property Sectıon (CCIPS), (Çevrimiçi), https://www.justice.gov/criminal-ccips Erişim Tarihi: 25.04.2021

yetkisiz erişim ve müdahale, yetkisiz erişim ve müdahalenin kolaylaştırılması ve bilişim suçlarına yönelik cezai müeyyideler düzenlenmiştir. [83]

[83] Dülger, a.g.e., 2015, s. 226

ÜÇÜNCÜ BÖLÜM

3. 5237 SAYILI TÜRK CEZA KANUNU MADDE 243,244 ve 245'in İNCELENMESİ

Bilişim sistemlerinin gelişmesi ile birlikte klasik suç – sanal suç farkı ortadan kalkmış, gerçek hayatta yaşanan hukuk ihlallerinin boyutunu aratmayacak suçlar bilişim sistemlerinde işlenmeye başlanmıştır. Böylelikle Türkiye'de de Avrupa'da yapılan düzenlemeler örnek alınarak iç hukuk sistemine entegre çalışmalarıyla birlikte bilişim suçlarına yönelik düzenlemeler açısından birtakım adımlar atılmıştır. Kuşkusuz bu yönde atılan en büyük hukuki adım, yeni TCK ile getirilen düzenlemeler olmuştur. 26.9.2004 kabul tarihli 5237 sayılı Türk Ceza Kanunu, bilişim suçlarına yönelik özel bir başlık altında hükümler getirmiştir. "Bilişim Alanında Suçlar" başlıklı onuncu bölümde düzenlenen hükümler üç madde altında toplanmıştır.[84]

3.1. BİLİŞİM SİSTEMİNE GİRME VEYA SİSTEMDE KALMA SUÇU (M.243)

3.1.1. Genel Olarak

5237 sayılı TCK'nın 243. Maddesinde düzenlenen "Bilişim Sistemine Girme" kenar başlıklı hükmüne göre *"1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı*

[84] Özbek, Doğaan, Bacaksız, a.g.e., s. 961

oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. (4) (Ek:24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakilleri, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır." Kanun koyucu düzenlenen bu madde ile bilişim sistemlerine hukuka aykırı olarak girmeyi veya bilişim sistemlerinde hukuka aykırı kalmaya devam etmeyi suç saymıştır.

Mülga 765 sayılı TCK ile düzenlemeyen bilişim sistemine girme suçu, 5237 sayılı TCK ile hukuk sistemimizde ilk kez düzenlenmiştir. Bilişim sistemlerinin daha etkin bir şekilde korunması için kanun koyucu bu fiili suç olarak düzenlemiştir. Ayrıca, Avrupa Siber Suç Sözleşmesinin 2. Maddesi ile taraf devletlere getirilen bilişim sistemlerine kasten ve haksız erişimin engellenmesine yönelik tedbirlerin alma yükümlülüğüne de uyulmuştur.[85]

243. maddenin iki suç içerdiği görülmektedir. Bunlardan ilki bilişim sistemlerine girme suçudur. Bu suçun oluşabilmesi için bir bilişim sistemine bilişim sisteminin sahibinin rızası ve izni olmaksızın yetkisiz bir şekilde erişmek suçun icrası için yeterli olacaktır. Bilişim sistemlerine bahsedildiği gibi yetkisiz erişim suçu, bilişim suçlarının en sık işlenen türüdür.[86] Bu suç tek başına bir suç olduğu gibi genellikle başka suçlara aracı suç olarak da kullanılmaktadır.

3.1.2. Korunan Hukuki Yarar

5237 sayılı Türk Ceza Kanunu'nda bilişim suçlarının ikinci kitapta *"topluma karşı suçlar"* bölümünde düzenlendiği görülmüştü. Buradan da anlaşılacağı üzere, bilişim suçlarının engellenmesi ile TCK öncelikle toplumsal düzenin korunmasını amaçlamaktadır. Bilişim sistemlerine girme veya orada kalma suçu ile de korunan hukuki değer konusunda bazı görüşler ileriye sürülmüştür.

---

85 Koca, Üzülmez, a.g.e., s. 806

86 Dülger, a.g.e., 2015, s. 343

Karagülmez 'in görüşüne göre düzenlenen suç ile korunan hukuksal değer: *Maddedeki fiildeki temadi (kalmaya devam etme), suçun unsuru niteliğinde olduğuna göre korunan hukuki yarar, bilişim sistemini kullananların belli bir süreden sonra rahatsız edilmemesidir. Bunun yanında, suçun hedefi durumundaki sistem kullanıcılarının (sahiplerinin) çıkarlarının zedelenmemesi de korunan hukuki yararlar arasındadır."*[87] Dolayısıyla yazar, bu suç ile kişilerin zarar görmesinin engellendiğini savunmuştur. Bu görüşe göre, bilişim sistemine erişilmesi veya orada kalınması ile her türlü zarar gören ve menfaatleri etkilenenler bilişim sistemi kullanıcılarıdır.

Dülger'in görüşüne göre: *"Bu suçla korunan hukuksal değer bilişim sisteminin güvenliğidir. Bilişim sistemine hukuka aykırı erişimin engellenmesiyle, sistemin maliki ya da kullanıcısı gibi bir şekilde sistemden faydalana kişilerin çok sayıdaki farklı türden çıkarları koruma altına alınır."* [88] Bu görüşe göre bu suç ile korunan hukuki yarar, kişilerin haklarının ihlali ve dolayısıyla bilişim sistemlerinin güvenliğinin korunmasıdır. Bilişim sistemlerinin korunması ile de çağımızın en önemli iletişim ve hizmet aracı olan bilişim alanı suçlardan ve hak ihlallerinden uzak kalarak toplumsal güven oluşacaktır.

Konuyla ilgili Yazıcıoğlu'nun görüşüne göre ise bir yandan bilişim sistemlerinin ve mülkiyet hakkının güvenliği korunarak bir yandan da Anayasa'nın 20. Maddesi ile düzenlenen özel hayatın korunmasının bilişim sistemleri kullanılarak ihlal edilmesi engellenmek istenmiştir.[89]

Farklı görüşler de incelendiğinde, suçla korunan hukuki yararların birden fazla olduğu, sistemin veya kişinin korunmasının yanında toplumun düzeninin ve özel hayatın gizliliğin korunması da amaçlanmaktadır. Tüm görüşler incelendiğinde ve kanun maddesi ile birlikte diğer bilişim suçlarının kanundaki yeri göz önüne alındığında 243. Madde ve kanun maddesinde düzenlenen suç ile korunan hukuki yararın karma olduğu söylenebilecektir. Suç ile öncelikle bilişim sistemlerinin korunduğu ve bilişim sistemlerine hukuka aykırı bir şekilde erişilmesinin veya orda

---

87 Karagülmez, a.g.e., s. 180

88 Dülger, a.g.e., 2015, s. 348

89 Yılmaz Yazıcıoğlu, **"Hukukumuzda TCK'nın 243. Maddesi Kapsamında Bilişim Sistemine girme Eylemi"**, Bilişim Hukuku Konferansı (09-10 Ekim 2008) (Aktaran) Özbek, Doğan, Bacaksız, a.g.e., s.962

kalınmasının engellediği görülmektedir. Bilişim sistemlerinin korunması ile birlikte kullanıcıların özel hayatı ve menfaatleri de korunacak ve toplumsal düzene karşı oluşabilecek suçlar engellenmiş olacaktır.

3.1.3. Suçun Maddi Unsurları

3.1.3.1. Fail

Ceza hukukuna göre fail, kanunda düzenlenen suç tanımındaki fiili gerçekleştiren kişidir. Tüzel kişiler işlenmiş bir suçun faili olamayacak, ancak güvenlik tedbirleri ile cezalandırılabileceklerdir.[90] *TCK'nın 20. Maddesi de fail hakkında açık bir şekilde düzenleme yapmıştır: "(1) Ceza sorumluluğu şahsidir. Kimse başkasının fiilinden dolayı sorumlu tutulamaz. (2) Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır."*

Kanun koyucu, 243. madde ile düzenlediği hüküm içeriğinde fail ile ilgili "kimse" ifadesini kullanmıştır. Hükümden anlaşıldığı üzere "giren" veya "kalmaya devam" eden "kimse" suçun faili olabilecektir. Bundan da anlaşılacağı üzere suçu işleyecek kişi için herhangi bir özellik taşıyan unsur belirtilmemiştir. Bu suçun faili herkes olabilecektir.

3.1.3.2. Mağdur

243. Madde metni incelendiğinde mağdur ile ilgili de herhangi bir özel düzenlemeye rastlanılmamaktadır. Böylelikle bu suçun mağduru da fail gibi herkes olabilecektir. Bu suçun icrası ile bilişim sistemine hukuka aykırı bir şekilde girilen

[90] Cengiz Apaydın, **"Bilişim Suçları ve Bilişim Ceza Hukuku"**, İstanbul, Mart 2017, s. 51

veya bilişim sisteminde hukuka aykırı bir şekilde kalmaya devam edilen kişi bu suçun mağdurudur. Suçun oluşması ve kişinin mağdur olması için yapılan erişimin kişinin rızası olmadan hukuka aykırı bir şekilde yapılması gerekmektedir. Bilişim sistemlerine erişim için rıza göstermiş olan bir kişi, sistemlerine erişilmesi veya sistemlerinde kalınması durumunda mağdur sıfatına haiz olamayacaktır. Kanun koyucu maddede *"hukuka aykırı"* ifadesi ile açık bir şekilde mağdur olunabilmesi için işlemin hukuka aykırı olmasını belirtmiştir. Böylelikle bilişim sistemine rızası olmadan hukuka aykırı olarak 3. Kişiler tarafından erişilen kişiler bu suçun mağduru olacaklardır.

Bilişim sistemine girilmesiyle birden fazla kişinin hakları ihlal ediliyorsa, hakkı ihlal edilen her kişi mağdur sıfatını kazanabilecektir.[91] Mağdur olabilmek için kişi veya kişilerin bilişim sistemi üzerinde hak veya yetki sahibi olması ve rızasının aranması gerekmektedir. Hukuka aykırı olarak girilen bir sistemde birden çok kişinin erişim yetkisi olması mağdur sayısını artıran bir etken olmaktadır.

3.1.3.3. Suçun Konusu

Suçun konusu, madde metninde düzenlenen suçtaki hareketin yöneldiği kişi ya da nesne olarak ifade edilebilecektir. 243. Madde fıkralarına ayrılarak incelendiğinde, birinci fıkrada düzenlenen suçun konusu bilişim sistemidir. Maddenin 2. Fıkrasında "*bedeli karşılığı yararlanılabilen sistemler"* ifadesi geçmektedir. Böylece 2. Fıkra ile düzenlenen suçun konusunu bedeli karşılığı yararlanılabilen sistemler oluşturacaktır. Son fıkrada ise sistemdeki verilerin yok olması veya değiştirilmesi düzenlenmiştir. Böylece son fıkrada düzenlenen suçun konusunu da bilişim sistemlerindeki veriler oluşturacaktır. Eğer hukuka aykırı bir şekilde girilen sistem bilişim sistemi değil ise, 243. Madde ile düzenlenen suç oluşmayacaktır. [92]

---

91 Artuk, Gökçen, Yenidünya, a.g.e., s.866

92 Koca, Üzülmez, a.g.e., s. 810

3.1.3.4. Hareket

Hareket, kanunda belirtilen suçun icrası için kişilerin gerçekleştirdiği eylemler veya ihmallerdir. Her hareket suça konu olamayacağı gibi, suç sayılan hareketlerin oluşması için de kişilerin hareketinin hukuka aykırı bir şekilde oluşması gerekmektedir. Suçun gerçekleşmesi için aranan maddi unsurlardan birisi olan hareket, bazen bir nedene bağlı olarak suç sayılabilecektir. Bazen de sırf hareketin gerçekleşmiş olması suçun icrası için yeterli olacaktır. Bazı suçlar için birden fazla hareketin birleşmesi gerekirken bazı suçlar için de seçimlik olan birden fazla suç kanun maddesinde düzenlenebilmektedir.

TCK'nın 243. Maddesinde düzenlenen suçta, suçun gerçekleşmesi için bilişim sistemine girme veya orada kalma hareketlerinden herhangi birisinin gerçekleşmesi düzenlenen suçun icrası için yeterli olacaktır. Suçun hareket unsurunun oluşması için bu iki seçimlik hareketten birisi gerçekleşmelidir.

Madde metninde belirtilen *"girme"* ifadesi farklı şekillerle yorumlanabilecektir. Bilişim sistemi ifadesi ile sanal ortamla birlikte fiziki bilişim sistemlerinin de kastedilmesi mümkündür. Bir kişinin bilgisayarına, telefonuna veya başka bir teknolojik aletine hukuka aykırı bir şekilde kişinin rızası alınmadan fizikken müdahale edilmesi de bir suç oluşturabilecektir. Fakat bu suç, TCK 243 ile düzenlenen bilişim sistemlerine girme suçunu değil TCK 151'de düzenlenen mala zarar verme suçunu oluşturacaktır. 243. Maddede belirtilen bilişim sistemlerine girme hareketi fiziksel bir girme hareketi değil bir bilişim sistemine erişmeyi ifade etmektedir.

Böylece kanun maddesi incelendiğinde iki seçimlik hareket ile bu suçun icrasının mümkün olacağı görülmektedir. Bunlardan birincisi bilişim sistemlerine girme/erişme hareketi bir diğeri de bilişim sisteminde kalmaya devam etme hareketidir. Her iki hareket için de hukuka aykırılık unsuru geçerlidir. İki hareket için de herhangi bir süre kanun maddesinde düzenlenmemiştir. Hareketlerden yalnızca birinin gerçekleşmesi suçun icrası için yeterli olacaktır.

Bilişim sistemine girilmesi veya orada kalınması ile 243. Madde ile düzenlenen suç oluşmuş olacaktır. Ayrıca bir başka suçun gerçekleşmesi suçun icrası için

aranmamaktadır. Yargıtay 11. Ceza Dairesi bir kararında: *''sanığın, katılanın yetkilisi olduğu Z. Limited Şirketi'nin Türkiye Ekonomi Bankası D. Şubesinde bulunan hesabına internet üzerinden giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında, sanığın eyleminin 5237 sayılı TCK m.243/1'de düzenlenen suçu oluşturduğu...''* diyerek sanığın hesaba giriş yaptıktan sonra herhangi bir harekette bulunmasa da suçu oluşturduğunu vurgulamıştır.[93]

243. maddenin 3. Fıkrasıyla düzenlenen hükme göre failin ağırlaştırılmış ceza ile yargılanabilmesi için ise bilişim sistemine haksız bir şekilde girilmesiyle birlikte bilişim sistemindeki verilerin değiştirilmesi veya yok edilmesi gerekmektedir. [94]

Suçun maddi unsurları değerlendirilirken, suçun işlenme şekillerinden de bahsetmek faydalı olacaktır. Bilişim suçları, her an, her yerde, suçun ortaya çıkması için herhangi bir ön hazırlık yapılmasına dahi gerek olmadan, çok hızlı ve gizli şekillerde ortaya çıkabilecektir. Bilişim suçlarının değişme, büyüme ve yayılma hızıyla paralel bir şekilde bilişim suçlarının tespit edilmesi ve önlemler alınması da hızlanmalı, kapsayıcı hukuksal düzenlemeler ile bu suçların işlenme şekillerinin önüne geçilmeli ve caydırıcılığı artırılmalı, bu yöntem için de gerekli siber altyapının oluşturulması gerekmektedir. Her gün büyüyen, ucu bucağı sınırlandırılamayan bir alandan her an farklı bir suç şekli ortaya çıktıkça, sayılı kuralların bu suçları önlemede yeterli olmayacağı aşikardır.

Bilişim suçlarının işlenme şekillerinde de farklılıklar görülmektedir. Bilişim suçlarının işlenebilmesi için, suçun bilişim alanında ya da bilişim alanına yönelik yapılması gerekmektedir. Sürekli değişen, yenilenen ve genişleyen bilişim alanında, hukuka aykırılıkların ortaya çıkma şekilleri ve suç tipleri, her geçen gün değişecek ve genişleyecektir. Bu suçların sayılması ve sınırlandırılması mümkün olmadığı için, belirli suç çeşitleri üzerinde durulacaktır.

Bilişim sistemlerine girme ve orada kalma suçu çeşitli yöntemler ile gerçekleştirilebilmektedir. Bilişim alanında yapılan siber saldırılar ve işlenen suçlar

---

93 Karagülmez, a.g.e., s.202

94 Özbek, Doğan, Bacaksız, a.g.e., s.967

gündeme alındığında, en çok karşılaşılan suç tiplerinden birisi Truva Atı (Trojan Horse) saldırılarıdır. Truva atı, mağdurun bilişim sistemine uzaktan erişilerek suç unsurlarının ortaya çıkarabilmesidir. Öyle ki mitoloji incelendiğinde Homeros'un Odise adlı eserinde, Yunanlıların Truva bölgesini uzun dönemler boyunca kuşattıklarını fakat bir türlü şehre hakim olamadıklarını ve son savaş stratejisi olarak onlarca askeri devasa boyutta yapılan atın içerisine saklayarak bu atı şehre hediye ederek ve atın içerisindeki askerlerin şehrin içerisine girildikten sonra şehrin kapılarını dışarıda bekleyen orduya açmalarıyla şehre girmeyi başardıkları görülmüştür.[95] Truva Atı adı verilen casus yazılım da, kişi veya kurumların telefon, bilgisayar, tablet vb. bilişim araçlarına erişilebilmesi, yönetilebilmesi ve değişiklikler yapılabilmesi için bilişim araçlarının arka kapılarını faillere açan bir yazılım türüdür. Mağdur, kendi rızası ile indirdiği ve ihtiyacını veya isteğini karşılayacağını düşündüğü dosyalarla, programlarla veya oyunlarla aslında Truva Atına bilişim aracının kapılarını açmış olur. Truva atı içeren yazılım, görünüşte ne kadar faydalı bir içerik veya program olarak gözükse de zararlı bir yazılımdır.[96] Truva Atları kendi kendilerine işlem yapamayan ve kendilerini çoğaltamayan, virüsler gibi saldırgan değil de faydalı gözüken yazılımlar olduğu için virüslerden ayrılmaktadır. Failin, mağdurun rızası ve haberi olmadan bilişim sistemine Truva atını yerleştirmesiyle ve bu yazılım vasıtasıyla erişim sağlamasıyla, fail mağdura yönelik suçunu gerçekleştirmiş olacak, suç unsurları tamamlanmış olacaktır.

Truva atları ile bilişim suçları çeşitli yöntemlerle işlenebilmektedir. En yaygın Truva atı türü Truva arka kapılarıdır. Bu yazılım ile fail, mağdurun bilgisayarını mağdur fark etmeden dahi kullanabilecek, çeşitli işlemleri mağdurun IP'si üzerinden gerçekleştirebilecektir. PSW yani parola Truva atları ise, mağdurun bilgisayarındaki tüm şifreleri kırmaya yönelik saldırlar bulunan bir yazılım türüdür. Truva casusları isimli saldırı türüyle ise casus yazılım, bilişim sistemi kullanıcısının ekran kayıt ve görüntüleri gibi hareketlerine erişim sağlarken, anahtar kırıcı Truva atıyla kullanıcının

---

95 Gürol Canbek, Şeref Sağıroğlu, **"Kötücül Ve Casus Yazılımlar: Kapsamlı Bir Araştırma",** (Çevrimiçi), https://dergipark.org.tr/tr/download/article-file/75575 Erişim Tarihi : 20.04.2021

96 Altunok, Vural, a.g.e., s.78

bilgisayar sisteminde klavye üzerindeki tüm hareketlerini kayıt altına alarak faile gönderir.

Bilişim sistemine girme ve orada kalma suçunun işlenmesineki en çok kullanılan yöntemlerden bir diğeri ise Süper Darbe (Süper Zapping) tekniğidir. Süper Darbe bir tanıma göre: *"Bilgisayar sistemlerinin çeşitli sebeplerle işlenmez hale gelmesi yani kilitlenmesi durumunda çok kısa bir süre içerisinde tekrar çalışmasını sağlamak üzere güvenlik kontrollerini aşarak sistemde değişiklik yapılabilmesi için geliştirilmiş bir programdır."*[97] Süper Darbe programı, tanımından da anlaşılacağı üzere aslında kullanıcıya fayda sağlayacak bir program olarak tasarlanmıştır. Fakat, saldırganlar bu programı kullanarak bilişim sistemindeki tüm güvenlik duvarlarını geçerek sistemi ele geçirebilmektedir. Böylece, kullanıcının bilgisi ve izni olmadan bilişim sistemlerine saldırganlar ulaşabilmektedir.

Bir diğer suç işlenme şekli ise İstenmeyen Mail (SPAM) tekniğidir. Bir tanıma göre SPAM: "*İstenmeyen elektronik posta manasına gelir."*[98] Başka bir tanıma göre is SPAM, *"Genel olarak internet ortamından aynı mesajın sayısız kopyası çıkarılarak mesaj konusu ile ilgili talebi olmayan kişilere istekleri dışında gönderilmesi şeklinde tanımlanmaktadır."* [99] E-posta kutularına haksız bir şekilde müdahalelerde genellikle SPAM yöntemi kullanılmaktadır.[100] İnsanlık, tarihte ilk kez SPAM içeren bir iletiyle 1 Mayıs 1978 tarihinde, Amerika Birleşik Devletleri'nin batı kıyısında olan tüm ARPANET adreslerine DEC-MARLBORO firmasının gönderdiği ürün tanıtımı içeren iletileriyle tanışmıştır.[101]

---

97 Oğuz Turhan, **"Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)".** Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Yayınlanmamış Tez, s.52., (Çevrimiçi), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf , Erişim Tarihi:30.04.2021

98 Bilgi ve İletişim Teknolojileri Kılavuzu, (Çevrimiçi), https://www.btk.gov.tr/uploads/pages/slug/kilavuz.pdf Erişim Tarihi: 30.04.2021

99 Naci Altan "**Bilgisayar Terimleri Ansiklopedik Sözlüğü**", Sistem Yayıncılık, 3. Baskı, İstanbul 2003, (Aktaran) Metin İkizler, M. Sinan Başar, **"Spam'ın Zararları ve Spam ile Hukuki Mücadele: ABD Örneği ve Türk ve Avrupa Birliği Hukukları ile Karşılaştırma,** Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi C.: 8, Sayı: 2, 2006, s.91-114, (Çevrimiçi), https://hukuk.deu.edu.tr/dosyalar/dergiler/DergiMiz8-2/pdf/mikizler.pdf Erişim Tarihi: 30.04.2021

100 Mete Tevetoğlu, **"Bilişim Hukuku"**, 2006, İstanbul, Kadir Has Üniversitesi Yayınları, s.527

101 Bilişim Teknolojileri Ve Siber Güvenlik Derneği, (Çevrimiçi), http://www.bs.org.tr/destekledigimiz-projeler/spam-mesaja-

SPAM ile saldırganlar, kullanıcıların herhangi bir verisini çalmak veya sistemlerine erişmek adına değil, kendilerine ait bilişim platformlarının reklamını yapmak, gelir elde etmek veya üye kazanmak gibi amaçlarla kullanıcılara ulaşmaktadır. Genellikle elektronik posta yoluyla iletilen SPAM kampanya, yasadışı, pornografik veya bahis temalarıyla kullanıcılara yönlendirilmektedir. İnternetin gelişmesi ve bilişim platformlarının çoğalmasıyla birlikte, e-posta haricinde sosyal medya platformları ile de kullanıcılara SPAM'lar iletilmektedir. Kullanıcılar, bu tür iletileri engelleyebildiği gibi, suç duyurusunda da bulunabilecektir. Öyle ki, kişilerin verilerinin izinsiz alınması, paylaşılması, maddi çıkar amacıyla kullanıcıların bilgilerinin çalınması ihtimalleri SPAM ile ortaya çıkmaktadır. Türkiye, SPAM Elektronik Postalarla mücadele etmek amacıyla bir proje ortaya çıkarmıştır. Bilgi Teknoloji ve İletişim Kurulu, bilişim alanında faaliyet gösteren firmalarla birlikte 2009 yılında SPAM iletilere karşı ortak faaliyet yürütmüştür.[102] Proje öncesinde dünyada istenmeyen e-posta sayıları noktasında üst sıralarda olan TRÜKİYE, proje ile istenmeyen eposta sayısını büyük oranda azaltarak saldırıların önüne geçmiştir.

Mantık bombası ise bilişim sitemine izinsiz girme suçunda kullanılan zararlı bir yazılım türüdür. Bir tanıma göre: *"Mantık bombası (logic bomb) belli bir programın içine kasıtlı olarak zararlı bir kod yerleştirilmesi işlemine verilen isimdir."*[103] Bir programın içerisine yerleştirildikleri için mantık bombalarının genellikle farkına varılamamaktadır. Bu virüs çeşidi, bilişim sisteminin içerisine yerleşerek bekleyebilmektedir. Programlandıkları vakit gelene kadar uykuda beklerler ve zararsız gözükürler. Harekete geçtiklerinde ise bilişim sisteminin çalışmasına yönelik saldırılarda bulunurlar.

Bukalemun virüsleri ise tıpkı adını aldıkları bukalemunlar gibi, bilişim sistemine zararsız ve hukuka uygun gözükerek girmekte ve sistem verilerini kullanıcının bilgisi ve rızası dahilinde olmadan çalmaktadır.

---

hayir/33#:~:text=Herhangi%20bir%20ileti%C5%9Fim%20yolu%20ile,nitelikte%20g%C3%B6nderilmesi%20Spam%20olarak%20adland%C4%B1r%C4%B1l%C4%B1r. Erişim Tarihi: 30.04.2021

[102] Mithat Yıldız ,**"Siber Suçlar Ve Kurum Güvenliği"**, Yayımlanmamış Tez, s.140 (Çevrimiçi), https://www.uab.gov.tr/uploads/pages/kutuphane/efcecbe1f21e9fe.pdf Erişim Tarihi:30.04.2021

[103] Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 15, Sayı 1, 2014, s.142, (Çevrimiçi) http://hukuk.deu.edu.tr/dosyalar/dergiler/dergimiz-15-1/senercelik.pdf Erişim Tarihi:30.04.2021

Bukalemun programları, kullanıcıların saldırıyı fark edebileceği ve zararlı bir yazılım olduğunu belli eden program türlerinden değildir. Bukalemun yazılımlarının çalışma şeklini Oğuz Turhan şöyle ifade etmektedir: *"Normal bir program gibi çalışan "bukalemun", aslında bir takım hile ve aldatmalar uygulayarak çok kullanıcılı sistemlerde kullanıcı adları ve şifrelerini taklit yeteneği sayesinde gizli bir dosyaya kaydederek, sistemin bakım için geçici bir süre kapatılacağına ilişkin bir uyarı verir. Bu sırada bukalemun programını kullanan kişi, bu gizli dosyaya ulaşarak kullanıcı adlarını ve şifrelerini ele geçirir"* [104]

İzinsiz bir şekilde bilişim sistemlerin bir diğer erişim şekli olan Scavenging yöntemi bir tanıma göre: "*Çöplenme veya atık toplama olarak adlandırılan yöntemi bilişim sisteminde gerçekleştirilen veri-işlem sonunda kalan bilgilerin depolanmasıdır."*[105] Kullanıcılar, bilişim sistemlerinde ihtiyacı olmadığı, kullanmadığı, gereksiz gördüğü veya yok etmek istediği bilgi veya belgeleri silerek bilişim sistemlerinin çöp kutusuna atmak suretiyle sistemden kaldırır. Fakat bu verilerin tam manasıyla yok edilebilmesi için daha farklı yöntemler gerekmektedir. Sadece silme komutu ile verilerin tam manasıyla bilişim tabanlarından ortadan kalktığından söz edilmesi teknik olarak mümkün değildir. Kullanıcıların silme işlemi gerçekleştirdiği bilişim sisteminde bu veriler, bilişim sisteminin hafızasında veya donanımlarının bir yerinde korunmaya devam etmektedir. Saldırganlar da Scavenging yöntemi ile kullanıcıların bu şekilde yok ettiğini düşündüğü verilerine erişebilmekte ve bu verileri kullanıcının rızası olmadan kullanabilmektedir.

Bilişim sistemlerine izinsiz erişim suçlarının işlenme türleri arasında en basit yöntemlerden birisi olan Data Diddling ile saldırganlar, kullanıcıların bilişim sistemlerine erişerek verilerinin değiştirilmesini, silinmesini ve sistemlerine teknik hatalar girilmesini sağlamaktadır. Bir tanıma göre Data Diddling yöntemi ile fail: *"Bilgisayara girdiği veya bilgisayarda bıraktığı veriler ile mevcut veriler üzerinde*

104 Oğuz Turhan, a.g.e., Çevrimiçi, s.50,
105 E. Altunok, A.F. Vural, a.g.e., s.78.

istediği yönde değişiklik yapma veya cihazı istediği yönde kullanma olanağına kavuşmaktadır." [106]

Bilişim sistemleri, yazılımlara ve sistemlerin içerisine kullanıcının dışında dışarıdan ve yetkisiz olabilecek tüm girişleri engellemeye yönelik tasarlanmıştır. Fakat bilişim sistemlerini oluşturan yazılımcı veya programcılar, ileride kullanıcının menfaatine yönelik ihtiyaç duyulması bazı kapıları açık bırakmaktadır. Ancak, kullanıcının menfaatine yönelik açık bırakılan bu kapılar, saldırganlar tarafından tespit edildiğinde bilişim sistemlerine erişilmesi ve sisteme girilmesi mümkün olabilecektir. Böylece kullanıcının rızası olmadan ve sistemdeki açığı tespit ederek müdahalede bulunamayacağı ve failin gizli bir şekilde bilişim sistemine erişebileceği gizli kapılar, bilişim sistemlerine yönelik suçlarda bir araç haline gelebilecektir. Gizli kapıların, kullanıcı tarafından fark edilmesi ve bu kapılar aracılığıyla sistemlerine gerçekleştirilebilecek saldırıları tespit edebilmesi oldukça zordur.

En basit ve en eski yöntemlerden birisi olan bilgisayar ya da bilişim virüsleri bir tanıma göre: *"Kendi kendini çoğaltma özelliğine sahip, kopyalarını başka sistemlere de bulaştırarak etkileyen yazılımlardır. Bunlar, biyolojik virüslerde olduğu gibi, kendi kendine çoğalıp, bulaşabilme ve sistemi hasta edebilme özelliklerine sahip olarak ve bulaştıkları sistemde bulunan yazılımları çökelterek, bilişim sistemlerine en fazla zararı verecek şekilde tasarlanmaktadırlar."*[107] Bilişim sistemlerinin kullanılmaya başlanılmasından bu yana en yaygın olarak rastlanılan ve en çok bilinen bilişim saldırıları çeşidi virüslerdir. Virüsler bilişim sistemlerinin ana donanımlarına ve yazılımlarına tutunarak, kendi kendilerine çoğalabilir ve yayılabilirler. Virüsler, bilişim sistemlerinin verimli çalışmasını engellemeye ve sistemdeki verileri yok etmeye yönelik saldırılarda bulunur. İlk bilgisayar virüsü olan "Brain" 1986 yılında geliştirildi. Dükkân sahibi olan iki kardeş, sistemlerine dadanan yazılım hırsızlarından kurtulmak için virüs geliştirdiklerini açıklamışlardı.[108]

---

106 R. Yılmaz Yazıcıoğlu, **"Bilgisayar Suçları, Kriminolojik Sosyolojik ve Hukuki Boyutları ile"**, 1. Baskı, İstanbul, Alfa Yayınları, s.152. (Aktaran) B. Zakir Avşar, Gürsel Öngören, s.52.

107 Avşar ve Öngören, a.g.e., s.54

108 Kaspersky, 2020, **"Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS"**, (Çevrimiçi), https://www.kaspersky.com.tr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs Erişim Tarihi:30.04.2021

Üzerinde durulması gereken bir diğer yöntem Ağ Solucanları tekniği ise bilişim sisteminin içine girerek kendi kendine çalışan zararlı yazılımlardır. Bu yazılımlar sıklıkla internet siteleri ve ağ üzerinde paylaşılan dosyalar ve posta ekleri ile yayılırlar.[109] Adından da anlaşılacağı üzere Ağ Solucanları, sistemde kendisine bir defa yer edindikten sonra o sistem içerisinde kendi kendine dolaşarak çoğalabilmektedir.

Ağ Solucanları, kullanıcıların dikkatsizliği ve bilgisizliği ile bilişim sistemlerine bulaşabilecektir. Kullanıcıların hesaplarına gelen abartılı kaos haberleri, yüksek miktarda ödül bildirimleri veya ilgi çekici arkadaşlık istekleri ile ilgili gelen elektronik postalar, sosyal medya mesajları veya internet pop-uplar'ı ağ solucanlarının bilişim sistemlerine bulaşma örnekleridir. Bu yöntemler ile kullanıcıların sistemlerine erişen solucanlar, internet hızını yavaşlatabilir, internet sitelerine erişimi kısıtlayabilir, bilgisayar sisteminin çökmesine veya saldırganların eline geçmesine sebep olabilir.

Bilişim sistemine izinsiz bir şekilde girme veya orada kalma suçunun gerçekleşmesi için ayrıca, selam tekniği (salami Techniques), tarama (scanning), sırtlama (pigybacking) ve yerine geçme (masquerading) yöntemleri suçlular tarafından kullanılmaktadır.

3.1.3.5. Netice

Bilişim sistemlerine girilmesi veya orada kalınmaya devam edilmesiyle suç oluşmuş sayılacaktır. Suçun gerçekleşmesi için her iki hareketin sonucunda bir netice aranmamaktadır. Madde metninde suçun gerçekleşmesi için herhangi bir yan gerekçe düzenlenmemiştir. Sırf hareket suçu olarak düzenlenen 243. Maddedeki bilişim suçları için mağdurun üzerinde ayrıca bir hukuka aykırı hareketin gerçekleşmesi gerekmemektedir. Bu hareketler ile birlikte başka suçların işlenmesi

[109] İTÜ Bilgi İşlem Dair Başkanlığı, **"Virüs, Solucan ve Truva Atı",** (Çevrimiçi), https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1 Erişim Tarihi:30.04.2021

gerekmemektedir. Fakat bu suçun işlenmesiyle birlikte farklı suçlara yönelik hareketlerin icrası nitelikli haller olarak sayılabilecektir.

3.1.4. Suçun Manevi Unsurları

Suçun manevi unsurları, suç ile kişinin arasındaki manevi bağları ifade etmektedir. Suçun işlenmesi için fail ile suç arasında bir bağ bulunması gerekmektedir. Suçun manevi unsuru belirlenirken kast ve taksir açısından düzenlenen madde incelenmelidir.

TCK. 243. Madde incelendiğinde herhangi bir özel kast veya taksir unsuruna rastlanılmamaktadır. Suçun işlenmesi için böylece genel kast yeterli olacaktır. Bilişim sistemine girme veya sistemde kalma suçunun manevi unsuru olan kastın gerçekleşmesi için failin bu suçu bilerek ve isteyerek işlemesi gerekmektedir.[110] *Bu suçun taksirle işlenmesi kanun koyucu tarafından madde metninde düzenlenmediği için mümkün olmayacaktır. Böylece failin bir bilişim sistemine taksirle yani özensiz veya dikkatsiz girmesi veya orada kalması söz konusu değildir.*

3.1.5. Hukuka Aykırılık

243. madde metninde herhangi bir hukuka uygunluk düzenlemesine yer verilmemiştir. Genel nitelikli olarak sayılabilecek hukuka uygunluk sebepleri bu suçta da geçerli olacaktır. Örneğin mağdurun rızası olduğu hallerde veya TCK 24/1. Madde ile düzenlenen görevin ifasından kaynaklanan bir erişim ile bilişim sistemine girme veya orada kalma hareketi suç teşkil etmeyecektir.

Kanun metninde bilişim sistemlerine hukuka aykırı olarak girilmesi yeterli olduğundan, failin fiilinin hukuksuz olduğunu bilmesi yeterli olacaktır. [111] Fakat kişi,

110 Artuk, Gökçen, Yenidünya, a.g.e., s.876
111 Koca, Üzülmez, a.g.e., s.815

bir bilişim sistemine kanunu verdiği yetkiye dayanarak girmişse veya bilişim sistemi sahibinin rızası mevcutsa fiil suç oluşturmayacaktır.[112]

3.1.6. Kusurluluk

Kusurluluk suçun icrası için sayılan maddeler gibi bir unsur değil, failin gerçekleştirdiği hukuka uygun olmayan eylem neticesiyle kınanma yargısıdır. [113]Failin ilgili suçtan dolayı sorumluluğunun bulunabilmesi için suçun maddi ve manevi unsurları ve hukuka aykırılık unsuruyla birlikte incelenmesinden sonra gerçekleştirdiği hareket yüzünden kınanabilmesi aranmaktadır.[114]

Failin gerçekleşen hukuka aykırı eylem ile kınanamıyor olması failin ceza almasını engelleyecektir. Suçun faili olunabilmesi için gerçekleşen hukuka aykırı eylemin fail ile bütünleşmiş olması gerekmektedir. Örneğin; bir kişinin bilişim sistemlerine erişmesi veya orada kalması cebir veya tehdit ile gerçekleşmiş ise kişinin kusurunun varlığından ve cezai sorumluluğundan bahsedilemeyecek, kişiyi zorlayanlar açısından cezai sorumluluk doğacaktır.[115] Yukarıda da görüldüğü gibi düzenlenen suç yalnızca kasten işlenebilecektir. Suçun oluşabilmesi için failin gerçekleştirdiği eylemin sonucunda hukuka aykırılık olduğu bilmesi ve istemesi ile birlikte bu davranışlarını suça yönlendirmesi gerekmektedir.

---

112 Veli Özer Özbek, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, **"Türk Ceza Hukuku Genel Hükümler"**, 7. Baskı, Ankara, 2014, s.912

113 İzzet Özgenç, "**Türk Ceza Hukuku Gazi Şerhi (Genel Hükümler)"**, 6. Baskı, Ankara, Seçkin Yayıncılık, 2011, s. 220,338 (Aktaran) Dülger, 2015, s.395

114 Dülger, a.g.e., 2015, s. 394

115 Hakan Karakehya, **"Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu",** TBB Dergisi, Sayı 81, 2009, s. 15 (Çevrimiçi), http://tbbdergisi.barobirlik.org.tr/m2009-81-498 Erişim Tarihi: 01.05.2021

3.1.7. Suçun Özel Görünüş Biçimleri

3.1.7.1. Teşebbüs

Türk Ceza Kanunu'nun 35. Maddesi ile düzenlenen suça teşebbüsün mümkün olması için failin suç işlemek kastıyla harekete geçmesi ve suça elverişli hareketlerde bulunması aranmaktadır. 35. Maddeye göre: "Kişi, işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaz ise teşebbüsten dolayı sorumlu tutulur." Dolayısıyla, failin elinde olmayan sebeplerle suçun tamamlanmamış olması gerekmektedir. Fail bu halde, kastettiği suçtan değil suça teşebbüsten yargılanacaktır.

Suça teşebbüs ile TCK 36'da düzenlenen gönüllü vazgeçme farklı kurumlardır. Suça teşebbüste fail suçun tamamlanmasını istemekte fakat elinde olmayan sebepler ile tamamlayamamaktadır. Fakat gönüllü vazgeçme ile fail, suçun icrasından bilerek ve isteyerek vazgeçer veya suçun tamamlanmasını önlerse gönüllü vazgeçmiş sayılacaktır.

İncelenen maddede iki ayrı seçimlik suç düzenlenmiştir. Bu suçlardan ilki olan bilişim sistemine girme suçunda teşebbüsün mümkün olduğu düşünülmektedir. Fail, örneğin bir kişinin bilgisayarına girmeye çalışırken kendi sisteminin çökmesiyle veya e-postalarına erişmek için virüs içeren bir maili birisine attığında kişinin iletilen maile bakmamasıyla niyetlendiği suçu tamamlayamamış ve teşebbüs aşamasında kalmış olacaktır. Madde metninde düzenlenen ikinci suç olan bilişim sistemin kalma suçu için öncelikle bilişim sistemine girilmesi gerekmektedir. Hukuka aykırı bir şekilde bilişim sistemine girildiğinde suçun icrası tamamlanmış olacağı için bilişim sisteminde kalma suçunda teşebbüs aranmayacaktır.

3.1.7.2. İştirak

TCK 37 ile suça iştirak hükümleri düzenlenmiştir. Kanun maddesine göre: "Suçun kanuni tanımında yer alan fiili birlikte gerçekleştiren kişilerden her biri, fail olarak sorumlu olur." Madde ile düzenlenen hükme göre suçun icrası esnasında faille birlikte fiili gerçekleştiren kişiler de fail gibi suçtan sorumlu olacaktır. Maddenin devamında düzenlenen hükme göre ise bir kişiyi suçun işlenmesinde aracı olarak kullanan kişi de suçun faili gibi sorumlu olacaktır.

243. madde ile düzenlenen bilişim suçunun işlenmesinde iştirak mümkün olabilecektir. Birden fazla kişi birleşerek bu suçun icrasını gerçekleştirebilecektir. Bu halde faillerin her biri müştereken bu suçtan sorumlu olacaklardır.

3.1.7.3. İçtima

TCK'nın Suçların İçtiması isimli bölümü 42,43 ve 44. Maddeler ile düzenlenmiştir. Bileşik Suç kenar başlıklı 42. Madde ile tek hareket sayılan iki suçun bileşik suç olarak değerlendirileceği düzenlenmiştir. Madde metnine göre: "Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz." Zincirleme suç kenar başlıklı 43. Madde ile ise bir suçun bir kişiye değişik zamanlarda birden fazla işlenmesiyle veya yine bir suçun birden fazla kişiye tek bir fiil ile işlenmesi durumunda bu madde hükümlerinin uygulanacağı düzenlenmiştir. Fikri içtima kenar başlıklı 44. Madde ile ise gerçekleştirdiği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişinin bu suçlardan en ağır cezayı gerektiren suçla yargılanacağı düzenlenmiştir. Fikri içtimaının zincirleme suçtan farklı, birden fazla olarak işlenen suçta aynı suç tipinin değil farklı suç tiplerinin icrasının gerçekleşmiş olmasıdır.

243. Madde incelendiğinde ise bilişim sistemine girme ve kalma suçu bir kişiye karşı ayrı ayrı zamanlarda işlenebilecek olduğundan zincirleme suç hükümlerinin uygulanması mümkündür. Bir bilişim sistemine girip orada kalmaya devam etme

suçunun zincirleme suç olup olmadığı konusunda zincirleme suçun konusu olan her suç bakımından ayrı ayrı inceleme yapılarak karar verilmesi gerekmektedir. Failin bilişim sisteminde kaldığı süreler farklıysa veya bir hareketinde sisteme sadece giriş bir diğerinde de sistemde kalmaya devam etmişse bu hallerde zincirleme suç hükümlerine göre değil her suçtan ayrı ayrı yargılanması gerekmektedir.

Bilişim sistemine girme ve orada kalmaya devam etme suçu ile başka şekillerde işlenebilen bilişim suçlarına da kapı açılmaktadır. Örneğin, bilişim sistemleri ile dolandırıcılık suçu TCK 158. Maddede düzenlenmiştir. Failin bilişim sistemlerine girerek dolandırıcılık yapabilmesi için öncelikle 243. Madde ile düzenlenen suçu işlemesi gerekmektedir. Bu ve benzeri birçok bilişim suçu, bilişim sistemine girme veya orada kalmaya devam etme suçunun icrası ile mümkün olabilmektedir. Bu şekilde bir başka suça köprü olan suçlara geçit suçu denmektedir.[116] Bir suça geçit suç denilebilmesi için gereken ilk kural ise basamak olarak kullanılan ilk suçun ikinci suça göre daha hafif olması ve iki suç arasında korunan hukuki değerin aynı olmasıdır.[117] Suçların mağdurlarının farklı olması, failin eylemleri ile sonuçların arasında aynı nedensellik bağının bulunmaması, önceki suçun daha ağır bir suç olması, failin ilk başta itibaren ağır suç kastıyla hareket ediyor olmaması durumlarında geçit suça göre bir değerlendirme yapılmayacaktır.

Fail, tek bir hareketle birden fazla farklı suç işlediğinde fikri içtima hükümlerine göre yargılanacaktır. 243. Maddenin konusu olan suçlarla birlikte başka suçların da fail tarafından tek bir eylem ile gerçekleşmesi mümkün olabilecek ve düzenlenen suç fikri içtima hükümlerine konu olabilecektir.

---

116 Dülger, a.g.e., 2015, s. 403

117 Kayıhan İçel, **"Görünüşte Birleşme (İçtima) İlkeleri Ve Yeni Türk Ceza Kanunu"**, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Yıl: 7, Sayı 14, Güz 2008 s. 47 (Çevrimiçi) https://www.ticaret.edu.tr/uploads/kutuphane/dergi/s14/035-049.pdf Erişim Tarihi:02.05.2021

3.1.8. Yaptırım

Kanun koyucu, TCK 243. Madde metninin düzenlenmesinde seçimlik iki suça yer vermiştir. Maddenin birinci fıkrası ile bilişim sistemlerine giren veya orada kalmaya devam eden kişilere bir yıla kadar hapis veya adlî para cezası verilecektir. Kanun metninden de anlaşılacağı üzere bu suçu işleyen faile bir yıla kadar hapis cezası veya adlî para cezası verilecektir. Madde metninde geçen *"veya"* ifadesi gereği cezalar seçimliktir. İki ceza aynı anda faile bu suçtan dolayı uygulanamayacaktır.

Maddenin 2. Fıkrasında ise cezayı hafifleten unsurlar sayılmıştır. Fıkraya göre 1. Fıkra ile sayılan suçların bedeli karşılığında yararlanılabilen sistemler hakkında işlenmesi halinde faile verilecek olan ceza yarı oranında indirilecektir.

Maddenin son fıkrasında ise 1. Fıkrada sayılan eylemlerin gerçekleşmesi ile sistemin içerdiği verilerin yok olması veya değişmesi durumunda faile altı aydan iki yıla hapis cezası verileceği düzenlenmiştir. Madde metninden de anlaşılacağı üzere, 3. Fıkrada sayılan ağırlaştırıcı sebebin gerçekleşmesi halinde faile verilecek hürriyeti bağlama suçu artırılırken adlî para cezası seçimi kaldırılmıştır.

TCK 243. Madde ile düzenlenen bilişim suçunun işlenmesi halinde davaya bakacak olan mahkeme 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkındaki Kanun'un 11. Ve 12. Maddeleri gereği Asliye Ceza Mahkemeleri, yetkili mahkemeler ise suçun işlendiği yer mahkemesidir.[118] Fakat bilişim suçlarının sanal ortamlarda gerçekleşmesi ve uluslararası bir boyutta sınırsızlığı olması sebebiyle yetkili mahkemenin tespit edilmesi sorun oluşturabilmektedir.[119]

---

[118] Uğur İhtiyaroğlu, **"Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi"**, Hakemli Makale, 2020, s.434 (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/1070186 Erişim Tarihi:02.05.2021

[119] Ahmet Gökçen, Kerim Çakır, Mehmet Emin Alşahin, Murat Balcı, **"Ceza Muhakemesi Hukuku"**, 3. Baskı, Adalet Yayınevi, Ankara, 2018, s.10

Türk Ceza Kanunu'nun 66. maddesi[120]ne göre bu suçta zamanaşımı süresi suçun işlenmesi itibariyle 8 yıldır.

3.2. BİLİŞİM SİSTEMİNİN ENGELLENMESİ VEYA BOZULMASI SUÇU İLE VERİLERİN YOK EDİLMESİ VEYA DEĞİŞTİRİLMESİ SUÇU (M.244)

3.2.1. Genel Olarak

TCK'nın 244. Maddesi ile bilişim sistemlerine ve bu sistemlerdeki verilere karşı yapılacak olan saldırılar suç olarak düzenlenmiştir. Maddenin birinci fıkrası ile bilişim sistemlerine, ikinci fıkrası ile bilişim sistemlerindeki verilere yönelik yapılan saldırılar ele alınmıştır. Böylece bu düzenleme ile bilişim sistemlerine ve bilişim sistemlerindeki verilere karşı işlenebilecek suçlar ayrı ayrı düzenlenmiş, her biri tek başına münhasır bir suç oluşturmuştur. Her ne kadar birçok suç unsuru konusunda ortaklık taşınıyor olsa da iki suçun farklı suç konularını oluşturuyor olması ve uygulanacak cezaların suçlara göre değişiklik gösterebileceği durumlar göz önüne alınarak suçların aynı madde içerisinde farklı fıkralarda farklı iki suç tipi olarak düzenlenmesi uygun görülmüştür. Kanun koyucu, bu düzenleme ile Avrupa Siber Suç Sözleşmesi'nin 4,5 ve 8. Maddeleri ile düzenlenen hükümlerine uyarak ilgili maddelerin iç hukuktaki yansımanı oluşturmuştur. [121]

244. maddenin birinci fıkrası ile bilişim sistemlerine müdahale suçu düzenlenmiştir. Madde metnine göre: *"(1)Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."* Düzenlenen bu suç ile Avrupa Siber Suç Sözleşmesinin 5. Maddesinde düzenlenen "sisteme müdahale" suçu ile paralellik sağlanmıştır. Kanun koyucu getirdiği bu düzenleme ile

120 TCK Madde 66'ya göre: *"Kanunda başka türlü yazılmış olan haller dışında kamu davası; … e)Beş yıldan fazla olmamak üzere hapis veya adlî para cezasını gerektiren suçlarda sekiz yıl geçmesiyle düşer.*

121 Artuk, Gökçen, Yenidünya, a.g.e., s.880

bilişim sistemlerine karşı yapılacak olan saldırıları engellemeye çalışmıştır. Bilişim sistemlerinin günümüzdeki etki alanı ve hayatın olağan akışı içerisinde tuttuğu yerin önemi göz önüne alındığında bu sistemlerin çalışmasının engellenmesi veya bozulması kişiler, kurumlar ve kamusal düzen açısından büyük zararlara sebebiyet verebilecektir. Hem ekonomik hem sosyal hem de kamusal alanda bilişim sistemlerinin kısa bir süreliğine dahi bozulması veya bu sistemlere ulaşılamaması büyük kitleleri etkileyebilecek büyük tahribatlara yol açabilecektir. Bu kayıpların önüne geçilebilmesi adına düzenlenen bu madde ile bilişim sistemlerine verilebilecek zararların önüne geçilmeye çalışılmıştır.

244. maddenin ikinci fıkrası ile ise bilişim sistemlerindeki verilerin korunması amaçlanmıştır. Maddenin ikinci fıkrasına göre: *"(2)Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır."* Kanun koyucunun düzenlediği bu madde Avrupa Siber Suç Sözleşmesi'nde de 4. Madde ile düzenlenen "verilere müdahale" suçu ile paralellik göstermektedir.

244. maddenin son iki fıkrası ile de suç ile ilgili diğer hükümler düzenlenmiştir: *"(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."*

3.2.2. Korunan Hukuki Yarar

5237 sayılı TCK'nın 244. Maddesinde birinci ve ikinci fıkra ile iki farklı suç tipi düzenlenmiştir. Birinci fıkrada bilişim sistemlerinin hedef alınmasıyla oluşabilecek suçlar düzenlenmişken ikinci fıkra ile bilişim sistemlerindeki verilerin hedef alınması düzenlenmiştir. Kanun koyucu iki fıkra ile hem bilişim sistemlerini

hem de bilişim sistemlerindeki verileri koruma altına almıştır. Böylece bu suç ile korunan hukuki yararın karma olduğu anlaşılmaktadır.

Birinci fıkrada düzenlenen suç ile bilişim sistemlerinin soyut ve somut tüm varlıkları koruma altına alınmıştır. Bilişim sistemlerine saldırı ile işleyişlerinin bozulması veya engellenmesi, bu sistemlerin sağlıklı bir şekilde çalışmamasına sebebiyet verecektir. Bozulma ile sistemler herhangi bir faaliyetini gerçekleştiremeyecek hale gelecek, engellenme ile de sistemlerin çalışması kesintiye uğrayacaktır. Bu fıkra ile düzenlenen suç ile bilişim sistemlerinin sağlıklı bir şekilde çalışması koruma altına alınmıştır.[122] Bir görüşe göre birinci fıkra ile korunan hukuksal değer mülkiyet hakkı ve hak sahibinin bilişim sistemleri üzerindeki özgürlüğüdür.[123] Başka bir görüşte ise korunan hukuksal değer sistemin çalışmasının sağlanması ve haberleşme özgürlüğünün korunmasıdır. [124] Öğretideki bir diğer görüş ise bu suçun TCK'nın 151. Maddesinde düzenlenen "mala zarar verme" suçunun hukuki konusuyla örtüştüğü ve korunan hukuksal değerin mülkiyeti korumaya ilişkin toplumsal menfaat olduğu yönündedir.[125]

Maddenin ikinci fıkrasıyla ise bilişim sistemlerindeki veriler korunma altına alınmıştır. Bu verilere saldırılması, tahrip edilmesi, yok edilmesi veya değiştirilmesi 244. Madde ile suç olarak düzenlenmiştir. Böylece ikinci fıkra ile bilişim sistemleri değil, sistemlerdeki veriler korunmuştur. Fıkra ile korunan hukuksal değer ise bilişim verilerine yönelik gerçekleştirilecek saldırıların önlenmesi ve bu sistemlerin kullanıcılarının verilerinin koruma altına alınmasıdır.

---

122 Dülger, a.g.e., 2015, s. 412

123 Levent Kurt, a.g.e., s. 162.

124 Mehmet Emin Artuk, Ahmet Gökçen, Ahmet Caner Yenidünya, **"Türk Ceza Kanunu Şerhi Özel Hükümler Madde 235-345"**, C. 5, Ankara, 2009, s.4659, (Aktaran) Dülger, 2015, s. 412

125 Sacit Yılmaz, " **5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar"**, Türkiye Barolar Birliği Dergisi, 2011, Sayı 92, s.68 (Çevrimiçi) 1

3.2.3. Suçun Maddi Unsurları

3.2.3.1. Fail

TCK 244. Madde incelendiğinde madde metninde kanun koyucunun suçun faili açısından herhangi bir ayırt edici özellik düzenlemediği görülmektedir. Bu sebeple bu suçun faili herkes olabilecektir. Bir başkasının bilişim sistemini bozan veya engelleyen veya bir başkasına ait bilişim sistemindeki verileri bozan, değiştiren, yok eden veya erişilmez kılan herkes bu suçun faili olabilecektir. Suçun faili eğer bir tüzel kişi yararına tüzel kişiliğin temsilcisi veya organı sıfatını taşıyan gerçek kişi olursa, tüzel kişi hakkında 246. Madde ile düzenlenen güvenlik tedbirleri uygulanır.[126]

3.2.3.2. Mağdur

Madde metninde kanun koyucunun mağdur için de herhangi bir özellik belirttiği görülmemektedir. Böylece bu suçun işlenmesi ile herkesin mağdur olabilmesi mümkün olacaktır. Maddede belirtilen suçların işlenmesi ile bilişim sistemlerinin işleyişi engellenen veya bozulan veyahut bilişim sistemlerindeki verileri bozulan, yok edilen, değiştirilen veya bu verilerine erişemeyen her kişi bu suç ile mağdur sıfatına haiz olabilecektir.

3.2.3.3. Suçun Konusu

244. Madde suçun konusu açısından incelenirken iki fıkranın ayrı ayrı değerlendirilmesi gerekmektedir. İlk fıkrada düzenlenen bilişim sistemlerinin engellenmesi veya bozulması suçunun konusunu bilişim sistemleri oluşturmaktadır.

126 Artuk, Gökçen, Yenidünya, a.g.e., s.882

İkinci fıkrada düzenlenen bilişim sistemlerindeki verilenin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması suçunun konusunu ise bilişim sistemlerindeki veriler oluşturmaktadır.

3.2.3.4. Hareket

TCK'daki 244. Madde suçunun gerçekleşmesi için maddede düzenlenen her iki seçimlik suçtan birisinin icrası suçun oluşması için yeterli olacaktır. Her iki suç tipinin içerdiği hareketler de ayrı ayrı değerlendirilecektir.

Birinci fıkra ile düzenlenen bilişim sistemlerini bozma veya engelleme suçu iki seçimlik hareket içermektedir. Her iki hareketin de tek başına gerçekleşmiş olması suçun oluşması için yeterli sayılabilecektir. Bilişim sisteminin bozulması hareketi ile sistemin hiçbir şekilde çalışamaz ve hizmet veremez hale gelmesi kastedilmiştir. Bilişim sistemi birçok şekilde bozulabilecektir. Fail, sisteminin yazılımını bozabileceği gibi donanımını da bozarak sistemin çalışmasını engelleyebilecektir fakat kanun açısından suçun işlenme şeklinin bir önemi yoktur. Önemli olan bilişim sisteminin bozulmasıdır. Sayılan hareket çeşitlerinin herhangi biriyle bilişim sistemlerinin çalışmaz hale gelmesiyle suç oluşmuş sayılacaktır. Bilişim sisteminin engellenmesi de bu suçtaki hareket unsurlarından bir tanesidir. Bu hareket ile sistem bozulmayacaktır fakat normal çalışması engellenmiş olacaktır. Engelleme hareketi yine virüsler vasıtası ile yazılım programları üzerinden gerçekleştirilebileceği gibi bazı parçaların sökülmesi veya tahrip edilmesi ile donanımsal açıdan da gerçekleştirilebilecektir. Ayrıca, bilişim sistemlerinin bulunduğu yerdeki teknik arızalara sebebiyet verilmesi gibi sistemin çalışmasını fiziksel ortamlar vasıtasıyla engellemek de bu suç kapsamında gerçekleştirilecek hareketlerden bir tanesi olarak değerlendirilebilecektir. Yine bu hareketlerden hangisi ile gerçekleşirse gerçekleşsin bilişim sisteminin çalışmasının engellenmesi ile suç ortaya çıkacaktır.

244. Maddenin ikinci fıkrası ile bilişim sistemlerindeki verilerin hedef alınarak gerçekleştirilebilecek suçlar düzenlenmiştir. Bu suçlar, bilişim sistemindeki verilerin bozulması, değiştirilmesi, yok edilmesi veya erişilmez kılınması, sisteme veri

yerleştirilmesi veya verilerin başka bir yere gönderilmesi ile gerçekleşecektir. Maddede düzenlenen suçlar seçimlik hareketlerden oluşur. Her bir hareketin ayrı ayrı ve münhasır olarak gerçekleşmiş olması madde ile düzenlenen suçun icrası için yeterli olacaktır.

Fıkra ile ilk düzenlenen hareket olan verileri bozma suçu, bir bilişim sisteminde yer alan verilerin failin bilişim sistemine göndereceği virüsler veyahut fizikken verilerin bulunduğu donanımlara hasar vermesi suretiyle işleyebilecektir.

Verilerin yok edilmesi ise bilişim sisteminde yer alan kullanıcıya ait birtakım verilerin sistemden silinmesi ve ortadan kaldırılması hareketiyle oluşacaktır. Bilişim sistemindeki verilerin yok edilmesi sürecinde bu veriler tamamen yok olmamış ve sistemde bir yerlerde korunuyor olsa bile bu suçun icrası gerçekleşmiş sayılacaktır.

Verilerin değiştirilmesi suçu, sistemde yer alan verilerin başka bir veri ile değiştirilmesi ile söz konusu olacaktır. Kullanıcıların bilişim sistemlerinde yer alan dokümanlarının veya şifrelerinin dönüştürülmesi ile suçtaki hareket unsuru gerçekleşmiş olacaktır. Verilerin değiştirilmesi ile veriler yok olmayacak fakat erişilmesi istenen verilerin yerine yanlış bilgilere ulaşılması sağlanacaktır.

Verilerin erişilmez kılınması suçu ile verilere ulaşılmasının engellenmesi amaçlanmaktadır. Fail, bu hareket ile bilişim sistemi kullanıcılarının verilere erişmesi engellemektedir. Bu suç, veriler yok edilmesiyle değil parola koyulması ya da verilerin yerinin değiştirilmesi gibi hareketlerle gerçekleşebilecektir.

Bir bilişim sistemine sistemin kullanıcısının rızasının olup olmamasının bir önemi olmaksızın erişen failin, fizikken veya yazılım programları ile birtakım veriler yüklenmesi ile bilişim sistemine veri yerleştirmek suçu gerçekleşmiş olacaktır. Bu suç ile failin sistemlere çeşitli verileri kullanıcının haberi olmaksızın yüklemesi düzenlenmiştir.

Fıkrada düzenlenen son suç şekli olan bilişim sistemindeki verilerin başka bir yere gönderilmesi suçu ise bilişim sisteminde mevcut olan verilerin o sistemin kullanıcısının rızası alınmaksızın bir başka yere gönderilmesi, kaydedilip taşınması veya kopyalanması ile tamamlanmış olacaktır.

244. madde ile düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun işlenme şekillerine en önemli örneklerden bir tanesi tavşan (Rabbits) tekniğidir. Bir tanıma göre Tavşanlar: "Adını aldıkları hayvan gibi çok hızlı üreyebilmekte ve bulundukları bilişim sisteminin içinde işlemciye sürekli anlamsız komutlar vermek suretiyle normal işleyişi engelleyerek sistemin yavaşlanmasına, en nihayet çalışamaz hale gelmesine sebep olmaktadırlar." Tavşan yazılımları, genellikle şirket bilgisayarları gibi ağa bağlı olan bilişim ortamlarında yayılmakta ve bu yazılımların amacı bilişim ağındaki ana ağa yerleşerek tüm işletim sistemini yok etmektir. Ayrıca, 243. Madde başlığında belirtilen bukalemunlar, çöpe dalma, veri aldatmacası, SPAM gibi teknikler ile de bilişim sistemlerine girildikten sonra sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu işlenebilecektir.

3.2.3.5. Netice

244. maddenin birinci ve ikinci fıkrası ile madde ile düzenlenen suçun oluşması için gereken hareketler ve bu hareketlerin sonuçları sayılmıştır. Böylece bu suç ile bir neticenin gerçekleşmesi aranmıştır. Bu suçun meydana gelmesi için failin bir bilişim sistemini engellemesi veya bozması, bilişim sistemindeki verileri bozması, değiştirmesi, yok etmesi, erişilmez kılması, bilişim sistemine veri yerleştirmesi veya bir bilişim sisteminden başka bir yere veri göndermesi gerekmektedir. Madde ile sayılmış olan bu hareketlerin gerçekleşmesi suçun oluşması için yeterli kabul edilecektir.

244. Maddenin üçüncü ve dördüncü fıkrası ile ise suçun nitelikli halleri düzenlenmiştir. Suçun bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bir bilişim sistemi üzerinde işlenmesi ile failin alacağı ceza yarı oranında artırılacaktır. Son fıkrada ise maddenin tümünde sayılan suçların işlenmesiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde kişiye iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezası verilecektir.

3.2.4. Hukuka Aykırılık

244. madde ile düzenlenen suçlar ile bilişim sistemleri ve bilişim sistemlerindeki veriler hedef alınmaktadır. Bu suçların kanun ile düzenlenerek cezai yaptırıma tutulması ile de bilişim sistemi kullanıcıları ve bilişim sistemlerindeki veriler koruma altına alınmaktadır. Bilişim sistemi kullanıcısının rızasıyla veya TCK 24/1. Madde ile düzenlenen görevin ifası ile madde metninde belirtilen eylemlerin gerçekleştirilmesi halinde hukuka aykırılık oluşmayacaktır.[127] 244. Madde ile düzenlenen suçlarda hukuka uygunluk halleri için verilebilecek örneklerden bir tanesi de 5651 sayılı İnternet Ortamında Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 8. Maddesine göre internet erişiminin uygulanmasıdır. Uygulamaya göre koruma tebiri veya idari yaptırım şekliyle 2 farklı şekilde erişim engellenmesi getirilebilmektedir. [128]

3.2.5. Kusurluluk

Sistemi engelleme, bozma, verileri yok etme veya değiştirme kenar başlıklı 244. Madde ile düzenlenen suçların icrasında da failin kusurlu kabul edilebilmesi için kınanabilmesi aranacaktır. Failin bu madde ile düzenlenen suçların icrasıyla kınanamıyor olması failin ceza almasını engelleyecektir. 243. Madde başlığı altında görüldüğü gibi failin 244. Madde ile düzenlenen suçları cebir veya tehdit ile gerçekleştirmiş ise failin kusurunun varlığından ve cezai sorumluluğundan bahsedilemeyecektir.

127 Koca, Üzülmez, a.g.e., s.831
128 Özbek, Doğan, Bacaksız, a.g.e., s.990

3.2.6. Suçun Özel Görünüş Biçimleri

3.2.6.1. Teşebbüs

244. madde ile düzenlenen suçların yarıda kalması veya suçun icrası tamamlanmadan elinde olmayan sebeplerden ötürü failin suçu gerçekleştirememiş olması mümkündür. Böylece bu madde ile düzenlenen suçlar için teşebbüs hükümleri uygulanabilecektir. Örneğin failin bir bilişim sistemine fizikken zarar verecekken yakalanmış olması veyahut bir bilişim sistemine failin virüs göndererek sistemin bozulmasını amaçlarken virüsün anti virüs programına takılmış olması failin teşebbüs aşamasında kaldığını gösterir.

3.2.6.2. İştirak

Kanun koyucu 244. Maddede düzenlediği unsurlarda iştirake özel bir hüküm getirmemiştir. Bu suçlara yönelik gerektiği hallerde Türk Ceza Kanunu'nun iştirake ilişkin genel hükümleri uygulanabilecektir.

3.2.6.3. İçtima

244. madde ile düzenlenen suçların zincirleme şekliyle işlenmesi mümkündür. Madde ile düzenlenen suçların zincirleme suç hükümlerine göre işlenmesi halinde fail TCK 43. Madde hükümlerine göre ceza alacaktır. Ancak dikkat edilmesi gereken noktalardan bir tanesi de maddede birden fazla suç tipi düzenlenmiştir. Zincirleme suç oluşabilmesi için madde metninde düzenlenen suçlardan bir tanesinin değişik zamanlarda bir kişiye karşı birden fazla işlenmesi gerekmektedir. Aynı suçun birden fazla kişiye karşı işlenmesi durumunda ise aynı neviden fikri içtima suçu gerçekleşecek ve faile karşı yine 43. Maddenin ikinci fıkrasına göre 43. Madde hükümlerin uygulanacaktır. Failin, 244. Madde kapsamında düzenlenen suçları

işlemek kastı yaptığı eylem ile TCK'da düzenlenen başka suçlara da sebebiyet vermesi mümkün olacaktır. Bu durumda ise TCK 4. Madde ile düzenlenen fikri içtima hükümlerine başvurulacak ve faile işlediği suçlardan en ağır cezayı gerektiren hüküm uygulanacaktır.

TCK 244. madde ile düzenlenen suç ile 142. Madde ile düzenlenen nitelikli hırsızlık suçunun bilişim sistemleri aracılığıyla işlenmesi suçu arasındaki ilişkiye değinmek gerekmektedir. Hırsızlık suçunun bilişim sistemleri vasıtasıyla işlenmesi halinde nitelikli hal oluşturacağı ve daha ağır bir cezaya hükmolunacağı madde ile düzenlenmiştir. Madde metnindeki kasıt, fiilin hırsızlık suçunu bilişim sistemlerini kullanarak işlemesidir. Buradaki amaç, bilişim sistemlerindeki veri değil, bilişim sistemlerindeki varlığın hırsızlık suretiyle çalınması olmalıdır. Örneğin, fail mağdurun internet bankacılığı şifresini öğrenerek hesaptaki parayı ele geçirmesi 142/2(e) ile düzenlenen suçu oluşturacaktır.[129] Yargıtay 11. Ceza Dairesinin 2011/11569 E. ve 2011/21245 K. Sayılı kararında da bu görüşe yönelik hüküm bulunmaktadır: *"Yargıtay Ceza Genel Kurulunun 17.11.2009 gün ve 2009/11-193-268 sayılı kararında ayrıntıları açıklandığı üzere, sanığın, şikayetçiye ait interaktif bankacılığa açık hesap bilgilerini ve şifreyi öğrenip kendi hesabına para transfer etmek şeklinde oluşan eyleminin TCK.nun 142/2-e maddesindeki bilişim suretiyle hırsızlık suçunu oluşturduğunun gözetilmemesi aleyhe temyiz olmadığından bozma sebebi yapılmamıştır. Toplanan deliller karar yerinde incelenip, yüklenen suçun sübutu kabul, oluşa ve soruşturma sonuçlarına uygun şekilde vasfı tayin, cezayı arttırıcı ve azaltıcı sebeplerin bulunmadığı takdir kılınmış, incelenen dosyaya göre verilen kararda eleştiri dışında bir isabetsizlik görülmemiş olduğundan sanık ve müdafiinin yerinde görülmeyen temyiz itirazlarının reddiyle hükmün istem gibi ONANMASINA, 31.10.2011 gününde oybirliğiyle karar verildi."*

3.2.7. Yaptırım

244. Madde metni incelendiğinde kanun koyucunun 1. Fıkrada düzenlenen bilişim sistemlerini engelleyen ve bozan kişiler için bir yıldan beş yıla kadar hapis

[129] Gökçen, Balcı, Çakır, a.g.e., s.46

cezası verdiği görülmektedir. Maddenin ikinci fıkrasında düzenlenen verilere yönelik gerçekleştirilebilecek suçlara karşı ise altı aydan üç yıla kadar hapis ile cezalandırılacağı belirtilmiştir. Kanun koyucu her iki suç tipi için de hürriyetten yoksun kılma cezasını düzenlemiştir. Maddenin üçüncü fıkrasına göre belirtilen hallerin gerçekleşmesiyle ise verilecek cezanın yarısı oranında artırılacaktır.

TCK 243. Maddesinde olduğu gibi 243. Maddedeki suçların işlenmesi halinde görevli mahkeme 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkındaki Kanun'un 11. Ve 12. Maddeleri gereği Asliye Ceza Mahkemeleri, yetkili mahkemeler ise suçun işlendiği yer mahkemesidir.

3.3. BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI SUÇU (M.245)

3.3.1. Genel Olarak

Bilişim sistemlerinin gelişmesi ile ekonomik düzenin en temel kurumlarından bir tanesi olan bankaların da neredeyse tüm işlemleri artık elektronik ortamda da yapılabilmektedir. Kullanıcılarına verilen hizmetin artırılması ve modern bilişim çağının yakalanması adına adeta bankalar arasında teknoloji hizmetlerini geliştirme yarışı başlamıştır. Böylece bankacılık hizmetleri ve kart kullanımının hem ticarette sağladığı kolaylıklar hem de yeni nesil ticari düzenin temel taşlarından olmaları gereği toplumun büyük bir kesiminin hayatına girdiğinden söz edilecektir. Ekonomik ve ticari ağın içerisinde büyük bir yer edinen ve toplumlar içerisinde yoğun seviyede yaygın ve etkin kullanılan hizmetlerin büyümesine karşı da elbette banka ve kredi kartlarına karşı işlenebilecek suçların sayıları paralel bir şekilde artmaktadır.

5237 Sayılı TCK'nın 245. Maddesi ile banka veya kredi kartlarının kötüye kullanılması suç sayılmıştır. Maddeye göre: *"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart*

sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. (2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır. (3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır."

Banka veya kredi kartlarının kötüye kullanılması suçuna yeni TCK ile münhasır bir madde ile bilişim suçlarına yönelik düzenlenen bölüm içerisinde yer verilmiştir.

245. madde birinci fıkrası ile bir kişinin başka bir kişiye ait banka veya kredi kartını elinde bulunduran kimsenin kart sahibinin rızası olmadan bu kartı kullanması veya kullandırtması ile haksız yarar sağlaması suç olarak düzenlenmiştir. Failin, kartı kart sahibinin rızasına uygun veya aykırı bir şekilde elinde bulundurduğunun bir önemi yoktur. Suçun oluşması için önemli olan kart sahibinin rızası olmadan kart üzerinden yarar sağlanmasıdır.

245. maddenin ikinci fıkrasıyla ise başkalarına ait olan banka hesapları ile ilişkilendirerek sahte banka kartı üretmek, satmak, devretmek, satın almak veya kabul etmek hareketleri suç sayılmıştır. Suçun temelinde sahte olarak üretilen veya sahteleştirilen banka veya kredi kartları bulunmaktadır. Madde ile sayılan suçlardan bir tanesinin icrası ile suç gerçekleşmiş sayılacaktır.

Maddenin üçüncü fıkrası ile ikinci fıkrasında belirtilen üretilerek veya dönüştürülerek elde edilen sahte kartlar ile kişilerin kendisi veya başkası adına yarar sağlaması suç olarak düzenlenmiştir. Kişilerin 245. Maddenin üçüncü fıkrası ile düzenlenen suçun icrası için önce ikinci fıkradaki sahte karta ulaşması veya oluşturması, sonrasında bu kart ile bir menfaat sağlaması gerekmektedir.

Kanun koyucu maddenin dördüncü ve beşinci fıkralarında ise şahsi cezasızlık sebepleri ve cezayı kaldıra ya da hafifleten şahsi sebepleri düzenlemiştir. Madde metnine göre: *"(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. (5) (Ek: 6/12/2006 – 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.*

TCK 245. Maddenin devamına 2016 tarihinde yeni bir suç tipi eklenmiştir. 245/A'ya göre: *"(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."* Bilişim suçları alanında düzenlenen bu yeni suç tipine göre bilişim sistemleri ile işlenebilecek olan bir bilişim suçunu gerçekleştirmek amacıyla bir cihaz, program, şifre veya kod oluşturan , ithal eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulundan failler cezalandırılacaktır.

3.3.2. Şahsi Cezasızlık Sebepleri ve Cezayı Kaldıran veya Azaltan Şahsi Sebepler

245. maddenin dördüncü fıkrasıyla birlikte birinci fıkrada düzenlenen başkasına ait banka veya kredi kartını kullanarak haksız yarar sağlama suçunu sayılan akrabalar arasında işlenmesi halinde şahsi cezasızlık hallerinin ortaya çıkması düzenlenmiştir.[130] TCK m. 245/4'e göre: *"(4) Birinci fıkrada yer alan suçun; a)*

[130] Mahmut Koca, İlhan Üzülmez, a.g.e., s.855

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."

TCK 245. Maddeye 06.12.2006 tarihli 5560 sayılı kanun ile eklenen 5. Fıkra ile 168. Madde ile düzenlenen etkin pişmanlık hükümlerinin birinci fıkrada düzenlenen başkasına ait banka veya kredi kartını kullanarak haksız yarar sağlama suçuna da uygulanacağı kanunlaştırılmıştır. Madde metnine göre: *"Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır".* Etkin pişmanlık hükümleri, onuncu bölüm malvarlığına karşı suçlar başlığı altında düzenlenmiştir. Madde metnine göre Hırsızlık, mala zarar verme, güveni kötüye kullanma, dolandırıcılık, hileli iflâs, taksirli iflâs suçları tamamlanması ve failin, azmettiren veya yardım edenin kovuşturma başlamadan önce bizzat pişmanlık göstermesi ve mağdurun zararını aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde etkin pişmanlıktan bahsedilebilecektir. Kovuşturma başlamadan önce ortaya çıkan etkin pişmanlık hallerinde verilecek ceza üçte ikisine kadar, kovuşturma başladıktan sonra fakat hüküm verilmeden önce gösterilen etkin pişmanlık hallerinde ise verilecek ceza yarısına kadar indirilir. Nitekim, suçtan dolayı verilecek olan ceza tamamen ortadan kalkmamakta fakat cezada indirim yapılabilmektedir.[131]

3.3.3. Korunan Hukuki Yarar

Bilişim alanında işlenen suçlardan banka veya kredi kartına karşı işlenilen suçlar maddesi ile 3 farklı suç tipi ve 245/A maddesi ile yasak cihaz veya programlar ile ilgili suçlar düzenlenmiştir. Düzenlenen bu suçlar ile öncelikle başkalarına ait kartlara karşı yapılacak hukuka aykırı müdahaleler veya erişimler suç unsuru sayılmışken diğer fıkralarda sahte kart üretilmesi ve kullanılmasının önüne geçilmeye

[131] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, "Türk Ceza Kanunu Özel Hükümler", Genişletilmiş ve Güncellenmiş 14. Baskı, Seçkin Yayınevi, Ankara, 2019, s.1009

çalışılmıştır. Böylece kart sahipleri, bankalar ve ticari satıcılara karşı yapılacak hukuksuzluklar cezai müeyyidelere bağlanmıştır.

Bu suçla korunan hukuksal değer hakkında ise çeşitli görüşler öne sürülmüştür Bir görüşe göre banka veya kredi kartlarının hukuka aykırı olarak kullanılmasıyla banka veya kart sahiplerinin zarara uğratılması ve bu zarardan faillerin menfaat elde etmesi engellenmiştir.[132]

Başka bir görüşteki yazar ise bu suçun sadece bilişim yolları kullanarak işlenebileceği için bu suçun bir bilişim suçu olması ve suçla korunan hukuki yararın da banka veya kredi kartı sahiplerinin mal varlığının korunmasıdır.[133]

Diğer bir görüşe göre 245. Madde ile düzenlenen suç ile korunan hukuksal değerler temelde güvene yönelik değerlerden oluşmaktadır. Bunlar hırsızlığa, dolandırıcılığa, güveni kötüye kullanma ve sahteciliğe karşı güvenin korunmasıdır. Yazar, bu değerlerin malvarlığının korunması etrafında toplanabileceğini savunmuş, hatta 245. Madde ile düzenlenen suçların malvarlığı ile ilgili suçlar başlığı altında toplanmasının daha doğru olacağını belirtmiştir.[134]

245. madde ile korunan hukuki yararın ağırlıklı olarak malvarlığının korunmasına yönelik olduğu görülmektedir. Gerçekten de banka veya kredi kartları ile kişilerin öncelikle maddi açıdan zararları ortaya çıkmaktadır. Fakat korunan değerin malvarlığına yönelik olması suçun malvarlığı ile ilgili olduğunu göstermemektedir. Banka veya kredi kartlarına yönelik suçlar bilişim sistemleriyle işlenmekte ve bilişim sistemleri aracılığıyla icra edilmektedir.

3.3.4. Suçun Maddi Unsurları

3.3.4.1. Fail

Kanun koyucu madde metni ile düzenlediği suçlarda faile yönelik herhangi bir özellik belirtmemiştir. Dolayısıyla herkesin bu suçta fail olması mümkündür. Suç ile

---

132 Cevat Özel, **"Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı"**, İstanbul Barosu Dergisi, C. 75, Sayı 7-8-9, 2001, s.862, (Aktaran) Karagülmez, a.g.e., s.260

133 Kurt, a.g.e., s.205

134 Dülger, a.g.e., s. 458

failin ya da bir başkasının menfaatine yarar elde edildiğinin ise bir önemi yoktur. Madde ile belirtilen başkasına ait olan banka veya kredi kartının her ne şekilde ele geçirilmiş olursa olsun kart sahibinin rızasına aykırı şekilde kullanılması veya kullandırılması hareketi ile suç icra edilmiş sayılacaktır. Suçun işlenmesi sonucunda menfaati sağlanan kişi eğer bir tüzel kişilik olursa, 246. Madde ile düzenlenen güvenlik tedbirlerine hükmolunur.[135]

3.3.4.2. Mağdur

Madde metni ile yine mağdura yönelik herhangi bir özellik belirtilmemiştir. Herkesin bu suç ile mağdur olabilmesi mümkündür. Banka veya kredi kartlarının sahibi olan veya kendisine verilmesini bekleyen kişiler bu suçun mağduru olabilecektir. Bu kartların maddede düzenlendiği şekilde hukuka aykırı kullanılmasıyla dolaylı yoldan firmaların veya bankaların da bu suçtan zarar görmesi mümkün olabilecektir. Öyle ki düzenlenen suç ile mağdur konumunda olan kişiler malvarlığında azalma olan kişilerdir. Kişilerin kartlarına yönelik suçun gerçekleştiği takdirde ilgili kurumlar suçtan zarar gören konumunda olacaktır. Yargıtay 6. Ceza dairesinin de bu konuyla ilgili 9.7.2012 tarihli, 2011/2110 E., 2012/13824 K. Numaralı kararında belirttiği bir görüşü mevcuttur: *"CGK'nın 04.10.2011 gün ve 2011/6-166-2011/213 sayılı kararında, 5464 sayılı Banka ve Kredi Yasasının 3. Maddesinde banka kartının 'mevduat hesabı veya özel cari hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanması sağlayan kart' olarak tanımlandığı, banka kartında mülkiyetin bankaya, 'kullanım hakkının ise kart hamiline ait olduğu', anılan Yasada kart hamilinin; banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek ya da tüzel kişi olduğunun belirtildiği, TCY'nın 245/1. Maddesinde düzenlenen suçun mağdurunun kredi veya banka kartı hamili olduğu, ayrıca birinci fıkrada; 'kartın kedisine verilmesi gereken kişi'den söz edilmekte olup, bu kişinin de esasen kart hamili olduğu, suçun işlenmesinde her ne kadar banka ve kredi kurumunun bilişim sistemi aracı olarak kullanıldığı ve banka kartlarının mülkiyeti bankaya ait ise de; bu hususlar*

[135] Artuk, Gökçen, Yenidünya, a.g.e., s.900

suçun mağduru olduğu anlamına gelmemekte olup, bu durumda banka veya kredi kurumlarının 'suçtan zarar gören' konumunda olduğu, eylemleri sonucu malvarlığında azalma meydana gelenin, diğer bir ifade ile 'suçun mağduru olan kişinin kart hamili olduğu', kart hamilinin malvarlığına yönelik bu suçun banka veya kredi kartları aracılığıyla işlenmiş olmasının korunan hukuki yararın mağdurun malvarlığı olduğu gerçeğini değiştirmeyeceği…"

3.3.4.3. Suçun Konusu

Banka veya kredi kartlarına yönelik düzenlenen suçlarda suçun konusu her fıkra için ayrı ayrı ele alınabilecektir. İlk fıkra ile düzenlenen suçta başkasına ait banka veya kredi kartına yönelik gerçekleştirilecek hareketler suç sayılmıştır. Bu hareketler ile failin kendisine veya başkasına yarar sağlaması suç olarak kabul edilmektedir. Böylece birinci fıkrada düzenlenen suçun konusunu failin kendisine veya başkasına yarar sağlaması oluşturacaktır.

Maddenin ikinci fıkrasın ile sahte banka veya kredi kartlarının üretilmesi, devredilmesi, satın alınması veya kabul edilmesi düzenlenmiştir. Bu fıkrada failin herhangi bir yarar sağlanması aranmamıştır. Dolayısıyla ikinci fıkradaki suçun konusunu sahte olarak üretilen banka veya kredi kartları oluşturacaktır.

245. maddenin son fıkrası ile sahte banka veya kredi kartlarının kullanılmasıyla yarar sağlanması düzenlenmiştir. Bu fıkrada düzenlenen suçun konusunu da sahte banka veya kredi kartları ve onlar ile sağlanan yarar oluşturacaktır.

245. maddeye getirilen ek madde ile bilgisayar programları veya cihazları ile işlenebilecek suçlar düzenlenmiştir. Dolayısıyla getirilen bu ek madde ile düzenlenen suçun konusu yasak cihaz ve programlardır.

3.3.4.4. Hareket

245. madde ile 3 farklı suç düzenlenmiştir. Birinci fıkra ile başkasına ait kredi veya banka kartı ile kişinin rızası olmadan yarar sağlanması hareketi düzenlenmiştir. Fıkrada belirtilen hareket kişinin kendisi veya başkasının menfaatine yarar sağlanmasıdır. Yarar sağlanmanın nasıl olacağı fıkra ile belirtilmediği için birinci fıkrada serbest hareketli suç düzenlenmiştir. Ayrıca başkasına ait kredi veya banka kartının haksız yarar elde etmek için kullanılması için önce bu kartların haksız bir şekilde elde edilmesi gerekmektedir. Dolayısıyla suç serbest hareketli birleşik suçtur.

İkinci fıkra ile sahte kartlar ile gerçekleştirilebilecek suçlar düzenlenmiştir. Bu suçlar başkasına ait banka hesabıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, bu kartların satılması, devredilmesi, satın alınması veya kabul edilmesi eylemleri ile gerçekleşmektedir. Kanun koyucu fıkra ile düzenlenen suçun hangi hareketler ile gerçekleştirilebileceğini düzenlemiştir. Dolayısıyla fıkrada düzenlenen suç tipi seçimlik hareketli suçtur. Ayrıca fıkra ile belirtilen kartların üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi için öncesinde başkasına ait bir hesap ile ilişkilendirilmesi gerekmektedir.

Maddenin üçüncü fıkrası ile sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle yarar sağlanması suçu düzenlemiştir. Kanun koyucu yine bu fıkra ile birini fıkradakine benzerlik göstererek suçun yarar sağlanması eylemiyle gerçekleşeceğini düzenlemiştir. Failin belirtilen kart tipleri hangi şekilde yarar sağladığının suçun icrası açısından bir önemi yoktur. Kanun koyucunun bu fıkra ile getirdiği hükümlere göre 3. Fıkra da serbest hareketli bir suçtan bahsetmektedir.

245/A'ya göre düzenlenen suçun icrası için yasak cihaz veya programların bir bilişim suçunun işlenmesi için imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması hareketlerinin gerçekleştirilmesi gerekmektedir. Suç bu programların bilişim suçu işlenmesi kastı ile yukarıda sayılan

hallerin icrası ile tamamlanacaktır. Dolayısıyla madde ile serbest hareketli bir suç düzenlemiştir ve failin bu hareketlerden herhangi birisi gerçekleştirmesi suçun icrası için yeterlidir.

3.3.4.5. Netice

Maddenin birinci ve üçüncü fıkrası ile suçun gerçekleşmesi için düzenlenen hareketin kişinin kendisi veya başkası menfaatine yarar sağlaması olduğundan bahsedilmişti. Dolayısıyla 245. Maddenin birinci ve üçüncü fıkralarında düzenlenen suçların tamamlanması için yarar sağlanması gerekmektedir. Suç işlemek kastıyla belirtilen hareketlere başlanmış veya tamamlanmış olsa da yapılan haksız eylemlerin 245. Maddenin birinci ve üçüncü fıkradaki suçlara tabi olabilmesi için haksız yararın sağlanma şartı aranmaktadır. Maddenin ikinci fıkrası ve getirilen ek madde ise bu fıkralarda düzenlenen hareketlerin tamamlanması ile suç tamamlanmış olacaktır.

3.3.5. Hukuka Aykırılık

5237 sayılı TCK'nın 245. maddesi ile düzenlenen banka veya kredi kartına yönelik suçlar, açıkça gerçekleştirilen eylemlerin kart sahibinin veya kartın kendisine teslim edeceği kişinin rızasına aykırı olarak icra edilmesi ile gerçekleştirilecektir. Madde ile düzenlenen eylemlerin kart sahibinin veya kartın gönderildiği kişinin rızası ile gerçekleşmesi halinde hukuka aykırılık oluşturulmayacaktır. İlgili kişilerin rızası 245. Maddede belirtilen suçlar için hukuka uygunluk sebebi oluşturacaktır. Ayrıca kanun koyucu tarafından açıkça düzenlenmediği için suçun taksirle işlenmesi mümkün değildir.

245. maddenin dördüncü fıkrası ile birinci fıkrada yer alan suçların işlenmesi halinde dahi cezaya hükmolunmayacağı şahsi cezasızlık sebepleri ve cezayı kaldıran şahsi sebepler düzenlenmiştir. Fıkra ile düzenlenen hükümdeki sebeplerin var olduğu

durumlarda failin birin fıkrada belirtilen suçları gerçekleştirmesi halinde dahi fail hakkında cezaya hükmolunamayacaktır. Dördüncü fıkra ile cezayı ortadan kaldıran sebeplerden failin faydalanabilmesi için bazı şartların uygunluğu gerekmektedir. Failin suçun icrası gerçekleştirdiği sırada evliliğinin devam etmesi, evlatlık kararının kesinleşmiş olması, kardeşler ile aynı konutta sürekli olarak birlikte yaşaması gerekmektedir.[136]

3.3.6. Kusurluluk

Banka veya kredi kartlarına karşı suçlar kenar başlıklı 245. Madde ile düzenlenen suçların icrasında da failin kusurlu kabul edilebilmesi için 243. Ve 244. Maddelerde olduğu gibi kınanabilmesi gerekecek, kınanmadığı hallerde fail kusurlu sayılamayacaktır. 243. Ve 244. Maddede belirtildiği gibi failin cebir veya tehdit altında olduğu durumlarda fail, kusurlu sayılamayacaktır.

3.3.7. Suçun Özel Görünüş Biçimleri

3.3.7.1. Teşebbüs

245. maddenin birinci fıkrası ile başkasına ait banka veya kredi kartlarının kullanılması ile kendisi veya başkasının menfaatine yarar sağlayan kişi suçu icra etmiş olacaktır. Suç serbest hareketli bir suçtur ve bu suç hareketlerinden yarar sağlanması ile suç tamamlanmış olacaktır. Başkasına ait banka veya kredi kartını haksız yere eline geçiren kişinin bu hareketten yarar sağlayamadan elinde olmayan sebeplerle suçu tamamlayamamış olması halinde suç teşebbüs aşamasında kalmış olacaktır. Örneğin fail başkasının banka veya kredi kartını ele geçirdikten sonra herhangi bir alışveriş

136 Sacit Yılmaz, **"Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu"**, TBB Dergisi, Sayı 87, 2010, s.291-292 (Çevrimiçi)

yapmaya yönelik hareket gerçekleştirmesiyle kartın bağlı bulunduğu banka hesabında bakiye olmadığı uyarısı alırsa veya para çekmeye çalıştığı ATM'nin karta el koymasıyla ve bu hareketler sonucunda yarar sağlayamazsa teşebbüsten sorumlu olacaktır. Ayrıca doktrinde tartışmalı olan meselelerden bir tanesi ise failin başkasına ait banka veya kredi kartını ele geçirmesinden sonra kart ile herhangi bir yarar sağlayamaması halinde failin teşebbüsten mi yoksa 141. Maddeden mi sorumlu olacağıdır.[137] Bir görüşe göre kanun koyucunun birleşik olarak düzenlediği bu suçun teşebbüs aşamasında olup olmadığı failin suç hareketine başlamasıyla ilgilidir. Fail eğer başkasına ait banka veya kredi kartını ele geçirerek başkası veya kendi adına haksız bir yarar sağlamaya yönelik harekete başlamadıysa 245. Madde ile düzenlenen suçun teşebbüs aşamasında kalmasından değil, kartın ele geçirilmesi açısından haksız bir durum varsa bu suçtan sorumlu olacaktır.[138] Başka bir görüşe göre ise failin suça teşebbüsten sorumlu olabilmesi için kastına bakılması gerekmektedir. Eğer fail bu suçun icrasına başladığında yarar elde etme kastıyla başlamış fakat elinde olmayan sebeplerle suçu tamamlayamamış ise 245. Madde ile düzenlenen suça teşebbüsten sorumlu olacaktır. Aksi halde fail kartı haksız yere elde etme suçundan sorumlu olacaktır.[139]

245. maddenin ikinci fıkrası ile düzenlenen madde ile seçimlik hareketli suç düzenlenmiştir. Fıkra ile sayılan hareketlerin bir tanesinin tamamlanmış olması ile suç tamamlanmış olacaktır. Failin bu hareketlerin herhangi birini suçun icrasına başladıktan sonra elinde olmayan sebeplerle tamamlayamaması halinde suç teşebbüs aşamasında kalmış olacaktır.

Maddenin son fıkrası ile düzenlenen sahte kartların kullanılması yolu ile yarar sağlama suçunun teşebbüs aşamasında kalması mümkündür. Fail, eğer sahte kartlara 245. Maddenin 3. Fıkrasında düzenlenen suçların icrası amacıyla sahip olduysa ve kullanmaya yönelik hareketini icra ederken elinde olmayan sebepler ile yarar

---

137 Türk Ceza Kanunu m. 141: *"(1) Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verilir."*

138 Yavuz Erdoğan, **"Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile)**, İstanbul, Legal Yayıncılık, 2012 (Aktaran) Dülger, a.g.e., 2015, s.508

139 Karagülmez, a.g.e., s. 271

sağlayamadıysa fail teşebbüsten 245. Maddenin 3. Fıkrasındaki suça teşebbüsten sorumlu olacaktır. Fakat fail, adı geçen kartları kullanamadan suç yarıda kaldıysa 245. Maddenin 3. Fıkrasına teşebbüsten değil 245. Maddenin ikinci fıkrasındaki suçun icrasından sorumlu olacaktır.

245. maddeye getirilen ek madde ile suçun tamamlanması için yasak cihaz ve programların kullanılması suretiyle gerçekleştirileceği düzenlenmiştir. Böylece failin elinde olmayan sebeplerle sayılan hareketlere başlanmış olmasına rağmen yasak cihaz ve programların kullanılamayarak suçun tamamlanmaması halinde fail teşebbüse göre sorumlu olacaktır.

3.3.7.2. İştirak

Kanun koyucu 245. Madde ve ek madde ile düzenlenen tüm suçlarda iştirake özel bir duruma hükmetmemiştir. Dolayısıyla TCK ile düzenlenen genel iştirak hükümleri bu maddeye uygulanabilecektir.

Maddenin beşinci fıkrası ile eklenen etkin pişmanlık gösterilmesi halinde verilecek cezanın indirilmesi durumunun iştirak halinde bu suçun işlenmesi halinde nasıl sonuçlanacağı tartışılmalıdır. 168. Madde metninde failin, azmettirenin veya yardım edenin bizzat pişmanlık göstermesi ve zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi aranmıştır. İştirak halinde bir kişinin bizzat pişmanlık göstererek zararı tamamen gidermesi ile ortaya çıkacak olan indirim halinin sadece bu kişi üzerinde mi yoksa suça iştirak eden diğer kişiler üzerinde de uygulanacağı hususunda, iştirak eden diğer kişilerin zararın giderilmesi konusundaki katkıları ve pişmanlık dereceleri araştırılmalıdır.[140]

[140] Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, a.g.e., s.1010

3.3.7.3. İçtima

245 maddenin birinci fıkrası ile düzenlenen suçun zincirleme şekilde işlenmesi mümkündür. Fail, başkasına ait banka veya kredi kartıyla kısa aralıklarla aynı yararı sağlayabilecektir. Örneğin, kendisine sadece koruması için bir süreliğine emanet edilen bir karttan üst üste ATM'den para çeken kişi, 245. Maddenin birinci fıkrasındaki suçu zincirleme şekilde işlemiş olacaktır. Fail, farklı kartlar ile aynı anda para çekmiş olursa her suç için ayrı ceza alacak, zincirleme suça tabi tutulmayacaktır. Ayrıca bu fıkra ile düzenlenen suçun başka suçlarla birlikte işlenerek içtima hükümlerine veya aynı anda başka suçların işlenmesi haliyle fikri içtima hükümlerine tabi olması mümkündür.

Maddenin ikinci fıkrası ile düzenlenen suç için de zincirleme suç hükümleri oluşması mümkündür. Fail, bir başkasına ait sahte bir banka veya kredi kartını değişik zamanlarda üretebilecek veya ürettiği kartı başka kişilere satabilecektir. Böylece fail hakkında zincirleme suç hükümleri uygulanabilecektir.

Maddenin üçüncü fıkrası ile düzenlenmiş olan sahte kartların kullanılması ile yarar sağlama suçunun zincirleme olarak işlenmesi mümkün olabilecektir. Kişi, örneğin bir başkasına ait ve üzerinde sahtecilik yapılmış bir kart ile zincirleme şekilde alışveriş yaparak yarar sağlayabilecektir. Ayrıca, madde metninde geçen "*daha ağır cezayı gerektiren başka bir suç oluşturmadığı taktirde"* ifadesi, bu suçun başka bir suç ile işlenmesi halinde suçların birleşmesi veya fikri içtima gibi hükümlerin uygulanamayacak olması açıkça düzenlenmiştir.[141] Öyle ki failin bu suçun icrasını gerçekleştirirken farklı suçlar da işlemiş olması halinde daha ağır cezayı hangi suç öngörüyorsa o suçun düzenlendiği madde uygulanacak, diğer maddeler suçun cezalanmasında nazara alınmayacaktır.

245. maddenin birinci fıkrasıyla düzenlenen *"başkasına ait bir kartı her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse"* suçun ayrıca 141 ve

[141] Dülger, a.g.e., 2015., s. 518

142. maddede düzenlenen hırsızlık suçunu oluşturup oluşturmayacağı hususunda farklı görüşler bulunmaktadır. 141. Madde ile düzenlenen hırsızlık suçu ile 245. Madde ile düzenlenen suçun bileşik suç olma durumu doktrinde birçok yazarın görüşüne göre uygun görülmemektedir. M. Koca ve İ. Üzülmez'e göre bileşik suçun varlığından söz edilebilmesi için söz konusu olan iki suçtan birinin diğerinin nitelikli hali veya unsuru olduğu kanunda açıkça belirtilmelidir. Yazarlar, bu husus gözetilerek bakıldığında 245. Maddenin 1. Fıkrasında herhangi bir unsur belirtilmemiş olması ile madde ile düzenlenen suçta herhangi bir bileşik suçtan bahsedilemeyeceğini belirtmiştir.[142]

Konuya değinen Dülger, 245/1. Maddede ile düzenlenen hükümde suçun oluşması için kartın ele geçirilmesinin veya bulundurulmasının yeterli olmayacağını, ayrıca kartın kullanılacağı veya kullandırılacağı ve haksız yarar elde edileceği halde suçun oluşacağını belirtmiştir. Yazarın belirttiğine göre hırsızlık suçu için ise yalnızca kartın zilyedinden rızasız bir şekilde alınması yeterli olacaktır. Dolayısıyla, bir eylem ile iki suçun aynı anda oluşabilmesi mümkün olmayacaktır. [143]

Konuyla ilgili Tezcan, Erdem ve Önok ise iki suç arasında tüketen-tüketilen norm ilişkisinden bahsetmekte ve kart ele geçirildikten sonra işlenen suç oluştuğu halde 245/1. Maddenin uygulanacağını belirtmektedir.[144] Bir normun, diğer normları kapsarsa, yani diğer normlar tarafından korunan hukuksal değerleri bünyesinde barındırıyorsa tüketen-tüketilen norm ilkesi ortaya çıkmaktadır. İlkeye göre fiile yalnızca tüketen norm hükümleri uygulanabilecektir.[145]

Yargıtay ise bu konuyla ilgili uyuşmazlıklarda uygulamayı şekillendiren bir kararında bileşik suç hükümlerinin uygulanamayacağını hem hırsızlık hem de başkasına ait banka veya kredi kartlarının kullanılması suretiyle haksız yarar elde edilmesi suçlarının ayrı ayrı ortaya çıktığını ve failin iki suçtan cezalandırılması gerektiğini belirtmiştir. Yargıtay Ceza Genel Kurulu'nun 30.03.2010 tarih, 2010/11-17 E., 2010/65 K. Sayılı kararı metninde konu detaylıca incelenmiştir: "

142 Koca, Üzülmez, a.g.e., s.859

143 Dülger, a.g.e., s. 541

144 Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **"Teorik ve Pratik Ceza Özel Hukuku"**, 8. Baskı, Ankara, 2012, s.771

145 İçel, a.g.e. ,s.38

Görüldüğü gibi her iki yasada da benzer şekilde tanımlanan hırsızlık suçu; başkasına ait taşınabilir bir malı sahibinin (zilyed) rızası olmaksızın faydalanmak kastı ile bulunduğu yerden almaktır. 5237 sayılı TCY'nin hazırlanmasında esas alınan asıl kural gerçek içtima olup "kaç fiil varsa o kadar suç, kaç suç varsa o kadar ceza" söz konusu olacaktır. Nitekim Adalet Komisyonu raporunda bu husus; "Ceza hukukunun temel kurallarından birisi, kaç fiil varsa o kadar suç, kaç suç varsa o kadar ceza vardır' şeklinde ifade edilmektedir. Bunun istisnaları, suçların içtimai bölümünde belirlenmiştir. Bu istisnalar dışında, işlenen her bir suçla ilgili olarak ayrı ayrı cezaya hükmedilecektir. Böylece verilen her bir ceza, bağımsızlığını koruyacaktır" şeklinde ifade edilmiştir (TBMM Adalet Komisyonu'nun 03.08.2004 gün ve 1/593-60 sayılı Raporu). Bu kuralın istisnaları ise, 5237 sayılı TCY'nin "suçların içtimai" bölümünde, 42 (bileşik suç), 43 (zincirleme suç) ve 44. (fikri içtima) maddelerinde düzenlenmiştir. Gerçek içtima kuralının istisnalarından birisi olan ve uyuşmazlık konusuyla yakından ilgisi bulunan bileşik suç, Yasa'nın 42. maddesinde; "Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir" şeklinde tanımlanmış ve bununla da yetinilmeyerek; "bu tür suçlarda içtima hükümleri uygulanmaz" hükmü getirilmiştir. Ceza Genel Kurulu'nun 13.02.1984 gün ve 322-64 sayılı kararında; "...eriyen ve eriten başka ifade ile kaynaşan suçlardan biri diğerinin unsuru veya ağırlaştırıcı sebebini teşkil ettiğinin yasada açıkça gösterilmesi şarttır ve bu şart suç ve cezaların kanuniliğinin gereğidir" denilerek bileşik suçta unsur ya da ağırlaştırıcı nedeni oluşturan suçun, bileşik suç olarak düzenlenen bağımsız suçun içinde mutlaka ve ayrıca gösterilmesi gerektiği vurgulanmıştır. 5237 sayılı Yasa'nın 245/1. maddesinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun yasadaki düzenleniş şekli göz önüne alındığında bileşik suç olarak düzenlenmediği görülmektedir. Banka veya kredi kartının kötüye kullanılması suçu ile birlikte oluşabilecek diğer suçlara yasada öngörülen ceza miktarları da bu suçun bileşik suç olarak düzenlenmediğini açıkça ortaya koymaktadır. Bu nedenle, banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi durumunda oluşabilecek hırsızlık, yağma, güveni kötüye kullanma, dolandırıcılık gibi suçlar ile banka veya kredi kartlarını kötüye kullanma suçu arasında gerçek içtima kuralı uygulanarak fail her bir suçtan ayrı ayrı cezalandırılmalıdır. (Veli Özer Özbek, Banka veya Kredi Kartlarının Kötüye

Kullanılması Suçu, Bilişim Hukuku Konferansı, Yargıtay Başkanlığı, 2008, s. 108; Fahri Gökçen TANER, ""Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu Bir Bileşik Suç mudur?" Ankara Üniversitesi Hukuk Fakültesi Dergisi, Yıl: 2007, Cilt 56, Sayı 2, s. 80) Bu açıklamalar ışığında birinci uyuşmazlık konusu değerlendirildiğinde; 5237 sayılı TCY'nin 245/1. maddesindeki banka veya kredi kartlarını kötüye kullanma suçu bileşik suç olarak düzenlenmemiş olup, yasa maddesinde geçen ""her ne surette olursa olsun" ifadesi banka veya kredi kartlarının sadece hukuka uygun yollardan ele geçirilmesini kapsamaktadır. Bunun sonucu olarak; sanığın kurduğu düzenek ile ATM makinesine para çekmek için gelen mağdurların şifresini de öğrenmek suretiyle ele geçirdiği, ekonomik değeri bulunduğunda kuşku bulunmayan menkul mal niteliğindeki banka kartı ile başka bir ATM cihazına gidip para çekmesi şeklinde gerçekleştirdiği eylemlerinde, banka veya kredi kartının kötüye kullanılması suçu yanında hırsızlık suçu da oluşmaktadır. Bu itibarla, sanığın eylemlerinin ayrıca hırsızlık suçunu oluşturmayacağına ilişkin Yargıtay C.Başsavcılığı itirazında isabet bulunmamaktadır. 2- Banka veya kredi kartlarının kötüye kullanılması suçunun yanında hırsızlık suçunun da oluştuğuna oybirliği ile karar verildikten sonra, sanık hakkında 5237 sayılı TCY'nin 145. maddesinin uygulanma koşullarının bulunup bulunmadığının araştırılmasının gerekip gerekmediği hususuna gelince: Konu daha önce de Ceza Genel Kurulu'nun önüne gelmiş ve 15.12.2009 gün ve 242-291 ile 13.11.2007 gün ve 210-234 sayılı kararlarda çözüme kavuşturulmuştur. 5237 sayılı TCY'nin 145. maddesinde; "(1) Hırsızlık suçunun konusunu oluşturan malın değerinin azlığı nedeniyle, verilecek cezada indirim yapılabileceği gibi, ceza vermekten de vazgeçilebilir" hükmü yer almakta iken, anılan hüküm suç tarihinden önce 29.06.2005 gün ve 5377 sayılı Yasa'nın 16. maddesi ile; "(1) Hırsızlık suçunun konusunu oluşturan malın değerinin azlığı nedeniyle, verilecek cezada indirim yapılabileceği gibi, suçun işleniş şekli ve özellikleri de gözönünde bulundurularak, ceza vermekten de vazgeçilebilir" şeklinde değiştirilmiş, madde ile hırsızlık suçlarına, "konu edilen değer" in azlığı nedeniyle yargıca, cezada indirim yapma veya ceza vermeme yönünde, geniş bir takdir yetkisi tanınmıştır. Anılan maddenin gerek ilk şekli, gerekse değiştirilmiş biçimi; ortak tanımlama ile, hırsızlık suçunun konusunu oluşturan değerin az olmasını temel almaktadır. Değer azlığı ile yasa koyucu tarafından neyin kastedildiği, duraksamaları önleyecek biçimde açıklığa kavuşturulmamış, rakamsal bir sınırlandırma

getirilmemiş, ancak yargıca, yargılama konusu maddi olayla ilgili olarak takdir ve değerlendirme yetkisi tanınmıştır. Ne var ki, yasa koyucu, yargıcın takdirini, soyut ve farklı bir disiplinle sınırlandırmıştır. O da; "az olarak kabul edilecek değerin" yargıcın takdirinde, ceza vermekten vazgeçmesini gerektirecek ehemmiyetsiz ölçüde olması, başka bir ifade ile değere dayalı ihlalin ceza verilmemeyi nesafeten haklı saydıracak alt düzeyde bulunmasıdır. Yargıç, çalınan veya çalınmaya kalkışılan bu değerin azlığını ya indirimli bir cezayla ya da suçun istenmesindeki özellikler itibarıyla ceza vermemekle değerlendirebilecektir. Maddenin ilk metninden sonraki değişiklikte; "suçun işleniş şekil ve özellikleri gö zönünde bulundurularak" ibaresinin, "cezada indirim" seçeneğinden sonra ve "ceza vermekten vazgeçilebilir" seçeneğinden önce yazılmasının, suça konu malın değerini farklılaştırmayacağı açıktır. Bu nedenle; "az ceza verme" seçeneğinde daha yüksek değerin aranacağı, "ceza vermekten vazgeçme" halinde ise daha az bir değerin aranmasının gerekli olduğu sonucuna ulaşılmamalıdır. Bu itibarla, 5237 sayılı Yasa'nın 145. maddesinin uygulanmasında, 765 sayılı TCY'nin 522. maddesinde öngörülen "hafif" ya da "pek hafif" kavramlarıyla irtibatlı bir yoruma gidilmemeli, Yargıtay'dan, anılan maddenin uygulanması sürecindeki içtihatlarına paralel şekilde, yıllık değer ölçülerini belirlemesi beklenmemelidir. 5237 sayılı Yasa'nın 145. maddesinin konuluş amacı gözetilmeli, anılan hükmün 765 sayılı TCY'nin 522. maddesinden farklı olduğu kabul edilmelidir. Yargıç, bu değerlendirmenin yanı sıra her somut olayda, suçun işleniş şekli, mağdur veya sanığın konumu, olayın gerçekleştiği yer ve zamanı dikkate alacak, 5237 sayılı TCY'nin 3. maddesinde işaret edildiği üzere, "işlenen fiilin ağırlığıyla orantılı" olacak şekilde bir cezaya hükmetmek suretiyle ceza adaletini sağlayacaktır. Görüldüğü gibi madde ile getirilen sistem, sadece malın değerinin objektif ölçütlere göre belirlenerek cezadan indirim veya ceza verilmemesinden ibaret değildir. Olayın özelliği, mağdurun konumu, failin kişiliği ve suçun işleniş şekli her olayda değerlendirmeye konu edilecek, meydana gelen haksızlığa faili iten etkenler ve bu haksızlığın mağdur üzerindeki etkileri de gözetilerek, maddenin uygulanıp uygulanmaması ve özellikle ceza verilmeme haliyle ilgili seçeneğin, eylemin failine uygun düşüp düşmeyeceği belirlenecek ve takdirin gerekçesi de kararda gösterilecektir. Ancak burada 5237 sayılı TCY'nin 147. maddesinde düzenlenmiş bulunan "ağır ve acil bir ihtiyacı karşılamak için hırsızlık suçunun işlenmesi" hali ile 145. maddede

*öngörülen "değer azlığı"kavramı karıştırılmamalıdır. 145. maddede öngörülen değer azlığı ile zorunluluk halini düzenleyen 147. maddenin uygulanma koşulları birbirinden farklı olup, 147. maddenin ayırıcı ölçütü hırsızlığın ağır ve acil bir ihtiyacı karşılamak için yapılmasıdır. Buna karşılık 145. maddenin uygulanmasındaki en önemli kriter kuşkusuz değer ölçüsüdür ve bu değerin "ceza vermeme" halini de haklı saydıracak düzeyde az olmasıdır. Bu açıklamalar ışığında ikinci uyuşmazlık konusuna ilişkin olarak somut olay değerlendirildiğinde; Sanığın ATM makinesine para çekmek veya işlem yapmak için gelen kişilerin banka kartını ele geçirebilmek için bir düzenek kurduğu, bankamatiğe taktığı bu düzenek nedeniyle işlem yapamayan ve kartları bankamatiğe sıkışan kişilerin yanına yardım etme görünümü altında yaklaştığı, şifrelerini öğrenebilmek amacıyla şifrelerini yeniden girmelerini istediği, böylece şifrelerini öğrendiği, sanığın kurduğu düzenek nedeniyle banka kartı ATM cihazına sıkışan mağdurların telefon etmek için uzaklaşması üzerine banka kartını tornavida ile çıkarttığı, ele geçirdiği banka kartı ile başka bir bankamatikten mağdurların hesabından para çektiği anlaşılmakta olup, bu şekilde gelişen olayda, suçun işleniş şekli itibariyle 5237 sayılı TCY'nin 145. maddesinin uygulanma koşullarının bulunmadığı sonucuna ulaşılmaktadır. Bu itibarla sanık hakkında hırsızlık suçundan hüküm kurarken 5237 sayılı TCY'nin 145. maddesini uygulamayan yerel mahkemenin takdirinde ve Özel Daire kararında bir isabetsizlik bulunmamaktadır. Sanığın eylemlerinin banka veya kredi kartının kötüye kullanılması suçunun yanında hırsızlık suçunu da oluşturduğu yönünde oy kullanan üç Kurul Üyesi; * sanık tarafından olay tarihinde hırsızlık yoluyla ele geçirilen banka kartlarının tekrar elde edilmesi için sahipleri tarafından yapılan masraflar hesaplanmalıdır Ayrıca bankaların zaman zaman müşteri kazanabilmek için hiçbir masraf almadan banka kartlarını müşterilerine verme eğilimleri olduğundan bu hususlar hırsızlık suçundan dolayı 5237 sayılı TCY'nin 145. maddesinin uygulanma koşullarının değerlendirilmesi amacıyla araştırılmalıdır. Bu nedenle de eksik araştırmaya dayanan yerel mahkeme hükmünün bozulması gerekir" düşüncesiyle karşı oy kullanmışlardır."* Bu kararıyla Yargıtay Ceza Genel Kurulu, iki suç tipi arasındaki ilişkiyi detaylıca ele alarak, karar sonrasında ortaya çıkacak olan uyuşmazlıklara da yön verecektir. Yazarların ve Yargıtay'ın görüşleri arasında bazı farklılıklar ortaya çıksa da tüm görüşlere göre iki suçun bileşik suç olarak değerlendiremeyeceği açıklığa kavuşmuştur. Başkasına ait banka veya

kredi kartını elinde bulunduran kimsenin bu kartı kullanarak haksız yarar elde etmesi halinde 245/1. Maddenin uygulanması gerektiği görülmektedir.

Uygulamada TCK 245. Maddenin üçüncü fıkrası ile TCK 158. Maddesinin birinci fıkrasının f bendine yer alan düzenlemeler benzerlik göstermektedir. Kanun koyucu ilgili düzenleme ile *"f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,"* işlenen suçları nitelikli dolandırıcılık olarak saymıştır. Yargıtay kararları geriye dönük incelendiğinde, banka veya kredi kartları ile kendisi veya başkası menfaatine haksız yarar sağlanması suçunun bilişim sistemlerine yönelik işlenmesi nitelikli dolandırıcılık suçu olarak değerlendirilmekteydi. Ancak, yeni TCK ile düzenlenen 245. Madde ile birlikte bu suçlar 158/1-(f) bendinin düzenlediği nitelikli dolandırıcılık suçunu değil 245. Madde ile düzenlenen suçu oluşturacaktır.[146] Öyle ki, hukuka aykırı hareketin gerçek kişilere yönelik değil de bilişim sistemlerine yönelik gerçekleştirilmesi sonucunda dolandırıcılık suçu yerine bilişim sularına yönelik düzenlemeler esas alınacaktır. Bilişim sisteminin bir araç olarak kullanılarak gerçek bir kişinin aldatılması halinde ise nitelikli dolandırıcılık suçu oluşacaktır[147] Yargıtay 11. Ceza dairesinin 2007/8423 E. Ve 2008/117 sayılı Kararı ile iki suç arasındaki fark daha net olarak anlaşılmaktadır: *"Somut olayda; sanığın, katılan Mücahit S'in kimlik bilgilerine göre düzenlenip kendi fotoğrafı yapıştırılmış ele geçirilemeyen sahte nüfus cüzdanını kullanarak katılan A A.Ş.nin Yenigün Şubesi'nde hesap açtırarak diğer katılan Murat Ç'ın bankada bulunan para hesabındaki var olan verileri (bilgileri) sahte kimlikle açtırdığı hesaba internet yoluyla havale edip hesap cüzdanı ibraz ederek banka şubesinden çektiğinin iddia ve kabul olunması karşısında; eyleminin, paranın sanığın açtırdığı hesaba intikaline kadar katılan Murat Ç'a yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle 5237 sayılı TCK. nun 244/4 maddesine uyan suçu oluşturduğu gözetilmeden, vasıflandırılmada yanılgıya düşülerek unsurları oluşmayan banka aracı kılınmak suretiyle nitelikli dolandırıcılık suçundan mahkûmiyet hükmü kurulması, 2- Sanığın hesap açtırmak için kullandığı sahte nüfus cüzdanının elde edilememesi ve sahteciliğin iğfal kabiliyetini haiz olup olmadığının*

146 Ali Parlar, a.g.e., s. 173

147 Ahmet Gökcen, Murat Balcı, Kerim Çakır, **"Malvarlığına Karşı Suçlar"**, Adalet Yayınevi, Ankara, 2018, s210

saptanamamış bulunması, aynı belgenin başka işlemler sırasında da kullanılıp aldatıcılık yeteneğinin tespit edilememesi, banka görevlilerinin ihmali davranışları sebebiyle hesabın açılmış olma ihtimali de nazara alındığında sırf sahte nüfus cüzdanı ile işlem yapılmasının iğfal kabiliyetinin varlığını kabul için yeterli olmadığı gözetilmeden yüklenen sahtecilik suçundan beraati yerine isabetsiz gerekçe ile yazılı şekilde mahkumiyet hükmü kurulması, Yasaya aykırı, sanık müdafiinin temyiz itirazları bu nedenle yerinde görülmüş olduğundan, hükmün 5320 Sayılı Yasanın 8/1. maddesi gereğince uygulanması gereken 1412 Sayılı CMUK'nun 321. maddesi gereğince BOZULMASINA, ceza yönünden kazanılmış hakkının saklı tutulmasına .22.01.2008 gününde oybirliğiyle karar verildi." Karar metninden de anlaşılacağı üzere Yargıtay'ın da görüşüne göre bilişim sistemine yönelik gerçekleştirilen suçlar 243, 244 ve 245. Madde ile düzenlenen suçlar kapsamına girmektedir.

Yargıtay 11. Ceza Dairesinin 2013/12333 E. Ve 2015/28785 K. sayılı bir başka kararında ise yine bilişim sistemlerine yönelik bir hareket bulunduğundan 245. Maddenin 3. Fıkrasının uygulanması gerektiğini belirtmiştir: *"Sanığın fiziki kredi kartı olmaksızın sadece kart numarasını kullanarak haksız yarar sağlanmasından ibaret eyleminin 5237 sayılı TCK'nun 245/1 maddesindeki "banka kartının kötüye kullanılması" suçunu oluşturacağı gözetilmeden; eylemin bölünmesi suretiyle sanığın hem 5237 sayılı TCK'nun 245/1 maddesi gereğince beraatine hem de 5237 sayılı TCK'nun 158/1 son maddesi gereğince dolandırıcılık suçundan mahkumiyetine dair karar verilmesi, Yasaya aykırı, sanığın temyiz itirazları bu itibarla yerinde görülmüş olduğundan…"*

3.3.8. Yaptırım

5237 sayılı Türk Ceza Kanunun 245. Maddesi ve ek madde ile düzenlenen suçların cezai yaptırımları kanun metninde açıkça belirtilmiştir. 245. Maddenin birinci fıkrasına göre başkasına ait kartları her ne suretle olursa olsun ele geçiren ve bulunduran kişilerin bu kartlar ile yarar sağlaması haline üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılacaktır. Kanun maddesinde

düzenlenen iki ceza hükmü arasında *"ve"* bağlacı kullanılmıştır. Dolayısıyla suçun işlenmesi ile hürriyetten yoksun bırakma ve adli para cezalarına aynı anda hükmedilecektir.

Maddenin ikinci fıkrasında düzenlenen sahte kartları üreten, satan, devreden, satın alan veya kabul eden kişiler üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır. Bu fıkra ile de getirilen cezalar seçimlik değil birlikte uygulanacak cezalardır.

Maddenin son fıkrasında düzenlenen sahte kartların kullanılması suçunu icra eden faillere yönelik ise gerçekleştirdiği fiil daha ağır bir cezayı gerektirmiyorsa dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur. Kanun koyucu, bu madde ile yine birleşik cezaya hükmetmiştir.

Maddeye 2016 yılında getirilen ek madde ile yasak program ve cihazlarla işlenebilen suçları icra eden faile yönelik bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

243 ve 244. Maddelerde olduğu gibi 245. Madde ve ek maddedeki suçların işlenmesi halinde görevli mahkeme 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkındaki Kanun'un 11. Ve 12. Maddeleri gereği Asliye Ceza Mahkemeleri, yetkili mahkemeler ise suçun işlendiği yer mahkemesidir.

SONUÇ

İnsanlık tarihinin ilk gününden bugüne kadar geliştirilen icatlar birbirini takip etmiş ve dönemlerinin yansımalarını oluşturmuştur. Toplumların bu icatlara gösterdiği refleksler ve reformlar her dönem değişmiştir. Teknolojinin en yeni icatlardan biri olmasına karşın aynı zamanda dünyanın değişimine yön veren en büyük icat olduğu da kuşkusuz bir gerçektir. Teknoloji ile birlikte hızla gelişen bilişim sistemleri artık sonu tespit edilemeycek kadar büyük bir ufuk çizmektedir. Haberleşme ve iletişim ağı için kurulan internet bugün, dünyaya pararel bir yaşam alanı oluşturmuştur.

Dijital dünyayla birlikte ekonomik ve sosyal sistemlerde bir çok değişiklik ortaya çıkmıştır. 2000'li yıllar ile birlikte insanlık blockhain, kripto para, yapay zeka ve dijital ticaret gibi kavramlarla tanışmıştır. Özellikle kripto para teknolojileri ile birlikte klasik kağıt paranın alternatifleri oluşmaya başlamıştır. İnsanlığın bir ihtiyaç üzerine ürettiği, ekonomik ve sosyal talepleri ile geliştirdiği teknolojiler ile birlikte sessiz bir bilişim devrimi yaşanmaktadır.

Hukuk ve adalet sistemleri insanlığın temel ihtiyaçları ve hakları gözetilerek düzenlenmektedir. Kanuni düzenlemeler, toplumların örf ve adetleri, coğrafi etkenleri ve inanç sistemleri göz önüne alınarak insan hayatını kapsayıcı bir şekilde oluşturulmaya çalışılır. Evrensel hukuk normları ise coğrafi şartların, örf ve adetlerin ve inanç sistemlerinin üzerinde tüm insanlığı kapsayıcı ilkeler getirmektedir. Dolayısıyla hak ve adaletin tesisi için insanlığın temel hak ve hürriyetlerinin her alanda korunması ve hukukun her alanda bir çerçeve ile kalkan görevini üstlenmesi gerekmektedir.

Hukuk, vuku bulmuş suçları cezalandırmayı değil, gerçekleşebilecek suçların önüne geçmeyi amaçlamalıdır. Suç kavramı bilişim ortamlarını kapsamayan gündelik hayatta ne kadar önlenmesi gereken bir hukuksuzluk terimi ise, bilişim sistemlerinde de bir o kadar önemli bir konumda yer almaktadır. Bilişim sistemleri kullanıcıları sanal kişiliklerden değil insanlarda oluşur. Dolayısıyla bilişim sistemlerinde işlenen suçları da sanal olarak değerlendirmek ve klasik suçlardan ayırmak hukuk açısından fahiş bir hataya sebebiyet verecektir.

Bilişim suçlarındaki yaygınlaşmayı kanuni düzenlemeler ile sınırlandırmak bilişim teknolojilerinin takip edilmesi zor bir şekilde gelişmesi ve değişmesinden ötürü olası gözükmemektedir. Teknolojinin gelişme hızıyla birlikte kanuni düzenlemelerin aynı hızda gelişim seyretmesi de pek mümkün değildir. Bundandır ki mevcut yaptırımların geniş ve ciddi müeyyidelerden oluşması, oluşabilecek suçların önüne geçmede yardımcı olabilecektir. Bu düzenlemelerin oluşturulmasındaki en büyük güçlük ise, kişisel veriler ve kişilerin hakları hukuk ile korunurken, yine ortaya çıkartılan hukuksal düzenlemeler ile kişilerin hak ve özgürlüklerine müdahale etmemektir.

Bilişim suçlarının önüne geçmek ve kişilerin hak ve özgürlüklerini korumak adına bu suçların yasal düzenlemeler ile sınırlandırılmadan belirtilmesi ve yaptırımlar ile caydırıcılığının artırılması gerekmektedir. Bu suçlar ve suçların yaptırımları belirlenirken temel ilkenin kişilerin hak ve özgürlüklerinin korunması olduğu gözden kaçırılmamalıdır. Yapılacak olan her yasal düzenleme, temelde kişilerin hak ve özgürlüklerinin korunmasını esas alırken, pratikte de uluslararası düzenlemeleri ve teknolojinin uluslararası boyutta gelmiş olduğu son seviyeyi baz alması gerekmektedir. Bu değişim ve gelişimi takip etmekle birlikte, suçların yaptırımlarının standart bir şekilde düzenlenmesiyle caydırıcılığının etkisinin kabul edilebilir hale getirilmesi ve artık toplumlar ve devletler nezdinde sabit bir suç fikri oluşturulması gerekmektedir. Suçun genel halleri gibi özel hallerinin düzenlenmesi, cezai normlar oluşturulması, klasik suçlar gibi yasal düzenlemelere yer verilmesi, suçun işleniş

şekilleri açısından müeyyideleri kuvvetlendiren düzenlemeler getirilmesi gerekmektedir. Böylece bilişim alanında işlenebilecek suçlardan önce bu alanda suç işlemeye hazırlanan failleri suça teşvik eden denetimsizlik ve hukuki açıklar önlenebilecek, oluşturulan ulusal ve uluslararası yasal düzenlemeler ve bu düzenlemelerin getirdiği müeyyideler caydırıcı olabilecektir. Bilişim suçlarının engellenmesine yönelik gerçekleştirilecek hukuksal reformların en önemli noktalarından bir tanesi de şüphesiz bu suçlara karşı uluslararası ittifak ile güncelliğini koruyan kapsayıcı düzenlemelerin getirtilmesidir.

Bilişim suçlarına yönelik alınabilecek bir diğer önlem ise toplumların bu konuda yeterli bilgi sahibi olması ve kanunlaştırılan düzenlemelerin toplumlarda unutulan veya göz ardı edilen hukuksal düzenlemeler yerine güncelliği ve önemi hakkında bilinçlendirilmesi olabilecektir. Bu suçlara karşı toplumsal bir mücadele gerçekleşmediği sürece etkisiz gözüken bilişim alanındaki hukuk ihlallerinin varlığı suç dünyasındaki yerini her zaman koruyacaktır. Bunun önüne geçmek için ise, bilişim sistemlerindeki herhangi bir araç ile bu alanda faaliyet gösteren, iş ve işlemler yapan kişilere veya kurumlara kullanılan bilişim yöntemi hakkında gerekli bilgilerin ve alınabilecek tedbirlerin anlatılması gerekmektedir. Eğitim sistemlerinin ilk etabından başlayarak bilişim alanına yönelik kademeli bir şekilde yapılabilecek ve güncelliğini koruyacak müfredat düzenlemelerinin yanında kamusal bilinçlendirme faaliyetleri ile gerekli toplumsal farkındalığın oluşmasının önünde herhangi bir engel yoktur. Böylece hem bu suçlara karşı kullanıcıların farkındalığı artabilecek, hem bu suçların işlenmesine yönelik caydırıcılık oluşturulabilecektir.

Devletlerin hukuk sistemlerinin bilişim sistemleriyle tanışması 1980'li yılların sonunda gerçekleşmiştir. Bilgisayarın ve bilişim teknolojilerinin kullanılmasından yıllar sonra bu alanlara özel kanuni düzenlemelerin hukuk sistemlerine girmesi elbette bu düzenlemelerde geç kalındığını göstermektedir. ABD, Almanya, Fransa gibi ülkelerin başını çektiği bilişim hukuku düzenlemeleri Avrupa Siber Suç Sözleşmesi, Birleşmiş Milletler çalışmaları ile belirli temellere oturtulmuştur. Her güne bir teknolojik devrimin sığdığı bilişim çağında, bilişim hukukuna yönelik çalışmaların ve reformların sabit kalmaması beklenmektedir.

Türk hukuk düzeni ise 1990'lı yıllarla birlikte bilişim kavramlarıyla tanışmıştır. Dönemin tıkanmış bürokratik düzeni ve siyasetin geri kalmış hegemonyası ile birlikte bilişim alanında olduğu gibi bilişim hukuku alanında da gereken atılımlar ülkemizde gerçekleşememiştir. Bilişim ile ilgili çalışmaların hukuk sistemlerinde gelişebilmesi için yalnızca hukuksal değil, her alanıyla bu sistemler ile ilgili kitlesel bilinçlendirme ve eğitim projeleri gerçekleştirilmelidir. Bununla birlikte oluşabilecek farkındalık hukuk sistemlerindeki bilişim reformlarına zemin hazırlayacaktır. Gerek eğitim sistemlerinin ilk etabından itibaren bilişim derslerinin kenara itilmiş saatler sınıfından çıkartılması, gerek lisans seviyesinde daha nitelikli ve evrensel teknolojilere uyumlu bir şekilde eğitimler verilmesi zorunlu hale gelmiştir. Öyle ki nesillerin, ilkokullarda tabletler vasıtasıyla eğitim aldığı, sınavlarının elektronik ortamlarda yapıldığı ve hayatlarının içerisinde sosyal veya fen bilimleri kadar yer etmiş bilişim sistemlerine ve bu sistemlerde haklarına tehdit oluşturan unsurlara yabancı bir şekilde gelişmesi hayatın akışıyla çelişki oluşturacaktır. Bilişim sistemlerine yönelik gerekli çalışmalarım yapılmasıyla bilişim teknolojilerinin pratikte kullanıldığı gibi teoride de zihinlerde sindirilmesiyle birlikte bilişim hukukuna duyulan ilgi ve alaka artacaktır.

Bilişim suçlarına yönelik Türk Hukukundaki en kapsayıcı hukuksal düzenlemeler Türk Ceza Kanunu ile yapılmıştır. 243,244 ve 245. Maddeler ile düzenlenen doğrudan bilişim suçlarına yönelik cezalar ile birlikte dolaylı şekilde bilişim suçlarıyla ilgili birtakım maddeler yine Türk Ceza Kanunu ve bazı özel düzenlemeler ile kanunlaşmıştır. 243. Madde ile *"Bilişim Sistemine girme veya orada kalma suçu"* düzenlenmiştir. Getirilen değişiklik ile *"ve"* ifadesinin *"veya"* ile değiştirilmesi isabetli olmuştur. İki suç farklı suç tiplerini oluşturmaktadır. Önceki düzenleme ile bilişim sistemine hukuka aykırı erişerek orada kalmayan kişiler suça karışmış olmayacak ve cezaya çarptırılmayacaktır. Son yapılan değişiklik ile bu karışıklığın ortadan kaldırılması bilişim sistemine haksız erişilmesi suçunun engellenmesi adına isabetli olmuştur.

Farklı kanunlar ve yönetmelikler ile getirilen düzenlemeler bilişim suçlarına ve sistemlerine yönelik hukuksal düzenlemelerin sayısını artırmaktadır. İlk bakışta bilişim suçlarının TCK ile düzenlenmesi suçların diğer TCK maddeleri ile ilişkisi ve benzerlikleri sebebiyle isabetli olarak gözükse de birçok farklı madde, kanun ve yönetmelikler ile dağınık olarak düzenlenmiştir. Bu dağınıklıkla birlikte bilişim suçlarının eski Türk Ceza Kanunu ile düzenlenmesi geleneği korunmaktadır. Getirilen yeni düzenlemeler ise ya bilişim suçları başlığı altına getirilmekte, ya da çeşitli kanun maddelerine eklemeler yapılarak hukuk sistemine entegre olmaktadır. Gerek bilişim alanı ile ilgili hükümlerin kapsayıcılığının ve ciddiyetinin artırılması, gerek bilişim alanına münhasıran bir düzenleme yapılması konusunda örnek hukuk devletleri arasına girilmesi bilişim suçlarının işlenmesinde caydırıcı rol oynayacak ve bilişim çağında bilişim hukukuna yönelik geç kalınmış bir adım atılmış olunacaktır.

Hukuk, her devrimden önce devrimin önlem ve tedbirlerini tespit etmeli ve adaletin gecikmesinin önüne geçmelidir. Bugün ise her güne bir bilişim devrimi sığdıran bir çağ yaşanmaktadır. Adaletli hukuk sistemleri dünün pişmanlıklarıyla değil geleceğe ilhamıyla anılmaktadır. Ekonomik sistemlerin temeli olan para birimlerinin, eğitim sisteminin direği olan sınavların, ticaretin kaynağı olan alışverişin değiştiği bu çağda hukuksuzluklara önlem almak adına değişimi beklemek en büyük adalet zaafı olacaktır. Örnek verilecek olursa gelişmiş devletlerin ileride sanal paraya geçmesi ve bu konudaki hukuki düzenlemeleri gerçekleştirmesini izleyen bir hukuk sistemi, ancak bu alanda büyük kayıplar verdikten sonra bir hukuki düzenlemeyi iktibas edebilecektir. Bu yönde atılması gereken en önemli adım, akademik, siyasal ve hukuksal alanlarda özel kurulların oluşturulması ve bu kurulların uluslararası gelişmeler ışığında alanında küresel nitelikteki uzmanlar ile çalışmasını sağlamaktır.

KAYNAKÇA

AKÇAKAYA, Murat, "E-Devlet Anlayışı ve Türk Kamu Yönetiminde E-Devlet Uygulamaları", Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2017, sayı 3, (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/421877

AKGÖZ, Burak Cesur, "Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri", Bilişim Uzmanlığı Tezi, 2018, Ankara, S.205 (Çevrimiçi) Https://Www.Btk.Gov.Tr/Uploads/Thesis/Burak-Cesur-Akoz-B-Uzm-Tezi-5d10d910e20e8.Pdf

AKINCI, Fisun Sokullu, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler Ve İnternette Çocuk Pornografisi", İstanbul, c.lıx s.1-2, 2001, (Çevrimiçi), https://dergipark.org.tr/tr/download/article-file/95989 Erişim Tarihi:30.04.2021

ALATAŞ, Şükrü, "Phıshıng: İnternet Denizinin Popüler Avlanma Yöntemi", (Çevrimiçi), http://ab.org.tr/ab07/bildiri/154.pdf

ALİUSTA, Cahit, Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, C. 4, No:2, 2018, (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/645923

ALTAN, Naci "Bilgisayar Terimleri Ansiklopedik Sözlüğü", Sistem Yayıncılık, 3. Baskı, İstanbul 2003

ALTUNOK, Ebru**, VURAL,** Ali Fatih, "BİLİŞİM SUÇLARI", (Çevrimiçi), https://dergipark.org.tr/tr/download/article-file/2088539

ARTUK, Mehmet Emin, **GÖKÇEN,** Ahmet, **YENİDÜNYA,** Ahmet Caner, "Türk Ceza Kanunu Şerhi Özel Hükümler Madde 235-345", Cilt 5, Ankara, 2009

ARTUK, Mehmet Emin, **GÖKÇEN,** Ahmet, **YENİDÜNYA,** Ahmet Caner, "Türk Ceza Hukuku Özel Hükümler", 15. Baskı, Adalet Yayınevi, Ankara, 2015

ATQİLL, Nichole, "Senior Legal Specialist Western Law Division Law Library Of Congess", April, 2002

AVŞAR, B. Zakir, **ÖNGÖREN**, Gürsel, "Bilişim Hukuku", İstanbul, Türkiye Bankalar Birliği Yayınları, 2010

AYDIN, D. Emin, **"**Bilişim Suçları ve Hukukuna Giriş**",** Doruk Yayınevi,1992

BALCI, Murat, "Yasadışı Kumar ve Bahisle Hukuksal Mücadele", Yeşilay Dergisi, 2021

BİÇKİN, İnci, "Elektronik İmza Ve Elektronik İmza İle İlgili Yasal Düzenlemeler", TBB Dergisi, 2006, sayı 63, (Çevrimiçi) http://tbbdergisi.barobirlik.org.tr/m2006-63-210

BOZKURT YÜKSEL, Armağan Ebru, Bulut Bilişimde Kişisel Verilerin Korunması (Personel Data Protection in Cloud Computing), Ankara, 2016, Yetkin Yayınları

CANBEK, Gürol, **SAĞIROĞLU,** Şeref, "Kötücül Ve Casus Yazılımlar: Kapsamlı Bir Araştırma", (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/75575

DÜLGER, Murat Volkan**; MODOĞLU,** Gözde**,** "Bilişim Suçları, Soruşturma Ve Kovuşturma Yöntemleri İle İnternet Ve İletişim Hukuku Uygulama Rehberi",

DÜLGER, Murat Volkan, "Bilişim Suçları ve İnternet İletişim Hukuku", Ankara, Seçkin Yayınevi, 6. Baskı, Eylül 2015

DÜLGER, Murat Volkan, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", Türkiye Adalet Akademisi Dergisi, Yıl:8, Sayı:31, Temmuz 2017, (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/981531

ELMALICA, Hasan, "Bilişim Çağının Ortaya Çıkardığı Temel BirİnsanHakkı Olarak Unutulma Hakkı", Ankara Üni. Hukuk Fak. Dergisi, sayı 65, 2016, (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/621578

EFE, Ahmet, "Bilişim Hukuku Alanındaki Sorunlar ve Risklerin Mevzuat Boyutuyla Analiz ve Çözümlemesi", Türkiye Noterler Birliği Hukuk Dergisi, 2016, sayı 1, s.175 (Çevrimiçi) https://www.researchgate.net/publication/309229256_Bilisim_Hukuku_Alanindaki_Sorunlar_ve_Risklerin_Mevzuat_Boyutuyla_Analiz_ve_Cozumlemesi

ERDEM, Merve, **ÖZOCAK,** Gürkan, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun Ve Türk Hukukunun Rolü", Ankara Üni. Hukuk Fak. Dergisi, 68, 2019, (Çevrimiçi), hhttps://dergipark.org.tr/tr/download/article-file/695490

ERSİN, Masum, **REFİK,** Samet, "Mobil BOTNET ile DDoS Saldırısı", BİLİŞİM TEKNOLOJİLERİ DERGİSİ, CİLT: 11, SAYI: 2, NİSAN 2018, (Çevrimiçi), https://dergipark.org.tr/tr/download/article-file/465726

GÖKÇEN, Ahmet**, ÇAKIR,** Kerim**, ALŞAHİN,** Mehmet Emin**, BALCI,** Murat**,** "Ceza Muhakemesi Hukuku", 3. Baskı, Adalet Yayınevi, Ankara, 2018

GÖKÇEN, Ahmet**, BALCI,** Murat**, ÇAKIR,** Kerim**,** "Malvarlığına Karşı Suçlar", Yayınevi, Ankara, 2018

HENKOĞLU, Türkay, "Bilgi Güvenliği ve Kişisel Verilerin Korunması", 2015, Ankara, Yetkin Yayınevi

İÇEL, Kayıhan, "Görünüşte Birleşme (İçtima) İlkeleri Ve Yeni Türk Ceza Kanunu", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi Yıl: 7, Sayı 14,

Güz 2008, (Çevrimiçi) https://www.ticaret.edu.tr/uploads/kutuphane/dergi/s14/035-049.pdf

İHTİYAROĞLU, Uğur, "Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi", Hakemli Makale, 2020, (Çevrimiçi) https://dergipark.org.tr/tr/download/article-file/1070186

İKİZLER, Metin, **BAŞAR,** M. Sinan, "Spam'ın Zararları ve Spam ile Hukuki Mücadele: ABD Örneği ve Türk ve Avrupa Birliği Hukukları ile Karşılaştırma", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 8, Sayı: 2, 2006, (Çevrimiçi), https://hukuk.deu.edu.tr/dosyalar/dergiler/DergiMiz8-2/pdf/mikizler.pdf

KARAGÜLMEZ, Ali, "Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri" 3. Baskı, Ankara, Seçkin Yayıncılık, 2011

KARAKEHYA, Hakan, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", TBB Dergisi, Sayı 81, 2009, (Çevrimiçi), http://tbbdergisi.barobirlik.org.tr/m2009-81-498

KENT, Bülent, "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu", Ankara Sosyal Bilimler Üniversitesi Bilişim Hukuku Dergisi, Haziran, Sayı 1, 2020, (Çevrimiçi) https://kutuphane.asbu.edu.tr/sites/idari_birimler/kddb.asbu.edu.tr/files/inline-files/Bilis%CC%A7im%20Hukuku%20Dergisi_8.pdf

KOÇAK, Hüseyin, **DANDİN,** Ali Nazmi, "Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri", Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi / Cilt: 19, Sayı: 1, Haziran 2017, s.145 (Çevrimiçi), https://dergipark.org.tr/tr/download/article-file/357841

ÜNSAL, Aydın**,** "Bilişim Terimleri Sözlüğü", Türk Dil Kurumu Yayınları, Ankara, Ankara Üniversitesi Basımevi, 1981

KURT, Levent**,** "Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması", Seçkin Yayıncılık, Ankara 2005, s. 162.

MASUM, Ersin, **SAMET,** Refik, "Mobil BOTNET ile DDoS Saldırısı", Bilişim Teknolojileri Dergisi, CİLT: 11, SAYI: 2, NİSAN 2018, (Çevrimiçi), https://dergipark.org.tr/tr/download/article-file/465726

MAHMUTOĞLU, Fatih. S., "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu", S.41 (Çevrimiçi) Https://Dergipark.Org.Tr/Tr/Download/Article-File/95993

MÜLLER, Heinrich, **WEİCHERT,** Frank, **"**Vorkurs Informatik Der Einstieg ins Informatikstudium**",** Springer Fachmedien

NİZAM, Ali**, CABİROĞLU,** Gökhan, "Yönetici ve Son Kullanıcılar İçin Bilişim", Mayıs 2014, İstanbul Fatih Sultan Mehmet Vakıf Üniversitesi Yayınları

ORTA, Mesut, "Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)", Yetkin Yayınları, Ankara, 2015

ÖNAL, Huzeyfe, "DOS/DDOS Saldırıları, Savunma Yolları Ve Çözüm Önerileri", (Çevrimiçi),https://www.bgasecurity.com/makale/dos-ddos-saldirilari-ve-korunma-yontemleri-kitabi/

ÖZBEK, Veli Özer**, KANBUR,** Mehmet Nihat**, DOĞAN,** Koray**, BACAKSIZ,** Pınar**,** Türk Ceza Hukuku Genel Hükümler", 7. Baskı, Ankara, 2014

ÖZDEMİRCİ, Fahrettin**, AKDOĞAN,** Zeynep**,** "Bilgi Sistemleri ve Bilişim Yönetimi, Beklentiler ve Yeni Yaklaşımlar", Ankara, 2017, Ankara Üniversitesi Basımevi

ÖZEL, Cevat**,** "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İstanbul Barosu Dergisi, C. 75, Sayı 7-8-9, 2001

ÖZEN, Muharrem, "Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku", Adalet Yayınevi, 2011

ÖZGENÇ, İzzet, "Türk Ceza Hukuku Gazi Şerhi (Genel Hükümler)", 6. Baskı, Ankara, Seçkin Yayıncılık

PARLAR, Ali, ""Türk Ceza Hukukunda Dolandırıcılık Suçları", 2. Baskı, Bilge Yayınevi, Ankara, 2015

SINAR, Hasan, "İnternet ve Ceza Hukuku", 2001, İstanbul, Beta Yayınevi,

ŞAMLI Rüya, "Türk ve Dünya Hukukunda Bilişim Suçları, Akademik Bilişim" 10 - XII. Akademik Bilişim Konferansı Bildirileri, 2010, (Çevrimiçi), https://ab.org.tr/ab10/kitap/samli_AB10.pdf

ŞEHİTOĞLU Onur, "Bilgisayar ve Ağ Üzerinden İşlenen Siber Suçlarla Mücadelenin Hukuksal Ve Güvenlik Boyutu", Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2004

TEZCAN, Mete, **ERDEM,** Mustafa Ruhan, **Önok,** R. Murat, "Teorik ve Pratik Ceza Özel Hukuku", 8. Baskı, Ankara, 2012

TURAN, Metin; "Bilişim Hukuku", Seçkin Yayınevi, 2020, 4. Baskı

TEVETOĞLU, Mete, "Bilişim Hukuku", 2006, İstanbul, Kadir Has Üniversitesi Yayınları TURAN, Metin; "Bilişim Hukuku", Seçkin Yayınevi, 2020, 4. Baskı

TOPALOĞLU, Murat**, ÖZKİŞİ,** Harun**, TEKKANAT,** Egemen, "Bulut Bilişim", 2017, Ankara, Seçkin Yayıncılık

TURHAN, Oğuz, "Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)". Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Yayınlanmamış Tez, (Çevrimiçi), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf

YAZICIOĞLU, R. Yılmaz, "Bilgisayar Suçları, Krimonolojik Sosyolojik ve Hukuki Boyutları ile", 1. Baskı, İstanbul, Alfa Yayınları

YILDIZ, Mithat, "Siber Suçlar Ve Kurum Güvenliği**"**, Yayımlanmamış Tez, (Çevrimiçi), https://www.uab.gov.tr/uploads/pages/kutuphane/efcecbe1f21e9fe.pdf

YILMAZ, Sacit**,** "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu", TBB Dergisi, Sayı 87, 2010, s.291-292 (Çevrimiçi) http://tbbdergisi.barobirlik.org.tr/m2010-87-611 Erişim Tarihi: 03.05.2021

YILMAZ, Sacit, "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", Türkiye Barolar Birliği Dergisi, 2011, Sayı 92, s.68 (Çevrimiçi) http://tbbdergisi.barobirlik.org.tr/m2011-92-669 Erişim Tarihi: 03.05.2021

Bilgi Teknolojileri ve İletişim Kurumu "Sık Sorulan Sorular", <https://tuketici.btk.gov.tr/guvenli-internet > Erişim Tarihi: 20.02.2021

Bilgi ve İletişim Teknolojileri Kılavuzu, <https://www.btk.gov.tr/uploads/pages/slug/kilavuz.pdf> Erişim Tarihi: 20.02.2021

Bilişim Teknolojileri Ve Siber Güvenlik Derneği, <http://www.bs.org.tr/destekledigimiz-projeler/spam-mesaja-hayir/33#:~:text=Herhangi%20bir%20ileti%C5%9Fim%20yolu%20ile,nitelikte%20g%C3%B6nderilmesi%20Spam%20olarak%20adland%C4%B1r%C4%B1l%C4%B1r> Erişim Tarihi: 20.02.2021

Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi <http://hukuk.deu.edu.tr/dosyalar/dergiler/dergimiz-15-1/senercelik.pdf> Erişim Tarihi: 20.02.2021

Güvenli Günler Bülteni <https://guvenligunler.com/wp-content/uploads/2017/05/GuvenliGunlerBulteni-Murat-Lostar-0216.pdf> Erişim Tarihi: 20.02.2021

Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması <https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-

Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679> Erişim Tarihi: 20.02.2021

İTÜ Bilgi İşlem Dair Başkanlığı, Virüs, Solucan ve Truva Atı <https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1>

Kaspersky, 2020, Bilgisayar Virüsleri ve Kötü Amaçlı Yazılımlarla İlgili Bilgiler ve SSS <https://www.kaspersky.com.tr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs> Erişim Tarihi: 20.02.2021

Siber Suç Sözleşmesi, <https://polis.osce.org/file/11326/download?token=1NGQndqh> Erişim Tarihi: 20.02.2021

Türk Dil Kurumu Sözlüğü <https://sozluk.gov.tr/ Erişim Tarihi: 20.02.2021

Türkiye İstatistik Kurumu, " Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması", 2020 <https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679> Erişim Tarihi: 20.02.2021