BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

TÜRK CEZA KANUNU KAPSAMINDA BİLİŞİM SUÇ VE CEZALARI İLE ÖRNEK YARGISAL KARARLARIN ANALİZİ VE MEVZUAT ÖNERİLERİ

Burak Cesur AKÖZ

Bilişim Uzmanlığı Tezi

Eylül 2018

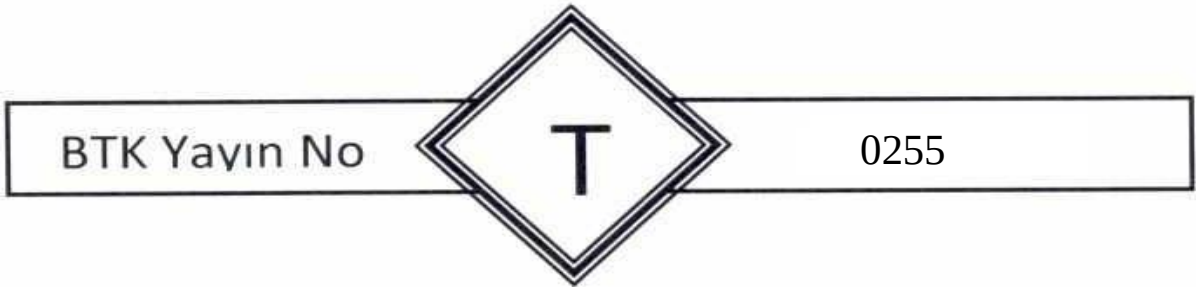
Ankara

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BTK
BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.



ISBN BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

TÜRK CEZA KANUNU KAPSAMINDA BİLİŞİM SUÇ VE CEZALARI İLE ÖRNEK YARGISAL KARARLARIN ANALİZİ VE MEVZUAT ÖNERİLERİ

Burak Cesur AKÖZ

Bilişim Uzmanlığı Tezi

Eylül 2018

Ankara

Burak Cesur AKÖZ tarafından hazırlanan "*TÜRK CEZA KANUNU KAPSAMINDA BİLİŞİM SUÇ VE CEZALARI İLE ÖRNEK YARGISAL KARARLARIN ANALİZİ VE MEVZUAT ÖNERİLERİ*" adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Meltem TURHAN
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : Kurul Üyesi, Hacı Adnan CENGİZ

Üye : Kurum Başkan Yardımcısı, Dr. Ahmet KILIÇ

Üye : Daire Başkanı, Bülent ARSAL

Üye : Müdür, Latif AYVA

Üye : Bilişim Uzmanı, Meltem TURHAN

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları ile Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri
Türü	Bilişim Uzmanlığı Tezi
Yazar	Burak Cesur AKÖZ
Teslim Tarihi	14 Eylül 2018
Anahtar Kelimeler	Bilişim Teknolojileri ve Ceza Hukuku İlişkisi, Bilişim Suçları, Bilişim Bağlantılı Suçlar, Siber Suçlar
Tez Danışmanı	Meltem TURHAN
Sayfa Adedi	vii+255

Günlük yaşamdan ticari işlere, şahsi kullanımdan kamusal hizmetlerden faydalanmaya kadar, bilişimin hayatımızın bel kemiği olduğu gerçeği yadsınamaz. Hızla artan internet kullanıcılarının kişisel ve mali verileri başta olmak üzere, önem atfettiği birçok değerin bilişim sistemleri üzerinde yer aldığı aşikârdır. Gerekli önlemler alınmasına rağmen her geçen gün kendini yeni teknolojilere uyarlayan kötü niyetli kişiler tarafından bilişim sistemlerine birçok farklı amaçla saldırı gerçekleştirilmesi mümkündür. Ancak söz konusu sistemlere bir gün değil bir dakika dahi ulaşılmaz olması veya önemli verilerin kaybı, telafisi mümkün olmayan zararlara yol açabilecektir. Bu tehlikelerin bertaraf edilebilmesi için uluslararası çalışmalar yakından izlenerek birçok adım atılmış, ülkemiz ceza yasasında da bilişim alanında suçlar başlığı altında suç ve cezalar düzenlenmiştir. Hayatın birçok alanında yer alması sebebiyle Türk Ceza Kanunu dışında örneğin; fikir ve sanat eserleri, elektronik imza, kişisel verilerin korunması gibi konuları düzenleyen yasalarda da bilişim alanında işlenebilecek suçlara ilişkin özel düzenlemeler yapılmıştır. Bu çalışmada esasen Türk Ceza Kanununda yer alan doğrudan bilişim suçları ile ceza kanunu ve diğer yasalarda düzenlenen dolaylı bilişim suçları; emsal yargı kararlarının analizi ile birlikte açıklanmaya çalışılmış, alınması gereken şahsi ve kurumsal önlemler ile mer'i mevzuatta yapılması gereken revizyonlardan bahsedilmiş ve bu alanda yapılması gerektiği değerlendirilen çalışmalar hakkında öneriler sunulmuştur.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY	
Thesis	IT Crimes within the Scope of Turkish Penal Code along with the Analysis of Precedents and Regulation Recommendations
Type	ICT Expert Thesis
Author	Burak Cesur AKÖZ
Submisson Date	14 September 2018
Key Words	Relation between IT Technologies and Criminal Law, IT Crimes, IT-Related Offences, Cybercrimes
Advisor	Meltem TURHAN
Total Page	vii+255

The fact that informatics (IT) are the backbone of our lives with respect to not only personal use but also for commercial activities and public services is undeniable. In this context, it is obvious that rapidly rising internet users' personal and financial data, and many other important information are stored via information systems. Despite necessary measures taken, it is possible to perform attacks on these systems for many different purposes by malicious persons who adapt themselves to new technologies day by day. Being inaccessible to aforementioned systems not only for a day but even for a minute or loss of critical data can cause irreparable damages. To eliminate this hazards, many steps have been taken, crimes and penalties were organized under the title of crimes in the field of informatics in the penal code of our country (TPC) by following international studies closely. Apart from penal code, specific regulations regarding cybercrimes has been made in different fields such as intellectual property, electronic signature, and personal data protection. This thesis tries to explain direct cybercrimes in the TPC, and indirect (IT-related) cybercrimes in the TPC and other regulations with analyzing judicial precedents. Furthermore, personal and institutional measures as well as revisions required in the legislation in force are discussed, and recommendations regarding what should be done in this field are presented.

TEŞEKKÜR

Tez çalışmam boyunca değerli yönlendirmeleriyle çalışmaya yön veren tez danışmanım Sayın Meltem TURHAN'a, birbirimize gerek iş yükü dağılımı, gerekse motivasyon konularında karşılıklı katkıda bulunduğumuz oda arkadaşım Sayın Cumali GÜRGÜN'e, çalışmayı takip edip katkılarda bulunan Sayın Mehmet ÖZCAN'a, bilgi ve tecrübesini çalışmayı daha iyi hale getirmek için paylaşan Sayın Bahadır Aziz SAKİN'e, şahsımı her konuda destekleyen ve bu süreçte desteklerini her daim hissettiğim Müdürümüz Sayın Latif AYVA'ya, Kurum Başkan Yardımcımız Sayın Aysel KANDEMİR'e ve Kurul Üyemiz Sayın Rıdvan KAHVECİ'ye, son olarak bu süreçte yardımlarını esirgemeyen tüm çalışma arkadaşlarım ile manevi desteklerinden dolayı eşim ve kızım başta olmak üzere tüm aileme teşekkürü bir borç bilirim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AB	Avrupa Birliği
AET	Avrupa Ekonomik Topluluğu
ABD	Amerika Birleşik Devletleri
AK	Avrupa Konseyi
	(İngilizce kısaltma CoE – Council of Europe olarak kullanılmıştır)
ASSS	Avrupa Konseyi Siber Suç Sözleşmesi
BKKK	5464 sayılı Banka Kartları ve Kredi Kartları Kanunu
bkz.	Bakınız
BM	Birleşmiş Milletler
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CD	Ceza Dairesi (Yargıtay ile birlikte kullanıldığında)
CMK	5271 sayılı Ceza Muhakemeleri Kanunu
CoE	Council of Europe (Avrupa Konseyi)
CPU	Central Process Unit (Merkezi İşlem Birimi)
dn.	Dipnot
EHK	5809 sayılı Elektronik Haberleşme Kanunu
ETCK	765 sayılı Eski (Mülga) Türk Ceza Kanunu
FSEK	5846 sayılı Fikir ve Sanat Eserleri Kanunu
IP	Internet Protocol (İnternet Protokolü)
ISS	İnternet Servis Sağlayıcı
İHEB	İnsan Hakları Evrensel Bildirgesi
KK	5326 sayılı Kabahatler Kanunu
KVKK	6698 sayılı Kişisel Verilerin Koruması Kanunu
LAN	Local Area Network (Geniş Alan Ağı)
m.	Madde
MK	4721 sayılı Türk Medeni Kanunu
MPLS	Multi Protocol Label Switching (Çok Protokollü Etiket Anahtarlama)

M2M	Machine to Machine (Makineden Makineye Haberleşme)
OECD	İktisadi Kalkınma ve İşbirliği Örgütü
ODTÜ	Orta Doğu Teknik Üniversitesi
s.	Sayfa
SOME	Siber Olaylara Müdahale Ekipleri
TCK	5237 sayılı Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TİB	Telekomünikasyon İletişim Başkanlığı
TMK	3713 sayılı Terörle Mücadele Kanunu
TÜBİTAK	Türkiye Bilim ve Teknik Araştırma Kurumu
ULAKBİM	Ulusal Akademik Ağ ve Bilgi Merkezi
URL	Uniform Resource Locator (Değişmeyen Kaynak Konumlayıcı)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
vb.	Ve benzeri
vd.	Ve devamı
WAN	Wide Area Network (Geniş Ağ Bağlantısı)
YCGK	Yargıtay Ceza Genel Kurulu
YHGK	Yargıtay Hukuk Genel Kurulu

GİRİŞ

Bilgi ve iletişim teknolojileri her geçen gün büyük bir hızla gelişmektedir. Bu gelişmeler zamanın etkin kullanımını sağlayarak hayatı birçok alanda kolaylaştırmaktadır. Yaşadığımız dönem adeta bir bilişim çağı olup, bu çağda hiçbir şey durağan kalmamaktadır. Nitekim teknolojinin baş döndürücü gelişimi sonucunda bir gün önce hayatımızda çok önemli yere sahip olan bir cihaz veya yazılım bir başka gün eskiyebilmekte ve ihtiyaçlara ayak uyduramaz duruma gelebilmektedir.

Bilgi ve iletişim teknolojileri ile üretilen cihazlar, geniş ağlar sayesinde kişilerin de birbirleriyle temas halinde olmalarını sağlamıştır. Sadece kişiler değil, cihazlar da kendi aralarında etkileşimde bulunmakta ve makineden makineye iletişim gibi kavramlar bilişim terminolojisine dâhil olmaktadır. Daha önce bu alanda sadece bilgisayarlardan söz edilirken; akıllı telefonlar, avuç içi cihazlar, saat ve kulaklıklar gibi giyilebilir ekipmanlar ve sayılamayan birçok cihaz bilişim sistemleri üzerinde işlem yapabilmektedir.

Anılan cihazlar ile şahısları etkileşim halinde bulunduran ve verilere çok hızlı erişimi sağlayan internet, cihazların dış dünyaya açılmasıyla kullanıcıların hayatını doğrudan etkilemeye başlamıştır. Ancak bu mecra kötü niyetli kişilerce olumsuz yönde de kullanılabilmektedir. Bilişim sistemleri üzerinde, gerçek dünyada işlenen suçlara kıyasla hem daha hızlı hem de daha kolay şekilde suç işlenebilmektedir. Bu durum, ülkemizle birlikte tüm dünyada bilişim suçlarında artışa sebebiyet vermektedir.

Bilişim suçları, teknolojik gelişmelere paralel olarak çok sayıda farklı yöntemle işlenebilmekte ve bu suçların sanal ortamda gerçekleşmelerinden ötürü tespitleri kolay olmamaktadır. Toplumu bu tehlikelerden korumak, bu suçlarla yasal yollardan mücadele edilmesini gerektirmektedir. Bilgi ve iletişim teknolojilerinin gelişimi, dinamik yapısı gereği hukuk kurallarından daha hızlı gerçekleştiğinden, bu alandaki boşlukları doldurmak da kolay olmamaktadır.

Ülkemizde bilgisayar ve özellikle internet kullanıcı sayısının artmasıyla ceza kanunumuzda da konuya özel düzenlemeler yapılmış ve bu düzenlemelerde uluslararası çalışmaların esas alınmasına çaba gösterilmiştir.

Çalışmamızın birinci bölümünde; bilişim alanına ilişkin temel kavramlar ile bilişim suçlarına ilişkin genel bilgilere yer verilmiştir. Bilişim ile suçun kesiştiği alan açıklanarak, bilişim suçları tanımlanmış ve bu suçların sınıflandırılmasına değinilmiştir. Yine bu bölümde, teknolojik gelişmelerle doğru orantılı olarak evrilen bilişim suçlarının işlenme yöntemlerinden (*modus operandi*) bahsedilmiş ve faillerin bu suçları işleme amaçları tartışılarak, bunun karşısında mağdurların yaklaşımı incelenmiştir.

Bu tür suçların genellikle ülke coğrafi sınırlarını aşması sebebiyle, çalışmanın ikinci bölümünde; bilişim suçlarının uluslararası boyutu ve ülkemiz düzenlemelerine yansımasından bahsedilmiştir. Uluslararası düzenlemeye duyulan ihtiyaçlardan bahsedilerek, bu alanda gerek taraf devletlerin sayısının yüksek olması, gerekse suçla mücadelede geniş ve etkin hükümler içermesi sebepleriyle en kapsayıcı uluslararası sözleşme niteliğini taşıyan ve ülkemiz tarafından da 2014 yılından itibaren iç hukukumuzun bir parçası haline getirilmiş olan Avrupa Konseyi Siber Suç Sözleşmesi (*Convention on Cybercrime*) incelenmiş, ayrıca sözleşmenin ceza hukukumuza etkilerinden de söz edilmiştir. Bölümün sonunda, 765 sayılı mülga Ceza Kanunu'nun ilgili hükümleri, 5237 sayılı Türk Ceza Kanunu'nda yer alan suç tipleri ile mukayeseli olarak incelenmiştir.

Üçüncü bölümde; çalışmamızın asıl başlığını oluşturan, 5237 sayılı TCK'da yer alan doğrudan bilişim suçlarına detaylı şekilde yer verilmiştir. Bu kapsamda, Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" başlığı altındaki tüm suç tipleri; korunan hukuki yarar, suçun maddi ve manevi unsurları, nitelikli halleri, yetkili merci ve yaptırımları, özellikle Yargıtay içtihatları ve diğer emsal yargı kararları analiz edilerek açıklanmaya çalışılmıştır. Ayrıca bilgi teknolojilerinde yakın zamanda öne çıkan dijital oyun sektörünün suçla ilgisi incelenmiş, bölüm sonunda da güncel istatistiki veriler ışığında tespitlerde bulunulmuştur.

Dördüncü bölümde, dolaylı bilişim suçlarına yer verilmiştir. Bilişim suçları her zaman doğrudan bilgi ve iletişim teknolojileri kullanılarak veya bu teknolojiyi barındıran somut bir cihaza karşı işlenmemektedir. Klasik bir suçta bu teknolojinin endirekt kullanımı veya bu teknolojiyi haiz cihazların suçta sadece araç olarak kullanılması suretiyle bilişim suçları "dolaylı" olarak da icra edilebilmektedir. Bilişim aracılığıyla işlenebilen 'diğer' suçların karşılığı olarak özetlenebilen dolaylı bilişim suçları, hem Türk Ceza Kanunu hem de ilgili alandaki diğer yasal düzenlemelerde bulunabilmektedir. Bu çerçevede, bilişim sistemine yetkisiz erişim doğrudan bir bilişim suçu iken, bilişim suretiyle dolandırıcılık veya fikri mülkiyet haklarının internet üzerinden ihlal edilmesi hususları dolaylı bilişim suçlarına örnek teşkil etmektedir. Doğrudan bilişim suçlarında bilişim sistemine dâhil olan bir eylem şart olduğu halde, dolaylı bilişim suçları sanal dünya dışında da işlenebilen klasik/geleneksel suçları işaret etmektedir. Dördüncü bölümde; dolaylı bilişim suçlarının önemli olduğu değerlendirilen örneklerine değinilmiş, ceza yasamız dışında ilgili diğer kanuni düzenlemelerde ne tür yaklaşımın öngörüldüğü açıklanmaya çalışılmıştır. Bu bölümde ayrıca dolaylı bilişim suçu olarak işlenebilecek olan siber zorbalık (*cyberbullying*) suçuna özel olarak yer verilmiş olup, küresel bir tehlike olan bu olgu açıklanarak ülkemizdeki etkisi incelenmiştir.

Beşinci ve son bölümde; mukayeseli hukukta bilişim suçları araştırılmış ve farklı coğrafyalara sahip değişik hukuk sistemlerini benimseyen ülkelerin bilişim suçlarına yaklaşımı incelenmiştir. Her ülke uluslararası standartların altında kalmadan kendi özel durumuna göre bu tür suçlarla mücadelede farklı yaklaşımlar benimseyebilmektedir. Bu kısımda ülke uygulamaları tetkik edilirken, ülkemiz düzenlemeleri ile karşılaştırma yoluna da gidilmiştir.

Sonuç bölümünde ise, kullanıcılar için bireysel olarak, ilgili kurumlar açısından da kurumsal olarak alınması gereken önlemler ile bunlara ilişkin öneriler aktarılmıştır. Ayrıca, ilgili yasal düzenlemelerde revizyona gidilmesi gerektiği değerlendirilen hususlar, gerekçeleriyle birlikte sunulmuştur.

1 BİLİŞİM ALANI ve BİLİŞİM SUÇLARINA İLİŞKİN GENEL BİLGİLER

Bilişim ile ceza hukukunun kesişim alanında bulunan unsurların çalışmanın asıl konusunu oluşturması sebebiyle, konu hakkındaki bazı önemli terimler bu bölümde açıklanmaya çalışılacak, bu temel kavramlar daha sonraki bölümlerde işlenecek olan konuların izahına da dayanak teşkil edecektir.

1.1 Bilişim ve Bilişime Ait Genel Kavramlar

Beşeri hayatta kişilerin maddi ve manevi varlığına dâhil olarak kabul edilebilecek ve artık dünyada ülkelerin fiziki/askeri gücünden daha öte bir değer taşıdığının kabul edilebileceği '*bilgi*'nin; oluşturulması, işlenmesi, muhafazası ve aktarımının insanlık için büyük önem arz ettiği aşikârdır.

Her geçen gün gelişen ve değişen teknoloji ile bugünün dünden ileri olduğu gerçeği karşısında, bilginin toplumu da etkileyen hatta şekillendiren bir değer olduğu yadsınamaz bir gerçektir. Bilgi ve teknoloji çağının yaşandığı şu dönemde bilginin en önemli güç olduğu genel kabul görmektedir. Ardı ardına yaşanan gelişmeler dikkate alındığında, bu denli güçlü bir değerin ekonomik, sosyo-kültürel ve hukuki yaşamı da etkilemesi kaçınılmazdır.

Bilişim; insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi olarak tanımlanmakta ve kavramın disiplinler arası bir özellik taşıdığı, bilgisayar da içinde olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları kapsadığı ifade edilmektedir (Türk Dil Kurumu-TDK, 2018a).

Bilişim[1] ile bilgisayarın sıkça birbirleri yerine kullanıldığı görülmekte ise de özünde bir makine olan bilgisayara nazaran, bilişim kelimesinin daha üst bir kavramı ifade ettiği kabul edilmektedir (Özen ve Baştürk, 2011, s.11). Zira bilgilerin oluşturulmasından, değiştirilmesine; muhafazasından, paylaşım ve gönderimine kadar olan süreçte, bilgisayarlardan ve/veya benzer diğer elektronik ortamlardan istifade edilmekte ve bu sürecin bütününü de 'bilişim' oluşturmaktadır.

1.1.1 Bilgisayar

Bilindiği üzere buharlı motor 'sanayi devrimi' diye adlandırılan bir dönemi başlatmış ve tarım toplumunun sanayi toplumuna dönüşmesine neden olmuştur. Bilgisayar da günümüzde 'bilişim devrimi' diye tanımlanan yeni bir dönemi/çağı başlatarak sanayi toplumunun bir bilgi toplumuna dönüşmesine yol açmıştır (Sarıaslan, 2012, s.145).

Günümüzde gerek kişisel alanda gerek iş hayatında profesyonel olarak ve daha sayılamayacak birçok sahada kullanımına rastlanan bilgisayarın, kesin ve tek bir tanımı bulunmamaktadır.

Gerçekten günümüz teknolojisinde özellikleri gereği bir işlemciye sahip olan ve bir ağa bağlanarak işlem yapan mobil telefonlar, alarm sistemleri, GPS ve çağrı cihazları vb. gibi birçok araç bulunmaktadır. Bilgisayarı bu gibi cihazlardan ayıran özellik, bilgisayarın bilişim (enformatik) özelliğine sahip olması yani 'genel amaçlı' kullanılabilme yeteneğidir (Özen ve Baştürk, 2011, s.10).

'Bilgisayar' sözcüğü, yabancı dilden çeviri örneklerinde Türkçeleştirme açısından oldukça başarılı bir kelime olup TDK sözlüğünde: *"çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bu işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin"* olarak ifade edilmektedir (TDK, 2018b).

[1] Fransızca "informatique" kelimesinin dilimize 'enformasyon' ve 'otomatik' kelimelerinin birleşiminden oluşan "enformasyon" adıyla geçtiği; aynı anlamı taşıyan ve yaygın olarak kullanılan "bilişim" kelimesinin de 'bilgi' ve 'iletişim' kelimelerinden türeyerek geldiği bilinmektedir.

Bilişim alanında ülkemizin de tarafı bulunduğu "Avrupa Konseyi Siber Suç Sözleşmesi"nin (ASSS) 1/a maddesinde *'bilgisayar sistemi'* tanımına yer verilerek; *"dijital verilerin otomatik olarak işlenmesi için geliştirilmiş donanım ve yazılımdan oluşan bir cihaz"* şeklinde tarif edilmiştir.

Süratle değişen ve gelişen teknoloji yanında bilgisayarın yerine getirdiği işlevlerin tümünü kapsayan bir tanımın yapılması oldukça güçtür. Sayılan sebeplerle bilgisayarın; bilgi (veri/data) alabilen, muhafaza edebilen, işleyebilen ve gönderimini sağlayabilen cihaz olarak kabulü mümkündür.

Bilgisayara ilişkin tanım yapmanın zorluğu ise, bilgisayarı oluşturan unsurların belirlenmesini gerektirmiştir. Bilgisayarı oluşturan temel unsurlar (günümüz itibarıyla); donanım [*hardware*] ve yazılımdır [*software*] (Erdoğan, 2012, s.24).

Bilgisayarın belirtilen özelikleri, bilgisayar benzeri cihazlarda örneğin; akıllı (gelişmiş) cep telefonları veya şahsi dijital ajandalarda da görülebilmektedir (Akarslan, 2015, s.31). Dolayısıyla bu çalışmada sadece bilgisayar temel alınmayacak; bilgisayar benzeri aygıtların da gerek toplumumuz gerekse dünyada oldukça fazla sayıda kullanıcı tarafından yaygın olarak kullanıldığı gözetilerek, bu cihazların dijital verilerin otomatik olarak işlenmesi için geliştirilmiş donanım ve yazılımı da haiz olmaları sebebiyle bu minvalde açıklamalarda bulunulacaktır.

1.1.2 İnternet

Bilgisayarın mevcudiyeti ve verilerin işlenmesinin yanında bilgisayar veya benzeri türdeki cihazların birbirleri ile bağlantılarının olması da önem taşımaktadır. Teknolojik gelişmeleri tetikleyen en önemli hadiselerden birinin de dünya çapındaki küçüklü büyüklü bilgisayar ağlarının kurulması ve varlığı değil, bütün bilgisayar ağlarını kapsayan genel bir ağ olan 'İnternet'in tesis edilmesi olduğu değerlendirilmektedir (Ergün, 2008, s.7).

İngilizce Inter[national] ve Net[work] kelimelerinden türetilen bu soyut kavram, esasen bir ortam olarak nitelendirilebilecek olup ulusal mevzuatımızda[2] da *"Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortam"* şeklinde tanımlanmaktadır.

İnternet ortamı üzerinde bilgisayar ve benzeri işlev gören cihazların birbirlerine bağlanması için belli bir adrese sahip olmaları şarttır. Bu bağlamda ağa bağlı cihazların aralarındaki iletişimi sağlayabilmesi adına bir 'IP adresi'ne (İnternet Protokolü-Internet Protocol) sahip olması gerekmektedir. IP adresi mevzuatımızda[3]; *"Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adres"* tarifi ile hükme bağlanmıştır.

Esasen askeri bir ihtiyaç olarak ortaya çıkan internetin anavatanının Amerika Birleşik Devletleri (ABD) olduğu bilinmektedir (Kurt, 2005, s.42). İnternetin ortaya çıkışı Amerika Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan Savunma İleri Düzey Araştırma Projeleri Kurumu'na (DARPA-*Defence Advanced Research Project Agency*) dayanmaktadır. 1969 yılında Amerikan Savunma Bakanlığı bilgisayar bilimlerini ve çeşitli askeri araştırma projelerini desteklemek için ARPANET (*Advanced Research Project Agency Network*-Gelişmiş Araştırma Projeleri Dairesi Ağı) adında Paket Anahtarlamalı Ağı oluşturmaya başlamış ve bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayarlarını da içererek büyümüştür (Orta Doğu Teknik Üniversitesi [ODTÜ], 2005).

İnternetin mimarlarının şu an olduğu gibi onu açık bir ağ olarak tasarlamadıkları; aksine askeri bir proje olarak geliştirdikleri ve belirli noktalarda hala onu geliştiren ABD'nin güvenlik stratejisinin bir parçası olmaya devam ettiği ifade edilmektedir (Kaya, 2010, s.7).

---

[2] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik m.3/1-(i)

[3] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik m.3/1-(h)

Ülkemizde ise ilk defa 12 Nisan 1993 tarihinde[4], Türkiye Bilim ve Teknik Araştırma Kurumu (TÜBİTAK) tarafından desteklenen bir projeye bağlı olarak ODTÜ'de gerçekleştirilen bağlantının temel amacı, akademik çevrede bilimsel veri iletişimini kullanmak olmuştur.

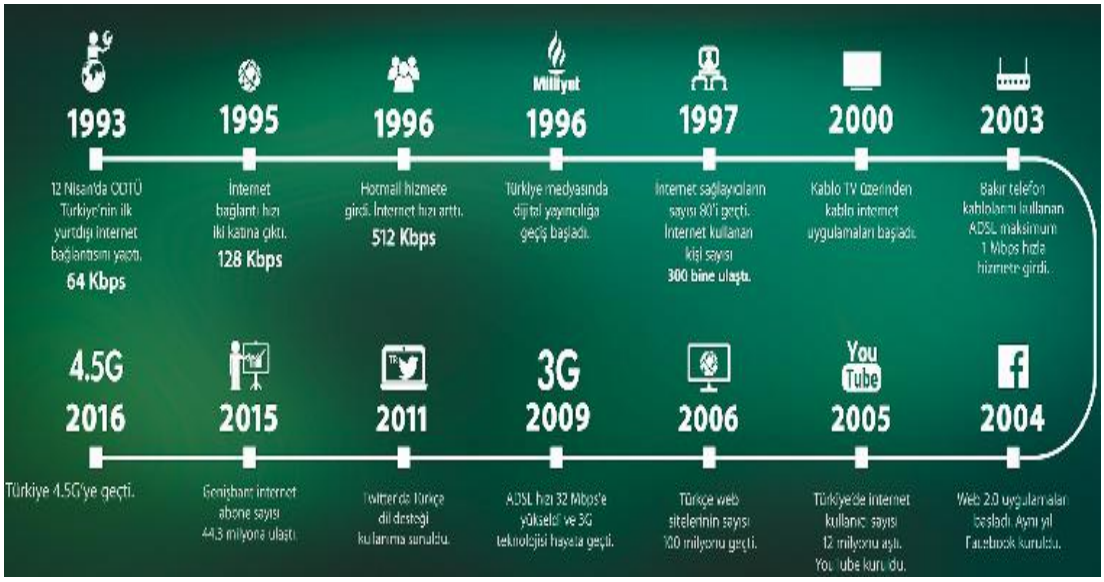
1996 yılında Türk Telekom'un TURNET, TÜBİTAK'ın da Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) çalışmaları çerçevesinde çeşitli ilerlemeler kaydedilmiştir. ULAKBİM'in[5] temel görevlerinden biri; en yeni teknolojileri kullanarak Türkiye çapında tüm eğitim ve araştırma kuruluşlarını birbirine bağlayacak olan Ulusal Akademik Ağ (ULAKNET) adıyla hızlı bir iletişim ağı kurmak ve bu ağ aracılığı ile bilgi hizmetleri vermektir. 1998 tarihinde TURNET projesinin büyüme ihtiyacından ötürü TTNET internet omurgası kurulmuş, 2000 yılında da mevcut omurgada yapılan değişiklikler ile iyileştirmeler sağlanmıştır. 2005'te Türk Telekom'un kurduğu IP/MPLS altyapısı ile IP omurgası kapasitesi arttırılmıştır (Bilgi Teknolojileri ve İletişim Kurumu [BTK], 2007, s.75).

2009 yılında 3G, 2015 yılında ise 4,5G teknolojisine geçen ve bugünlerde 5G için çizilen hedefler doğrultusunda emin adımlarla yürüyen ülkemizde 25 inci yılını tamamlayan internet, dünyada olduğu gibi ülkemizde de birçok evreden geçmiştir. Bu çerçevede; ülkemizde internetin tarihçesi ve gelişimi aşağıdaki şekilden de izlenebilmektedir (BTK-BilgiZone, 2018a).

[4] 64 Kbps kapasiteli kiralık hat ile ODTÜ Bilgi İşlem Daire Başkanlığı sistem salonundaki yönlendiriciler kullanılarak, ABD'de NSFNet'e (*National Science Foundation Network*) TCP/IP protokolü üzerinden Türkiye'nin ilk Internet bağlantısı gerçekleştirilmiştir.
(http://www.internetarsivi.metu.edu.tr/tarihce.php) [Erişim Tarihi 07.03.2018]

[5] *www.ulakbim.gov.tr* adresinden ulaşılabilmektedir.

Şekil 1.1 Türkiye'de İnternetin Tarihçesi ve Gelişimi



Böylesine devrimsel nitelikte bir olgu olan internetin; insanlığa ve kalkınmaya büyük faydası olduğu gerçeğinin yanında serbestçe dolaşılan, sınırları olmayan ve kişilerin gerçek kimlikleri dışında hareket edebilmelerine olanak sağlayan bir alan olmasından ötürü, birçok sakınca ve riskleri de ihtiva ettiği yadsınamaz bir gerçektir. Faydalı yönleriyle ele alındığında insanlığa büyük katkı sağlayabilecek bu teknolojik gelişmenin, kötü niyetli kişiler elinde de bir silaha dönüştürülebilmesi de pekâlâ mümkündür.

İnternetin sağladığı fırsat ve faydalar ana başlıklar altında şu şekilde sıralanabilir (BTK, 2016a):

- Güncel haber ve bilgiye erişim
- Görüş ve bilgi paylaşımı
- Zaman ve mekândan bağımsız, eşzamanlı ve eşzamansız iletişim
- Ekonomik ve hızlı haberleşme olanağı
- Görsel ve işitsel öğelerle iletişim kalitesini arttırma

Bunların yanında küresel dünyadaki teknolojik gelişmelere paralel olarak muasır medeniyet seviyesine ulaşılmasında da internetin önemli bir yeri olduğunu kabul etmek gerekmektedir.

İnternetin sebep olabileceği tehlike, risk ve zararlar ise aşağıdaki gibi özetlenebilir (BTK, 2016b):

- Yanlış ve/veya zararlı bilgiye erişim;
- Siber zorbalık,
- Sanal dolandırıcılık,
- Kişisel bilgilerin paylaşımı ve kimlik hırsızlığı (*Identity Theft*),
- Zararlı yazılımlar,
- Oltalama (*Phishing*),
- Pornografi /Çocuk istismarı/ Fuhuş
- Yasadışı kumar
- İnternet bağımlılığı ve diğer sağlık sorunları (internet üzerinde aşırı zaman geçirmeye bağlı olarak görülebilecek fiziki rahatsızlıklar)
- Yabancılarla çevrimiçi ve çevrimdışı iletişim
- Şiddet/Nefret/Irkçılık faaliyetleri
- Yasadışı silah ticareti ve sağlığa zararlı madde kullanımı
- Telif hakları ihlali

Sayılanların yanında, bilişim suçlarına maruz kalma hususunun da internet kullanımının risk ve zararlarına eklenebilmesi mümkündür.

Ülkemizde 2008 yılında 6 milyon civarında olan genişbant internet abone sayısı, 2017 yılı sonu itibarıyla 69 milyona yaklaşmıştır (BTK, 2018a, s.17). Yaklaşık 10 yıllık bir zaman aralığında internet kullanıcılarının sayısı takribi %1150 gibi oldukça yüksek bir oranda tırmanarak 70 milyon bandına dayanmıştır. Aşağıdaki grafikten de görüleceği üzere anılan abonelerin; 11,9 milyonu sabit abone iken, mobil abone sayısı 56,9 milyon olarak gerçekleşmiştir (BTK, 2018a, s.10 ve s.51).

2018 yılı sonlarında bu yükselen trendin devam etmesi halinde ülkemiz nüfusunu geçen sayıda internet kullanıcısına ulaşılacağı öngörülmekte olup, bu durum aynı zamanda bilişim suçlarına maruz kalabilecek aday sayısının da oldukça fazla olacağını ortaya koymaktadır.

Şekil 1.2 Yıllara Göre Genişbant & Mobil İnternet Abone Sayıları

Kullanıcı sayısı her geçen gün artan internetin dinamik yapısı sebebiyle, üzerinde gerçekleştirilen işlem sayısının baş döndürücü olduğu bilinmektedir. Artık haberleşme, iletişim, bilgi paylaşımı hatta gündelik işlerden ticari işlere, yerel hususlardan uluslararası meselelere kadar klasik yaklaşımdan uzaklaşılıp, bunların yerini tamamen internet teknolojisinin aldığını söylemek yanlış olmayacaktır.

Nitekim bankacılık işlemlerini gerçekleştirmek, sosyal medyada aile üyeleri ve arkadaşlarla iletişim halinde olmak, mağazaların internet sitesi üzerinden elektronik yolla alışveriş yapmak, resmi geçerliliği bulunan belgelere erişim ve ilgili kamu kurumlarının verdiği hizmetlerden yararlanmak adına belirli portalların kullanılması, hemen her gün kişiler tarafından sıkça tercih edilen ve bilişim ağlarının içerisinde yer alınan durumlardan sadece birkaçıdır.

Aşağıdaki şekilden de görülebileceği üzere; sadece altmış saniyelik kısa bir zaman diliminde yazılı bir mektubun, posta yoluyla gönderiminin sağlanması imkân dâhilinde bile değilken, dijital dünyada bu süre zarfında 156 milyon gibi oldukça büyük sayıda elektronik postanın gönderildiği görülmektedir. Yine aynı süre içerisinde internet üzerinde bulunan arama motorlarından 3.8 milyon bilgi araması yapıldığı gibi, konuşma uygulamalarından biri vasıtasıyla 2 milyon dakika arama gerçekleştirilmektedir.

Şekil 1.3 Dijital Dünyada 60 Saniyede Gerçekleşen İşlem Sayıları

(BTK-BilgiZone, 2018b)

1.1.3 Bilişim sistemi

Bilgisayar ve internet kavramlarının açıklanmasından sonra bilgisayar ve benzeri cihazların çalışma prensipleri ve birbirleri ile iletişimlerinin sağlanması bağlamında içinde bulundukları sistemin açıklanması gerekmektedir.

Bilişim sistemi; bilgisayar, çevre birimleri, iletişim altyapısı ve yazılımlardan oluşan veri işleme, saklama, iletmeye yönelik bir sistemdir (Gül, 2016, s.25).

Adalet Bakanlığı tarafından 2011 yılında çıkarılan Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik'in *"Tanımlar ve kısaltmalar"* kenar başlıklı 3 üncü maddesinin birinci fıkrasının (b) bendinde bilişim sistemi; "*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi"* olarak tanımlanmıştır.

Bilişim sitemlerinde hareket noktası "bilgisayar" gibi görünse de bilgisayar tanımını birebir karşılamayan birçok başka araç ve gereç de bu sistem içerisinde kullanılmaktadır. Nitekim yukarıdaki Yönetmelikte yer alan tanımda dahi bilişim sisteminin bilgisayardan ibaret görülmesi haklı olarak eleştirilmiş ve hatalı bulunmuştur (Erdoğan, 2012, s.16).

Bununla birlikte Yargıtay 18.03.2015 tarihli bir kararında (8. CD, E.2014/30037, K.2015/14023) cep telefonunun bilişim sistemi kapsamında bulunmadığı savıyla beraat kararı veren yerel ceza mahkemesinin kararını bozarak, cep telefonlarının da bilişim sistemine dâhil olduğunu açık şekilde ve etkili bir gerekçeyle ifade etmiştir:

"...Bilgisayarın çalışmasını düzenleyen tüm programlara işletim sistemi denilmekte olup ***işletim sistemlerinin sadece bilgisayarlarda değil cep telefonlarında, tablet PC'lerde de kullanılması mümkündür****. İşletim sistemleri Windows 8, Android, Linux gibi isimler almaktadır.*

...Donanımla yazılım arasındaki bağlantıyı sağlayan işletim sistemi çalışmadığı takdirde bilgisayarın kullanılması, program yüklenmesi olanaksızdır.

...Somut olayda; katılanın cep telefonundan çekilmediği halde sanığın; "Sen Hacer'i değil, parayı seviyorsun...., kızım seninle görüşmez, bırak kızımın peşini, dolanma peşinde, seni uyarıyorum, Hacer'in seninle işi olmaz, bir daha bir araya gelmeniz ben hayattayken imkansız" şeklindeki mesajı oluşturduğu ve telefonuna geldiği iddiasıyla boşanma dava dosyasında delil olarak ibraz ettiğinden bahisle açılan davada, sanık

suçlamayı kabul etmemiş, bilirkişi raporunda ise iletişim detaylarında suça konu mesajlaşmaya dair kayıt bulunmadığı, ancak cep telefonlarına özel yazılımlar yüklenerek veya internet vasıtasıyla mesaj oluşturulabileceği belirtilerek mesaj çekilen ve mesaj alan cep telefonlarının incelenip, iletişim kayıtlarıyla karşılaştırılması gerektiğinin bildirilmesi karşısında, ***cep telefonlarında mobil işletim sistemleri bulunduğu ve program yüklenebilmesinin mümkün olduğu gözetilerek****, taraflara ait cep telefonları alınıp uzman bilirkişi tarafından incelenip, iletişim kayıtlarıyla karşılaştırılmak suretiyle program yükleme veya internetten gönderme şeklinde suça konu mesaj gönderilip gönderilmediğinin araştırılması, sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken,* ***cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, yasaya aykırı, katılanın temyiz itirazları bu itibarla yerinde görülmüş olduğundan*** *hükmün bu sebepten dolayı 5320 sayılı Yasanın 8/1 inci maddesi uyarınca uygulanması gereken 1412 sayılı CMUK.nun 321 inci maddesi gereğince (bozulmasına), 18.03.2015 tarihinde oybirliğiyle karar verildi"* (Corpus, 2018).

Yukarıdaki karardan da görüleceği üzere, sadece bilgisayarlar değil; günümüzde taşınabilir (mobil) olmaları amacıyla boyutları küçülen ancak işlevsel olarak büyüyen ve bilgisayarlar kadar yetkin işlem kapasitesine sahip akıllı telefonlar, tablet/cep bilgisayarları, araç bilgisayarları, makineden makineye iletişim (Machine to Machine-M2M) sistemlerinde yer alan cihazların işlemcileri de bu kapsamda bilişim sistemi sayılabilecektir.

Bu nedenle bilgisayar olarak nitelendirilmemesine rağmen veri-iletişimi sağladığı için bilişim alanına dâhil unsurlardan sayılması gereken diğer elektronik, manyetik, mekanik araçlar (örneğin. WAP uyumlu, girilen verileri saklayabilen, işleyebilen, aktarabilen cep telefonları ile üzerindeki WEB paneli sayesinde ağa bağlanıp veri aktarımı yapabilen elektronik ev aletleri) veyahut bunları veri iletişim için birbirine bağlayan soyut veya somut ağlar üzerinde bilişim suçlarının işlenebileceği doktrinde kabul edilmektedir (Artuk vd., 2014, s.126). Örneğin internet üzerinden erişilebilen

bir mikro dalga fırın, kolaylıkla bir ev kundaklama aracı haline gelebilmekte ve suçta kullanılan bu alet olarak adli sürece dâhil olabilmektedir (Tanrıkulu, 2014, s.14)

5237 sayılı Türk Ceza Kanununun (TCK) gerekçesinde de, bilişim sistemi ile kastedilen husus açık bir biçimde ortaya konulmuş; *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma imkânı veren manyetik sistemlerdir"* denilmiştir (Adalet Bakanlığı, 2005).

Sonuç olarak, bilişim sisteminin genel olarak bilgisayardan daha geniş bir anlama sahip olduğu, bununla birlikte otomatik yani insan müdahalesi olmadan işlem yapabilmesi ve veri işleyebilmesinin gerektiği vurgulanmakta; ancak gerekçede yer alan sistemin manyetik olması ise eleştirilerek bunun sistemin zorunlu bir unsuru olarak kabul edilmemesi gerektiği belirtilmektedir (Ketizmen, 2008, s.19). Yine bilişim sistemlerinin en önemli aracı olan bilgisayarın bile tamamının manyetik yapı taşımadığı, ileride manyetik olmayan pek çok bilişim cihazının üretilebileceğinden bahisle kanun koyucunun gerekçeyi yazarken özensiz davrandığı görüşü de mevcuttur (Erdoğan, 2012, s.11).

Eleştirilerin tarafımızca da yerinde olduğu değerlendirilmekte olup; manyetik olmayan fakat bilişim sistemi içerisinde yer alan diğer işlemleri yapabilen bir sistemin ve/veya cihazın kapsam dışında bırakılmasının içerik bakımından sınırlama yaratabileceği düşünülmektedir.

1.1.4 Bulut bilişim

İnternet olgusu geliştikçe birçok farklı alanda da kullanım varyasyonlarına yol açmaktadır. Bu kullanım alanlarından en önemlilerinden biri de birçok veriyi içinde barındırabilen "Bulut Bilişim" sistemleridir. Bu sistemde, kişiler ev ya da iş bilgisayarlarında veri depolamak yerine, bunları bir internet sunucusuna kaydederek uzaktan erişim ile işlem yapma imkânına sahip olmaktadır.

Kavram üzerinde birçok tanım yapılsa da en yaygın şekilde benimsenen ve literatürde sıklıkla atıfta bulunulan tanım ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yapılmış olup aşağıdaki gibidir (Ebem, 2013, s.5):

"Bulut bilişim, düşük yönetim çabası veya hizmet sağlayıcı etkileşimi ile hızlı alınıp bırakılabilen ayarlanabilir bilişim kaynaklarının (örneğin; ağlar, sunucular, depolama, uygulama ve hizmetler) paylaşılır havuzuna istendiğinde ve uygun bir şekilde ağ erişimi sağlayan bir modeldir."

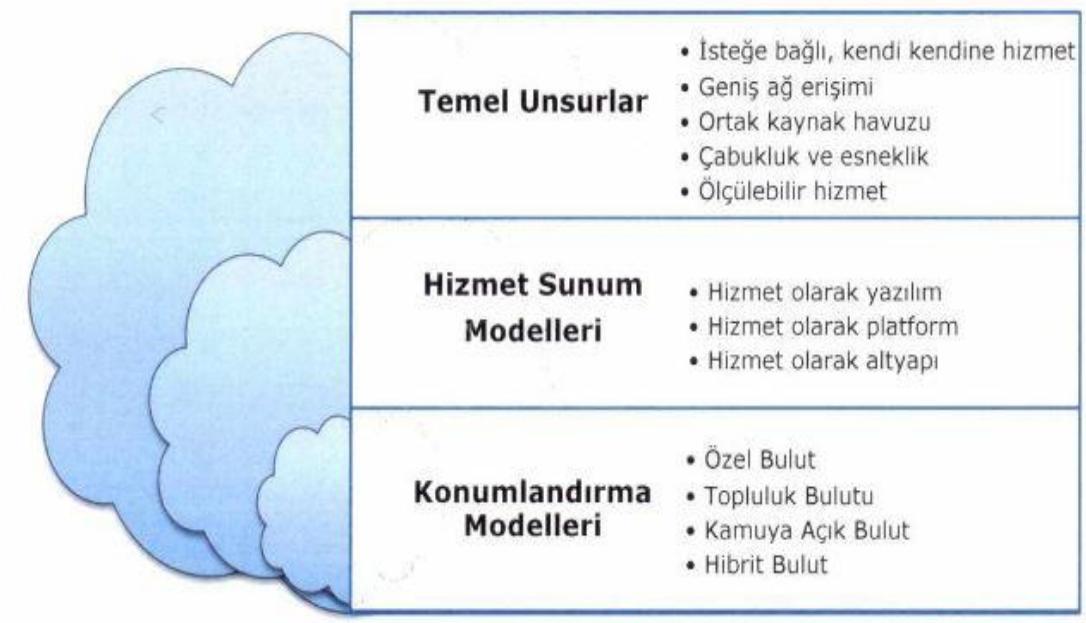
Artan geniş bant hızları, her geçen gün daha yüksek miktarlarda veri taşınmasına imkân verirken bu iletişim altyapısını kullanan bulut bilişim ortaya koyduğu avantajlar ile işletmelere daha geniş bir alanda dış kaynak kullanımı sağlamaktadır (Kaya, 2016, s.11).

Bulut bilişim, kullanıcılarına masraf ve zaman bakımından büyük avantaj sağlamakta ancak; bunun yanında sunucuların çalışamaz hale gelmesi veya kişisel-gizli verilerin topluca tutulduğu bir mecra olarak bilişim suçu faillerine oldukça çekici gelmesi gibi riskleri barındırmaktadır ki bunlardan birinin gerçekleşmesi halinde kullanıcının veriye ulaşması ve/veya yürütmekle yükümlü olduğu bir işi yapamaması söz konusu olabilecektir (BM, 2013, s.282).

Bilişim teknolojileri sektöründe önemli bir araç olan bulut bilişim hizmeti, akıllı cep telefonlarının işletim sistemlerinde de yer almaya başlamıştır. Örneğin; sektörde büyük bir yere sahip olan Apple şirketinin *iCloud* hizmeti bunlardan biridir. Söz konusu firma; 2017 yılında 30 milyar dolar gelir elde etmişken, bunun 4 milyar dolarını bulut bilişim hizmetini verdiği iCloud ürünü üzerinden kazanmış, 2020 yılında firmanın aynı hizmetten elde edebileceği gelir ise 6 milyar dolar olarak öngörülmüştür (Statista, 2018a).

Bilgisayar ağları, depolama ortamları sunucular vb. gibi çok sayıda bilişim ortamlarında işlerlik kazanan, esnek bir model olan bulut bilişimin çeşitli özellikleri, hizmet ve kurulum modelleri bulunmaktadır (Turan, 2016, s.225).

Şekil 1.4 NIST Tanımı Çerçevesinde Bulut Bilişim



1.2 Bilişim Suçları

Bilişim ve bilişim sistemlerinin açıklanmasından sonra çalışma konusu olan bilişim suçları müessesesinin açıklanabilmesi için suç tanımının ortaya konarak "bilişim suçları" kavramının olabildiğince açık şekilde izah edilmesi yerinde olacaktır.

1.2.1 Suç terimi

Toplum, toplumsal kurallar ile ayakta tutulabilen, belirli düzenlemelere ve sınırlara ihtiyaç duyan bir olgudur. Bu kapsamda beşeri bir davranışın tezahürü olan suç; törelere, ahlak kurallarına aykırı davranış olarak ismen tanımlanmış, hukuki olarak da yasalara aykırı davranış, cürüm olarak ifade edilmiştir (TDK, 2018c).

Genel bir suç tanımı mevzuatta yer almamakta olup; TCK'da da böyle bir kavramın açıklanması yoluna gidilmemiştir. 765 sayılı Eski (Mülga) Türk Ceza Kanunu'nda (ETCK) suçların tasnifinde kullanılan cürümler ve onlardan daha az haksızlık içeriğine

sahip kabahatlerin ayrımı da 5237 sayılı Yeni Türk Ceza Kanunu (YTCK) ile kaldırılmıştır.

Kabahatler ise kanunun karşılığında idari yaptırım uygulamasını öngördüğü haksızlıklar olarak ifade edilmektedir[6]. Genel olarak hakkında adli müeyyide yerine idari yaptırımlar uygulandığından kabahatler *idari suç* olarak da kabul edilmektedir.

Suç kavramının sözlük karşılığından hareketle; bir davranışın sadece yasalara aykırı olması yanında ahlak, töre gibi yazısız ve teamüli kurallara aykırılığın da suç kavramına temel oluşturabileceği görülmektedir. Zira bir toplumda hukuk kurallarını öncelikle o toplumun ahlak, töre, etik gibi evvelden beri süregelen olgularının şekillendirdiği aşikârdır. Nitekim ahlak ve hukuk kuralları müşterek bir zemine sahip olup[7] bu müşterek kaynak ise "*davranış normları*" dır. Bu itibarla, hukuki olan bir davranış aynı zamanda ahlakidir; ahlaka aykırı bir davranış da hiçbir zaman hukuki koruma altına alınamaz (Özgenç, 2014, s.27).

Bu ortak ilişkiye karşın; ahlaka aykırı olmasına rağmen hukuk düzenini bozucu boyuta ulaşmayan fiiller sadece ahlaki sorumluluk doğuracak, hukuki sorumluluğa vücut vermeyecektir. Örneğin kişinin yalan söylemesi ahlaken yanlış bir hareket iken bu fiil bir başkasının hayatını etkileyebilecek bir sonuca ulaştığı takdirde (iftira, yalan beyan/tanıklık gibi) cezai sorumluluktan söz edilebilecektir. Yine davranış normlarıyla yasaklanmış bulunan bir cinsi ilişki biçimi, dokunulmaz mahrem bir alanda, kişilerin özel hayatı içerisinde cereyan ettiği sürece hukuki sorumluluğa yol açmayacak; ancak bu eylem özel hayatın dışında aleniyet kazanması halinde hukuken müdahale etme imkânı doğacaktır (Özgenç, 2014, s.28).

---

[6] 5326 sayılı Kabahatler Kanunu (KK) m.2

[7] Yazılı hukuk kurallarının olmadığı yerde, diğer davranış kurallarının da toplum ve insanlar üzerinde büyük etkisi olduğu, birtakım düşünürler tarafından da dile getirilmiştir:

"Yasaların yasaklamadığını, utanma kontrol eder" (L. Annaeaus Seneca)
"*Ahlak olmayan yerde, kanun bir şey yapamaz*" (Napoleon Bonaparte)

Yine tanımlama temel alındığında bir suça vücut verebilecek hususun ancak bir "davranış" olabileceği tespit edilmektedir. Ceza hukukçularının büyük çoğunluğunun düşüncesine uygun olarak, günümüz hukuku yönünden normun ihlalinden ve dolayısıyla suçtan söz edilebilmesi için bir insan davranışının varlığı daima zorunlu olup davranışsız suçların varlığı kabul edilemez (Toroslu, 2009, s.114). Bu davranış icrai (aktif) olmayıp ihmali (pasif) bir davranış da olabilir. Ancak burada asıl önemli olan; davranış dışında örneğin bir fikir, düşünce ve/veya kanaati nedeniyle kişilerin suçlanamayacağı dolayısıyla cezalandırılamayacağıdır[8].

Yine suçun ortaya çıkmasından başka suçun sayısı da önem taşımaktadır. Şu halde bir hedefe yönelmiş çeşitli faaliyetler aynı zamanda gerçekleştirilmişse, yani bunlar arasında uzunca bir zaman aralığı yoksa ortada tek bir hareket ve tek bir suç varken; hedef aynı olsa da faaliyetler arasında önemli bir zaman aralığı olması birden çok harekete ve neticeten birden çok suça vücut verecektir (Toroslu, 2009, s.116). Örneğin bir bilişim sisteminde sunulan hizmetlerin durdurulmasına/engellenmesine yönelik tek bir teknik saldırı ile sonuca ulaşılabileceği gibi birçok sayıda saldırı ile de bu suç işlenebilir. Yapılan izahatlar ışığında, bu hukuka aykırı fiiller arasında önemli bir zaman aralığı yoksa ve anılan faaliyetler aynı hedefe yönelmişse, birden çok icrai hareket (davranış) gerçekleşse dahi tek suç oluşacaktır.

Sonuç olarak suçu; insanların toplum içerisinde birlikte yaşamalarının temini, toplumsal düzenin devamı için korunması gereken hukuki değerleri ihlal eden belli insan davranışları (tipik haksızlıklar) olarak tanımlamak (Koca ve Üzülmez, 2014, s.39) mümkündür.

[8] Ülkemizde en yüksek norm olarak kabul gören Anayasa'nın 25 inci maddesi, aşağıdaki hükmü havidir:

"Düşünce ve kanaat hürriyeti
MADDE 25*- Herkes, düşünce ve kanaat hürriyetine sahiptir.*
Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce ve kanaatleri sebebiyle kınanamaz ve suçlanamaz."

Genel hukuk ilkeleri uyarınca ve özellikle ceza hukukunda, bir davranış mer'i mevzuatta suç olarak kabul edilmedikçe devlet gücü olan yaptırıma sahip olması düşünülemez[9]. Suç kişinin düşüncesinden doğan iradi bir fiildir. Düşünce, yasağın konusu olamaz; ancak düşüncenin ifadesi yasaklanabilir (Hafızoğulları ve Kurşun, 2007, s.25).

Her suç, bir hukuki değere aykırılık teşkil edeceğinden, suç; ceza normuyla korunan hukuksal bir değerin veya menfaatin ihlali sayılacaktır. Bu hukuksal değerin temel özelliği ise ceza düzenlemeleriyle korunmuş olmasıdır. Hukuk düzenleri, suç niteliğindeki eylemleri ceza tehdidiyle yasaklayarak bu ihlali engellemeye çalışmaktadır (Ercan, 2008, s.83). Bu konudaki yasal emirler, mutlak bir değere sahip olup herhangi bir kimse yönünden ve şartsız olarak uyulması gereken kurallardır (Toroslu, 2009, s.36). Bununla birlikte, bu emredici buyruklar, bunları bilmeyenlere dahi uygulanır[10].

Ceza tehdidinin de suçu önleyecek nitelikte bir caydırıcılığa sahip olması; ancak bunun yanında ihlal edilen hukuki değer ile her somut olayda fail ve mağdurun sübjektif özellikleri ve diğer tüm olguların hakkaniyetli şekilde ele alınarak, olaya uygun cezaya hükmedilmesi toplumsal beklenti olarak önem arz etmektedir.

1.2.2 Bilişim ve suçun kesişimi

Bilişim ve iletişim; teknolojinin büyük hızla gelişmesine paralel olarak yaşamımızın ayrılmaz bir parçası olmuştur. Gelişen teknolojinin kötüye kullanılmasıyla yeni suç alanları, araçları ve tipleri ortaya çıkmış; diğer bir deyişle bilişim teknolojisi, fiil ve fail tipolojisini temelden değiştirmiştir (Erdoğan, 2012, s.42).

---

[9] Zira TCK'nın "*Suçta ve cezada kanunîlik ilkesi"* kenar başlıklı 2 nci maddesi: *"Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunda yazılı cezalardan ve güvenlik tedbirlerinden başka bir ceza ve güvenlik tedbirine hükmolunamaz"* düzenlemesini amirdir.

[10] Kanunun bağlayıcılığı kenar başlıklı TCK'nın 4 üncü maddesi; ceza kanunlarını bilmemenin mazeret sayılmayacağını hükme bağlamıştır.

Bilişim suçları bağlamında; bilişim sistemlerine karşı mı, yoksa bu sistemlerin aracılığı ile mi suçun meydana geleceği sorusu akla gelebilmektedir. Yine suçta kullanılan araçlar ve işleniş şekilleri de suç tiplerinin ortaya çıkması bağlamında bilişim alanı ile ceza hukukunun bir başka kesişim alanıdır.

Bilişim suçlarının hızlı evrimi ile hukukun ağır işleyen yapısı, problemlerin ortaya çıktığı noktada çatışmakta, hukukun nefesi bilişim suçlarına yetmemektedir (Erdoğan, 2012, s.43). Nitekim yasal düzenlemelere ihtiyaç duyulması karşısında; mevzuat hazırlık süreci, yürürlük safhası, uygulamanın kamu ve özel sektörde sağlıklı şekilde yerleşmesi, olası eksiklik ve sorunların giderilmesi gibi süreçlerin eşzamanlı olarak etkin şekilde uygulanabilmesi her zaman mümkün olamamaktadır.

Bilişim suçları ile muhatap olan uygulayıcıların teknik terimler nezdinde; suçun oluşması ve işleniş şekillerinin anlaşılması açısından bu kavramın sağlıklı bir şekilde algılanması ehemmiyet arz etmektedir.

1.2.3 Kavram çatışması ve tanımlama sorunu

Bilişim ile suçun kesiştiği bu konuda bir kavram kargaşası yaşandığı, literatürde de aynı anlama gelen birçok farklı kavramın kullanıldığı görülmektedir. Nitekim birçok farklı şekilde ifade edilen; *siber suç, sanal suç, internet suçu, bilgisayar suçu, bilgisayar ile ilgili suç, bilgisayarlara karşı işlenen suç, bilişim suç hukuku, bilişim sistemi aracılığıyla işlenen suç, bilişim alanında işlenen suç* ve *bilişim suçu* bu alanı karşılamak için kullanılan kavramlardır (Dülger, 2015, s.78). Anılan tanım ve kapsam sorunu nedeniyle bu suçlara *çizgisiz çerçeveli suç* da denilmektedir (Akarslan, 2015, s.36).

Bu kavramlar doktrinde haklı olarak yoğun şekilde eleştiriye maruz kalmıştır. Zira bilişim alanındaki hızlı gelişimin de göz önünde bulundurularak, suç teşkil edecek eylemlerin hem teknik hem hukuki açıdan tüm yönleriyle ele alınarak en kapsayıcı kavramın kullanılması gerekmektedir.

İnternet suçu kavramı bakımından; her ne kadar internet en yaygın kullanılan ağ olsa da bunun dışında başka ağların da (intranet[11], ekstranet vb.) bulunduğu ve bu ağlar aracılığıyla da suç işlenebildiği; suçun işlendiği ortama göre farklı şekilde isimlendirilmelerinin doğru olmadığı belirtilmiştir (Yenidünya ve Değirmenci, 2003 s.31-32).

Bilgisayar suçu bakımından; yazılım ve donanımı ile bilgisayar tarifi dışında kalan tüm cihazlar, onunla aynı veya benzer işlevi görse dahi "bilgisayar" sözcüğünün içerisine hapsedilmiş olacaktır (Taşkın, 2008, s.12). Ayrıca, bilişim sisteminin geniş yorumlanmasına dair yukarıda sunulan Yargıtay 8. Ceza Dairesi kararında da açıkça ifade edildiği gibi, bilişim alanında işlenen suçlar sadece bilgisayarlar aracılığıyla değil; mobil internet hizmeti sunan cep telefonları, tabletler, avuç içi bilgisayarlar ve IP TV gibi birçok farklı cihazla da işlenebilmektedir. Hatta bazı yazarlarca bilgisayarın suçun hedefi olabilmesi savından hareketle, bilgisayarın donanımı veya yazılımlarının çalınması dahi bilişim suçlarının tasnifine dâhil edilmektedir (Karagülmez, 2014 s.69). Kanaatimizce suç konusunun bilgisayar olabileceği hırsızlık veya mala zarar verme suçlarında; bir bilgisayar ile bir ziynet eşyasına zarar verilmesi/çalınması arasında fark bulunmamakta olup bilgisayarın salt maddi varlığına halel getirilmesinin bilişim suçları kapsamı içerisinde sayılması yerinde değildir[12]. Bununla birlikte; suçun işlendiği materyal ile tarif yapılması konunun doğasına da aykırıdır ve herhangi bir suç aleti ile adlandırılan bir suç da ceza mevzuatımızda yer almamaktadır.

Siber/sanal suç bakımından; işlenen suçların sanal değil gerçek olması, amaçlanan kavramı ifade etmekte yetersiz kalması ve siber sözcüğünün yabancı kökenli olması

[11] İntranet sadece belirli bir kuruluş içindeki bilgisayarları, yerel ağları (LAN) ve geniş alan ağlarını (WAN) birbirine bağlayan, çoğunlukla TCP/IP tabanlı, küçük internet olarak da adlandırılabilecek özel bir ağdır. Temel oluşturulma amaçları ise, kuruluş bünyesindeki bilgileri ve bilgi işlem kapasitesini paylaşmaktır. İntranetler, şirket(ler) içi tele-konferans uygulamalarında ve farklı birimlerdeki kişilerin bir araya gelebildiği iş gruplarının oluşturulmasında da kullanılırlar (BTK, 2007, s.81).

[12] Ancak işlenen hırsızlık suçundaki saik (asıl gerekçe/motivasyon) bilgisayarın fiziki varlığının maddi değeri yerine içerisinde bulunan verilerin temini ve/veya bunların üçüncü kişilerle menfaat karşılığı paylaşılması ise burada yetkisiz olarak sistem üzerindeki verilerin ele geçirilmesinden söz edilebileceğinden bilişim suçundan bahsedilmesi mümkün olacaktır.

eleştirilmiştir (Dülger, 2015, s.79). Siber suç terimi ile aslında bilişim suçlarının ifade edildiği, bununla birlikte bilişim suçlarının tek bir bilişim sistemince işlenen şekli değil, bilişim sistemi ağları aracılığıyla (özellikle internet) işlenen suçların kastedildiğini, bilişim suçları kavramının siber suçları da içine alan bir kavram olduğu da ifade edilmektedir (Yenidünya ve Değirmenci, 2003 s.31-33).

Kanımızca; özellikle konuya ilişkin olarak siber sözcüğünün başlığında bulunduğu uluslararası bir sözleşme bulunması[13], Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın ilgili kısımları uyarınca BTK bünyesinde Ulusal *Siber* Olaylara Müdahale Merkezi (USOM) kurulması, yine kamu idaresi içerisinde Emniyet Genel Müdürlüğü nezdinde faaliyet gösteren *Siber* Suçlarla Mücadele Daire Başkanlığı'nın bulunması ve global platformlarda da bu ibarenin yoğun olarak kullanılması hasebiyle "siber suçlar" teriminin de bu suçların karşılığı olarak kullanılabileceği; ancak gerek kamu gerek özel sektör uygulamalarında kavram karmaşası yerine yeknesak olarak "bilişim suçları" teriminin tercihinin yerinde olacağı değerlendirilmektedir.

TCK sistematik yorumlandığında da doğrudan bilgisayar veya benzeri bir cihaz bağlamında suç tanımlamalarının yapılmadığı; nitekim suçun işlendiği ortam veya ekipman gibi değişken faktörlerle isimlendirme yoluna gitmek yerine isabetli olarak bilişim alanında suçlar tabirinin kullanıldığı görülmektedir.

Sonuç olarak; siber suçlar ve özellikle bilişim suçları terimleri üzerinde genel olarak ittifak sağlandığı, güncel tarihli kaynakların tümüne yakınında ise "bilişim suçu" kavramının kullanıldığı görülmektedir.

Bilişim suçlarının tanımlanması hususunda ise tam bir uzlaşma olmasa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu (AET) Uzmanlar Komisyonunun 1983 yılı Mayıs ayında yaptığı tanımlama olup bu tarife doktrin ve yargı kararlarında da yer verildiği görülmektedir (Orta, 2015, s.85). Anılan komisyona göre bilişim suçları: *"Bilgileri, otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri*

[13] Avrupa Konseyi Siber Suç Sözleşmesi (ASSS)

kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" şeklinde tanımlanmıştır.

1.2.4 Bilişim suçlarının sınıflandırılması

Bilişim suçlarının tasnifinde ortak bir kanaate varılmasa da öğreti ve uygulamalara göre iki ana kategoride işlenebileceği hususunda görüş birliğine varılmıştır (Taşkın, 2008 s.10). Birleşmiş Milletler (BM) 10. Kongresinde de bilişim suçları; bilgisayar ağlarında veya ağlarına karşı gerçekleştirilen her türlü eylem olarak kabul görmekte ve bu suçlar dar anlamda siber suçlar ve geniş anlamda bilişim (siber) suçları olmak üzere iki alt kategori içinde değerlendirilmektedir (Avşar ve Öngören, 2010, s.48). Bunlardan ilki bilişim sistemlerine karşı işlenen suçlar iken, diğeri ise bilişim sistemleri aracılığıyla işlenen suçlardır.

Çalışmamızın da konusunu oluşturan bilişim sistemlerine karşı işlenen suçları *"doğrudan/dar anlamda/gerçek bilişim suçları"* olarak adlandırmak mümkündür. Direkt olarak bilişim sistemlerine karşı işlenmeyip, bu sistemler aracılığıyla bir başka suça dair fiilin ifası suretiyle icra edilebilecek suçlara ise *"dolaylı/geniş anlamda/bilişim bağlantılı/bir diğer suçun unsuru olan/ bilişim suçları"* demek kanımızca doğru olacaktır[14].

Bu şekilde bir tasnifin, hem 5237 sayılı TCK'nın sistematiğinde hem de Yargıtay Ceza Genel Kurulu'nun (YGCK) birkaç kararında[15] kabul edildiği bilinmektedir (Orta, 2015, s.86, dn.408 ; Doğu, 2016, s.83 dn.2).

[14] Nitekim yeni tarihli (Eylül-2016) bir kaynak olarak kabul edilebilecek Sn. Ahmet GÜL'ün eseri de bu sınıflandırmayı esas alarak başlığında bu ibare ile (Doğrudan-Dolaylı Bilişim Suçları) literatürde yerini almıştır. Yine aynı görüşte birçok farklı yazar da bulunmaktadır. Bkz: Dülger, 2015, s.83 ; Orta, 2015, TBMM, 2012a s.816, s.85 Taşkın, 2008, Ketizmen, 2008 s.12 ; Kurt, 2005, s.279; vs.)

[15] YCGK'nun 17.11.2009 tarihli, E.2009/11-193, K.2009/268 sayılı kararı; YCGK'nun 02.04.2013 tarihli, E.2012/15-1293, K.2013/111 sayılı kararı.

İlk tasnif, genel olarak çalışmamızın konusunu oluşturan ve gerçek anlamda bilişim suçlarını ifade eden fiillerden ibaret olup bu suçların niteliği ve sayısı ülkemiz düzenlemelerine bakıldığında sınırlı sayılı[16] (tahdidi) şekildedir. İkinci tasnifte ise geleneksel veya klasik denebilecek diğer suçlara atıfta bulunulmaktadır. Zira bu sınıflandırmada, cezai hüküm içeren herhangi bir norma aykırılık teşkil edebilecek ve bilişim sistemlerinin bu suçun sadece bir unsuru olabileceği -bu sistemler olmaksızın da işlenebilmesi mümkün olan- diğer suçlar işaret edilmektedir.

Her iki sınıflandırma da ayrı ayrı önem taşıdığından, çalışmanın ilgili yerlerinde; "doğrudan bilişim suçları" ve "dolaylı bilişim suçları" açısından detaylı açıklamalar yapılacaktır.

1.3 Bilişim Suçlarının İşlenme Biçimleri (Modus Operandi)

Her suçta olduğu gibi bilişim suçlarında da bunu işleyen kişi veya grupların belirli bir veya birkaç motivasyonu bulunmakla birlikte, suç işleyen kişileri suçtan vazgeçirecek veya suç işlemeye devam etmesine sebep olacak mağdur davranışları da bu konuda önem taşımaktadır.

Suçun işlendiği ortam ve suç sonucunda elde edilecek verilerin çeşitlilik arz etmesi, teknolojik boyutun bu suç tipinde oldukça büyük oranda önem taşıması gibi sebeplerle, faillerin yeteneği ve ulaşılması istenen bilginin muhafaza edildiği sistemin büyüklüğüne göre suç işleme yöntemleri de farklılık gösterecektir.

1.3.1 Bilişim suçlarında faillerin saiki ve mağdurların yaklaşımı

Suçlarda failin suç işleme motivasyonu/güdüsü olarak adlandırılabilecek saik, çok farklı sebeplere dayanabilir ve bu nedenler ile suçun işlenme şekillerinin birbirleriyle bağlantılı olması her zaman beklenmez.

[16] TCK m.243-246 arasında sayılan suç ve cezalar.

Bilgisayar teknolojisi ve internetteki hızlı gelişmeler, teknolojiye bağlı suçlu davranışlarını doğurmakta ve etkilemekte olup yeni suçlarla ilgili suçlu eylemleriyle başa çıkmak için uzmanlaşmayı içeren yasalara ihtiyaç duyulmaktadır (Karagülmez, 2014, s.63).

Bilişim suçlarının işleniş sayısındaki artışa rağmen buna maruz kalan mağdur gerçek veya tüzel kişilerin, bu tür suçların bildirilmesinde oldukça pasif kaldığı ve aşağıdaki sebeplerden ötürü ihbar yapmaktan çekindiği ifade edilmektedir (Redstor, 2018):

- Kolluk kuvvetleri ve yasaların yardım edemeyeceği düşüncesi,
- Nasıl ihbarda bulunulacağı hakkında yeterli bilgiye sahip olmama,
- Bilişim sistemlerindeki güvenlik açıklarını kabul etmede isteksizlik,
- Somut olayın adli kolluk ve yargılama işlerini meşgul edecek değerde görülmemesi,
- Soruşturma ve kovuşturmanın ticari faaliyetleri yavaşlatacağı/aksatacağı fikri

Mağdurların bu suçları kamuoyundan saklamak istemeleri yukarıdaki gibi sıralanabilmekte olup özellikle tüzel kişiler (genellikle ticari şirketler) seviyesinde gerçekleşen suçlar, kimseye duyurulmadan çözümlenmeye çalışılmakta olup bunların sebepleri; şirket yöneticilerinin bilgisayar suçları nedeniyle, kolluğun şirketin iç işlerine karışarak detaylı bilgi sahibi olmalarını istememeleri ve bu tür bir araştırmanın şirketin (genellikle hissedarları nezdinde) itibar kaybına neden olacağına inanılmasıdır. Bu tür eylemler, yetkili makamlara bildirilmediklerinden iş dünyası içerisinde gizli kalmakta ve bu nedenle bazı failler suçlarını toplumdan rahatça gizleyebilmektedir (Tulum, 2006, s.52).

Bu çerçevede; gerçekleşen asıl sayıdan çok daha az ihbarın yapılmasının, bu suçu işleyenlere bir yeşil ışık yaktığı, dolayısıyla faili suçtan vazgeçirmekten çok suç işlemeye devam kararını güçlendirdiği, bunun sonucu olarak da bu tür davranışların suçu işleyen açısından sonucuna katlanılmaksızın yaptırımsız bırakıldığı vurgulanmaktadır (Zdnet, 2018).

Yine İngiltere Suç Ajansı (*National Crime Agency-NCA*) tarafından yapılan bir değerlendirme raporu kapsamında; bilişim suçlarının olağandan az ihbar edilmesinin devam eden bir sorun olduğu, ülkelerinde sadece %38'lik bir kesim tarafından kolluk kuvvetleri ve ilgili yasal düzenlemelerin bu konuda karşılık verebilecek yapıda olduğuna güvenildiği ve bu durumun kolluk güçleri ve adli mercilerin aksiyon almaları hususunda engellemeler yarattığı ifade edilmektedir (NCA, 2018, s.46). Bununla birlikte, bu güvenme oranının gelişmekte olan veya az gelişmiş ülkelerde daha da azalacağı düşünülmektedir.

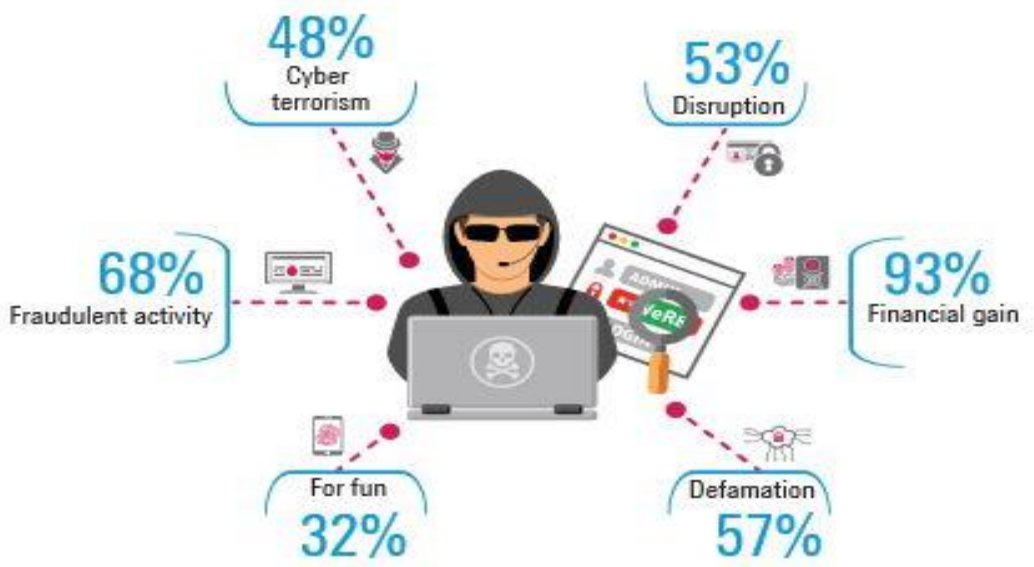
Bilişim suçları faillerinin ise genel olarak; işte yaşanan çeşitli olumsuzluklar veya işten çıkarılma, politik amaç gütme, sadece eğlenmek isteme, cinsel tatmin arzusu, ciddi psikolojik rahatsızlıklar, öfke ve intikam alma duygusu (vandalizm, sabotaj, yağma gibi), mali zorluklar ve maddi menfaat sağlama isteği, bilgisayarı aşabilme duygusu (operatör makine ilişkisinden kaynaklanan sorunlar da dâhil) sebepleriyle suç işledikleri belirtilmektedir (Koçak ve Dandin, 2017, s.143).

Emniyet güçleri ile birlikte yapılan bir çalışmada, bilişim suçu faillerinin özellikle 5 ana konuyu motivasyon noktası olarak temel aldığı sonucuna ulaşılmıştır (KPMG, 2018, s.7):

- Mali kazanç sağlama (*Financial gain*)
- Dolandırıcılık (hile/sahtekârlık) içeren eylemler (*Fraudulent activity*)
- Hakaret (*Defamation*)
- Sistemin işleyişini bozma (*Disruption*)
- Siber Terörizm (*Cyber terrorism*)
- Eğlence ve Zevk (*For fun*)

Bu çalışmada sayılan temel saik konularında yüzdesel dağılım da hesaplanmış olup aşağıdaki gibidir:

Şekil 1.5 Bilişim Suçlarının İcrasında Faillerin Motivasyonu



1.3.2 Modus Operandi kavramı

'Modus Operandi' kavramı Latince kaynaklı olup, bir failin suç teşkil eden eylemlerinde ayrıştırılabilecek bir biçim veya yöntemi ifade etmektedir (Encyclopaedia Britannica, 2018). Bu kavram kısaca, faillerin tavrı dâhilinde suç işleme yöntemi veya metodu olarak ifade edilebilir.

Bilişim teknolojisinde yaşanan ilerlemeler, suçlu davranışlarında ya da suça iten unsurlar içerisinde önemli bir araç olmuştur (Karagülmez, 2014, s. 65). Bu araçların, teknolojik ilerlemeyle doğru orantılı olarak geliştiği ve dolayısıyla bilişim suçlarının işlenme tekniklerinin zamanla değişiklik gösterdiği ve göstereceği söylenebilir.

Bilişim suçları, diğer geleneksel suçlardan özellikle işleniş şekillerinin çok çeşitli ve öngörülemez olmasıyla ayrılmaktadır. Bu tür suçların modus operandilerinin tanımlanmasında ve tespit edilmesinde yarar görülmekte olup, bu tanımlama ve tespit işleminin sınırlayıcı değil örnekleyici olduğuna dikkat çekilmelidir. Zira suçun işlendiği ortam ele alındığında, her geçen gün kendini yenileyen teknolojik gelişme

karşısında kesin bir belirlemeye gitmek büyük bir hata olacak ve bu suçlarla mücadelede geri düşülmesine sebep olunacaktır (Turhan, 2006, s.47).

Sayılan sebeplerle teknolojik gelişmeler paralelinde, bir dakika sonrasında dahi, bir bilişim suçunun işlenmesinde farklı bir metot geliştirilmesi ve uygulamaya konulması mümkündür. Bu bağlamda; aşağıda ifade ve analiz edilecek teknikler sadece şu ana kadar görülmüş ve bu suçların icrasında en yaygın kullanılan modus operandiler olup, bu alandaki gelişmeler paralelinde bunların sayısının her geçen gün artabileceği göz önüne alınmalıdır. Bu alanda suç işleme yöntemlerinin fazlalaşması ve farklılaşması, suçun önlenebilmesini teminen, bilişim sistemi güvenliği ile ilgili alınabilecek önlemler bakımından da aynı derecede artışı beraberinde getirmelidir.

1.3.3 Bilişim suçlarında en yaygın icra metotları

Yukarıda da bahsedildiği üzere bilişim suçlarının işlenme yöntemleri sayıca fazla ve teknolojik gelişmelere göre farklılık gösterebilecektir. Bu nedenle aşağıda, genel olarak bu suçların icrasında en çok başvurulan yollara yer verilecektir.

1.3.3.1 Dos-DDoS saldırıları (Denial of service - Distributed DoS attacks)

Bir kişinin bir sisteme düzenli veya arka arkaya[17] yaptığı saldırılar sonucunda sistemin kimseye hizmet veremez hale gelmesi veya o sisteme ait tüm kaynakların tüketiminin amaçlandığı DoS (*Denial of Service* - Hizmet/Servis Dışı Bırakma) saldırısı, bir hizmet aksatma metodudur (Dülger, 2015, s.132).

DDoS (*Distributed Denial of Service* - Dağıtık Hizmet/Servis Dışı Bırakma) atakları ise bir saldırganın daha önceden tasarladığı birçok makine üzerinden hedef bilgisayara

[17] Bu saldırıya benzer bir başka yöntem "*Eşzamansız Saldırılar*" (A*synchronous Attacks*) olarak adlandırılmakta olup bu saldırılarla; sistem, mevcut programları eşzamanlı yani aynı anda kullanamadığından; bilgisayar, kullanıcı taleplerini belli bir düzen ve sıra içinde yerine getirirken bu bekleme sırasında verilerin değiştirilmesi yoluna gidilmektedir (Kurt, 2005, s.68). Ancak görüldüğü üzere her iki saldırı aynı olmayıp DoS saldırılarında hizmetin devre dışı bırakılması, diğer yöntemde ise sistemin sıraya aldığı verilerin tahribatı (değiştirme, yok etme) söz konusu olmaktadır.

saldırı yaparak hedef sistemin hizmet veremez hale gelmesini amaçlayan bir saldırı yöntemi olup "zombi" adı verilen araçlarla eşzamanlı yapılan bu işlem, saldırının boyutunu artırırken saldırganı da gizlemektedir (Dülger, 2015, s.132).

Bilgisayar ve internet güvenliği alanında faaliyet gösteren bir firma ile bir araştırma şirketi[18] birlikteliğiyle tanzim edilen "2016 Kurumsal BT Güvenlik Riskleri" anketinin sonuçlarına göre; ülkemizdeki işletmelerin yaklaşık beşte biri (%14) DDoS saldırılarına karşı hiçbir şekilde korunmamakta ve yarısından fazlası (%60) ise bu saldırılara karşı etkili olmayan dâhili koruma donanımına güvenerek faaliyetlerini sürdürmeye devam etmektedir. Ayrıca, DDoS saldırısı başlatıldığında hedef şirketin çevrimiçi varlığı devre dışı bırakılacağından; hasarın son derece yıkıcı olabileceği, iş akışının duracağı ve kritik öneme sahip süreçlerin tamamlanamayarak ciddi itibar zedelenmesi yaşanabileceği ifade edilmiştir (CyberMag, 2017, s.33).

Dünyada DDoS saldırıları, en yoğun kullanılan ilk 10 yöntem arasında bulunmakta olup; bu metodun diğer atak yöntemleriyle yüzdesel olarak kıyaslanması sonucunda 2015 yılında % 9.7 olarak gerçekleştiği, 2016 yılında % 11.2 oranına çıktığı, 2017'de ise % 4.2 dolaylarında kaldığı görülmektedir (Passeri, 2018).

Ülkemizde de 2017 yılı verilerine göre toplam 50.747 DDoS saldırısının gerçekleştiği işletmeciler tarafından USOM'a raporlanmıştır (BTK, 2018b).

1.3.3.2 Truva atı (Trojan horse)

Adını; mitolojik bir savaşta kullanılan ve aslında armağan olarak gönderilip, içerisinde saldırı amacıyla saklanmış askerleri barındıran ihtişamlı ahşap yapıdan alan bu yazılımın; görünürde masum, ancak arka planda saldırgan olduğunu belirtebiliriz.

[18] Kaspersky Lab ve B2B International

Truva atları, diğer birçok zararlı yazılımda olduğu gibi kullanıcılar tarafından internette veya e-posta yoluyla ücretsiz kullanabilecekleri basit programlar ya da ekran koruyucular gibi küçük ama ilgi çekici uygulamalar aracılığıyla kullanılan cihaza bulaşmaktadırlar (Akarslan, 2015, s.94).

Görüldüğü üzere birçok kullanıcının ilgisini çekebilecek programların ücretsiz olarak sunulması halinde truva atı da bu programların içine entegre olarak bunu indiren kişinin cihazına programla birlikte fark edilmeden yüklenmektedir.

Truva atı yazılımı görünüşte zararsız, hatta yararlı gibi görünmekle beraber, gerçekte yıkıcı bilgisayar komutları içeren, kullanıcıya kendisini normal bir uygulamaymış gibi göstererek çok iyi tasarlanmış maskelerle aldatmaktadır (Kurt, 2005, s.63).

Truva atları ile bilişim virüsleri, her ne kadar zararlı yazılım ortak paydasına sahip olup benzerlik taşısa da, truva atlarının kendi kendilerine çoğalma özelliklerinin olmaması ve zararsız bir yazılımmış gibi görünebilme niteliğini haiz olmaları nedeniyle bilgisayar virüslerinden ayrıldığı belirtilmektedir (Dülger, 2015, s.120).

Anlatılanlar ışığında; truva atlarının zararlılığının kullanıcının hareketlerine bağlı olduğu açık olup bunların aktif hale gelebilmesi için her kurbanın içinde truva atı gizlenen programı yüklemesi ve/veya çalıştırması gerekmektedir. Çünkü truva atları diğer zararlı (kötücül) yazılımlar olan bilişim virüsleri veya solucanları gibi kendi başlarına işlem yapamazlar (Turhan, 2010, s.41).

O halde truva atı yazılımını ihtiva eden bir program indirilip, kullanıcı tarafından çalıştırılmadıkça (dolayısıyla truva atı aktive edilmedikçe) cihaza herhangi bir zararlı yazılımın etki etmesi mümkün olmayacaktır.

Diğer taraftan bilişim virüsleri veya solucanlar mevzu bahis olduğunda, iradi olarak herhangi bir indirme işlem gerçekleştirilmese de, kişinin rızası ve bilgisi dışında cihazına zararlı yazılımın giriş yapması ve sistemi olumsuz olarak etkilemeye başlamasından söz edilebilecektir.

1.3.3.3 Virüsler (Viruses)

Bilgisayar virüsleri yazılmaları kolay, tespiti güç yazılımlar olup kendi kendilerine çoğalıp diğer programlara bulaşabilmeleri yani kolonileşebilmeleri mümkün olan programlardır (Kurt, 2005, s.69-70). Bilgisayar ve benzeri cihazlara zarar verebilecek, akla gelen ilk kötücül program virüsler olmaktadır.

Virüslerin bulaştığı cihazlara verebileceği zarar türleri aşağıdaki gibi sıralanabilir (Akarslan, 2015, s.92):

- Cihazda hata veya uyarı mesajları alınmasına sebep olma
- Cihazın kilitlenmesi, kapanması ve açılamaz hale gelmesine yol açma
- Cihazda kullanılmak istenen bir dosyaya erişimin engellenmesi
- Dosyaların bir kısmı veya tamamının kullanılmaz hale getirilmesi
- Cihaza yerleşerek kullanıcının yaptığı işlemlerin veya bilgilerin (finansal, kişisel, iletişim vb. veriler) yetkisiz üçüncü kişiler tarafından bilinmesi hatta bu kişilerin cihaza uzaktan erişimine yol açması

Yukarıdaki zarar türlerinden yola çıkarak, son yıllarda özellikle fidye yazılım[19] (*ransomware*) türündeki virüslerin cihazlara ve dolayısıyla kullanıcılara büyük zarar verdiği bilinmektedir.

Fidye yazılımlar; cihaz sistemine veya cihazdaki dosyalara erişimi engelleyen zararlı bir yazılım olup saldırgan tarafından bu veriler, fidye olarak belirlenen meblağ ödenene dek tutulmakta, eğer talepler yerine getirilmezse sistem veya şifrelenen dosyalar erişilemez halde kalmakta ya da silinmektedir (US-Cert, 2016).

[19] Dünya genelinde on binlerce kuruluşun 'WannaCry' olarak bilinen bilgisayar virüsünün saldırısına uğradığı ve bu zararlı yazılımın bilgisayar içindeki verileri kilitleyip, belgelerin yeniden kurulumu için kullanıcılardan her defasında 300 dolar ödeme talep ettiği ve bu fidye yazılımdan Türkiye'nin de aralarında olduğu en az 99 ülkenin etkilendiği belirtilmiştir (BBC, 2017).

Cihazına fidye yazılım içeren virüs bulaşan kişinin bunu ödemesi durumunda ise; bu tür suçluların faaliyetlerinin destekleneceği ve işlerini büyütmesine yol açacağı yanında dosyaların geri alınmasının da garanti edilmediği (nitekim kurbanların %20'sinin ödeme yapmasına rağmen dosyalarının silindiği ifade edilmektedir) vurgulanmaktadır (Kaspersky, 2016). Bunlara ek olarak fidye ödenmesine rağmen saldırganın, kişinin cihazına gizli bir yazılım bırakması ve/veya kişisel verilerini elinde tutması mümkündür. Ayrıca saldırganın, rahatça haksız maddi menfaat temin edebildiği kullanıcıya tekrar benzer yollarla saldırıda bulunmasının da beklenebileceği düşünülmektedir.

1.3.3.4 Oltalama (Phishing)

"Phishing" sözcüğü, İngilizce 'balık tutma' anlamına gelen 'Fishing' sözcüğünden esinlenerek, olta atıldığından en azından bir balık yakalanabileceği düşüncesinden hareketle 'Fishing' sözcüğündeki "f" yerine "ph" harfinin kullanılmasıyla oluşturulmuş olup kısaca, bilgi girmeyi gerektiren bir internet sayfasının kopyasının yapılarak kullanıcının hesap bilgilerini çalmayı amaçlayan internet dolandırıcılığına verilen isimdir (BTK, 2018c). Türkçe olarak ise oltalama veya yemleme kavramları kullanılabilmektedir.

"Ph" ibaresinin açılımının ise "*password harvesting*" yani şifrenin elde edilmesi kavramından geldiği ifade edilmekte olup bu yöntemin özel ve gizli kalması gereken, başkaları tarafından bilindiğinde kişilerin zor durumda kalmasına neden olabilecek gizli bilgilere erişmek ve onları elde etmek için sanki bu bilgileri kişiye veren ve güvenilir bir yerden geliyormuşçasına görünen e-postalar ya da web siteleri hazırlayıp kullanıcılardan bu bilgileri paylaşmalarını isteme eylemlerinin tümünü kapsadığı belirtilmektedir (Gözüşirin, 2011, s.41).

Bu tür saldırılar, 'web sayfası hırsızlığı ve yönlendirmesi' olarak da adlandırılmakta olup kullanıcının ulaşmak istediği sayfaya benzer hazırlanan başka bir web sayfasına yönlendirilerek bu sayfada işlem yapılmasıyla verilere erişime yol açıldığının altı çizilmektedir (Kurt, 2005, s.73).

Bu metodun bir diğer türünün de çok bilinen web sayfalarına ulaşmak için adresi küçük farklılıklarla yanlış yazanların adresin neresinde yanlış yapacağını öngörerek bu yönde bir sayfa oluşturulması olduğu dile getirilmektedir (Kurt, 2005, s.73). Nitekim kripto/şifreli para[20] ile ilgili bir internet sitesi olan "*falc**o**ncoin.io"* gerçek alan adı mevcut iken, sadece tek harf değiştirilerek "*falc**a**ncoin.io"* alan adı kötü amaçlı olarak 27 Aralık 2017 tarihinde satın alınmış ve 19 Şubat 2018'de kodların görünmeye başlamasından sadece birkaç gün önce güncellenerek, bu kodlarla kurbanın sistemine saldırganın tam erişim sağlayabileceği bir uzaktan erişim aracı ile verilerin elde edilmesi sağlanmıştır (STM[21], 2018, s.8).

Sayılan sebeplerle kullanıcıların, alan adının yazımından, güvenli site uzantılarına kadar ve özellikle finans kuruluşlarından veya kişisel verilerin tutulduğu sosyal medya hesaplarından (oltalama var ise gönderilmiş gibi gösterilen) kullanıcı adı-şifre vb. verilerin girilmesini/sıfırlanmasını talep eden e-postalara yüksek düzeyde ihtimam göstererek yaklaşması gerekmektedir.

Bu yöntemle ele geçirilen kişisel verilerin ihlali, yetkisiz bankacılık işlemlerinde bulunma ve kredi kartı kullanarak büyük alışverişler yapılması gibi suçlarda kullanılmaktadır. Bu eylemlerde kullanıcılar, sahte siteler, e-postalar yoluyla gerçeğe çok yakın senaryolarla aldatılmaya çalışıldığından, bu tür saldırıların başarılı olabilmesinde kullanıcının rolü büyüktür (Türkiye Büyük Millet Meclisi [TBMM], 2012, s.748).

---

[20] Kriptografik/şifreli olarak güvenli işlem yapmaya ve ek sanal para arzına olanak sağlayan dijital değerler olup kripto-paralar, alternatif para birimidirler, dijitaldirler ve aynı zamanda sanal paradırlar. Bu değerler, merkezi elektronik paraların ve bankacılık sistemlerindekinin aksine, merkezi olmayan yapıdadırlar. Merkezi olmayan bu yapının kontrolü Blok-Zincir (Block-Chain) işlem veri tabanları tarafından gerçekleştirilir (Çarkacıoğlu, 2016, s.8). Bu para birimleri web-tabanlı, kriptografiye dayanan denkler arası (peer to peer) ödeme sistemleri olup en bilinen ve hali hazırda en başarılı örnek olan Bitcoin, ilk olarak 2008 yılında dolaşıma sokulmuştur (Marian, 2016, s.923).

[21] Türk Silahlı Kuvvetleri (TSK) ve Savunma Sanayii Müsteşarlığı'na (SSM) sistem mühendisliği, teknik destek, proje yönetimi, teknoloji transferi, lojistik destek hizmetleri; görevlerini gerçekleştirmek amacıyla Savunma Sanayii İcra Komitesi Kararı ile 1991 yılında kurulan ve %34 hissesi SSM elinde bulunan bir şirkettir (Savunma Teknolojileri Mühendislik ve Ticaret A.Ş) [*https://www.stm.com.tr/tr/hakkimizda/sirket-profili]*

1.3.3.5 Arka/Gizli kapılar (Back/Trap doors)

İşletim sistemleri veya çok işlevli kullanıcı sistemleri hazırlanırken ileride ihtiyaç duyulabileceği öngörüsüyle, sistem şifrelerinde değişiklik yapabilmek veya yeni şifreler girebilmeyi sağlamak üzere gerek sisteme bırakılan çeşitli giriş olanakları sağlayan gizli kapıların program tamamlandığında ortadan kaldırılması, gerekse de bunun rıza ile veya sehven kaldırılmaması üzerine bu kapıların yasadışı faaliyetlere hizmet etmesi söz konusu olabilir (Ergün, 2008, s.19).

Yukarıda sayılan ve bilişim sisteminin çalışmaması ihtimaline karşılık programcısı tarafından her zaman müdahale imkânı için kullanılan bu kapılar legal görünümdedir ancak bunların zararlı yazılımlar aracılığıyla da açılabilmesi ve kullanılması mümkündür (Akarslan, 2015, s.98). Arka kapıların kötücül bir program ile açılması yanında bu kapıların programcı dışında ve sistemin iyileştirilmesi, çalışmaması tehlikesini bertaraf etme gibi olumlu sebepler haricinde özellikle de yetkisiz biri tarafından kullanılmasının işlemi illegal hale getireceği değerlendirilmektedir.

6 Mart 2018'de Türkiye, Rusya ve Ukrayna'daki bilgisayarları etkileyen MediaGet olarak adlandırılan BitTorrent istemcisinin, arka kapı içeren bir varyasyonu nedeniyle yaklaşık yarım milyon gibi yüksek sayıda bilgisayara zararlı yazılım bulaştığının tespit edildiği raporlanmıştır (STM, 2018, s.16).

1.3.3.6 İstem dışı elektronik postalar (Spam mails)

İstem (rıza) dışı e-postalar; genellikle bir ürünün reklamı, pazarlanması ve pornografik içerikli reklam ile mesajların dünya çapında kitlelere ulaştırılması amacıyla kullanılan, bünyesinde çok sayıda mail adresini barındıran kuruluşların sahip oldukları veri tabanlarını satmalarıyla arttığı belirtilen bir kavramdır (Dülger, 2015, s.129-130).

İstek dışı haberleşme olarak da adlandırılan spam; aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte

gönderilmesi şeklinde tanımlanmakta olup, aşağıdaki karakteristik özellikleri taşıdığından bahsedilmektedir (Öztürk, 2009, s.27-28):

- ***Elektronik Veri Özelliği***: Spam mesajlar e-postalar başta olmak üzere mobil servisler üzerinden alınan hizmetlerde de ciddi sorunlara yol açmaktadır.

- ***Toplu Gönderim ve Tekrarlanma***: Spam mesajlar rastgele ve yığın ileti halinde, tekrarlı bir şekilde gönderilmektedir.

- ***Gizli/Yanlış Mesaj Kaynağı***: Spam mesajlar genellikle e-postanın başlık bölümündeki gönderen bilgisinin gizlenmesi veya yanlış bir bilgiyle değiştirilmesi şeklinde iletilmektedir. Spam üreticileri de genellikle yetkilendirilmemiş üçüncü taraf e-posta sunucularını kullanmaktadır.

- ***Zorlama Niteliği***: Spam mesajlar muhataplarına dağıtım listesinden veya üyelikten çıkma (*unsubscribe*) ya da bir sonraki mesajı almama seçeneği sunmadıklarından ötürü zorlayıcı mahiyettedir.

- ***Saldırgan/Yasadışı İçerik***: Spam mesajlar genellikle sahtecilik faaliyetlerinde kullanılmakta ve aldatıcı içerik (virüs, solucan vb.) taşıdığından tehdit unsuru sayılmaktadır. Bununla birlikte içerik, rahatsız edici cinsel unsurlar veya terör propagandası gibi illegal mesajlar da olabilmektedir.

- ***İzinsiz İletişim Verisi Kullanımı***: Spam üreticileri, kullanıcının rızası olmaksızın (bilgisi ve isteği dışında) toplanan iletişim bilgilerini (e-posta adresi, GSM numarası vb.) kullanmaktadır. Bu verilerin ele geçirilmesi zararlı yazılımlar aracılığıyla yapılabildiği gibi, sözlük yöntemi denilen deneme yoluyla harf dizelerinden anlamlı adresler üretilmesi metoduyla da gerçekleştirilebilmektedir.

Spam mesajların reklam ve pazarlama hususları kapsamında ticari hayatta tüketicileri rahatsız ettiği ve zaman/işlem ve hatta veri kaybına neden olduğu sonucuna ulaşılmakta olup, sorunla mücadele kapsamında, Ticaret Bakanlığınca (TB) konu ile ilgili bir yasa ve bu yasaya dayanarak çıkarılan ikincil mevzuat yürürlüğe konulmuş durumdadır.

Anılan yasa 05.11.2014 tarihinde yürürlüğe giren 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun olup; telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletiler "ticari elektronik ileti" sayılmıştır. Mezkûr Kanunun 6 ncı maddesi uyarınca da; ticari elektronik iletilerin, alıcılara ancak önceden onayları alınmak kaydıyla (opt-in yaklaşımı) gönderilebileceği düzenlenmiştir.

6563 sayılı Kanuna dayanılarak çıkarılan ve 15.07.2015 tarihli, 29417 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'te konuya ilişkin olarak vatandaşların, elektronik ortamda e-Devlet[22] kapısı veya Bakanlığın (TB) internet sitesi üzerinden veyahut yazılı olarak şikâyetçinin ikametgâhının bulunduğu yerdeki il müdürlüğüne şikâyette bulunabilmesi imkânı getirilmiştir.

Bahsi geçen Yönetmelik'in kapsam maddesinde yönetmelik hükümlerinin; 05/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu (EHK) kapsamındaki işletmecilerin abone ve kullanıcılarına; münhasıran kendi mal ve hizmetlerini tanıtmak, pazarlamak ya da işletmesini tanıtmak amacıyla gönderdiği ticari elektronik iletilere uygulanmayacağı hükme bağlanmıştır.

5809 sayılı Elektronik Haberleşme Kanunu'nun (EHK) 50 nci maddesine dayanılarak hazırlanan Pazarlama ve Tanıtım Gibi Amaçlarla Haberleşme Yapılmasına İlişkin

[22] *https://www.turkiye.gov.tr/gtb-ticari-elektronik-ileti-sikayet-sistemi* adresinden ulaşılabilmektedir.

Usul Ve Esaslar metninde de; abone ve/veya kullanıcıların iletişim bilgilerinin (numara, e-posta adresi vb.) işletmeciler tarafından bir mal ya da hizmetin sağlanması sırasında temin edilerek, ispat yükümlülüğü işletmecide olmak üzere ancak abone ve/veya kullanıcılara bilgilendirme yapılması ve ret imkânı sağlanması (opt-out yaklaşımı) halinde sunulan veya benzeri mal ya da hizmetlerle ilgili pazarlama ve tanıtım amaçlı haberleşme yapılabileceği kuralı getirilmiştir.

İlaveten; işletmeciler tarafından bir mal ya da hizmetin sağlanması sırasında elde edilen iletişim bilgilerinin, cinsel içerik iletimi maksadıyla yapılacak haberleşmelerde kullanılabilmesi için izin alınması zorunlu tutulmuştur.

Getirilen yasal önlemlerin sorunu azaltması beklenmekte olup kullanıcıların kişisel temelde alacağı tedbirler de ehemmiyet arz etmektedir. Bu bağlamda, kişilerin spam mesaj olarak gördüğü şüpheli gönderici veya içerik ihtiva eden mesaj/postaları açmaması, açarsa da cevap vermemesi ve işlem yapmaması, işlem yapmadan önce mesajın göndericisi olarak görünen kurum veya şirketlerin yetkili birimleriyle mutlaka sözlü veya yazılı görüşme yaparak bir nev'i konfirmasyon/doğrulama mekanizması geliştirmesinin zarardan korunmak bakımından büyük önem taşıyacağı değerlendirilmektedir.

1.3.3.7 Botnet saldırıları (Botnet attacks)

Botnet terimi; "robot" kelimesinin ikinci hecesi ile "network" sözcüğünün ilk hecesinin birleştirilmesiyle oluşturulmuş ve merkezi bir kontrol noktasına bağlanmış zombi bilgisayar yığınını ifade etmekte olup bu yöntemle, virüs ya da diğer zararlı yazılımların bulaştırılması suretiyle birçok bilgisayar, sahiplerinin haberi olmaksızın uzaktan ve tek bir noktadan kötü amaçlar doğrultusunda yönetilmekte ve kontrol edilmektedir (Turhan, 2010, s.44-45).

Zombi (köle) bilgisayar, 13/07/2014 tarihli ve 29059 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nde; *"herhangi bir amaçla kullanılmak üzere, zararlı*

yazılımlar veya kötü niyetli kişiler tarafından uzaktan yönetilen internete bağlı bilgisayar" şeklinde tanımlanmıştır.

Köle bilgisayarda cihaza, kişilerin rızası ve bilgisi dışında yetkisiz şekilde ve uzaktan yönetim suretiyle erişilerek, cihazın tek merkez üzerinden asıl fail/ler tarafından kullanılması söz konusu olmaktadır. Dolayısıyla zombi/köle edilen cihazlardaki önemli tüm bilgilerin ele geçirilmesinin yanında, bu tür cihazlar aynı zamanda bir başka bilişim suçunu işlemekte araç olarak kullanılmaktadırlar.

Bu metotta, zararlı yazılımın yüklendiği cihazlar açık olduğu sürece, belirli aralıklarla saldırgana ait sunucu ile iletişime geçer ve saldırganın yapmak istediği herhangi bir işlemin olup olmadığına bakar. Zararlı yazılımın bulaştığı cihazlar zararlı bot yazılımında bulunan kodların içeriğine göre bilgileri toplamak üzere saldırganın sunucusuna gönderir ve bu bilgiler saldırgan tarafından uzak masaüstü bağlantısı ile kontrol edilir (Dülger, 2015, s.133).

1.3.3.8 Çöpe dalma (Scavenging)

Atık toplama olarak da adlandırılan bu yöntemde, bilişim sisteminin çalışmasından geriye kalan veri ve bulguların toplanması söz konusu olup, bu işlem yazıcı çıktısının toplanması şeklinde olabileceği gibi, bilişim sisteminde işlem görüp ihtiyaç duyulmadığından silinmiş verilerin gelişmiş yöntemlerle tekrar geri getirilmesiyle elde edilmesi şeklinde de gerçekleşebilmektedir (Doğan, 2014, s.21).

Pek tabii bilgisayardan yazıcıya veya faksa gönderilen fiziksel nüshada (hardcopy) yer alan bilgilerin herhangi bir şekilde ele geçirilmesi veya atıldığı yerden gizlice temin edilmesi kişisel verilerin ihlali durumunu doğursa da, doğrudan bir bilişim suçuna vücut vermeyecektir. Ancak bir bilgisayar veya benzeri işlemleri yerine getirebilen bir cihaz sisteminden, bilişim teknolojilerinin kullanılarak elektronik ortamdaki verilerin (softcopy) çekilmesi, silinse dahi bu bilgilerin özel programlarla ele geçirilmesi gibi durumlarda bilişim suçundan söz etmek mümkün olacaktır.

Bu usulle kişilerin dokunulmaz alanına girilerek, sırlarının masuniyeti ihlal edilmek suretiyle ticari, askeri, istihbari, toplumsal çok kritik sırlar öğrenilebilir, haksız menfaatler elde edilebilir (Kurt, 2005, s.62).

1981 yılında takma ad olarak Captain Zap'i kullanan Pat Riddle'ın, telefon şirketlerinin arkasında topladığı telefon sistemleri hakkında kitapçıklar ve şirket içi bilgi notlarından faydalanarak elde ettiği telefon numaralarıyla Amerikan Hava Kuvvetleri bilgisayarları başta olmak üzere, Pentagon ve Beyaz Saray'ın sistemlerine bağlanması ve bu sistemlerden birçok veri elde etmesi bu yöntemin kullanıldığı önemli örneklerden birisi olarak gösterilebilir (Boğa, 2011, s.47).

1.3.3.9 Tavşanlar ve bukalemunlar (Rabbits and chameleons)

Tavşan olarak nitelendirilen yazılımlar, adını aldıkları hayvan gibi çok hızlı üreyebilmekte ve bulundukları bilişim sisteminin içinde işlemciye sürekli anlamsız komutlar vermek suretiyle normal işleyişi engelleyerek sistemin yavaşlamasına, en nihayet çalışamaz hale gelmesine sebep olmaktadırlar (Dülger, 2015, s.126). O halde bu tür yazılımların bilişim sistemi içerisinde mükerrer şekilde yayılarak, sistemin işlem gücünün zayıflamasına ve boş yere dolmasına yol açtığı söylenebilir.

İşinden atılan bir programcı, işten ayrılırken şirketin bilgisayarına, tek işlevi kendinin tam bir kopyasını üretmek olan "*Sarmaşık*" adında bir program bırakır ve bu program kendini kopyaladıktan sonra 24 saatlik bir uykuya dalar. Bir gün sonra *Sarmaşık*'ın iki kopyası kendilerini tekrar çoğaltır ve bu işlem katlanarak sürüp gider. Sadece iki haftanın sonunda şirket bilgisayarının yan işlevlerinde gecikmeler ve bariz hatalar çıkmaya başlar. Artık belleği *Sarmaşık*'ın tıpatıp aynı 16.384 kopyasını yani 6,5 milyon baytlık bir çöpü barındırmaktadır. 20 gün sonra ise bilgisayarın hiçbir işlem yapamaz hale geldiği görülür. Çünkü belleğini *Sarmaşık*'ın yarım milyondan fazla kopyası kaplamıştır. Görüldüğü gibi tavşan yöntemini kullanan çok küçük ve basit işlevli bir program, çok kısa bir sürede kendisini fark ettirmeden büyük bir şirketin bütün sistemini hizmet veremez hale getirmiştir (Ergün, 2008, s.24).

Bukalemunlar ise, truva atı yazılımının bir türü olup sisteme girmeden önce normal çalışan ve zararsız görüntüsü veren, sisteme girdikten sonra ise hukuka aykırı eylemlerine başlayan, sistemdeki verileri ve kullanıcı ad-şifrelerini kopyalayıp gizli bir şekilde saklayabilen programlardır (Doğan, 2014, s.31). Böylece, truva atında olduğu gibi bukalemunun da önce masum yazılım izlenimi verip, daha sonra adını aldığı hayvanın özelliğinden hareketle rengini belli etmekte olduğu görülmektedir.

Bukalemunların program taklidi tıpkı gerçek yazılımların simülasyonu olan tanıtım (demonstrasyon) programlarında olduğu gibidir ve bir bukalemun her defasında çok kullanıcılı bir sistemde istenilen verilerin girileceği yerleri taklit edecek şekilde dâhiyane bir biçimde programlanır (Kurt, 2005, s.75).

Normal ve zararsız bir program gibi çalışan bukalemun, aslında bir takım hile ve aldatmalar uygulayarak, sistemlerde kullanıcı adları ve şifrelerini, taklit yeteneği sayesinde gizli bir dosyaya kaydederek, sistemin bakım için geçici bir süre kapatılacağına dair bir uyarı verir. Bu sırada bukalemun yazılımını kullanan kişi, bu gizli dosyaya ulaşarak verileri ele geçirip istediği eylemleri gerçekleştirebilir (Turhan, 2006, s.50).

1.3.3.10 Diğer yöntemler

Bölümün başında da ifade edildiği üzere, her suçun işleniş yöntemi farklılık arz edebilir. Özellikle, bilişim ve teknoloji alanında icra edilmesinden ötürü bilişim suçlarında bu metotlar, diğer suçların işleniş biçimi ve yöntemleri bağlamında çok daha fazla çeşitlilik içermektedirler.

Yukarıdaki kısımda bilişim suçlarının modus operandilerinden en yaygın rastlananları ve en etkili örneklerine yer verilmeye çalışılmıştır. Bununla birlikte, konu hakkında doktrinde ve uygulamada; mantık/zaman bombaları, süper darbe, tarama/keşif, sırtlama, yerine geçme, gizlice dinleme, veri aldatmacası, salam tekniği, tuş kaydedici (keylogger) vb. daha birçok usul bulunduğu ifade edilmekte olup daha önce de vurgulandığı üzere her geçen gün bu yöntemlere yenisinin eklenmesi olasıdır.

Nitekim bir yıl öncesine kadar adı duyulmayan ve güncel bir siber tehdit olarak öne çıkan ‘gizli kripto para madenciliği’ (cryptojacking) yönteminde; fail tarafından hedeflenen bilgisayarlara bir kripto para yazılımı yerleştirilerek, bu cihazların hem işlemci güçleri hem elektrik enerjileri gizlice kullanılmakta olup mağdurların sahip olduğu yüksek değerli kripto para unsurları ele geçirilmektedir (CyberMag, 2018).

Bilişim alanındaki gelişmelere paralel olarak; sayılan yöntemlerin de saldırganlar tarafından geliştirilebileceği, teknik ve hukuki önlemlerle işlenmesi zorlaştırılan veya daha iyi usuller altında icra edilebileceği keşfedilen hususlarda birtakım metotlardan vazgeçilebileceği, yine buna maruz kalan kullanıcıların tavrı ile devletlerin yaklaşımına göre tekniklerin her zaman değişime uğrayabileceği göz önünde bulundurulmalıdır.

2 BİLİŞİM SUÇLARININ ULUSLARARASI BOYUTU VE ULUSAL DÜZENLEMELERE YANSIMASI

Bu bölümde bilişim suçlarının sadece ulusal değil hatta öncelikle uluslararası arenada taşıdığı önem ve ilgili önemli çalışmaların detayına yer verilerek bunların yerel mevzuata taşınmasından bahsedilecektir.

2.1 Genel Olarak

Çalışmanın konusu olan bilişim suçları; telekomünikasyon ve bilişim teknolojilerinin hızla gelişmesiyle, sabit veya taşınabilir cihazlar kanalıyla, bilişim sistemleri üzerinden ve ülke sınırlarını aşan mahiyette işlenebilmektedir. Bu kapsamda, verinin sonsuz niteliğinden paylaşım hızına, kontrol ve denetleme zorluğundan mücadele yöntemlerine kadar artık bu tür suçların sadece ulusal bir nitelik taşıdığını söylemek mümkün değildir.

1980'lerin başından beri İktisadi Kalkınma ve İşbirliği Örgütü (OECD), Avrupa Konseyi (AK), BM, Interpol gibi uluslararası organlarca yapılan çeşitli çalışmalar sonucunda, bilişim suçları bağlamında küresel bir farkındalığın oluşturulması ve etkin mücadelenin sağlanmasına çalışıldığı belirtilmektedir (Clough, 2010, s.21).

Global gelişmeler, vatandaşlığın boyutlarını zenginleştirmiş ve sadece ülkesine karşı sorumluluklarının bilincinde olmanın yeterli olmayıp bütün insanlığa karşı kendisini sorumlu hisseden, evrensel bilince sahip vatandaşların yetiştirilmesi gerektiği fikrini ortaya çıkarmıştır. Bu özelliklere sahip olan kişilere de, literatürde "*küresel vatandaş*" (global citizen) denilmektedir (Kan, 2009, s.25-26). Küresel vatandaşlığın konuşulduğu bu devirde ülkelerin idari, hukuki ve teknik altyapılarının da özellikle organize suçlara karşı uyumlu tutulması ve etkin işbirliği içerisinde çalışılması büyük önem arz etmektedir.

Bu çerçevede, uluslararası kuruluşlarca bilişim suçları alanında birçok çalışma gerçekleştirilmiş olup bunlar her geçen gün geliştirilerek, ülkelerin suçla mücadele ve vatandaşlarının haklarının korunması noktasında rehber dokümanlar/uygulamalar oluşturulmaya gayret gösterilmektedir. Bu tür çalışmalar ülkelerin iç dinamiklerinde de yer edinerek, gerekli yasal, idari ve teknik düzenlemelerin tetikleyicisi olmaktadır.

Bu bölümde bilişim suçlarıyla ilgili olarak genel kabul gören uluslararası sözleşme olan Avrupa Konseyi Siber Suç Sözleşmesi (ASSS) ve ek protokollerinden bahsedilerek, sözleşmenin mahiyeti ve içeriğine yer verilip, ülkemize yansımaları ifade edilmeye çalışılacak ve bu suretle Türkiye'de bilişim suçlarının yasal gelişimine değinilecektir.

2.2 Uluslararası Gereklilikler

Günümüz kullanım alışkanlıkları karşısında bilişim suçlarına maruz kalma oranı artmış ve bu durum yukarıda da bahsedildiği üzere ulusal düzenlemeleri aşarak uluslararası düzenleme gerekliliklerine yol açmıştır.

Bilgisayar ağları marifetiyle işlenen suçların kontrolü; suç teşkil eden eylemin elektronik ortamda gerçekleşmesi, internetin kullanıcılarına içinde bulundukları devletin sınırları dışında da hareket etme olanağı sağlaması ve bu tür ağları kullananların kendilerine en uygun hukuki çevreyi seçme imkânına sahip olmasından ötürü zorluk arz etmektedir.

Ülkelerin suçla mücadele birimlerinin teknolojiye hâkim olması ve kısa sürede çok sayıda veriye ulaşabilen bir mücadele sistemine sahip olması ihtiyacında olduğu; dolayısıyla değişen dünya şartlarına uyumlu olarak ülkelerin suçlulardan daha üstün teknoloji ve yeteneğe sahip olması gerektiği ifade edilmektedir (Çam, 2015, s.164).

Bu bağlamda, özellikle yargılama yetkisi kapsamında bu tür suçlarda uluslararası düzenleme yapılması gerekliliği üç ayrı başlık altında irdelenebilir (Weber, 2003, s.426 vd.):

2.2.1 Mevzuat eksikliği

Bilişim sistemi alanındaki aykırı fiil ve sonuçların henüz yasalarında suç olarak belirlenmediği birçok ülke bulunmaktadır. Örneğin 2000 yılının Mayıs ayında dünya çapında 45 milyon bilgisayara bulaşan ve 6.7 ila 10 milyar dolar arasında maddi zarara yol açtığı hesaplanan *"I Love You"* virüsünün ana şüphelisi tespit edilip, Filipinler'de bulunmasına rağmen saldırı anında anılan ülkede bilişim suçlarına ilişkin herhangi bir mevzuat olmaması sebebiyle ceza almamıştır.

Suç ve cezaların kanuniliği ilkesi evrensel bir ceza hukuku ilkesi olması nedeniyle, bir ülkede suç olarak kabul edilmeyen bir husus, failler açısından o ülkeyi sığınılacak liman haline getirmektedir.

2.2.2 Kaynak ve ileri teknoloji eksikliği

Ülkeler kimi zaman da bilişim suçlarının araştırılması hususunda yeterli teknoloji ve kaynağa sahip olmayabilirler. Nitekim Ekim 2002'de merkezi internet kök sunucuları nezdinde koordine edilmiş bir DoS saldırısının gerçekleşmesi ve bu sayının artması üzerine Europol, sınır aşan bilişim suçlarının tetkikini teminen İleri Teknoloji Suç Merkezi kurmuş; ancak merkezdeki çalışmalarda kaynak, teknoloji ve yetersiz personel gibi sorunlar sebebiyle gerekli aksiyon alınamamıştır.

Ülkeler nezdinde, suç faillerini izleyecek, işlenen eylemleri tanımlayıp analiz edebilecek ve ortaya çıkan delilleri sağlıklı şekilde değerlendirebilecek bir altyapının bulunmaması halinde bu tür suçların yaptırıma bağlanması ve önüne geçilmesinde büyük zorluklar yaşanabilecektir.

2.2.3 Uygulanabilir ortak işbirliği hükümlerinin eksikliği

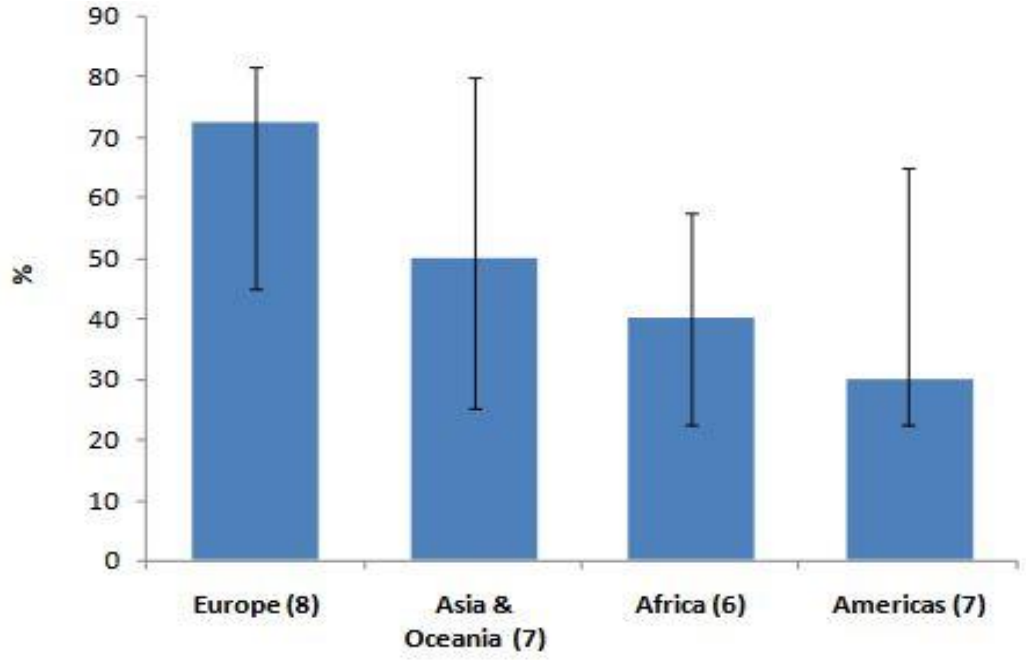
Gerek saldırının yapıldığı gerekse hedef ülkelerin gerekli mevzuata, yeterli soruşturma donanım ve yetkilerine sahip olmalarına rağmen adli takibat, uygulanabilir işbirliği noksanlığından ötürü engellenebilmektedir.

Önemli bir örnek olarak; 2000 yılının baharında uluslararası hackerlar tarafından güvenlik dosyalarının kırılması, kredi kartı numaraları elde edilmesi suretiyle Amerikan bankaları ve kredi kartları sistemlerinde yer alan bilgiler "danışmanlık servisleri" adı altında pazarlanmakta ve kurbanlardan para sızdırılmaktaydı. Sonucunda hedef alınan kişi ve işletmelerin çok büyük zarara uğradığı ve sistemlerinden hackerları uzak tutamadıklarının ortaya çıkması üzerine FBI tarafından Rusya'da ikamet eden iki şüpheli belirlendi. ABD o dönem kırktan fazla karşılıklı adli yardımlaşma anlaşmasına taraf olmasına rağmen; Rusya ile ABD arasında imza edilen iki taraflı anlaşmalarda bilişim suçlarına ilişkin bilgi alışverişlerinde bulunulmasına dair herhangi bir hüküm bulunmamaktaydı. Aynı yılın Kasım ayında bazı Rus otoritelerinin de yardımıyla FBI gizli bir operasyon gerçekleştirdi. Bu operasyonda olay şüphelisi iki hackera ABD nezdinde iş teklifleri gönderildi. Kurgulanmış görüşmelerde FBI, şüphelileri takip ederek sistem şifrelerine ulaşmış, gerekli somut delilleri elde edip adli süreci başlatabilmiştir.

Görüldüğü üzere; bilişim suçları alanında ülkeler arası mevzuatın uyumu, kaynak ve teknoloji etkinliği, yeterli ve donanımlı personelin bulunması yanında hızlı ilerleyen ve küresel alanda karşılıklı açık işbirliğinin sağlanmasını teminen dünya genelini kapsayıcı geniş ve uygulanabilir uluslararası düzenlemeler yapılması gereği hissedilmiştir.

Bilişim suçları ile karşılaşan personelin, bu konunun genellikle "ulus aşırı/sınır aşan/sınır ötesi" bir unsur olduğu yönünde saptamalarının olduğu ifade edilmekte olup; Avrupa, Asya, Afrika ve Amerika kıtalarındaki bazı ülkeler nezdinde gerçekleştirilen bir anket çalışmasında, bu sınır ötesi boyutun en yüksek Avrupa ülkelerinde gözlendiği sonucuna ulaşılmıştır (BM, 2013, s.183):

Şekil 2.1 Bilişim Suçlarının Sınır Aşan Boyutlarının Yüzdesel Dağılımı



2.3 Avrupa Konseyi Siber Suç Sözleşmesi

Amaçları, insan hakları, hukukun üstünlüğü, çoğulcu demokrasi ilkelerini korumak ve güçlendirmek; azınlıklar, ırkçılık, hoşgörüsüzlük ve yabancı düşmanlığı, sosyal dışlanma, uyuşturucu madde ve çevre konularındaki sorunlara çözüm aramak; Avrupa kültürel benliğinin oluşmasına ve gelişmesine katkıda bulunmak olarak özetlenebilen Avrupa Konseyi, 5 Mayıs 1949 tarihinde Strazburg merkezli olarak kurulmuş olup bu Konsey, ülkemizin İkinci Dünya Savaşı'ndan sonra Avrupa ile kurduğu ilk kurumsal bağı temsil etmektedir. Türkiye konseye, kuruluşundan üç ay sonra, Yunanistan ve İzlanda ile birlikte Ağustos 1949'da davet edilmiş ve örgütün kurucu üyeleri arasında sayılmaktadır (Dışişleri Bakanlığı, 2018).

Devletlerin klasik egemenlik fikrine dayalı yersel yetki anlayışı, teknolojinin söz konusu olmadığı, gerçek, yani fiziksel dünyada işlenen suçlar açısından tasarlanmış olsa da, siber suçlarda fail belirli bir devletin yargı yetkisi dâhilinde bulunmakta iken,

failin eylemleri, diğer birçok ülkedeki bilişim sistemlerini ve mağdurları etkileyebilmektedir (Önok, 2013, s.1234).

İnternet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası belge olan Avrupa Konseyi Siber Suç Sözleşmesi belge, özellikle telif haklarının ihlali, bilgisayarla bağlantılı sahtecilik, çocuk pornografisi ve güvenlik ağlarının ihlali konuları üzerine odaklanmakta olup sözleşmeyle ilgili iç hukuk gereklerinin yerine getirildiğinin ilgili Bakanlıklarca bildirilmesi üzerine 10 Kasım 2010 tarihinde Strazburg'da ülkemiz tarafından imzalanmıştır (TBMM, 2012b, s.4).

Anayasamızın 90 ıncı maddesine göre, Türkiye Cumhuriyeti adına yabancı devletlerle ve milletlerarası kuruluşlarla yapılacak antlaşmaların onaylanması şarttır. Bu onay mekanizması ise yine aynı maddede düzenlendiği üzere bir yasa (Uygun Bulma Kanunu) çıkarılması suretiyle yerine getirilebilecektir. Anılan maddenin son fıkrası uyarınca, usulüne göre yürürlüğe konulan uluslararası antlaşmalar normlar hiyerarşisi içerisinde 'kanun' gücünde olmaktadır. Bununla birlikte bunlar hakkında anayasaya aykırılık iddiasıyla anayasal yargı yoluna gidilmesi yani Anayasa Mahkemesi'ne başvurulması da mümkün olmamaktadır.

Mezkûr sözleşme, akde taraf olan devletlerin ilgili mevzuatını uyumlulaştırmayı ve etkin bir uluslararası işbirliğini sağlamayı hedeflemektedir. Nitekim ülke yasaları, yersellik ilkesi gereğince genel olarak ülke sınırları içerisinde uygulanabilmekte; ancak bu suçların coğrafi sınırları aştığı gerçeğinin yanında milletlerarası bir koordinasyonun sağlanması da elzem olmaktadır.

Bu tür suçlarla mücadeleye katkı sağlanması ve vatandaşlarımızın mağduriyetlerini azaltmak açısından söz konusu sözleşme ülkemizce 2010 yılında imzalanmış, 2 Mayıs 2014 tarihinde ise 6533 sayılı Kanunla uygun bulunarak yürürlüğe girmiştir. Bu suretle iç hukukumuzun bir parçası sayılan sözleşmenin uygulanması zorunlu hale gelmiştir. 6533 sayılı Uygun Bulma Kanunu'nun başlığında ise "bilişim suçları" veya "siber suç"

kavramları kullanılmamış, "sanal ortamda işlenen suçlar" ibaresinin kullanılması uygun görülmüştür[1].

Uluslararası kimliği üst düzeyde olan antlaşma, Macaristan'ın başkenti Budapeşte'de 23/11/2001 tarihinde imzaya açılmış; AK üyesi 47 ülkenin 46'sı tarafından imza edilmiş, sadece Rusya Federasyonu tarafından imzalanmamıştır (Council of Europe [COE], 2018a). Bununla birlikte bahsi geçen sözleşme; AK üyesi olmayan ABD, Kanada, Japonya, Avustralya ve İsrail'in de aralarında bulunduğu 14 ülke tarafından da imza edilip yürürlüğe konmuştur[2].

Sözleşmedeki suçlar hem günümüz hem de gelecek teknolojisine uygulanabilir olduğu için, teknolojiden bağımsız bir dil tercih edilmiştir (Erdoğan, 2012, s.67).

2.3.1 Sözleşmenin yapısı, amacı ve içeriği

ASSS, bilişim suçlarına karşı küresel düzeyde kapsayıcı bir belge olarak karşımıza çıkmakta olup, toplamda kırk sekiz maddeden teşekkül dört bölüme ayrılmıştır.

Sözleşmenin açıklayıcı memorandumu/raporu (*explanatory report*) tetkik edildiğinde; sözleşmenin amaçları şu şekilde sıralanmaktadır (CoE, 2001b, s.4):

i. Bilişim suçları ve bu suçlara bağlı fiillere yönelik alanlarda ülkelerin maddi ceza hukuku kurallarının uyumlaştırılması.

---

[1] 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunması Kanunu *(http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler//2014/05/20140502-12.htm/20140502.htm&main=http://www.resmigazete.gov.tr/eskiler//2014/05/20140502-12.htm)*

[2] Konsey üyesi olup söz konusu sözleşmenin yürürlük tarihi uygulaması en geç olan ülkeler; Andorra (Mart 2017), Yunanistan (Mayıs 2017), ve Monako (Temmuz 2017)'dur. Konsey üyesi olmayıp sözleşmenin en geç yürürlüğe girdiği ülke ise Filipinler (Temmuz 2018)'dir. *(https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=3v48WmgI)*

ii. Bu suçların ve bilişim sistemleri kullanılarak işlenen veya delilleri elektronik ortamda bulunan diğer suçların soruşturulması ve kovuşturulması için gerekli olan ulusal ceza usul hukuku (muhakeme) yetkilerinin belirlenmesi.

iii. Hızlı ve etkin bir uluslararası işbirliği rejiminin oluşturulması.

Bu kapsamda sözleşmenin hedefinin kısaca; ortak bir ceza politikasının oluşturulması ile toplumun bilişim suçlarına karşı korunması, özellikle gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi olduğu söylenebilmektedir (Ergün, 2008, s.60).

Sözleşme bölümleri incelendiğinde şekil ve esasa ilişkin (maddi hukuk ve usul hukuku) düzenlemeler yanında yargılama yetkisi ve uluslararası işbirliği hususlarına da yer verildiği görülmektedir. Başlıklar halinde sıralanan konular tetkik edildiğinde ise sözleşmenin; hem doğrudan bilişim suçlarına hem de bilişim yoluyla işlenen suçları içeren, bunun yanında delil toplama dâhil olmak üzere adli bilişime[3] de yer veren, soruşturma-kovuşturma safhalarını da detaylandıran geniş kapsamlı bir metin olduğu söylenebilmektedir.

Birinci bölüm diğer yasal düzenlemelerde olduğu gibi tanımlamalara ayrılmış, sözleşmede yer verilen terimler ve temel kavramlar tanımlanmaya çalışılmıştır.

İkinci bölümde sözleşmeye taraf olacak ülkelerin ulusal düzeyde alması gereken önlemlere yer verilmiştir. Bu çerçevede, önce maddi ceza hukuku düzenlemeleri bağlamında, birtakım suç tipleri tanımlanmakta; ardından da, ceza muhakemesi hukuku düzenlemeleri bağlamında, birtakım şekli tedbirlere yer verilmekte ve yargı yetkisine dair bazı genel ilkeler belirlenmektedir.

[3] Adli Bilişim (*Computer Forensics*); bilgisayarda, bilgisayar çevre birimlerinde ve yan bileşenlerinde, internet, iç ağlar dâhil (intranet) bilişim sistemlerinde yer alan elektronik delillerin araştırılması ve analiz teknikleri kullanılarak incelenmesi sonucu yargılamada suçluluğun ispatında, hukuk davalarında ise anlaşmazlıkların giderilmesinde kullanılmak üzere yürütülen işlemleri kapsayan süreç olarak tanımlanabilmektedir (Orta, 2015, s.152)

Sözleşmenin üçüncü bölümünde yukarıda anılan yetkilerin kullanımı bakımından suçluların iadesi de dâhil olmak üzere uluslararası adli yardımlaşmanın çerçevesi çizilmektedir.

Son kısım olan dördüncü bölümde ise sözleşmenin uygulanmasına dair birtakım usul hükümlerine ve teknik hususlara yer verilmektedir.

2.3.2 Sözleşmede düzenlenen suç tipleri

Sözleşmede işlenen suçlar ve devamında düzenlenen ilave (yan) yükümlülükler ile cezalar, metnin ikinci kısmında yerini bulmuştur. Sözleşmede suçlar dört farklı kategoride ele alınarak dokuz suç tipi olarak tanzim edilmiştir. Bu kategori ve suç tipleri ise aşağıdaki gibi tasnif edilmiştir:

- **1.Kategori**: Bilgisayar veri veya sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine ilişkin suçlar
    - Birinci Kategori Suç Tipleri:
        - Yetkisiz (yasadışı) Erişim (madde 2)
        - Yetkisiz (yasadışı) Müdahale (madde 3)
        - Verilere Müdahale (madde 4)
        - Sistemlere Müdahale (madde 5)
        - Cihazların Kötüye Kullanımı (madde 6)
- **2. Kategori**: Bilgisayarla bağlantılı (bilgisayar aracılığıyla işlenebilen) suçlar
    - İkinci Kategori Suç Tipleri:
        - Bilgisayar Aracılığıyla Sahtecilik (madde 7)
        - Bilgisayar Aracılığıyla Dolandırıcılık (madde 8)

- **3. Kategori**: İçeriğe ilişkin suçlar
    - Üçüncü Kategori Suç Tipi:
        - Çocuk Pornografisi (madde 9)
- **4. Kategori**: Fikri mülkiyet haklarının ihlaline ilişkin suçlar
    - Dördüncü Kategori Suç Tipi:
        - Telif Hakları ve Bağlantılı Hakların İhlal Edilmesi (madde 10)

Sözleşme incelendiğinde bilişim suçlarının sadece bilgisayar ve veriye yönelik fiilleri esas almadığı, bilişim sistemlerinin kullanılması ve özellikle internetin yaygınlaşmasıyla niceliksel olarak ortaya çıkan sorunları da kapsadığı görülmekte olup, sözleşme metninde bu suçların asgari bir uzlaşmayı temsil ettiği ve taraf devletlerin kendi mevzuatında başka suçları da öngörebileceği belirtilmiştir (Ketizmen, 2008, s.53).

2.3.3 Uluslararası işbirliği hükümleri

Sözleşme metninde uluslararası işbirliğine ilişkin genel ilkeler 23 ila 35 inci maddeler arasında kaleme alınmış olup ülkeler arası yardımlaşma, suçluların iadesi, ihtiyaç duyulan verilerin hızlı ve etkin paylaşımı gibi düzenlemeleri içermektedir.

Birden çok ülkenin eşit yargılama yetkisi olduğu durumlarda, suçun işlendiği yerin (*locus delicti*) belirlenmesi ve aynı fiilden ötürü kişinin bir kişinin yalnızca bir kez yargılanması (*ne bis in idem*) prensibinin uygulanması problemleri ortaya çıkabilmektedir (Havuz, 2007, s.54).

Bir ülkede bir işlenen bir bilişim suçunun neticeleri bir başka ülkenin sınırları içerisinde gerçekleşebilecek dolayısıyla bu tür suçların delilleri ulusal sınırları aşan mahiyette olabilecektir. Sözleşme bu durumu öngörerek bilişim suçlarıyla mücadelede işbirliğini öne çıkarmış, sözleşmeye taraf devletlere bu işbirliğini sağlayabilmek amacıyla yargılama yetkilerini ve adli yardım hükümlerini daha özgün bir şekilde düzenleme yükümlüğü getirmiştir (Ünal, 2011, s.143).

Bilişim suçlarının çok uluslu ve sınır aşan suçlar olması itibariyle, deliller ancak işbirliği ve yardımlaşma ile toplanabilecek; bu durumda da birden fazla ülkenin emniyet teşkilatları, kriminal laboratuvarları ve ceza usul yasaları devreye girecek, nihayetinde toplanan delillerin hukuka uygun delil olarak değerlendirilebilmesi için, ilgili ülke ceza usul yasalarının hukuki düzlemde insan haklarını düzenleyen uluslararası bir kısım sözleşmelere uygun olması gerekecektir. Böylece bir ülke tarafından toplanan delil, başka bir ülkenin mahkemesi tarafından değerlendirilerek nihai hükme esas alınacağından, sayılan tüm sebepler neticesinde, bilişim suçlarında delillerin güvenliği ve güvenilirliği ile adaletin isabetli tesisi arasında doğrudan bir bağlantı olduğu aşikârdır (Yetim, 2014, s.184-185).

Sözleşmenin iade hususuna ilişkin 24 üncü maddesinin 7/a düzenlemesine göre; konuya dair herhangi bir anlaşmanın mevcut olmadığı durumlarda, geçici tutuklama veya suçluların iadesi talebinin iletilmesi ve/veya alınmasına yetkili mercilerin AK Genel Sekreterliği'ne bildirilmesi gerekmektedir. Ülkemiz bu kapsamda yetkili makam olarak Adalet Bakanlığı'nı belirlemiştir[4].

Sözleşmenin 27 nci maddesinin birinci fıkrasına göre; taraf ülkelerin aralarında herhangi bir yardım anlaşması olması halinde taraflar, mevcut anlaşmayı dikkate alarak bu konudaki sözleşme hükümlerinin bir kısmının veya tamamının uygulanmamasını kararlaştırabilirler. Ayrıca aynı maddeye istinaden, aralarında

[4] Ülkemizin ve sözleşmeye taraf diğer ülkelerin konu hakkında belirlediği yetkili makamların listesine: *"https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=3v48WmgI"* bağlantısından ulaşılabilmektedir.

yardım anlaşması olmasına rağmen taraf ülkeler, bu konudaki sözleşme hükümlerinin kısmen veya tamamen uygulanabileceğini de kabul edebilirler.

Karşılıklı yardım talepleri hususunda herhangi bir anlaşmanın olmadığı durumlarda, sözleşmenin 27 nci maddesinin 2/c düzenlemesine istinaden bu taleplerde bulunmak, talepleri yanıtlamak, taleplerin gereğini yerine getirmek veya yerine getirecek makamlara bu talepleri iletmekle yükümlü olarak yine Adalet Bakanlığı yetkili merci olarak belirlenmiştir.

Bilgisayar sistemleri ve verileriyle ilgili suçlar konusundaki soruşturma ve davaların yürütülmesi ya da bir suça ilişkin olarak elektronik ortamda delil toplanabilmesi işlemlerine en kısa sürede yardım temin edilmesini sağlamak üzere, haftanın 7 günü 24 saat boyunca iletişime elverişli (açık) bir irtibat noktasının belirlenmesini hükme bağlayan sözleşmenin 35 inci maddesinin birinci fıkrası bağlamında ülkemiz; bu temas noktasını Emniyet Genel Müdürlüğü – Bilişim Suçlarıyla Mücadele Daire Başkanlığı[5] olarak Konseye iletmiştir.

Sözleşmenin bu kısmındaki düzenlemelerin, bilişim suçlarının küresel karakteristiği bakımından uluslararası işbirliği çerçevesinde kritik derecede önemli ve oldukça yararlı olduğu değerlendirilmektedir.

2.3.4 Bilişim sistemleri aracılığıyla işlenen ırkçı ve yabancı düşmanı eylemlerin suç haline getirilmesi için ek protokol

İkinci Dünya Savaşı'ndan sonra yoğun bir göç yaşayan Avrupa, uzun yıllardan beri yabancı işçiler de barındırmaktadır. Özellikle Orta Avrupa ülkelerinde yoğun yabancı nüfusun artışından sonra çok sayıda örgütlü ırkçı eylemler ve gösteriler baş göstermiş, bu örgütlerin birbirleriyle iletişime geçmeleri ve propaganda yapmalarını en kolay,

[5] 28/02/2013 tarih ve B.05.1.EGM.0.65.35539/31772 sayılı Olur'a istinaden Bilişim Suçlarıyla Mücadele Daire Başkanlığının ismi "Siber Suçlarla Mücadele Daire Başkanlığı" olarak değiştirilmiştir. (*https://www.egm.gov.tr/Sayfalar/SiberSuclarlaMucadeleDaireBaskanligi.aspx*)

ucuz ve güvenli yöntemi bilişim sistemleri dolayısıyla internetin kullanımı olmuştur (Dülger, 2015, s.203-204).

Bazı devletlerin ifade özgürlüğünün kısıtlanmasına dönük endişeleri sebebiyle, ırkçılık ve yabancı düşmanlığının bilişim sistemleri aracılığıyla işlenmesinin cezalandırılması konusunda yeterli uzlaşı sağlanamadığından, bu konunun düzenlenmesi esas Sözleşme dışında Ek Protokol şeklinde bir düzenlemeyi gerekli kılmıştır (Önok, 2013, s.1242).

İhtiyaçlara binaen hazırlanan ihtiyari Ek Protokol[6], Fransa'nın Strazburg şehrinde 28/01/2003 tarihinde imzaya açılmış; AK üyesi 47 ülkenin içerisinde Türkiye'nin de bulunduğu 39'u tarafından imzalanmıştır[7]. AK üyesi olmayan ülkelerden ise sadece Kanada ve Güney Afrika tarafından imza edilmiş, Senegal tarafından ise 1 Nisan 2017 tarihinden doğrudan uygulama yoluna gidilerek yürürlüğü sağlanmıştır.

Ek protokol mahiyeti gereği ana sözleşmeden ayrı bir yasal enstrüman olup, herhangi bir ülke ana sözleşmeyi imza edip yürürlüğe koysa dahi ek protokolü imza etme veya yürürlüğe koyma zorunluluğu da bulunmamaktadır.

Türkiye 19/04/2016 tarihinde anılan Ek Protokol metnini imzalasa da henüz kanunla uygun bulma ve yürürlük aşamalarını gerçekleştirmemiştir. AB genişleme politikası kapsamında hazırlanan bir çalışma dokümanında, ayrımcılık yapmama ilkesinin, yasal zeminde yeterince korunmamakta ve pratikte uygulanmamakta olmakla eleştirilen ülkemizin ayrıca, ayrımcılığın genel olarak yasaklanmasını öngören Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 12 No.lu Protokolü'nü de onaylayarak, Irkçılık ve Hoşgörüsüzlüğe karşı Avrupa Komisyonu tavsiyelerini uygulaması gerektiği ifade edilmektedir (Avrupa Komisyonu, 2018, s.38).

---

[6] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems *(https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f* bağlantısından orijinal metine ulaşılması mümkündür)

[7] Söz konusu Ek Protokol'ü imzalamayan ülkeler; Azerbaycan, Bulgaristan, Gürcistan, Macaristan, İrlanda, Rusya, Slovakya ve İngiltere'dir.

Protokol metnine bakıldığında ırk, din, renk, nesil veya ulusal ya da etnik kökene dayanan kişi veya kişi gruplarına karşı; nefret, ayrımcılık, şiddet hususlarını savunan veya teşvik eden her türlü yazılı materyal, herhangi bir görsel ya da bunları temsil eden fikir ve teorilerin bilişim sistemleri aracılığıyla yayılması hususunun engellenmesinin amaçlandığı görülebilmektedir.

Aslında Avrupa'da birçok ülkede bu fiillerin daha önceden gerek mevzuat gerek yargı kararlarıyla yasaklandığı bilinmektedir. Örneğin 2000 yılında Nazi olgusunu öven ve Yahudilere karşı yürütülen soykırım ile II. Dünya Savaşı'nda yapılan diğer zalimce fiillerin kabul edilmediği/yalanlandığında dair mesajların internette yayılması üzerine bunların sansürlenmesi hakkında Alman Federal Mahkemesi kararları bulunmaktadır. Ancak bu şekilde genel kabul gören bir Ek Protokol ile bu konuların ülkeler nezdinde "uyumlaştırılmış" hale geldiği ve gerek ülke içerisinde gerekse ülke dışında sunulsun, yasa dışı her türlü içeriğin engellenmesinin zorunlu tutulduğu belirtilmektedir (Deibert vd., 2008, s.190).

Konusu itibariyle ülkemiz coğrafyasını çok etkilemediği düşünülse de, özellikle Suriye'de süren iç savaş sebebiyle vatanlarını terk etmek zorunda kalan milyonlarca[8] yabancının ülkemize yerleşmesiyle, nüfus yoğunluğumuzun farklılaşması karşısında anılan Ek Protokolün yürürlüğe konulması ile ilgili işlemlerin tekrar gözden geçirilmesinin önem arz edeceği değerlendirilmektedir.

2.3.5 Sözleşmeye ikinci ek protokol ekleme çalışmaları

Tarafların görüş alışverişinde bulunmaları hususunu düzenleyen Sözleşmenin 46 ncı maddesi ile sözleşmenin uygulanması, bilişim suçları ve delillerin elektronik ortamda toplanmasıyla ilgili önemli hukuki, siyasi ya da teknolojik gelişmelerinin etkileri ve

[8] Ülkemizdeki mülteci sayılarına bakıldığında; 2000 yılında 5000'den az olan Suriye vatandaşı sayısının 2017 yılında 3.3 milyona ulaşmasıyla, ülkemizin en yüksek sayıda göç alan ilk 5 ülke arasına girdiği görülmektedir (BM, 2017 s.14). Bu sayının 2019 yılı itibarıyla 4 milyonu aşacağı öngörülmektedir.

sözleşme için ekleme ya da değişiklik yapma imkânı konularında istişarede bulunabilecekleri bir çerçeve yaratılmıştır.

Anılan istişarelerde, Madde 40, 41 ve 42 uyarınca yapılan bildirimler ve çekincelerin etkileri de dâhil olmak üzere, özellikle sözleşmenin yürürlüğü ile uygulanmasında karşılaşılan konular incelenebilecektir.

Bahsi geçen düzenlemeye istinaden konvansiyon komitesi tarafından, sözleşmenin etkin kullanımı ve uygulanmasına olanak sağlanması amacıyla bilgi alışverişinin sağlanması ve gelecek dönemde gerekmesi halinde revizyona gidilmesi konularında 2018 yılı Temmuz ayında birtakım çalışmalar başlatılmıştır (CoE, 2018b).

11 Temmuz 2018 tarihinde Konsey merkezi olan Fransa'nın Strazburg şehrinde başlatılan çalışmalarda, ASSS'ne ikinci bir ek protokol hazırlanması konusunda adım atılmıştır. Bu çalışmalarda hazırlanan taslak metinde; ülkelerin ortak yardımlaşma safhalarındaki isabetsiz ve masraflı tercümeler sorunu ile ortak dil seçimi yanında ağır ve gerçekleşmesi muhtemel riskler için acil ortak yardımlaşma mekanizmalarının işletilmesi gibi konular üzerinde durulmuştur (CoE, 2018b).

İlgili taraflarca söz konusu taslak metine ilişkin görüşlerin ise 15 Eylül 2018 tarihine kadar iletilmesi talep edilmiştir. Toplanacak görüşlerin değerlendirilmesini müteakip 26 Kasım 2018 tarihinde yine Konsey merkezinde (Strazburg/Fransa) istişarelere devam edileceği duyurulmuştur (CoE, 2018ç).

2.4 Türk Hukukunda Bilişim Suçları ve Gelişimi

Bilişim suçlarının sayılan farklı özellikleri karşısında, uluslararası gereklilikler de göz önüne alınarak, ülkemizin küresel dünyada gerek nitelik gerekse nicelik olarak sürekli artış gösteren bu konuyu ceza mevzuatında düzenlemesi ihtiyacı hâsıl olmuştur.

Bu bölüm içerisinde; bilişim suçları kavramının ulusal ceza hukuku içerisine alınması, düzenlemelerin sistematiği, kaynağı ve sebepleri yanında gerçekleştirilen değişiklikler ve günümüz mevcut durumu ile içerik hakkında bilgi verilecektir.

2.4.1 Türk ceza hukukunda bilişim suçlarının düzenleme sistematiği

Bilişim suçlarının düzenlenme şekline mukayeseli hukukta bakıldığında iki farklı sistematik yöntemin genel olarak uygulandığı görülmektedir (Erdoğan, 20, s.92-93):

Birinci sistemde bilişim suçlarına ilişkin yasal çalışmalar 'özel' bir kanun ile düzenlenmektedir. Bu sisteme örnek olarak ABD'de 1986 tarihli Bilgisayar Sahtekârlığı ve Bilgisayarın Kötüye Kullanılması Kanunu (*Computer Fraud and Abuse Act*), İngiltere'de 1990 tarihli Bilgisayarın Amaca Aykırı Kullanımı Kanunu (*Computer Misuse Act*), Hindistan'da 2000 tarihli Bilgi Teknolojileri Kanunu (*Information Technology Act*) bu suç tiplerini özel bir kanun içerisinde incelemişlerdir.

İkinci sistemde bilişim suçlarına ülkenin hâlihazırda 'mevcut ceza kanunu' içerisinde yer verilmektedir. Bu sistemde bilişim suçları toplu ve ayrı bir fasıl halinde düzenlenebilirken, korunan hukuki menfaate göre ceza kanunlarının ilgili bölümlerindeki maddelere birtakım yeni fiillerin eklenmesi veya mevcut suç tariflerinin bilişim suçlarını da kapsayacak şekilde yeniden düzenlenmesi de mümkündür. Fransa, Türkiye ve Lüksemburg gibi ülkelerde bilişim suçları toplu ve ayrı bir fasıl altında yerini bulmuşken; Almanya, Kanada, Japonya ve İsveç gibi ülkelerde korunan hukuki menfaat (değer) ölçüsü öne çıkmaktadır.

Geleneksel (klasik) suçlara ilişkin mevcut normların ceza hukukunun genel ilkelerinin izin verdiği ölçüde, siberuzay[9] ortamında işlenen suçlar için de uygulanabileceği; ancak siberuzay ortamının özgün niteliğinden kaynaklanan ve mevcut normlarla karşılanabilmeleri olanaksız olan ihlaller açısından yine ceza hukukunun genel ilkeleri

[9] Siberuzay kavramı; bilgisayar ve diğer bilgi teknolojileri (IT) cihazlarının bir ağa bağlanması suretiyle, kişilerin birbirleri ile iletişim halinde olduğu, sınırları belli olmayan görünüşte de var olmayan bir ortam/alan olarak tanımlanabilmektedir (McQuade, 2009, s.53).

çerçevesinde yeni hükümlerin ihdas edilebileceği doktrinde belirtilmektedir (Sınar, 2001, s.77). Nitekim ülkemizde de bu mahiyette bir düzenleme mevcuttur.

Ülkemiz ceza mevzuatında sistematik; doğrudan (dar anlamda) bilişim suçlarının ayrı bir fasılda, toplu şekilde ve yeni hükümlerin ihdası şeklinde gerçekleşse de, hukuki değerlerle bağlantılı geleneksel bazı suç tiplerinin içerisinde de bilişim suçlarına ilişkin özel atıflara yer verilmesi sebebiyle (örneğin hırsızlık ve dolandırıcılık) ülkemizde karma bir sistemin benimsendiği söylenebilmektedir (Başbüyük, 2010, s.153).

Konu hakkında düzenleme gerçekleştirilmeden önce bilişim suçları kapsamındaki fiillerin hırsızlık, dolandırıcılık, nas-ı ızrar (mala zarar verme) gibi klasik suç tipleri ile değerlendirilmeye çalışıldığı; çoğu kez suçun unsurlarının örtüşmemesinden ötürü hatalı uygulamaların meydana geldiği veya yasal boşluk sebebiyle bu tür eylemlerin yaptırım dışı kalmasının söz konusu olabildiği belirtilmekte olup, söz konusu düzenlemenin *"Bilişim tekniği çağdaş hayatta büyük süratle yaygınlaştığı için, yerleştirilmiş program, veri ve diğer bütün unsurları en büyük hassasiyetle korumak zarureti bu (babdaki) hükümlerin getirilmesini gerektirmiştir"* gerekçesi ile ilk kez ceza mevzuatımıza dâhil olduğu ifade edilmektedir (Taşdemir, 2001, s.42-43).

2.4.2 765 sayılı (mülga) Türk Ceza Kanunu'nda yer alan bilişim suçları

Bilişim suçlarına yönelik Türkiye'de ilk yasal düzenleme, 765 sayılı ETCK'ya 1991 yılında eklenen *"...bilgileri otomatik işleme tabi tutan sistem..."* ibaresidir. Bundan sonra ortaya çıkan ihtiyaçlar neticesince birçok kanuna bilişim ile ilgili hükümler derç edilmiştir (BTK, 2016c).

Kanun koyucu; 14.06.1991 tarihli ve 3756 sayılı Kanunun 20 nci maddesi ile 765 sayılı ETCK'ya 525 inci maddeden sonra gelmek üzere "*Bilişim alanında suçlar*" ana başlığı altında Onbirinci Bab'ı eklemiştir. Yapılan bu önemli düzenlemede 5 Ocak 1988 tarihli 88-19 sayılı Fransız Ceza Kanunu'ndan esinlenilmiştir (Yazıcıoğlu, 2001, s.31). Söz konusu 525 inci madde, yasa içerisinde a, b, c ve d şeklinde sıralanmış ve ilk üç

maddede suç tipleri ve asıl cezalar yer almışken, son maddede fer'i cezalar hükme bağlanmıştır.

Bilişim suçlarının ceza mevzuatımıza ilk kez 765 sayılı ETCK nezdinde girmesi sebebiyle, güncel ceza mevzuatı içerisindeki bilişim suçlarının işlenmesinden önce ETCK'da yerini bulan bilişim suçları ile ilgili düzenlemelerden kısaca bahsedilecektir.

2.4.2.1 Verilerin ele geçirilmesi ve zarar vermek amacıyla dağıtımı

Bilişim sistemini işaret eden *"bilgileri otomatik işleme tabi tutan sistem…"* ibaresi ile başlayan söz konusu hükümde[10] sistem içerisinde bulunan herhangi bir veri, program ya da benzer diğer bir unsurun ele geçirilmesi suç fiili olarak tanımlanmıştır.

Maddede ele geçirilen unsurun 'hukuka aykırı' şekilde ve mutlaka 'bilişim sisteminden' alınmış somut olmayan bir öğe olması gerekmektedir. Zira bilişim sisteminin tutulduğu donanımın haksız ele geçirilmesinde bu maddede yazılı bilişim suçunun işlenmeyeceğinde tereddüt bulunmamaktadır. Bu nedenle veri, program veya diğer unsurların donanım değil yazılım cinsinde haksız şekilde ele geçirilmesi ile suç sübut bulacaktır.

Hükmün ikinci fıkrasında, sayılan soyut unsurların bir başkasına zarar vermek amacıyla; 'kullanılması' , 'nakledilmesi' veya 'çoğaltılması' hallerinde de maddede yazılı cezanın uygulanacağı belirtilmiştir. Bu bağlamda, maddede sayılan eylemlerden hepsinin değil yalnızca birinin icra edilmesi suretiyle suçun işlenebilmesi mümkündür.

---

[10] **Madde 525/a** – (Ek: 6/6/1991 -3756/21 md.)
Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve bir milyon liradan on beş milyon liraya kadar ağır para cezası verilir.

Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir.

Bu norm ile özel hayatın gizliliği, sırrın masuniyeti ve hatta iletişim özgürlüğü, ayrıca ilgili unsurlar üzerindeki mülkiyet hakkı himaye altına alınmaktadır (Eker, 2006, s.111).

2.4.2.2 Verilere veya sisteme zarar verme ve hukuka aykırı yarar sağlama

Mezkûr maddenin[11] birinci fıkrasında veri veya verinin işlendiği sisteme zarar verilmesi, bozulması suretiyle yararlanma imkânının kısıtlanması veya sona erdirilmesi suç olarak düzenlenmiştir. Bilişim suçlarının işlenme şekillerinden sayılan herhangi bir saldırı tipi (örneğin virüs, truva atı vs.) ile bu suçun işlenebilmesi mümkündür.

Anılan fıkrada; veri ya da bilgileri otomatik işleme tabi tutmuş sistemi tahrip etmek, değiştirmek, silmek ve sistemin işleyişine engel olmak, suçun oluşması için yeterli fiillerden sayılmıştır.

Maddenin ilk fıkrasında hem bilişim sisteminin, hem de bu sistem içerisinde yer alan veriler veya diğer unsurların zarar görmemesi amaçlanmakta olup sistemin ayrılmaz parçası konumunda olmasa da (sistemden ayrı bir şekilde veri depolama özelliğini haiz olan) CD, USB gibi materyaller de öncelikle bilişim sistemi için tasarlandığından suçun konusunu oluşturabilecektir (Karagülmez, 2014, s.155, 157).

Kanuni düzenlemenin ikinci fıkrasındaki suçun oluşması için verilerin kullanılması değil, sistemin kullanılması şart koşulmuş olup manipülasyon (veri işlemi etkileme/yanlış yönlendirme) niteliğindeki hareketler, kredi kartlarının kötüye

[11] **Madde 525/b** – (Ek: 6/6/1991 -3756/22 md.)
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 işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beş milyon liradan elli milyon 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 iki milyon liradan yirmi milyon liraya kadar ağır para cezası verilir.

kullanılması[12], internet bankacılığı işlemleri, şifreli yayın kuruluşlarının yayınlarının bilişim sistemleri aracılığıyla çözülmesi[13] şeklindeki hareketler madde kapsamına alınmıştır (Akbulut Bozdoğan, 2001 s.21-22).

İkinci fıkradaki düzenleme ile ETCK'da yer alan dolandırıcılık, hırsızlık, güveni kötüye kullanma eylemlerinde aranan suç eşyasının taşınabilir somut bir varlık olması gerekliliği ortadan kaldırılmakta ve bilişim suçlarının konusunu oluşturan, somut olmayan nesne niteliğindeki verilerle meydan getirilen eylemler suç haline getirilmektedir (Dülger, 2015, s284).

Esasen ikinci fıkrada yerini bulan suçta korunan değerin, doğrudan bir bilişim suçu anlamında değil, bilişim aracılığıyla işlenen ve kişinin malvarlığı değerlerini hedef alan manada değerlendirilmesi gerektiği düşünülmektedir. Nitekim Yeni TCK'da bu fıkrayı karşılayan suç klasik dolandırıcılık suçunun 'nitelikli' hali olarak isabetli şekilde malvarlığına karşı suçlar alanında düzenlenmiştir.

[12] Yargıtay bu hükmün anılan eylemler bakımından uygulanabileceğini kabul etmişti (YCGK'nun 10.04.2001 tarihli ve 2001/6-30 esas ve 2001/57 sayılı kararı). Ancak bu kez de kartın ele geçiriliş ve kullanılış şekli çerçevesinde bilişim suçunun mu yoksa klasik dolandırıcılık suçunun mu söz konusu olması gerektiği tartışılmış, nihayetinde yeni TCK'nın 245'inci maddesindeki düzenleme ile bu tartışma sonlanmıştır (Erdağ, 2010, s.295).

[13] ETCK döneminde uygulamada şifre çözücü cihazların, bunları kiralayan şirketlerle yapılan anlaşmalara aykırı olarak başkalarının yararına sunulması fiileri ceza davalarına konu olsa da mahkemeler konunun cezai olmayıp hukuki nitelikte olduğundan bahisle açılan ceza davalarını reddetmekteydi. Bu konudaki ihtiyaç ise yeni TCK'nın 'karşılıksız faydalanma suçu' kapsamındaki cezai sorumluluk ile çözülebilmiştir (Karakehya, 2009, s.10).

2.4.2.3 Sahte belge oluşturulması ve kullanılması amacıyla verilerde tahrif

Bahsi geçen düzenlemede[14] yer alan suç tipi esasen girişindeki cümleyle oldukça sınırlayıcı niteliktedir. Zira madde; "*hukuk alanında delil olarak kullanılmak maksadıyla*" ibaresiyle ardından gelen diğer eylemleri, ancak bu saikle icra edilmesi halinde cezalandırılacağı şeklinde kısıtlamaktadır.

Söz konusu maddede yer alan kısıtlayıcı bu ibare, esasen bu suç tipinin manevi unsurlarından sayılan "özel kast" hususunu işaret etmektedir. Bu çerçevede, her somut olayda yargı merci tarafından sahte belge oluşturmanın asıl amacının araştırılarak hükme ulaşılması gerekecektir.

Anılan hükümde iki ayrı suç tipi düzenlenmiş olup bunlardan ilki, sahte belgenin tanzimi amacıyla bilişim sistemlerine veri veya diğer unsurların yerleştirilmesi (yaratılması) ya da mevcut verilerin bozulması iken diğeri, tahrif edilen verilerle oluşturulan belgelerin bilerek ve istenerek (rıza ile) kullanılmasıdır. Maddede sayılan iki suç tipinin cezaları da gerek alt gerek üst sınırları yönünden ayrılmış durumdadır.

İzah edilen suçlardan ilki aslında klasik evrakta sahtecilik suçuna benzemekle birlikte, aradaki fark fiziki eylemlerle (kazıma, el ile yazma vb.) yapılan bir müdahale dışında bilişim sistemi üzerindeki eylemlerle tahrifatın sağlanmasıdır. Mezkûr suçun gerçekleşmesi için bir bilişim sistemine girilerek sahte belgenin hazırlanması yeterli olup tanzim edilen sahte belgenin kullanılması zorunluluğu bulunmamaktadır (Nacar, 2010, s.74).

Sayılan maddede yer alan ikinci suç türünde ise bilişim sistemine girilmek suretiyle veri işlemek veyahut mevcut veriyi bozmak fiillerinden biri ile oluşturulan sahte belgenin, sahtelik niteliğinin 'bilinmesi' şart koşulmuştur. Yapılan düzenlemeden,

[14] **Madde 525/c** – (Ek: 6/6/1991 -3756/23 md.)
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.

tahrifatı hem yapıp hem de kullanan kişilerle birlikte, tahrifatı bizzat yapmasa da bunun yapıldığını bilerek kullananların da madde kapsamında değerlendirileceği anlaşılmaktadır (Kurt, 2005, s.122).

2.4.2.4 Ek yaptırımlar (Fer'i cezalar)

ETCK'nın 525 inci maddesinin son düzenlemesi olan 525/d maddesinde[15] ilk üç maddede olduğu gibi ayrı herhangi bir bilişim suç tipi ve asli bir ceza belirlenmemiş, ancak bu suçları işleyen kişilere karşı fer'i nitelikte (asıl hükmedilen cezanın yanında) ilave cezaların uygulanması öngörülmüştür. Düzenlemenin lafzına bakıldığında cümlenin "...*verilir*" ifadesi ile sonlandığı görülmekte, ceza hâkimine bu konuda herhangi bir takdir yetkisi tanınmadığı ve yazılı durumlarda her halükarda bu yan cezalara da hükmedilmesinin zorunlu olduğu sonucuna ulaşılmaktadır.

Madde metninde sadece Kanunun 525/a ve 525/b maddelerindeki hükümleri ihlal eden kişilerin; meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten belli bir süre men edilmesi düzenlenmiştir. Anılan maddede 525/c maddesinde yer alan suç tiplerini icra eden kişilere karşı neden 525/d'de yazılı fer'i cezaların uygulanmayacağı ise açık olarak yer almamıştır.

Kanımızca 525/c maddesinde yazılı fiillerin işlendiği alan da bilişim sistemi olduğundan ve 525/c'de yazılı fiillerin de bir meslek veya sanatın icrası sırasında işlenebilmesi söz konusu olduğundan bu maddenin yan cezaların kapsamına alınmaması bir eksiklik olmuştur. Bununla birlikte; bilişim sistemleri kullanılarak oluşturulan hukuka aykırı belgeyi, bu niteliğini bilerek kullanan kişilerin durumunu düzenleyen 525/c'de yer alan ikinci suç tipi kapsamında, bu suç faillerinin sahte belgeyi kendisinin yaratmaması koşuluyla fer'i cezadan bağışık tutulmuş olması da o

[15] **Madde 525/d** – (Ek: 6/6/1991 -3756/24 md.)

525 a ve 525 b maddeleri hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak, meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma cezası da verilir.

dönem için sistematiğe daha uygun bir düzenleme olabilirdi. Nitekim bu kişinin suçun bilişim ortamında işlenmesi aşamasına iştirak etmeyip, bir başkası tarafından hukuka aykırı oluşturulan sahte belgeyi sadece kullanmış olması mümkündür.

Ayrıca 765 sayılı Kanunun 25 inci maddesine göre, muayyen bir meslek ve sanatın tatili hususu üç gün ila iki yıl arasında sınırlandırılmış olup, 525/d düzenlemesinde 25 inci maddede sayılı azami süreye aykırı olarak 'üç yıla kadar' meslek ve sanatın icrasının tatili cezası verilebilmesinin bir eksiklik olduğu ifade edilmektedir (Karagülmez, 2014, s.164).

2.5 5237 Sayılı Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları

1926 yılından beri kullanılmakta olan ve sayısız değişiklik geçiren 765 sayılı ETCK, özellikle 1985 yılından itibaren yoğunlaşan yeni bir ceza kanunu yapma gayret ve girişimleri neticesinde 1 Nisan 2005 tarihinde yerini 5237 sayılı YTCK'ya bırakmış olup bahsi geçen kanunla birlikte bilişim suçları da çağın gereklerine göre yorumlanarak ilgili kanun maddeleri yeniden düzenlenmiştir (Kızıltan, 2007, s.55).

Yeni TCK'da, özel hükümleri içeren suç tipleri ve yaptırımların yer aldığı ikinci kısımda, devleti önde tutan anlayıştan sıyrılarak bireyin ön plana çıkarıldığı ve Avrupa'nın modern ceza kanunlarına sistematik uyumun sağlandığı belirtilmektedir (Avcı, 2004, s.211).

Bu kısımda ulusal mevzuatımızda hâlihazırda geçerli ve genel kanun niteliğinde olan 5237 sayılı Kanunda düzenleme alanı bulan bilişim suçları mahiyetindeki düzenlemeler ve 765 sayılı Kanun ile aralarındaki farka kısaca değinilecektir.

2.5.1 Genel bilgi

Bilişim suçlarının, doktrin, uygulama ve yargı kararlarında; doğrudan (gerçek) bilişim suçları ve dolaylı (bilişim bağlantılı) bilişim suçları biçiminde bir tasnife tabi tutulduğu

çalışmamızda belirtilmişti[16]. Nitekim 5237 sayılı mer'i ceza yasamızda da ayrı bir başlık altında dar anlamda (doğrudan) bilişim suçları tanzim edilmiş, bunun yanında, birtakım geleneksel suçların içerisine bilişim bağlantılı yollarla icra edilebilecek fiiller ve sonuçları derç edilmek suretiyle bir sistematik geliştirilmiştir.

5237 sayılı Türk Ceza Kanunu'nun Üçüncü Kısmında "Topluma Karşı Suçlar" ana başlığı altında düzenlenen suç tipleri on grup suçtan teşekküldür. Bilişim suçları, "Bilişim Alanında Suçlar" başlığı ile bu kısmın 10 uncu bölümünde, 243 ila 246 ncı maddeler arasında yerini almaktadır.

2.5.2 Bilişim alanında suçlar bölümünde düzenlenen suç tipleri

5237 sayılı YTCK ile *"Bilişim Alanında Suçlar"* başlığı altında 243, 244 ve 245 inci madde kapsamında üç ana suç tipi düzenlenmiş, 2016 yılında yeni bir suç tipi söz konusu başlık içerisine derç edilmiş ve konuyla ilgili son hüküm olan 246 ncı madde ile de tüzel kişiler hakkında cezai tedbirlere yer verilerek bölüm sonlandırılmıştır.

Bu çerçevede anılan Kanunda yer alan bilişim suçları kenar başlıkları aşağıdaki gibidir:

- Bilişim sistemine girme (m.243)
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme (m.244)
- Banka veya kredi kartlarının kötüye kullanılması (m.245)
    - Yasak cihaz veya programlar (m.245/A)
- Tüzel kişiler hakkında güvenlik tedbiri uygulanması (m.246)

Yukarıda tadat edilen suçlar, çalışmamızın üçüncü bölümünde her suç tipi bakımından ayrı ayrı ve detaylıca inceleneceğinden bu kısımda ayrıntıya yer verilmeyecektir.

[16] Bkz. Bölüm 1 - Başlık 1.1.4 *Bilişim Suçlarının Sınıflandırılması*

2.6 Eski ve Yeni Türk Ceza Mevzuatı Kapsamında Bilişim Suçlarının Karşılaştırılması

5237 sayılı TCK'nın ikinci kitap, üçüncü kısım, onuncu bölümünde yer alan bilişim suçları; korudukları hukuksal değer gözetilmeksizin, bilişim ortak paydası altında toplanarak ayrı bir fasılda toplu olarak tasnif edilmiş olup bilişim sistemleri kullanılmak suretiyle işlenen diğer (dolaylı) bilişim suçlarına ise korudukları hukuksal değer gözetilerek yer verilmiştir (Yaycı, 2007, s.67).

Klasik suçlara derç edilen bilişim ile ilişkilendirilebilecek suç tiplerine örnek; YTCK'daki m.142/2-e'de düzenlenen "*bilişim sisteminin kullanılması suretiyle nitelikli hırsızlık suçu*" ve 158/1-f'de düzenlenen "*Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçu*" verilebilir.

ETCK'da bulunmayıp ondan farklı olarak, YTCK'nın 245 inci maddesinde düzenlenen "*Banka ve kredi kartlarının kötüye kullanılması suçu*" açısından bir ayrım yapılmayarak, koruduğu hukuksal değer gözetilmeksizin bilişim sistemlerine karşı suçlar bölümünde düzenlendiği belirtilmektedir (Uçar, 2014 s.48). Bu suç tipinin koruduğu yasal menfaatin farklı olduğu kanaati ile bu suçun sistematik açıdan daha doğru olabileceğinin değerlendirildiği başka bir başlık altında düzenlenmesi gerektiğine dair tartışma/eleştirilere bu suç tipinin ayrıntılarıyla inceleneceği üçüncü bölüm içerisinde yer verilecektir.

5237 sayılı Kanun ele alındığında ilk düzenleme alanı bulan suç tipinin 'bilişim sistemine girme' olduğu görülmektedir. Bu suç tipi her ne kadar 765 s. Kanun'da yer alan 525/a maddesine benzetilebilse de ETCK'da sisteme sadece girip çıkılması (güvenlik duvarı vb. tedbirler aşılarak dahi) herhangi bir suç oluşturmamakta çünkü verinin 'ele geçirilmesi' şart olarak sayılmaktaydı. Böylece herhangi bir verinin elde

edilip edilmediğine bakılmaksızın hukuka aykırı bir bilişim sistemine girilmesi 5237 s. YTCK ile hüküm altına alınmıştır[17].

İlaveten 765 sayılı ETCK'da yer alan *"bilgileri otomatik işleme tabi tutan sistem"* ibaresi, 5237 sayılı YTCK'da isabetli olarak *"bilişim sistemi"* kavramı ile değiştirilmiş; böylece bu alandaki düzenlemeler, veri iletişimi sağlayan (cep telefonları dâhil) tüm cihaz ve sistemleri kapsayacak şekilde kaleme alınmıştır (Değirmenci, 2005, s.199).

Yine ETCK'da bulunmayıp ondan farklı olarak, YTCK'nın 245 inci maddesinde *"Banka veya kredi kartlarının kötüye kullanılması"* kenar başlıklı suç tipi de kendisine yeni yasada düzenleme alanı bulmuştur.

Ayrıca ETCK'nın bilişim suçlarını düzenleyen hükümlerinde geçen 'program', 'veri' veya 'herhangi bir unsur' kavramları yerine YTCK'da sadece 'veri' ibaresi kullanılmıştır. 5237 s. Kanunun 243 üncü maddesinin gerekçesinde, sistem içindeki bütün soyut unsurların veri terimi kapsamında sayıldığı açıkça ifade edilmiştir (TBMM, 2016a).

Eski ve yeni Türk ceza mevzuatında yer alan bilişim suçlarının hükümler temelinde kıyaslandığı tablo ise aşağıda sunulmaktadır:

[17] Bilişim sistemine girme suçu; 1997, 2000 ve 2003 tarihli Ceza Kanunu Ön Tasarıları'nda sürekli olarak öngörülse de bir türlü yasalaşamamış; YTCK ile 2005 yılında ancak yürürlüğe konabilmiştir (Kurt, 2005, s.136)

Tablo 2.1 ETCK ile YTCK'da Bilişim Alanında Düzenlenen Suçların Madde Bazında Karşılaştırılması

765 Sayılı ETCK	**5237 Sayılı YTCK**
m. 525/a-1	m.135, m.136
m. 525/b-1	m. 244/1-2
m. 525/b-2	m. 158/1-f, m. 142/2-e, m. 244/4, m.245
m. 525/c	Doğrudan karşılığı olmamakla birlikte; bilişim sistemi nezdinde işlenmesi şartıyla ve uygulanabildiği ölçüde m.204-208 arasındaki hükümler ile m.245/A
-	m.243
-	m.245
m. 525/d	-

3 5237 SAYILI TÜRK CEZA KANUNUNDA YER ALAN BİLİŞİM ALANINDA SUÇLAR (DAR ANLAMDA/DOĞRUDAN BİLİŞİM SUÇLARI ve CEZALARI)

Ekonomik ve sosyal alanlarda teknoloji kullanımının artık alternatiften öte zorunluluk olduğu bir çağda yaşadığımız aşikârdır. Nitekim fiziksel olarak bulunulan yerden ayrılmadan kişinin; ailesi ve tanıdıklarıyla bilişim ve haberleşme teknolojilerinin sağladığı avantajla yazılı, sesli ve görüntülü görüşebildiği sosyal medya araçlarını kullanması, iş başvurusunda bulunması, bankacılık ve alışveriş faaliyetlerini sürdürmesi, vergi ve benzeri mali yükümlülüklerini ifa etmesi, adli sicil kaydı, askerlik yükümlülüğü, sigortalı hizmet süresi vb. hizmetlere ilişkin belge edinmesi, hatta makineden makineye iletişim cihazları (M2M) ile irtibat kurarak akıllı ev eşyalarını harekete geçirmesi ve sayılması zor daha birçok imkâna günümüz teknolojisinde ulaşmak mümkündür.

Kavram olarak ister 'bilişim alanında suçlar', ister 5237 sayılı TCK'nın gerekçesindeki gibi 'bilişim sistemlerine karşı suçlar', ister 'bilişim suçları' veya başka bir isimlendirme kullanılsın; bilgisayar sistemleri ve internetin hiç olmadığı kadar 'gerçek' olduğu ve 'sanalın' veya 20. yüzyılın ikinci yarısından itibaren etkisi hissedilmeye başlanan sosyo-ekonomik dönüşümün beşeri hayatın bir parçası olmasının sonucu olarak, birçok alan yanında elbette hukuk alanında özellikle ceza hukukunda himayenin konusu olarak kanun koyucular, araştırmacılar ve uygulayıcılar bakımından farklı düzenlemelerin, değişik tartışmaların ve uygulamaların yapıla geldiği genellikle 'eski yapı' üzerine inşa edilmeye çalışılan, zengin, karmaşık, çetrefil, aynı zamanda zemini kaygan yeni bir hayat alanı ortaya çıktığı ifade edilmektedir (Hafızoğulları ve Özen, 2016, s.443).

Bu kapsamda 20. yy.'ın son çeyreğinde ortaya çıktığı genel kabul gören bilişim suçlarının, ülkemiz mer'i ceza mevzuatındaki durumuna maddeler bazında, uygulama ve yorumlamada yardımcı olacak ilgili yargı kararlarının da analizine yer verilmek suretiyle bu bölümde detaylı şekilde değinilecektir.

3.1 Bilişim Sistemine Girme

Bilişim sistemine girme suçu, 5237 sayılı Türk Ceza Kanunu'nda bilişim suçlarının ayrı bir başlık altında düzenlendiği ikinci kitabın, "Topluma Karşı Suçlar" üst başlıklı üçüncü kısmının, "Bilişim Sistemlerine Karşı Suçlar" başlıklı onuncu bölümünün ilk maddesinde (m.243) düzenleme alanı bulmuştur. Bahsi geçen kanuni düzenlemenin metni ise aşağıdaki gibidir:

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

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(4) ***(Ek: 24/3/2016-6698/30 md.)*** *Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*

Bilişim sisteminin ve verilerin gizliliği ile güvenliğinin (dokunulmazlığının) ihlaline ilişkin düzenlenen bu suç tipi, öncelikle bir bilişim sistemine girmeyi gerektirmektedir. Söz konusu 'giriş' eyleminin, her ne kadar madde kenar başlığında 'yetkisiz' vb. bir ifade yer almasa da 'hukuka aykırı' bir şekilde gerçekleşmesi gerektiği aşikârdır.

5237 Kanunun gerekçesinde, bilişim sistemi kavramı açıklanmış; *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma*

imkânı veren manyetik sistemlerdir[1]*"* şeklinde ifade edilmiştir (Adalet Bakanlığı, 2005; TBMM, 2016a). ASSS ise bilişim sistemini; bir veya birçok unsuru, bir programın işleyişi aracılığıyla verilerin otomatik işleme tabi tutulmasını sağlayan, birbirine bağlanmış veya benzer bir veya birden fazla cihaz olarak tarif etmektedir (CoE, 2001a).

ASSS'nin 2 nci maddesinde bu suçu karşılayan 'yasadışı erişim' başlığı altında; bilişim sisteminin tamamı veya bir kısmına kasten ve hukuka aykırı olarak erişilmesinin suç olarak tanımlanması kapsamında, ilgili yasal düzenlemelerin yapılması ve gerekli önlemlerin alınması vurgusu yapılmaktadır.

Günümüzde en sık karşılaşılan bilişim suçlarından birisini bilişim sistemlerine yetkisiz erişimler oluşturmaktadır (Kadir, 2010, s.626). Her bilişim suçunun, öncelikle bilişim sistemine bir şekilde erişimi zorunlu kılmasından ötürü bu tespite katılmak mümkündür.

Bilişim sistemine girme suçu ile bir nevi "engelleme suçu" yaratılmak istenmektedir. Zira bilişim suçlarının büyük bir çoğunluğu sisteme girilmek suretiyle başlamaktadır (Erdoğan, 2010, s.1365)

3.1.1 Suçla korunan hukuki değer

Çalışmamızın *"Suç Terimi"* kenar başlıklı bölümünde de ifade edildiği üzere, suç oluşturan her eylem, bir hukuksal değerin ihlaline vücut vermektedir.

Ketizmen; bu maddenin kapsadığı hukuki konuda asıl olan yaklaşımın 'malvarlığına ilişkin' bir değerin korunması olduğu, dolayısıyla suçun hukuki konusunun mameleki bir değer olarak öngörüldüğünü ileri sürmekte, diğer korunan özel hayatın gizliliği unsurlarının ikincil planda olduğunu belirtmektedir (2008, s.94 vd.).

[1] *"…manyetik sistemler…"* ibaresine karşı eleştiriler için bkz. Bölüm 1 - Başlık 1.1.3 *Bilişim Sistemi*

Erdoğan; bu maddede korunan hukuki yararın ‘karma’ nitelikte olduğunu dile getirmekte ve bunları toplum düzenini koruma, özel hayat ve haberleşmenin gizliliği, sistem sahibi ve kullanıcının menfaatleri, başka suçların işlenmesinin önlenmesi ve bilişim sisteminin güvenliği şeklinde sıralamıştır (2012, s.120 vd.).

Ceza mevzuatının bu suçu düzenlerken muhafaza altına almak istediği yasal menfaat; ‘bilişim sisteminin güvenliği’ olup bu sisteme hukuka aykırı erişimin engellenmesiyle, sistemin maliki veya kullanıcısı olan kişilerin veri gizliliği, özel hayatın dokunulmazlığı, emniyet duygusu vs. türden çok sayıdaki farklı çıkarları koruma altına alınmaktadır (Dülger, 2015, s.348). Nitekim esas değer verilen bilişim sisteminin güvenliğinin korunmasıyla, kişinin malvarlığı değerleri de dâhil olmak üzere diğer çıkarları evleviyetle muhafaza altında tutulmuş olacaktır.

Buna paralel olarak ASSS’nin açıklayıcı raporu incelendiğinde; bu suçun bilişim sistemlerine (gizlilik, bütünlük, kullanıma açıklık dâhil) yönelik tehlikeli tehdit ve saldırılar şeklindeki eylemleri kapsadığı belirtilerek; koruma ihtiyacının, gerçek ve tüzel kişilerin bilişim sistemlerini rahatsız edilmeden ve engellenmeden yönetme, işletme ve kontrol etme ihtiyaçlarını yansıttığı ifade edilmektedir. Bu kapsamda sadece izinsiz girme eyleminin ilke olarak başlı başına yasadışı olması gerektiğinin altı çizilmektedir (CoE, 2001b, s.9).

Bir bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalınmaya devam edilmesinde, doğrudan kişi ya da kuruluşa zarar verilmemiş olsa da; güvenlik sistemlerinin kırılarak bilişim sistemine girilmesi ile bu sistemin doğruluğu ve erişilmez olduğuna ilişkin güvenilirliği kapsamındaki yasal faydaya zarar verilmektedir (Çekiç, 2006, s.89).

3.1.2 Suçun maddi unsurları

3.1.2.1 Fail ve mağdur

TCK'nın *"Faillik"* kenar başlığını haiz 37 nci maddesinde suçun kanuni tanımında yer alan fiili gerçekleştiren kişi veya kişilerin fail olarak sorumlu tutulacağı hükme bağlanmıştır.

Bu suç; maddenin lafzı tetkik edildiğinde suçu işleyen yani fail açısından herhangi bir özel nitelik arz etmemektedir. Madde metninde *"...giren veya ... kalmaya devam eden kimse"* ibaresinin kullanıldığı görülmektedir. Bu nedenle bu suç 'herkes' tarafından işlenebilecektir.

Suçun işlenebilmesi için failin bilişim sistemleri nezdinde belli bir yetkinliği bulunması gerektiği düşünülmekle birlikte, failin mutlaka böyle bir yeteneğe sahip olması veya bunu meslek olarak sürdürmesi zorunlu olmadığından, bu yetkinlik suçun bir unsuru olarak görülmemektedir. Zira bu konuda basit düzeyde bilgisi veya ilgisi olan ve suç işleme güdüsüne sahip herhangi biri tarafından mezkûr suçun icra edilebilmesi mümkündür.

Ceza hukukunda özellikle anayasada yerini bulan suçların kanuniliği ve şahsiliği ilkesi[2] başta olmak üzere; kusurluluk ile iradi hareket unsurları birlikte gözetildiğinde tüzel kişilerin suçun faili olamayacağı, dolayısıyla cezai sorumluluklarının da bulunmadığı kabul edilmektedir. Nitekim TCK'nın 20 nci maddesinde tüzel kişiler hakkında ceza yaptırımının uygulanamayacağı; ancak suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımların saklı olduğu hükme bağlanmıştır. Anılan güvenlik tedbirleri aynı yasanın 60 ıncı maddesinde yer almakta olup, yargılama sonucunda suçun yararına işlendiği sabit olan tüzel kişiliğe, sayılan tedbirlerin tatbiki söz konusu olabilecektir.

[2] Anayasa m. 38

Örneğin; iki farklı tüzel kişiye ait iki ayrı internet alışveriş (e-ticaret) sitesi sahibi tüzel kişilerden birinin temsilcisinin, rakip internet alışveriş sitesi sistemine bir 'hacker' ile anlaşarak girmesi durumunda hacker ve tüzel kişi temsilcisinin şahsi cezai sorumluluğu olduğu gibi; yararına suç işlenen ilgili tüzel kişi hakkında da güvenlik tedbirine hükmedilmelidir (Gürocak, 2010, s.9).

Adli mercilerce bilişim suçları ile ilgili olarak ilk takip edilecek muhatap kişi, internet hizmetini alabilmek için servis sağlayıcı ile sözleşme imzalayan "abone" olmaktadır. Ancak her zaman ilgili cihaz sahibi veya abone suç teşkil eden fiili icra eden kişi olmamakta, bu nedenle cezai sorumluluk ve yaptırıma maruz kalma konusunda isabetsizlikler yaşanabilmektedir. Bu durumlara en uygun örnek; abonenin cihazı veya internet/modem şifresini üçüncü kişilerle paylaşması durumudur.

Kablosuz internet kullanımı nedeniyle abone harici kişilerin ortak kullanımı yanında yeterli IP numarası olmadığından NAT (ağ adresi dönüşüm) uygulaması yapılmakta ve faillerin IP adresleri üzerinden tespiti imkânsızlaşmaktadır (Gül, 2016, s.42).

Fail veya faillerin belirlenebilmesini teminen delillendirme hususunun büyük önem arz ettiği şüphesizdir. Ancak bilişim suçlarında fiziksel kanıtların yanı sıra, adli bilişim disiplininin konusunu teşkil eden "dijital deliller" büyük rol oynamaktadır. Dijital delillerde aşağıdaki konuların göz önünde bulundurulması gerektiği ifade edilmektedir (Turan, 2016, s.79):

- Fiziksel delilleri (örneğin parmak izi) ya da DNA gibi delilleri de bünyesinde bulundurabilirler
- Yargı sınırlarını kolay ve çabuk aşabilirler
- Kolay değiştirilip, bozulabilirler
- İşletilebilir ve imha edilebilirler
- Zamana karşı hassas olabilirler

Sayılan sebeplerle suç konusu cihaz, sistem ve veriler üzerinde kanıt elde etme süreçlerinin 'derhal' işletilmesi, arama-kopyalama-el koyma gibi tedbirlerin de yetkin personel tarafından eksiksiz şekilde icra edilmesinin elzem olduğu değerlendirilmektedir.

Burada, elektronik delillerin hukukiliği konusunda Yargıtay'ın (16. Ceza Dairesi) güncel tarihli (14.7.2017) bir kararında (E.2017/1443-K.2017/4758) önemle vurgulanan hususlara değinmek uygun olacaktır. Bahsi geçen karara göre:

- **Ceza Muhakemesinin amacı** usul ve kuralların ön gördüğü ilkeler doğrultusunda **maddi gerçeğin her türlü şüpheden uzak bir biçimde kesin olarak belirlenmesi**dir.
- Ceza muhakemesinde **hangi hususun hangi delillerle ispat olunacağı konusunda bir sınırlama bulunmamaktadır**.
- Avrupa İnsan Hakları Mahkemesi'nin yerleşik içtihatlarına göre **kanıtların kabulü ve değerlendirilmesi** öncelikle **ulusal mahkemelerin görevidir**.

Üst mahkemenin kararı analiz edildiğinde, somut olaydaki gerçek durumun ortaya çıkarılması hususunda, yerel mahkemelere delil ve değerlendirme (kanaat) serbestisi tanındığı görülmektedir.

Uygulamada karşılaşılan hatalardan bir tanesi de, toplu internet kullanımının bulunduğu yerlerde bilişim suçu işlenmesi halinde IP adresinin üzerine kayıtlı olduğu kişinin suçun faili olarak kabul edilip cezalandırılması olup, IP adresi üzerine kayıtlı olan kişinin eylemle hiç alakası olmadığı halde üçüncü bir kişinin eyleminden sorumlu tutularak cezalandırılması hukuka aykırı olarak görülmektedir (Bikirli, 2015, s.13). Konuya ilişkin olarak Yargıtay 11. Ceza Dairesi'nin 14.05.2010 tarihli ve E.2009/23397, K.2010/6054 sayılı bozma kararı da aşağıdaki gibidir:

"Sanığın, … İnternet Cafe'nin sahibi olduğu, iş yerinde 70 adet bilgisayarın gözetimi ve denetimi için gerekli hassasiyeti göstermemesi sebebiyle kusurlu olduğu gerekçesiyle cezalandırılmasına karar verilmiş ise de adı geçen işyerinin IP numarası 81… 170 olan bilgisayardan müştekinin elektronik posta adresine girilmesinden ***sanığın sorumluluğu olmamasına rağmen****, atılı suçtan beraatine dair karar verilmesi gerekirken yazılı şekilde cezalandırılması..."*

Mezkûr bozma kararının **suç ve cezaların şahsiliği** gibi oldukça kritik bir ilkenin korunması kapsamında isabetli olduğu değerlendirilmekte olup her somut olayda asıl failin araştırılarak, sorumluluğu bulunmayan kişilere cezai sonuçların yüklenmesinden kaçınılması gerekmektedir.

Yukarıdaki kararları destekler mahiyette Yargıtay 8. Ceza Dairesi'nin 03.11.2014 tarihli ve E.2014/21702, K.2014/24201 sayılı kararı ise aşağıda sunulmaktadır (Demir vd., 2015, s.5):

"…Sanık tarafından e-posta adresine ***giriş yapılıp yapılmadığı****, adrese ait* ***şifrenin değiştirilip değiştirilmediği****,* ***değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığı****nın ilgili internet sağlayıcısından sorulmadığı anlaşılmıştır.*

Bu itibarla yukarıda açıklanan yöntem izlenerek eksiklikler yerine getirilip sonucuna göre tüm deliller birlikte değerlendirilip ***gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini*** *gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması hatalıdır. "*

Anılan yargı kararları ve evrensel olan suç ve cezaların şahsiliği ilkesi çerçevesinde; cezai sorumluluğun her zaman görünürdeki kişiye yüklenemeyeceği, gerçek failin bilişim sistemi üzerindeki her hareketinin, gerek yer gerek zaman bakımından kesin tespiti ile gerekmesi durumunda uzman bilirkişi marifetiyle de delillerin desteklenmesi gerektiği sonuçlarına ulaşılmaktadır.

Suçun mağduru ise; bir bilişim sistemi üzerinde kullanılan cihazına hukuka aykırı olarak erişim sağlanan ve bundan ötürü menfaati tehlikeye giren kişi sayılacaktır. Bu kişinin de mutlaka cihazın maliki olması gerekli değildir. Cihazın herhangi bir şekilde kullanıcısı olan kişi de (cihazı/sistemi sürekli kullanmasa da o kişinin oturumuna isabet eden kısımlar bakımından) bu suçun mağduru olabilecektir.

Hafızoğulları ve Özen'e göre; bu suça bilinçli olarak 'kişilere karşı suçlar' arasında yer verilmemesi ve suçun yasada 'Topluma Karşı Suçlar' kısmı altında yer alması sebepleriyle kamu idaresinin suçun mağduru olacağı, kişilerin ise sadece suçtan zarar gören kişi niteliğinde sayılabileceği belirtilmiştir (2016, s.445). Anılan yazarlarca herkese güvenli bilişim ortamı sağlanmasının kamu düzeninden sayıldığı ifade edilse de; şahsi kullanım ağırlıklı cihazlar ile kişiler arasında verilen izin ve/veya yetkinin aşılması durumlarının, her zaman kamu idaresi ile ilişkilendirilmesinin mümkün olamayacağı düşünüldüğünden, kişilerin bu suçun mağduru olabileceği değerlendirilmektedir.

Failin eylemi ile birden fazla kimsenin hakkı muhtel olmakta ise, bu kimselerin hepsi suçun mağduru olacaktır (Doğan, 2014, s.72). Örneğin bir kimsenin kişisel dosyalarını arkadaşının bilgisayarında muhafaza etmesi halinde, bu bilgisayara haksız erişim sağlanarak söz konusu dosyalara ulaşılması halinde hem bilgisayar sahibi hem de veri sahibi mağdur sıfatını taşıyacaktır.

3.1.2.2 Hareket ve netice

Suç, kanunilik ilkesi gereği ancak yasal tanımda yer alan icrai veya ihmali hareketlerin fail tarafından iradi olarak icra edilmesi suretiyle işlenebilir.

Bilişim sistemine girme veya orada kalma suçunun düzenlendiği madde metni incelendiğinde, suçun konusunu oluşturan bilişim sisteminin bütünü veya bir kısmına hukuka aykırı olarak girilmesinin veya orada kalmaya devam edilmesinin 'hareket' unsurunu işaret etmekte olduğu görülmektedir.

Bahsi geçen hükümde bilişim sistemine girme veya kalma şeklinde iki ayrı hareket düzenleme alanı bulmuştur. Kanuni tanımda birbirinin alternatifi olarak gösterilen hareketlerden biri ile işlenebilen suçlara "seçimlik (serbest) hareketli suç" adı verilmekte olup, seçimlik hareketlerden hepsinin gerçekleştirilmesi beklenmeksizin, bunlardan birinin icrasıyla suç oluşacaktır (Özgenç vd., 2012, s.21). Seçimlik hareketlerden birinin gerçekleşmesi suça vücut vereceğinden kanuni tanımında yer alan alternatif eylemlerin birkaçı veya hepsinin icra edilmesi halinde gerçekleştirilen hareket sayısınca değil yalnızca tek bir suç meydana gelecektir. Bu suç, virüsler ve arka/gizli kapı yöntemi ile işlenmeye müsaittir.

Maddede yer alan 'girme' sözcüğü yerine, suçun işlendiği alan olan bilişim istemine yönelik bir eylemin söz konusu olması sebebiyle 'erişim' kavramının kullanılmasının daha uygun olacağı değerlendirilmektedir. Nitekim 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna dayanılarak çıkarılan alt düzenlemelerde de[3] 'erişim' kavramı tercih edilmiş ve bu kavram *"herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılması"* şeklinde ifade edilmiştir. Yine ASSS'nin bu suça karşılık gelen 2 nci maddesinde düzenlenen suç tipinin *illegal access* kenar başlığı ile düzenlendiği görülmekte olup *'access'* tabiri girişten (*entrance*) ziyade, teknik olarak erişim kavramını daha çok karşılayan ve bu konuda yaygın olarak kullanılmakta olan bir terimdir.

Nitekim Yargıtay 8. Ceza Dairesi'nin 07.05.2014 tarihli ve E.2013/10402, K.2014/11836 sayılı ilamında da giriş yerine erişim/erişilme kavramı tercih edilmiş, aynı kararda sisteme çeşitli giriş yöntemleri izah edilerek, bu suçun başkasına ait cihazın açılarak içindeki verilerin izlenmesi veya uzak mesafeden haksız erişim ile işlenebileceği hususları üzerinde durulmuştur:

[3] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik m.3/1-e ; İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik m.3/1-c

*"... **Bilişim sistemine girmek, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir**. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. **Bu suç, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir**. Girmede, iletişimin kablolu veya kablosuz olmasıyla **mesafenin yakın ve uzak olması arasında da fark yoktur**. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (Windows, Linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır..."*

ASSS ve açıklayıcı raporu dayanak alındığında, bilişim sisteminin 'bir kısmına girilmesi' tabirinden de bilişim sisteminin, *"donanım, bileşenler, yüklenen sistemin saklanan verileri, dizinler, trafik ve içerikle ilişkili veriler"* gibi unsurlarından bir yahut birkaçına girilmesi anlaşılabilmektedir (Eker, 2006, s.123).

Karagülmez; 243 üncü maddede bir bilişim sistemine yetkisiz erişimin tek başına suç olmadığını, yetkisiz erişimden sonra erişilen sistemde kalmaya devam etme filiyle suçun gerçekleşeceğini dolayısıyla bu suçun 'yetkisiz erişim + sistemde kalmaya devam etme' şeklinde formüle edilebileceğini dile getirmiştir (2014, s.201).

243 üncü maddenin gerekçesine bakıldığında *"Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının veya bunları elde etmiş olmasının önemi yoktur. **Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir**"* ifadesi ile bilişim sistemine salt hukuka aykırı giriş eyleminin suçun sübutu için kâfi olduğu vurgulanmaktadır. Ayrıca maddenin ilk

kanunlaşan metninde bilişim sistemine haksız girme "ve" sistemde kalma lafzı mevcutken 2016 yılında yapılan değişiklikle[4] 've' ibaresi isabetli olarak 'veya' bağlacı ile değiştirilmiş ve suçun tanımında belirlilik sağlanmıştır. Bu nedenle hükmün gerekçesi ile metinde yapılan lafız değişikliği göz önüne alındığında, yukarıdaki görüşe katılmak mümkün olmamaktadır.

Bilişim sistemine girildikten sonra orada kalmaya devam etmek, sisteme giren failin sistem içinde bir süre kalması (bu arada sistem üzerindeki verileri kontrol edebilir, veri akışını izleyebilir, veriler üzerinde oynama yapabilir veya sistemi bozmaya yönelik işlemler icra edebilir veyahut hiçbir şey yapmayabilir) şeklinde gerçekleşebilir (Kurt, 2005, s.149).

Hukuka aykırı olarak girilen bilişim sisteminde 'bir süre' kalınması ibaresi de muğlak bir ifadedir. Bu nedenle bu sürenin suçun sübutu bakımından nasıl tayin edileceği bir sorun olarak karşımıza çıkmaktadır.

Failin sisteme girdiğini fark etmesiyle hemen çıkmaması durumunda suçun işlendiğinin kabul edildiği ve bu durumun tespitinin kolay olmadığından kısa süreli (anlık) giriş çıkışların suç olarak kabul edilemeyeceği görüşü de literatürde mevcuttur (Gül, 2015, s.59). Madde metninde yer alan sisteme girme 'veya' sistemde kalma ibaresi göz önüne alındığında; haksız şekilde girilen bir bilişim sisteminde bir dakika veya bir hafta kalınmasının suçun gerçekleşmesi açısından herhangi bir farkı olmadığı düşünülmektedir. Ancak sonuç cezanın takdirinde sistemde kalınan süre ile failin elde ettiği veri büyüklüğünün önem arz edebileceği değerlendirilmektedir.

Apaydın tarafından da eşyanın doğası gereği failin bilişim sistemine bir amaç için girmesinin beklendiği, sisteme girme amacı için kalacağı süre ne kadar az olursa olsun korunan hukuki menfaatlerin ihlal edilmiş olacağı sebebiyle suçun oluştuğunun kabul edilmesi gerektiği belirtilmiştir (2017a, s.61). Ayrıca süre olgusunun sübjektif özelliği

[4] 24/03/2016 kabul tarihli, 07/04/2016 tarih ve 29677 Sayılı Resmi Gazete'de yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 30 uncu maddesi.

de mevcut olup haksız girilen bir bilişim sisteminde kimi failin birkaç saniyede çok önemli verileri elde edebilmesi mümkün iken, birtakım faillerin günlerce sistemde kalmasına rağmen herhangi bir veriyi öğrenememesi mümkündür.

Bununla birlikte bir bilişim sisteminde haksız kalınan süre içerisinde herhangi bir verinin ele geçirilip geçirilmemesi de bu suçun bir unsuru değildir. Madde gerekçesinde de *"...Sisteme, hukuka aykırı olarak giren* ***kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının veya bunları elde etmiş olmasının önemi yoktur...****"* vurgusu yapılmıştır (TBMM, 2016a).

Hareket ile meydana gelen hukuka aykırı sonucun birden sona ermeyip zaman içinde devam ettiği ve en önemli özelliğinin suçun tamamlanması ile bitmesi aşamalarının farklı zamanlarda gerçekleştiği suçlara "mütemadi (kesintisiz) suç" denilmekte olup bu tür suçlarda hareketin icrası devam ettiği sürece suç da işlenmeye devam etmektedir (Yerdelen, 2014, s.114). ASSS ile de paralelliği sağlayan 07.04.2016 tarihinde gerçekleştirilen revize ile 've' ibaresi 'veya' bağlacı ile değiştirilmiştir. Anılan tarihten önce suçun mütemadi özelliği haiz olduğu söylenebilecektir. Ancak bu tarihten sonra, madde gerekçesi de temel alındığında bu suçun sırf hareket suçu olduğu ve suçta herhangi bir netice aranmadığı sonucuna da kendiliğinden ulaşılabilmektedir.

Mütemadi suçlar hareket kesintiye uğradığı veya nihayete erdirildiği anda tamamlandığından; lehte kanun ilkesi, zaman aşımı, yetkili mahkeme gibi unsurlar ani hareket suçlarıyla farklılık gösterebilmektedir. 2016 öncesi düzenlemede 've' ibaresinin hem sisteme girme hem de sistemde kalmaya devam etme hareketinin birlikte aranmasının failin lehine bir durum olduğu açıktır. Zira 2016 değişikliğinden sonra sadece sisteme girilmekle veya bir başkasının haksız girdiği sistemde kalma iradesinin devam etmesi ile suç oluşacaktır. Eylemdeki alternatif bu genişletmenin failin aleyhinde olması sebebiyle, suçun zamanının tayin edilmesi özellikle TCK'nın 7 nci maddesinde yerini bulan "lehte kanun ilkesi" kavramının uygulanması bakımından önem arz etmektedir.

Madde gerekçesinde de altı çizildiği üzere sisteme haksız ve kasten girilmesi suçun oluşumu için gerekli ve yeterlidir. Failin eylemi neticesinde sistemin zarara uğramasına yönelik yakın bir tehlikenin oluşması ya da somut bir zararın gerçekleşmesi aranmadığı için bu suç aynı zamanda 'soyut tehlike suçu' niteliğini taşımaktadır (Apaydın, 2017a, s.60).

Tehlike suçu, icra edilen fiilin suçun konusu üzerinde bir zarar meydana getirme tehlikesi söz konusu olan suç tiplerinden olup failin cezalandırılabilmesi için, herhangi bir zararın gerçekleşmesine gerek duyulmamakta; dolayısıyla bu suçun tamamlanması açısından da, failin bilişim sisteminde kaldığı süre içerisinde mağdura zarar verici bir fiilde bulunup bulunmamasının herhangi bir önemi bulunmamaktadır (Kızıltan, 2007, s.65). Bu husus ayrıca Yargıtay 11. Ceza Dairesi'nin 26.03.2009 tarihli ve E.2008/18190, K.2009/3058 sayılı kararında da açıkça ifade edilmiştir (Corpus, 2018):

"... Sanığın, katılanın yetkilisi olduğu Z. T. İmalat Pazarlama Sanayi ve Ticaret Limited Şirketi'nin Türkiye E. Bankası Denizli şubesinde bulunan hesabına internet üzerinden izinsiz 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.nun 243/1 inci maddesinde düzenlenen suçu oluşturduğu gözetilmeden*** *yazılı şekilde (5237 sayılı TCK.nun 244/4, 35/2 nci maddeleri gereğince) hüküm tesisi, yasaya aykırı olup bozmayı gerektirmiştir. Suçun hareket suçu olduğu görülmektedir ..."*

3.1.3 Suça etki eden sebepler (Nitelikli haller)

Suçun yasada yazılı olan temel hali ile ilgili olmakla birlikte, suçun temel halinde korunan hukuki menfaate yönelen eylemin veya eylem neticesinde meydana gelen sonuçların bazı durumlarda kanun koyucu tarafından daha hafif veyahut daha ağır bir yaptırımla korunması gerekmektedir.

Suçun temel halinin yer aldığı Kanun veya farklı bir kanunda atıfta bulunularak ceza hükmü niteliği taşıyan bir başka düzenleme ile ilgili suçun öngörülen temel cezasının

arttırılması veya indirilmesini sağlayan bu durumlar, suç ve cezaya etki eden nitelikli haller olup düzenleme sistematiği ve kanunilik ilkesi başta olmak üzere her suçun özelliğine göre ayrı ayrı ele alınmaktadır.

Nitelikli haller; konut dokunulmazlığını ihlal suçunun ağırlaştırıcı sebeplerinden olan 'gece' işlenmesinde olduğu gibi (TCK m.116/4) zaman kavramını, adam öldürme suçunun ağırlaştırıcı nedenlerinden biri olan 'altsoy ve üstsoya karşı' işlenmesinde olduğu gibi (TCK m.82/1-d) akrabalık ilişkisini de temel noktaya koyabilmektedir. Bununla birlikte; hırsızlık suçunda hafifletici sebep olan 'malın değerinin azlığı' hususunda olduğu gibi (TCK m.145) suçun hukuki konusunun veya cinsel saldırı suçunun ağırlaştırıcı sebebi olan 'silahla veya birden fazla kişi tarafından birlikte' işlenmesinde olduğu gibi (TCK m.102/3-d) suçun işlenme biçiminin (eylemin türü ve şiddeti ile kullanılan vasıtaların) esas alınabilmesi mümkündür.

Bu çerçevede 243 üncü maddede düzenlenen bilişim sistemine girme veya orada kalmaya devam etme suçunun Kanunda düzenlenen nitelikli halleri aşağıda açıklanacaktır.

3.1.3.1 Daha az cezayı gerektiren (hafifletici) nitelikli hal

Söz konusu suçun düzenlendiği 243 üncü maddenin ikinci fıkrasında bu suçun hafifletici sebebi yer almaktadır.

Anılan fıkrada ilk fıkrada yer alan suçun işlenebileceği seçimlik eylemlerin *"bedeli karşılığı yararlanılabilen hizmetler"* içeren bir bilişim sistemi nezdinde işlenmesi halinde verilecek cezada indirim yapılacak, bu indirim ise temel cezanın yarısı oranında olacaktır.

Bedeli karşılığında yararlanılabilen sistemler ibaresi, bilişim suçları bakımından ceza mevzuatımıza ilk kez girmiş ve yoruma açık bir kavramdır (Karagülmez, 2014, s.208).

Öncelikle, bu sistemlerin otomatlar veya yayın hizmeti sunan dekoderler gibi cihazlar olmadığı açıktır. Çünkü TCK'nın 163 üncü maddesinin ilk fıkrasında net bir şekilde otomatlar aracılığıyla sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan faydalanan kişinin cezalandırılacağı belirtildiğinden, otomatlar TCK'nın 243 ve 244 üncü maddeleri kapsamında değerlendirilemezler (Erdoğan, 2012, s.148).

TCK'nın 163 üncü maddenin ikinci fıkrasında da "telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibi veya zilyedinin rızası olmadan yararlanan" kimsenin cezalandırılacağı belirtildiğinden bu özel düzenleme gereğince dekoder; TCK m.243 kapsamında bir bilişim sistemi değil, TCK 163/2 kapsamında bir aygıt olarak değerlendirilmelidir (Doğan, 2014, s.76).

Konu hakkında değerlendirmenin, bilişim sistemine girme veya müdahale oluşturmayıp, yukarıdaki görüşleri destekler nitelikte TCK. 163/2 hükmü çerçevesinde nitelendirilmesi gerektiğinin vurgulandığı, Yargıtay 8. Ceza Dairesi'nin E.2013/8905 ve K.2014/19651 sayılı kararı aşağıdaki gibidir (Corpus, 2018):

*"...Katılanın tek yönlü olarak **frekanslarla veya elektromanyetik dalgalar aracılığıyla yaptığı şifreli yayının** sanığa ait uydu alıcısına ulaşması üzerine **gerekli donanım ve yazılım kullanılarak kartın şifre çözme kabiliyetinin internet ortamından paylaştırılması suretiyle şifreli yayınların sanık aracılığıyla başkaları tarafından şifresiz olarak izlenmesinin sağlandığı** olayda, **katılan tarafından kullanılan bilişim sistemine herhangi bir müdahalede bulunulmadığı** anlaşıldığından, **eylemin TCK.nun 163/2 nci maddesinde belirtili karşılıksız yararlanma suçunu oluşturduğu** gözetilmeden, yazılı şekilde hüküm kurulması ... gereğince bozulmasına ... karar verildi."*

Bir görüşe göre, bedeli karşılığı yararlanılabilen sistem kavramından dört şey anlaşılır (Dülger, 2015, s.374): Birincisi, internet üzerinden ücretli üyelik karşılığında hizmet veren web siteleri (e-posta, gazete-dergi aboneliği, mevzuat-içtihat programları gibi); ikincisi internet kafe gibi yerlerde belli bir bilişim sisteminden ücreti ödenerek

yararlanılması; üçüncüsü, bir kuruluş tarafından belli bir anlaşma karşılığında, belli bir hizmetin abone olan kişilere mesaj olarak reklam amaçlı ileti yollanması; dördüncüsü, belli bir zaman ya da dönem gibi süre sınırlamasıyla bedel karşılığında internet hizmetinin sağlanmasıdır.

Başka bir görüşe göre, bedelini ödemeden internet kafedeki bilgisayara (internete) girilmesi ve orada kalınması bu sistem çerçevesinde olmayıp bedeli ödenmeden internet kafedeki bilgisayara girilmesi gerçekleşse bile, bu girme değil, 'kullanma' fiiline vücut vermektedir (Karagülmez, 2014, s.210). Zira TCK.'nın 243 üncü maddesinin ikinci fıkrasında kastedilen, bilişim sisteminin kullanıldığı mekân değil, bizzat bu sistemin içerisindeki elektronik yapıda sunulan ücretli hizmetlerdir (Parlar, 2011, s.19). Suçun konusunu bedeli karşılığında bir bilişim sistemi üzerinden verilen hizmet oluşturduğundan, bu görüşe katılmak mümkün olup özellikle ücret karşılığında hizmet veren tüm web siteleri veya uygulamaların madde kapsamında olduğu düşünülmektedir.

Söz konusu hafifletici sebep hakkında da farklı görüşler yer almaktadır. Birtakım görüşlerde bunun isabetli olduğu, nitekim bedeli ödenince kullanıma açılan bir bilginin, öğrenilmesinin hiçbir şekilde istenmeyen şahsi bir bilgiden daha az değerli olduğu, dolayısıyla verilerin masuniyeti açısından bir fark olduğu ve failin sadece bedeli dolanmak istediği gibi sebeplerle bu indirimin yerindelik taşıdığı savunulmaktadır (Doğan, 2014, s.79-80; Pallı, 2008, s.154). Karşıt görüşlerde ise; böyle bir indirim sebebinin düzenlenmesine gerek bulunmadığı (Erdoğan, 2012, s.151), hatta bu durumda sistemde yer alan hizmeti ücret ödeyerek kullanan kişiler ile sistemin sahibinin mali çıkarlarına da zarar verildiğinden bahisle bu tür eylemlerin ağırlaştırıcı hal olarak düzenlenmesi gerektiği ileri sürülmektedir (Taşkın, 2008, s.36; Dülger, 2015, s.378).

Kanımızca; bedeli karşılığında hizmet veren sistem ibaresinin yer aldığı ikinci fıkrada ilk fıkradaki suçun temel haline atıf yapılmakta olup, failin her halükarda sisteme haksız giriş yaptığı açık olduğundan; ayrıca bu suçta netice aranmaması sebebiyle veri elde edilmesi gibi bir hususun veya elde edilen verilerin mahiyetinin hiçbir önem

taşımadığı birlikte gözetildiğinde, bu hafifletici sebebin madde metninde yer almasına gerek olmadığı değerlendirilmektedir.

3.1.3.2 Neticesi sebebiyle ağırlaşmış nitelikli hal

TCK'nın 27 nci maddesinde neticesi sebebiyle ağırlaşmış suç kavramının tanımı yapılmasa da birtakım özellikleri ve failin sorumluluğu ile ilgili hususlara yer verilmiştir. Buna göre kastedilenden daha ağır veya başka bir neticenin oluşumuna sebebiyet verilmesi hali neticesi sebebiyle ağırlaşmış suç olarak düzenlenmiş ve failin sorumlu tutulabilmesi için bu netice bakımından (ağır sonuç) en azından taksirle (kasttan daha hafif bir kusurla, dikkat ve özen yükümlülüğüne aykırı davranarak) hareket etmesi gerektiği hükme bağlanmıştır.

Neticesi sebebiyle ağırlaşmış suçlarda suçun oluşması için aranan neticeden başka ve fakat daha ağır bir sonuç meydana gelmekte ve bu nedenle failin cezası artırılmakta olup bu suç türü, birinci aşamada failin istediği asıl sonuç, ikinci aşamada ise ağır netice olmak üzere iki safhada gerçekleşmektedir; ayrıca hareket ile neticenin arasında nedensellik (illiyet) bağı var olmalı, ağır neticeden sorumluluk için ise yasada açıklık (kanuni düzenlemenin varlığı) bulunmalıdır (Özbek, 2007a, s.223).

Neticesi sebebiyle ağırlaşmış suç kavramından söz edilebilmesi için gerçekleşen neticenin fail tarafından kural olarak istenmeyen bir netice olması gerekmekte olup, eğer söz konusu netice failin kastı kapsamında ise ve bu netice başka bir suçun unsuru niteliğinde ise neticesi sebebiyle ağırlaşmış suçtan söz edilemez (Doğan, 2010, s.6-7).

Bahse konu maddenin üçüncü fıkrası, suçun neticesi sebebiyle ağırlaşmış halini düzenlemekte olup, düzenlemede bu fiil nedeniyle sistemin içerdiği **veriler yok olur veya değişirse**, verilecek cezanın artırılması öngörülmüştür.

Öncelikle 'veya' lafzından hareketle, seçimlik hareketli olduğu açık olan bu suça dair cezada artırım halinin yer aldığı üçüncü fıkrada geçen 'bu fiil' yerine; 'bu fiiller' veya

'bu maddede sayılan fiillerden biri' ibaresinin kullanılmasının daha uygun olacağı değerlendirilmektedir.

Söz konusu fıkraya yönelik komisyonun değişiklik gerekçesinde de: *"Üçüncü fıkrada, bu suçun **neticesi sebebiyle ağırlaşmış hâli** düzenlenmiştir. Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, **bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir**."* denilerek (TBMM,2016), failin bu sonucu 'istememesi' özellikle vurgulanmıştır. Sonuç olarak, suçun bu fıkrasının uygulama alanı bulabilmesi açısından failin iradesinin kritik önem taşıdığı görülmektedir.

Kanımızca düzenlemenin lafzında belirtilen 'fiil sonucunda veriler değişir veya yok olursa' ibaresi ile bilişim sistemine giren failin gerçek iradesi dışında sayılan durumların gerçekleşebileceği, dolayısıyla bu durumun da öngörülebilir olmasından ötürü failin en azından taksirle ağırlaştırılmış sonuçtan sorumlu tutulması hedeflenmiştir. Burada bir çeşit kusursuz sorumluluk halinin mevcut olduğu ve kanunun bir tür 'taksir karinesi' kabul ettiği görüşü de mevcuttur (Hafızoğulları ve Özen, 2016, s.450).

Suçun ilk iki fıkrasında netice aranmazken bu suçun ağırlaştırıcı nedenini düzenleyen suç tipi için fıkrada yazılı neticelerden birinin gerçekleşmesi yeterli ve gereklidir. Bu hükmün uygulanabilmesi için failin kastı olmaması ön şarttır. Zaten failin böyle bir sonucun gerçekleşeceğini bilmesi ve istemesi halinde kastın varlığından söz edilecek ve bu eylem bir başka suça[5] vücut verecektir.

[5] Bilişim sistemindeki verileri "**kasten**" bozma, yok etme, değiştirme veya erişilmez kılma ile sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi eylemlerinin suç olarak düzenlendiği TCK. m.244 üncü maddesinin ikinci fıkrası burada uygulama alanı bulacaktır.

3.1.3.3 Terör amacı ile işlenmesi halinde ağırlaşmış nitelikli hal

Terör olgusunu ilk maddesinde tanımlayan 3713 sayılı Terörle Mücadele Kanunu'nun (TMK) *"Terör amacı ile işlenen suçlar"* başlıklı dördüncü maddesinde; birinci maddede belirtilen amaçlar doğrultusunda, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde maddede sayılan birtakım suçların işlenmesi halinde bunların "terör suçu" sayılacağı hükme bağlanmıştır (Dülger, 2015, s.380).

Katalog şeklinde sayılan bu suçlar arasında TCK'nın 243 üncü maddesi de yer almakta olduğundan, bu yasal düzenleme de suçun ağırlaştırıcı nitelikli sebebini teşkil etmektedir.

TMK'nın *"Cezaların artırılması"* kenar başlıklı 5 inci maddesinde; Kanunun 4 üncü maddesinde yazılı suçları işleyenler hakkında, ilgili kanunlara göre tayin edilecek hapis veya adli para cezalarının yarı oranında artırılarak verilmesi amir hüküm olarak tanzim edilmiş ve bu suretle tayin olunacak cezalarda, gerek o fiil gerekse her türden ceza için belirli olan cezanın üst sınırının aşılabileceği belirtilmiştir.

Anılan maddede son olarak suçun örgüt faaliyeti kapsamında işlenmesinin, bir başka Kanunda ağırlaştırıcı sebep olarak öngörülmesi halinde yalnızca bu hükmün uygulanacağı, ancak bu halde artırmanın cezanın üçte ikisinden az olamayacağı ve nihayet bu madde hükümlerinin çocuklara (TCK. m.6/1-b uyarınca 18 yaşını doldurmamış kişiler) tatbik edilemeyeceği düzenlenmiştir.

3.1.4 Bilişim sistemine erişmeksizin teknik araçlarla verileri izleme

Bilişim teknolojilerindeki gelişme ve imkânlar gözetilerek bilişim sistemine girmeksizin verilerin izlenmesi fiilinin de suç olarak öngörülmesinin gerektiği, nitekim bu hususun Adalet Bakanlığı tarafından kurulan bir Komisyon tarafından hazırlanan 2007 tasarısında da yer aldığı literatürde ifade edilmektedir (Karagülmez, 2014, s.231).

Mezkûr suçun son fıkrasına 24/03/2016 tarihinde 6698 sayılı Kanunun 30 uncu maddesi ile "bilişim sistemine erişim sağlanmasa da teknik araçlarla verilerin ve veri nakillerinin izlenmesi" bağımsız bir suç tipi olarak eklenmiştir.

Değişikliğe ilişkin alt komisyon raporunda; *"...**Sanal Ortamda İşlenen Suçlar Sözleşmesinin[6] 3'üncü maddesiyle, üye ülkeler, yasadışı araya girme eylemini cezalandırmaya davet edildiğinden, 5237 sayılı Kanunun 243'üncü maddesinde değişiklik öngörülmüştür**. Böylece bilişim sistemlerinin bütününe veya bir kısmına hukuka aykırı olarak girmekle birlikte belirli bir süre kalmak da suçun unsuru olarak düzenlenmiş olmasına rağmen Sözleşmeye uyum amacıyla sadece sisteme/sistemlere girmek fiili suç olarak düzenlenmektedir. **Verilerin izlenmesi eylemi, bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesini ifade etmektedir**. Bütün elektronik veri transferleri, bu çerçevede korunması amaçlanan veri transferinin gizliliği kapsamında kalmaktadır. Yasadışı araya girme eylemleri, temelde bilişim sistemlerine girilmeksizin işlenen fiillerdendir. Bu doğrultuda Sözleşmeye uyum amacıyla yine aynı maddenin birinci fıkrasına hüküm eklemek suretiyle, bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla izleyen kişinin altı aydan üç yıla kadar hapis cezası ile cezalandırılması öngörülmüştür"* denilmektedir (TBMM, 2016b).

İhdas edilen suç tipinin özellikleri aşağıdaki gibi özetlenebilir (Gül, 2016, s.65-66):

- Bilişim sisteminin kendi içinde veya bilişim sistemleri arasındaki veri nakilleri suçun konusu olabilecektir.
- Eylem sisteme girmeksizin gerçekleştirilmeli, teknik araçlarla izleme, eylemin bir parçası olmalıdır.
- İzleme fiilinin kasten ve hukuka aykırı olarak icra edilmesi gerekmekte olup hukuka uygunluk sebepleri suçun oluşumunu engelleyecektir.

[6] Bu ibareyle Avrupa Konseyi Siber Suç Sözleşmesi (ASSS) işaret edilmektedir. Ülkemizde anılan sözleşmenin uygun bulunduğu yasa olan 6533 sayılı Kanunun başlığında "Sanal Ortamda İşlenen Suçlar Sözleşmesi" kavramı tercih edilmiştir.

Bu suçun; sisteme erişim sağlanmaksızın kişinin ziyaret ettiği sayfaları veya şahsi verilerini kayda alan ve teknik araç olarak kabul edilebilecek bir uygulama/program veya kamera ile işlenmesi örnek teşkil edebilir.

Fıkranın lafzında *'sisteme girmeksizin'* ibaresinin kullanılması ama asıl suçun *'Bilişim sistemine girme'* kenar başlığına sahip olmasının bir çelişki yarattığı düşünülmekte olup; ayrıca verilecek ceza bağlamında da bir farklılaşmaya gidilmesinden ötürü böyle bir düzenlemenin yine bilişim alanında suçlar başlığı altında fakat ayrı bir maddede düzenlenmesinin daha uygun olacağı değerlendirilmektedir.

3.1.5 Suçun manevi unsurları ve hukuka aykırılık

Suçun manevi unsuru, suçu oluşturan eylem ile bu eylemi icra eden kişi arasındaki bağı ifade etmektedir.

Ceza hukuku açısından bireyin yasal tanımda belirtilen suçu oluşturan eylemi gerçekleştirmesinin tek başına sorumlu tutulması için yeterli olmadığı, failin ayrıca bu eylemi gerçekleştirirken kusurlu bir şekilde hareket etmesi gerektiği ve hatta bu konuda "ceza hukukunda hiçbir konunun failde bulunması gereken irade kadar önemli ve temel bir sorun oluşturmadığı" ifade edilmektedir (Dülger, 2005, s.65).

Kusurun tipik şekli, kasttır. Kural olarak suçlar kasten işlendiği takdirde cezalandırılır ve dolayısıyla suç tiplerinde ayrıca kasttan bahsetmeye gerek yoktur (Gökpınar, 2008, s.200).

TCK'nın 22 nci maddesine göre; kast gibi bilme ve isteme unsurlarını doğrudan barındırmadan, dikkat ve özen yükümlülüğüne aykırılık dolayısıyla, bir davranışın suçun kanuni tanımında belirtilen neticesinin öngörülmeyerek gerçekleştirilmesi haline "taksir" denilmektedir. Bir suçun oluşumu için asıl olarak kast aranmakta olup suçun taksirli haline sorumluluk yüklenecek ise bu durumun mutlaka kanunda öngörülmesi gerekmektedir.

Maddenin ilk iki fıkrası için özel bir durum öngörülmediğinden failin kastla hareket etmesi gerekmektedir. Nitekim madde gerekçesinde de her iki fıkra bakımından genel kastın yeterli olduğu belirtilmiştir. Üçüncü fıkradaki neticesi sebebiyle ağırlaşmış sonuçtan failin sorumlu tutulabilmesi için ise ilgili bölümde de açıkladığımız üzere failin kastı bulunmamalıdır. Bu durumda fail, gerçekleşen ama istemediği sonuçtan taksiri oranında sorumlu tutulacaktır.

ASSS'nin açıklayıcı raporunda da cezai yükümlülükten söz edilebilmesi için sözleşmede ele alınan bütün suçların "kasıtlı" olarak işlenmesinin gerekli olduğu, bazı durumlarda ise özel kastın aranabileceği ve bu hususun ulusal yoruma bırakılmasının uygun olacağı ifade edilmiştir (CoE, 2001b, s.8).

Suçun gerçekleşmesi için sisteme girme ve kalmanın hukuka aykırı şekilde gerçekleşmesi gerekmektedir. Sistemin özel bir güvenlik önlemi alınarak korunup korunmadığı de (cihaza şifre konması veya bilişim sisteminin özel güvenlik yazılımlarıyla muhafazası vs.) hukuka aykırı olarak erişim sağlama eyleminin suç olma özelliğinde herhangi bir fark yaratmayacaktır.

Kusurluluğu ortadan kaldıran nedenler ile hukuka uygunluk sebepleri ve şahsi cezasızlık halleri de diğer suçlarda olduğu gibi bu suçta da uygulama alanı bulabilecektir.

Kanun hükmünü yerine getiren kişiye ceza verilemeyeceği hususunu düzenleyen TCK'nın 24 üncü maddesi çerçevesinde; örneğin Ceza Muhakemesi Kanunu'nun (CMK) 134 üncü hükmü ve bununla ilgili olarak Adli ve Önleme Aramalar Yönetmeliği'nin 17 nci düzenlemesine dayanılarak bilişim sistemlerine yetkili kişilerce usulüne uygun girilmesi ve orada kalmaya devam edilmesi halinde bu suç açısından hukuka uygunluk nedeni oluşacaktır (Dülger, 2015, s.391-392).

TCK'nın 25 inci maddesinin ilk fıkrasında "meşru savunma (müdafaa)" hali düzenlenmiştir. Söz konusu düzenlemeye göre kendisi veya üçüncü bir kişiye ait hakka

yönelen haksız bir saldırıyı, o andaki durum ve şartlara göre saldırıyla orantılı biçimde defetmek zorunluluğu ile işlenen fiillerden dolayı faile ceza verilmemesi hükme bağlanmıştır.

Teknik açıdan bilişim sistemine yapılan saldırıyı o anda fark etmek her zaman mümkün olmayıp, mağdurun saldırıyla orantılı şekilde karşı eyleminin icrası ve bunun adli sürçte ispatı bir hayli zor olacak ve bununla birlikte; bir an için bilişim suçlarında meşru savunmanın söz konusu olması halinde, bu hal bilişim suçlarını teşvik ederek daha çok arttıracak, yargı sürecinde kişilerin *"uğramış olduğum saldırıya karşılık veriyordum"* savunmasına mahal verecektir ki bunun kabulü mümkün değildir (Dülger, 2015, s.392). Meşru savunmanın düzenlendiği metne bakıldığında saldırıyı defetmenin kaçınılmaz bir yolu karşı saldırı olmayıp kişinin sistemi kapatması veya ivedi önlem alması olabilecektir. Bu nedenle bu suçta meşru müdafaa kuramının uygulanamayacağı değerlendirilmektedir.

TCK'nın 25 inci maddesinin ikinci fıkrasında ise cezai sorumluluğu ortadan kaldıran bir durum olarak "zorunluluk (ıztırar) hali" düzenleme alanı bulmuştur. Burada kişinin, kendisinin veya başkasının sahip olduğu hakka yönelik bir tehlikeyi gidermek amacıyla gerçekleştirdiği davranış dolayısıyla ceza sorumluluğu olmayacağı öngörülmüş; kişinin tehlikeye bilerek neden olmaması, tehlikeden suç olan bir harekete başvurmadan kurtulmanın olanaklı bulunmaması, tehlikenin ağır ve muhakkak olması şartları yanında tehlikenin ağırlığı ile konu ve kullanılan araç arasında orantılılık ilkesi de kabul edilmiştir (Turabi, 2012, s.283-284). Meşru savunmada haksız saldırıda bulunan kişiye karşılık verilirken, zorunluluk halinde fail veya insan iradesi haricinde gerçekleşen bir olay neticesinde, fail dışında üçüncü bir kişiye zarar verilmek zorunda kalınmaktadır.

Sayılan kanuni tanım ve şartlar çerçevesinde, bu suçta belli durumlar altında zorunluluk halinden faydalanılabileceği düşünülmektedir. Örneğin; yaşanan bir çığ felaketinde mahsur kalan bir kişinin, soğuk ve diğer dış tehlikelerden korunabilmesi için yakınındaki bir evi zorlayarak girmesi ve evde iletişim aracı olarak sadece bir bilgisayar bulabilmesi halinde, bu bilgisayarın şifresini çözerek bilişim sistemine

girmesi ve yardım istemesi eylemleri kapsamında, faile gerek konut dokunulmazlığını ihlal, gerekse bilişim sistemine girme veya orada kalmaya devam etme suçu bakımından ceza verilemeyeceği değerlendirilmektedir.

TCK m.26'daki ilgilinin rızası düzenlemesi uyarınca; örneğin cihaz sahibinin açık rızasıyla bu cihazı kullanan ve bilişim sistemine erişim sağlayan üçüncü bir kişi açısından suç oluşmayacaktır. Ancak bu iznin sona erdirildiğinin bitirildiğinin bildirilmesi halinde suçun oluşmaması için sistemden çıkış işleminin gerçekleştirilmesi gerekmektedir. Zira daha önceden kişiye verilmiş bir yetkinin bittiği andan itibaren de yapılacak tüm erişimlerin yetkisiz olacağı dolayısıyla bu tür bir erişimin hukuka aykırı olacağı değerlendirilmektedir. Rıza kural olarak eylem öncesinde elde edilmesi gereken bir olgu olsa da bilişim sistemi sahibinin rızası olmaksızın failin sisteme girdiği ve orada kaldığı sırada (yani eylemden sonra), sistem sahibi rıza verilmesi halinde de hukuka aykırılık ortadan kalkacağından suçun oluşmayacağı belirtilmektedir (Erdoğan, 2012, s.160).

TCK m.28'deki cebir ve tehdit düzenlemesi ele alındığında; örneğin bir bilişim uzmanının kafasına silah dayanması ya da kendisine önemli bir zarar verileceği tehdidinde bulunulması suretiyle sisteme girme eyleminin cebren yaptırılması halinde, fail bundan sorumlu olmayacak ancak burada faili bu yolla zorlayan kişiler 'dolaylı fail' olarak eylemden sorumlu tutulacak ve cezalandırılacaklardır (Dülger, 2015, s.397).

Hata (yanılgı) müessesesinin düzenlendiği TCK'nın 30 uncu maddesinin özellikle dördüncü fıkrasında '*kaçınılmaz*' hataya düşen kişinin cezalandırılamayacağı hükme bağlanmıştır.

Hatanın kaçınılabilirliği; kişinin bilgi düzeyi, gördüğü eğitim, içinde bulunduğu sosyal ve kültürel çevre koşulları, kişisel yetenekleri, mevcut bilgisini kullanmasının ondan ne ölçüde beklenebilir olduğu ve hukuksal-ahlaki değer yargıları gibi sübjektif nitelikler göz önünde bulundurularak belirlenebilecektir (Değirmenci, 2014, s.146).

Gerçekten, failin tipin bir unsuruna ilişkin bilgisizliğinin kendi taksirinden kaynaklanmadığı durumlarda, faile yüklenebilecek taksirli bir eylem bulunmadığına göre taksirli sorumluluk halinden söz edilmesi mümkün olmayacaktır. Bu gibi durumlarda, yanılgının taksiri de kaldırdığı kabul edilmektedir (Erman, 2006, s.28).

Buna örnek olarak, daha önce suç işlememiş ve işlemeyeceği kanaati de sosyal çevresinde mevcut olan bir kişinin işlediği hırsızlık sonucu ele geçirilen bir bilgisayarın faturasıyla birlikte, failin belli bir münasebetinin de bulunduğu bilgisayar servisi ve yazılım işlerinde yetkin bir kişiye götürülmesi ve bu kişi tarafından bilişim sistemine girilmesiyle orada kalınması fiilinin 'kaçınılmaz' bir hataya vücut verebileceği sebebiyle cezalandırılmaması gerektiği verilebilir.

3.1.6 Suçun özel görünüş biçimleri

3.1.6.1 Teşebbüs, iştirak ve içtima

Suça teşebbüs haline TCK'nın 35 inci maddesinde yer verilmiş olup; kasten suçu işlemeye elverişli hareketlerle doğrudan icraya başlanılmasına rağmen, failin elinde olmayan sebeplerle eylemi bir başka deyişle suçu tamamlayamaması durumunda, suçun asıl cezasından değil teşebbüsten dolayı sorumluluğun söz konusu olacağı ifade edilmiştir.

Bilişim sistemine girme veya kalma eylemlerinin 'sırf hareket suçu' ve 'neticesiz suç' niteliklerini haiz olduğu değerlendirildiğinden hareketlerin icrası ile suç meydana gelmektedir. Bu nedenle sisteme girmeye hazırlık hareketleri kapsamında failin icraya başlayıp elinde olmayan sebeplerle bunu tamamlayamaması halinde suça teşebbüsün mümkün olduğu değerlendirilmektedir. Salt hareketin icrası ile suç sübut bulacağından ve suçta netice aranmadığından bu suçta gönüllü vazgeçme hükümlerinin ise uygulanamayacağı düşünülmektedir.

Teşebbüsün mümkün olduğu hallere herhangi bir şekilde failin sistem ile arasındaki bağlantısının kesilmesi örnek verilebilir. Mesela icra hareketlerine başlanıldığı halde,

elektriğin kesilmesi gibi elde olmayan nedenlerden ötürü eylemin tamamlanamaması durumunda teşebbüsün varlığından söz edilebilecektir (Demir vd., 2015, s.5).

İştirak hali ise, suçun tek bir kişi yerine birden çok kişi tarafından işlenebilmesi durumudur. Bir başka ifadeyle, tek bir kişi ile işlenmesi olanaklı olan bir suçun, birden fazla kişi tarafından ortak bir irade ve bu iradenin planı dâhilinde hareket edilerek gerçekleştirilmesidir (Mahmutoğlu, 2005, s.57).

5237 sayılı YTCK iştirak müessesesini tamamıyla yeniden düzenlemiş; bu bağlamda iştirak kategorilerini faillik (asli ve dolaylı), azmettirme ve yardım etme başlıkları altında üç temel noktada toplamış, bağlılık kurallarını düzenleyerek, sirayet meselesini de köklü bir çözüme kavuşturmuştur (Akarslan, 2015, s.46).

İncelediğimiz suçun düzenlendiği yasa hükmü ve içeriğinde suça vücut veren iradi hareketler tetkik edildiğinde, suç için iştirak açısından herhangi bir ayrı özelliğinin bulunmadığı görülmekte ve iştirakin her halinin bu suç için mümkün olabileceği değerlendirilmektedir.

Bilişim suçlarını birden fazla kişinin işlemesi durumunda, bunlardan her birisinin ‘müşterek fail’ olarak sorumlu tutulacağı belirtilmektedir (Kurt, 2005, s.266). Yine suçun işlenmesi için faili teşvik eden; mekân, cihaz, bağlantı araç ve gereçleri veya haksız erişime sebep olacak yazılımı temin ederek suçun icrasını kolaylaştıran kişinin de ‘yardım eden’ sıfatıyla iştirakçi olabileceği değerlendirilmektedir.

Ceza hukukunun temel prensiplerinden biri; “kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar da ceza vardır” (*quot crimina, tot poenae*) ilkesi olup ceza hukukumuzda cezaların içtimaı (gerçek içtima) asıl kuraldır ve işlenen her suçtan ayrı cezaya hükmedilerek, her bir ceza bağımsızlığını korur (Göktürk, 2014, s.31).

Bu kuralın istisnası ise “suçların içtimaı” müessesesidir. Suçların içtimaı hallerinde, fail tarafından birden çok suç işlenmiş olmasına rağmen, çeşitli sebeplerle faile bütün suçların cezaları ayrı ayrı saptanıp toplanarak verilmek yerine tek bir ihlal varmış gibi

tek bir ceza verilir (Merki, 2009, s.7). Bahse konu düzenlemeler, TCK'nın 42-44 maddeleri arasında toplanmıştır.

Anılan yasa maddelerine göre içtima türleri aşağıdaki gibidir:

- İşlenen suçun bir başka suçun unsuru veya ağırlaştırıcı sebebi olması ile tek fiil sayılan *"Bileşik (mürekkep) suç"* (TCK m.42) Bunlar zaten kanunla açıkça düzenlenmiş ve birbiri içerisinde eriyerek tek suç sayılan durumlardır.
- Suç işleme kararı kapsamında değişik zamanlarda tek bir kişiye karşı aynı suçun işlenmesi veya bir suçun birden fazla kişiye karşı tek bir fiille icra edilmesi durumu olan *"Zincirleme suç"* (TCK. m.43)
- Tek bir fiil ile birden fazla suçun oluşumuna sebebiyet verilmesi hali olan "Fikri içtima" (TCK. m.44)

Bileşik suçun oluşabilmesi için biri diğerinin ağırlaştırıcı nedeni ya da unsuru olan iki ayrı suç bulunması gerektiğinden, bu suçun yasada tanımlanan maddi unsurları bakımından böyle bir olasılık söz konusu olmayacaktır (Taşkın, 2008, s.33).

Bilişim sistemine girme suçunun zincirleme suç şeklinde işlenmesinin ise mümkün olacağı düşünülmekte olup böyle bir durumda kanuni düzenleme gereği failin cezası arttırılacaktır. Örneğin aynı suç işleme kararının icrası kapsamında, bir bilişim sitemine girip orada kalmaya devam eden failin, ertesi gün aynı şekilde aynı kişiye ait sisteme girip orada kalması ve daha sonraki zamanlarda da bu eylemini ara ara devam ettirmesi durumunda TCK 43/1 hükmünden; tek bir eylemi ile birden fazla bilişim sistemine girip kalırsa TCK m. 43/2 hükmünden zincirleme suç kuramı uygulanacaktır (Doğan, 2014, s.97).

Zincirleme suç müessesesinin oluştuğu hakkında verilen Yargıtay 8. Ceza Dairesi'nin E.2014/3984, K.2014/13848 sayılı kararında: *"...sanığın, katılan* ***şirketten ayrıldıktan sonra şirkete ait bilgisayar programına girdiğini kabul etmesi*** *ve* ***değişik zamanlarda bu programa girdiğinin*** *dosya içerisindeki belgelerden* ***anlaşılmış olması*** *karşısında,*

sanığın oluşan eylemi nedeniyle ***bilişim sistemine izinsiz girme suçundan TCK'nin 243, 43. maddeleri gereğince*** *cezalandırılması..."* şeklinde hükmedilmiştir (Apaydın, 2017a, s.95). Kararın analizi bağlamında; sanığın şirketten ayrılması ile şirkete ait bilgisayar programına girilmesi, eylemin 'hukuka aykırılık (haksızlık)' unsurunu, aynı kişiye karşı (şirket tüzel kişiliği), değişik zamanlarda, aynı suçun işlenmesi de 'zincirleme suç' unsurlarını işaret etmektedir.

Bilişim sistemine hukuka aykırı erişim veya sistemde kalmaya devam etme, bilişim sistemlerine erişilerek işlenmesi zorunlu bulunan başka bilişim suçlarının işlenmesi için de bir araç olduğundan bu itibarla 243 üncü maddede yer alan suç, daha sonra işlenen bu suçlar bakımından bir 'geçit' olma özelliği taşımaktadır (Erdoğan, 2010, s.1418). Geçitli suç kuramı kabul edilecek olursa, daha önceki suç teşkil eden fiil veya fiiller cezalandırılmaksızın, failin amaçladığı daha ağır neticeyi haiz, yani ulaşılan nihai suçtan cezalandırılması gerekmektedir.

Ancak bir diğer görüşe göre de; ilgili suçlarda, mesela bilişim sistemine zarar verilmesi için mutlaka sisteme hukuka aykırı olarak girilmesi gerekmez; örneğin bir şirket yetkilisi ya da servis görevlisi tarafından pekâlâ sisteme hukuka uygun olarak giriş yapabilecek ve sistemde kalmaya devam edildikten sonra sisteme zarar verilmesi söz konusu olabilecektir; bununla birlikte sisteme girilmeksizin sistemin fiziki yapısına zarar verilerek de bu suçun işlenmesi mümkün olabileceğinden sisteme zarar vermek için (TCK m.244) sisteme hukuka aykırı olarak girmek (TCK m.243) yönünde mutlak bir zorunluluk bulunmamaktadır (Dülger, 2014, s.78).

Sonuç olarak bilişim sistemine girme, diğer bir suçun unsuru veya zorunlu hareketini mutlaka içermiyorsa, fail hem bilişim sistemine haksız erişimden hem de amaç suçtan ayrıca cezalandırılacaktır (Karakehya, 2009, s.22).

Yukarıda ortaya konulan görüşlerden son belirtilenlere katılmak mümkündür. Zira bahsedilen her iki suçun da koruduğu hukuki değer aynı değildir ve daha ağır neticeli olan suç için mutlaka bir bilişim sistemine haksız girişin gerekli olmadığı örneklerle açıklanmıştır. TCK. m.243'teki suç ile diğer bilişim suçları yanında; özel hayatın

gizliliğini ihlal, kişisel verilerin ele geçirilmesi, haberleşmenin haksız engellenmesi ve dinlenmesi vb. türden dolaylı bilişim suçu şeklinde işlenebilecek diğer suçların da içtima hali için aynı kanı geçerliliğini devam ettirecektir.

Konuya ilişkin olarak Yargıtay 12. CD.'nin 15.09.2014 tarihli ve E.2014/649, K.2914/17770 sayılı kararı tetkik edildiğinde; tek bir hareketle bilişim sistemine giriş ve kişisel verilerin ele geçirilmesi kapsamında 'ayrıca' (ilaveten) bilişim suçundan da mahkûmiyet kararı verilmesi gerektiğinin altı çizilmiştir: *"...Katılanın facebook hesabına giriş için kullandığı elektronik posta adresini, rızası dışında ele geçiren sanık hakkında* ***verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkûmiyet kararı verilmesinde bir isabetsizlik görülmemiş, bilişim sistemindeki katılana özel kısma girip, hukuka aykırı olarak sistemde kalmaya devam eden ve katılanın bilişim sistemindeki kendisine ait kısma erişimini engelleyen sanık hakkında, TCK'nın 244/2'nci maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan ayrıca mahkûmiyet kararı verilmesi*** *gerektiğinin gözetilmemesi ..."* (Apaydın, 2017a, s.91).

Ceza muhakemesinin amacı, hiçbir duraksamaya yer vermeden maddi gerçeğin ortaya çıkarılması olup akla uygun, realist, olayın bütünü veya bir parçasını temsil eden kanıtların bütün olarak değerlendirilmesi ile sonuca ulaşılması gerekmekte ve varsayımlar neticeye esas olmamalıdır. Zira ceza yargılamasında kuşkunun bulunduğu yerde mahkûmiyet kararından söz edilemeyeceği ilkesi evrenseldir (Öztürk ve Erdem, 2007, s.185).

Bu çerçevede maddi gerçekliğin ortaya çıkarılarak hukuki uyuşmazlığın çözüme kavuşturulması kapsamında; failin kastı da dâhil olmak üzere, iradi eylem yanında, failin icra ettiği hareket ile ihlal edilen suç hükümleri arasındaki bağlantı (zorunluluk ilişkisi) yargı yerince araştırılarak, içtimaın türünün belirlenmesinin uygun olacağı değerlendirilmektedir.

3.1.7 Yaptırım ve yetkili adli merci

Bütün suçlar toplumun varlığı ve gelişmesi yönünden tehlikeli sayıldıklarından, re'sen soruşturulmaları ve kovuşturulmaları bir kural olsa da bir kısım suçlarda soruşturma ve kovuşturma 'şikâyet' şartına bağlanmıştır (Toroslu, 2009, s.421-422). Hangi suçların şikâyete tabi olup olmadığı hususu kanunda açıkça düzenlenmesi gerekmekte olup madde metni tetkik edildiğinde böyle bir şartın bulunmaması nedeniyle bu suçun soruşturma ve kovuşturma aşamalarının re'sen yürütüleceği anlamı çıkmaktadır.

Suçun kanunda tanzim edilen yaptırımlarını ise, bahse konu düzenlemenin dört fıkradan teşekkül olması sebebiyle ayrı ayrı incelemek gerekmektedir.

Birinci fıkra kapsamında (m.243/1) verilecek ceza 1 yıla kadar hapis veya adli para cezası şeklinde 'seçimlik' ceza olarak tanzim edilmiştir. Cezalar seçimlik olarak düzenlendiği için her iki ceza türünün birlikte uygulanması mümkün değildir.

Aşağıda yer alan konuyla ilgili Yargıtay 11. CD.'nin 29.03.2012 tarihli ve E.2012/3398, K.2012/4441 sayılı kararı analiz edildiğinde; bu suç kapsamında faile hem hapis cezası hem de adli para cezasına hükmedilmesinin kanun yararına bozma sebebi olarak görüldüğü sonucuna varılmaktadır:

"... 5237 sayılı Türk Ceza Kanunu'nun ***243/1. maddesinde; hapis ve para cezalarının seçimlik olarak öngörüldüğü gözetilmeden, her ikisine de hükmolunması isabetsiz olup****, kanun yararına bozma istemine atfen düzenlenen ihbarnamede yer alan düşünce yerinde görüldüğünden ... kararın bozulmasına..."* (Karagülmez, 2014, s.226).

Hapis cezalarının ağırlaştırılmış müebbet, müebbet ve süreli olmak üzere üç türü mevcuttur (TCK m. 46). Maddenin ilk fıkrasında öngörülen cezanın süreli olduğu görülmekte olup TCK'nın 49 uncu maddesi çerçevesinde alt sınırı bir aydan az olamayacaktır. Aynı maddenin son fıkrasında ise bir yıl ve daha az süreli hapis cezası "kısa süreli" olarak adlandırılmaktadır. Bu tür hapis cezalarının TCK'nın 50 nci

maddesi uyarınca, belli şartlar altında bazı seçenek yaptırımlara[7] çevrilebilmesi mümkündür.

Bununla birlikte, cezanın iki yıl ve daha az süreyle hapis cezasına cevaz vermesi karşısında, şartları sağlaması halinde TCK m. 51 uyarınca bu cezanın ertelenmesi[8] söz konusu olabilecektir. Son olarak fail; kasten işlemiş olduğu suçtan dolayı hapis cezasına mahkûmiyetin kanuni sonucu olarak, işlemiş bulunduğu suç dolayısıyla mahkûm olduğu hapis cezasının infazı tamamlanıncaya kadar, içerisinde seçme ve seçilme ehliyeti, velayet, vesayet ve kayyımlık gibi hakları da barındıran ve TCK'nın 53 üncü maddesinde tahdidi olarak sayılan belli hakları kullanmaktan yoksun bırakılacaktır.

Bu fıkradan hükmedilecek yaptırımda, hapis cezası yerine adli para cezasına karar verilmesi halinde bu tür cezaların hesaplama yöntemini gösteren TCK'nın 52 nci maddesi uygulama alanı bulacaktır. Anılan maddeye göre başka bir yasa hükmünde farklı gün sayısı belirtilmediği takdirde, adli para cezasının alt sınırı '5' üst sınırı ise '730' gündür. Adli para cezası; kişinin ekonomik durumu ve şahsi diğer halleri takdir edilerek, hükmedilen gün sayısı ile '20' ila '100' Türk Lirası (TL) arasında karar verilecek miktar çarpılarak hesaplanır. Bu meblağın hükümlü tarafından devlet hazinesine ödenmesi neticesinde ceza infaz edilmiş sayılacaktır.

5237 sayılı TCK ile "*Gün Para Cezası*" sistemi benimsenmiş olup buna göre, adli para cezalarının belirlenmesi "lira" değil, "gün" üzerinden belirlenecektir. Gün sayısının para birimlerine çevrilmesinde ilk olarak suça ilişkin kanun maddesinde belirtilen alt ve süt sınırlar arasında temel gün sayısı belirlenecek ve gün sayısı üzerinden TCK'nın

[7] Anılan seçenek yaptırımlar: adli para cezası, zararın aynen iade veya tazmin suretiyle tamamen giderimi, belirli bir süreyle sınırlı olarak; bir eğitim kurumuna devam edilmesi, belli yerlere gitmek veya belirli etkinlikleri yapmaktan men edilme, ilgili ehliyet ve ruhsat belgelerinin geri alınması, belirli bir meslek veya sanatı icra etmekten yasaklanma ve kamuya yararlı bir işte çalıştırılma şeklindedir.

[8] Hapis cezasının ertelenmesi halinde kişiye 1 ila 3 yıl arasında belirlenen bir denetim süresi tanınmaktadır. Kişinin bu denetim süresi içinde kasıtlı bir suç işlemesi veya kendisine yüklenen yükümlülüklere hâkimin uyarısına rağmen, uymamakta ısrar etmesi halinde; ertelenen cezanın kısmen veya tamamen infaz kurumunda çektirilmesine karar verilecektir.

61 inci maddesindeki sıra dikkate alınarak yapılan artırım ve indirimden sonra sonuç gün cezasına karar verilecek ve nihayet en az yirmi ve en çok yüz Türk Lirası üzerinden ödenecek adli para cezası miktarına ulaşılacaktır (Taneri, 2016, s.156).

Hesaplanan nihai meblağ, 1 yıl kadar ertelenebilir veya süresi 48 ayı geçmemesi şartıyla taksitlendirilebilir. TCK'nın 61 inci maddesinin dokuzuncu fıkrasında yer alan hükümle, adli para cezasının seçimlik ceza olarak öngörüldüğü suçlarda bu cezaya ilişkin gün biriminin alt sınırı, o suç tanımındaki hapis cezasının alt sınırından az; üst sınırı da, hapis cezasının üst sınırından fazla olamayacaktır. Hâkimin TCK m.243/1 maddesinde öngörülen adli para cezasını takdir etmesi durumunda, cezanın alt sınırı TCK m. 49/1 hükmü gereğince bir aylık adli para cezasından aşağı hesaplanamayacaktır (Meran, 2008, s.568).

Açıklamalar neticesinde, bilişim sistemine girme veya sistemde kalma suçunun düzenlendiği maddenin ilk fıkrası kapsamında ödenecek asgari adli para cezası miktarı 30 gün x 20 TL = 600 TL; azami adli para cezası miktarı ise 365 gün x 100 TL = 36500 TL olacaktır.

Verilecek sonuç ceza, davanın görüldüğü mahkeme hâkiminin takdirinde olup TCK'nın *"Cezanın Belirlenmesi ve Bireyselleştirilmesi"* başlıklı üçüncü bölümünde yer alan 61, 62 ve 63 üncü maddeler kapsamında yasada belirlenen birçok durumun birlikte gözetilmesiyle her somut olayda ayrı ayrı ele alınarak karara bağlanacaktır.

Suçun ikinci fıkrasında düzenlenen hafifletici halinde ise verilecek cezanın yarı oranına kadar indirileceği hükme bağlanmıştır. Bu kapsamda hapis cezası verilecek ise bu süre bir yılın yarısı olan altı ayı geçemeyecek, adli para cezasına karar verilmesi halinde de bu meblağa 600 ila 18250 TL arasında hükmedilebilecektir.

Suçun üçüncü fıkrasında düzenlenen neticesi sebebiyle ağırlaşmış halinde, suçun ağırlığından ötürü tek bir yaptırım öngörülmüş ve seçimlik ceza alternatifinden vazgeçilmiştir. Bu fıkra kapsamında suç işleyen fail sadece hapis cezasına

çarptırılabilecek; bu bağlamda faile verilecek ceza 6 aydan az 2 yıldan fazla olamayacaktır.

Suçun son fıkrasında bağımsız bir suç tipi olarak düzenlenen bilişim sistemine girmeksizin teknik araçlarla verilerin izlenmesi suçunda da faile sadece hapis cezası tatbik edilebilecek olup cezanın alt sınırı bir yıl üst sınırı ise üç yıl olarak tanzim edilmiştir.

Suçun işlenmesi halinde davaya bakacak olan mercii, adli yargı yerleri olup bu konuda ceza mahkemelerinin görevli olduğu açıktır. 5235 sayılı Adli yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 8 inci maddesi kapsamında ceza mahkemeleri; asliye ceza mahkemeleri, ağır ceza mahkemeleri ve diğer kanunlarla kurulan diğer ceza mahkemeleri olarak ifade edilmiştir. Sulh ceza mahkemeleri ise mahkeme özelliğini kaybederek, aynı kanunun 10 uncu maddesi gereği "Sulh Ceza Hâkimliği" şeklinde teşkilatlanmıştır.

Söz konusu kanunun 10, 11, 12 ve 13 üncü maddelerinde sırasıyla; sulh ceza hâkimliği, asliye ceza mahkemesi, ağır ceza mahkemesi ve diğer ceza mahkemelerinin görevleri sayılmıştır. Anılan düzenlemeler incelendiğinde, 243 üncü maddede sayılan suçlara ilişkin iş ve davalar, sulh ceza hâkimliği ve ağır ceza mahkemeleri görevine girmemektedir. Dolayısıyla bahsi geçen Kanunun 11 inci maddesi gereğince, bu suça ilişkin olarak görevli kılınan adli merci "Asliye Ceza Mahkemesi" olup ilgili dava ve işlere bu mahkeme tarafından bakılacaktır.

Yer yönünden yetkili asliye ceza mahkemesinin tayini ise 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) bu hususu düzenleyen 12 ve devamındaki madde hükümlerine göre yapılacaktır. Sayılan düzenlemelerde "suçun işlendiği yer" mahkemesi genel yetkili mahkeme olarak karşımıza çıkmaktadır.

Doktrinde bazı yazarlar failin suçu hareketi gerçekleştirdiği yerde işlemiş sayılacağını savunmakta iken, bazı yazarlar ise neticenin gerçekleştiği yerin yetkiyi belirlemede en

uygun kıstas olacağını ileri sürmekte; Yargıtay ise suçun işlendiği yere dair, neticenin gerçekleştiği yer görüşüne katılmaktadır (Aydın, 2013, s.45).

Suçun işlendiği yer ibaresinin açıklanabilmesi için TCK'nın 8 inci maddesine bakmak gerekmektedir. Bu madde uyarınca; fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılacaktır. Dolayısıyla bu suç tiplerinin uzaktan erişim yollarıyla da işlenebildiği gerçeği karşısında, hareketin icra edildiği yer ile neticenin meydana geldiği yerin farklı olması durumunda hem hareketin yapıldığı hem de neticenin meydana geldiği yer, suçun işlendiği yer olarak kabul edilecektir. Bilişim suçlarının özellikleri dikkate alınarak suç; hareket, hareketin kısımları ve neticenin gerçekleştiği her yerde işlenmiş sayılmalıdır (Demir vd., 2015, s.6).

Bu tür suçların uluslararası bir karakter taşıdığı gerçektir. Devletler birbirlerinin yargılama yetkisini tanımıyorsa, ortada ulusal yetki yönünden bir uyuşmazlık söz konusu olup bu uyuşmazlık Lahey'deki Milletlerarası Adalet Divanı tarafından devletler hukuku normlarına göre çözülecektir (Toroslu ve Feyzioğlu, 2008, s.55-56). Bununla birlikte; konuya ilişkin yapılan uluslararası çalışmalar ve özellikle imza edilen Avrupa Konseyi Siber Suç Sözleşmesi'nin uluslararası işbirliği hükümleri çerçevesinde devletlerarası bir sorunun söz konusu olmayacağı düşünülmektedir.

CMK'nın 272 ve devamı maddeleri uyarınca; ilk derece mahkemesi sayılan Asliye Ceza Mahkemesi'nin bu suç kapsamındaki yargılama neticesinde verilen hükümlerine karşı, hükmün tefhim (kararın duruşmada doğrudan kişinin yüzüne okunması) veya tebliğinden itibaren, yedi gün içerisinde 'Bölge Adliye Mahkemesi' nezdinde istinaf kanun yoluna başvurulması istisnalar[9] haricinde mümkündür.

CMK'nın 286 ncı maddesi gereğince, Bölge Adliye Mahkemesi ceza dairelerinin bozma dışında kalan hükümleri 'Yargıtay' nezdinde temyiz edilebilir. Anılan

[9] Anılan maddenin üçüncü fıkrası uyarınca; üç bin TL dâhil adli para cezasına mahkûmiyet hükümlerine, üst sınırı beş yüz günü geçmeyen adli para cezasını gerektiren suçlardan beraat hükümlerine ve son olarak Kanunlarda kesin olduğu yazılı olan hükümlere karşı istinaf yolu kapalıdır.

maddenin ikinci fıkrası ile de temyiz edilemeyecek dokuz istisnai durum düzenlenmiştir.

Son olarak; bilişim suçlarında bilgisayarda arama, kopyalama ve el koyma tedbirlerinin 'hemen/derhal' gerçekleştirilmemesinin delillere erişmeyi imkânsız kılabileceği düşüncesiyle, elektronik verilerin kaybolma tehlikesiyle karşılaşılmamasını teminen sayılan tedbirlere olabilecek en kısa sürede başvurulması gerektiği belirtilmektedir (Ünal, 2011, s.133).

3.2 Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

5237 sayılı TCK'da bilişim sistemlerine karşı suçların düzenlendiği alanda ikinci suç olarak yerini bulan *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* suçu, 244 üncü maddede yer almış olup madde metni aşağıdaki gibidir:

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

Bu alandaki suç tiplerinde ilk olarak bilişim sistemine haksız erişim ile sistemde kalma veya sisteme girmeksizin teknik araçlarla izleme fiilleri suç olarak tanımlanmışken, izleyen maddede (TCK. m.244) sistemin işleyişinin engellenmesi, bozulması ve sistem içerisinde yer alan verilerin değiştirilmesi ile yok edilmesi fiilleri iki ayrı maddede

yaptırıma bağlanmıştır. Maddenin son fıkrasında da bu fiiller sonucu haksız çıkar elde edilmesi hususunu cezalandırma amacı taşıyan bir başka suç tipinin düzenlendiği görülmektedir. 244 üncü madde, 01.06.2005 tarihinde yürürlüğe girmiş ve bugüne kadar herhangi bir değişikliğe uğramamıştır.

Maddenin tasarı durumundaki ilk halinde sayılan tüm fiiller birinci fıkrada toplanarak, ortak ceza çerçevesinde bir ila üç yıl arası hapis cezası öngörülmüşken, TBMM Genel Kurulu'nun 16.09.2004 tarihli 121 inci birleşiminde teklif edilen önerge kabul edilmiş; *"suç tanımlarında belirliliği sağlamak ve ceza miktarlarını işlenen fiillerin ağırlığına uygun olarak belirlemek amacıyla madde metninde değişiklik yapılması uygun görülmüştür"* gerekçesiyle şuan yürürlükte olan metin kabul edilmiştir (TBMM, 2004).

Sonuç olarak ilk fıkrada; bilişim sisteminin işleyişinin engellenmesi veya bozulması, ikinci fıkrada ise bilişim sistemindeki verileri bozma, yok etme, değiştirme ya da erişilmez kılma ile sisteme veri yerleştirme, var olan verileri başka bir yere gönderme fiilleri düzenlenmiş ve aynı maddede bulunan bu iki suç tipine ilişkin olarak sonuç cezanın farklı hadlerden uygulanması uygun görülmüştür.

Anılan hükümle; ASSS'nin 4 üncü maddesinde yer alan *verilere müdahale* suçu ile 5 inci maddesinde tanzim edilen *sistemlere müdahale* suçu karşılanmaya çalışılmıştır.

3.2.1 Suçla korunan hukuki değer

Hükmün gerekçesinde bilişim sistemlerine karşı işlenen suçları cezalandırılmakta olduğu ve böylece sistemlere yöneltilen zarar fiillerini özel bir suç hâline getirdiği; ayrıca maddede geçen fiillerin, aracın fizik varlığını ve sistemin işlemesini sağlayan bütün diğer unsurları kapsadığı açıkça ifade edilmiştir.

Doktrinde özellikle birinci fıkradaki suçla korunan hukuksal değer konusunda farklı görüşler bulunsa da bunlar birbirine yakın menfaatler olup bunlar; sistemin işleyişi ve

özellikle donanımsal yanı, mülkiyet hakkı, haberleşme özgürlüğü, teknolojik gelişim özgürlüğü gibi başlıklar altında toplanabilmektedir (Dülger, 2015, s.412).

İkinci fıkrada korunan verilerin ise bilişim sisteminin içerisinde yer alsa dahi sistemin işleyişine ilişkin veriler olmadığı, zira sistemin işleyişine etki edecek verilere müdahale durumunda birinci fıkranın tatbikinin gerekeceği; diğer bir deyişle ikinci fıkrada sistemin içinde dâhil bulunan ancak sistemin yapıtaşı olmayan verilerin korunduğu belirtilmiştir (Erdoğan, 2012, s.215). Dolayısıyla ikinci fıkranın uygulanabilir olması için sistemde değiştirilen veya silinen verilerin, sistemin çalışması için 'olmazsa olmaz' bir unsur olmaması, sistem üzerinde fonksiyon yitirilmesi gibi bir duruma mahal vermemesi gerekmektedir.

Maddede genel olarak muhafaza altına alınan hukuki yarar, madde gerekçesinde de belirtildiği üzere, sistemlere yöneltilen zarar fiillerini özel bir suç haline getirme düşüncesinden hareketle; bilişim sisteminin varlığı ve işlemesini sağlayan öğeler, yani hem bilişim sistemi hem de sistem içerisinde yer alan veriler veya diğer unsurların zarar görmemesinden ibarettir (Karagülmez, 2014, s.237).

Yine ASSS'nin açıklayıcı raporu tetkik edildiğinde, bu suçu karşılayan düzenlemeler bağlamında korunan yasal menfaatin; bilgisayar verileri ve bilgisayar programlarının da, fiziksel nesneler gibi kasıtlı hasar verme girişimlerine karşı koruma altına alınmasının yanında, saklanan veri ya da programların bütünlüğü ve uygun biçimde çalışmaları ile kullanımı yararı olduğuna dikkat çekilmiştir (CoE, 2001b, s.11).

Bu çerçevede; suçla korunan hukuki değerlerin, bilişim sistemi üzerinde işlem yapan cihazın (veriyi taşıyan araçlar da dâhil) fiziki durumu ile içerisindeki soyut nitelikteki verilerin zarar görmeksizin işlemeye devam etmesi olduğu değerlendirilmektedir.

3.2.2 Suçun maddi unsurları

3.2.2.1 Fail ve mağdur

Suçun yasal tanımlamasında yer alan hareketlerin icra edilebilmesi açısından fail için herhangi bir özellikli durumun bu suç için düzenlenmediği görülmektedir.

Nitekim madde metni incelendiğinde; *"...bozan kişi..."* , *"...gönderen kişi..."* şeklindeki ibarelerden, bu suçun 'herkes' tarafından işlenebileceği kanaati mevcut olmaktadır.

Yine bilişim sistemine girme suçunda olduğu gibi, bu suçu işleyebilecek failin, bilişim alanında belli oranda bir yetkinliğinin olması gerektiği düşünülse de bu ne suçun ne de failin özelliklerinin bir şartıdır.

Suçu meydana getirecek nitelikteki fiilleri gerçekleştiren kişinin faillik sıfatının tespiti için mülkiyet, kullanım veya tasarruf yetkisinin göz önünde bulundurulması gerekmektedir: Örneğin TCK'nın 244 üncü maddesinin ikinci fıkrasındaki suçun faili, veriler üzerinde tasarruf yetkisine sahip olmayan kişi olup sistemin işleyişinin engellenmesi veya bozulması fiili açısından ise suçun faili sistemin sahibi veya kullanıcısı dışındaki kişi veya tasarruf yetkilisi dışında bir kişi olabilecek, dolayısıyla TCK'nın 244'üncü maddesinde yer alan suçların işlenip işlenmediğinin tespitinde malik veya kullanıcının ya da tasarruf yetkilisinin kim olduğunun tespit edilmesi büyük önem taşıyacaktır (Akbulut, 2016, s.19).

Bilişim sisteminin sahibi olan kişinin, sistemde rızasıyla yer almasını sağladığı üçüncü şahıslara ait verileri değiştirmesi veya verilere zarar vermesi halinde sistem sahibinin ikinci fıkradaki suçun faili olabileceği değerlendirilmektedir. Özellikle bulut bilişimde hizmet sunan sistem sahibi kişi veya şirketlerin, hizmetten yararlanan üçüncü kişilere ait verilere zarar verebilmesi riski bulunmakta olup bu tür hizmetlerin sunulması çerçevesinde bu suçun icra edilebileceği düşünülmektedir.

Bu suç mağdur açısından da herhangi bir özellik göstermemekte olup herkes suçun mağduru olabilir. Mağdurun bilişim sistemi üzerinde 'hak sahibi' olmasının yeterli olduğu, bunun sadece mülkiyet hakkı kapsamında düşünülmeksizin nispi hakka vücut veren sözleşmesel (akdi) bağlarla da mevcut olabileceğinin altı çizilmiştir (Kurt, 2005, s.163). Ayrıca kişi, veri üzerinde fikri mülkiyet hakkına sahip biri ise bu kişinin de suçun mağduru olması söz konusu olabilecektir.

Daha önce verdiğimiz örnekle de ilişkilendirilebileceği üzere; bulut bilişim hizmeti sunan sistem sahibi gerçek veya tüzel kişi ile bu hizmeti almak için akdi bir bağ kuran hizmet alıcısı kişi örneğinde mağdur, hareketin yöneldiği hukuki değere göre değişebilecektir. Bulut üzerinde verileri bozulan kişi asıl mağdur iken, sistemin güvenliğinin aşılması ve haksız erişim sağlanması sebebiyle de bulut sistemi sahibi böyle bir davada mağdur değil mahkemece kabulü halinde katılan olabilecektir.

Mağdurun bu suçta bilişim sistemi veya onu barındıran cihazın maliki veya zilyedi olması gerekmediği belirtilmekte olup, suç oluşturan hareketlerin gerçekleştirilmesi sonucunda; bilişim sistemine ve/veya verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşılması ve kullanılmasında çıkarı bulunan ve bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi bulunan kişinin de mağdur sıfatını taşıyabileceği ifade edilmektedir (Dülger, 2015, s.414).

3.2.2.2 Hareket ve netice

Suça ilişkin madde metni incelendiğinde, suçu teşkil edecek birçok hareketin sayıldığı görülmektedir. İlk ve ikinci fıkrada tanzim edilen suçlar açısından hareketlerin 'seçimlik' olduğu anlaşılmakta, bu hususa maddenin gerekçesinde de yer verilmektedir.

Bu suç genellikle icrai hareketle işlenebilecek bir suç tipidir; ancak, teknik destek sorumlusunun, kasıtlı olarak bir virüs saldırısını önlemek için gerekli yazılımları sisteme yüklememesi ya da sistemi dışarıdan saldırıya karşı savunmasız bırakması

halinde olduğu gibi bazı durumlarda suç icrai bir hareket yapmaksızın failin ihmali suretiyle de işlenebilir (Kızıltan, 2007, s.78).

Suçun ilk fıkrasında bilişim sisteminin işleyişini 'engellemek' veya 'bozulması' şeklinde iki ayrı eylem ele alınmıştır. Seçimlik suçun doğası gereği herhangi bir eylemin sistemin işleyişinin engellenmesi veya bozulmasına mahal vermesi suçun oluşması için gerekli ve yeterlidir.

- Bilişim sisteminin *işleyişinin engellenmesi* eylemi:

Kanun koyucu ilk fıkrada, eylemin kapsamını geniş tutma amacı gütmüştür. Bu çerçevede bilişim sistemine yapılan müdahale, veri işlem yapılmasını kesintiye uğratmışsa veya önlemişse sistemin işlemesine engel olunmuş olup bu anlamda sisteme ve unsurlarına zarar veren veya sistemin işlevde bulunmasını önleyen hareketler, sistemin işlemesine engel olmak kavramı altına girmektedir (Akbulut, 2016, s.27).

Daha önce de ifade ettiğimiz üzere; gerek bilişim sistemi üzerindeki soyut nitelikteki verilere uzaktan erişilmesi, gerekse sistemi barındıran fiziki cihaza bu maddede sayılan amaçla müdahale edilmesi veya zarar verilmesi bu suça vücut verecektir.

Bu suçun işlenmesinde çeşitli özellikle Dos-DDoS atakları gibi siber saldırılar suretiyle sistemin yavaşlatılması, erişilmez kılınması, kilitlenmesi gibi hususların kullanımı mümkün iken, cihazın fiziki varlığının gizlenmesi veya ortadan kaldırılması yanında, mevcut değilken sisteme şifre konulması veyahut hâlihazırdaki erişim şifresinin değiştirilmesi de suça yol açacaktır.

Sistemin işleyişinin engellenmesi, normalde sistemin yerine getirdiği fonksiyonlarını ifa etmesi kapsamında; eskisi kadar hızlı çalışmaması, veri alış verişi yapamaması, veri işleme hızının düşmesi, istenilen performansı göstermemesi, dosya ve programları çalıştırmaması, kısaca normal şartlarda yerine getirebildiği işlevlerini hiç ya da gereği gibi yapamamasını ifade etmektedir (Kurt, 2005, s.164). Pek tabi bu suçun oluşumu

için işlev yerine getirememe neticesinin, failin eylemi ile neden-sonuç ilişkisi içerisinde olması (illiyet bağının kurulması) gerekmektedir. Nitekim cihazın teknik ve ekonomik ömrünü tamamlaması veya cihaza olması gerekenden fazla sayıda işlem yaptırılmasından ötürü sistemin yavaşlamasının bu kapsamda değerlendirilemeyeceği düşünülmektedir.

Engelleme eyleminin geçici ya da sürekli olmasının suçun meydana gelmesi açısından herhangi bir önemi bulunmamaktadır (Meran, 2008, s.571). Bir seferlik dahi olsa kişinin yetkili olduğu bilişim sistemine erişiminin kasten men edilmesi hali suçun oluşumu için yeterlidir.

ASSS'nin açıklayıcı raporunda, sözleşmeye taraf devletlerin engelleme fiilinin yaptırıma bağlanabilmesi için engellemenin "ciddi ölçüde" olması gerektiği konusunda düzenleme yapma haklarının saklı olduğu ifade edilmiştir. Yine aynı raporda örneğin asgari düzeyde bir tahribatın dahi ciddi sayılabileceği veya sistemi yavaşlatan önemli virüs ve DoS saldırısı gibi metotların bu mahiyette addedilebileceği belirtilmiştir (CoE, 2001b, s.12).

- Bilişim sisteminin *işleyişinin bozulması* eylemi:

Bozmak ifadesiyle, bilişim sisteminin kendisinden beklenilen işi yapamayacak duruma getirilmesi, düzeninin karıştırılması, sisteme zarar verilmesi veya kötü duruma getirilmesi kastedilmekte olup, bir başka deyişle bilişim sisteminin işleyişinin bozulması, sistemin kısmen ya da tamamen işleyemez hale getirilmesidir (Dülger, 2015, s.419).

Her engelleme bir bozma değildir ancak engellemenin kısmen olması da yeterli olacağından, sistemin işleyişinin bozulması ayrıca sistemin işleyişinin engellenmesi sonucunu doğuracak, yani her bozma fiili engelleme neticesine de yol açacaktır. Bu husus ASSS'nin 5 inci maddesinde de verilerin bozulması yoluyla sistemin işleyişinin engellenmesi ifadesiyle yer almaktadır (Karagülmez, 2014, s.238).

Bozmanın da engelleme gibi kısmen veya tüm bilişim sistemi üzerinde olup olmamasının suçun sübutu açısından bir önemi bulunmamaktadır. Bu fiil de seçimlik türde olduğundan sistemdeki verilerle oynanması, sisteme virüs vb. saldırıların yapılması veya verilerin yer aldığı sistemi barındıran cihaz ya da taşıyıcının bu amaçla zarar uğratılması da bozma sonucuna yol açabilecektir.

Suçun ikinci fıkrasında bilişim sistemi yerine daha çok sistemde yer alan verilere dikkat çekilmiştir. Bu bağlamda verileri; 'bozmak' , 'yok etmek' , 'değiştirmek' ve 'erişilmez kılmak' ile bilişim sistemine 'veri yerleştirmek' veya 'var olan verileri başka yere göndermek' şeklinde farklı türde fiiller ele alınmıştır.

- Bilişim sisteminde yer alan *verilerin bozulması* eylemi:

Birinci fıkradan farklı olarak bilişim sisteminin değil, sistemde bulunan verilerin 'bozulması' söz konusudur. Bir üst başlıkta açıklandığı üzere bu kez kısmen veya tamamen kullanılmaz hale getirilen husus bilişim sistemi değil, verinin kendisi olmaktadır.

Bozma fiili; verilerin belirlenen amaç doğrultusunda (usulüne uygun) kullanılmasının ortadan kaldırılmasını sağlayacak şekilde verilere zarar verilmesini ifade etmekte olup, birbirine bağlı veri cümlelerinin yerlerinin değiştirilerek anlamının karıştırılması veya ilâve hususların katılması ya da veri cümlelerinden tek tek verilerin silinmesi suretiyle verilerin kullanılabilirliğine zarar verilmesi bu fiile örnek olarak verilebilir (Akbulut, 2016, s.32).

- Bilişim sisteminde yer alan *verileri yok etme* eylemi:

Yok etmek hareketi, bozma fiilinden bir adım sonrası olup artık veriye ulaşılamaz hale gelecek şekilde varlığına son verilmesi anlamına gelmektedir. Bu eylemin verinin bozulması fiilinden farkı, verinin tasarruf alanından çıkartılması veya ortadan kaldırılmasıdır (Ketizmen, 2008, s.139).

Bilişim sistemlerinde yok edildiği ‘zannedilen’ veri, her zaman gerçekten yok edilemeyebilir. Örneğin bilgisayarımızda silinen bir veri, ilk olarak geri dönüşüm kutusu adı verilen bir yere gönderilmekte ve buradan kolayca geri alınabilmektedir. Bu klasörden de verinin tekrar silinmesi halinde ise özel bazı yöntemler kullanılmadığı sürece o veriye ulaşılması ve kullanılması mümkün olmamaktadır.

Verilerin kolayca geri alınabileceği şekilde silinmesinde yok etmenin gerçekleşmediği ancak; bilişim sisteminin belleğindeki verilerin geri dönmeyecek şekilde silinmesine yol açan format uygulaması ya da geri dönüşüm kutusundaki verilerin oradan da silinmesi durumunda verilerin yok edildiğinin kabul edilmesinin gerektiği belirtilmektedir (Taşkın, 2008, s.47).

Diğer bir görüşe göre formatta da veriler silinmemekte, veri kurtarma programlarıyla bunların geri getirilmesi mümkün olabilmektedir. Ayrıca verilerin gerçek anlamda silinmesinin *“wipe”* adı verilen bir işlemle gerçekleştirilebileceği ifade edilerek, yok etme fiilinden mutlaka böyle bir işlemin anlaşılmaması gerektiği; suçun oluşumunda verilerin mağdur açısından yok edilmiş olmasının yeterli olacağı vurgulanmıştır (Dülger, 2015, s.421).

Son görüşe katılmak mümkün olup; verinin kolayca veya özel yöntemlerle geri getirilebilmesinin yok etme fiili kapsamında herhangi bir fark yaratmayacağı düşünülmektedir. Zira başkasına ait verileri silme konusunda rıza tanınmamış (yetkisiz) bir kişinin basit dahi olsa herhangi bir silme eyleminde bulunmaması gerekir. İlaveten, kanunda verinin kısmen ya da tamamen geri getirilebilir/kurtarılabilir olup olmadığına dair bir netice de aranmamıştır. Ayrıca bu suçta kullanılan cihaz sadece bilgisayar olmayıp örneğin bir mobil telefonda marka-modele göre değişmekle birlikte bu kolaylığın kullanıcısına sağlanamayabileceği ve kullanıcının böyle bir zahmete katlanmaması gerektiği kanaati mevcuttur. Bu hususun sadece verilecek ceza kapsamında bir takdiri sebep olabileceği veyahut verilerin yok edilmesi yerine veriye erişimin engellenmesi fiili kapsamında bir kanaat oluşturulmasına gerekçe teşkil edebileceği değerlendirilmektedir.

Veriyi taşıyan depolama araçlarının da (CD, DVD, taşınabilir bellek vb.) ortadan kaldırılması verilerin yok edilmesi fiiline vücut vereceğinden suçun oluşumuna yol açacaktır.

- Bilişim sisteminde yer alan *verileri değiştirme* eylemi:

Verilerin değiştirilmesi fiili, failin hangi saik ile işlediğinden bağımsız olarak, bilişim sisteminde mevcut bulunan verilerin, aslından farklı bir hale dönüştürülmesi anlamına gelmektedir.

Verilerin değiştirilmesinde amaç, veriyi yok etmek veya erişilmez kılmak demek değil, veriye ulaşıldığında verinin orijinal halinin dışında yanlış bilgilere erişilmesini sağlamaktır; zira veri değiştirildiğinde sistem işleyişine devam etmektedir (Yılmaz, 2011, s.74).

- Bilişim sisteminde yer alan *verileri erişilmez kılma* eylemi:

Verilerin erişilmez kılınması, verilerin malikinin veya ilgilisinin istediği zaman dilediği verilere ulaşmasının engellenmesi anlamına gelmekte olup; verinin bütünlüğü korunmasına (bozulmamış/yok edilmemiş) rağmen hak sahibi, virüs bulaştırılması, şifre konulması vs. birçok çeşitli sebeple kendi verilerine erişememektedir (Dülger, 2015, s.422).

Yargıtay, kişinin rızası dışında e-posta veya sosyal medya şifrelerinin değiştirilmesi suretiyle asıl kullanıcının sisteme erişimin engellenmesini de bu kapsamda değerlendirmiştir. Yüksek Mahkemenin 8. Ceza Dairesi'nin 17.03.2016 tarihli ve E.2015/11993, K.2016/3544 sayılı kararında bu hususun altının çizildiği görülebilmektedir (Corpus, 2018):

"...Şikayetçiye ait facebook adresine sanık tarafından şifresinin kırılması yoluyla girildiği ve şifresinin değiştirilmesi suretiyle erişilemez hale getirildiği iddiasıyla açılan davada, sanığın tüm aşamalardaki savunmasında şifreyi kendisinin

değiştirmediğini savunması karşısında, ***sanığa ait bilgisayardan şikayetçinin facebook hesabına giriş yapıldığı tespit edilmişse de, şikayetçinin adresine girişinin engellendiğine dair bir tespitin bulunmaması karşısında****; şikayet tarihinden önce facebook adresinin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı araştırılarak ve şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarasından sağlanan erişim sonucu değiştirildiği ilgili internet sağlayıcısından ve facebook şirketinden sorulup* ***erişilmez kılındığı takdirde TCK.nun 244/2., aksi takdirde aynı yasanın 243/1 inci maddesi kapsamındaki suçu oluşturacağı gözetilerek*** *sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmayla yazılı şekilde hüküm kurulması...”*

Söz konusu Yargıtay ilamı özellikle 243 üncü madde ile ilişki kurduğu için önem taşımakta olup; kararda özetle şahsi sosyal medya hesabına girişin ‘engellenmesi’ söz konusu ise 244/2 hükmünün, engelleme yok ancak herhangi bir şekilde ‘haksız erişim’ söz konusu ise 243 üncü maddenin tatbikinin uygun olacağına isabetli şekilde hükmedilmiştir.

- Bilişim sistemine *veri yerleştirme* eylemi:

Bahsi geçen suçun diğer hareket ve neticelerinde, sistem üzerinde yer alan verilerin bozulması, yok edilmesi gibi fiillerden bahsedilmekte iken; hükmün bu kısmında sistemde mevcut olmayan bir verinin, sistem üzerine işlenmesinden söz edilmektedir.

Yerleştirme fiili, bilişim sisteminin orijinalinde mevcut olmayan verilerin sisteme dâhil edilmesi anlamına gelmektedir (Eker, 2006, s.125). Dâhil etme hususu, doğrudan veya herhangi bir teknolojik vasıta ile sistem sahibinin rızası dışında gerçekleşen yükleme, kaydetme, ekleme gibi eylemleri kapsayabilecektir.

Bilişim sistemine veri yerleştirme fiili, “cd-rom” “harici disk” ya da “usb bellek” gibi fiziki veri depolama araçlarından birisi vasıtasıyla sisteme veri kaydetmek şeklinde yapılabileceği gibi; internet gibi bir bilişim ağı aracılığı ile uzaktan veri yüklemek

şeklinde de gerçekleştirilebilecek olup sisteme hukuka uygun veya aykırı girilmesinin bu suç açısından önemi bulunmamaktadır (Kızıltan, 2007, s.83).

Bununla birlikte; failin amacı veya verinin yasal olup olmamasının da suçun oluşumunu etkileyen bir unsur olmadığı değerlendirilmektedir. Sisteme olmayan bir veriyi yerleştiren fail bu suçu o anda işlemektedir; mağdura zarar verme amacı, ancak ceza ve/veya tazminat tayininde gözetilebilecek bir husus olabilecektir.

- Bilişim sisteminde var olan *verileri başka bir yere gönderme* eylemi:

Verileri başka bir yere göndermek kavramının hukuk doktrininde; sistemin içerisinde yer alan verilerin yerini değiştirmek, mağdura ait verilerin gerek mağdurun bilişim sisteminde farklı bir dosyaya, gerekse farklı bir bilişim sistemine gönderilmesi, bir bilişim sistemi içerisindeki verilerin başka bir bilişim sistemine ya da veri taşıma cihazına aktarılması, kaydedilmesi ya da kopyalanması; sistemde yer alan orijinal verilerin herhangi bir surette (orijinal yerinden, konumundan) başka bir yere taşınması, götürülmesi, gönderilmesi eylemleri şeklinde tanımlandığı ifade edilmektedir (Erdoğan, 2011, s.203).

Bu hareket kapsamında verinin niteliğinin önem arz ettiğinin altı çizilerek; bunun kişisel veri mahiyetinde olmasının başka bir suça (TCK. m.136) , parayı temsil eden veri niteliğinde olması halinde ise yine başka bir suça (TCK. m.142) vücut vereceği vurgulanmıştır (Dülger, 2015, s.428-429).

Bu suçun ilk fıkrası, 243 üncü maddede olduğu gibi neticesiz değil neticenin arandığı bir suç tipidir. Zira kanunda sayılan eylemler ile sistemin işleyişinin engellenmesi veya verilerin bozulması gibi sonuçların gerçekleşmesi beklenmektedir.

Kanun koyucu bu suçta neticeyi belirlerken, isabetli bir şekilde çok geniş davranmış ve boşluğa mahal vermemiştir. Ancak bilişim teknolojileri dikkate alındığında yapılan bir hareket sonucunda buradaki neticelerden birkaçı aynı anda gerçekleşebilir. Örneğin; bir verinin bulunduğu yerden kesilerek alınıp başka bir sisteme kaydedildiği

durumda veriyi yok etmek, erişilmez kılmak ve başka bir yere göndermek neticelerinin tamamı oluşmaktadır. Bu gibi hallerde birden fazla netice meydana gelse de ortada bir hareketle gerçekleştirilen tek bir suç vardır ve bu durumda tek ceza tayin edilmelidir (Erdoğan, 2011, s.194).

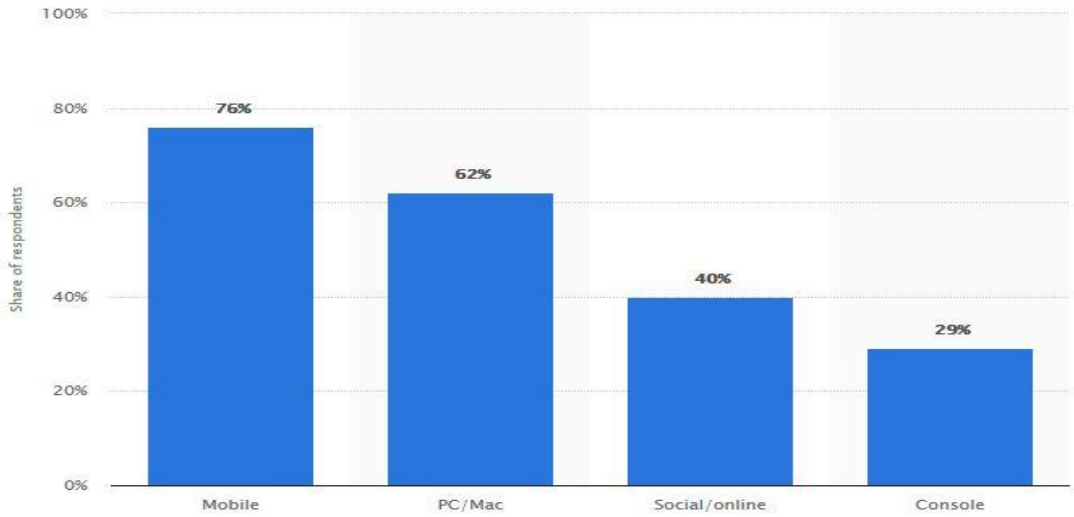
3.2.3 Dijital oyun sektörünün suçla ilgisi

1970'lerde ortaya çıkan ve şahsi bilgisayarlar, oyun konsolları veya mobil cihazlar vasıtasıyla oynanabilen, oynandığı platforma göre de bilgisayar oyunları, konsol oyunları ile yakın zamanda ortaya çıkan mobil ve çevrimiçi oyunlar alt kategorilerine ayrılabilen elektronik oyunlara 'dijital oyunlar' denmekte olup bu oyun platformları 'milyar dolarlar' ile ifade edilen bir sektör yaratmıştır (Statista, 2018b).

Hikâyeden karakterlere, bilgisayar efektlerinden sinema araçlarına, tasarımdan pazarlamaya ve daha birçok alanda geniş bir yelpazeden oluşan dijital oyun sektörü de bilişim alanında suçlar alanında faillere cezbedici gelmektedir.

Tüketicilerin dijital oyunlar bakımından platform tercihleri ise aşağıdaki gibidir (Statista, 2018c):

Şekil 3.1 Tüketicilerin Dijital Oyun Platformu Tercihleri



Diğer platformlardan çok daha sonra ortaya çıkmasına rağmen, tüketicilerin bilgisayar ve konsol ortamı yerine mobil cihazlar üzerinde oyun oynamayı tercih ettikleri görülmektedir.

2018 yılının Nisan ayında Bilgi Teknolojileri ve İletişim Kurumu nezdinde gerçekleştirilen Dijital Oyunlar Kongresi'nde; krizlerden en az etkilenen ve katma değeri çok yüksek olan bu sektörün, hızla geliştiği ve büyüdüğüne dikkat çekilmiş, dünyada 1 milyarın üzerinde kişinin dijital oyun oynadığı bilgisi paylaşılmıştır (BTK, 2018).

Dijital oyunların genellikle bağımlılık[10], şiddete eğilim, sosyal ilişkilerden uzaklaşma, zaman ve enerjinin uygun kullanılmaması, fiziki deformasyon vb. şekilde zararlarından bahsedilse de (BTK-BilgiZone, 2018c), tersi bulguları olan çalışmalar da mevcut olup bu tür oyunların faydaları; stres ve depresyonu azaltma, beyni rahatlatma, görüşü iyileştirme, karar verme mekanizmalarını güçlendirme vb. olarak sıralanmaktadır (Türkiye Oyun Geliştiricileri Derneği-Toged, 2014).

Dijital oyun sektöründe oyun geliştiricilerin fikri haklar (özellikle telif hakları) konusunda sorun yaşadığı, oyuncuların ise genellikle büyük bir zaman ve maddiyat harcadıkları oyun karakterlerinin başkalarının eline geçme problemleri ile karşı karşıya oldukları belirtilmiştir (Şıracı, 2016a).

Bu çerçevede çevrimiçi (*online*) dijital oyunların ticari değer taşıdığı yadsınamaz. Ayrıca tüketicilerin bu tür oyunlara büyük zaman ve para ayırdığı gerçekleri karşısında, bu oyunlara bağlı hesapların ve içerisindeki karakterlerin, bilişim sistemlerinin usulsüz kullanılması suretiyle kaybedilmesi mümkündür. Nihayet, adli merciler nezdinde de dijital oyunlar hususu dikkate alınarak konuya özel kararlara hükmedilmektedir.

[10] Oyun bağımlılığının, Dünya Sağlık Örgütünce (*World Health Organization*-WHO) 'hastalık' olarak tanımlandığı ve bazı ülkelerce de asli bir sağlık meselesi olarak ele alındığı ifade edilmektedir (BBC, 2018).

Konuya ilişkin olarak güncel sayılabilecek, Yargıtay 13. Ceza Dairesi'nin 10.10.2017 tarihli ve E.2016/2155, K.2017/10403 sayılı kararı aşağıdaki gibidir:

"...Katılanın 23.10.2011 tarihinde ... isimli oyunu oynarken ***bilgi ve rızası dışında e-posta adresine girilerek şifresinin ve e-posta adresinin değiştirildiğini ve oyun karakterlerinin çalındığını****, karakterlerini çalan şahsın olaydan 10 dakika önce kendisine mesaj gönderdiğini, oyun içi iletişim sayesinde çalınan oyun karakterlerini ... isimli şahsın satın aldığını beyan ettiği; dosya kapsamına göre olay günü sanığın babası adına kayıtlı ve fakat* ***sanık tarafından kullanılan IP adresi üzerinden katılanın e-posta adresine erişimin sağlandığı****... oyun sitesinden suç tarihinde katılanın kullanıcı adı ve şifresi ile oyuna giriş yapılıp yapılmadığının sorularak, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren ... ve/veya kimin kullanımında olduğunun ve olaydan önce katılana mesaj gönderen kişinin kim olduğunun araştırılarak, yine talimat mahkemesinde beyanı alındığı sırada katılan tarafından dosyaya ibraz edilen CD içeriği ile tüm deliller birlikte değerlendirilip, gerektiğinde bilişim suçlarından anlayan tercihen bilgisayar mühendisi bir bilirkişiden rapor da alınmak suretiyle, toplanan ve toplanacak delillerin birlikte değerlendirilmesi ile sonucuna göre tüm deliller çerçevesinde ... karar verilmesi,*

*...****Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının****; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği, bu itibarla;* ***suçun sübutu halinde eylemin, 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturacağı****... Eylemin sübutu halinde* ***tek suç oluşturacağı****..."* (Yargıtay, 2018)

Mezkûr kararın analizi bağlamında dijital oyun hesaplarındaki ögelerin (karakter, eşya, sanal dünyaya ait diğer veriler vb.) hukuka aykırı olarak ele geçirilmesi ve erişilmez kılınması TCK m.244/2'deki suça; bundan yarar sağlanması (bahse konu ögelerin kullanılması ve/veya bir başkasına menfaat karşılığı temin edilmesi) halinde ise bu kez TCK m.244/4'teki suçtan ceza verilebilecektir. Bu kapsamda, dijital oyun platformlarını kullanan özellikle küçük yaştaki kişiler korunmaya çalışılmaktadır.

3.2.4 Suça etki eden sebepler (Nitelikli haller)

3.2.4.1 Suçun ağırlaştırılmış nitelikli hali

Suçun düzenlendiği 244 üncü maddenin üçüncü fıkrasında, ilk iki fıkrada icra edilen fiillerin; *bir banka veya kredi kurumuna*[11] *ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi* durumu ağırlaştırılmış nitelikli hal olarak düzenlenmiştir.

Kanuni düzenlemede bu hükümle kamu kurumları ve finans kuruluşlarının bilişim sistemlerine karşı işlenen fiillere ayrı bir önem atfedilmiş olup suçun üçüncü fıkrasına dayanılarak hüküm kurulması halinde faile verilecek ceza yarı oranında artırılacaktır.

Nitelikli hal uygulamasının yalnızca banka veya kredi kurumu ya da kamu kurum ve kuruluşlarıyla sınırlanmasının, bir şirket veya işletme açısından da sistemin işleyişinin engellenmesinin çok fazla önem taşıyabileceği gerekçesiyle eksik düzenleme niteliğinde olduğu belirtilmiş ve sınırlamanın sadece belirtilen kurum ve kuruluşlarla ilgili olarak tanzim edilmesi eleştirilmiştir (Akbulut, 2016, s. 52).

Kanımızca; ASSS'de yer alan "ciddi ölçü" kavramı bu kez bir bakıma bu fıkrada karşılanarak düzenleme alanı bulmaktadır. Devletin yasama, yürütme, yargı erklerini icra eden kamu kurum ve kuruluşlarında öncelikle devlet sırrı niteliğini haiz veriler bağlamında milli güvenliğin temini, vatandaşlara kamusal hizmetin kesintisiz ve sağlıklı sunulması dolayısıyla bu hususun toplumun büyük kısmını ilgilendirmesi gibi sebeplerden ötürü kamudaki bir bilişim sistemine karşı sayılan fiillerin işlenmesinin bireysel bir faydadan daha önemli tutulması yerinde olmuştur. Yine çok sayıda kişinin yüksek mali veriler içeren hesaplarını elinde bulunduran finans kuruluşlarının, bu

[11] 5411 Sayılı Bankacılık Kanunu uyarınca Banka: mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını ifade etmekte iken; TCK'nın 158 inci maddesinin birinci fıkrasının (j) bendinde geçen kredi kurumundan, banka olmamasına karşın faiz karşılığında olsun veya olmasın kanunen borç para vermeye yetkili kılınan kurumların anlaşılacağı madde gerekçesinde belirtilmektedir.

alanda daha çok hedef alınmaları sebebiyle bu tür kuruluşların bilişim sistemlerine karşı işlenecek suçlar ile bir kişiye karşı bu suçun işlenmesi çerçevesinde mağduriyetler karşılaştırıldığında terazi, çoğunluğun ekonomik verileri tarafında ağır basacağından ağırlaştırıcı düzenlemenin isabetli olduğu değerlendirilmektedir.

Ayrıca sayılan yapılarda görev yapan banka görevlisi veya kamu personelinin herhangi farklı bir ağa ihtiyaç duymaksızın, hatta güvenlik duvarı vb. koruyucu unsurları aşmaları gerekmeden kolayca bu suçu işleyebilmelerinin mümkün olması nedeniyle bu kişilerin fail olmaları durumunun da ağırlaştırıcı sebep olması savunulmaktadır (Erdoğan, 2012, s.197). Bu görüşe katılmak mümkündür. Zira anılan birimler bünyesinde görev yapan kişilerin sisteme erişim sağlamasından, verilere erişmesine ve işlem yapmasına kadar dışarıdaki bir failden çok daha fazla olanağa sahip olduğu açıktır. Bu kapsamda bu kişilerin kendilerine duyulan güveni ihlal etme ve özellikle sahip oldukları kamu görevlisi sıfatı ile bağdaşmayacak bu hareketlerinin daha ağır bir ceza ile karşılanması uygun olacaktır.

Son olarak 3713 sayılı Terörle Mücadele Kanunu'nun *"Terör amacı ile işlenen suçlar"* kenar başlıklı dördüncü maddesinde katalog şeklinde sayılan suçlar arasında TCK'nın 244 üncü maddesi de yer almakta olduğundan, aynı Kanunun *"Cezaların artırılması"* başlığını haiz 5 inci maddesi de uyarınca sayılan cezai hükümler sonucunda bu suçun ağırlaştırıcı nitelikli bir hali daha hukuk düzenimizde yerini almış olmaktadır.

Bu suça ilişkin olarak herhangi bir hafifletici neden öngörülmemiştir.

3.2.5 Suç tanımındaki eylemlerin haksız çıkar sağlamak için işlenmesi

Mezkûr suçun son fıkrasında, bilişim sistemi kullanılarak hukuka aykırı yarar elde edilmesi eylemi ile ilk üç fıkrayı kapsayan ayrı bir suç tipi düzenlenmiştir.

Söz konusu düzenlemede, maddede sayılan fiillerin işlenmesi suretiyle bir kişinin kendisi veya bir başkasının yararına haksız bir çıkar oluşması durumunun başka bir suç oluşturmaması halinde bu maddeden ceza verilebileceği hükme bağlanmıştır.

Bu suçta bilişim sistemine yapılan müdahaleler suretiyle haksız çıkar oluşturulması söz konusudur. Yani hareket bir başka kişiye değil sisteme ve verilere yönelmiş durumdadır.

Haksız çıkar bir diğer deyişle 'hukuka aykırı yarar' unsuru; genellikle bu suçta uygulamada ekonomik değeri olan mali bir yarar olsa da, tamamen duyguları tatmine yönelik manevi bir yarar da olabilir (Dülger, 2015, s.443). Nitekim bir ticari ya da şahsi sırrın veya mağdurun üzerinde çalıştığı özellikli bir projenin haksız olarak ele geçirilerek, bir başkasının bilmemesi gerektiği halde öğrenilmesi söz konusu olabilir ve bu çerçevede haksız çıkar her zaman mali bir unsur olmayabilir.

Bu düzenlemede odak noktası, bilişim sistemi aracılığıyla yarar sağlama fiillerinde kişiye karşı bir hile yapılması sonucunda kişinin aldatılmasının söz konusu olmaması nedeniyle, kişiye karşı hileli hareketin yapılması unsurunun yerini, bilişim sisteminin işleyişine veya veriye müdahale edilmiş olması unsurunun almış olmasıdır (Ketizmen, 2008, s.149).

Fıkranın gerekçesinde; *"...Üçüncü fıkrada ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için,* ***fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir****. Bu bakımdan,* ***fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir****..."* denilmektedir (TBMM, 2004).

Madde metninde yer almamasına rağmen, kanun maddelerinin yorumlanması için büyük önem taşıyan gerekçede "daha ağır ceza gerektiren" ibaresinin uygulamada sorun yaratabileceği değerlendirilmektedir. Yasal metinde sadece bu suçun başka bir

suç oluşturmaması unsuru aranmakta olup; haksız çıkar sağlanması çerçevesinde genellikle bu suçtan daha yüksek cezaları içeren mal varlığına karşı suçlarla karşılaşılmasının söz konusu olması sebebiyle, madde gerekçesinde olmaması gereken bir ibarenin kayıtlara geçmiş olduğu kanaati mevcuttur.

Konuya ilişkin olarak Yargıtay 11. Ceza Dairesi'nin 07.10.2009 tarihli ve E.2009/1616, K.2009/11328 sayılı kararı aşağıdaki şekildedir (Corpus, 2018):

*"...**Dolandırıcılık suçu**; hileli davranışlarla bir kişinin aldatılıp onun veya bir başkasının zararına, failin kendisine veya bir başkasına yarar sağlaması suretiyle oluşur. **Suçun maddi unsurunu oluşturan hareketlerin, gerçek bir kişiye yöneltilmiş olması, onun kandırılarak çıkar SAĞLANMASI GEREKİR**. **Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunda ise, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler araç olarak kullanılıp gerçek kişiler aldatılarak ÇIKAR SAĞLANMAKTADIR.** Bankaların etkin işlevi bulunan çek, hesap cüzdanı, dekont gibi maddi varlıklarının kullanılması halinde ise, banka vasıta kılınarak dolandırıcılık SUÇU OLUŞACAKTIR*

*Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, **kişilere yönelik hileli davranışlarla aldatılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde "bilişim sistemine girerek haksız çıkar sağlama suçu" gerçekleşecektir**"*

Yukarıdaki kararın analizi bağlamında; başka bir suçu oluşturmama ibaresi ile "yardımcı/tali" bir norm mahiyetinde kuralın varlığından söz konusu olup, öncelikle icra edilen eylemin bir başka suça vücut verip vermeyeceği araştırılması gerekmektedir. Burada eylem ile birlikte failin yöneldiği hedef yani kastı da büyük önem taşımaktadır. Failin hedefi 244 üncü maddede yer alan fiillerden biri ile bilişim sistemlerine müdahale ve haksız çıkar sağlamak ise yani asıl hedef olan örneğin bir kısım para, altın vb. değerlerin ele geçirilmesi kastı varsa bilişim sistemleri

kullanılarak hırsızlık suçu meydana gelecektir. Bilişim sistemine girilse dahi bir kişinin aldatılarak yapmaması gereken bir işleme yönlendirilmesi suretiyle çıkar sağlama söz konusu ise bu kez de bilişim sistemleri kullanılarak dolandırıcılık suçundan hüküm kurulması beklenecektir.

Nitekim Yargıtay 2. Ceza Dairesi'nin 25.02.2016 tarihli ve E.2014/20601, K. 2016/3182 sayılı kararında (Corpus, 2018):

"Sanığın müdahile ait ***şirketin hesaplarına internet üzerinden girerek başka hesaplara para aktarıp menfaat temin etmesi*** *şeklindeki olayda, eylemin TCK'nın 142/2-e maddesine göre* ***hırsızlık suçunu oluşturduğunun anlaşılması*** *karşısında* ***suç vasfında yanılgı sonucu aynı Kanun'un 244/1-4 maddesi gereğince yazılı şekilde cezalandırılmasına karar verilmesi ... Bozmayı gerektirmiştir****"* denilerek madde metnindeki 'başka bir suçu oluşturmama' ibaresine işlerlik kazandırılmıştır.

Bu suça örnek olarak vergi mükellefi olan bir failin kendisi veya bir başkası adına Hazine ve Maliye Bakanlığı'nın ilgili bilişim sistemlerine erişim sağlayarak ödenmeyen vergi ve sair yükümlülüklerini ödenmiş şeklinde değiştirilmesi verilebilir. Bu örnekte erişilen bilişim sistemi ayrıca bir kamu kurumuna (Bakanlık) ait olduğu için 244 üncü maddenin üçüncü fıkrasındaki ağırlaştırıcı neden de uygulama alanı bulacak ve faile verilecek ceza yarı oranında artırılacaktır.

Yine fiziki ortam yerine bilişim sistemleri aracılığıyla sunulan bir eğitim veya sertifika programına ilişkin olarak, bu sistemlere erişmek suretiyle kendisi veya başkasının bu eğitimi almamasına rağmen almış gibi sistemde oynama yaparak sertifika üretilmesi de haksız çıkar sağlanması anlamına gelecektir.

Bu suçta mağdurun her zaman bilişim sisteminin sahibi veya kullanıcısı olması da gerekmemektedir. Failin örneğin rakip bir firma ya da kişi hakkında manipüle edici haberler çıkmasına sebep olan bir veri değişimi, veri bozulması veya veri gönderimi hareketlerinin icrası sonucunda, bilişim sistemi sahibi değil bundan doğrudan zarar gören kişi veya şirket ve hisse sahipleri mağdur sıfatını taşıyacaktır.

Maddenin tümünü kapsayacak somut bir olaya örnek vermek gerekirse; fail, bir bilişim sistemine virüs, bilgisayar solucanı, truva atı gibi sistem için zararlı programları göndermek suretiyle sistemin içinde yer alan verilere 'zarar' verirse 244 üncü maddenin ikinci fıkrasında yer alan suçu, aynı virüs ile sistemin tamamının 'işleyişini engeller veya bozarsa' aynı maddenin birinci fıkrasında yer alan suçu işlemiş olacak; nihayet bu kişi söz konusu eylemi ile 'virüs koruma programları üreten bir firmanın ürün satışlarını artırmayı amaçlıyorsa ve bu amacına da ulaşırsa' yani bu eylemden ötürü haksız çıkar sağlamış olursa maddenin son fıkrası hükmünden cezalandırılacaktır (Turhan, 2006, s.146).

Bu fıkrada yer alan suç tipinden söz edilebilmesi için bir başka suçun (uygulamada genellikle hırsızlık, dolandırıcılık, zimmet vb.) oluşmaması ön şartı oldukça önemlidir. Bu nedenle her somut olayda bu hususun özellikle gözetilmesi büyük önem taşıyacaktır.

3.2.6 Suçun manevi unsurları ve hukuka aykırılık

Bir önceki suçta da izah edildiği üzere ASSS'de düzenlenen tüm suçlar açısından failin kastla hareket etmesi zorunludur. Burada bahsedilen genel kast olup, taraf ülkeler belli durumlara has olmak üzere bazı suçların tanımında özel kast unsurunu da arayabilecektir.

Bir suçun taksirle işlenebilmesi için bu durumun kanunda açıkça öngörülmesi şarttır. Söz konusu suç incelendiğinde suçun taksirli halinin tanzim edilmediği görülmekte olup suçun taksirle işlenmesi mümkün değildir. Bu kapsamda suçun manevi unsurunun 'kast' olduğu açıktır. Fail burada icra ettiği eylemin bilişim sistemini engellediği, verileri bozduğu veya bu suretle kendisi ya da bir başkasına haksız çıkar sağladığını bilmeli ve istemelidir.

Her suçta olduğu gibi bu suçta da hukuka uygunluk sebepleri suçun oluşumunu engelleyici nitelikte rol oynayacaktır. Dolayısıyla cihaz veya sistem sahibinin rızasıyla

erişim sağlayan bir bilgisayar uzmanının sistemi iyileştirmek için format vb. işlemler uygulamak zorunda olması halinde suç oluşmayacak ancak verilen rızanın/yetkinin sınırının aşılması halinde, örneğin tamir için verilen bilgisayardan gerekmediği halde verilerin alınması ya da silinmesi vb. hallerde suçun gerçekleştiği kabul edilecektir.

Bilişim suçlarının ilki olan sisteme haksız erişim eyleminde de bahsedildiği üzere bu suç tipinde de meşru müdafaanın kabulü mümkün olmayacaktır. Ancak bu suçta verilere ve sisteme zarar verme eylemi, gerek ASSS'de gerekse TBMM'nin gerekçesinde açıkça ifade edildiği üzere verilerin bulunduğu fiziksel eşyaya zarar verilmesini de kapsadığından; bilişim sistemini barındıran cihaz veya depolama ünitelerine fiziki temasla saldırı gerçekleştiriliyorsa, diğer şartların da mevcudiyeti halinde meşru savunma olanaklıdır (Erdoğan, 2011, s.164).

Görevin ifası kapsamındaki fiiller de fiilin hukuka uygunluğunu sağlayacak olup örneğin 5651 sayılı Kanun gereğince erişimin engellenmesi kararının verilmesi ve bu kararın yerine getirilmesi durumunda fiil, sistemin işleyişinin engellenmesi suçunu oluşturmayacak; yine belirli döneme ait veya bazı şartların gerçekleşmesi şartıyla, vergi borçlarının silinmesi yolunda ilgili kamu otoritesince karar alınması ve buna dayanılarak yapılan düzenleme çerçevesinde vergi borçlarının elektronik ortamda silinmesi durumunda, verileri silen kişi verileri yok etmekten veya haksız çıkar sağlamaktan sorumlu tutulmayacaktır (Akbulut, 2016, s.40).

3.2.7 Suçun özel görünüş biçimleri

3.2.7.1 Teşebbüs, iştirak ve içtima

Suç serbest hareketli ve neticenin arandığı bir suç olduğundan teşebbüsün mümkün olacağı düşünülmektedir. Failin bilişim sisteminin işleyişini bozmak veya engellemek için icra hareketlerine başlayıp elinde olmayan nedenlerle engelleme veya bozma sonucunu gerçekleştiremezse eylem teşebbüs aşamasında kalmış sayılacaktır; örneğin failin amaca elverişli bir virüsü sisteme göndermesine karşın, anti virüs programı

sayesinde sistemin işleyişini engelleyememiş veya sistemi bozamamışsa, bu suça teşebbüsten cezalandırılmalıdır (Erdoğan, 2012, s.202).

Suçun son fıkrasında yer alan haksız çıkar sağlama suçu açısından ise Yargıtay'ın farklı kararları bulunmakta olup 2008 tarihli bir kararında (6. CD. E.2008/555, K.2008/12249) verinin failin ulaşmasını istediği sisteme gitmiş olup olmaması suçun tamamlanması açısından önemsenmemişken; 2009 tarihli bir başka kararında ise (11. CD. E.2009/3700, K.2009/6207) sistem aracılığıyla gönderilen yararın fiilen elde edilmemesi halinde teşebbüs aşamasında kalındığı sonucuna ulaşılmıştır (Dülger, 2015, s.453).

Yukarıdaki kararlar analiz edildiğinde Yargıtay'ın iradesi çerçevesinde haksız yararın "elde edilmesi" mutlak surette aranmaktadır. Ancak kanımızca haksız çıkar sağlayan işlemi oluşturan hareketin gerçekleştirilmesi yeterli olup failin ya da üçüncü bir kişinin bu yararı fiilen elde etmemesi veya vazgeçmesi suçun oluşumunu engellememelidir. Bu kapsamda, şartları oluşması halinde en fazla "gönüllü vazgeçme" hükümlerinden yararlanılmasının söz konusu olabileceği ve bu kapsamda o aşamaya kadar işlenen suçlardan sorumluluğun devam edeceği değerlendirilmektedir.

Bu suç açısından iştirake yönelik özel bir hüküm bulunmadığından, suça iştirakin her türü mümkün olup bu çerçevede TCK'nın 37 vd. iştirak müessesesini düzenleyen genel hükümlerin tatbiki söz konusu olabilecektir. Suçun son maddesinde yerini bulan haksız çıkar sağlama eylemi kapsamında, failin sisteme müdahale eden ve verilerle oynayan kişi olmasına karşın fayda sağlayan kişinin üçüncü bir şahıs olmasında iştirak maddeleri uygulanamaz. Çünkü haksız çıkar sağlama suçunun yasal tanımında *"kendisinin veya başkasının yararına"* fiilin işlenmesi hususu hüküm altına alınmıştır. Pek tabii sistemi veya verileri engelleyen, bozan kişinin birden fazla kişi olması halinde iştirak durumu işlerlik kazanacaktır.

Bilişim sistemini barındıran cihaz ya da depolama aygıtlarına verilen fiziksel zarar kapsamında, failin kastı sadece eşyanın zarar görmesi ise bu kez 244 üncü maddede düzenlenen suç yerine TCK 151 nci maddede yerini bulan "mala zarar verme" (nas-ı

ızrar) suçu nedeniyle ceza verilmesi gündeme gelecektir. Ancak fail, başkasının mülkiyetinde olan bir sisteme zarar vermek suretiyle verileri de yok etmişse hem mala zarar verme suçunu hem de m. 244/2'yi ihlal edecek, suçlar tek fiille gerçekleştirilmiş olacağından fikrî içtima hükümlerine göre sorumluluğun tayini gerekecektir (Akbulut, 2016, s.45). Failin kendi bilgisayarını parçalaması durumunda ise kişinin kendi mülkiyetindeki mala karşı mala zarar verme suçu işlemesi mümkün olmayacak; ancak içerisinde bir başkasına ait verilerin bulunması ve bunlara zarar verilmesi halinde m. 244/2'den hüküm kurulacaktır.

Maddenin son fıkrasında tanzim edilen haksız çıkar sağlama suçu ise açıkça fıkrada *"...başka bir suç oluşturmaması halinde..."* lafzı geçtiğinden yardımcı nitelikte bir cezai normdur. Bu nedenle bilişim sistemi üzerinde icra edilen eylemin aynı zamanda bir başka suça vücut vermesi durumunda içtima hükümleri uygulanmayarak m. 244/4'te düzenlenen suçtan değil oluşan 'diğer' suçtan ceza verilecektir.

Aynı suç işleme kararının icrası kapsamında, bir mağdurun bilişim sistemine karşı, farklı zamanlarda, 244 üncü maddede sayıla fiillerin işlenmesi durumunda TCK m. 43/1'de düzenlenen zincirleme suç hükmünün uygulanması söz konusu olacaktır.

Bir virüsün internet sitesinde yayınlanması neticesinde, çok sayıda kişinin bu virüsü bilişim sistemine indirmesi ve sistemlerinin zarar görmesi halinde, TCK m. 43/2 kapsamında zincirleme suç olgusunun tatbiki mümkün olacaktır (Dülger, 2014, s.19).

Son olarak 243 üncü madde kapsamında açıklandığı üzere, failin kastı da dâhil olmak üzere iradi eylemi yanında, failin eyleminin suçlar arasındaki zorunluluk ilişkisi gibi hususlar yargı yerince araştırılarak içtimaın türünün belirlenmesinin uygun olacaktır. Bu çerçevede 244 üncü maddede yazılı suçlar için mutlaka 243 üncü maddede sayılan fiillerin gerçekleşmesi gerekmediğinden 'gerçek içtima' hükümlerinin uygulanarak her suçtan ayrı ayrı ceza verilmesi gerekir. Ancak kişinin bilişim sistemine girme veya orada kalması fiilinde, failin kastının asıl olarak sistemin işleyişini engelleme veya sistemdeki verileri bozma ya da bu suretle haksız çıkar sağlamak olduğu ortaya çıkıyorsa, 243 üncü maddede sayılı fiillerin 'geçit' özelliğinden söz edilerek fikri

içtima hükümleri uygulanması dolayısıyla tek ama en ağır sonuçlu suçtan ceza verilmesi değerlendirilebilecektir.

3.2.8 Yaptırım ve yetkili adli merci

Söz konusu suç re'sen soruşturulan ve kovuşturulan (şikâyete tabi olmayan) bir suç olup 4 ayrı fıkradan oluşmakta ve her fıkrada ayrı yaptırım aralıklarına rastlanmaktadır.

Birinci fıkra kapsamında (m. 244/1) verilecek ceza, bir yıldan beş yıla kadar hapis cezası olarak öngörülmüştür. Düzenlemede ayrıca alternatif adli para cezası yaptırımına yer verilmemiştir.

İkinci fıkrada tanzim edilen suç türünde ise verilecek ceza, altı aydan üç yıla kadar hapis cezası şeklinde hükme bağlanmıştır. Bu fıkrada da adli para cezası yaptırımı mevcut değildir.

Maddenin üçüncü fıkrasında neticesi sebebiyle ağırlaşmış nitelikli hal düzenlenmiş olup ilk iki fıkrada sayılan hangi fiil işlendi ise, faile o fıkrada tatbik edilecek ceza 'yarı oranında' artırılarak verilecektir. Böylece failin ilk fıkraya uyan eylemi ile bir kamu kurumu veya finans kuruluşunun bilişim sistemine müdahale etmesi halinde, alt sınırdan ceza verilmesi düşünülüyor ise bu süre iki yıl, üst sınırdan ceza uygulanması söz konusu ise bu süre on yıla kadar çıkabilecektir.

Verilecek sonuç ceza, 243 üncü madde için yaptığımız açıklamalar paralelinde, hâkimin takdirinde olup TCK'nın *"Cezanın Belirlenmesi ve Bireyselleştirilmesi"* başlıklı üçüncü bölümünde yer alan 61 ve devamı hükümler kapsamında, yasada belirlenen durumların birlikte gözetilmesiyle, her somut olayda ayrı ayrı ele alınarak karara bağlanmalıdır.

Maddenin son fıkrasında ayrı bir suç tipi olarak düzenlenen haksız çıkar sağlama suçunda ise iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına

hükmolunacağı ifade edilmiştir. Fıkrada yazılı ‘ve’ bağlacı sebebiyle para cezası alternatif değil, hürriyeti bağlayıcı cezaya ‘ek’ yani ilave bir yaptırım olarak birlikte uygulanacaktır.

Konuya ilişkin adli mercilerin görev ve yetkilerini düzenleyen 5235 sayılı Kanunun 10, 11 ve 12 nci maddeleri gereğince, 244 üncü maddedeki suçlarla ilgili dava ve işlere “Asliye Ceza Mahkemesi” tarafından bakılacaktır. Son olarak 243 üncü madde kapsamındaki suçlara ilişkin olarak yaptığımız “yer yönünden yetkili mahkeme” hakkındaki açıklamalarımız bu suç için de geçerlidir.

5271 sayılı CMK’nın, kanun yollarına ilişkin hükümleri bu suç için de geçerli olup şartları oluşması durumunda verilen hükümlerin Bölge Adliye Mahkemesi bünyesinde istinaf, Yargıtay nezdinde de temyizi kabildir.

3.3 Banka veya Kredi Kartlarının Kötüye Kullanılması

5237 sayılı TCK’da, bilişim sistemlerine karşı suçlar başlığı altında düzenlenen bir diğer suç olan Banka ve Kredi Kartlarının Kötüye Kullanılması, 245 inci maddede yerini almış olup suça ilişkin yasal metin aşağıdaki gibidir:

Banka veya kredi kartlarının kötüye kullanılması
Madde 245- (Değişik: 29/6/2005 –5377/27 md.)

(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.

(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,*

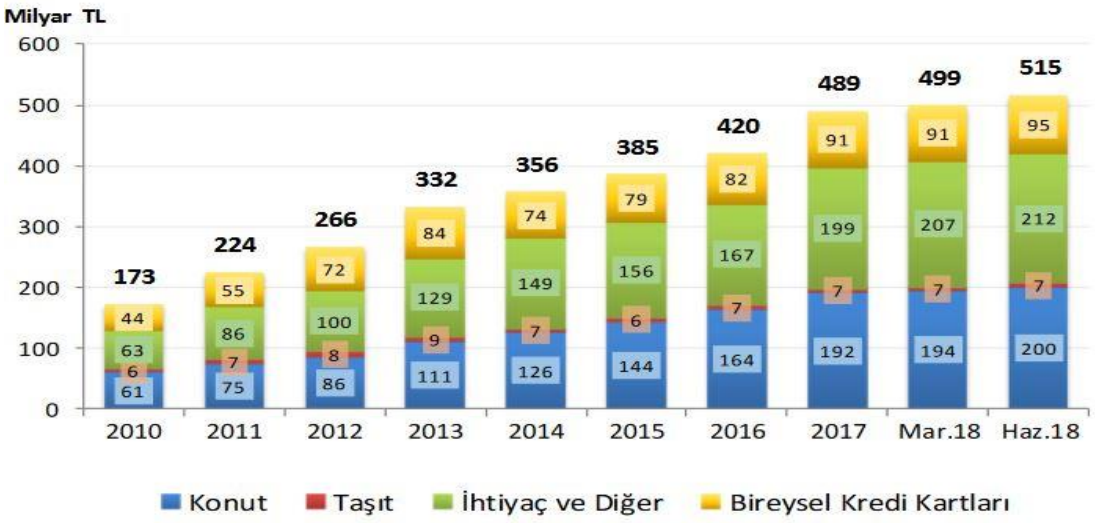
Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(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.

Yaşamak için tüketmek durumunda olan kişiler, her zaman nakit para değerlerini kullanmamakta, özellikle yüksek fiyatta taşınır mal veyahut gayrimenkul gibi taşınmazların satın alınması halinde banka ve kredi kuruluşlarının sıkça kullanımı gündeme gelmektedir. Günümüzde artık kişilerin nakit para taşımak yerine günlük alışverişlerini de kredi kartları ile gerçekleştirdiği bilinmektedir.

Finans sektörünün büyüklüğü, kişilerin tüketim alışkanlıkları ve alım gücü ile orantılıdır ve vatandaşlarımızın kredi kullanımı açısından artan oranda seyreden bir eğilim içerisinde olduğu görülmektedir. Bu bağlamda 2010-2018 yılları arasında gerçekleşen bireysel tüketicilerin kredi tercihlerine ilişkin grafik aşağıdaki gibidir (BDDK, 2018, s.12):

Şekil 3.2 Bireysel Tüketicilerin Kredi Tercihleri (2010-2018)



Görüldüğü üzere Haziran 2018 döneminde bireysel kredi kartları ile yapılan harcamalar 95 milyar TL olarak gerçekleşmişken; konut, ihtiyaç ve diğer krediler ise bunun iki katı oranında seyrederek 200 milyar TL civarında izlenmektedir. Tablodan da görülebileceği üzere bu nicelikler artan bir eğilim içerisindedir.

Bu kadar yüksek oranda mali trafiğin olduğu bir alanın suçluların çekim alanına girmemesi düşünülemez[12]. Bu çerçevede, kanun koyucu tarafından banka veya kredi kartlarının kötüye kullanımı başlığı altında üç farklı suç tipi sayılmış, bunların cezai sonuçları da bilişim suçları başlığı altında en yüksek hadlere sahip olmak üzere düzenlenmiştir.

Düzenleme alanındaki suçlardan ilki, ‘gerçek’ bir kredi kartını yetkisiz veya verilen yetkiyi aşarak kullanarak haksız çıkar sağlama; ikincisi bu kartların ‘sahte’ olarak üretimi, devri ve kabulü; üçüncüsü ise ‘sahte’ olarak üretilen kartların kullanılması suretiyle hukuka aykırı yarar sağlanmasıdır.

[12] 2018 yılının ilk 6 ayı itibarıyla, ülkemizde 64 milyonun üzerinde kredi kartı, 136 milyonun üzerinde banka kartı olduğu; internet üzerinden yapılan kartlı ödeme işlemlerinin ise 2017 yılında yaklaşık 100 milyon iken 2018'in ilk 6 ayı içerisinde 60 milyon civarında olduğu belirtilmektedir (BKM, 2018). Söz konusu veriler, bankacılık ve finans sektörünün kart sahipliği ve kartların internet kullanımı çerçevesinde oldukça büyük olduğunu göstermektedir.

Çağımızda en etkili ödeme aracı olan banka ve kredi kartlarının sahte üretimi, devri, satılması, kabulü vb. aşamalardaki her eylemin cezalandırılması suretiyle, gerçek veya tüzel kişilerin bilişim alanı kullanılarak malvarlıklarına zarar verilmesinin önlenmesi amaçlandığından, bu eylemlerin özel bir suç tipi olarak düzenlenmesinin yerinde olduğu belirtilmekte olup bu suç tipinin bilişim suçlarının en çok işlenen şekli olduğu ifade edilmektedir (Apaydın, 2017b, s.44).

Ülkemizde pek çok kişide birden fazla kredi kartının bulunması, kredi ve banka kartlarının seyyar tezgâhlarda dağıtılmaya devam edilmesi, her geçen gün tedavüldeki banka ve kredi kartlarının sayısının artması, bu alanı çok ciddi suç işlenme riskleriyle karşı karşıya bırakmaktadır (Karagülmez, 2014, s.287). Bu risklere; kullanıcıların gerek fizik dünyadaki işlemlerinde, gerekse bilişim dünyasında örneğin internet bankacılığı uygulamalarında yeterince bilinçli ve dikkatli davranmaması eklenebilir.

ASSS metni incelendiğinde, bu suça karşılık gelen, doğrudan veya dolaylı bir bilişim suçunun yer almadığı görülmektedir. Bu durumun, suçun genel karakteristiğinin bilişim alanından çok mali değerlere yönelik olmasından ileri geldiği düşünülmektedir.

3.3.1 Suçla korunan hukuki değer

Esasen hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçları ile korunmak istenen hukuki değerler, bu maddedeki suç tipleriyle muhafaza altına alınmak istenen yasal menfaatleri oluşturmakta olup bu kapsamda; hırsızlık ve dolandırıcılık suçları ile ‘malvarlığı’, güveni kötüye kullanma suçu ile ‘kişisel güven’, sahtecilik suçunda ise devlet tarafından fertlere yüklenilen hukuk alanınla inandırıcılığı olan belgelere olan güven korunmak istenmekte ancak bunlar içerisinde en baskın olanı kişinin malvarlığı olmaktadır (Dülger, 2015, s.457).

Bilişim alanında suçlar bölümü, TCK’nın üçüncü kısmı olan Topluma Karşı Suçlar başlığı altında düzenleme alanı bulmuştur. Ancak; bu suç neticesinde failin elde ettiği

haksız değerler ve mağdurun kaybı genel olarak 'malvarlığı' üzerinde yoğunlaşmaktadır. Nitekim kanunun lafzı incelendiğinde *'yarar sağlama'* odak noktası olarak belirlenmiş olduğundan suçun ekonomik niteliği öne çıkmaktadır.

Yargıtay Ceza Genel Kurulu da 30.03.2010 tarihli ve E.2010/11-17, K.2010/65 sayılı kararında bu suçun 'malvarlığına karşı işlenen suçların özel bir şekli olduğu ve etkin pişmanlık hükümlerinin uygulanabilir olmasının da bu sonuca ulaşmada gösterge sayılabileceğinin altı çizilmiştir (Corpus, 2018):

"... Öğretide benimsenen görüşler ışığında; somut olayımızda olduğu gibi ***başkasına ait kredi kartıyla sahibinin rızası hilafına para çekilmesinden ibaret eylemin*** *aynı zamanda* ***mal varlığına karşı işlenen suçların özel bir şekli olduğu*** *konusunda duraksama bulunmadığını kabul ETMEK GEREKMEKTEDİR.*

19.12.2006 günlü Resmi Gazete'de yayımlanarak yürürlüğe giren, 5560 sayılı Yasa'nın 11 inci maddesiyle 5237 sayılı Yasa'nın 245 inci maddesine eklenen 'birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun mal varlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır' hükmüne yer verilmesi suretiyle bir anlamda 5237 s. Kanunda da ***kredi kartının kötüye kullanılması suçunun mal varlığına karşı işlenen suçlarla irtibatı*** *açık bir şekilde VURGULANMAK İSTENMİŞTİR..."*

Yukarıdaki açıklamalar ve yargı kararları ile korunan hukuki değerin bireyin malvarlığı olması karşısında, bu suçun malvarlığına karşı suçlar yerine bilişim alanında suçlar bölümünde düzenlenmesi hususundaki eleştiriler literatürde adeta bir görüş birliği oluşturmuştur (Dülger, 2015, s.458; Karagülmez, 2014, s.289; Erdoğan, 2012, s.295; Yılmaz, 2010, s.267; Ketizmen, 2008, s.187).

Korunan hukuki değerlerin karma nitelikte olduğu kabul edilerek, bankacılık sektöründeki bilişim sistemlerine olan güven değeri de bu kapsamda düşünülse dahi; doktrin ve yargı kararlarında bu suça ilişkin olarak öne çıkan hukuki menfaatin 'malvarlığının korunması' olduğu kanaati mevcuttur. Bu kapsamda aynı koruma

amacına sahip veya birbirine yakın yasal menfaatlere dair normların sistematik olarak aynı başlık altında yer alması beklenmektedir. Bu nedenle sarf edilen eleştirilere katılmak mümkündür. Sonuç olarak, bu suçun TCK'nın *'Kişilere Karşı Suçlar'* isimli ikinci kısmının, onuncu bölümündeki *'Malvarlığına Karşı Suçlar'* başlığı altında düzenlenmesinin uygun olacağı değerlendirilmektedir.

3.3.2 Suçun maddi unsurları

3.3.2.1 Fail ve mağdur

Yasa metni incelendiğinde suçun faili bakımından sadece 'kişi' lafzı geçtiğinden bu konuda herhangi bir özellik göstermediği anlaşılmaktadır. Dolayısıyla fail 'herkes' olabilecektir. İstifade edilecek haksız yararın, failin kendisi veya başkası için edinmesinin suçun oluşumu açısından bir önem taşmadığı maddede belirtilmektedir.

5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun (BKKK) 3 üncü maddesinde kart hamili; banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişi şeklinde tanımlanmıştır. 5237 sayılı TCK'nın bununla ilgili suçu düzenleyen maddesinde ise 'kart sahibi' veya 'kartın kendisine verilmesi gereken kişi' ibareleri yer almaktadır.

Kartın hamili ile kartın sahibi her zaman aynı kişiler olmayabilir. Kartın hamili o an için kartın taşıyıcısı olup kartla ilgili yapılacak iş ve işlemlerden yarar sağlayacak olan kişiyi işaret etmektedir. Ayrıca BKKK'nın 16 ncı maddesi uyarınca hamil, kartın kötüye kullanımını engellemek için gerekli tüm önlemleri almak, kayıp veya çalınma durumunda ise kartı çıkaran kuruma derhal bilgi vermekle yükümlü tutulmuş; aksi takdirde öğretide 'bizzat katlanma yükümlülüğü' olarak adlandırılan tazmin sorumluluğuna tabi kılınmıştır (Açıkgül, 2007, s.173)

BKKK, TCK'dan daha sonraki tarihli bir düzenleme olduğu için 'kart sahibi' ibaresinin değişiklik çalışmalarında 'kart hamili' şeklinde revize edilmesinin,

mevzuatta da yeknesaklık sağlanması adına daha uygun olacağı değerlendirilmektedir. Kartın kendisine verilmesi gereken kişi de kart hamili olarak anlaşılmalıdır.

Bu çerçevede mağdur, banka veya kredi kartının bağlı olduğu hesabın mudii olan gerçek kişiler olup birer tüzel kişilik olan banka ve kredi kuruluşları ise bu suçların mağduru olmakla birlikte suçtan zarar gören durumundadır. Suçun mağduru ile suçtan zarar gören kavramları birbirlerinden farklıdır; Şöyle ki, suçun mağduru suçtan doğan ceza ilişkisinin tarafı olduğu halde, suçtan zarar gören kimse hukuk ilişkisinin tarafıdır ve iddiası esas itibariyle hukuksal nitelik taşımaktadır (Yılmaz, 2010, s.268).

Konuya ilişkin olarak Yargıtay 6. Ceza Dairesi'nin 09.07.2012 tarihli ve E.2011/2110, K.2012/13824 sayılı kararı aşağıda sunulmaktadır (Dülger, 2015, s.463-464):

"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 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****..."*

Hayali hesaplara bağlı olarak üretilen kartlarla işlem yapılarak, doğrudan banka veya finans kurumunun malvarlığında zarara yol açılmışsa, ilgili banka ya da finans kurumu suçun mağduru sayılır (Parlar, 2011, s.53). Yargıtay da sahte kart oluşturulması ve bu tür kartlardan haksız yarar sağlanmasını düzenleyen m.245/2 ve m.245/3'te yer alan suçlarda adına kart üretilen kişilerin davaya katılma hakkının bulunmadığına karar vermekte (Yargıtay 8. CD.'nin 25.02.2015 tarihli ve E.2014/22056, K.2015/12531 sayılı kararı) ve suçun mağdurunu 'banka' kabul etmedir (Gül, 2016, s.123).

Yargıtay'ın (8. CD.) 12.04.2018 tarihli ve E.2017/22384, K.2018/4133 sayılı güncel kararında da bu husus dile getirilmiş, kararda ayrıca sahte üretilen kart bakımından 'kartları gerçeğe aykırı olarak üretilen banka sayısınca' suçun oluşacağı hükme bağlanmıştır (Yargıtay, 2018):

"...Başkasına ait banka hesabıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi TCK.nun 245/2. maddesinde; sahte banka veya kredi kartını kullanarak kendisine veya bir başkasına yarar sağlanması ise anılan maddenin 3. fıkrasında birbirinden bağımsız ve ayrı ayrı suçları oluşturduğu, sanıkların ***bir bankaya ait gerçek bir kredi kartının manyetik şerit bilgilerinin kopyalanarak sahte bir kredi kartı üretmesi ve bu kartı kullanmak suretiyle yarar sağlamaları halinde suçtan zarar görenin ilgili banka olduğu, kartları gerçeğe aykırı olarak üretilen banka sayısınca*** *TCK.nun 245/2. maddesi ... sahte olarak üretilen kartların alışverişte kullanılması halinde ise, banka sayısınca TCK.nun 245/3. maddesi ile aynı bankaya ait birden fazla kart ile veya bir kart ile değişik zamanlarda para çekilmesi veya harcama yapılması halinde ise TCK.nun 43. maddesi uyarınca* ***uygulama yapılması gerektiği****..."*

3.3.2.2 Şahsi cezasızlık halleri

Suçun dördüncü fıkrasında bu suçta fail olabilecek, ancak 'şahsi cezasızlık sebebiyle' bu kişiler üzerinde cezai sorumluluğun doğmasına engel birtakım haller sayılmıştır.

Sayılan haller, hukuka uygunluk sebebi değildir ve esasen ortada mevcut bir suç vardır. Ancak bu suçu işleyen belli kişiler böyle bir düzenlemeyle cezadan bağışık tutulmaktadır. Dolayısıyla iştirak halinde suç işleyenlerden biri (şerik) hakkında cezalandırmayı önleyen şahsi bir sebep veya şahsi cezasızlık sebebinin bulunmaması diğer şeriklerin sorumluluğunu etkilemeyecek; diğer şerikler eylemlerinden dolayı sorumlu olacaklardır (Kaymaz, 2012, s.148). Yani şahsi cezasızlık sebebinden sadece kanunda ifade edilen kişi veya kişiler faydalanabilecek olup iştirak halinde suç işlenmesi halinde bu kişi dışındaki herkes cezai sonuca katlanacaktır.

Bu kapsamda TCK m.245/4 uyarınca, aşağıdaki durumlarda atıfta bulunulan kişi suçun faili olsa da cezalandırılması mümkün olmayacaktır:

- **Evlilik birliği içerisindeki eşler** arasında bu suçun işlemesi durumu, (haklarında ayrılık kararı[13] verilmesi hariç)

- **Üstsoy** (anne-baba-anneanne-dede ve varsa bunların üstleri) veya **altsoy** (çocuk-torun-torunun çocuğu ve varsa bunların altları) veya **bu derece kayın hısımları** (kayınvalide-kayınpeder ve varsa üstleri ile bunların çocuk-torun ve varsa altları) ya da **evlat edinen ile evlatlık** zararına bu suçun işlenmesi,

- **Aynı konutta yaşamak şartı ile kardeşler** arasında bu suçun işlemesi hali.

Şahsi cezasızlık sebebinin kabul edilişin temelinde, bu türden bir suçun işlenmesi halinde problemin aile içinde çözülebileceği ya da mazur görülebileceği ve aile içi barışın korunabileceği düşüncesi yatmaktadır (Apaydın, 2017a, s.556). Yani Kanun bu kişilerin akrabalık bağını yakın bularak, ailevi ilişkilerin zarar görmemesini teminen bu kişileri cezai sorumluluktan kurtarmak istemiştir.

[13] Boşanma gibi evliliği sona erdirmeyen, ortak hayatın yeniden kurulması olasılığının bulunduğu ve evlilik birliğinin eşlere yüklediği birlikte yaşama dışında kalan bütün yükümlülüklerin devam ettiği bir karar türü olup, bu karara hâkimin takdir edeceği 1 ila 3 yıl arasında bir zaman aralığı ile sınırlı olmak üzere hükmedilmesi mümkündür (Akıntürk, 2006, s.285). Eşlerin böyle bir karar alınmasıyla genelde fiziken ayrı yaşaması ve ortak hayatı tekrar kurmalarının kesin olmaması sebepleriyle, TCK bu kişilerin şahsi cezasızlık sebeplerinden yararlanmasını yerinde olarak uygun görmemiştir.

Cezai yükümlülüğün bulunmaması, hukuki sorumluluğun da olmadığı anlamına gelmemektedir. Bu bağlamda böyle bir eyleme maruz kalan kişinin, bunun tazminini zamanaşımı süresi içerisinde hukuk mahkemeleri nezdinde talep edebilmesi mümkündür.

Suç, ancak yukarıda sayılan kişiler zararına işlendiğinde cezasızlık nedeni uygulanır yani suçtan zarar gören banka ise bu madde uygulanamaz (Bilgen, 2010, s.71). Yine söz konusu cezasızlık sebepleri sadece 245 inci maddenin ilk fıkrasındaki suç tipi için benimsenmiş olup, maddenin ikinci ve üçüncü fıkrasında düzenlenen durumlar için uygulanma olanağı bulunmamaktadır.

Boşanma davaları hala devam etmekte olan (boşanma hükmü verilse de bu kesinleşene dek) eşlerin 'evlilik birliği' içerisinde olduğunun kabulü ve kardeşlere dahi aynı evde ikamet şartı getirilmişken bu yakınlıktan daha uzak olan kayın hısımları için bu şartın aranmaması gibi sebeplerle şahsi cezasızlık hükümleri eleştirilmektedir (Dülger, 2015, s.460). Zira boşanma safhasında olan eşlerden birinin veya husumeti olan kayın hısımlarından birinin zarar vermek amacıyla ilgili kişinin kredi kartını ele geçirip, usulsüz/aşırı harcama yapması halinde bu suç oluşmayacaktır. Bu eleştiriler karşısında, suçun bu kişilere karşı şikâyete bağlı kılınmasının kısmi bir çözüm yaratabileceği değerlendirilmektedir.

3.3.2.3 Hareket ve netice

Suç tanımında yer alması sebebiyle öncelikle banka ve kredi kartının tanımlamaları yapılarak farkının ortaya konması gerekmektedir.

5464 sayılı BKKK'nın *"Tanımlar"* kenar başlıklı üçüncü maddesinde banka kartı: "*Mevduat hesabı veya özel cari hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanmayı sağlayan kart"* şeklinde ifade edilmiştir.

Banka kartları, kart hamilinin bir şifre vasıtasıyla kendi hesabında işlem yapması ile bankanın kurduğu sisteme hukuka uygun olarak girmeyi sağlamaktadır. Bu kartların temel özelliği kart kullanıcısına bir '*kredi olanağı sağlamaması*' ve kartın kullanıcısı kişinin kartı, bankanın bilişim sisteminin bir parçası olan makineleri (bankamatik, ATM [*Automated Teller Machine*] veya POS [*Point of Sale*]) kullanarak banka nezdindeki hesabına ulaşması ile '*hesap bakiyesindeki tutar kadar*' para çekilmesini/işlem yapılmasını sağlamasıdır (Özbek, 2007b, s.1027).

Kredi kartları ise BKKK'nın üçüncü maddesinde: "*nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kart veya fizikî varlığı bulunmayan kart numarası"* olarak tanımlanmıştır.

Kredi kartları, mülkiyeti bir banka veya finans kurumuna ait olan ve banka ile kart hamili arasında yapılan 'sözleşme' gereği, belirli koşullar altında kullanıcısına limitiyle sınırlı 'kredi olanağı sağlayan' bir kredi aracıdır (Doğan, 2014, s.159).

Yasadaki tanımlar tetkik edildiğinde, bu suçun mutlaka basılı/fiziki kartlar üzerinde işlenmesi zorunluluğu bulunmamakta olup failin belli bazı bilgileri bilmesiyle, fiziki varlığı olmasa da kart fonksiyonlarının çalıştığı sistem veya cihazlar kanalıyla suçu işleyebilmesi mümkün görülmektedir.

Suçun birinci fıkrasında başkasına ait banka veya kredi kartıyla haksız çıkar sağlanması düzenlenmiştir. Suç konusu kartın, failden 'başkasına' ait ve hâlihazırda kullanılan 'gerçek' (sahte olmayan) ve bir kart olması zorunludur.

Yine suçta kullanılan kartın kullanıma açık (kapatılmamış/iptal edilmemiş) ve işlem yapabilme fonksiyonunu haiz olması da şart olup kartın iptal edilmesi durumunda suçun "işlenemez" mahiyette olduğuna ilişkin Yargıtay 8. Ceza Dairesi'nin E.2013/19446, K.2014/11361 sayılı kararı aşağıdaki şekildedir (Gül, 2016, s.120):

"... Sanık M.K'nın hırsızlık suretiyle ele geçirdiği ***suça konu kredi kartlarının, mağdur H.B. tarafından iptal edilmesi nedeniyle kullanılmasının mümkün***

bulunmayıp vasıtanın elverişli olmaması karşısında, eylemin işlenemez suç niteliğinde olduğu *gözetilerek sanıkların atılı suçtan beraatleri yerine yazılı şekilde mahkûmiyetlerine karar verilmesi…"*

Anılan fıkrada 'her suretle olursa olsun' 'ele geçirmek' veya 'elinde bulundurmak' lafzı geçtiğinden suçta kullanılan kartın hukuka uygun veya aykırı şekilde edinilmesi önem taşımamaktadır. Kartı hukuka uygun şekilde elinde bulunduran kişinin, kart hamilinin rızası dışında veya verdiği yetkiyi aşarak hareket etmesi, fıkrada yazılı 'rıza olmaksızın' unsurunu karşılayacaktır.

Yine başkasına ait banka veya kredi kartı ile yarar sağlama suçunun oluşabilmesi için, yararın elde edilmesi, kartın kullanılmasının sonucu olmalıdır. Yararın elde edilmesi ile kartın kullanılması arasında doğrudan bir illiyet bağı yoksa örneğin; failin mağduru silahla tehdit ederek bankamatikten para çekmeye zorlaması veya mağdurun çektiği parayı alıp kaçması durumunda, TCK 245/1 değil, sırasıyla yağma ve hırsızlık suçları oluşacaktır (Ergün Okuyucu, 2013, s.1072).

Banka veya kredi kartlarının kötüye kullanılması suçunun ilk fıkrası zarar suçu mahiyetinde olup, suçun tamamlanmış olması için hareket yeterli değildir; ayrıca karşı taraf aleyhine bir zarar meydana gelmeli, dolayısıyla suçun tamamlanmış olduğunun kabul edilmesi için, failin kendisine veya başkasına haksız yarar sağlamış olması gerekmektedir (Tufanoğlu, 2014, s.36). Suç, failin kendisi veya bir başkasına yarar sağladığı anda sübut bulacaktır.

Maddede geçen 'kullanma veya kullandırtma' ibareleri ise icra hareketinden ibaret olup ihmal ile bu suçun işlenemeyeceği anlamına gelmektedir (Hafızoğulları ve Özen, 2016, s.464).

Suçun ikinci fıkrasında düzenlenen sahte kart ile ilgili eylemler bakımından; 5464 sayılı yasada düzenlenen ve banka ya da kredi kartı çıkarmaya yönelik usulsüz hareketlerin cezai sonucunu düzenleyen hükmün de incelenmesi önem arz etmektedir. Söz konusu madde aşağıdaki gibidir:

Gerçeğe aykırı beyan, sözleşme ve eki belgelerde sahtecilik
MADDE 37 *– Banka kartı veya kredi kartını kaybettiği ya da çaldırdığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar bir yıldan üç yıla kadar hapis ve ikibin güne kadar adlî para cezası ile cezalandırılırlar.*

Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler

Söz konusu özel yasa hükmü ile 245 inci maddede düzenlenen suç tipleri karıştırılabilir olsa da Yargıtay 8. Ceza Dairesi 27.03.2018 tarihli güncel kararı ile (E.2017/17576, 2018/3373) failin eylemleri ve hükümlerin uygulanabileceği zaman aralığı hakkında kuşkuya yer vermeyecek açıklıkta bir karara hükmetmiştir (Yargıtay, 2018):

*"5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun **37/2**. maddesinde yer alan "kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler" şeklindeki düzenlemenin **sözleşmenin imzalanmasını da kapsayacak aşamaya kadar uygulanabileceği**, kredi kartı **sözleşmesinin düzenlenmesinden sonra kartın üretilmesi halinde ise TCK.nun 245/2. maddesine temas eden suçu oluşturacağı** cihetle; sanığın mağdur…'a ait sahte nüfus cüzdanını kullanmak suretiyle Finansbank … şubesine müracat ederek kredi kartı talebinde bulunduğu ve **bankayla sözleşme yapıldığı, kredi kartı başvurusunun ise banka tarafından reddedildiği ve kartın üretilmediğinin anlaşılması karşısında, 5464 sayılı Kanunun 37/2. maddesinde düzenlenen suçun oluştuğu** gözetilmeden, suç vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması..."*

Yargıtay burada gerçeğe aykırı bilgi ve belgelerle bankaya başvurulması ve sözleşme imzalanması safhalarını 5464 sayılı Kanun kapsamında görmekte ancak bu başvuru sonucunda kartın üretilmesi halinde artık TCK m.245/2'den söz edilebileceğini

vurgulamaktadır. Sahte üretilen bu kartın kullanılarak yarar temin edilmesi halinde de m.245/3'te düzenlenen suç meydana gelecektir.

Sonuç olarak bankaya gerçeğe aykırı beyan sunmak suretiyle kart başvurusunda bulunan kişinin, başvurusunun yerinde görülmeyerek kartın düzenlenmemesi halinde ortada sahte bir kart bulunmadığından 5464 sayılı BKKK'nın 37/2 hükmü uygulanabilecek; ancak böyle bir başvuru sonucunda kartın oluşturulması durumunda bu kez TCK. m.245/2'de sayılan 'sahte kart üretilmesi' ve/veya 'kabul edilmesi'nin sonuçları ortaya çıkacaktır (Apaydın, 2017a, s.477).

Sahte kartın üretilmesi, satılması, satın alınması, devri veya kabul edilmesi hususları ayrı ayrı 245 inci maddenin ikinci fıkrasında sayılmıştır. Bu çerçevede; sahte bir kartın üretilmesi, satımı, kabul edilmesi durumlarında, böyle bir kart 'kullanılmasa dahi' suç oluşacaktır. Fıkrada sayılan seçimlik hareketlerin icra edilmesi yeterli olup suçun oluşumu için zarar aranmadığı için suç 'tehlike' suçudur (Demir vd., 2015, s.95). İlk ve üçüncü fıkralarda ise 'haksız yarar temini' netice olarak arandığından, mağdur nezdinde bir zararın oluşması şart olmakta ve bu durum da sayılan suçların 'zarar' suçu olduğunu ortaya koymaktadır.

Genel olarak banka veya kredi kartlarının kötüye kullanılmasına ilişkin hareketleri içeren yöntemler, aşağıdakilerle sınırlı olmasa da büyük oranda aşağıda belirtilen fiillerle işlenmektedir (Bilgen, 2010, s.30-31):

- Kartın kaybı veya çalınması halinde, kötü niyetli kişiler tarafından kullanılması veya ATM ile işlem yapılırken kart hamili dışında birinin kartın şifresini edinmesi akabinde kartı ele geçirerek işlem yapması,

- Kötü niyetli kişilerin, banka ve kart çıkartan kuruluşlardan sahte belgelerle kredi kartı edinmeleri,

- Kart hamilinin müracaatı sonucu banka tarafından çıkartılan kartların posta, özel kargo şirketleri ve banka şubesi aracılığıyla kart hamiline ulaştırılmaması, kartı ele geçiren kişinin de arkasını imzalayarak kullanması,

- Boş plastik plakalar üzerine gerçek kredi kartı numaralarının kabartma olarak basılması işyerlerinde *imprinter* cihazı ile satış belgesi üzerine aktarılarak bankadan tahsil edilmesi,

- Kredi kartlarının üzerindeki kabartma numaraların kesilerek değiştirilmesi veya ütülenerek yerine yenisinin basılması,

- Kartın arka yüzünde bulunan manyetik şerit bilgilerinin *encoder* denilen bir cihaz aracılığıyla kopyalanması veya kodlanarak içine elektronik yollardan başka kart bilgileri yazılarak kullanılması (Gerçek kartın manyetik şeridi silinerek manyetik şerit kodlayıcısı ile başkalarına ait bilgilerin kodlanması)

- Kredi kart numarası kullanılarak posta ve telefon ile yapılan siparişlerde, önceden ayarlanmış bir adrese mail gönderilmesi.

3.3.3 Suça etki eden sebepler

Mezkûr suçun ağırlaştırıcı veya hafifletici nitelikli hali, TCK veya cezai hükümler içeren diğer herhangi bir yasada bulunmamaktadır. 245/4 düzenlemesinde ise sadece sayılan kişilerle sınırlı olarak, şahsi cezasızlık hallerine yer verilmiştir.

3.3.4 Yasak cihaz veya programlar ile ilgili suç sayılan eylemler

245'inci maddenin devamında, 6698 sayılı KVKK'nın 30 uncu maddesi ile TCK'ya 245/A şeklinde bir madde ilave edilerek yeni bir suç tipi daha ihdas edilmiştir. Yasa metni aşağıdaki gibidir:

Yasak cihaz veya programlar

Madde 245/A- (Ek: 24/3/2016-6698/30 md.)

(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

Maddeye ilişkin alt komisyon raporunda; *5237 sayılı Kanuna "Yasak cihaz veya programlar" başlıklı 245/A maddesinin eklenmesi öngörülmüştür. Böylece bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bir bilişim suçunun 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 faillerin cezalandırılması amaçlanmaktadır.* ***Mezkûr Sözleşmenin 6'ncı maddesiyle sözleşmeci taraflar, bilişim alanında suç işlenmesini kolaylaştıran cihazların kötüye kullanılmasını cezalandırmaya davet edilmektedir. Bilişim suçları ile bilişim sistemleri araç kılınarak işlenen suçlarla etkin ve caydırıcı bir şekilde mücadele edebilmek için bu tür eylemlerin suç ve ceza politikaları bakımından sınırlandırılması ve yaptırıma bağlanmasında yarar görülmektedir****. Maddede tanımlanan* ***suçun oluşumunda kişinin suç işleme kastı dikkate alınmak zorundadır****. Buna göre,* ***bu tür cihaz ve programların, bilişim sistemlerinin güvenliğini test etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacaktır****. Ayrıca, failin cezalandırılabilmesi bakımından* ***söz konusu cihaz, program, şifre veya güvenlik kodunun suçun işlenmesine elverişli olması gerekir****"* denilmektedir (TBMM, 2016b).

Söz konusu raporda 'mezkûr sözleşme' ibaresi ile ASSS'ne atıfta bulunulmaktadır. Gerçekten de ASSS'nin 6 ncı maddesinde "Cihazların kötüye kullanımı" kenar başlığı altında özetle; sözleşmede yer alan suçların işlenmesi amacıyla kullanılabilecek cihaz

veya programların satılması, tedariki, dağıtımı ve/veya bulundurulmasının suç olarak öngörülmesinin gerektiği belirtilmektedir (CoE, 2001a).

Anılan sözleşmenin açıklayıcı raporunda da; bu hükümle belli cihazların kötüye kullanılması suretiyle, spesifik yasadışı fiillerin kasıtlı olarak bilişim sistemlerinin veya verilerinin gizliliği, bütünlüğü ve kullanıma açıklığına karşı olarak sözleşmede tanımlanan suçları işlemek amacıyla icra edilmesinin ayrı ve bağımsız bir suç olarak tanımlandığı ifade edilmiştir. Devamında, bu suçları işlemek için genellikle erişim araçlarının (hacker araçları) ya da belli başka araçların bulundurulması gerektiği aktarılarak, bu araçları suç işleme amacıyla elde etmeye yönelik olarak üretim ve dağıtım alanında bir tür karaborsanın doğmasına yol açabilecek, güçlü bir eğilim olduğunun altı çizilmiştir. Bu tehlikelerle daha etkin bir biçimde mücadele edebilmek için, ceza hukukunun potansiyel 'tehlike' taşıyan bu özel durumları bu alanda belli birtakım suçların işlenmesinden önce, kaynağında yasaklaması gerektiği de raporda ayrıca vurgulanmaktadır (CoE, 2001b, s.12).

Madde metni, komisyon raporu, ASSS'de düzenlenen hükümler ve açıklayıcı memorandum birlikte ele alındığında; suçun, herhangi bir zarar neticesi öngörülmediğinden 'tehlike' suçu mahiyetinde olduğu görülmektedir. Ayrıca bilişim suçları alanında suç işlemeye elverişli olabilecek her türlü cihaz suç kapsamında kabul edilebilecektir. Bunlara örnek olarak, kredi kart bilgilerini kopyalamaya yarayan encoder, bilişim sistemlerine haksız erişim sağlanmasına olanak veren şifre kırıcı veya casus yazılımlar verilebilir.

Maddede geçen "*...**bu Bölümde yer alan suçlar** ile **bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar**..."* oldukça önemli bir ibaredir. Böylece, gerek doğrudan bilişim suçları gerekse TCK veya diğer yasalarda bilişim sistemlerinin kullanılması suretiyle işlenebilecek dolaylı bilişim suçlarının icrası bağlamında kullanılabilecek herhangi bir cihaz veya program kapsama alınmıştır.

Maddede tanımlanan suçun oluşumunda kişinin suç işleme kastı dikkate alınmak zorunda olup; bu tür cihaz ve programların, bilişim sistemlerinin güvenliğini test

etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacak, örneğin sızma/zafiyet testi (*pentest*) yapan şirketler elinde bulunan bu araçlar, bilişim sistemi sahibi ile imzalanan sözleşme çerçevesinde kullanıldığı için hukuka aykırılık ortadan kalkacaktır (Şıracı, 2016b).

Bu düzenlemeden önce herhangi bir kişisel bilgi kopyalandığı, sahte oluşturulmuş ya da kullanılmış kart bulunmadığı takdirde faile ceza vermek mümkün değildi ve sadece suç işlemeye hazırlanmış cihazları bulundurmak hazırlık mahiyetinde idi. Böylece bu düzenleme ile bu hazırlık hareketleri de suç kapsamına alınmıştır (Gül, 2016, s.208).

Benzer düzenlemeler, ilgili kişilerin haklarını korumak ve suç teşkil edebilecek eylemlerin, işlenmeden önlenebilmesini teminen özel bazı yasalarda da yer almıştır.

Örneğin 5809 sayılı EHK'nın 55 inci maddesi gereğince Kurum (BTK) tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgilerinin (IMEI numaraları) yeniden oluşturulması, değiştirilmesi, kopyalanması, çoğaltılması veya herhangi bir amaçla dağıtılması mümkün değildir. Bu fiillerin işlenmesine yönelik yazılım, her türlü araç veya gereçlerin ithalâtı, üretimi, dağıtımı veya tanıtımının yapılması, bulundurulması ve aracılık edilmesi de mezkûr maddenin ikinci fıkrasında yasaklanmış ve aynı Kanunun 63 üncü maddesinin dokuzuncu fıkrası ile bu yasağın yaptırımı, 'bin günden on beş bin güne kadar adli para cezası' olarak karşılık bulmuştur.

Yine 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun (FSEK) 72 nci maddesinde; 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 kişinin altı aydan iki yıla kadar hapisle cezalandırılması öngörülmüştür.

Söz konusu suç, banka ve kredi kartlarının kötüye kullanılması suçunu müteakiben 245/A maddesi ile düzenleme alanı bulmuştur. Bu düzenleme şekliyle maddenin sadece 245 inci maddeye hasredildiği kanısına varılabilmektedir. Söz konusu suçun,

özellikle bilişim alanında daha büyük bir suçun işlenmesinin önlenmesi açısından önemli bir yere sahip olduğu düşünülmekte olup aynı başlık altında ancak ayrı bir madde olarak düzenlenip diğer maddelerin de buna göre teselsül ettirilmesi suretiyle TCK'da yerini almasının daha uygun olabileceği değerlendirilmektedir.

3.3.5 Suçun manevi unsurları ve hukuka aykırılık

Bilişim alanındaki diğer suçlarda olduğu üzere bu suç da kasten işlenebilen suçlardandır. Nitekim bu husus ASSS'de düzenlenen suçların tamamında kastla hareket edilmesinin zorunlu olduğu düzenlemesine paraleldir. Bahsedilen kast maddede sayılı tüm suçlar bakımından genel kast olmaktadır.

Suçun üçüncü fıkrasında yer alan 'yarar sağlama' ifadesinin özel kast olarak algılanabileceği düşünülse de bu ibare, failin amacını değil suçun neticesini yansıtmaktadır. Zira failin bunu yarar sağlamak 'amacıyla' işleyip işlemediğini karşılayacak bir kelime de anılan fıkrada yer almamaktadır. Aynı düşüncede Dülger; suç tipinde normatif olarak failin eylemini belli bir saik ile işlediğine dair bir tanım bulunmadığını, bu güdünün yorum yoluyla çıkarılabilecek olsa da suç tipinde yer almadığı için özel kast olarak kabul edilmesinin mümkün olmadığını, ayrıca yorum yoluyla da olsa bu suçta özel kast bulunmadığını ifade etmektedir (2015, s.505).

Fail bu suçun ilk fıkrası için başkasına ait bir kartı, hamilinin rızası olmaksızın kullanmak suretiyle yarar sağlamış olduğunu; ikinci fıkrası için sahte bir kart ürettiği, sattığı, devrettiği veya kabul ettiği gibi eylemleri icra ettiğini; üçüncü fıkrası için ise sahte bir karttan yarar sağladığını bilmesi ve istemesi yeterlidir.

Suçun taksirli halinin yasada açıkça gösterilmesi şartından ötürü böyle bir düzenleme olmaması sebebiyle bu suçun taksirle işlenmesi olanaklı değildir.

Bu suç ile (özelikle ikinci fıkra) hukuka uygunluk nedenleri bağdaşmayacaktır. Zira bir kimseye ait banka hesabı ile ilişkilendirilerek sahte banka veya kredi kartı üretmek,

sahte kartı satmak, satın almak, devretmek ve/veya kabul etmek her zaman hukuka aykırıdır (Hafızoğulları ve Özen, 2016, s.468).

Kişi bu suç özelinde ancak TCK m. 30/4 gereğince 'kaçınılmaz' bir hataya düştüğünden bahisle bu hatadan yararlanabilir ve cezalandırılmaz. Örneğin; başkasına ait kartı kendisine ait zannederek kullanan kişi kasıtlı hareket etmiş sayılmayacağından, hataya düşen kişinin cezalandırılması söz konusu olmayacaktır (Ergün Okuyucu, 2013, s.1073).

Bununla birlikte m. 245/1 kapsamında kart kullanımı için tanınan rıza veya kartın şifresinin verilmesi halinde TCK m.26'daki 'ilgilinin rızası' hükmünden istifade edilebilmesi mümkün olacaktır. Ancak rızayı alan kişinin, rızayı veren kişi tarafından tanınan yetkinin sınırlarını aşmadan işlemde bulunması şarttır. Aksi takdirde yetki aşılarak yapılan işlemler, aşılan kısımdan itibaren suça vücut verecektir.

Rızanın hukuka uygunluk nedeni olarak kabul edilebilmesi için, mağdurun rıza açıklama yeteneğinin bulunması gerekmektedir. Rıza açıklamasında bulunan kimsenin ruh ve akıl sağlığının yerinde olması, rıza açıklama yeteneğini ortadan kaldıran bir durumun bulunmaması şarttır. Rıza gösteren kimse, suç tipi ile korunan hukuki değer ve yararlardan hangi oranda vazgeçtiğini ve karşılaşabileceği risk ile zararları biliyorsa, anlama yeteneğinin var olduğu kabul edilir (Yılmaz, 2010, s.273).

3.3.6 Suçun özel görünüş biçimleri

3.3.6.1 Teşebbüs, iştirak ve içtima

Banka ve kredi kartlarının kötüye kullanılmasıyla ilgili 245 inci maddenin birinci ve üçüncü fıkralarında, suçun tamamlanması için yararın sağlanması gerekmekte olup yarar sağlanamadan hareketlerin yarıda kalması/kesilmesi durumunda teşebbüs söz konusu olacaktır (Uçar, 2014, s.84).

Yargıtay 8. Ceza Dairesi'nin konuya ilişkin 01.02.2018 tarihli ve E.2017/19101, K.2018/875 sayılı kararı aşağıdaki gibidir (Yargıtay, 2018):

"...TCK'nın 245/1. maddesinde düzenlenen kredi kartını kötüye kullanma suçunun oluşabilmesi için ***başkasına ait kredi kartı kullanılarak menfaat sağlanması gerekmekte*** *olup; suça konu kredi kartıyla yapılan işlemin, suç tarihinin ertesi günü işyeri tarafından iptal edilerek sanığa kargoyla satışa konu ürün yerine boş koli gönderildiği ve* ***sanığın koliyi teslim aldığı sırada yakalanması nedeniyle istenilen menfaatin sağlanamadığı anlaşılmakla, suçun teşebbüs aşamasında kaldığı****..."*

Görüldüğü üzere başkasına ait kredi kartının sadece elde bulundurulması suça yol açmamakta, suçun oluşumu için menfaat sağlanması şart olmaktadır. Fail ele geçirdiği kartı kullanmasına rağmen bundan yarar sağlamazsa TCK m. 245/1'e teşebbüsten; ele geçirdiği kartı kullanmasa dahi, ele geçirme şekli ayrı bir suça vücut veriyorsa o suçtan ayrıca cezalandırılmalıdır (Erdoğan, 2012, s.320). Yararın aynen arandığı TCK m.245/3 için de bu durumun geçerli olduğu değerlendirilmektedir.

Suçun ikinci fıkrasında herhangi bir netice aranmadığından ancak failin hareketleri parçalara bölünebiliyor ise teşebbüsten söz edilebilecektir. Örneğin; failin sahte kart üretmek üzere çalışırken yakalanması veya bu tür bir kartın devri için anlaşma sağlasa da bunun gerçekleşmesinden önce olayın ortaya çıkması hallerinde bu suça teşebbüs mümkündür (Dülger, 2015, s.510). Failin sahte kredi kartı oluşturmak amacıyla çalışırken yakalanması, anılan fıkraya teşebbüsten sayılsa da eğer failin çalıştığı cihaz veya programlar bu tür suçları işlemeye elverişli özel cihazlar ise fail ayrıca TCK m. 245/A'da düzenlenen suça teşebbüsten değil bu suçu işlemekten 'tam' olarak cezalandırılabileceği düşünülmektedir.

İncelenen suç tipleri iştirak açısından herhangi bir özellik göstermediğinden, TCK'nın iştirake dair maddelerinin somut olaya tatbiki mümkün olup birden fazla kişi tarafından suçun işlenmesi halinde iştirak hükümleri uygulanabilecektir.

Bu suçta iştirakten söz edebilmek için kartların kullanılması veya kullandırılması aşamasında ortak ve anlaşmalı suç işleme iradesi olması gerekmekte; dolayısıyla kartın ele geçirilmesi aşamasında işlenmiş bir suç varsa, bu suçun işlenmesine iştirak etmemiş ama kartın kötüye kullanılması suçuna iştirak etmiş olan diğer fail, kartın ele geçirilmesi için işlenen müstakil suçtan sorumlu olmayacak, bunun yerine suçluyu kayırma veya suç eşyasını saklama suçlarından sorumlu tutulabilecektir (Tufanoğlu, 2014, s.45).

Suçu incelerken, fail ve mağdurun açıklandığı bölümde Yargıtay'ın güncel bir kararı ile (8.CD. 12.04.2018-E.2017/22384, K.2018/4133) 'banka sayısınca' suçun oluşacağı, dolayısıyla suçların birleşmeyeceği ifade edilmişti. Dolayısıyla ilk fıkra bakımından kart hamili kadar, ikinci fıkra bakımından ise sahte oluşturulan kart ile ilgili finans kuruluşu sayısınca 'gerçek suç' oluşacağı ve içtima uygulanmayacağı açıktır. Bu durum, mağdurun farklı kişi veya kuruluşlar olması halinde geçerlidir. Yoksa bir suç kararının icrası kapsamında, aynı kişiye karşı farklı zamanlarda bu suçun işlenmesi halinde zincirleme suç hükümleri uygulanacaktır.

Nitekim Yargıtay 8. Ceza Dairesi'nin 16.06.2018 tarihli ve E.2016/3862, K.2016/8047 sayılı kararında bu durum açıkça işlenmiştir (Yargıtay, 2018):

*"...**Şikayetçiye ait kredi kartını değişik zamanlarda birden çok kez kullanan** sanık hakkında hüküm kurulurken TCK.nun 43. maddesinde düzenlenen **zincirleme suç** hükümlerinin uygulanmaması suretiyle eksik ceza tayini ... gereğince bozulmasına..."*

Ayrıca ilgili diğer suçlar, 245 inci maddede düzenlenen suçların bir unsuru olmayıp şartları oluşan her suçtan ayrıca cezaya hükmedilmelidir. Konuya ilişkin durumlarda nasıl uygulama yapılacağı, oldukça açık ve net şekilde Yargıtay 11. Ceza Dairesi'nin 05.07.2012 tarihli ve E.2011/10197, K.2012/13350 sayılı kararında gösterilmiştir (Demir vd., 2015, s.98):

"... 5237 sayılı Yasanın 245/1. maddesinde düzenlenen 'banka veya kredi kartlarının kötüye kullanılması' suçunun yasadaki düzenleniş şekli göz önüne alındığında bileşik

suç olarak düzenlenmediğinin görüldüğü, 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 koyduğu, bu nedenle, ***banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi durumunda oluşabilecek hırsızlık, yağma, güveni kötüye kullanma gibi suçlar ile banka veya kredi kartlarını kötüye kullanma suçu arasında gerçek içtima kuralının uygulanarak failin her bir suçtan ayrı ayrı cezalandırılması gerektiği****, 5237 sayılı TCK'nın 245/1 maddesindeki 'her ne surette olursa olsun' ifadesinin banka veya kredi kartlarının sadece hukuka uygun yollardan ele geçirilmesini kapsadığı,* ***kartın ele geçirilmesi aşamasına kadar eylemlerin suç teşkil etmesi durumunda, bu aşamaya kadar olan eylemleri suç teşkil etmesi durumunda, bu aşamaya kadar olan eylemlerin yasada karşılığı ne ise o suçtan cezalandırılacağı****..."*

Böylece her ne suretle olursa olsun ele geçirilen kartlardan istifade edilmesi hususu 245 inci maddede sayılan suçlar kapsamına girse de, kartın 'ele geçiriliş şekli'nin nasıl gerçekleştiği kritik öneme sahiptir. Kartı ele geçirme eyleminin bu suçtan farklı bir suça vücut vermesi halinde gerçek içtima kuralına göre 'ayrıca' oluşan suçtan failin cezalandırılması gerekmektedir.

245 inci maddenin üçüncü fıkrasında '...fiil daha ağır bir cezayı gerektiren bir başka suç oluşturmadığı takdirde...' ibaresinin yer almasının bir sonucu olarak bu fıkrada yer verilen eylemler açısından, diğer suçlar arasında zincirleme suç haricinde içtima oluşması mümkün görülmemektedir.

3.3.7 Etkin pişmanlık

Malvarlığına ilişkin suçlar özelinde TCK'ya 2005 yılında 5377 sayılı Kanun ile eklenen 'etkin pişmanlık' müessesesine, bu suçun son fıkrası ile göndermede bulunulmaktadır (Hafızoğulları ve Özen, 2016, s.465).

245 inci maddenin beşinci fıkrasında; "***Birinci fıkra kapsamına giren fiillerle ilgili olarak*** *bu* ***Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri***

uygulanır" denilerek TCK m.168'e atıf yapılmaktadır. Ayrıca madde lafzından, etkin pişmanlıktan sadece 245/1 suçunu işleyenlerin yararlanabileceği anlaşılmakta olup sahtecilik fiilleri ve sahte kart kullanımı suretiyle yarar sağlanması hususlarını içeren iki ve üçüncü fıkralarda yazılı suçları işleyenler, bu düzenlemeden istifade edemeyecektir.

Atıf yapılan etkin pişmanlık düzenlemesi ise TCK m. 168'de yerini bulmuş olup aşağıdaki gibidir:

Etkin pişmanlık
Madde 168 – (Değişik: 29/6/2005 – 5377/20 md.)
(1) Hırsızlık, mala zarar verme, güveni kötüye kullanma, dolandırıcılık, hileli iflâs, taksirli iflâs suçları tamamlandıktan sonra ve fakat bu nedenle hakkında kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde, verilecek cezanın üçte ikisine kadarı indirilir.
(2) Etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi halinde, verilecek cezanın yarısına kadarı indirilir.
(3) Yağma suçundan dolayı etkin pişmanlık gösteren kişiye verilecek cezanın, birinci fıkraya giren hallerde yarısına, ikinci fıkraya giren hallerde üçte birine kadarı indirilir.
(4) Kısmen geri verme veya tazmin halinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır.
(5) ***(Ek: 2/7/2012 – 6352/84 md.)*** *Karşılıksız yararlanma suçunda, fail, azmettiren veya yardım edenin pişmanlık göstererek mağdurun, kamunun veya özel hukuk tüzel kişisinin uğradığı zararı, soruşturma tamamlanmadan önce tamamen tazmin etmesi halinde kamu davası açılmaz; zararın hüküm verilinceye kadar tamamen tazmin edilmesi halinde ise, verilecek ceza üçte birine kadar indirilir. Ancak kişi, bu fıkra hükmünden iki defadan fazla yararlanamaz*

Söz konusu madde incelendiğinde, failin gösterdiği pişmanlık durumu ve eylemleri yanında bunun hangi aşamada gerçekleştiğinin de önem taşımakta olduğu ile değişen

oranlarda faile cezayı indiren kişisel nedenlerden yararlanmasına imkân tanındığı görülmektedir. Düzenlemenin üçüncü fıkrası yağma, beşinci ve son fıkrası ise karşılıksız yararlanma suçuna özel olarak tanzim edildiğinden TCK m. 245 açısından uygulanamazlar.

Banka veya kredi kartlarının kötüye kullanılması suçu kapsamında, failin gösterdiği pişmanlığın hangi aşamada gerçekleştiğine bağlı olarak cezada yapılacak indirim oranı değişecek olup süreç aşağıdaki gibi özetlenebilir:

- Fail, hakkında **soruşturma veya kovuşturma başlamadan önce** pişmanlık göstererek **mağdurun zararını aynen karşılar** (edindiği değer/nesnenin aynısı) **veya tazmin ederse** (edindiği değer harcanmış/tüketilmişse yerine geçecek tazmini değer) cezası **2/3** oranında indirilecektir.

- Fail hakkında **kovuşturma başlamışsa, hakkında ilk derece mahkemesince ceza kararına hükmedilene kadar** pişmanlık göstermesi ve **aynen iade ya da tazmin gerçekleştirmesi** durumunda cezası **1/2** oranında indirilecektir.

- **Kısmen geri verme veya tazmin** halinde, failin **etkin pişmanlıktan yararlanabilmesi mağdurun rızası ile mümkündür**.

Etkin pişmanlık hükümlerine ilişkin olarak, karar verilmeden önce gerekli araştırmanın yapılması suretiyle fail nezdinde uygulama olanağının değerlendirilmesi gerekmektedir. Nitekim Yargıtay 11. Ceza Dairesi'nin iki farklı kararında da bu hususa değinilmiştir (Turan ve Külcü, 2014, s.37):

*"...**sanığa, şikâyetçinin zararını karşılama olanağı tanınıp**, kısmen ödeme halinde de şikâyetinin devam edip etmediği saptanarak, **pişmanlık koşullarının gerçekleşmesi**..."* (13.02.2007 tarihli ve E.2006/3987, K.2007/740 sayılı karar)

"...Kredi kartının kötüye kullanılması suçu, kullanılan kart sayısınca oluşur; yakalandığında kendisini "deniz" olarak tanıtan sanığın eyleminin, "iftira suçunu oluşturup oluşturmayacağının belirlenmesi amacıyla, Deniz'in gerçek kişi olup olmadığının ibraz edilen kimliğe göre nüfus idaresinden kaydı getirtilerek tespiti ve sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekir; gerçek kimliği Soruşturma aşamasında anlaşılan ***sanık hakkında etkin pişmanlık hükümlerinin uygulanıp uygulanmayacağının karar yerinde tartışılması zorunludur****..."* (21.11.2006 tarihli ve E.2006/5704, K.2006/9321 sayılı karar)

Mezkûr kararların analizi kapsamında; etkin pişmanlık hükümleri her ne kadar failin iradesi ile gerçekleşmesi gerekse de, failin bu hususu bilmemesi veyahut mahkemece bu olanağın yeterince açıklanmaması gibi durumlar söz konusu olabilecektir. Bu nedenle en azından yargılama sürecinde böyle bir imkândan açık şekilde faile bahsedilmesi ve hüküm verilmeden önce varsa failin gösterdiği pişmanlık ile tazmin hususu göz önünde bulundurularak sonuç cezaya hükmedilmesinin gerektiği değerlendirilmektedir. Failin pişmanlık gösterip, mağdurun zararını gidermesi karşısında hâkimin ceza indirimini mutlak olarak uygulaması gerekmektedir. Zira düzenlemenin lafzında '*indirilebilir*' veya *'hâkimin takdirindedir*' ifadeleri yerine "*...oranında indirilir"* ibaresi, cezanın hafifletilmesini zorunlu kılmaktadır.

Failin gösterdiği pişmanlık 'iradi' olmalıdır. Yoksa kolluk kuvvetleri veya bir başkası tarafından, suç sonucu elde edilen değerlerin sahibine iadesi halinde pişmanlık hükmünden yararlanılması söz konusu olmayacaktır.

İşlenen suçun sonucunda mağdurun uğradığı zararın aynen geri verme veya tazmin suretiyle giderilmesinin, bizzat fail tarafından yapılması da şart olmayıp burada asıl olan failin bu yöndeki irade ve isteğidir (Özbek, 2007, s.1039).

Yargıtay Ceza Genel Kurulu'nun 27.05.2008 tarihli ve E.2008/11-127, K.2008/174 sayılı kararında da (Dülger, 2015, s.567); *"...yargılama boyunca gerek sözleriyle, gerekse birtakım davranışlarıyla* ***pişmanlığını ortaya koymuş ancak herhangi bir ödemede bulunmamış olan hükümlünün ... ailesini harekete geçirmek suretiyle***

ödemenin yapılmasını sağladığı *anlaşılmakla ... hakkında 5237 sayılı Yasanın 168. maddesinde düzenlenmiş bulunan* ***etkin pişmanlık hükümlerinin uygulanmasına bir engel bulunmadığı****ndan..."* denilerek, failin gerçek pişmanlık iradesine sahip olması; ancak kendisinin bizzat ödeme yapmasında birtakım engeller bulunması halinde, mağdurun zararının failin bir akrabası veya yakını tarafından giderilmesinin mümkün olabileceği açıklığa kavuşturulmuştur.

Etkin pişmanlık, görüldüğü üzere suçun oluşumunu ve cezayı tamamen ortadan kaldırmamakta sadece şartların oluşması halinde ceza indirimi imkânı sağlamaktadır. Bu nedenle, fail dışında suça iştirak eden diğer kişiler bakımından bu hükmün ayrı ayrı uygulanması gerekecektir. Dolayısıyla pişmanlık göstermeyen ve zararın giderilmesinde katkıda bulunmayan suç ortaklarının hafifletilmiş değil 'tam' cezai sorumlulukları devam edecektir.

3.3.8 Yaptırım ve yetkili adli merci

İncelediğimiz suç kapsamındaki üç ayrı suç tipinin her birinin farklı hadlerde yaptırıma bağlandığı görülmektedir.

245 inci maddenin birinci fıkrasında tanımlanan suçun işlenmesi halinde faile '*üç yıldan altı yıla kadar hapis cezası*' ve '*beş bin güne kadar adli para cezası*' verilecektir.

İkinci fıkrada düzenlenen suç tanımındaki eylemlerden birinin gerçekleştirilmesi halinde fail hakkında '*üç yıldan yedi yıla kadar hapis cezası*' ve 'o*n bin güne kadar adli para cezası*' kararı verilebilecektir.

245 inci maddenin üçüncü fıkrasında yer alan suçun icrası halinde ise, bu fiil daha ağır cezayı gerektiren bir başka suça vücut vermiyorsa fail bakımından *'dört yıldan sekiz yıla kadar hapis cezası*' ve '*beş bin güne kadar adli para cezası*'na hükmedilebilecektir.

Kanunda ‘veya’ ibaresi yerine ‘ve’ ifadesinin kullanımı ile bu cezaların birbirinin alternatifi olarak değil, birlikte uygulanmak zorunda oldukları sonucuna ulaşılmaktadır. Bu suçta anılan cezalara birlikte hükmolunması gerektiğinin gözetilmemesi, Yargıtay tarafından bozma nedeni sayılmıştır[14] (Yargıtay, 2018).

TCK’nın 52 nci maddesi uyarınca adli para cezasına, beş günden az ve ‘kanunda aksine hüküm bulunmayan hallerde’ yedi yüz otuz günden fazla olmamak üzere hükmedilebilecektir. Kanunda aksine hüküm şeklinde TCK m.245/1 ve m.245/3 için para cezasının üst sınırı beş bin; TCK m.245/2 için ise on bin gün olarak öngörülmüştür. Yasada hapis cezasının alt sınırının üç-dört yıldan başlarken, para cezasının üst sınırı yüksek tutulsa da alt sınırının beş gün olması eleştirilmektedir (Dülger, 2015, s.570).

Eleştiriye katılmak mümkündür; zira alt sınırdan hapis cezası olarak 3 veya 4 yıl alan bir failin, para cezasını da gün ve miktar olarak alt sınırdan alması halinde 5 x 20 = 100 TL gibi bir meblağa katlanması yeterli olacaktır. Bu nedenle maddede yapılacak *‘alt sınırı yüz*[15] *günden aşağı olmamak üzere...’* minvalinde bir revizyon ile yüksek oranda hükmedilebilecek hapis cezası yanında artık çok düşük kalmayacak oranda adli para cezası verilebilmesi yolunun açılabileceği değerlendirilmektedir.

Söz konusu suç, re’sen soruşturma ve kovuşturmaya tabi olup şikâyet aranmamaktadır.

Adli mercilerin görev ve yetkilerinin sayıldığı 5235 sayılı Kanunun 10, 11 ve 12 nci maddelerinin birlikte değerlendirilmesi durumunda, 245 inci maddedeki suçlarla ilgili dava ve işlerin, “Asliye Ceza Mahkemesi” görev alanında yer aldığı görülmektedir.

[14] Yargıtay 8. Ceza Dairesi'nin 21.03.2016 tarihli ve E.2015/15032, K.2016/3612 sayılı kararı.

[15] Örnek olarak yüz gün verilmiş olup böylece en alt miktar olan 20 TL ile çarpımı sonucu 2000 TL veyahut en üst miktar olan 100 TL ile çarpım sonucu 10.000 TL para cezasına hükmedilebilmesi mümkün olacaktır. Nitekim ceza yargılamasında genellikle alt sınırdan ceza verilmesi uygulamasına gidilmekte pek tabii bu durum failin ve suçun özeliklerine göre artırılabilmektedir. En üst gün fakat en alt miktardan para cezası takdir eden hâkimin mer’i mevzuata göre faile verebileceği ceza 5000 x 20 = 100.000 TL olacak; nihayet azami düzeyde adli para cezası verilmek istenirse bu kez meblağ 5000 x 100 = 500.000 TL.'ye kadar çıkabilecektir. Bu meblağ TCK. m.245/2 için 10.000 güne kadar çıkabileceğinden, azami sınır hesaplamaları iki kat olarak ele alınmalıdır.

243 üncü maddede tanzim edilen suçlara dair "yer yönünden yetkili mahkeme" konusundaki açıklamalarımız bu suç için de geçerlidir.

5271 sayılı CMK'nın, ilk derece mahkemesi kararlarının tekrar incelenmesini sağlayan kanun yollarına ilişkin düzenlemeleri bu suç için de uygulanabilecektir. Bu kapsamda, ilk derece yargı yerince verilen kararların Bölge Adliye Mahkemesi'nde istinaf, Yargıtay'da da temyiz yoluna götürülebilmesi mümkündür.

3.4 Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması

Bilişim alanında suçlar alanındaki hükümlerden TCK m.246 ile doğrudan bilişim suçlarına ilişkin TCK düzenlemeleri son bulmaktadır. Söz konusu düzenleme aşağıdaki gibidir:

Tüzel kişiler hakkında güvenlik tedbiri uygulanması
Madde 246- *(1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*

Daha önceki bölümlerde de bahsettiğimiz üzere; ceza hukukunda suçların kanuniliği ve şahsiliği ilkesi yanında, kusurlu davranış ile iradi hareket unsurlarının yalnızca gerçek kişiler için geçerli olabileceği hususlarının birlikte değerlendirilmesi sonucunda tüzel kişilerin suçun faili olamayacağı kabul edilmektedir.

Suçla tüzel kişi yararına menfaat sağlanması, fail olmamakla birlikte tüzel kişinin doğrudan veya dolaylı biçimde suçun içinde olmasını gerektirmektedir (Hafızoğulları ve Özen, 2016, s.471).

TCK'nın 20 nci maddesinde: *"**Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır***" denildiğinden, tüzel kişiler cezadan bağışık tutulsa da bir suç dolayısıyla kanunda öngörülmek şartıyla haklarında güvenlik tedbiri yaptırımı uygulanabilecektir.

Bazı durumlarda tüzel kişi bakımından önemli pozisyonda bulunan gerçek kişilerin bilişim suçlarından mahkûmiyet giymesi, ilgili şirketin en baştan yetkilendirilmesine dahi engel bir durum teşkil etmektedir. Nitekim Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliğinin "*Yetkilendirme başvuru şartları*" kenar başlığını haiz 7 nci maddesinin birinci fıkrasının (c) bendinde; yetkilendirilecek şirket hisselerinden en az yüzde onuna sahip gerçek kişi ortaklar ve tüzel kişiliği idare ve temsile yetkili kişiler ile şirket hisselerinden en az yüzde onuna sahip tüzel kişi ortakların hisselerinin en az yüzde onuna sahip gerçek kişi ortakların; TCK'nın bilişim alanında düzenlenen suçlarından hürriyeti bağlayıcı ceza ile hüküm giymemiş olması aranmaktadır.

Tüzel kişiler hakkında güvenlik tedbirine hükmedilmesi hususundaki genel düzenleme, TCK'nın 60 ıncı maddesi olup mezkûr maddenin metni aşağıdaki gibidir:

Tüzel kişiler hakkında güvenlik tedbirleri
Madde 60- *(1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkûmiyet halinde,* ***iznin iptaline*** *karar verilir.*
(2) ***Müsadere*** *hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.*
(3) Yukarıdaki fıkralar hükümlerinin uygulanmasının ***işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hâkim bu tedbirlere hükmetmeyebilir.***
(4) Bu madde hükümleri ***kanunun ayrıca belirttiği hallerde*** *uygulanır.*

Öncelikle maddenin son fıkrasından başlamak gerekmektedir. Çünkü bir suç sebebiyle tüzel kişiliğe güvenlik tedbiri uygulanması ancak kanunun ayrıca belirttiği durumlarda söz konusu olabilecektir. Nitekim bilişim alanında suçlar bölümünde yer alan 243 ila 245 inci maddeler arasındaki suçlarla ilgili olarak bu özel hüküm TCK. m.246 ile karşılık bulmaktadır.

Yasada güvenlik tedbiri olarak düzenlenen ilk husus ‘faaliyet izninin iptali’dir. Bunun uygulanabilmesi için ilk koşul özel hukuk tüzel kişisine, belirli bir faaliyette bulunabilmeyle alakalı verilen bir iznin varlığı; ikinci koşul ise anılan iznin sağladığı yetkinin kötüye kullanılması suretiyle tüzel kişi yararına kasıtlı bir suç işlenmesidir (Karagülmez, 2014, s.375).

Özel hukuk tüzel kişileri bakımından öngörülen ikinci güvenlik tedbiri ise ‘müsadere’ olup; tüzel kişi yararına işlendiği belirlenen suç bakımından müsadere hükümlerindeki koşullar da gerçekleşmiş ise, iyi niyetli üçüncü kişilerin hakları korunması şartıyla, o suçla bağlantılı olan eşya ve maddi çıkarların müsaderesine hükmedilecektir (Meran, 2008, s.600).

Yasa koyucu üçüncü fıkra ile ‘orantılılık’ ilkesi bağlamında işlenen suçu dikkate alıp, tüzel kişi hakkında güvenlik tedbirlerinin uygulanması sonucu doğabilecek çok ağır sonuçları; örneğin çok sayıda kişinin işsiz kalması veya iyi niyetli üçüncü kişiler bakımından telafisi güç zararların meydana gelmesini önlemeyi amaçlamıştır (Parlar, 2011, s.203). İyi niyetli üçüncü şahıslar; tüzel kişilik özellikle halka açılmışsa küçük hissedarlar ya da şirkete güvenerek aralarında büyük iş sözleşmeleri imza eden diğer firmalar olabilecektir.

3.5 İncelenen Suçlar Hakkında Güncel İstatistiki Veriler ve Analizi

TCK’nın ‘Bilişim Alanında Suçlar’ bölümünde düzenlenen suçların ihlal edilen maddeler çerçevesinde; suç ve sanık sayısı ile yargılama sonucu verilen kararlar bakımından gerçekleşme oranlarına istatistikler üzerinden değinerek birtakım analizler yapılmasında fayda görülmekte olup konuya ilişkin veriler aşağıda sunulmaktadır (Adalet Bakanlığı, 2018a-2018b):

Şekil 3.3 TCK'da Düzenlenen Bilişim Suçları Kapsamında Ceza Mahkemelerinde Açılan Davalardaki Suç ile Sanıkların Özellikleri ve Sayıları (2017)

İlgili Kanun Madde	Açılan Davalardaki Suç Sayısı	Sanık Sayısı										
		Gerçek Kişi									Tüzel Kişi Sayısı	Toplam
		T.C. Uyruklu							Yabancı Uyruklu			
		12-15 Yaş		15-18		18 VE Üzeri Yaş						
		E	K	E	K	E	K	Yaş ve Cinsiyeti Bilinmeyen	E	K		
243/1	498	17	3	11	7	372	77	0	10		1	498
243/3	49	7	1	1		34	6	0				49
244/1	159	5		4		129	16	1	4			159
244/2	1.313	20	1	39	2	1.103	140	0	6	2		1.313
244/4	436	7	1	11	2	381	31	0	3			436
245/1	25.988	826	28	716	53	19.708	4.374	7	215	30	31	25.988
245/2	1.437	5		19		1.287	85	0	37	4		1.437
245/3	1.860	15		17		1.542	102	0	180	4		1.860
245/A-1	41					29	2	0	8	2		41

Şekil 3.4 TCK'da Düzenlenen Bilişim Suçları Kapsamında Ceza Mahkemelerinde Açılan Davalarda Verilen Kararların Türleri ve Sayıları (2017)

İLGİLİ KANUN MAD.	ÇIKAN DAVALARDAKİ SUÇ SAYISI	MAHKUMİYET	BERAAT	HÜKMÜN AÇIKLANMASININ GERİ BIRAKILMASI	DİĞER KARARLAR	TOPLAM
243/1	484	108	226	97	95	526
243/3	57	2	24	11	20	57
244/1	382	79	100	27	216	422
244/2	1.065	378	400	222	274	1.274
244/4	457	238	157	46	167	608
245/1	24.966	13.176	3.849	1.599	15.321	33.945
245/2	872	834	134	12	458	1.438
245/3	1.198	1.176	239	13	591	2.019
245/A-1	16	2	7	2	6	17

Söz konusu veriler analiz edildiğinde;

- TCK m.245/1'de düzenlenen banka veya kredi kartının ele geçirilmesi suretiyle haksız çıkar sağlanması suçunun 25.988 suç sayısı olarak en çok işlenen suç olduğu ve bilişim alanında suçlar başlığı altında düzenlenen tüm suçlar arasında **%90'ı aşan** oranda gerçekleştiği,

- Erkek suçlu sayısının kadın suçlu sayısına oranla çok daha yüksek oranda seyrettiği,

- Suçların az sayıda da olsa 18, hatta 15 yaş altı faillerce de işlenebildiği, nitekim genç neslin bilişim sistemlerini kötüye kullanabilecek düzeyde teknolojik donanıma sahip olabileceği,

- Bilişim alanında suçlarda yargılama sonucunda mahkûmiyet ve beraat kararları tetkik edildiğinde **%75** oranında mahkûmiyet, yaklaşık **%25** oranında beraat kararına hükmedildiği,

Görülmektedir.

4 BİLİŞİM SİSTEMLERİ ARACILIĞIYLA İŞLENEBİLEN SUÇLAR (GENİŞ ANLAMDA/DOLAYLI BİLİŞİM SUÇLARI VE CEZALARI)

TCK'nın bilişim alanında suçlar başlığı altında bu alanda işlenebilecek suçların hepsi düzenlenmemiş olup bunun gerçekleştirilmesi de mümkün değildir. Zira bilişim sistemleri artık hayatın her alanında kullanılmaktadır; örneğin kişiler haberleşmelerini, bankacılık faaliyetlerini, alışverişlerini, fikri çalışmalarını, araştırmalarını bilişim sistemleri üzerinden yapmakta ve kendilerine ait olan çeşitli bilgileri yine bu sistem üzerinde kaydederek muhafaza etmektedir (Gül, 2016, s.24).

Çalışmamızın üçüncü bölümünde detaylı şekilde incelediğimiz TCK'nın 243 ila 246 ncı maddeleri dışında kalıp da bilişim sistemleri kullanılması suretiyle örneğin; hırsızlık, dolandırıcılık, hakaret, tehdit, şantaj, fikri hakların ihlali vb. birçok farklı suç tipi işlenebilmektedir. Dolaylı bilişim suçları, teknolojik gelişmeye paralel olarak olumsuz kullanım metotlarının da gelişmesiyle çok daha fazla suç tipini kapsayabilecektir. Çalışmamız devamında dolaylı bilişim suçlarının en önemli görülen tiplerine yer verilecektir.

4.1 5237 Sayılı Türk Ceza Kanunu Düzenlemeleri

4.1.1 Bilişim sistemlerinin kullanılması suretiyle hırsızlık

TCK'nın 141 inci maddesinde hırsızlık, zilyedinin[1] rızası olmadan başkasına ait taşınır bir malın, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alınması fiili olarak ifade edilmiştir. Taşınır mal ise bir yerden diğer bir yere taşınması mümkün olan, bir maddi varlığa sahip şeyler olarak tanımlanmaktadır (Ertaş, 2006, s.453). Dolayısıyla, bu suç için korunan hukuksal değer, kişilerin malvarlığı ve onun üzerinde mülkiyet hakkıdır.

[1] Eşya üzerinde tam hukuki hâkimiyet (*Rechtsherrschaft*) olarak tanımlanan mülkiyet hakkından farklı olarak zilyetlik, eşya üzerinde fiili hâkimiyeti (*Tatherrschaft*) ifade etmekte olup fiili hâkimiyet yanında kişide zilyet olma iradesi de aranmaktadır (Ertaş, 2006, s.74). Hırsızlık suçunda çalınan malın kişinin zilyedinde bulunması yeterli olup mala malik olması şart değildir.

TCK'nın 142 nci maddesinin ikinci fıkrasının (e) bendinde ise, hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi, suçun 'nitelikli' hali sayılmış olup hırsızlık suçunun işlenmesi sırasında bilişim sistemlerinin kullanılması halinde, hırsızlık suçunun basit halinden daha ağır bir cezaya (üç yıldan yedi yıla kadar hapis cezası) hükmedileceği düzenlenmiştir.

Ancak, TCK'nın 142 nci maddesinin ikinci fıkrasının (e) bendinde bilişim sistemlerinin kullanılması suretiyle hangi hırsızlık fiillerinin bu suçu oluşturacağı açıklığa kavuşturulmamıştır. Bu sebeple, TCK 142/2-e maddesindeki nitelikli halin bazı yönlerden TCK'nın 244/4'teki 'bilişim sistemine veya verilere müdahale suretiyle haksız çıkar sağlama' suçu ile benzerlik gösterdiği ve bazı durumlarda bu iki suçtan hangisinin oluşacağı konusunda doktrinde tartışmalar bulunmaktadır.

Hırsızlık suçunun bu nitelikli halinden söz edilebilmesi için, bir kimsenin zilyedi olduğu bir malın 'bilişim sistemleri kullanılarak' ondan alınması veya o mal üzerinde fiili hâkimiyet kurulması gerekmekte olup burada zilyedi olunan malın alınması ile kastedilen, bilişim sisteminin kullanılması suretiyle verilerin değil taşınabilir şeylerin çalınmasıdır (Parlar, 2011, s.106). Zira verinin nakli veya yok edilmesi fiilleri TCK'nın 244/2 düzenlemesinde ayrı bir suç olarak sayıldığından hırsızlık kapsamına girmeyecektir.

Bu bağlamda bir bankanın bilişim sisteminde yer alan 'para', söz konusu sistemde 'veri' olarak yer almakta, para da hırsızlık kavramını oluşturan 'mal' kavramına dâhil olmakta; dolayısıyla amaca uygun bir yorumla burada şeklen veri değil, bunun 'temsil ettiği değer' olan paranın suç açısından dikkate alınması gerekmektedir (Dülger, 2015, s.603). Bilişim sisteminde bulunan bir veri, bilgi veya programın izinsiz olarak başka yere gönderilmesi veya bulunduğu yerden alınması hırsızlık suçunu oluşturmamakla birlikte, bu yolla başkasına ait para üzerinde zilyedinin tasarruf olanağını kaldırarak, paranın başka yere gönderilmesi hırsızlık suçu kapsamında değerlendirilmelidir (Şen, 2012, s.325).

Yargıtay 13. Ceza Dairesi'nin 10.10.2013 tarihli ve E.2012/14783, K.2013/28348 sayılı kararında da bu şekilde bir değerlendirme yapılmıştır (Corpus, 2018):

"...Müştekiye ait hesaptan ***internet bankacılığı kullanılarak başka bir hesaba para transfer edilmesi*** *şeklinde gerçekleştirilen eylemde* ***suça yönelik kastın; var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yönelik olması*** *nedeniyle sanıkların fiilinin 5237 sayılı TCK.nın* ***142/2-e maddesindeki nitelikli hırsızlık suçunu oluşturduğu****..."*

Esasen burada fail, başkasına ait taşınır bir malı bulunduğu yerden fiilen almamakla birlikte, bilişim sistemi kullanmak suretiyle taşınır malı kendisine veya başkasına yarar sağlamak amacıyla izinsiz şekilde zilyedinin hâkimiyet noktasından başka bir yere naklederek haksız edinim sağlamaktadır.

4.1.2 Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık

TCK'nın 157 nci maddesi uyarınca dolandırıcılık, hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamaktır. TCK'nın 158 inci maddesinin birinci fıkrasının (f) bendinde ise dolandırıcılık suçunun bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesinin nitelikli dolandırıcılık suçuna vücut vereceği ve verilecek cezanın artırılarak uygulanacağı (üç yıldan on yıla kadar hapis[2] ve beş bin güne kadar adli para cezası) konusunu hükme bağlanmıştır.

Dolandırıcılık suçunu düzenleyen TCK'nın 157 nci maddesine göre, suçun hareket unsurunu oluşturan hileli davranışın, gerçek kişiye karşı yapılmış olması gerekmektedir. Dolayısıyla bir otomasyonun işleyiş mekanizmasına müdahale edilerek bir makineden para çekilmesi halinde makineye karşı bir hile kullanılmış

[2] 24.11.2016 tarihinden önce maddedeki yaptırımlar iki yıldan yedi yıla kadar idi. Bu nedenle suçun işlenme zamanı bu tarihten önce olan kişiler bakımından 'lehte kanun' prensibinden ötürü eski cezai hadler uygulanacaktır. Ayrıca aynı maddenin son fıkrası uyarınca; (f) bendi kapsamında işlenen bilişim suretiyle dolandırıcılık suçunda hapis cezasının alt sınırı dört yıldan, adli para cezasının miktarı ise suçtan elde edilen menfaatin iki katından az olamayacaktır.

olmasına rağmen bir insana karşı hileli davranışta bulunulmadığından, dolandırıcılık suçu oluşmayacaktır (Ergün, 2008, s.126-127).

Dolandırıcılık, failin hileli davranışlarla mağduru aldatarak onun veya bir başkasının zararına yarar sağlamasıdır. Bilişim sistemine ve veriye müdahale etmek suretiyle haksız çıkar sağlanması suçunda ise fail, dolandırıcılıktan farklı olarak mağdurun aldatılmış iradesi doğrultusunda yarar sağlamamakta, sisteme veya veriye müdahale şeklindeki teknik hile, kişiye karşı yapılmamaktadır (Yılmaz, 2018, s.58-59).

Yargıtay 11. Ceza Dairesi'nin 12.10.2009 tarihli ve 2008/11060 E. 2009/11936 K. sayılı kararında; *dolandırıcılık suçu; hileli davranışlarla bir kişinin aldatılıp onun veya bir başkasının zararına, failin kendisine veya bir başkasına yarar sağlaması suretiyle oluşur.* ***Suçun maddi unsurunu oluşturan hareketlerin, gerçek bir kişiye yöneltilmiş olması, onun kandırılarak çıkar sağlanması gerekir****. Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, hileli davranışlarla* ***gerçek kişiler dolandırılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde 'bilişim sistemine girerek haksız çıkar sağlama suçu' gerçekleşecektir****..."* denilerek, hileli gerçekleştirilen hareketlerin insana karşı değil bilişim sistemine karşı gerçekleştirilmesi halinde dolandırıcılıktan söz edilemeyeceği hususuna değinilmiştir.

Uygulamada en sık karşılaşılan bilişim sistemleri aracılığıyla dolandırıcılık eylemleri, failin bir kişiye ait sosyal medya ya da e-posta hesabının şifrelerini ele geçirerek, bu kişinin yakınlarına kendisini profil sahibi gibi tanıtıp belli bir menfaat istemesiyle gerçekleştirilmekte olup bu yöntem genel olarak 'phishing' (oltalama) metodunun karakteristiğini taşımaktadır (Dülger, 2015, s.616). Bu yöntemin özellikleri ilgili bölümde açıklanmış olup özetle; failin karşısındaki kişiler nezdinde farklı bir kişiliğe (o kişilerin tanıdığı) bürünmesi suretiyle link göndermek, verileri elde edecek bir web sitesine yönlendirmek veya cep telefonlarına iletilecek şifrenin talep edilmesi gibi hareketlerle haksız çıkar sağlaması durumu, nitelikli dolandırıcılığa örnek teşkil edecektir.

Yargıtay 15. Ceza Dairesi'nin 01.07.2013 tarihli ve E.2013/14846, K.2013/12178 sayılı kararı da bu yönde kanaatler içermektedir (Corpus, 2018):

*"...Sanığın, katılanın facebook hesabını kullandığı sırada, katılanın arkadaşı olan B. H. E'.nin **facebook hesabını bir şekilde ele geçirerek katılana mesaj gönderdiğini**, internet banka hesabı kullanıp kullanmadığını sorduğu, kullandığını öğrenince de kendisinden iade etmek şartıyla 450,00 TL para istediği, **katılanın Akbank internet bankacılığı aracılığıyla sanığın vermiş olduğu 0532 584 93 14 numaralı GSM hattına 450,00 TL para gönderdiğini**, daha sonra B. H. E'.nin facebook sayfasının dondurulduğunu görünce şüphelendiği ve bankadan yaptığı araştırmada gönderdiği paranın 9 dakika sonra Antalya Kumluca'da bulunan ATM'den çekildiğini öğrendiği, **B.'yi aradığında facebook hesabının çalındığını söylediği**, ATM güvenlik kamera kayıtlarının temin edilerek emanete alındığı, havalenin yapıldığı 05... numaralı GSM hattının sanık M'nin annesi F.Ç. adına kayıtlı olup sanığın gözaltına alındığı 25.12.2012 tarihinde yapılan üst aramasında suça konu hattın sanığın cep telefonuna takılı halde üzerinde bulunduğu o**layda, nitelikli dolandırıcılık suçunun oluştuğu** yönündeki kabulde bir İSABETSİZLİK GÖRÜLMEMİŞTİR..."*

Hileli davranışa ancak gerçek şahısların muhatap olabilmesi nedeniyle bu suçun doğrudan bilişim suçlarında sayılan davranışlar ile karıştırılması nitelikli hırsızlık suçuna göre daha zordur. Söz konusu suç 244 üncü maddede yazılı fiillerin işlenmesi suretiyle haksız çıkar sağlama (TCK m.244/4) ile karışabilecek olsa da bu hükümdeki '*... başka bir suç oluşturmaması ...*' ibaresiyle yardımcı norm tipine bürünmesi karşısında, dolandırıcılık şartları var ise TCK m.244/4'ten bahsedebilmenin mümkün olmayacağı değerlendirilmektedir.

Konuya ilgili Yargıtay Ceza Genel Kurulu 11.06.2013 tarihli ve E.2013/15-239, K.2013/289 sayılı kararında net ifadelerle bu durumu destekleyici bir sonuca hükmetmiştir (Corpus, 2018):

"...Günümüzde bilişim sistemleriyle sesli-görüntülü haberleşme, elektronik imzanın kabulü, yeni ticari ilişkiler, internet bankacılığı hizmetiyle para transferleri ve bunlar gibi pek çok yenilik toplumsal hayata girmiş, bilişim gerek iş gerekse günlük hayatta vazgeçilemeyecek kadar önemli bir noktaya ulaşmış, ***bilişim teknolojileri daha hızlı ve ucuz bir nitelik arz etmesi nedeniyle, klasik yöntemlere nazaran daha fazla tercih edilir DURUMA GELMİŞTİR. Bu sistemlerin güvenle kullanılması, aynı anda hızlı ve kolayca birçok kişiye ulaşılması ve diğer taraftaki failin kontrol imkânını azaltması nedeniyle nitelikli HAL SAYILMIŞTIR****.*

Bilişim sisteminin aldatılmasından söz edilemeyeceği için, ancak bu sistemin araç olarak kullanılarak bir insanın aldatılması yani dolandırılması halinde bu bendin UYGULANMASI MÜMKÜNDÜR. Aksi halde yani sisteme girilerek bir kişi aldatılmayıp sistemden yararlanılarak çıkar sağlanmışsa bilişim suçu veya bilişim sistemi kullanılmak suretiyle hırsızlık suçunun oluşması SÖZ KONUSU OLACAKTIR*...*

Bilişim sistemlerinin aynı anda birçok kişiye ulaşmasındaki çabukluk ve sağladığı kolaylığa dayanarak "www.sahibinden.com" adlı internet sitesinde emsallerine göre fiyatını da ucuz göstererek araç satışı için ilan veren sanığın, bu ilanı görüp kendisini telefonla arayan şikâyetçiden kapora adı altında 250 Lira alması şeklinde gerçekleşen olayda; ***sanığın bilişim sistemini araç olarak kullanmak suretiyle suçu işlediği anlaşılmakla, eylemin TCK'nun 158 inci maddesinin 1 inci fıkrasının (f) bendinde düzenlenmiş olan nitelikli dolandırıcılık suçunu oluşturduğu*** *KABUL EDİLMELİDİR..."*

Gerek nitelikli hırsızlık, gerekse nitelikli dolandırıcılık suçu bakımından kanunda etkin pişmanlık hükümlerinin uygulanabileceği öngörülmüştür.

En yaygın dolandırıcılık yöntemleri ise aşağıdaki gibi sıralanabilir (Gül, 2016, s.36-37):

- ***Sahte Unvanlar:*** Telefon ve internet üzerinden kredi kartı masraflarının geri alınması veya bir kuruluştan sigorta yaptırıldığı konusunda ikna edilen kişinin kalan borcunu ödemesi aksi halde icra yoluna başvurulacağı tehdidiyle avukat gibi hareket eden kişilerin hileli eylemleri sık rastlanan durumlardandır. Bununla birlikte; türlü rütbelerde polis memuru, Cumhuriyet Savcısı ve hâkim gibi unvanların da sıkça kullanıldığı görülmekte olup emniyet güçleri tarafından belirli aralıklarla bu kapsamda bilgilendirme mesajları vatandaşların cep telefonlarına gönderilmektedir. Halkın bilgilendirilmesi amacıyla gönderilen bu mesajlarda *"adınıza çok sayıda hat çıkarılmış ve terör örgütü tarafından kullanılıyor"* ya da *"banka hesaplarınıza giriliyor, biz bu şahısları tespit etmeye çalışıyoruz"* gibi ikna edici cümlelerin yanı sıra, *"Operasyonun gizliliği var, kimsenin duymaması gerekiyor, herhangi bir şahsa söylerseniz, olayı deşifre ederseniz gözaltına alınırsınız"* şeklinde kişileri tehdit eden, korku ve panik uyandıran ifadelere inanılmaması yönünde uyarılar yapılmaktadır (Kaya vd., 2013, s.104).

- ***Fatura Ödeme/Sorgulama Siteleri***: İnternet üzerinden telefon veyahut elektrik, su vb. faturalarını ödeyenlerin fatura tahsilatı veya sorgulama adıyla sahte sitelerde hileli davranışlar sonucu dolandırıcılığa uğraması mümkündür.

- ***Şüpheli e-Postalar***: Çalışmamızın 'spam mail' metodunun anlatıldığı bölümünde de aktarıldığı üzere, özellikle bankadan gönderilmiş görüntüsü verilen e-postalar kanalıyla birçok kişi dolandırılmaktadır. Kişilerin bankanın anılan sahte e-postalara tıklaması ve şifrelerini girmesiyle, ilgili hesaplara faillerin erişimi olanaklı kılınmaktadır.

- ***Sahte İş İlanları***: İşsiz vatandaşlara iş vaadi ile bünyelerinde boş pozisyon olduğu ve maaş/avans yatırılması için mağdurlardan edinilen hesap ve kart bilgileri dolandırıcılığın bir başka metodu olarak karşımıza çıkmaktadır.

- ***Ödül Vaadi***: Verilen internet sitesine girilmesi veya gönderilen telefonun aranması sonucunda, sözde ödüle ulaşılabileceği hilesi ile şahısların dolandırılmalarına uygulamada yaygın olarak rastlanmakta olup mağdurların kişisel verilerinin ele geçirilmesi veya yüksek cep telefonu faturaları ile karşı karşıya bırakılmaları söz konusu olabilmektedir.

- ***Sosyal Medya Arkadaşlarının Hesaplarının Ele Geçirilmesi***: Sosyal medya uygulamalarında kişilerin arkadaş listesinde bulunan birinin hesabını ele geçiren dolandırıcılar tarafından mağdur kişiyle normal bir iletişim kurularak güven ortamı sağlanmakta ve daha sonra kişilerden para talep edilmekte ya da telefonlarına/e-postalarına gelecek bir şifreyi kendilerine göndermeleri talep edilmekte ve nihayet edinilen bilgiler vasıtasıyla kişiler maddi zarara uğratılmaktadır.

- ***Dolandırıcı Siteler***: Kişilerin iyi niyetine güvenerek, güvenli imajı çizen arkadaşlık, e-ticaret ve çeşitli hizmetler sunan internet siteleri de bilişim suretiyle dolandırıcılığın bir başka yöntemidir. Sitede yer alan ürünlerin gösterildiğinden farklı marka-modelde, renkte veya özellikle çok daha altında bir kalitede ürün gönderilmesi durumu da buna örnek teşkil etmektedir. Zira kişi, sitede yer alan ürün özellikleri ve görselleri ile hileye uğratılmaktadır.

4.1.3 Özel hayata ve hayatın gizli alanına ilişkin suçlar

TCK'nın "Kişilere Karşı Suçlar" başlıklı ikinci kısmının dokuzuncu bölümünde 132 ila 140 ncı maddeler arasında; kişiler arasındaki haberleşmeye ilişkin ihlaller, özel hayatın gizliliğine müdahale ve kişisel verilerin korunmasına dair suç tipleri düzenlenmiştir.

Başlıkta yerini bulan özel hayatın gizliliğinin ihlal edilmesi hususu 136 ncı maddede yaptırıma bağlanmış ve bu fiilin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi hâlinde cezanın alt sınırının bir yıldan az olamayacağı ifade edilmiştir. Ayrıca

kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa edenler de aynı maddeye dayanarak cezalandırılabilecek olup, fiilin basın ve yayın yoluyla işlenmesi hâlinde de aynı cezaya hükmedilebilecektir.

Bölümde sayılan suç tiplerinin bilişim sistemleri aracılığıyla işlenebilmesinden ziyade, bu ihlallerin devam ettiği sürenin mağduriyeti arttırıcı bir unsur olduğu yadsınamaz bir gerçektir. Başlığa dâhil bazı suçlar çalışma devamında açıklanacaktır.

4.1.3.1 Haberleşmenin gizliliğini ihlal, haksız dinleme ve kayda alma

Bölüm altında yerini bulan ilk suç tipleri 132 ve 133 üncü maddede bulunan *haberleşmenin gizliliğini ihlal* ile *kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması*dır.

Haberleşmenin gizliliği aynı zamanda anayasal düzeyde korunan özel bir alandır. Anayasanın 22 nci maddesinde herkesin haberleşme hürriyetine sahip olduğu, haberleşmenin gizliliğinin esas ve dokunulmaz olduğu hükme bağlanmıştır. İnsan Hakları Evrensel Bildirgesi'nin 12 nci maddesinde de benzer şekilde haberleşme özgürlüğüne karışılmaması ve yasa tarafından korunma hakkına sahip olunduğu belirtilmektedir.

Haberleşme kanunda tanımlanmamış olup genel anlamda, düşünce iletmeye elverişli araçlarla uzakta bulunan kimseler arasında iletişimde bulunmak; dar anlamda ise belli kişiler arasında, elverişli araçlarla düşüncenin iletilmesi olarak ifade edilebilmektedir (Hafızoğulları ve Özen, 2009, s.11).

Suçun maddi konusu haberleşme olup, haberleşmenin türü (mektup, telefon, e-posta vb.) önem taşımamaktadır. Kişiler hür biçimde haberleşmenin sağlanması ve içeriğinin başkalarınca öğrenilmemesi hakkına sahip olduğundan bunun ihlali halinde suç oluşacaktır. Haberleşmenin aleni bir ortamda yapılması halinde ise, örneğin bir sohbet sitesinde genel kanalda herkesle kurulan iletişimin konusunun haberleşmenin gizliliği kapsamında değerlendirilmesi mümkün görülmemektedir.

Haberleşmenin gizliliğinde failin ayrıca haberleşmenin içeriğini ‘kayıt’ etmesi durumunda suç nitelikli hal alacak ve verilecek ceza ağırlaştırılacaktır. Sadece kayıt işlemi, ağırlaştırıcı sebep için gerekli ve yeterlidir. Kaydın mutlaka dinlenmesi veya kullanılması gerekmemektedir.

Suçun ikinci fıkrasında haberleşme tarafları dışından birinin, üçüncü fıkrasında ise haberleşmenin taraflarından birinin haberleşme içeriğini ‘ifşa’ etmesi yaptırıma bağlanmıştır. Fıkranın son cümlesinde ise haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde de aynı cezaya hükmolunacağı öngörülmüştür.

İfşa halinde, haberleşmenin içeriğinin “hukuka aykırı” olarak açıklanması gerekmekte olup örneğin kişiler arasındaki telefon konuşmalarına ilişkin kayıtların, savcılık veya mahkemeye verilmesi, duruşmada açık bir şekilde dinlenmesi veya okunması hâlinde suç oluşmayacak; buna karşılık, henüz soruşturma aşamasında iken, kişiler arasındaki konuşma içeriklerinin, hukuka uygun bir şekilde kayda alınmış olsalar bile, örneğin televizyonlarda veya gazetelerde yayınlanması hâlinde, bu suç oluşacaktır (Yokuş Sevük, 2009, s.180). Nitekim uygulamada genellikle boşanma ve ceza davalarında hukuka aykırı olarak haberleşme içeriklerini kaydettiği veya ifşa ettiği bilinmektedir. Ancak bu türde bir delil CMK’nın 206 ncı maddesi uyarınca kanuna aykırı elde edildiğinden reddedilecek ve elde etme fiilini icra eden kişiye ilgili suçlardan ceza verilmesi söz konusu olacaktır.

4.1.3.2 Kişisel verilerin hukuka aykırı verilmesi, ele geçirilmesi ve kaydı

TCK’nın 135 ve 136 ncı maddelerinde *kişisel verilerin hukuka aykırı olarak kaydedilmesi, dağıtılması ya da ele geçirilmesi* suçları düzenleme alanı bulmuştur. 137 nci maddede ise verileri sistem içinde yok etmekle yükümlü olanların, yasal süreler bitmesine rağmen bu işlemi yapmamaları hali yaptırıma bağlanmıştır.

Kişisel verilerin korunması hakkı, yalnızca kişisel çıkarların korunması ile ilişkili olmayıp, insan onuru ve temel özgürlükler gibi çok daha geniş bir alana hizmet

etmektedir (Küzeci, 2010, s.75). Kişisel verilerin korunması hakkı, bir temel hak olarak hem yasal bir temele veya ilgilinin rızasına dayanmaksızın kişisel verilerine yönelik hukuka aykırı müdahaleler karşısında bireyin korunmasını, hem de bireyin bu veriler hakkında karar verme özgürlüğünün güvence altına alınmasını amaçlamakta; ayrıca anayasada temellerini bulan insan onuru ve kişiliğin geliştirilmesi hakkı ile ilişkisi, kamusal organların kişisel verileri toplarken ve işlerken bu haklara riayet etme yükümlülüğünü de beraberinde getirmektedir (Şimşek, 2008, s.114).

Daha önceki dönemlerde az sayıda kişi/kurumun elinde yazılı halde dosyalanmış bilgiler, bilgi teknolojilerinin gelişmesi ile sayısal ortama aktarılmış, internetin yaygınlaşması sonucunda da ilgili ilgisiz herkesin erişimine açılmıştır. Ayrıca bu verilerle sanal alanda verilerin gerçek sahibiymiş gibi sahte profiller oluşturulması ve bunlar aracılığıyla suç işlenmesi halinde, mağdur ve masum gerçek veri sahibinin adli merciler önünde sanık ve/veya davalı olarak bulunmak zorunda bırakılması dahi söz konusu olabilmektedir (Dülger, 2015, s.632).

Kişisel verilerin korunması hakkına ilişkin olarak Anayasa'nın 20 nci maddesinde genel çerçeve belirlenmiş olmasına karşın, uygulayıcıya yol gösteren ve kişisel verilerin korunmasına ilişkin usul ve esasların belirlendiği kanun KVKK olup yasada; kişisel verilerin işlenmesine ilişkin olarak gözetilmesi gereken işlemler (verilerin hukuka uygun olarak ve belirli meşru amaçlar için işlenmesi, ilgilinin rızasının alınarak saklanması ve gerektiğinde bu bilgilerin güncellenmesi gibi veri sahibine karşı sorumlulukların yerine getirilmesini kapsayan temel hususlar) açık olarak düzenlenmiştir (Henkoğlu, 2017, s.245).

TCK, kişisel verilerin ceza hukuku açısından korunması açısından kişisel verileri hukuka aykırı işleyenler hakkında etkin bir yaptırım sistemi getirmiş olup, mezkûr hükümler konuyla ilgili AB direktifleriyle de uyum göstermekte; nitekim KVKK da kişisel verilerin korunması alanında yeni yaptırımlar getirmeyip burada bahsedilen hükümlere atıfta bulunmaktadır (Ayözger, 2016, s.91). Kanunda öngörülen yükümlülüklere aykırı davranılması halinde uygulanacak idari yaptırımlar ise 18 inci maddede düzenlenmiş olup bu kapsamda; aydınlatma ve veri güvenliğini sağlama,

Kişisel Verileri Koruma Kurulu kararlarını yerine getirmeme ile sicile kayıt ve bildirim yükümlülüklerine aykırı davranılması kabahat olarak öngörülerek, idari para cezası yaptırımına bağlanmıştır (KVKK, 2018, s.72). İdari yaptırımlara Kurul tarafından karar verilecek olup her idari işlemde olduğu gibi verilen bu yaptırım kararlarına karşı da yargı yolu (idare mahkemeleri nezdinde) ilgililere açıktır.

KVKK'ya göre kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi işaret etmektedir. Geniş anlamda ise; belirli veya belirlenebilir bir kimsenin kimliğine, etkin kökenine, fiziksel özelliklerine, sağlık durumuna, genetik verilerine, öğrenim veya istihdam durumuna, ikamet adresine, kredi kartı bilgilerine, banka ve sigorta kayıtlarına, adli arşiv ve genel bilgi toplama kayıtlarına, düşünce ve inançlarına, alışveriş alışkanlıklarına, telefon rehberine, fotoğrafına, bilgisayarının IP adresine, parmak izine, cep telefonundan gönderdiği kısa mesajlarına, e-postalarına, sosyal paylaşım sitelerindeki aktivitelerine, en son gittiği restoran, bar ya da müzeye kadar ilgilisi olduğu ve kişiyi tanımlayan her türlü bilgidir (Ayözger, 2016, s.6)

TCK'nın 135 inci maddesinde kişisel verilerin hukuka aykırı kaydedilmesi suç sayılmış ve altı aydan üç yıla kadar hapis cezası öngörülmüşken, maddenin ikinci fıkrasında; kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kaydetmenin cezasının ise 2016 yılındaki değişiklikle isabetli olarak yarı oranında artırılacağı öngörülmüştür.

Burada, yasa koyucunun hükmün birinci fıkrasında ve ikinci fıkranın belirtilen bölümünde suçun oluşabilmesi için kaydın "*hukuka aykırı*" olarak yapılmasını ararken "*kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine*" ilişkin bilgilerin kayıt edilmesi açısından bu ibareye yer vermemiş olması dikkat çekmekte olup belirtilen türdeki bilgilerin kaydının her durumda hukuka aykırı olacağı söylenebilir. Zira burada bazı veri türleri özel nitelikte görülmüş ve farklı bir düzenlemeye tabi tutulmuştur (Küzeci, 2010, s.309). KVKK'nın 6 ncı maddesinde de; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve

güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri "özel nitelikli kişisel veri" olarak ele alınmış ve işlenmesi daha sıkı koşullara bağlanmıştır.

135 inci maddedeki suçun oluşması için kişisel verilerin yayınlanması ya da başkasının kullanımına açılması gerekmemekte olup verilerin hukuka aykırı olarak kaydedilmesi yeterlidir ve suçun gerçekleşmesi için maddede ayrıca bir zararın da meydana gelmesi aranmadığı için kayıt etme işlemin gerçekleşmesiyle suç meydana gelmiş olacağından bu bir soyut tehlike suçudur (Dülger, 2016, s.129).

Kişisel verilere ilişkin suç oluşturan eylemler aynı zamanda kişilik hakkının ihlaline yol açmakta olup, ihlal hangi araçla ve hangi alanda gerçekleşirse gerçekleşsin ilgili yasalar olan Medeni Kanun (m.24-25) ve Borçlar Kanunu (m. 49 vd.) uygulama alanına sahiptir; nitekim ihlalin özel hukuk açısından sonlandırılması ve zararın tazmini bu suretle sağlanabilecektir (Dülger, 2016, s.116). Dolayısıyla bu suçların işlenmesi durumunda, failin sadece cezai değil hukuki sorumluluğa da (tazmin yükümlülüğüne) katlanması gerekecektir.

4.1.3.2.1 Veri koruma hukukunda güncel uluslararası gelişmeler

Avrupa İnsan Hakları Sözleşmesinin 8 inci maddesiyle koruma altına alınan özel hayatın gizliliği ve ailenin korunması hakkı ile AB Temel Haklar Şartı'nda yer alan özel hayat ve aile hayatına saygı hakkı (m.7) ve ayrıca düzenlenen kişisel verilerin korunması hakkını (m.8) temel alan AB veri koruma hukuku bakımından 95/46 sayılı Direktif bu alandaki korumanın en önemli parçalarından birini oluşturmakta iken ekonomik faaliyetler içerisinde verinin kullanımı ve rolünün hızla değişmesi öncelikle düzenleyici çerçevede bir değişimi, yani Direktif'in güncellenmesi ihtiyacını doğurmuş ve söz konusu düzenlemede yapılacak güncelleme, çok daha yüksek düzeyli bir gizlilik korunmasının sağlaması için gerekli görülmüştür (Kalkınma Bakanlığı, 2017, s.10).

Genel Veri Koruma Tüzüğü (*General Data Protection Regulation-GDPR*) bu gereklilik kapsamda 2012 yılında taslak çalışmalarına başlansa da tüzük 2018 yılında ancak yürürlüğe konulabilmiştir.

Kalkınma Bakanlığı'nın çalışma raporunda; 173 paragraflık resital bölümü ve 99 maddeden oluşan temel tüzük metniyle yaklaşık 90 sayfadan oluşan GDPR'nin oldukça kapsamlı bir veri koruma çerçevesi sunduğu ve GDPR'nin köklü yenilikler öngördüğü[3] üç temel özelliği ifade edilmektedir (2017):

i) Kişisel verilerin ve veri sahiplerinin daha etkin korunması,
ii) Veri işleyenler ile veri kontrolörlerinin sorumluluklarının artırılması,
iii) Uygulama alanı bakımından daha güçlü düzenlemelere sahip olması.

Tüzükte dikkat çeken ve kişisel veriler bağlamında oldukça önem taşıyan "Unutulma Hakkı" (*Right to be Forgotten*[4]) olmaktadır. AB kaynaklı gelişen bu hakkın; kişilerin üçüncü kişiler nezdinde 'unutulmayı' talep ettiği ve kendileri hakkında istenmeyen herhangi bir dijital verinin silinmesini istediği bir müessese olduğu ifade edilmektedir (Gündoğan Özer, 2013, s.12).

Bu hak özellikle sosyal medya kullanıcıları bakımından büyük önem taşımaktadır. Kullanıcı sayılarının milyarları[5] aştığı bu mecralarda, kullanıcıların ilgili veya ilgisiz birçok bilgisinin depolandığı bilinmektedir.

---

[3] Aynı raporda Tüzük gücünde bir düzenlemeyle üst derece uyumlaştırma sağlanarak uygulamadaki farklılıkların giderildiği, veri işleyenlerin tamamının (üçüncü taraflar dâhil; örneğin bulut hizmet sağlayıcıları) sorumlu tutulduğu, AB vatandaşlarına birlik dışında da koruma sağlandığı, mağdurlara tazminat talebi imkanı tanındığı, unutulma hakkı ve veri taşınabilirliği hakkının düzenlendiği, güçlendirilmiş rıza sisteminin getirildiği, daha sıkı yaptırımların öngörüldüğü (20 milyon Avro veya hizmet sağlayıcının küresel gelirinin yüzde dördü gibi önemli miktarlar), başlangıçtan ve tasarımdan itibaren koruma yaklaşımının (*data protection by default-by design*) benimsendiği gibi önemli değişikliklerin yürürlüğe konulduğu ifade edilmektedir (2017, s.14-18).

[4] Bunun yanında Tüzükte bu hak 17 nci maddede "*Right to Erasure*" ibaresi ile birlikte kullanılmıştır (*https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN*).

[5] 2018 yılı başı itibarıyla Facebook 2.2, YouTube 1.9, WhatsApp 1.5, Facebook Messenger 1.3, WeChat ve Instagram da 1 milyar aktif kullanıcı ile faaliyet göstermektedir (*https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/)*.

Çevrimiçi alanda faaliyet gösteren büyük firmaların 'bedava' hizmet verdiği düşünülse de aslında bu hizmetleri kullanmak için ödenen bedel çok daha yüksektir; zira yüklediğimiz bir resmin veya yaptığımız bir yorumun değerini gelecek bir zaman için tahmin etmek çok kolay değildir. Nitekim senelerce bedava görünen hizmetin bedeli, esasen bir daha asla silinmeme riskini barındıran 'özel hayat/veri gizliliği' ile ödenmiş bulunmaktadır (Kulevska, 2013).

Unutulma hakkı AB'de ilk kez Mario Costeja Gonzales adlı bir İspanyol avukatın Google'da adıyla arama yaptığında, borcundan dolayı evini satmak zorunda kalmasına yönelik bir haberin bulunmasından şikâyet etmesi sonucunda dava yoluyla tartışılmış ve 2014 yılında verilen AB Adalet Divanı kararında özetle aşağıdaki sonuçlara varılmıştır (Taşkın, 2016, s. 325-326):

- Üçüncü kişiler tarafından aranan içeriklere ulaşılmasına aracılık ettiklerinden arama motorları denetleyicidir. Bu motorlar sayesinde kullanıcılar, üçüncü kişilerce internete yerleştirilen içerikleri bulur. Ayrıca arama motorları; verileri indeksleyip, depolayıp ve son olarak kullanıcıların rahatça ulaşabilmesi için sistematik hale getirdiklerinden sorumludurlar.

- Arama motorunun işleteni, internette üçüncü kişilerce yayınlanan veri, veri öznelerinin adıyla arandığında bulunabilen öznelere ilişkin bilgiler ve sonuçları motordan kaldırmakla yükümlüdür.

- Veri öznesinin adıyla çıkan aramalar sonucunda ortaya çıkan bilgilerin arama motorundan kaldırılması için, adı geçen verilerin, verilere ulaşan üçüncü kişiler nezdinde veri öznesi hakkında önyargılara yol açması gerekmez. Veri öznesi, hakkındaki bilgilerin üçüncü kişiler tarafından erişilememesini isteme hakkına sahiptir. Bu hak, arama motorunun ekonomik çıkarıyla kıyaslandığında daha üstündür. Başka bir deyişle, veri öznesinin kişilik hakkı, kamunun o bilgilere ulaşma hakkına göre üstün ve önceliklidir.

Türk hukukunda unutulma hakkına, Yargıtay ve Anayasa Mahkemesi'nin bazı kararlarında yer verilmiştir. Nitekim Anayasa Mahkemesi'nin 2013/5653 başvuru numaralı ve 03/03/2016 tarihli kararında başvurucunun Anayasanın 17 nci maddesinde güvence altına alınan şeref ve itibarın korunması hakkının ihlal edildiğine karar vermiş ve unutulma hakkından genişçe bahsederek, ihlal gerekçesini bu hak kapsamında değerlendirmiştir (Anayasa Mahkemesi, 2016):

"...Unutulma hakkı, internet ortamında bir haberin uzun süredir kolayca ulaşılabilir olması nedeniyle kişinin şeref ve itibarının zedelenmesi durumunda gündeme gelmektedir. Bu ***hakkın amacı, internetin yaygınlaşması ve sağladığı imkânlar nedeniyle ifade ve basın özgürlükleri ile kişilerin manevi varlığının geliştirilmesi hakkı arasında gerekli hassas dengenin kurulmasını sağlamaktır****. O hâlde bu yol, internet ortamında haber arşivini koruma altına alan basın özgürlüğünün ve halkın haber ve fikirlere ulaşma özgürlüğünün özüne dokunmayacak ve aynı zamanda hak sahibinin çıkarlarını koruyacak şekilde kullanılmalıdır.*

...Bu bağlamda haber konusunun, haberin arşivde kolaylıkla ulaşılabilir kılınması için gerekli bulunan toplumsal açıdan haber değerinin devam etmesi veya haberin geleceğe ışık tutacak niteliğe sahip olması özelliklerini taşıdığı söylenemez.

...Sonuç olarak ***başvurucu hakkında yapılan haberler unutulma hakkı kapsamında değerlendirilmesi gereken haberlerdir****.* ***İnternet ortamının sağladığı kolaylıklar gözetildiğinde başvurucunun şeref ve itibarının korunması için anılan habere erişimin engellenmesi gerekmektedir****. Bu bağlamda erişiminin engellenmesine yönelik talebin reddedilmesiyle ifade ve basın özgürlükleri ile kişinin manevi bütünlüğünün korunması hakkı arasında adil bir dengenin kurulduğu söylenemez..."*

Şahsa bağlı hak ve özgürlükleri doğrudan ilgilendirmesi sebebiyle, küresel düzenlemelerle paralellik sağlanmasını da teminen, bu hakkın ülkemiz mevzuatında da tanınmasının gerekli olduğu değerlendirilmektedir.

4.1.3.3 Ortak hükümler

Özel hayata ve hayatın gizli alanına ilişkin suçların; kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hâlinde TCK'nın 137 nci maddesi uyarınca verilecek ceza yarı oranında artırılacaktır.

Düzenlenen bu hüküm oldukça yerindedir. Zira faaliyet gösterilen alan itibarıyla, kişilerin şahsi verilerine rahatça erişebilecek faillerin diğer kişilere oranla daha yüksek bir ceza tehdidi altında tutulması gerekmektedir. 5809 sayılı EHK'nın 63 üncü maddesinde de; elektronik haberleşme hizmeti vermek üzere yetkilendirilmiş bulunan işletmecilerin personelince, TCK'nın bu bölümünde öngörülen suçların işlenmesi halinde ilgili cezalara hükmolunacağı, ilaveten 137 nci maddeye göre yapılacak artırımın yarım değil bir kat olarak uygulanacağı hususu düzenlenmiş, böylece maddede sayılan personel bakımından cezai sorumluluk genişletilmiştir.

Ayrıca bu bölümde düzenlenen suçlar; kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, TCK'nın 139 uncu maddesi gereğince şikâyete tabi olup re'sen kovuşturulmamaktadır. Kanunun bu bölümdeki son maddesi olan 140 ıncı madde uyarınca da, bu suçların işlenmesinde suça karışan tüzel kişiler hakkında güvenlik tedbiri uygulanacaktır.

4.2 5846 sayılı Fikir ve Sanat Eserleri Kanunu düzenlemeleri

Fikri mülkiyet hakları, şahsa ait ancak maddi nitelikte olmayan fikir ve düşünceler üzerindeki hak ve yetkileri ifade etmektedir. Bu kapsamda, büyük emek ve çaba sarf edilerek ortaya çıkarılan fikir ve sanat eserlerini meydana getiren eser sahiplerinin haklarının muhafaza altına alınması gereklidir.

Fikir ve düşünceler maddi bir varlık üzerinde cisimlenmiş olsa bile, hakkın konusu, maddi varlık olmayan, o madde içinde cisimlenmiş olan fikri ürün ya da çabadır (Kılıçoğlu, 2006, s.2).

İnsan Hakları Evrensel Bildirgesi'nin (İHEB) 27 nci maddesi aşağıdaki gibi olup herkesin bilim, edebiyat veya sanat alanına katılmak ilerlemek ve faydalanmak ile yarattığı eserlerin korunmasını isteme hakkını haiz olduğunu açıkça belirtmektedir:

"Herkes, topluluğun kültürel faaliyetine serbestçe katılmak, güzel sanatları tatmak, ilim sahasındaki ilerleyişe iştirak etmek ve bundan faydalanmak hakkını haizdir.

Herkesin yarattığı, her türlü bilim, edebiyat veya sanat eserlerinden mütevellit manevi ve maddi menfaatlerin korunmasına hakkı vardır."

Buna paralel olarak Anayasamızın 27 nci maddesinin birinci fıkrası; *"**Herkes, bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına sahiptir**"* hükmünü haizdir. İlaveten 64 üncü maddede; "*Devlet, sanat faaliyetlerini ve sanatçıyı korur.* ***Sanat eserlerinin ve sanatçının korunması****, değerlendirilmesi, desteklenmesi ve sanat sevgisinin yayılması için gereken tedbirleri alır*" denilerek eser ve eser sahiplerinin korunması hakkında devlete gerekli tedbirleri alma yükümlülüğü getirilmiştir.

Dünyada dengeli ve ulaşılabilir bir fikri mülkiyet sistemi oluşturabilmek ve yönetebilmek için oluşturulmuş uluslararası kuruluşların önde geleni Birleşmiş Milletler nezdinde teşkilatlanan 191 üye devlete sahip Dünya Fikri Mülkiyet Örgütü'dür (WIPO [World Intellectual Property Organization], 2018). Türkiye, WIPO'ya 12 Mayıs 1976'dan beri üyedir.

Bununla birlikte Dünya Ticaret Örgütü üyesi ülkelerce kabul edilen Trade-Related Aspects of Intellectual Property Rigths (TRIPS) adı verilen anlaşma da bu konuda oldukça önem taşımaktadır. TRIPS, bugüne kadar fikri mülkiyet alanında uluslararası düzeyde kabul edilen en kapsamlı anlaşma olup bu alanda diğer uluslararası anlaşmalara atıfta bulunmakla birlikte, bırakılan boşlukları da doldurma işlevi görebilecek nitelikte olması ve kapsam-yaptırım açısından daha geniş kabul edilmesi en önemli özelliğidir (Kültür Bakanlığı, 2018).

TRIPS de tıpkı ASSS gibi bir çerçeve anlaşma olup, üye ülkeler ulusal mevzuat hazırlama ve uyumlaştırma aşamasında belirli oranlarda serbestiye sahipken, kabul edilen asgari standartlara uymak zorundadır.

ASSS'nin 10 uncu maddesinde; Bern, Roma ve Wipo Telif Hakları Anlaşmaları'nda belirtilen istisnalar saklı kalmak üzere, bilgisayar sistemleri aracılığıyla ticari boyutta ve kasten gerçekleştirilen ihlallerin, ulusal yasalarda suç olarak tanımlanması için hukuki düzenlemelerin yapılması ve ihtiyaç duyulan diğer önlemlerin yerine getirilmesi gerektiği dile getirilmiştir.

Ülkemizde fikir ve sanat eserleri ile ilgili genel düzenleme 5846 sayılı *Fikir ve Sanat Eserleri Kanunu* (FSEK) olup mezkûr yasada düzenlenen cezai hükümlerin çalışmamızla ilgili olan kısımları anlatılacaktır.

4.2.1 Eser ve eser sahibinin hakları

5846 sayılı FSEK'te 1995 yılında yapılan değişiklik ile bilişim yazılımları (bilgisayar programları) da eser kavramı içerisine alınmış; buna gerekçe olarak ülkemizde hızla gelişen yazılım sektörünün ürünleri olan bilişim yazılımları üzerindeki fikri hakların FSEK tarafından açık ve net bir şekilde korunmaması gösterilmiştir (Dülger, 2015, s.749).

Bu çerçevede; her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları FSEK'in 2 nci maddesi gereği eser sayılmaktadır. Eser türleri kanun içerisinde; ilim ve edebiyat, müzik, sinema ve güzel sanat eserleri olmak üzere dört kategoriye ayrılmıştır. Bilişim yazılımları, yasaya göre ilim ve edebiyat eserleri arasında yerini almıştır.

Kanunda cezai hükümler, özellikle eser sahipleri ile bağlantılı hak sahiplerinin mali ve manevi hakları çerçevesinde toplandığından bunların belirtilmesi gerekmektedir:

Tablo 4.1 Eser Sahiplerinin Yasal Hakları

Mali Haklar	***Manevi Haklar***
İşleme Hakkı (m.21)	Umuma Arz Yetkisi (m.14)
Çoğaltma Hakkı (m.22)	Adın Belirtilmesi Yetkisi (m.15)
Yayma Hakkı (m.23)	Eserde Değişiklik Yapılmasını Yasaklama Yetkisi (m.16)
Temsil Hakkı (m.24)	
İşaret, Ses ve/veya Görüntü Nakline Yarayan Araçlarla Umuma İletim Hakkı (m.25)	Eser sahibinin zilyet ve malike karşı hakları (m.17)
Güzel Sanat Eserlerinin Satışından Pay Alma Hakkı (m.45)	

Manevi haklar eser sahibinin ekonomik olmayan hakları olarak da ifade edilebilen, sahibinin eseri ile arasındaki manevi bağı devam ettiren, herhangi bir sözleşme ile devredilemeyen, miras ile de geçişi mümkün olmayan haklardır (Uysal, 2010, s.37-38). Mali haklar ise; süre, yer ve muhteva itibariyle sınırlı veya sınırsız, karşılıklı veya karşılıksız olarak eser sahibi ya da mirasçıları tarafından başkalarına devredilebileceği gibi, sadece kullanma yetkisinin de devrinin olanaklı olduğu ekonomik özelliği daha önde olan haklardır (Akarslan, 2015, s.75). Bunun yanında eser sahibi olmasa da bunu icra eden sanatçılar, fonogram yapımcıları ve radyo-televizyon kuruluşlarının da eser sahibi ile bağlantılı hakları mevcut olup bunlar FSEK m.80'de sayılmıştır.

Eser ve bağlantılı hak sahiplerine karşı işlenen ve suç teşkil eden eylemler FSEK m.71 ve devamında tanzim edilmiştir.

4.2.2 Mali, manevi veya bağlantılı haklara tecavüz

FSEK'te koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakların ihlalini içeren durumlar 71 inci madde kapsamında aşağıdaki şekilde özetlenebilir:

- Hak sahibi kişilerin yazılı izni olmaksızın mali haklarına ve eserin değiştirilmesi hakkına zarar verilmesi ve/veya bunların her türlü ticarete konu edilmesi, depolanması, yayılması halinde fail hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur. [*Mali haklara + manevi haklardan eserin değiştirilmesi hakkına tecavüz suçu*]

- 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 yıldır ve adlî para cezası verilemez. [*Eseri haksız sahiplenme suçu-Manevi hakkın ihlali*]

- Bir eserden kaynak göstermeksizin iktibasta bulunan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır. [*İntihal suçu*]

- Hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır. [*Alenileşmemiş eserin açıklanması suçu-Manevi hak ihlali*]

- Bir eseri, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır. [*Tanınmış kişilerden haksız istifade suçu*]

Maddenin son fıkrası ile ilk fıkradaki faillere özgü olarak bu suç için özel bir ‘etkin pişmanlık hali’ öngörülmüş olup; hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişinin, **kovuşturma evresinden önce** bunları **kimden temin ettiğini bildirmek suretiyle yakalanmalarını sağladığı takdirde**, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilecektir.

4.2.3 Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri

Bir bilgisayar programının kopyalanarak hukuka aykırı olarak çoğaltılmasını önlemek amacıyla ilave programlar eklenebilmekte olup; bu şekilde ilave programlar ile korunmak istenilen bir bilgisayar programını etkisiz kılmaya yönelik program veya teknik donanımı üretmek, satışa arz etmek ya da şahsi kullanım amacı dışında elde bulundurmak suç sayılmaktadır (Karagülmez, 2014, s.177). Suçun yaptırımı FSEK'in 72 nci maddesi uyarınca altı yıldan iki yıla kadar hapis cezasıdır.

Maddenin uygulamasına rastlanmadığı ve aslen TCK'nın bilişim alanında suçlar bölümünde düzenlenmesi gerektiği yönünde görüşler mevcuttur (Dülger, 2015, s.769-770). Buna katılmak mümkündür, zira 24.03.2016 tarihinden itibaren uygulanabilir hüküm olan TCK'nın 245/A (Yasak Cihaz ve Programlar) maddesi ile aynı hukuki yarar korunmakta ve ihlal cezalandırılmaktadır. Bu nedenle FSEK'te yer alan bu cezai düzenlemenin mülga kılınmasının uygun olacağı değerlendirilmektedir.

4.2.4 Erişimin engellenmesi (Uyar-Kaldır sistemi)

FSEK, internet süjelerinin sorumluluğu konusunun yasal düzenlemeye kavuşturulmasında ülkemizde adeta öncü sayılabilecek bir rol üstlenmiş, 2004 yılında Ek-4 üncü maddesinde yapılan değişiklikle internet servis sağlayıcıları ve içerik sağlayıcılarının sorumlulukları düzenlenerek, ilk kez bu konuda bir yasal düzenleme getirilmiştir (Özen ve Baştürk, 2011, s.100) Bunun sebebinin internet ortamında kolay, hızlı ve yüksek sayıda telif hakkı ihlalinin gerçekleştirilebilmesi olduğu değerlendirilmektedir. Konuya ilişkin yasa hükmü aşağıdaki gibidir:

Ek Madde 4 – (Ek: 21/2/2001 - 4630/37 md.)
...(Değişik üçüncü fıkra: 3/3/2004-5101/25 md.) Dijital iletim de dâhil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi ***içerik sağlayıcılar tarafından*** *eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış* ***haklarının ihlâli halinde, hak sahiplerinin başvuruları üzerine ihlâle konu eserler***

***içerikten çıkarılır**. Bunun için **hakları haleldar olan** gerçek veya tüzel kişi öncelikle bilgi **içerik sağlayıcısına başvurarak üç gün içinde ihlâlin durdurulmasını ister**. **İhlâlin devamı halinde** bu defa, **Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlâle devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir**. **İhlâlin durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır**. Servis sağlayıcılar, bilgi içerik sağlayıcılarının isimlerini gösterir listeyi her ayın ilk iş günü Bakanlığa bildirir. Servis sağlayıcılar ile bilgi içerik sağlayıcıları, Bakanlıkça istendiği takdirde her türlü bilgi ve belgeyi vermekle yükümlüdür. Bu maddede belirtilen hususların uygulanmasına ilişkin usul ve esaslar Bakanlık tarafından çıkarılacak bir yönetmelikle belirlenir.*

Uyar-Kaldır sistemi olarak da adlandırılan sistem; telif hakkı ile korunan bir içeriğin, herhangi bir internet sitesinde hak sahiplerinden izinsiz olarak yer aldığının tespiti halinde, eserin hak sahipleri veya üyesi bulunduğu meslek birliklerinin, site yetkililerine uyarı göndermek suretiyle haksız içeriğin siteden kaldırılmasını yasal olarak talep etme sürecidir.

Eser üzerindeki hak sahiplerinin ilgili içerik sağlayıcısına uyarısı üzerine, haksız içeriğin siteden üç gün içerisinde kaldırılması gerekmektedir. Kaldırılmadığı takdirde, hak sahiplerinin Cumhuriyet Savcılığına başvurarak sitede yer alan haksız içeriğe erişimin engellenmesini talep edebilmeleri mümkündür. Cumhuriyet savcılığınca bu kez internet servis sağlayıcısından, içerik sağlayıcıya verilen hizmetin durdurulması istenecek ve servis sağlayıcısı da bu talebi üç gün içerisinde karşılayacaktır.

Görüldüğü üzere FSEK'te, 5651 sayılı Kanun'da olduğu gibi doğrudan bir işlem yerine kademeli bir engelleme sistemi benimsenmiştir.

Facebook, Google, Yandex, Twitter gibi kendine ait ihbar sistemi olan bazı siteler de mevcut olup, telif hakkı ihlallerinin bildiriminin öncelikle sitedeki yönergeler kapsamında takip edilerek daha kolay ve hızlı sonuç alınabileceği kanaati mevcuttur.

Mezkûr düzenleme; sadece savcının emriyle hâkim kararı olmadan erişim engelleme kararının verilebileceği, kanun yolunun öngörülmemesi sebebiyle denetiminin de yapılamayacağı gerekçeleriyle hatalı bulunmaktadır (Taşkın, 2016, s.343). Bu bağlamda, savcının kararı ile erişimin engellenmesine karar verilmesi, hızlı karar alınması açısından etkili olsa da, bu kararın tıpkı FSEK m.75'teki el koyma kararında olduğu gibi hâkim onayına sunulması ve onaylanması halinde devamı, aksi halde de derhal kaldırılması yoluna gidilmesinin yerinde olacağı, ayrıca karşı tarafa da ihtisas mahkemeleri nezdinde itiraz hakkının tanınmasının hakkaniyete daha uygun olacağı değerlendirilmektedir.

4.2.5 Soruşturma, kovuşturma ve yetkili adli merci

Her iki suçun da soruşturulması ve kovuşturulması FSEK m.75'teki açık düzenleme uyarınca şikâyete bağlıdır, re'sen yapılamaz. Aynı maddede usul hükümlerine de değinilmiş; bu çerçevede hak sahiplerinin veya üyesi oldukları meslek birliklerinin[6] haklarını kanıtlayan belge ve sair delilleri Cumhuriyet Başsavcılığına vermeleri gerektiği, aksi takdirde kovuşturmaya yer olmadığı kararı verileceği hükme bağlanmıştır. Ayrıca eser üzerinde manevi ve malî hak sahibi kişilerin şikâyet haklarını kullanabilmelerini teminen başta Millî Eğitim Bakanlığı, Kültür ve Turizm Bakanlığı yetkilileri olmak üzere ilgili gerçek ve tüzel kişiler tarafından haberdar edilmeleri de maddede düzenlenmiştir.

75 inci maddenin son fıkrasında; Cumhuriyet savcısının suç konusu eşya ile ilgili CMK hükümlerine göre el koyma tedbirine ilişkin gerekli işlemleri yapabileceği; ayrıca gerek görmesi hâlinde hukuka aykırı olarak çoğaltıldığı iddia edilen eserlerin, çoğaltılmasıyla sınırlı olarak faaliyetin durdurulmasına karar verebileceği öngörülmüştür. Faaliyetin durdurulması kararı yirmi dört saat içinde hâkimin onayına

[6] Meslek Birlikleri; fikir ve sanat eseri sahipleri ile bağlantılı hak sahiplerinin ve süreli olmayan yayınları çoğaltan veya yayanların ortak çıkarlarını korumak, kanun ile tanınmış hakların idaresini ve takibini, alınacak ücretlerin tahsilini ve hak sahiplerine dağıtımını sağlamak üzere ilgili mevzuata uygun kurulmuş birlikler olup özel hukuka tabi tüzel kişilerdir. Örnek olarak; MÜ-YAP verilebilir.

sunulmalı, hâkim tarafından da yirmi dört saat içinde onaylanmalıdır. Aksi takdirde karar hükümsüz kalır.

FSEK'in 76 ncı maddesinde ceza davalarında görevli yargı yerinin Sınai Mülkiyet Kanununun 156 ncı maddesinin birinci fıkrasında belirtilen mahkemeler olduğu düzenlenmiştir. Bu mahkemeler 'Fikri Ve Sınai Haklar Ceza Mahkemesi' olup bunların kurulmamış olduğu yerlerde bu mahkemenin görev alanına giren dava ve işlere, o yerdeki asliye ceza mahkemesince bakılacaktır.

4.3 5070 Sayılı Elektronik İmza Kanunu Düzenlemeleri

Gelişip değişen ve dinamik yapıya sahip olan teknoloji karşısında, hukuki işlemlerin elektronik yolla yapılmasına olanak sağlanması ihtiyacına binaen elektronik imza gündeme gelmiş ve AB'nin 1999/93 sayılı Direktifi model alınarak, 5070 sayılı Elektronik İmza Kanunuyla (EİK) ülkemizde uygulama alanı bulmuştur (Biçkin, 2006, s.110).

Elektronik imza, EİK'in 3 üncü maddesinde; *"başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"* şeklinde tanımlanmıştır. İzleyen maddede güvenli (nitelikli) elektronik imza da tanımlanmış ve münhasıran imza sahibine bağlı, onun tasarrufunda kullanılan, sahibinin kimliğini belirleyen, ayrıca imzalanan veride değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza olarak ifade edilmiştir.

EİK'in 8 inci maddesi uyarınca; elektronik imzalarla ilgili hizmetleri sağlayan elektronik sertifika hizmet sağlayıcıları, BTK'ya bildirimde bulunduktan iki ay sonra faaliyete geçebilir. Hizmet sağlayıcıları, güvenli ürün ve sistem kullanarak hizmetin güvenli sunulması ve sertifikaların taklit ile tahrif edilmesini önleyen tedbirleri almakla yükümlüdür. Şartları yerine getirmeyen hizmet sağlayıcıya BTK tarafından 1 ay süre verilir ve bu süre zarfında faaliyet durdurulur. Süre sonunda eksiklikler giderilmemişse hizmet sağlayıcının faaliyetine son verilir. Hizmet sağlayıcılar ayrıca

mali sorumluluk sigortası yaptırmak zorunda olup, hizmetlerinde ücret konusunda BTK'nın belirleyeceği alt ve üst sınırlarına uymakla yükümlüdürler. Kanunun 15 inci maddesi gereğince, BTK gerek duyacağı herhangi bir zamanda hizmet sağlayıcıyı denetleyebilecektir.

Elektronik imza, hukuk düzenimizde birçok alanda yenilik getirmiş ve önemli yasal niteliklerle donatılmıştır. Örneğin elektronik imzanın; 6098 sayılı Borçlar Kanunu'nda geçerli sözleşmelerin kurulmasında kullanılması, 6102 sayılı Ticaret Kanunu'nda tacirler arası bazı işlemlerin (sözleşmeden dönme, fesih ve temerrüt ihbarları) yapılabilmesi, 6100 sayılı Hukuk Muhakemeleri Kanunu'nda senetle aynı kuvvette ispat aracı olması ve aksi ispat edilmedikçe kesin delil olarak kabul edilmesi özel olarak düzenlenmiştir.

EİK'in 16 ve 17 nci maddelerinde adli suçlar yerini bulmuş olup yetkili adli mercilerce uyuşmazlık giderilecektir. Kanunun 10 ve devamı maddelerindeki aykırılıklara (kabahatler/idari suçlar) ilişkin olarak ise idari para cezaları BTK tarafından verilecektir. BTK'nın rolü burada önem arz etmekte olup EİK'in 19 uncu maddesinin ikinci fıkrası uyarınca; idari para cezasını gerektiren eylemlerin işlendikleri tarihten itibaren geriye doğru 'üç yıl içinde üçüncü kez' işlenmesi hâlinde Kurum tarafından elektronik sertifika hizmet sağlayıcısı tüzel kişinin faaliyet izninin iptaline karar verilecektir.

4.3.1 İmza oluşturma verilerinin izinsiz kullanımı

EİK'in 16 ncı maddesinde karşılığını bulan bu suçta; kişinin rızası dışında imza oluşturma aracı veya verisini elde eden, veren, kopyalayan ve yeniden oluşturanlar ile bu şekilde elde edilen imza oluşturma araçlarını kullanarak elektronik imza oluşturanlar, bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adli para cezasıyla cezalandırılabilmektedir.

Suçun sübutu için elektronik imza oluşturmak şart olmayıp, bu yönde kast yeterlidir (Orta, 2015, s.132). Yani hareketlerin e-imza oluşturmak amacıyla icra edilmesi yeterli

ve gereklidir. Bu suçun TCK. m.243/1'deki bilişim sistemine girme veya sistemde kalma suçu ile içtima halinde olması mümkündür; ancak EİK, TCK'ya göre özel yasa olduğunda çatışma durumunda özel kanun olan EİK'teki düzenlemenin uygulanması gerekecektir (Taşkın, 2008, s.143).

4.3.2 Elektronik sertifikalarda sahtekârlık

EİK'in 17 nci maddesinde düzenlendiği üzere; tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli elektronik sertifikaları taklit veya tahrif edenler ile bu türdeki sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılabilecektir.

Elektronik sertifika, kısmen ıslak imzada söz konusu olan 'imza sirküsü'ne benzetilebilecek olup bu suçta e-imzanın güvenilirliği korunmaktadır; nitekim güveli elektronik imzanın temel özelliklerinden biri de imza sahibinin kimliğini tespit eden yapıda olmasıdır (Karagülmez, 2014, s.192). Bu nedenle sahtecilik eylemine doğrudan iştirak etmese de, sertifikanın sahte yani aslında başkasına ait olduğunu bilerek kullanan kişilerin de aynı cezaya çarptırılması öngörülmüştür.

Her iki suçun da failinin elektronik sertifika hizmet sağlayıcısı çalışanları olması durumunda kişiye bağlı ağırlaştırıcı neden sebebiyle verilecek ceza yarısına kadar arttırılacaktır.

4.4 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Düzenlemeleri

İnternet süjelerinin tanımının yapıldığı, hak ve sorumluluklarının ilk kez belirlendiği, belirli suçlar bakımından erişimin engellenmesi usul ve esaslarının ilk kez düzenlendiği, internet ortamındaki bir içerik sebebiyle hakları ihlal edilen kişilere bu içeriğin yayından kaldırılmasını sağlama uygulamalarına ilk kez yer verildiği yasa olan 5651 sayılı Kanunda 'sınırlı sayıda suçla etkin mücadele' esası altında özellikle

düşünce açıklama özgürlüğünü kısıtlama bağlamında eleştirilere maruz kalmamak amacıyla kapsam kısıtlı tutulmuştur (BTK, 2007, s.8-9).

İnternet ortamında yasadışı içeriklerle ilgili 5651 sayılı yasanın;

- 8 inci maddesinde yer alan katalog suçlar,
- 8/A maddesinde millî güvenlik ve kamu düzeninin korunması,
- 9 uncu maddesinde kişilik haklarının ihlali,
- 9/A maddesinde özel hayatının gizliliğinin ihlali

durumlarında ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi tedbiri uygulanmakta olup 8 inci maddedeki katalog suçlara ilişkin hüküm ve madde 8/A düzenlemesi dışında erişimin engellenmesi kararları Erişim Sağlayıcıları Birliği tarafından yerine getirilmektedir (BTK, 2018d, s.106).

Kanunun 8/A, 9 ve 9/A maddeleri kapsamında verilecek erişimin engellenmesi kararları; ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir. Ancak, teknik olarak engellemenin yapılamadığı veya ilgili içeriğin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik (alan adından veya IP adresinden engelleme gibi) erişimin engellenmesi kararı verilebilir.

4.4.1 Katalog suçlar ve erişimin engellenmesi kararlarının hukuki niteliği

Kanunun 8 inci maddesine göre; içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesi kararı verilebilecektir:

- İntihara Yönlendirme (TCK m.84)
- Çocukların Cinsel İstismarı (TCK m.103/1, m.226/3)

- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (TCK m.190)
- Sağlık için tehlikeli madde temini (TCK m.194)
- Müstehcenlik (TCK m.226)
- Fuhuş (TCK m.227)
- Kumar oynanması için yer ve imkân sağlama (TCK m.228)
- Atatürk aleyhine işlenen suçlar (5816 sayılı Kanun hükümlerine muhalefet)

Söz konusu suçların toplumsal duyarlılığının yüksek olduğu, aile, gençler ve özellikle çocuklar gibi özel olarak korunması gerekli kesimler bakımından önem arz ettiği açıktır. Anılan suçlar, bilişim sistemleri aracılığıyla çok daha hızlı, kolay ve yaygın şekilde işlenebilmektedir.

Erişim engelleme kararı maddenin ikinci fıkrasına göre adli merciler tarafından verilmesi halinde (soruşturma evresinde hâkim-kovuşturma evresinde mahkeme), ilgili hükümde zikredildiği üzere *"koruma tedbiri"* mahiyetinde olmaktadır. Ancak Kanunun bir bilişim suçları yasası olmadığı, yeni suçlar ihdas etmeyip ceza muhakemesi ile idare hukuku hükümlerinin bir karışımını içerdiği, Kanunun aslen 8 inci maddede sayılan suçları ve etkilerini sona erdirmeyi amaçladığı dolayısıyla kararın önleyici/koruyucu tedbir değil bastırıcı/sonlandırıcı nitelik arz ettiği doktrinde ifade edilmekte olup, karara karşı herhangi bir itiraz olmaması halinde engellemenin süresiz nitelikte olduğu da ayrıca eleştirilmektedir (Canata, 2016, s.195). 6518 sayılı Kanunla 2014 yılında bu fıkraya, kararın amacı gerçekleştirecek nitelikte görülmesi halinde belirli bir süreyle sınırlı olarak verilebileceği hususu eklenerek bu tür eleştiriler aşılmaya çalışılmıştır. Maddenin onuncu fıkrasında, erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumlularının, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, adli para cezası ile cezalandırılacakları[7] düzenlenmiştir.

[7] 2014 yılında 6518 sayılı Kanun ile yapılan değişiklikten önce bu kararlara uymamanın cezası, altı aydan iki yıla kadar hapis cezası idi.

Maddenin on birinci fıkrasında ise idari tedbir olarak verilen engelleme kararlarının yerine getirilmemesinin idari para cezasına sebebiyet vereceği; bu cezanın verilmesinden itibaren yirmi dört saat içerisinde kararın yerine getirilmemesi halinde ise BTK[8] tarafından yetkilendirmenin iptal edilebileceği hükme bağlanmıştır. Anılan hükümden erişim engelleme kararının 8 inci maddenin dördüncü fıkrasına göre BTK tarafından verilmesi halinde bu kez işlemin *"idari tedbir"* adını aldığı anlaşılmaktadır. İdari tedbir olarak erişim engelleme kararı, katalog suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya yurt içinde bulunsa dahi çocukların cinsel istismarı, fuhuş ve müstehcenlik suçlarını oluşturan yayınlar bakımından re'sen Kurum Başkanı tarafından verilebilmektedir.

07.02.2018'de Resmi Gazete'de yayımlanan, 15.11.2017 tarihli ve E.2015/76, K.2017/153 sayılı Anayasa Mahkemesi kararıyla[9]; yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde, müstehcenlik suçu özelinde re'sen Kurum Başkanınca erişim engelleme kararı verilebilmesi yetkisinin iptaline karar verilmiştir. Mezkûr iptal kararı yayımından itibaren bir yıl sonra (07/02/2019) yürürlüğe girecektir.

Kurum tarafından verilen erişim engelleme kararlarının %99,76'sını; çocukların cinsel istismarı, fuhuş, müstehcenlik ile kumar oynanması için yer ve imkân sağlama suçları oluşturmaktadır[10].

4.4.1.1 Kumar oynanması için yer ve imkân sağlanması

TCK'nın 228 inci maddesinde düzenlenen bu suçta kumar, tanımlar maddesi dışında ayrı bir şekilde bu hükümde "*kazanç amacıyla icra edilen ve kâr ve zararın talihe bağlı*

[8] Genel olarak Kanun metninde yer alan ibareler bağlamında; Telekomünikasyon İletişim Başkanlığı (TİB), 17.08.2016 tarihli ve 671 sayılı KHK'nın 22 nci maddesi gereğince kapatılmış olup tüm görev ve yükümlülükleri de BTK'ya devredildiğinden, ilgili mevzuatta TİB ve TİB Başkanına yapılan atıflar "Kuruma" ve "Kurum Başkanına" yapılmış sayılmıştır.

[9] *http://www.anayasa.gov.tr/icsayfalar/basin/kararlarailiskinbasinduyurulari/genelkurul/detay/pdf/2017-153.pdf*

[10] *http://www.guvenliweb.org.tr/dosya/brEi5.pdf*

olduğu oyunlar" şeklinde ifade edilmiştir. Kumarın oynandığı mecra ayrıca belirtilmediği ve 5651 sayılı Kanunun adında 'internet ortamında yapılan' ibaresi geçtiği için geniş bir yorumla bilişim sistemlerinin (herhangi çevrimiçi bir ortamın) dâhil olduğu bir alanda kumar oynatılması da suç sayılacaktır.

Suçun bilişim sistemlerinin kullanılması suretiyle işlenmesi uygulamada oldukça sık rastlanan bir hususken, bu konu maddenin üçüncü fıkrasına 2018 yılında ancak girebilmiş ve bu hal suçun basit halinden daha ağır bir cezaya tabi tutulmuştur.

Mezkûr suçun erişim engelleme kapsamına alınması; kumar oynamaya maddi imkanı olan kimselerin diğer ülkelerde bulunan kumarhaneleri tercih ederek ekonomik girdi yaratması, vergi ödenmeksizin cep telefonlarından dahi ulaşılabilen online kumar sitelerinin öne çıkması gibi sebeplerle eleştirilmekte, belli kriterler dâhilinde suç kapsamının daraltılmasının uygun olabileceği ifade edilmektedir (Dülger, 2015, s.961).

Bununla birlikte kumar dışında; spor ve spor dışındaki hususları da içerisinde barındıran bahis (*betting*) sitelerine özellikle çocuk ve gençler nezdinde artan bir eğilim ile erişim sağlandığı görülmektedir. Özellikle erişimin engellenmesi çerçevesinin bu konuda genişletilebilmesi bağlamında, 'kumar' ibaresine ilaveten 'bahis' sitelerinin de suç kapsamına alınması gerektiği değerlendirilmektedir.

4.4.1.2 Atatürk aleyhine işlenen suçlar

Erişimin engellenmesi kapsamında TCK dışında yer alan tek eylem Atatürk aleyhine işlenen suçlar olup bu husus 5816 sayılı Yasa ile düzenlenmiştir. Bu suçlar; Atatürk'ün hatırasına alenen hakaret veya sövme ile Atatürk'ü temsil eden heykel, büst ve abidelerin veya kabrinin tahribi, kırılması, bozulması ya da kirletilmesi eylemleri olarak sayılmıştır. Bu suçlardan sadece hakaret ve sövme eylemleri internet üzerinden işlenebilecek olup diğer fiiller ancak maddi ortamda icra edilebileceğinden erişim engellemesine muhatap olamayacak ancak bunları içeren her türlü yayın engellemeye konu olabilecektir.

5651 sayılı Kanun yürürlüğü girdikten sonra ilk engelleme kararı bu suç kapsamında Ankara 11. Sulh Ceza Mahkemesi tarafından verilmiş ve Youtube sitesine erişim engellenmiş, engellemenin kaldırılmamasında ilgili şirketin gereken işbirliğini göstermemesinin etkili olduğu ileri sürülmüştür (Kaya, 2010, s.118).

4.4.1.3 İntihara yönlendirme

TCK'nın 84 üncü maddesinde; başkasını intihara azmettiren, teşvik eden, bu kararı kuvvetlendiren ya da başkasının intiharına herhangi bir şekilde yardım eden kişinin iki yıldan beş yıla kadar hapis cezası ile cezalandırılacağı; ayrıca intihar sonucunda ölüm halinde cezanın dört ila on yıl sınırına yükseltileceği düzenlenmiştir.

Maddenin üçüncü fıkrası gereği intihara 'alenen' teşvik, üç yıldan sekiz yıla kadar hapis cezasına vücut verecektir. Aynı fıkrada bu fiilin basın ve yayın yolu ile işlenmesi hâlinde, failin dört yıldan on yıla kadar hapis cezası ile cezalandırılacağı öngörülmüştür. Basın ve yayın yolu ile kavramı TCK'nın 6 ncı maddesinde "*her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar...*" şeklinde ifade edildiğinden, internet üzerinden intihara yönlendirme bu madde kapsamında değerlendirilecek ve suçun oluşumu hususunda yeterli şüphe bulunması halinde ilgili site hakkında erişimin engellenmesi yoluna gidilebilecektir.

Öte yandan intihar eğiliminde olanların bu düşüncelerden kurtulmak için interneti bir araç olarak da kullanabildiği, internette çeşitli sivil toplum örgütlerinin kişileri bu düşüncelerden kurtarmak için ücretsiz danışmanlık hizmetleri verdiği bilinmekte olup intiharla ilgili içeriğin uygun teknik kullanılmadan engellenmesinin, zaten sayıca az olan önleme çalışmalarına engel olabileceği belirtilmektedir (Kaya, 2010, s.91). Bu nedenle ilgili sitelerde intihara teşvik ile ilgili kısımların engellenmesi, intihar fikrinden uzaklaştırma ve vazgeçirme gibi amaçları bulunan yardım amaçlı sitelerin de gözetilerek erişimin engellenmesi işlemlerinde dikkatli ve özenli davranılması gerektiği değerlendirilmektedir.

4.4.1.4 Zararlı madde ve uyuşturucu temini ile kullanımı kolaylaştırma

TCK'nın 190 ıncı maddesi, uyuşturucu veya uyarıcı madde kullanımını 'alenen' özendiren veya bu nitelikte yayın yapan kişilerin cezalandırılmasını öngörmüştür. TCK m.194'te ise sağlık için tehlike oluşturabilecek maddeleri çocuklara, akıl hastalarına veya uçucu madde kullananlara 'veren veya tüketimine sunan' kişilerin cezalandırılması hükme bağlanmıştır. 194 üncü maddede 'alenen' veya 'basın ve yayın yolu ile' kavramları kullanılmamıştır. Dolayısıyla, bu tür maddelerin temini yönünde internet yayını yapılmasının TCK kapsamında suç teşkil eden bir eylem olmadığı, ancak bu yayının erişim engellenmesi kapsamında dikkate alınabileceği değerlendirilmektedir.

Sağlık için tehlikeli maddeler genel ibaresi de gerek vatandaşlar gerekse adli mercilerde görevli kişiler bakımından uygulamada karışıklık yaratabileceğinden TCK'da m. 194'te yazılı suça ilişkin olarak ilgili bu maddelerin birkaçına en azından örnekleme yöntemiyle yasada yer verilmesi 've benzeri' ifadesiyle de metnin bitirilerek, somut olayda ilgili maddenin ayrıca değerlendirilmesi kanaati mevcuttur.

4.4.1.5 Fuhuş, müstehcenlik ve çocukların cinsel istismarı

TCK'nın 227 nci maddesinde fuhuş suçuna ilişkin eylemler sıralanmış; fuhuş yapmayı kolaylaştıracak her eylem (kişi tedariki, kaçırma, nakil, barındırma vb.) ile fuhşa teşvik gibi fiillerin cezalandırılması öngörülmüştür. Madde incelendiğinde çocukların ve yetişkinlerin fuhşunun farklı cezai sonuçlara bağlandığı görülmektedir. İlk fıkra çocuklara hasredilmiş ve daha ağır müeyyideleri haiz iken, ikinci fıkra yetişkinlere ilişkin benzer hükmü daha hafif bir cezayı öngörerek düzenlemektedir.

Ceza hukukunda hazırlık hareketleri genel olarak suç teşkil etmez ancak bunun istisnaları mevcuttur. Fuhuş suçunun çocuklara karşı işlenmesi de bunlardan biri olup bu suça hazırlığın her halinin yaptırıma bağlandığı ilk fıkrada açıkça düzenlenmiştir. Bu kapsamda, çocukların fuhşa yönlendirilmesini sağlayan ikna, maddi menfaat vaadi,

zorlama gibi her türlü hazırlık eylemi cezaya muhataptır ve failin cezai sorumluluğu, suçun tamamlanmış hali ile aynı olacaktır.

Fuhşa teşvik, aracılık ve kolaylaştırma gibi fiillerin internet kanalıyla çok daha geniş kesimlere karşı ve hızlı şekilde işlenebilmesi mümkündür. Bu nedenle sayılan fiillerin internet ortamında yapılan yayınlarla icra edildiği yönünde yeterli şüphe bulunması halinde ilgili siteye erişim engellenebilecektir.

Fuhşa ilişkin eylemlerin sohbet ve sosyal ağ siteleri gibi alanlar üzerinden gerçekleştirilmesi de yaygın olup teşvik-aracılık bağlamında sitenin içerik sağlayıcısı ve diğer ilgilileri arasında bağlantı kurulması gerekmekte olduğu; nihayetinde bazı sosyal ağların milyonlarca kullanıcısı olduğu gerçeği karşısında bu tür fiiller için ilgili sitenin 'araç' olarak kullanılması sebebiyle bu sitenin cezalandırılmasının ceza sorumluluğunun şahsiliği ilkesine aykırılık teşkil edeceği ifade edilmektedir (Kaya, 2010, s.112). Ancak sosyal ağlar aleni olarak fuhuş konusunda yoğun olarak kullanılan mecralar olduğundan, bu türdeki sitelerde sorumlu olan sağlayıcıların; oto-denetim kapsamında içerik ve görsel denetleyen, fuhşa aracılık sağlayan profilleri engelleyecek aktif sistemler barındırmaları, belirli engelleme kriterlerini devreye almaları ve en önemlisi bu ağlarda gerçekleşen ihlallerin BTK'ya bildirilmesini müteakip olumlu işbirliği kurularak ivedi aksiyon almalarının önemli olduğu değerlendirilmektedir.

Müstehcenlik ise TCK'nın 226 ncı maddesinde yer almakta olup çocukların cinsel istismarını da içeren geniş bir düzenlemeyi haizdir. Hükümde müstehcen söz, yazı ve görüntülerin içeriğinin çocuklarla herhangi bir şekilde paylaşılması, çocukların girebileceği veya görebileceği alanlarda bulundurulması, özel olarak satış yapabilecek yerler dışında satışa konu edilmesi, promosyon olarak verilmesi, reklamının yapılması vb. hareketler suç sayılmıştır. Bu tür içeriklerin basın ve yayın yoluyla yayını veya buna aracılık da suçun nitelikli hali olarak öngörülmüştür.

Çocukların cinsel istismarı aslen TCK'nın 103 üncü madde ve devamında işlense de bu maddede fiilen istismar yer almaktadır. Çocukların dâhil edildiği (çocuğa genellikle direkt fiziki müdahalenin olmadığı) cinsel görüntüler ve bilişim sistemleri aracılığıyla

işlenebilecek diğer suç oluşturan eylemler ise 226 ncı maddede yerini bulmuştur. Pek tabii bu içeriklerin üretiminde çocuğa fiziki müdahalede bulunan kişiler ayrıca 103 üncü maddede yer alan ağır cezalara tabi tutulacaktır.

226 ncı maddenin üçüncü fıkrasında müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanan kişilerin cezalandırılacağı; ayrıca bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunanların da ilk cümlede yer alan eylemlerden daha hafif olmak üzere yaptırıma tabi tutulacağı hükme bağlanmıştır.

Araştırmacılar; çevrimiçi ortamda çocukların karşılaşabileceği riskleri içerik, iletişim ve yönlendirme olarak üçe ayırmakta ve buna göre bir zarar tipolojisi listesi oluşturmaktadır (Unicef, 2017, s.72):

Tablo 4.2 Çocuklar Özelinde Bilgi Teknolojileri Bağlantılı Zararların Tipolojisi

	İçerik Zararları	***İletişim Zararları***	***Yönlendirme Zararları***
Şiddet ve Saldırganlık	• Kendine zarar verme • İntihar eğilimi • Ayrımcılık • Şiddet, korku, aşırılık içeriklerine maruz kalma	• İdeolojik ikna • Nefret söylemi • Aşırılık (radikalizm)	• Siber-zorbalık, takip ve taciz • Akranlar arası şiddet ve düşmanca eylemler
Cinsel İstismar	• İstenmeyen/zararlı pornografik içeriğe maruz kalma	• Cinsel taciz • Cinsel talep/teklif/ teşvik/ayartma • İstismara zemin hazırlama	• Başka çocukların cinsel istismarı • Çocuk istismarı materyallerinin üretim ve tüketimi • Çocukların kullanıldığı uygunsuz görüntüler

Ticari Sömürü	• Gizli pazarlama (ürün yerleştirme) • Çevrimiçi kumar	• Kişisel verilerin ihlali ve uygunsuz kullanımı • Hacking faaliyetleri • Hırsızlık ve dolandırıcılık • Cinsel şantaj	• Çocukların cinsel istismarının canlı yayınlanması • Cinsel şantaj ve şantaj amaçlı ticaret/dağıtım yapma • Cinsel sömürünün seyahat ve turizm alanlarında kullanımı

- *İçerik Riskleri*: Çocuğun hoş karşılanmayan ve uygun olmayan içeriğe maruz bırakılmasıdır. Bunlar cinsel, pornografik ve şiddet görüntüleri, ırkçı, ayrımcı ya da nefret söylemleri ile anoreksiya, kendine zarar verme, intihar gibi sağlıksız ya da tehlikeli davranışları içerebilir.

- *İletişim Riskleri*: Çocuğun bir yetişkinle uygun olmayan iletişimde bulunması veya cinsel amaçlı teklif/talep alması, sağlıksız veya tehlikeli bir davranışa çekilmesi ya da ikna edilmesi gibi hususlardan oluşabilir.

- *Yönlendirme Riskleri*: Çocukların diğer çocuklara karşı nefret söyleminde bulunması, ırkçılığı teşvik etmesi, cinsel görüntüler dağıtması ve buna ilişkin materyaller üretmesi şeklinde gerçekleşebilir. Bu risk içerisinde çocuk hem mağdur hem de kendisi fail olabilmektedir.

Çocukların cinsel istismarı konusu, uluslararası sözleşme ve protokoller açısından ele alındığında; Türkiye BM Çocuk Haklarına Dair Sözleşme'yi imzalamış ve anılan sözleşme 1995 yılında yürürlüğe girerek iç hukuk normu halini almıştır. Daha sonra Çocuk Hakları Sözleşmesine eklenen ihtiyari bir protokolle, çocukların ekonomik istismardan ve çocuk açısından tehlike arz edebilecek veya çocuğun eğitimini aksatabilecek veya çocuk sağlığına; çocuğun fiziksel, zihinsel, ruhsal, ahlaki ya da sosyal gelişimine zarar verebilecek herhangi bir işte çalışmaktan korunma hakkının bulunduğu göz önünde bulundurularak: Çocukların satışı, çocuk fahişeliği ve çocuk pornografisi amacı ile yapılan kayda değer ve giderek artan uluslararası çocuk ticaretinden ciddi endişe duyulması ve çocuk pornografi ve istismarının internet ve

diğer gelişen teknolojiler üzerinde artan erişebilirliğinden endişe duyularak sözleşme çocuğun korunması ve uyumu, gelişimi hakkında özel olarak düzenleme yapılmış ve bu protokol ülkemizce 2002 yılında onaylamıştır (Akarca, 2010). Son olarak 201 sayılı Çocukların Cinsel İstismar ve Sömürüye karşı Korunmasına İlişkin Avrupa Konseyi Sözleşmesi (Lanzarote Sözleşmesi), Türkiye tarafından 7 Aralık 2011 tarihinde onaylanmış ülkemiz açısından 1 Nisan 2012 tarihinde yürürlüğe girmiştir[11].

Lanzarote Sözleşmesi'nin merkezinde çocukların korunması amacı yer almakta olup sözleşme her yönüyle çocuk haklarına saygı, çocukların esenliğinin sağlanması, görüşlerine, ihtiyaçlarına ve endişelerine cevap verilmesi ve her zaman yüksek menfaatlerine göre hareket edilmesi konularına odaklanmıştır. Nitekim sözleşmeye göre devletlerin ceza hukuku bakımından alması gereken tedbirler aşağıdaki şekilde sıralanmıştır (Çakmut Yenerer, 2016, s.38):

- Yasal olarak cinsel faaliyetlere girebilecek yaşa erişmemiş bir çocukla bu tür faaliyetlere girişmek gibi belirli davranışların ceza gerektiren suç sayılmasının sağlanması,
- Özellikle internet olmak üzere yeni teknolojiler kullanılarak çocuklara cinsel açıdan zarar verecek davranışların, örneğin çocukların kandırılmasının (cinsel amaçlı tekliflerde bulunulmasının) suç olarak kabul edilmesi,
- Etkili, orantılı ve caydırıcı bir ceza sistemini yerleştirebilmek için açık ve net ortak ölçütler geliştirilmesi,
- Çocuklara karşı işledikleri cinsel suçtan dolayı hüküm giymiş suçlular hakkındaki verilerin toplanıp saklanması.

Çalışmamızın üçüncü bölümünde yer verdiğimiz ASSS metninde de çocuk pornografisi 9 uncu maddede özel olarak yer almış; bilişim sistemleri üzerinden çocuk pornografisi üretimi, dağıtımı, sunulması, erişim sağlanması, yayılması, bulundurulması gibi eylemler yasaklanmıştır (CoE, 2001a). Eylemlerin geniş tutulmasının sebebi açıklayıcı raporda; çocuk pornografisi bulundurmanın bu tür

[11] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures

malzeme için talep canlandırması ve üretimden-bulundurmaya kadar zincirin tüm parçaları için cezai sonuçlar getirmenin, çocuk pornografisi üretimini azaltmanın etkin bir yolu olduğu şeklinde açıklanmıştır (CoE, 2001b, s.16). TCK m.226/3 ile karşılaştırıldığında ülkemiz mevzuatında da anılan eylemlerin tümünün suç olarak tanzim edildiği ve ASSS ile paralellik sağlandığı görülmektedir.

ASSS ayrıca çocuk pornografisinin ne anlama geldiği hakkında 9 uncu madde ile açık ve belirli bir tanımlamada da yapmıştır. Buna göre çocuk pornografisi aşağıdakileri içeren hususlardan oluşabilecektir (CoE, 2001a):

- Küçüğün (çocuğun) cinsel olarak müstehcen harekete katılımı,
- Küçük gibi görünen kimselerin cinsel olarak müstehcen harekete katılımı,
- Küçük veya öyle görünen kimselerin cinsel olarak müstehcen bir eyleme katıldığını gösteren gerçeğe yakın görüntüleri barındıran içerikler.

Böylece çocukların veya o algıyı yaratmaya çalışan görünürde kişilerin doğrudan dâhil oldukları cinsel davranışlar ile simülasyon veya benzeri tekniklerle gerçeğe yakın sanal tasvirler kanalıyla da çocuk pornografisinin teşviki önlenmeye çalışılmaktadır. TCK'da da bu ibareler 'çocuk', 'temsili çocuk görüntüsü' ve 'çocuk gibi görünen kişiler' şeklinde işlenmiştir.

Her ülke 'çocuk/küçük' ölçütünü kendi yasal sistemi bağlamında tanımlayacaktır. Ancak ASSS bu konuda 9 uncu maddenin üçüncü fıkrası ile 18 yaşından küçük kişilerin anlaşıldığını ancak yerel mevzuatta bu yaşın düşürülebileceğini fakat bu yaşın da 16 yaşın altında belirlenemeyeceğini belirtmiştir. Dolayısıyla sözleşmeye taraf bir ülke çocuk/küçük tanımını 16 yaşın üzerinde herhangi bir yaş olarak yerel coğrafya, kültür ve yaklaşımı ile belirleyebilecektir. Ülkemizde çocuk deyiminden ceza hukuku anlamında TCK'nın 6 ncı maddesi uyarınca '18 yaşını doldurmamış kişi' anlaşılacaktır.

4.5 Çocuklar ve Gençlerin Korunması Bakımından Siber Zorbalık

Siber zorbalık; elektronik ortamda bir birey veya grubun, başkalarına yönelik kasıtlı ve tekrarlayan aşağılama, iftira, dedikodu, nefret, taciz, tehdit, utandırma, dışlama, küçük düşürme, müstehcen içerikler yollama yoluyla, psikolojik ve sosyal yönden rahatsız edici, olumsuz davranışlarda bulunma eylemlerini ifade etmektedir (BTK, 2018d, s.155). Siber Zorbalık Araştırma Merkezi tarafından bu kavram kısaca; bilgisayar, cep telefonları ve diğer elektronik cihazlar kanalıyla kasıtlı ve tekrar eden şekilde kişilere zarar verilmesi şeklinde tanımlanmaktadır (Unicef, 2017, s.74).

Siber zorbalık; eğitim kurumları, ortak alanlar hatta kişinin kendi evinde dahi 7/24 gerçekleşebilecek olup bilgisayarlar, akıllı telefonlar ya da benzer herhangi bir elektronik cihaz ile e-posta, sms, sosyal medya mesajları/yorumları ve uygun olmayan bilgi ya da görüntülerin ifşası şeklinde ortaya çıkabilmekte, kısa süre içerisinde birçok kişiye ulaşması ile zorbalığa maruz kalan tarafından oldukça yıkıcı bir etkiye sahip olabilmektedir.

Erkek ve kız çocuklarının maruz kaldıkları zorbalık türleri genelde aynı olsa da yoğunluk dereceleri farklılık göstermektedir. Erkek çocuklar daha çok cinsel içerikli mesaj (*sexting*) veya görüntü gönderimi ya da fiziksel zarar tehditleriyle rahatsız edilirken, kız çocukları açısından erkek çocuklar için sayılanlar yanında; yalan ve dedikodu yayma, sırlarının ifşa edilmesi, grup arkadaş veya e-posta listesinden çıkarılma şeklinde zorbalık gerçekleşebilmektedir. Dijital ortamın sağladığı kolaylıkla çocuklar/gençler hızlıca rol değiştirerek siber zorba olabildikleri gibi siber zorbalığın mağduru da olabilmekte ve nihayet siber zorbalık; mağdurun depresyona girmesine, özgüvenini yitirmesine ve bunların sonucu olarak eğitime devam etmemesi gibi sonuçlara yol açabileceği gibi yıkıcı etkilerinin son noktası olarak maruz kalan kişide intihar düşüncesi dahi oluşturabilmektedir (Helpguide, 2018). Nitekim çok sayıda küçük yaşta siber zorba mağdurunun yaşamını bu nedenle sonlandırdığı bilinmektedir[12].

[12] https://nationalpost.com/news/canada/amanda-todd-suicide-2012 (2012)

2017 yılı sonunda Samsung Electronics Türkiye ve BTK işbirliğiyle siber zorbalığa karşı *"Siber Zorba Olma! #farkinavar"* hareketi başlatılmış, kampanya dâhilinde pilot 20 okul ile başlayacak eğitimlerde çocukların, gençlerin, ailelerin ve öğretmenlerin teknolojinin kötü amaçlı kullanımına karşı farkındalık ve kişilik haklarının korunması konusunda duyarlılıklarının artması hedeflenmiştir. BTK Başkanı tarafından; ülkemizde siber zorbalığa maruz kalanların oranının yüzde 20 olduğu, Amerika'da siber zorbalıkla mücadele etmek zorunda kalanların yüzde 20'sinin intiharı düşündüğünü açıkladığı beyan edilmiş, bu rakamların sadece siber zorbalığa maruz kaldığını açıklayan kişilerden oluştuğu vurgulanarak, bunu açıklamamış kişiler de göz önünde bulundurulduğunda bu oranların çok daha yükselebileceği ifade edilmiştir (Samsung, 2017). Gerçekten çalışmamızda da belirttiğimiz üzere, diğer bilişim suçlarında olduğu gibi bu uygunsuz eylemin de ihbar edilmesi konusunda özellikle çocuklar ve gençler pasif kalmakta, bu durum mağduru daha da içinden çıkılmaz bir sonuca doğru sürüklemektedir. Samsung ve BTK'nın bu ortak sosyal sorumluluk projesinde, siber zorbalığın aşağıdaki şekillerde karşımıza çıkabileceğinin altı çizilmiştir (2017):

- Mobil cihazlar aracılığı ile bireylerin görüntülerini izinsizce çekip paylaşmak,
- Sosyal ağlar ya da sohbet odaları gibi ortamlarda bireyleri aşağılayıcı, alay edici, tehditkâr, cinsel taciz veya şiddet içeren mesajlar göndermek,
- Kişisel bilgilerin rıza dışı ve habersiz sosyal medya aracılığıyla paylaşılması,
- Sosyal ağlarda birisi hakkında dedikodu yaymak,
- Bir kişiye ilişkin karalayıcı, aşağılayıcı web sayfaları hazırlamak,
- Başkası adına sahte hesap açıp, onun kimliğine bürünmek,
- Bir kişinin çevrimiçi ortamdaki tüm hesaplarını ısrarlı biçimde takibe almak,

---

https://www.nbcnews.com/news/us-news/new-jersey-family-sue-school-district-after-12-year-old-n788506 (2017)

https://edition.cnn.com/2018/01/23/us/florida-cyberstalking-charges-girl-suicide/index.html (2018)

https://www.thestar.com.my/news/regional/2018/01/11/suicide-of-australian-teen-ad-star-sparks-cyberbullying-campaign/ (2018)

- Ortak tanıdıkları etkileyerek hedef olarak seçilen bireyi arkadaş listelerinden silmelerini ve bloke etmelerini, yani sosyal olarak dışlamalarını sağlamak,

Bir araştırmaya göre Türkiye'deki ebeveynlerin %32'si çocuklarının siber zorbalık kurbanı olabileceğinden korkmakta ve %7'si çocuklarının son 12 ayda en az bir siber zorbalık olayının kurbanı olduğunu söylemekte olduğu; ayrıca araştırmayı gerçekleştiren şirketin yaptığı ankette dünya çapında her 10 çocuktan 6'sının siber zorbalık konusunda endişe duyduğu ortaya çıkarılmıştır (Kaspersky, 2017).

Siber zorbalık; istatistikler ve eylemin çocuklar ile gençler üzerinde düşünüldüğünden çok daha büyük bir etkiye sahip olması göz önüne alındığında oldukça ciddiye alınması gereken bir konudur. Siber zorbalık veya siber takip (*cyberstalking*) gibi birçok usulsüz hareketin bir arada bulunduğu özel bir suç tipi ülkemiz mevzuatında yer almamaktadır. Siber zorbalık kapsamındaki fiillerin cezalandırılması, klasik suçları düzenleyen hükümler ile karşılanabilecek olsa da sayılan yıkıcı hatta ölümcül sonuçların gerçekleşmesi ve bu suçların işlenmesinin kolaylığı karşısında, caydırıcılığın temini sebebiyle suçun işleniş biçimleri açısından yasal düzenleme yoluna gidilerek cezai sorumluluk çerçevesinin çizilmesi ve ülkemiz ilgili kamu kurumları ile özel sektör paydaşlarının bir araya geldiği projelerin arttırılarak, çalışmaların çıktılarının somut olarak izlenmesinin çocuk ve gençlerin korunması bağlamında büyük önem arz edeceği değerlendirilmektedir.

5 MUKAYESELİ HUKUKTA BİLİŞİM SUÇLARI

5.1 Genel Olarak

Bilişim suçlarının farklı ülkelerdeki hukuki altyapısının ve ne tür eylemlerin yaptırıma bağlandığının araştırılması, ülkemizin konuyla ilgili düzenlemeleri ile kıyas yapılabilmesine olanak vererek, daha etkin ve faydalı olduğu değerlendirilen hususlarda revizyona gidilmesi için gerekçeler teşkil edebilecektir.

Bilişim suçları konusunda, yasal düzenlemelere sahiplik bağlamında 95'i gelişmekte olan 138 ülke kapsamında yapılan uluslararası bir çalışmada; bu ülkelerin %72'sinin bilişim suçları hakkında yasal bir düzenlemeye sahibi olduğu (bu tür suçları yaptırıma bağlayan bir ceza yasasının veya özel bir kanunun bulunması) %27'ye tekabül eden 30'dan fazla ülkenin ise bu yönde bir hukuki düzenlemesinin bulunmadığı (%9'unun taslak düzenleme çalışmalarının devam ettiği) belirtilmektedir[13] (UNCTAD, 2018).

Çalışma kapsamında taslak dahi olsa herhangi bir mevzuat çalışması bulunmayan ve yasal düzenleme sahibi olmayan ülkeler: Libya, Afganistan, Moğolistan, Kongo, Çad, Mozambik, Honduras, Guyana, Surinam, Moritanya, Sierra Leone, Gine, Somali, Laos, Papua Yeni Gine, Eritre, Orta Afrika Cumhuriyeti şeklinde sıralanmakta olup taslak düzenlemelere başlayan ülkelerin ise genellikle Afrika kıtasında yoğunlaştığı görülmektedir (2018).

5.1.1 Amerika Birleşik Devletleri

İnternetin doğduğu yer olarak Amerika Birleşik Devletleri bugüne kadar, internet ve bilgisayar dünyasındaki her türlü gelişmeye öncülük ettiği gibi, internetin suç aracı olarak kullanılması ve bu suçların düzenlenmesi olgusunun da ilk olarak ortaya çıktığı yer olma özelliğine sahiptir (Çeken, 2004).

[13] Erişim tarihinde ilgili internet sitesinde beyan edildiği üzere, anılan çalışmadaki verilerin 01.04.2018 tarihi itibarıyla güncel olduğu belirtilmektedir.

Federal bir devlet olan ABD'de eyaletler (federe devletler) nezdinde de yasa çalışmaları yapılabilmekte ancak federal yasalar tüm devlette genel geçerli olan düzenlemeler olmaktadır. Nitekim ilk federal kanun (*Computer Fraud and Abuse Act-CFAA*) yürürlüğe girdiğinde devleti oluşturan eyaletlerin 47'siinde bilgisayar suçlarına ilişkin düzenlemeler yer almaktaydı (Erdoğan, 2012, s.57). Ayrıca; ABD, Avrupa Konseyi üyesi olmamasına rağmen ASSS'ni imzalayan ülkelerden biri olup sözleşmede sayılan yükümlülüklere tabidir.

Başlangıçta kısa ve dar ölçekli olması amaçlanan; ancak günden güne artan ve bilgisayar güvenliğini tehdit eden eylemler sonucunda CFAA Kongre tarafından 1988,1989,1990 ve 1994 yıllarında 4 kez çeşitli değiştirilmiş olup temel olarak, korumalı bir bilgisayara yetkisiz ve izinsiz erişimi yasaklamaktadır (Çeken, 2004). CFAA; bilişim suçlarına çok genel bir yaklaşım ile üç alanda düzenleme getirmektedir (Kızıltan, 2007, s.33):

- Atom enerjisi, savunma ve dış politika alanındaki gizli bilgilere, Birleşik Devletlerin zararına veya yabancı bir ülkenin faydasına olacak şekilde ulaşmak için bir bilgisayara yetkisiz olarak girmek,
- Finansal bir kurumun finans kayıtlarına veya tüketici bilgilerine ulaşmak veya bunları kullanmak amacıyla bir bilgisayara hukuka aykırı olarak girmek,
- Hükümet işlerinde kullanılan bir bilgisayara kasten girmek veya bu bilgisayardaki bilgilere erişmek veya çalışmasını engellemek veya zarar vermek veya değişiklik yapmak

Ülke açısından dikkat çeken bir başka kanun ise 11 Eylül saldırısından sonra tedbir amacıyla düzenleme alanı bulan Terörizmle Mücadele Yasası (*USA-Patriot Anti Terrorism Act*) olup bu yasayla CFAA değiştirilerek yaptırımlar daha ağır hale (15 yıla kadar veya ölüm olması durumunda müebbet hapis cezası) getirilmiş ve uluslararası hukukta ABD çıkarları aleyhinde bu suçun işlenmesi halinde Amerikan mahkemelerinin yargısal yetkisi düzenlenmiştir (Dülger, 2015, s.218). Bu yasa ile

'sanal terörizm' (*cyberterrorism*) suç tipi de ilk kez oluşturulmuş ve özellikle güvenlik hizmeti veren kamu kurumlarının bilişim sistemlerine hukuka aykırı erişimler ve bu sistemlerde bulunan verilere yönelik saldırılar suç haline getirilmiş, ayrıca sayılan fiillere teşebbüsün dahi tam işlenmiş suçtan cezalandırılacağı hükme bağlanmıştır (Çeken, 2004).

Siber terörizm tanımı yine ABD orijinli çıkmış olup 2003 yılında Kongre raporunda *"Belirli gruplar veya gizli ajanlar tarafından, şiddet odaklı olarak belli bir kitleyi etkilemek veya hükümet politikalarını değiştirmek amacıyla bilişim sistemlerinin (bilgisayarların) silah veya hedef olarak kullanılması"* şekilde ifade edilmiştir (McQuade, 2009, s.55). Bu suç tipinin failleri, belirli bilişim sistemlerine saldırı gerçekleştirerek toplumda korku-infial uyandırmak suretiyle istedikleri siyasal değişiklikleri gerçekleştirme amacını taşırlar.

Sanal terörizmde; ciddi saldırılarla kontrol ve yönetimin failin eline geçmesi söz konusu iken, devletin askeri kayıtları başta olmak üzere diğer gizli bilgileri ele geçirilebilmekte ve nihayet toplum için önemli olan ve internet ya da başka bir iletişim ağına bağlı bulunan herhangi bir sisteme saldırıda bulunulması suretiyle verilen zarar sadece sanal ortamda kalmayıp fiziksel ortama da taşınabilmektedir (Sönmez, 2018, s.37-38). Zira ulaşım, telekomünikasyon, enerji gibi büyük ölçekli sektörlerin siber terör eylemleri sonucu sekteye uğraması halinde, zararın maddi boyutu ve mağdurların sayısı oldukça yüksek olacaktır.

Türkiye'de doğrudan bu ad altında bir suç tipi yer almasa da 5651 sayılı Kanunun 8/A maddesinin erişim engelleme boyutuyla bunu karşılayabileceği düşünülmektedir. Bu suçun bilişim kanalıyla hızlı örgütlenme, kolay işlenme ve büyük zararlar yaratabilme gibi özellikleri karşısında TCK'ya aktarımı konusu ayrıca değerlendirilmelidir.

Ülkedeki bilişim suçlarının soruşturulma programı, ABD Adalet Bakanlığı nezdindeki Bilgisayar Suçları ve Fikri Haklar Bölümü (Computer Crime and Intellectual Property Section-CCIPS) tarafından yürütülmekte olup başlıca görevleri aşağıdaki gibidir (Karagülmez, 2014, s.107):

- Bilişim alanında gerçekleşen güncel olayları rapor halinde topluma sunmak,
- Bilişim suçlarıyla ilgili yasal sorunları, bu suçlarla mücadele yöntemlerini, soruşturma usulünü ve gerekli bilgileri toplumla paylaşmak,
- Bilişim suçlarının soruşturma ve kovuşturma evreleriyle ilgili yasal boşlukları tespit edip gerekli çalışmaları yapmak.

Özel sektör paydaşları, akademik kurumlar ve hükümet dışı organizasyonla ile iç içe çalışan birim, bilişim suçlarıyla mücadele kapsamında görevli olan kişilere eğitim de vermektedir. Ayrıca her sene detaylı bir sempozyum[14] düzenleyerek, sonuçlarını kamuoyu ile paylaşmaktadır.

Ülkede 2017 yılında en çok gerçekleşen üç bilişim suç tipinin; bedeli ödenen mal/hizmetin alınamaması, kişisel verilerin ihlali ve phishing olduğu görülmektedir (IC3, 2017, s.20). Sayılan ilk üç suç tipi ihbar edilenlerle sınırlı olup 140.000'in üzerinde vakaya tekabül etmektedir.

5.1.2 İngiltere

İngiltere'de bilişim suçları 29 Haziran 1990 tarihli *Computer Misuse Act* (CMA) ile düzenlenmiş olup bu kanunla yetkisiz olarak bilgisayarlara girilmesi veya değişiklik yapılması yahut benzeri müdahalelerde bulunulması önlenmeye çalışılmıştır (Erdoğan, 2012, s.58). Söz konusu kanuna daha sonra 2006 ve 2007 yıllarında sırasıyla Polis ve Adalet Yasası (*Police and Justice Act*) ve Ağır Suçlar Yasası (*Serious Crime Act 2007*) ile yeni suç tipleri de eklenmiştir (Dülger, 2017, s.171).

CMA'ya göre bir kişi, yazılım ya da verinin erişimini kontrol etmek için yetkilendirilmemiş veya bu kişi, söz konusu olan yazılım veya veriye erişmek için

[14] 2016 yılında "Sınır Aşan Boyutta Elektronik Kanıtların Elde Edilmesi Ve İşbirliği" 2017 yılında ise "Bilişim Suçlarının İstismar Ve Şiddet Yönü" başlıkları altında sempozyumlar düzenlenmiştir (*https://www.justice.gov/criminal-ccips/cybercrime-symposium*)

yetkilendirilmiş olan bir kişiden rıza almamışsa, bu erişim yetkisiz kabul edilmektedir (Dülger, 2017, s.198).

CMA'da ayrıca başka bir suçun işlenmesini sağlamak veya kolaylaştırmak amacıyla yetkisiz erişim de yasaklanmakta ve program ile verilerin yetkisiz değiştirilmesi de ayrı bir suç tipi olarak karşımıza çıkmaktadır (Ergün, 2008, s.65). Ülkemiz ceza yasasında sadece adam öldürme suçunun (TCK. m.82) da bir başka suçun icrasını kolaylaştırmak amacıyla işlenmesi ağırlaştırıcı sebep olarak sayılmış iken esasen yetkisiz erişim sonrası asıl amaçlanan başka suçların olması halinde bu durumun da ayrı bir nitelikli hal sayılmasının caydırıcı etkiye sahip olabileceği değerlendirilmektedir.

CMA'da bilgisayar, veri, program tanımlarına bilinçli olarak yer verilmemiş, değişen teknoloji karşısında bu tanımlamaların yapılmamasının uygun olduğu ve bunun her somut olayda bu kavramların yargı yerlerince yorumlanmasına izin verdiği belirtilmiştir (Apig, 2004, s.4) Bu bakış açısı ülkemiz mevzuatı açısından da geçerli olup hatta ülkemiz bir adım daha öne geçerek "bilişim sistemleri" kavramını kullanarak her yeni gelişmeyi ve aygıtı kapsayabilecek isabetli bir düzenleme yapmıştır (Dülger, 2017, s.145).

İngiliz hukukunda ayrıca müstehcenlik ve çocuk pornosu alanına ilişkin de düzenlemeler yapılmış olup 1964 tarihli Müstehcen Yayınlar Kanunu ve 1984 tarihli Telekomünikasyon Kanunu'nda yapılan değişikliklerle 'yayın' terimi kapsamına bilişim sisteminde bulunan veriler de dâhil edilerek sanal alanda yapılan pornografik yayınlar düzenlenmek istenmiştir (Dülger, 2015, s.222).

İngiltere ayrıca çocukların cinsel aktivitelere hazırlanması hususunu işaret eden "*cybergrooming*" müessesesini de yaptırıma bağlamıştır. Bu deyimde, çocuk gerçek bir mağdura dönüşmeden potansiyel kurban olarak korunmakta olup genellikle ilk adım olarak çocuğun güvenini kazanan failin ikinci adım olarak çocuğu cinsel yönden istismar etmesi söz konusu olmaktadır (Clough, 2010, s.343). Çeşitli manipülatif ya da kontrol edici tekniklerin kullanıldığı, kırılgan mağdurun tercih edildiği ve cinsel

davranışların normal gösterilmesi için güven ortamının oluşturulduğu bu suç tipi, 2003 tarihli Cinsel Suçlar Yasası (*Sexual Offences Act*) ile tanzim edilmiş olup şu hareketleri düzenlemektedir (Dülger, 2017, s.192-193):

- Fail, çocuk mağdur ile bu konu hakkında kasten görüşme sağlarsa,
- Fail ile çocuk mağdur görüşmek kastıyla dünyanın herhangi bir yerine seyahat ederse ya da dünyanın herhangi bir yerinde görüşme için ayarlama yaparsa.

Düzenlemeden ve suçun özünden anlaşıldığı üzere; bu suça hazırlık hareketlerinin cezalandırılması ile çocuk mağdurların gerçek bir istismara maruz kalmadan korunabilmesi, çocuk seks turizminin önlenebilmesi ve internet üzerinde çocuklarla girilen iletişimde gerekli özenin gösterilmesinin amaçlandığı kanaati mevcuttur.

Söz konusu davranışların (özellikle çocukların cinsel amaçlı konular için teşviki ve ikna edilmesi, bu amaçla buluşmalar vb. ayarlanması) internet kapsamında eşsiz bir anonimlik sağlanarak failin gerçek kimliğini, yaşı gibi karakteristik özelliklerini saklama imkanı vermesinden ötürü yasaklanması gerektiği 2011/92/EU sayılı AB Direktifi ile de hükme bağlanmış; gerek online gerek off-line cinsel istismara hazırlık hareketlerinin yasaklanması hususunda üye ülkelerin cezalandırma yoluna gidebileceği belirtilmiştir[15]. Çocukların korunmasına ilişkin yerel ve uluslararası sorumluluklarımız kapsamında benzer düzenlemenin ülkemiz yasalarında da yer almasının faydalı olacağı değerlendirilmektedir.

İngiltere, bilişim suçları ile mücadele etmek ve özellikle online dolandırıcılıkları ortaya çıkarmak için 2015-2016 yılı bütçesinden '250 milyon euro' ayırmış, dönemin hükümet temsilcisi de; tüketicilerin güven içinde, online ürün ve hizmet alım/satımı yapmalarını istediklerini ve bu yüzden dolandırıcı sitelerin tespitinde gerekirse fazladan bütçe kullanılabileceğini beyan etmiştir (Sönmez, 2018, s.58-59).

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093

5.1.3 Almanya

Avrupa Birliği'nin kurucu ülkelerinden olan Almanya, ülkemiz ceza düzenlemelerini de etkilemiştir. 765 sayılı ETCK İtalya model alınarak hazırlansa da; Alman Ceza Kanunu (ACK) incelendiğinde 5237 sayılı TCK ile birçok hükmünün benzerlik taşıdığı görülebilmektedir (Plagemann ve Yenisey, 2015).

Bilişim ortamlarının düzenlenmesi ile ilgili olarak Alman Hukuku'nda 2007'de yürürlükten kaldırılan Alman Tele Hizmetler Kanunu (*Teledienstegesetz*) yerine; internet haklarını belirleyen, genel olarak tüm elektronik bilgi ve iletişim hizmetleri ve sağlayıcılar için geçerli kılınan Tele Medya Kanunu (*Telemediengesetz*) yürürlüktedir (Turan, 2017, s.34).

Bununla birlikte bilişim suç ve cezalarına ilişkin genel düzenlemeler Alman Ceza Kanunu'nda yer almıştır. Ancak ACK'da, TCK'da olduğu gibi 'Bilişim Alanında Suçlar' veya benzeri bir açık bölüm/kısım altında düzenleme yoluna gidilmemiş olup ülkenin ceza yasasında yer alan bilişim suçları aşağıdaki gibi özetlenebilir (Levin ve Ilkina, 2013, s.22):

- **Madde 202a - Veri casusluğu** (*Data espionage)*: Yetkisiz erişim suretiyle failin veri elde etmesi hususu 3 yıla kadar hapis veya adli para cezası ile yaptırıma bağlanmıştır. Maddenin ikinci fıkrası 'veri' tanımını yaparak; elektronik veya manyetik ya da başka türlü doğrudan algılanabilir olmayan şekilde saklanan veya iletilen hususlar olarak belirtmiştir. Ülkemiz mevzuatında ise veriye ilişkin bu şekilde açık bir tanımlama yoluna gidilmemiştir.

- **Madde 202b - Oltalama** (*Phishing)*: Türk ceza hukukunda doğrudan bu ad altında bir suç olmasa da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen nitelikli dolandırıcılık (TCK m.158/1-f) suçu ile benzer mahiyette olduğu değerlendirilmektedir. Almanya bu konuda 2 yıla kadar hapis veya adli para cezası öngörmüş iken, ülkemiz mevzuatında benzer olan suç için 3 yıldan 10 yıla kadar hapis cezasına ilaveten adli para cezasının hükme bağlanması;

Almanya'nın bu suç konusunda ülkemizden daha esnek bir yaklaşım gösterdiğini ortaya koymaktadır.

- **Madde 202c - Veri casusluğu ve oltalama suçlarına hazırlık fiilleri** (*Acts preparatory to data espionage and phishing)*: Söz konusu düzenlemede bilişim suçlarına hazırlık hareketlerinin cezalandırılma amacı olduğu görülmektedir. Almanya bu suça ilişkin olarak 1 yıla kadar hapis veya adli para cezasını yeterli görmüştür. Ülkemizde ise 2016 değişikliği ile TCK'ya alınan "Yasak Cihaz veya Programlar" bu suçu karşılamakta olup yine ülkemiz mevzuatında bu suçun karşılığında 1 ila 3 yıl arasında hapis cezası ve ek olarak adli para cezasının belirlenmesi tespiti ile Almanya'dan daha sıkı bir cezalandırma politikası içerisinde olduğumuz söylenebilecektir.

- **Madde 202d - Çalıntı verileri alıp satma** (*Datenhehlerei*): 2015 sonunda yapılan değişiklikle ACK'ya giren bu suç; genellikle erişilebilir olmayan ve hukuka aykırı bir fiille başka birinden ele geçirilen verilerle, kendisi veya başkasına yarar sağlamak ya da diğer bir kişiyi zarara uğratmak amacıyla hareket edilmesini suç saymakta olup 3 yıla kadar hapis veya adli para cezasını öngörmektedir. Maddenin düzenlenmesindeki amacın; şahsi ya da kurumsal verilerin hukuka aykırı elde edilerek, küresel alanda menfaat karşılığı başkalarına sağlanması durumlarının korunması olduğu ile TCK m.244/1'de çalıntı verilerin sağlanması ve veri hırsızlığı hususunda hüküm kurulması yönünde çalışmaların yapılması gerektiği ifade edilmektedir (Turan, 2017, s.46).

- **Madde 303a - Yetkisiz veri değişikliği** (*unlawfully deleting, suppressing, rendering unusable or altering data*): Verinin hukuka aykırı şekilde silinmesi, yok edilmesi, değiştirilmesi ve kullanılmaz hale getirilmesini cezalandıran maddede 2 yıla kadar hapis veya adli para cezası hükme bağlanmıştır. Söz konusu hükümde bu eylemlere teşebbüsün de cezalandırılacağı açıkça ifade edilmiştir. TCK'nın aynı yönde düzenlenen 244 üncü madde hükmünde ise ceza yine Almanya'dan daha ağır olarak 1 ila 5 yıl arasında hapis olarak ele alınmıştır.

- **Madde 303b - Bilgisayar Sabotajı** (*Computer sabotage*): Hem cihazın kendisi hem depolama aygıtlarını tahrip etmek, hem de sistem üzerinde gerçekleştirilecek çeşitli fiillerle zarar verilmesini suç sayan maddede ayrı ayrı oranlarda cezalar düzenlenmiştir. Bu kapsamda; suçun temel hali 3 yıla kadar hapis veya adli para cezası sonucuna bağlanmışken bir başkasına zarar verilmesi hali 5 yıla kadar hapis veya adli para cezasına vücut vermektedir. Eğer zarar bir işletme, girişim veya kamu kurumu aleyhine oluşmuşsa veya sayılanlar aleyhine büyük oranda zarar verecek ciddi fiilleri içeriyorsa (örgütlü suçluluk hali, yüksek mali ve ticari kayıp, halkın yararlandığı temel mal ve hizmetler veya ülkenin milli güvenliğine karşı fiiller) bu kez ceza 6 aydan 10 yıla kadar hapis cezası olarak karşımıza çıkmaktadır. TCK'da ise benzer suçta nitelikli hal olarak; banka, kredi kurumu veya kamu kurum/kuruluşuna karşı işlenmesi hali düzenlenmiştir. Söz konusu fiiller bağlamında zarar gören kişi ve kurum ile zarar verilen alan-sektör ile ilgili detaylı düzenleme yapılarak 'ciddi zarar ölçütü' gözetilmek suretiyle, ülkemiz ceza yasasında da daha etkin bir yaptırım rejiminin uygulanmasının uygun olabileceği değerlendirilmektedir.

Avrupa Konseyi üyesi olan ülke, ASSS'ni imzaya açılış tarihi olan 23/11/2001 tarihinde imzalamış, Mart 2009'da onaylamış ve Temmuz 2009'da yürürlüğe koymuştur (CoE, 2018a).

Ülke mevzuatında yer verilen bilişim suçları ve karşılığında öngörülen yaptırım miktarları incelendiğinde, eylemin ve sonuçlarının ciddiyetine rağmen hafif cezai hükümlerin tatbik edildiği görülebilmektedir. Nitekim Almanya Federal Kriminal Dairesi (*Bundeskriminalamt*-BKA) Başkanı Holger Münch tarafından; organize suç örgütleri ve bilişim suçlarıyla mücadele etmek için bu tür suç faaliyetlerinin devlete ve devlet kurumlarına verebileceği büyük zararları hesaba katılarak 'daha sert' yasa düzenlemeleri yapılması gerektiği ifade edilmiştir (BKA, 2017a).

Bilişim ile ilgili konularda bütçesinde 1.6 milyar Euro ayıran Almanya'da, Savunma Bakanı Ursula von der Leyen tarafından; askeri sırlar ve bilişim silahları nedeniyle

hackerların hedefinde olan Alman ordusunun korunmasını teminen, Siber ve Bilgi Alanı Yönetimi adlı yeni bir 'bilişim ordusu' kurarak bu saldırılarla mücadele edecek bir proje geliştirildiği açıklanmış, proje kapsamında bu ünitede 13.500 kişi çalışacağı ifade edilmiştir (DW, 2017).

BKA tarafından yayınlanan 2017 yılı raporuna göre ülkede bilişim suçları kapsamındaki sayısal veriler ise aşağıdaki gibidir (BKA, 2017b):

- Doğrudan bilişim suçları 2016 yılına göre %4 artış göstererek **85.960** olarak gerçekleşmiştir.
- İnternetin 'araç' olarak kullanıldığı dolaylı bilişim suçları ise ülkedeki tüm suçların %4.4'üne tekabül etmiş ve **251.617** olarak kayda geçmiştir.
- Online bankacılık sistemine karşı **1.425** oltalama eylemi gerçekleşmiş ve her olayda ortalama **4.000 Euro** zarar gözlenmiştir.
- Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık fiillerinde 2016 yılındaki mali kayıp 50.9 milyon Euro iken, 2017 yılında bu sayı **71.4** milyona tırmanmıştır.
- Mobil cihazlar üzerinden kötücül yazılımla işlenen bilişim suçlarında **%54** artış yaşanmıştır.

5.1.4 İtalya

İtalya'da bilişim suçlarıyla mücadele edebilmek için 23 Aralık 1993 tarihli ve 547 sayılı *"Modificazioni ed integrazioni alie norme del códice pénale e del códice di procedura pénale in tema discriminalita informática"* adlı yasayla İtalyan Ceza Kanunu (İCK) ve Ceza Usul Kanunu'nda bazı değişiklikler yapılmıştır (Erdoğan, 2012, s.60).

İCK'nın revize edilen 392 nci maddesine göre zarar verilen "eşya" tanımı genişletilerek veri ve yazılımı da kapsaması sağlanmış, böylece bir yazılımı tamamen veya kısmen tahrip etmek, değiştirmek, silmek veya bilişim sisteminin işlemesini engellemek suç haline getirilmiş ve 420 nci madde ile de kamusal yararı olan bilişim sistemlerine yönelik aynı fiiller yaptırıma bağlanmıştır (Picotti, 2012).

İCK'nın 491 bis maddesiyle sahtecilik suçunun uygulama alanı genişletilerek, ispat kuvvetini haiz veri veya bilgi içeren bir dokumanın özel olarak oluşturulması yasaklanmıştır. İCK'nın 615-ter maddesi de gerek bilişim sistemine yetkisiz erişimi, gerekse sistemde haksız şekilde kalmayı cezalandırmayı öngörmekte olup ayrıca hacking araçları (*hacking tools*) denilen suçta kullanılabilecek her türlü eşyanın kullanımı, üretimi, tedariki, kabulü 615-quinquies maddesiyle suç sayılsa da 'bulundurma' (*possession*) konusunda açık bir yaptırım hükmü bulunmadığı ifade edilmiştir (Picotti, 2012). İtalya ile ülkemizdeki yetkisiz erişim suçuyla (TCK m.243) paralellik bulunsa da, TCK 245A'da yer alan yasak cihaz ve programların (hacking tools) üretimi, kabulü, tedariki, kullanımı yanında bulundurulmasının da cezalandırılması, ülkemiz ceza politikasının bu konuda daha genişletici, sıkı ve caydırıcı bir nitelik taşıdığını göstermektedir.

Küçüklerin (çocuk) pornografik materyallerde kullanımı, bunun üretimi, yayılması ve bulundurulması gibi eylemler İCK'nın 600-ter maddesi ile cezalandırılmakta ancak salt böyle bir materyale erişim yaptırıma bağlanmamaktadır (Picotti, 2012).

İCK'nın 617-quater maddesi, haberleşmenin hukuka aykırı olarak; dinlenmesi, engellenmesi veya araya girilmesiyle ilgilidir, ayrıca iletişimin içeriğinin herhangi bir kitle iletişim aracıyla ifşa edilmesi de şikâyete bağlı bir suç olarak düzenlenmiştir; ancak özel ağırlaştırıcı sebeplerin varlığı halinde re'sen kovuşturma yapılabilmekte olup bu nedenler aşağıdaki gibidir (Karagülmez, 2014, s.125):

- Suçun devlet, kamu kurumu veya kamu hizmeti gören kuruluşların kullandığı bilişim sistemi veya telematik bir sistem zararına işlenmiş olması,
- Bir kamu görevlisi veya hizmetlisinin görev ve yetkilerini kötüye kullanarak ya da sistem operatörlerinin bu sıfatlarını kötüye kullanarak suçu işlemesi,
- Özel dedektiflik yetkisinin kötüye kullanılarak işlenmesi.

İCK'ya eklenen 635 bis hükmü ile başkasının bilişim sistemini, yazılımlarını veya verilerini kısmen ya da tamamen yok etme, tahrip etme veya kullanılmaz hale getirme; 640ter maddesi ile de bilişim sistemleri aracılığıyla işlenen dolandırıcılık eylemleri suç haline getirilmiş bu suretle sistemin işleyişini değiştirerek ya da sisteme ait verilere hukuka aykırı etkide bulunarak kişinin başkası zararına, kendi veya başkası yararına haksız kazanç sağlaması yaptırıma bağlanmıştır (Dülger, 2015, s.224).

5.1.5 Japonya

Japonya'da 22 Haziran 1987 tarihli "Ceza Hukuku Alanında Bazı Hükümlerde Değişiklik Yapılmasına İlişkin Kanun" ile ceza kanununa bilişim suçları da dâhil edilmiş, 13 Şubat 2000 tarihinde yürürlüğe giren "İnternete Haksız Girmenin Yasaklanması Hakkında Kanun" ile de ceza hukuku alanında önemli düzenlemeler getirilmiştir. Japonya'da yapılan bu değişikliğin en önemli özelliği, Japon yasa koyucusunun 'suçla korunan hukuksal değeri' dikkate alarak yasal düzenlemeyi yapmasıdır (İlbaş, 2009, s.14-15).

45 sayılı Japon Ceza Kanunu'nun (JCK) 246 ncı maddesinde bilgisayar dolandırıcılığı düzenlenmiş; kendi veya üçünü kişi yararına elektromanyetik kayıtlar (belge) kapsamında yanlış bilgi vererek veya yetkisiz komut/programlara suretiyle mülkiyet hakkına tabi bir verinin kaybı, değiştirilmesi ya da üretiminin 10 yıla kadar cezaya vücut vereceği öngörülmüştür. Kanunun 234 üncü maddesinde de bilişim sistemine zarar vererek iş yapmaya engel olma fiilleri üst sınır olarak 5 yıla kadar hapis veya 1 milyon Yen para cezasına tabi tutulmuştur (JLT, 2018).

Gerek hürriyeti bağlayıcı gerekse para cezası tayininde alt sınır bulunmaması dikkat çekici olup bu durumun, uyuşmazlığı gören mahkeme hâkimine her somut olaya özel detaylı değerlendirme ve takdir hakkı tanımasına imkân sağladığı düşünülmektedir.

Japonya'da ayrıca 2000'de yürürlüğe giren 128 sayılı Bilgisayara Yetkisiz Erişim Yasası (*Act on Prohibition of Unauthorized Computer Access*) ile yetkisiz erişim fiili

suç olarak düzenlenmiş olup aşağıdaki haller (m.3) yetkisiz erişim kapsamında sayılmıştır (Karagülmez, 2014, s.138):

- Erişilmesi kontrol altında olan (sınırlandırılan) ve kişiye özel şifreyle erişim imkânı olan bilgisayara, telekomünikasyon hattı yoluyla girilmesi (sistem yöneticisi ile şifre kontrolü yapan yetkili ve ilgili diğer kişilerin fiilleri hariç),
- Girişi kontrol edebilen özel bir bilgisayardaki işlemle belli kişilerin kullanımına tahsis edilen bilgisayara, veriye (şifreyle girilenler hariç) telekomünikasyon hattı yoluyla girilmesi veya giriş kontrol fonksiyonunu kaldıracak şekilde işlem yapılması (yine yönetici ve ilgili yetkililerin eylemleri istisna tutulmuştur),
- Özel bir bilgisayarda yapılan işlemle sınırlı kişilere özgülenen ve başka bir bilgisayarla girişi kontrol edilen bilgisayarların, yetkisiz erişimle telekomünikasyon hattı yoluyla başkaları tarafından kullanılabilir hale getirilmesi.

Anılan Kanunun 4 üncü maddesiyle bir kişinin giriş kontrol fonksiyonu ile ilişkilendirilen kodlarının edinilmesi ve başkalarına verilmesi de yasaklanmış olup cezai hükümleri düzenleyen 11 vd. maddelere göre 3 üncü maddenin ihlali durumunda üç yıla kadar hapis veya azami 1 milyon Yen para cezası; 4 üncü maddeye muhalefet halinde ise bir yıla kadar hapis veya üst haddi 500 bin Yen para cezasına hükmedilmesi mümkündür (JLT, 2018).

Dijital pornografi açısından Japon Ceza Kanunu yanında 52 sayılı Çocukların Korunması ve Çocuk Fahişeliği ve Çocuk Pornografisinin Cezalandırılması Kanunu (*The Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children*) hükümleri işletilmektedir (Natsui, 2003, s.15).

Ülkede emniyet birimlerine 2012 yılında 78 bin civarında, 2017 yılında ise -bu verinin takriben iki katı- yaklaşık 130 bin bilişim suçu ihbarı yapıldığı belirtilmektedir (Statista, 2018d).

SONUÇ

Günümüzde kişilerin ve onların da üzerinde, devletlerin sahip oldukları en önemli güç 'bilgi'dir. Bilginin korunması ise hem şahsi hem de devletlerarası bir gerekliliktir. Nitekim fiziki veya askeri olarak daha güçlü olan değil, daha çok ve daha kritik veriye sahip olan tarafın galip geleceği bir çağın içinde olduğumuz açıktır. Artık sanayi devrimi, evrimini tamamlayarak yerini bilişim çağına bırakmış, bu çağ ise sanayi toplumunun bilgi toplumuna dönüşmesini sağlamıştır.

Bilişim çağı hızla gelişmekte olup, hızına yetişmek adeta bir medeniyet göstergesi haline gelmiştir. Bilgi ve iletişim teknolojileri temelinde geliştirilen bilgisayar ve benzeri işlem yapan büyük-küçük birçok cihazın, nihayetinde sayısız insana ulaşmasını mümkün kılan internetin de geliştirilmesiyle artık sistemin kullanıcısı olan hemen herkesin temas içinde olması zorunlu bir sonuç olarak karşımıza çıkmıştır.

Her ne kadar nimet olarak bahsedilebilse de; bilgi ve iletişim teknolojileri sayesinde geliştirilen cihazların, bilişim sistemlerinin ve internetin; kullanıcısı bireyler tarafından kötüye kullanılması mümkündür. Faydalı yönleriyle ele alındığında insanlığa büyük katkı sağlayabilecek teknolojik gelişmeler, kötü niyetli kişiler elinde bir silaha dönüşebilmektedir. Bu sistemlerin doğrudan veya dolaylı olarak kötüye kullanılması suretiyle meydana gelen bilişim suçları; bu suçların hızlı, kolay, zaman ve mekândan bağımsız şekilde işlenebilmesi ve tespit edilmesinin oldukça güç olması gibi sebeplerle tüm dünya ile birlikte ülkemizin de ortak bir sorunu haline gelmiştir.

Bilişim suçu tanımları çok sayıda ve farklı olsa da genel kabul gören ifade AET'nin; *"Bilgileri, otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"* tanımlamasıdır.

2018 yılına, çoğunluğu mobil abone olan 70 milyona yakın internet kullanıcısıyla giren ülkemizde kullanıcı sayısının yüksekliği, aynı zamanda bilişim suçu mağduru adaylarını da çoğaltmaktadır.

Yüksek sayıda olan bu nüfus, hemen her işinde bilgi ve iletişim teknolojilerini kullanmaktadır. Bir kişinin günlük yaşam kesitini ele aldığımızda; sabah katılacağı bir toplantının akıllı cihazı tarafından hatırlatılması, toplantıda hızla erişmesi gereken bir dokümanın bilişim sistemleri üzerinden ve hatta kullanıyorsa bulut bilişim hizmetinden faydalanılarak edinilmesi, toplantı sonuç raporunun depolama aygıtlarında tutulması yanında, gün içinde gerçekleştirmesi gereken finansal işlemlerin internet bankacılığı üzerinden yapılması, resmi işlerde kullanılması zorunlu olan bazı belgelerin e-Devlet gibi portallar üzerinden oluşturulması, sosyal medya hesapları aracılığıyla uzakta bulunan kişiler ile görüşülmesi, ihtiyaç duyulan mal/hizmete e-ticaret siteleri vasıtasıyla ulaşılması ve daha sayılamayacak kadar fazla, ancak hayatımızın her anında ve günlük olarak tekrar eden bu iş ve işlemler, aslında bilişim teknolojilerine ne kadar muhtaç olduğumuzu da ortaya koymaktadır.

Hal böyle iken, bilgi ve iletişim teknolojileri ile üretilen cihazlara ve bu cihazların fonksiyonel olarak işlem yaptığı bilişim sistemlerine karşı suç işlenmesi hali, maddi ve manevi yönden çoğu zaman telafisi mümkün olmayan zararlara yol açmaktadır.

Bilişim suçu failleri, teknolojik gelişmelere hızla adapte olarak, her geçen gün değişen ve gelişen yöntemlerle suç teşkil eden eylemleri gerçekleştirmeye devam etmektedir. Esasen teknolojinin kötüye kullanımı, yeni suç alanları ve araçlarının ortaya çıkmasının yanı sıra, fiil ve fail niteliklerini de temelden değiştirmiştir.

Bilişim suçları doğrudan ve dolaylı bilişim suçları olarak iki farklı şekilde sınıflandırılmakta ve bu tasnif Yargıtay içtihatlarında da kendini göstermektedir. Bu çerçevede, doğrudan bilişim suçları sadece TCK'da "Bilişim Alanında Suçlar" başlığı altındaki düzenlemelerden ibaret iken; dolaylı bilişim suçları, cezai hüküm içeren herhangi bir norma aykırılık teşkil edebilecek ve bilişim sistemlerinin bu suçun sadece bir unsuru olabileceği, yani bu sistemler olmaksızın da işlenebilmesi mümkün olan diğer suçları işaret etmektedir. Nitekim bilişim sistemindeki verilerin bozulması doğrudan, bilişim sistemleri kanalıyla hakaret ve tehdit eylemlerinin icrası ise dolaylı bilişim suçlarına emsal teşkil etmektedir.

Bilişim suçları başta ‘hacking’ faaliyetleri olmak üzere; DoS atakları, Truva atı saldırıları, oltalama (phishing), spam gibi sayısı ve sınırı belirlenemeyen, her geçen gün değişen ve gelişen birçok farklı yöntemle işlenebilmektedir. Faillerin amaçlarından en önde geleni maddi menfaat sağlamak iken; mağdura manevi zarar vermek, sistemi aşma becerisiyle kendini tatmin etmek hatta sadece eğlence güdüsü dahi amaç kapsamında olabilmektedir.

Failleri bilişim suçlarını işlemeye teşvik eden önemli bir husus da mağdurların çeşitli sebeplerle bu suçları ihbar etmekte çok yüksek oranda pasif kalmasıdır. Gerçek kişiler suç ihbarının nasıl yapılacağı konusunda genelde bilgisiz ve üşengeç olup yasaların ve emniyet birimlerinin işi çözemeyeceğini düşünmektedir. Diğer taraftan; tüzel kişilerin ise, suçtan zarar görmesi halinde bilişim sistemlerinin zafiyetlerinin ortaya çıkacağı düşüncesi ve hissedarlar nezdinde itibar kaybı yaşanacağı savıyla bu suçlara maruz kalındığında genellikle sessiz kalma yolu seçilmektedir. Ayrıca diğer ülkelerde de bilişim suçlarının cezalandırılmaması ‘mevzuat eksikliği’ yönünden, devletlerin kaynak ve teknoloji eksikliği sebepleri ‘gelişmişlik’ yönünden, ortak işbirliğinin sağlanmaması da ‘suç ve suçlunun takibi’ yönünden birer sorun olup, failleri bu konuda cesaretlendiren ve gizlenmelerini sağlayan diğer unsurları oluşturmaktadır.

Bilişim suçları alanında uluslararası kimliği en üst düzeyde antlaşma olan ASSS, şuan itibariyle Avrupa Konseyi üyesi ülkeler ve üye olmasalar dahi konuyla ilgili düzenlemeleri uygun bulan diğer birçok devlet tarafından uygulamaya konulmuş olan kapsayıcı bir küresel metin haline gelmiştir. İnternet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası belge niteliğini taşıyan mezkûr sözleşme, bilişim suçlarının coğrafi sınırları aştığı gerçeği ve milletlerarası bir koordinasyonun sağlanması gereği karşısında, sözleşmeye taraf devletlerin mevzuatını uyumlulaştırmayı, suç delillerinin usulünce toplanmasını ve etkin, hızlı bir uluslararası işbirliği rejimini geliştirmeyi hedeflemektedir. Anılan sözleşme, bilişim suçlarına ilişkin ‘asgari’ bir çerçeve çizmiş olup, taraf devletlerin kendi mevzuatında bu alana dair başka suçları da öngörebileceğini belirtmiştir.

Ülkemiz, bilişim suçlarıyla mücadele kapsamında gerekli ilk adımı Fransız Ceza Kanunundan esinlenerek 1991'de 765 sayılı mülga TCK'ya 525 vd. hükümlerini ekleyerek atmış, böylece ceza yasamız ilk kez bilişim suçlarıyla tanışmıştır. Mülga ceza yasasının, günümüz koşulları ve toplumun ihtiyaçları karşısında yetersiz kalması neticesinde 01/04/2015 tarihinde 5237 sayılı yeni TCK kabul edilmiştir. Yeni TCK'nın "Topluma Karşı Suçlar" üst başlığı altında 243 ila 246 ncı maddeleri arasında sayılan suç tipleri, doğrudan bilişim suçlarını oluşturmaktadır.

TCK'nın düzenlediği ilk bilişim suçu 243 üncü maddedeki bilişim sistemine girmedir. Bu suç tipi, bilişim sisteminin ve verilerin gizliliği ile güvenliğinin ihlalini korumaktadır. Bu suç yeni yasa ile ilk kez getirilmiş olup, siber suç sözleşmesi ile paralellik sağlanmıştır. Bu önemli suç tipinde bilişim sistemine salt yetkisiz erişimin sağlanması suç sayılmış, suçun oluşumu için ayrıca kullanıcıya zarar verilmesi şartı aranmamıştır. Sistemdeki verilerin değişmesi veya yok olması ise suçun ağırlaştırıcı sebebi olarak karşımıza çıkmaktadır.

Yetkisiz erişim suçunun ilk hali ile yasada; bilişim sisteminin bütünü veya bir kısmına hukuka aykırı olarak giren 've' orada kalmaya devam eden kişinin cezalandırılacağı öngörülmüştür. Her ne kadar madde gerekçesi; *"Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir"* izahatında bulunsa da, mutlak şekilde uyulması gereken suç ve cezada 'kanunilik' ilkesi, kanunun lafzında ne varsa onun uygulanmasını gerektirmektedir. Bu noktadan hareketle başlatılan doktrindeki yoğun eleştiriler sonucunda, nihayet 2016'da 've' ibaresi 'veya' ile değişerek gerek öğretideki eleştirileri gerekse yargı mercilerindeki farklı uygulamaları bertaraf edebilmiştir.

2016 yılında suçun son fıkrasına, "bilişim sistemine erişim sağlanmasa da teknik araçlarla verilerin ve veri nakillerinin izlenmesi" fiili bağımsız bir suç tipi olarak eklenmiştir. ASSS'nin 3 üncü maddesinde üye ülkeler yasadışı araya girme eylemlerini cezalandırmaya davet edildiğinden, bu değişiklik sözleşmeye uyum anlamında da olumlu bir adım olarak görülmektedir. Yeni ihdas edilen bu suçta, bilişim sistemine doğrudan erişim sağlanmasa da, örneğin bir kullanıcının sistemdeki

faaliyet dökümünün/veri trafiğinin kayda alabilecek bir yazılımla takip edilmesi gibi hususlar cezalandırılabilecektir.

TCK'da düzenlenen doğrudan bilişim suçlarından ikincisi 244 üncü maddede sayılan; sistemi engelleme, bozma verileri yok etme veya değiştirme suçudur. Söz konusu hükümle; ASSS'nin 4 üncü maddesinde yer alan *verilere müdahale* suçu ile 5 inci maddesinde tanzim edilen *sistemlere müdahale* suçu karşılanmaya çalışılmıştır.

Suçun düzenlendiği maddenin ilk fıkrası sistemin işleyişinin engellenmesi ve bozulmasını, ikinci fıkrası ise sistemde yer alan verilere ilişkin ihlalleri düzenlemektedir. Dolayısıyla ilk fıkra sistemin ana öğelerinin kullanılmaz hale getirilmesini, diğer fıkra ise sistemde yer alan ve sistemin işleyişine engel olmayacak önemdeki verilerin bozulmasını yaptırıma bağlamaktadır.

Madde ile sadece bilişim sistemi soyut olarak korunmamaktadır. Ayrıca sistem üzerinde işlem yapan cihaz veya depolama aygıtlarının fiziki varlığına müdahale edilmesi de -maddede sayılan hareketlerin sonucunun amaçlanması kaydıyla- bu suçu oluşturacaktır. Amaç cihazın fiziksel varlığının zarar görmesi ise, klasik mala zarar verme suçundan yargılama yapılabilecek, içerisindeki verilerin yok olması da aynı eylem sonucu gerçekleştiğinden fikri içtima uygulanarak en ağır suçtan ceza verme yoluna gidilebilecektir. Failin hukuki (tazminat) sorumluluğu ise devam edecektir.

Yine dünya üzerinde bir milyarın üzerinde kullanıcı sayısına sahip olması ve katma değerinin çok yüksek olması ile dikkat çeken dijital oyun sektörü, faillerin de çekim alanına girmektedir. Kullanıcıların bu oyunlara ciddi zaman ve para ayırdığı bilinmektedir. Nitekim oyun içerisindeki bir hesap ya da oyun karakterinin çalınması da Yargıtay kararlarına konu olmuş, tatbik edilecek maddenin TCK m.244'te yer alan bilişim suçu düzenlemesi olduğuna hükmedilmiştir. Bu minvalde alınan kararlar, sektörün özellikle çocuk ve genç kullanıcılarını korumak açısından önem taşımaktadır.

Bu suçun kamu kurumları ve finans kuruluşlarının bilişim sistemlerine karşı işlenmesi hali ise yasada isabetli olarak ağırlaştırıcı sebep olarak öngörülmüştür.

Mezkûr suçun son fıkrası bir başka suça vücut vermemek kaydıyla 244 üncü maddede sayılı fiillerin fail veya bir başkası adına haksız yarar sağlaması haline ilişkindir. Bu kapsamda fail, bilişim sistemi üzerinde ödemediği bir vergiyi tahsil edilmiş gibi gösterecek veri oynamalarında bulunması veya o eğitimi almamasına rağmen elektronik ortamda kendi adına sertifika üretilebilmesini sağlaması halinde bu suç tipi uygulama alanı bulabilecektir.

Bankacılık ve finans sektöründe 2018 yılı Haziran ayı itibarıyla 500 milyar TL civarında kredi trafiği seyredilmektedir. Böylesine yüksek oranda meblağın işlem gördüğü alan pek tabii faillere de çekici gelmektedir. Bu kapsamda TCK'da bilişim suçları başlığı altında son olarak "Banka veya kredi kartlarının kötüye kullanılması" suçları 245 inci maddede yerini almıştır. Bu suçlardan ilki, 'gerçek' bir kredi kartını yetkisiz kullanarak haksız çıkar sağlama; ikincisi bu kartların 'sahte' olarak üretimi, devri ve kabulü; üçüncüsü ise 'sahte' olarak üretilen kartların kullanılması suretiyle hukuka aykırı yarar sağlanmasıdır. Çalışma kapsamında da ifade edildiği üzere bu suç, bilişim suçları başlığı altında en çok işlenen tipi oluşturmaktadır.

Suçun genel karakteristiğinin bilişim alanından çok mali alana yönelik olması doktrinde yoğun olarak eleştirilmektedir. Zira suçun koruduğu yarar, genel olarak kişilerin malvarlığı değerleri üzerinde toplanmaktadır. Yargıtay da suçun malvarlığına karşı işlenen suçların özel bir şekli olduğunu ve etkin pişmanlık hükümlerinin uygulanabilir olmasının da bu sonuca ulaşmada gösterge sayılabileceğini belirtmiştir. Zira suçun düzenlendiği 245 inci maddenin son fıkrası, TCK m.168 ile öngörülen ve malvarlığına ilişkin suçlarda uygulanabilecek olan 'etkin pişmanlık' hükmüne atıfta bulunmaktadır. Ayrıca bu suç, ASSS metninde de yer alan suç tiplerinden biri değildir.

Kredi kartlarının birçok farklı yöntemle sahtesi oluşturulabilmekte olup, sahte kartlar kullanılmasa da üretimi, satımı, kabulü ve devri yasaklanmıştır. Kredi kartının sahte üretiminin banka personelini yanıltmak suretiyle gerçekleştirilmesi halinde TCK ile birlikte, BKKK'nın 37 nci maddesinin ikinci fıkrası hükmü de uygulama alanı bulacaktır. Fıkranın lafzından ve Yargıtay uygulamalarından, sahte bilgi ve belgelerle

kart üretmeye sevk eyleminde; sözleşmenin imzalanıp kartın oluşturulmasına kadar BKKK; kartın sahte üretimi aşamasından sonra ise TCK hükümlerinin uygulanabileceği sonucuna ulaşılmaktadır.

2016 yılında TCK'ya 245/A hükmü eklenerek; bir cihaz, program, şifre veya sair güvenlik kodunun bilişim alanında işlenebilen suçlarda kullanılması veya buna mahsus oluşturulması durumunda, bunları üreten, dağıtan, depolayan, satan, kabul eden ya da bulunduran kişinin cezalandırılması hükme bağlanmıştır. Böylece ASSS ile uyum sağlanmış ve 'potansiyel tehlike' taşıyan bu özel durumlar, bu alanda suç işlenmesinden önce kaynağında yasaklanmış olmaktadır. Maddede yazılı cihaz veya programlara örnek olarak şifre kırıcılar veya casus yazılımlar verilebilir.

Bilişim suçlarının işlenmesinde fail ya da mağdur olmaları ceza hukuku kuralları gereği mümkün olmayan tüzel kişilerin yararına suçun işlendiğinin sabit olması halinde, TCK'nın 60 ve 246 ncı maddeleri gereğince, varsa faaliyet izninin iptali veya müsadere tedbirlerinin uygulanması söz konusu olabilmektedir.

Edinilen güncel istatistikler analiz edildiğinde; doğrudan bilişim suçları içerisinde banka ve kredi kartlarının kötüye kullanılması suçlarının %90'ı aşan oranda işlendiği, erkek suçlu sayısının kadın suçlulara nazaran daha yüksek olduğu, suçların 18 ve hatta 15 yaş altı faillerce de işlenebildiği, yargılamalar sonucunda %75 oranında mahkûmiyet, %25 oranında da beraat kararına hükmedildiği görülmektedir.

Doğrudan bilişim suçları yanında, bilişim sistemleri aracılığıyla/kanalıyla işlenebilecek olan diğer suç tipleri 'dolaylı' bilişim suçları olarak ifade edilmektedir. Nitekim bilişim sistemlerinin sayılamayacak kadar çok alanda kullanılabilmesi, bu alanda işlenebilecek klasik suç sayısını da oldukça artmıştır. Dolaylı bilişim suçları hem TCK'da hem de bu alanda işlenebilecek suçları yaptırıma bağlayan diğer kanunlarda yer alabilmektedir. Çalışmamızda dolaylı bilişim suçlarının önemli örneklerine yer verilmiştir.

TCK'da yer alan dolaylı bilişim suçlarından öne çıkanlar, bilişim sistemlerinin kullanılması suretiyle hırsızlık ve dolandırıcılık suçlarıdır. Her iki suçta da bilişim sisteminin kullanılması suçun 'nitelikli' hali olup sonuç cezayı ağırlaştırmaktadır.

Nitelikli dolandırıcılıkta ise, hırsızlıktan farklı olarak eylemin 'hile' ile gerçekleştirilmesi söz konusudur. Sisteme veya veriye müdahale şeklindeki teknik hile, kişiye karşı yapılmadığından bu suça vücut vermez. Uygulamada en sık karşılaşılan bilişim sistemleri aracılığıyla dolandırıcılık eylemi, 'oltalama' metodunun karakteristiğini taşıyan, failin bir kişiye ait sosyal medya ya da e-posta hesabının şifrelerini ele geçirerek, kişinin yakınlarına kendisini profil sahibi gibi tanıtıp menfaat talebinde bulunmasıdır. Nitelikli dolandırıcılığı düzenleyen 158 inci madde, 2013 ve 2016 yıllarında değişikliğe uğrayarak ceza hadleri yükseltilmiştir.

Yine TCK'da yer alan önemli bir diğer dolaylı bilişim suçu ise özel hayata ve hayatın gizli alanına ilişkin suçlardır. Bu başlık altında toplanan suçlar, konusu itibarıyla esasen Anayasa ile de güvence altına alınmıştır. Bu suçlar TCK'nın 132 ve devamındaki maddelerde yer alan; haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kaydı, özel hayatın gizliliğini ihlal, kişisel verilerin kaydı, bu verilerin hukuka aykırı olarak verilmesi, ele geçirilmesi ve yok edilmesidir.

Anılan düzenlemelere göre haberleşmenin ihlali cezalandırılmakta, bu ihlal kayıt suretiyle gerçekleşirse -kayıt dinlensin veya dinlenmesin- ceza bir kat artırılmaktadır. Haberleşme içeriğinin ifşa edilmesi ise failin haberleşmenin tarafı olup olmaması ve karşı tarafın rızası olup olmadığına göre değişen aralıklarda cezaya tabi tutulmaktadır. Uygulamada genellikle boşanma ve ceza davalarında, haberleşme içerikleri hukuka aykırı olarak kaydedilmekte veya ifşa edilmektedir. Hâlbuki bu türde bir delil CMK uyarınca kanuna aykırı elde edildiğinden kullanılamayacak, ayrıca bu fiilleri işleyen kişiler ayrı bir ceza yargılamasına maruz kalabilecektir.

TCK'nın 135 ve 136 ncı maddelerinde düzenlenen kişisel verilerin ihlaline ilişkin suçlar ise sıkça işlenen ve koruduğu hukuki değer itibarıyla oldukça önem arz eden suçlardandır. Kişisel verilerin korunmasına dair Anayasanın 20 nci maddesinde genel

çerçeve belirlenmiş, uygulayıcıya yol gösteren ve bu verilerin korunmasına ilişkin usul ve esasların belirlendiği düzenleme ise 2016 tarihli ve 6698 sayılı KVKK olmuştur.

TCK, kişisel verileri hukuka aykırı işleyenler hakkında etkin bir yaptırım sistemi getirmiş olup, mezkûr hükümler konuyla ilgili AB direktifleriyle de uyum göstermektedir. KVKK da kişisel verilerin korunması bağlamında yeni yaptırımlar geliştirmemiş ve konu hakkında TCK'daki hükümlere atıfta bulunmakla yetinmiştir.

Kişisel verilerin hukuka aykırı kaydı, TCK'nın 135 inci maddesi ile suç sayılmış, özel nitelikli kişisel verilerden olan; siyasî, felsefî veya dinî görüş, ırkî köken; ahlâkî eğilim, cinsel yaşam, sağlık durumu veya sendikal bağlantı mahiyetindeki verilerin kaydında ise verilecek cezanın yarı oranında artırılacağı düzenlenmiştir.

Veri koruma hukuku uluslararası alanda da önem atfedilen bir konu olup, bu alanda birçok sözleşme ve direktif hayata geçirilmiştir. KVKK'nın hazırlanmasında esas alınan 95/46 sayılı AB direktifinin güncellenmesi ihtiyacı kapsamında 2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü (GVKT) ile bu alanda daha etkin koruma, veri işleyenlerin sorumluluğunun ve cezai sonuçların artırılması ve uygulama alanının geniş tutulması gibi önemli hususlarda köklü yenilikler getirilmiştir.

İlaveten; uluslararası düzenlemeler ile AB Adalet Divanı kararlarında sözü edilen, GVKT ile de açıkça benimsenen "Unutulma Hakkı"nın özellikle kullanıcı sayısının milyarları aştığı sosyal medya kullanıcıları bakımından önem taşıdığı değerlendirilmektedir. Bu hak kişilere, üçüncü kişiler nezdinde 'unutulmayı' isteme ve kendileri hakkında istenmeyen herhangi bir dijital verinin silinmesini talep etme imkânı vermektedir. Ülkemizde de bazı yargı kararlarında atıfta bulunulan bu hak, henüz mevzuatımızda açıkça düzenlenmemiştir.

Kişisel verilere dair suç teşkil eden eylemler, aynı zamanda kişilik hakkının ihlaline yol açtığından hukuk mahkemelerinde zararın tazmininin talep edilmesi mümkündür.

Özel hayata ve hayatın gizli alanına ilişkin suçlar başlığı altındaki eylemlerin; görevinin verdiği yetki kötüye kullanılmak suretiyle kamu görevlisi tarafından veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hâli, cezayı artıran bir sebep olarak görülmüştür. Hatta 5809 sayılı Elektronik Haberleşme Kanununda bu suçları işleyen kişinin yetkilendirilmiş işletmecilerin personeli olması halinde, yapılacak artırımın yarım yerine bir kat olarak uygulanacağı ifade edilmiş ve cezai sorumluluk isabetli olarak genişletilmiştir.

Fikri mülkiyet hakları da bilişim suçları açısından oldukça önemlidir. 5846 sayılı FSEK, fikir ve sanat eserleri ile ilgili genel düzenlemeleri içermektedir. Kanunda; her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları 'eser' sayılmaktadır.

FSEK'teki cezai hükümler genel olarak, eser sahipleri ile bağlantılı hak sahiplerinin mali ve manevi hakları çerçevesinde toplanmıştır. Buna göre, hak sahiplerinin izni olmaksızın eserin çoğaltılması, dağıtılması, değiştirilmesi, kaynak göstermeksizin iktibasta bulunulması gibi eylemler yaptırıma bağlanmıştır. Sayılan hareketlerde özellikle çoğaltım ve dağıtım, bilişim sistemleri üzerinden hızla ve kolayca gerçekleştirilebilmektedir.

İnternet ortamında kolay, hızlı ve yüksek sayıda telif hakkı ihlalinin gerçekleştirilebilmesi sebebiyle, FSEK'in Ek-4 üncü maddesi ile hukukumuza ilk kez 'erişimin engellenmesi' dâhil edilmiştir. Uyar-Kaldır olarak da adlandırılan sistem; telif hakkı ile korunan bir içeriğin, herhangi bir internet sitesinde hak sahiplerinden izinsiz olarak yer aldığının tespiti halinde, site yetkililerine uyarı gönderilmesi suretiyle haksız içeriğin siteden kaldırılması sürecini ifade etmektedir. Uyarıya rağmen içeriğin kaldırılmaması halinde, savcılığa başvuru imkânı doğacak ve savcılık talimatıyla ihlalin sona erdirilmesi yoluna gidilecektir.

Dolaylı bilişim suçlarına bir diğer örnek ise elektronik imza ile ilgili yasada yer alan cezai hükümlerdir. AB'nin 1999/93 sayılı Direktifi model alınarak ülkemizde 5070 sayılı Kanunla (EİK) ile elektronik imzaya ilişkin hükümler uygulama alanı bulmuştur.

Elektronik imza; sözleşmeler, ticari işler, bilgi-belge üretimi ve usul hukuku bağlamında önemli niteliklere sahiptir. EİK'te imzayı oluşturan verilerin yeniden oluşturulması ve izinsiz kullanımı ile sahte sertifika yapımı (taklit veya tahrif) ve bunların bilerek kullanımı suç sayılmıştır. İmza sahibinin kimliğini tespit niteliği, elektronik imzanın temel özelliklerinden biri olduğundan, sahtecilik eylemine iştirak etmese de bundar haberdar kullanıcılara da aynı ceza öngörülmüştür. Failin elektronik sertifika hizmet sağlayıcısı çalışanı olması hali de cezayı ağırlaştırıcı neden sayılmıştır.

Bu suçlar, internet ortamında yapılan yayınlar bakımından da önem taşımaktadır. Bu çerçevede, sınırlı sayıda suçla etkin mücadele esası ile katalog sekiz suçun takibini yapan 5651 sayılı Kanun; ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak erişimin engellenmesi uygulamalarına olanak tanımaktadır. Yasada tadat edilen suçlar; toplumsal duyarlılığı yüksek, özellikle çocuklar ve gençlerin korunması bakımından önemli olan müstehcenlik, fuhuş, kumar, uyuşturucu ve sağlık için tehlikeli madde kullanımı, intihara yönlendirme gibi suçlardır. Ortak bir değer olması sebebiyle, Atatürk aleyhine işlenen suçlar da kapsama alınmıştır.

Erişim engellenmesi kararları, adli merciler tarafından verilmesi durumunda 'koruma tedbiri', kurum yetkilisi (BTK Başkanı) tarafından verilmesi halinde ise 'idari tedbir' olarak adlandırılmaktadır.

Özellikle çocuklar ve gençler, internet üzerindeki yayınlar kapsamında uygunsuz içerik, yabancılarla iletişim ve yönlendirilme gibi risklere maruz kalmaktadır. Bu riskler; mağdur olan çocuğun kendisine zarar vermesi, intihar eğilimine sahip olması, ayrımcılık ve nefret söylemi ile cinsel içeriklere maruz kalması, her yönden taciz, tehdit ve şantaja uğrayabilmesi, kişisel verilerinin ele geçirilmesi, kumara yönlendirilmesi, akranları arasında şiddete başvurması gibi daha sayılamayacak birçok somut zarara uğraması sonucuna kadar gidebilmektedir.

Türkiye çocukların istismarını önlemek ve korunmalarını en üst düzeyde sağlamak amacıyla bu konuda uluslararası geçerliliği olan BM Çocuk Haklarına Dair Sözleşme

ile ihtiyari ek protokollerini imzalamış ve yürürlüğe koymuştur. Bu konuda Avrupa Konseyi'nin 201 sayılı Lanzarote Sözleşmesi de onaylanmış, AB'nin 2011/92/EU sayılı Direktifi de uyumlaştırılarak TCK ve ilgili diğer mevzuata aktarımı tamamlamıştır. Tüm bu işbirliği çalışmalarıyla çocukların; sağlık, kişisel-ruhsal-ahlaki gelişim, eğitim, ekonomi, cinsel istismar vb. yönlerden etkin korunmasının sağlanması amacıyla gerekli adımlar atılmıştır. Ülkemizin taraf olduğu ASSS'nin 9 uncu maddesinde de bilişim suçu bağlamında çocuk pornosuna ilişkin eylemler açık şekilde belirlenmiş ve sayılan hareketlerin cezaya tabi tutulması hususu işlenmiştir.

Çocuklar ve gençlerin son dönemlerde bilişim ortamında karşılaştığı bir diğer sorun olan siber zorbalığa da (*cyberbullying*) çalışmamızda değinilmiştir. Elektronik ortamda bir birey veya grubun, başkalarına yönelik kasıtlı ve tekrarlayan aşağılama, iftira, dedikodu, nefret, taciz, tehdit, utandırma, dışlama, küçük düşürme, müstehcen içerikler yollama yoluyla, psikolojik ve sosyal yönden rahatsız edici, olumsuz davranışlarda bulunma eylemleri olarak tanımlanabilen siber zorbalığın mağdurlar üzerinde yarattığı intihar eğilimiyle ölüme kadar varan yıkıcı etkileri anlatılmıştır. Konuyla ilgili olarak BTK ve ilgili özel sektör paydaşlarının kilometre taşı sayılabilecek projelerinden de bahsedilerek, bu tür çalışmaların arttırılmasının öneminden de söz edilmiştir.

Diğer ülkelerdeki olumlu uygulamaların analizinin, mevzuat değişikliği çalışmalarında ve suçun takibinde yarar sağlayacağı gözetilerek, çalışmanın son bölümünde mukayeseli hukukta bilişim suçları incelenmiş ve ülkemiz ile kıyaslanabildiği ölçüde incelenen ülkelerde faydalı görülen düzenlemelerin iktibas edilmesinin uygun olacağı yönünde değerlendirmelerde bulunulmuştur. Bu kapsamda incelenen ülkeler ABD, İngiltere, Almanya, İtalya ve Japonya olmuştur.

Bilişim suçları, ceza kanunlarında yer alabileceği gibi (örneğin Türkiye, İtalya) ceza yasası dışında diğer kanunlara cezai hükümlerin konulması suretiyle de (örneğin İngiltere) düzenlenebilmektedir. Dünya üzerinde 30'dan fazla ülkenin ise bilişim suçlarını cezalandırabilecek bir yasal düzenlemeye sahip olmadığı tespit edilmiştir.

ÖNERİLER

Bilişim dünyasında yüzde yüz güvenlik sağlamanın mümkün olmadığı konusunda mutabakat olsa da gerçek ve tüzel kişi kullanıcılar tarafından alınacak önlemlerle bilişim suçlarından korunabilmek olanaklıdır.

Bu kapsamda; bilişim suçlarının güncel işlenme yöntemleri takip edilerek, önemli verileri ihtiva eden cihaz ve yazılımların güçlü şifreler ve koruma programlarıyla güvenli tutulması gerekmektedir. Yine, kişisel ve mali verilerle ilgili işlemlerin herkese açık ağlardan yapılmaması, şahsi her bilginin sosyal medya hesaplarında paylaşılmaması ve ilgili kurumlarca gerçekleştirilen eğitim/farkındalık çalışmalarına katılım sağlanmasında fayda görülmektedir.

Çalışmamızda bahsedildiği üzere; suçların bildirilmesindeki pasif tavır da suçu arttıran bir unsur olduğundan, ihbar ve adli mercilere intikal konusunda mağdurların aktif yaklaşımı önem arz etmektedir. Zararlı içerik ve bilişim suçları kapsamında, bunların ihbar edilebilmesini teminen Bilgi Teknolojileri ve İletişim Kurumu ve Emniyet Genel Müdürlüğü'nün ilgili internet siteleri[16] kullanılmalıdır.

Ayrıca; adli takibatta ilk muhatap alınacak kişinin abone olması gerçeği karşısında, cihaz ve ağ şifrelerinin paylaşımı hususunda da azami dikkatin gösterilmesi elzemdir.

Çocuk ve gençlerin bilişim suçlarından korunması bağlamında da dijital dünyada geçirilen vaktin nitelik ve nicelik açısından denetlenmesi oldukça önemlidir. Ayrıca kişisel verilerin önemi ve paylaşımındaki sakıncaları hakkında gerekli uyarılar yapılmalıdır. İlaveten küçükleri cinsel içeriğe, şiddete, ayrımcılığa maruz bırakan; intihara, başkalarına zarar vermeye, eğitimini aksatmaya yönlendiren dijital oyunlar (örneğin Mavi Balina, Momo, Mariam vb.) başta olmak üzere her türlü içerik/uygulamanın kullanımı engellenmelidir.

[16] *https://www.ihbarweb.org.tr/ - https://www.egm.gov.tr/sayfalar/ihbar.aspx*

Bilişim ve iletişim alanında faaliyet gösteren işletmecilerce talep halinde ücretsiz olarak sağlanan ve etkin koruma örnekleri bulunan "filtreleme" yöntemlerinden[17] faydalanılması da, çocuk ve gençlerin maruz kalabileceği zararlı içeriklerden korunması açısından fayda sağlayacaktır.

Bilişim suçları konusunda BTK başta olmak üzere ilgili kamu kurum ve kuruluşları ile özel sektör aktörlerinin de etkin işbirliği ve koordinasyon içerisinde tedbirler alması elzemdir. Bu bağlamda;

- Eğitim ve bilinçlendirme çalışmaları ile farkındalık yaratılması;

    - Bu tür çalışmalar toplumun her kesimine, hedef kitlenin eğitim-kültür düzeyine göre ayrıştırma yapılarak süreklilik arz edecek şekilde sunulmalıdır. Çocuk ve gençlerin korunması özelinde; ebeveynler, eğitim kurumları, sivil toplum kuruluşlarının da dâhil edildiği eğitimler düzenlenmelidir.

    - Uygulayıcı kamu ve özel sektör personeli ile yargı mensuplarına ayrıntılı teknik ve hukuki eğitimler verilmeli, uygulamalı pratik çalışmalar üzerinden somut olay örnekleri analiz edilmeye çalışılmalıdır.

    - Üniversitelerin mühendislik ve hukuk fakülteleri başta olmak üzere, bilişim hukuku ve bilişim suçları alanında gerekli teknik ve hukuki kazanımları içeren dersleri müfredata eklemeleri ve ayrıca yüksek lisans-doktora programlarına da dâhil etmeleri oldukça faydalı görülmektedir.

    - Bilişim yoluyla işlenen suçlar açısından, sms, radyo ve televizyonlarda kamu spotları ile kamuya açık alanlarda afiş, poster vb. ile halkın bilinçlendirilmesi özellikle önem taşımaktadır.

[17] *http://www.guvenliweb.org.tr/dokuman-detay/ebeveyn-denetim-araclari*

- Güncel sorunlar saptanarak, teknolojinin gelişim hızının gerisinde kalınmaksızın çözümler üretilmesi için ilgili paydaşlarla hızlı ve işbirliği halinde faaliyet gösterilmesi elzemdir.

- Kritik görev ifa eden kamu kurumlarının bilişim sistemlerindeki zayıf noktaları belirleyebilecek zafiyet testlerini kısa aralıklarla uygulamaları ve gerekli önlemleri almaları, sistemde bulunan önemli verilerin korunması açısından ehemmiyet teşkil etmektedir.

- Bilişim suçlarının uluslararası kimliği öne çıkmakta olduğundan, devletlerarası yardımlaşma ve işbirliğinin bu suçlarla mücadelede en önemli unsurlardan biri olduğu kabul edilmektedir. Bu kapsamda konuyla ilgili sözleşme ve ek protokollerinin gecikmeksizin yürürlüğe konması ve diğer ülkelerle diplomatik ilişkilerin olumlu devam etmesine azami özen gösterilmesi gelişme sağlayacaktır.

Çalışma konumuza ilişkin olarak değinilen ve uygulanmasının faydalı olacağı değerlendirilen mevzuat önerileri aşağıda sunulmaktadır;

- Bilişim suçları klasik suçlardan birçok yönden (işleyiş, fail ve mağdur tipolojisi, suçla verilen maddi ve manevi zararın hızla ve yaygın nitelikte olması, delil toplama ve ayrıştırma vb.) ayrılmaktadır. Bu alanda fikri mülkiyet uyuşmazlıklarına özel olarak geliştirilen Fikri ve Sınai Haklar Mahkemesi modeli örnek alınarak yeni bir yasal düzenleme ile "*Bilişim Ceza Mahkemeleri*" (BCM) kurulması önerilmekte olup, konuya dair ilk uygulamada dikkate alınması gerektiği değerlendirilen hususlar ve öngörülen faydalar aşağıdaki gibidir:

  ⇨ BCM'lerin kanun gücünde bir düzenleme ile Adalet Bakanlığı'nca istatistikler analiz edilerek, suç yoğunluğunun tespit edildiği pilot şehirlerde başlatılarak ülke geneline yayılması,

⇨ Uygulamada birliğin sağlanması ve içtihat farklılıklarının önüne geçilebilmesini teminen BCM kararlarının temyizi bakımından Yargıtay'da belirlenen tek bir ceza dairesinin görevli kılınması,

⇨ BCM'lerde görev alacak personelin bilişim hukuku alanında eğitimli ve donanımlı personel arasından seçilmesine dikkat edilerek, yurt içi ve yurt dışı yoğun eğitimlerle bu yöndeki yeteneklerinin artırılması ve benzer yöndeki eğitimlere ilgili emniyet mensuplarının da dâhil edilmesi; daha sonra ABD'deki CCIPS yapılanmasında olduğu gibi her yıl bilişim suçları ile ilgili ayrı ve detaylı bir başlıkta sempozyumlar düzenlenmesi,

⇨ İhbarların değerlendirilmesi ve ilk incelemelerin yapılıp adli mercilere sevki açısından Emniyet Genel Müdürlüğü, erişimin engellenmesi hususu başta olmak üzere 5651 sayılı Kanunla verilen yetkilerin ifası bakımından Bilgi Teknolojileri ve İletişim Kurumu, ASSS kapsamında uluslararası işbirliği için ülkemizce belirlenen makamın bu işleri koordine edebilmesi için Adalet Bakanlığı tarafından belirlenecek yeterli sayıda yetkin personelin BCM'ler nezdinde özel ofislerinin (irtibat büroları) bulundurulması ve bu suretle hızlı-gizli-önemli işlerin takibinde sorunların aşılması ve adliye personelinin ilgili kişilerle birebir görüşme olanağının sağlanması,

⇨ Üçer aylık dönemler itibarıyla konuyla ilgili tüm istatistiklerin (suç tipi, fail ve mağdur özellikleri, kullanılan yöntem, lokasyon, tahmini maddi zarar, mahkûmiyet türü, ne kadar sürede sonuçlandığı vb.) ve sonuç analizlerinin yer aldığı raporların kamuoyu ve ilgili kurumlarla paylaşılması,

⇨ Bilişim suçları ve bilişim aracılığıyla işlenebilecek suçlar kapsamında mevzuat çalışmalarına ilgili kamu kurumlarıyla birlikte katılım sağlanarak, uygulamada yaşanan sorunların dile getirilmesi suretiyle, mevzuat düzenlemelerinin teknolojinin gelişim hızına yetişebilmesinin sağlanması,

⇨ Modelin uygulanmasında olumlu çıktılar alınması halinde ceza yargılaması dışında, bu tür suçlarda kişisel ve mali verilerin de zarar gördüğü gözetilerek

tazminat, haksız fiil, haksız rekabet, sebepsiz zenginleşme vb. yöndeki hukuki taleplerin çözülebilmesini teminen Bilişim Hukuk Mahkemeleri'nin de kurularak BCM'ler ile aynı yapı içerisinde geliştirilmesi.

- BM'nin 2017 tarihli bir raporunda ülkemizin en yüksek sayıda göç alan ilk 5 ülke arasına girdiği görülmektedir. Bu kapsamda ASSS'nin bilişim sistemleri aracılığıyla işlenen ırkçı ve yabancı düşmanı eylemlere karşı ek protokolü imzalansa da (19.04.2016) yürürlüğe konup iç hukukumuza aktarılması için gerekli çalışmaların yapılmasının yerinde olacağı kanaati mevcuttur.

- 5237 sayılı TCK'da yapılması gerektiği değerlendirilen değişikliklere aşağıda yer verilmektedir:

  ∑ Bilişim alanındaki suçlar, bireysel olarak ya da büyük çaplı saldırıların gerçekleştirilmesi ve maddi menfaatler edinilmesi kapsamında birden fazla kişi ile hatta örgüt faaliyeti kapsamında da işlenebilmektedir. Sayılan hallerin suçun 'nitelikli' hali sayılarak cezayı ağırlaştırıcı sebep olarak kabul edilmesi caydırıcılık sağlayabilecektir. Bu kapsamda yasa metnine; *"birden fazla kişi veya örgüt faaliyeti kapsamında işlenmesi halinde verilecek ceza yarı oranında artırılarak hükmolunur"* cümlesinin eklenmesi önerilmektedir.

  ∑ Bu alanda işlenen suçlarda elektronik delillerin verilerin kaybolma tehlikesinin bertaraf edilebilmesini teminen CMK'nın "Bilgisayarda arama, kopyalama ve el koyma" tedbirini düzenleyen 134 üncü hükmüne *"5237 sayılı Türk Ceza Kanunu'nun Bilişim Alanında Suçlar başlıklı Onuncu Bölümü'nde işlenen suçlar çerçevesinde bu tedbirlere* ***derhal*** *başvurulur"* cümlesinin eklenmesi ve madde kenar başlığındaki 'Bilgisayarda' ibaresi yerine de 'Bilişim sistemlerinde' kavramının kullanılmasının uygun olacağı düşünülmektedir.

  ∑ 244 üncü maddede yer alan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunda fiillerin; bir banka veya kredi kurumu ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi durumu ağırlaştırılmış hal

olarak düzenlenmiştir. İlaveten bu yerlerde görev yapan banka görevlisi veya kamu personelinin güvenlik unsurlarını aşması gerekmeksizin suçta sayılan sistem ve verilere kolayca erişip suçu işleyebilmesinin mümkün olması ve kendilerine duyulan güveni ihlal etme ve özellikle sahip oldukları görevle bağdaşmayacak bu hareketlerinin daha ağır cezai sonuçlara bağlanması kapsamında üçüncü fıkranın devamında; *"Sayılan yapılarda görevli personel tarafından işlenmesi halinde verilecek ceza yarı oranında artırılır"* cümlesinin ilave edilmesi, amaçlanan nitelikli halin pekiştirilmesini sağlayacaktır. Benzer düzenleme İtalya'da da mevcuttur. Ayrıca aynı madde kapsamında sisteme erişimi tamamen engelleyen veya verileri bozan kişinin bu eylemlerinin telafisi olmayan (geri döndürülemez) zarara yol açması halinde verilecek cezanın örneğin *iki yıldan az olamaz* şeklinde yükseltilmesi, sistem için önemsiz bir veriyi bozan kişi ile çok daha ağır bir sonuca sebebiyet veren kişinin aynı cezaya muhatap olmasını engelleyebilecektir.

∑ Banka ve kredi kartlarının kötüye kullanılması suçunun bilişim alanında işlenen suçlar başlığı altında yer alması konusundaki katıldığımız doktrindeki eleştirilere ilaveten, Yargıtay da bu suçun malvarlığına karşı işlenen suçların özel bir şekli olduğunu ifade etmektedir. Ayrıca ASSS'de bu eylemler bilişim suçu kapsamında sayılmamaktadır. Hâlihazırda bilişim sistemlerindeki verilerin değiştirilmesi, nakli ve bundan yarar sağlanması, somut olaya göre doğrudan bilişi suçları veya bilişim sistemleri aracılığıyla hırsızlık ya da dolandırıcılık suçlarına dair hükümler ile karşılanabilmektedir. Sonuç olarak, bu suçun TCK'nın 'malvarlığına ilişkin suçlar' kısmına alınmasının sistematik açıdan yerinde olacağı değerlendirilmektedir.

∑ 245 inci madde kapsamında TCK'dan daha yeni düzenleme olan BKKK'da 'kart hamili' ibaresi tercih edildiğinden, olası bir değişiklik çalışmasında TCK'da da 'kart sahibi' yerine kart hamili kavramının kullanılması yerinde olacaktır. Ayrıca bu suça ilişkin şahsi cezasızlık sebeplerinde 'eşlerden biri' ifadesinden önce gelmek üzere "*aralarında boşanma davası dâhil, adli merciler nezdinde herhangi uyuşmazlığın bulunmadığı*" kısmının eklenmesi; yine şahsi cezasızlık sebeplerinde, kayın hısımları her türlü cezadan bağışık tutulmuşken, kardeşlere bu cezasızlık sebebinden faydalanabilmesi için aynı evde yaşamak şartı getirilmesinin

hakkaniyete uygun olmadığı değerlendirildiğinden, bu şartın kardeşler açısından kaldırılması yerinde görülmektedir.

∑ Çalışmada yer verilen istatistikler tetkik edildiğinde, banka ve kredi kartlarının kötüye kullanılmasının oldukça yoğun işlenen bir suç olduğu karşımıza çıkmaktadır. Bu kapsamda ilgili kamu kurumları (BDDK, BTK, Hazine ve Maliye Bakanlığı, Ticaret Bakanlığı vb.) ile özel sektör paydaşlarının (Türkiye Bankacılar Birliği, Tüketici Dernekleri vb.) bir araya gelerek, kullanıcı güvenliği konusunda teknik ve hukuki çalışmaları gerçekleştirmesinin (3D Secure gibi kademeli ödeme sistemlerinin yaygınlaştırılması, e-ticaret sitelerinin yetkilendirilmesi, mobil cihazlar aracılığıyla finansal işlemlerin icrası için güvenli yazılımlar geliştirilmesi vs.) suçla mücadelede büyük fayda sağlayacağı değerlendirilmektedir.

∑ Bilişim alanında suçlar bölümünde sayılan suçlarda, hapis cezasına ek olarak hükmedilmesi öngörülen adli para cezası hadlerinin, hürriyeti bağlayıcı ceza ile uyumlu halde olması beklenmektedir. Örneğin alt sınırı en az üç yıldan başlayan banka ve kredi kartlarının kötüye kullanılması suçunda, hapis cezası yanında hükmedilecek adli para cezasının üst sınırı yüksek (5000 güne kadar) tutulsa da, bir alt sınır öngörülmediğinden yasa uygulaması gereği 100 TL ile bu cezanın ifa edilebilmesi mümkün olabilmektedir. Bu çerçevede, hâkimlerin yeterli gerekçe sunmaksızın ceza alt sınırından ayrılmasının Yargıtay tarafından bozma sebebi yapıldığı gerçeği karşısında, bu suçlarda hapis cezasına ilaveten hükmedilecek tüm adli para cezalarına uygun bir alt sınır belirlenmesi (örneğin '*alt sınırı yüz günden aşağı olmamak üzere*' gibi) hakkaniyete uygun olacaktır.

∑ Haberleşmenin gizliliğini yaptırıma bağlayan 132 nci maddenin son fıkrası, haberleşme içeriğini basın ve yayın yoluyla ifşa etmenin 'aynı' suça vücut vereceğini düzenlemektedir. Ancak basın ve yayın yoluyla işlenen fiiller TCK'da genelde ağırlaştırıcı sebep sayılmakta ve haberleşme içeriği gibi önemli ve gizli kalması gereken bir hususunun bu yolla ifşa edilmesinin aynı cezaya tabi tutulması hakkaniyete uygun düşmemektedir. Ayrıca aynı cezaya hükmolunacak bir halin kanunda tekrarlanmasının da bir işlerliği bulunmamaktadır. Sayılan sebeplerle

suçun basın ve yayın yoluyla işlenmesi halinde, cezanın yarı veya üçte bir oranında artırılması yönünde bir hüküm eklenmesinin gerekli olduğu kanaati mevcuttur.

∑ Toplumda büyük infial yaratabilecek ve meşru siyasal otoriteyi de sarsma hatta yok etme gücü bulunan, özellikle temel yararlanılan hizmetlerden telekomünikasyon, enerji, savunma, ulaşım, sağlık gibi büyük ölçekli sektörlerin de sıkça hedef alındığı 'siber terörizm' eylemleri/saldırıları çerçevesinde, ABD ve Almanya örnekleri incelenerek, bu konuda ivedi olarak yüksek hadli/caydırıcı yaptırımların öngörülmesi gerektiği değerlendirilmektedir.

∑ Özellikle çocuk ve gençleri hedef alması, ciddi yıkıcı sonuçlara sebebiyet vermesi sebepleriyle, bilişim sistemleri kullanılarak gerçekleştirilen zorbalık (*cyberbullying*) eylemlerinin TCK veya 5651 sayılı Kanun ile suç kapsamına alınarak, caydırıcı cezaların belirlenmesi gerektiği değerlendirilmektedir.

TCK dışında çalışma konusu suç türlerine ilişkin hüküm içeren diğer yasalarda yapılması gerektiği düşünülen revizyon çalışmaları aşağıda sıralanmaktadır:

- AB'nin uygulamalarında uzun süredir kabul gören ve Genel Veri Koruma Tüzüğü ile de yasal metin olarak uluslararası düzenlemelerde yer bulan "Unutulma Hakkı" (*Right to be Forgotten / Right to Erasure*), her ne kadar Anayasa Mahkemesi ve Yargıtay'ın bazı kararlarında olumlu atıflar yapılsa da, ülkemiz mevzuatında açık tanınmış bir hak değildir. Gerek kişisel hakları doğrudan ilgilendirmesi, gerekse uluslararası düzenlemelerle paralellik sağlanması açısından anılan hakkın KVKK veya 5651 sayılı Kanun'a dâhil edilmesinin uygun olacağı görüşümüz mevcuttur.

- 5846 sayılı FSEK'in Ek-4 üncü maddesi gereğince telif hakkı ile korunan bir içeriğin, herhangi bir internet sitesinde hak sahiplerinden izinsiz olarak yer aldığının tespiti halinde işletilebilecek olan "Uyar-Kaldır" sisteminde uyarıya rağmen içeriğin kaldırılmaması halinde Cumhuriyet Savcısı sürece dâhil olmakta; ancak bu karar hâkim onayına sunulmamakta ve karşı tarafa herhangi bir itiraz hakkı tanınmamaktadır. Anılan düzenlemede verilen savcılık kararının hâkim

onayına sunulması, 24 saat geçmesine rağmen onaylanmayan kararın kendiliğinden hükümsüz kalması ve kararda karşı tarafa süresi ile mercii açıkça bildirilen itiraz yolunun tanınmasının yerinde olacağı değerlendirilmektedir.

- Kumar oynanması için yer ve imkân sağlanması suçunun ayrıca bir erişim engelleme sebebi teşkil etmesinden ötürü; genelde yurtdışına yönelim ile ülke dışına ekonomik girdi sağlandığı ve cep telefonlarından dahi ulaşılabilen kumar ve bahis sitelerinin öne çıktığı gözlemlenmektedir. Bu nedenle bu eylemin işlenmesinin belli yaş, maddi tavan oranları, işletilecek yer ruhsatı vb. şekillerde tekrar ele alınmasının uygun olabileceği düşünülmektedir. Ayrıca 5651 sayılı Kanun incelendiğinde kumar dışında özellikle 'bahis' konusunda idari tedbir olarak erişimin engellenmesi kararı verilemeyeceği değerlendirilmektedir. Bahis (*betting*) sitelerinin hızla artması ve kolay ulaşılabilir olması nedenleriyle kapsama alınmasının gerekli olduğu düşünülmektedir.

- İntihara yönlendirme ve uyuşturucu kullanımını kolaylaştırma suçları bakımından internette çeşitli sivil toplum örgütlerince kişileri bu düşüncelerden kurtarmak için ücretsiz danışmanlık hizmetleri verdiği bilinmektedir. Bu çerçevede erişim engelleme kararı verilirken, ilgili içeriğin uygun teknik kullanılmadan engellenmesinin, zaten sayıca az olan önleme çalışmalarına engel olabileceği; bu nedenle otomatik engelleme sistemleri yerine her bir web sitesinin münferit olarak engellenmesinin faydalı olacağı kanaati mevcuttur.

- KVKK'da kişisel verilerin ihlaline ilişkin suçlarda TCK'ya atıf yapılmaktadır. AB Genel Veri Koruma Tüzüğü ile de bu tür ihlallerin yüksek hadlerle yaptırımlara bağlandığı bilinmektedir. Bu nedenle KVKK'da yapılması düşünülen ilk değişiklik çalışmasında, uluslararası gelişmelerin de gözetilerek, kişisel verilerin ihlalinde verilebilecek idari ve adli cezalar çerçevesinde detaylı bir çalışma yapılması ve bunun yasaya aktarılmasının yararlı olacağı düşünülmektedir.

- 5651 sayılı Kanuna 2015 yılında eklenen ve milli güvenlik gibi çok önemli bir alanda erişimin engellenmesi yetkisi tanıyan 8/A maddesinin üçüncü fıkrasında, önce ihlalin gerçekleştiği kısmın engellenmesi (URL vb. şekilde) uygulaması öne

çıkarılmıştır. Kanun 2007 yılında çıkmasına rağmen bu önemli değişiklik 2015 yılında gerçekleşmiş ve Anayasa Mahkemesi bu durumun gerisinde kalan 8 inci maddede tadil yapılmadığına refleks göstererek, Kanunda yeknesaklık sağlanması amacıyla 8 inci maddeye yönelik yürütülen bir davada iptal kararı vermiştir. İptalin gerekçesi; müstehcenlik oluşturan yayınlara re'sen erişim konusunda belirlilik ilkesinin ihlal edildiği ve kademeli bir sistemin uygulanmadığıdır. İptal hükmü 1 yıl sonra yürürlüğe girecek olup gelinen noktada BTK tarafından yeni bir düzenleme yapılmadığı takdirde, 07/02/2019 tarihinde Türkiye'de müstehcenlik suçunun internet ortamında işlenmesi halinde re'sen erişimin engellenmesi mümkün olmayacaktır. Bu kapsamda maddenin yeniden düzenlenmesi kapsamında dördüncü fıkrasının son cümlesine aşağıdaki şekilde ekleme yapılmasının sorunu çözebileceği değerlendirilmektedir:

- *Bu fıkra kapsamında verilen erişimin engellenmesi kararı, içeriğe erişimin engellenmesi yöntemiyle (URL, vb. şeklinde) verilir. Ancak, teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir. Kurum başkanında bu fıkraya göre verilecek re'sen erişim engelleme kararları, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi hâlde, karar kendiliğinden kalkar.*

Bilişim çağının yaşandığı günümüzde, bu alanda işlenebilecek suçların yöntem ve sayısı durmaksızın artmaktadır. Artık sadece bilgisayarlar değil, akıllı telefonlar, avuç içi cihazlar, giyilebilir ekipmanlar ve hatta son dönemlerde konuşulan yapay zekâ teknolojisi ile dünyamız çevrelenmektedir. Bu kapsamda; tekil kullanıcıların şahsi, kamu ve özel sektörün ise kurumsal olarak gerekli her türlü tedbiri almaları, gelişmeleri yakından izlemeleri ve en nihayetinde suçla mücadelede yerel ve ulusal mevzuatın takip edilerek geliştirilmesinin kritik önemi haiz olduğu değerlendirilmektedir.

KAYNAKLAR

AÇIKGÜL Hacı Ali, 2007, Kredi Kartı Sözleşmeleri, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk (Medeni Hukuk) Anabilim Dalı

ADALET BAKANLIĞI, 2005, Türk Ceza Kanunu Gerekçesi, *http://www.ceza-bb.adalet.gov.tr/* (Erişim Tarihi: 11.03.2018)

ADALET BAKANLIĞI, 2018, Adli Sicil ve İstatistik Genel Müdürlüğü, *http://www.adlisicil.adalet.gov.tr/Istatistikler/1996/2017TckAcilanDavaSucVeSanikSayisi.pdf*
http://www.adlisicil.adalet.gov.tr/Istatistikler/1996/2017TckUyarincaKararaBaglananDavalardakiSucVeKararSayilari.pdf (Erişim Tarihi: 13.08.2018)

AKARCA Mehmet, 2010, Çocukların Ceza Hukukundaki Yeri ve Korunması, Yüksek Yargı Kurumlarının Avrupa Standartları Bakımından Rollerinin Güçlendirme Projesi Sunumları,
http://www.anayasa.gov.tr/files/insan_haklari_mahkemesi/sunumlar/ym_4/Akarca.pdf (Erişim Tarihi: 29.08.2018)

AKARSLAN Hüseyin, 2015, Bilişim Suçları, Seçkin Yayıncılık, Ankara

AKBULUT BOZDOĞAN Berrin, 2001, Türk Ceza Kanunu'nun 525a, 525b, 525c Maddeleri ile 1997 Tasarısının Karşılaştırılması, Panel - Bilişim Suçları, T.C. Adalet Bakanlığı Hâkim ve Savcı Adayları Eğitim Merkezi Başkanlığı, Ankara

AKBULUT Berrin, 2016, Sistemi Engelleme Bozma Verileri Yok Etme Veya Değiştirme, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 24, Sayı: 2

AKINTÜRK Turgut, 2006, Türk Medeni Hukuku - İkinci Cilt - Aile Hukuku, Beta Yayıncılık

ANAYASA MAHKEMESİ, 2016, Unutulma Hakkına İlişkin Basın Duyurusu, *http://www.anayasa.gov.tr/icsayfalar/basin/kararlarailiskinbasinduyurulari/bireselbasvuru/detay/94.html* (Erişim Tarihi: 18.08.2018)

APAYDIN Cengiz, 2017a, Bilişim Suçları ve Bilişim Ceza Hukuku, Acar Matbaacılık (Yazarın Kendi Yayını), İstanbul

APAYDIN Cengiz, 2017b, Başkalarına Ait Banka Hesaplarıyla İlişkilendirilerek Sahte Banka veya Kredi Kartını Üretmek Satmak Devretmek Satın Almak veya Kabul Etmek, Terazi Hukuk Dergisi, Sayı: 127 (s.44-56)

APIG, 2004, Revision of the Computer Misuse Act: Report of an Inquiry by the All Party Internet Group, *https://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf*, (Erişim Tarihi: 03.09.2018)

ARTUK Mehmet Emin, GÖKÇEN Ahmet, YENİDÜNYA Ahmet Caner, 2014, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara

AVCI Mehmet, 2004, Türk Ceza Kanunu, TC Tasarıları ve Özellikle 2004 TCK Tasarısı'nın Genel Olarak Değerlendirilmesi, Türk Ceza Kanunu Reformu: İkinci Kitap: Makaleler, Görüşler, Raporlar, Türkiye Barolar Birliği, Ankara

AVRUPA KOMİSYONU, 2018, AB Genişleme Politikasına İlişkin 2018 Bilgilendirmesi Ekindeki Komisyon Çalışma Dokümanı – 2018 Türkiye Raporu

AVŞAR Zakir, ÖNGÖREN Gürsel, 2010, Bilişim Hukuku, Türkiye Bankalar Birliği Yayınları (Yayın No: 270), İstanbul

AYDIN Murat, 2013, Ceza Muhakemesinde Yetki ve Görev Meselesinde Bazı Sorunlara İlişkin Değerlendirmeler, Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, C.3, S.1 (s.29-60)

AYÖZGER Çiğdem, 2016, Kişisel Verilerin Korunması – Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dâhil, Beta Yayıncılık, İstanbul

BAŞBÜYÜK İsa, 2010, Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılmasıyla İşlenmesi, Ceza Hukuku Dergisi, Yıl: 5, Sayı: 14, Seçkin Yayıncılık

BBC, 2017, "5 soruda Türkiye'yi de etkileyen fidye yazılımı 'WannaCry'" *https://www.bbc.com/turkce/haberler-39906717* (Erişim Tarihi: 23.04.2018)

BBC, 2018, Gaming Addiction Classified as Disorder by WHO, *https://www.bbc.com/news/technology-42541404* (Erişim Tarihi: 28.07.2018)

BDDK, 2018, Türk Bankacılık Sektörü Temel Göstergeleri, *https://www.bddk.org.tr/WebSitesi/turkce/Istatistiki_Veriler/TBSGG/dosyaTbs/veri_0014_37.pdf* (Erişim Tarihi: 29.07.2018)

BİÇKİN İnci, 2006, Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler, Türkiye Barolar Birliği Dergisi, Sayı: 63 (s.109-126)

BİKİRLİ Yükselen Alper, 2015, 5237 Sayılı Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları, Power Point Sunusu, Türkiye Adalet Akademisi, http://www.taa.gov.tr/indir/alper-yukselen-bikirli-yargitay-8-ceza-dairesi-uyesi-c2F5ZmF8MWM1YmEtNTVkNzQtYjNiNjgtZGFhNWUucHB0eHwyMTg/ (Erişim Tarihi: 22.07.2018)

BİLGEN Tülay, 2010, Türk Ceza Kanununda Banka Veya Kredi Kartlarının Kötüye Kullanılması, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Programı

BKA, 2017a, Interview: "Wir brauchen mehr Strafanzeigen", *https://www.bka.de/DE/Presse/Interviews/2017/170420_InterviewMuenchGDV.html*

BKA, 2017b, Bundeskriminalamt - Bundeslagebild Cybercrime 2017, *https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html*

BKM, 2018, Pos-Atm-Kart Sayıları, *https://bkm.com.tr/pos-atm-kart-sayilari/*; İnternetten Yapılan Kartlı Ödeme İşlemleri, *https://bkm.com.tr/internetten-yapilan-kartli-odeme-islemleri/* (Erişim Tarihi: 31.08.2018)

BM, 2017, International Migration Report, United Nations, *http://www.un.org/en/development/desa/population/migration/publications/migrationreport/docs/MigrationReport2017_Highlights.pdf* Department of Econonomic and Social Affairs, New York

BM, 2013, Comprehensive Study on Cybercrime, United Nations Office On Drugs And Crime, New York, *http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf*

BOĞA Uğur, 2011, Bilişim Suçlarıyla Mücadele Yöntemleri, Radyo ve Televizyon Üst Kurulu (RTÜK) Uzmanlık Tezi, Ankara

BTK, 2007, 5651 Sayılı Kanun Kapsamında İnternet Aktörleri (Kitapçık)

BTK, 2016a, *http://internet.btk.gov.tr/internetin-getirdigi-firsat-ve-faydalar-detay-60.html* (Erişim Tarihi: 07.03.2018)

BTK, 2016b, *http://internet.btk.gov.tr/internetin-riskleri-ve-zararlari-detay-61.html* (Erişim Tarihi: 07.03.2018)

BTK, 2016c, *http://internet.btk.gov.tr/turkiye-de-bilisim-hukuku-detay-70.html* (Erişim Tarihi: 14.05.2018)

BTK, 2018a, Pazar Verileri Raporu (2017/4. Çeyrek), *https://www.btk.gov.tr/uploads/pages/2017-q4.pdf* (Erişim Tarihi: 10.03.2018)

BTK, 2018b, Siber Güvenlik Zirvesi (10 Nisan 2018), *https://btk.gov.tr/haberler/siber-dunyada-en-zayif-halka-kadar-gucluyuz* (Erişim Tarihi: 21.04.2018)

BTK, 2018c, Phishing (Şifre Çalma) Nedir, *https://tuketici.btk.gov.tr/tr-TR/Sik-Sorulan-Sorular/Guvenli-Internet* (Erişim Tarihi: 22.04.2018)

BTK, 2018ç, 1 Milyarın Üzerinde İnsan Dijital Oyun Oynuyor, *https://www.btk.gov.tr/haberler/1-milyarin-uzerinde-insan-dijital-oyun-oynuyor* (Erişim Tarihi: 28.07.2018)

BTK, 2018d, Bilgi Teknolojileri ve İnternetin Bilinçli Güvenli Kullanımı, İnternet Daire Başkanlığı, *http://www.guvenliweb.org.tr/dokuman-detay/bilgi-teknolojileri-ve-internetin-bilincli-guvenli-kullanimi-kitabi* (Erişim Tarihi: 29.08.2018)

BTK-BilgiZone, 2018a, Türkiye'de İnternetin Tarihçesi ve Gelişimi, *https://bilgi.zone/turkiyede-internetin-tarihi/* (Erişim Tarihi: 18.04.2018)

BTK-BilgiZone, 2018b, Dijital Dünyada 60 Saniyede Gerçekleşen İşlem Sayıları, *https://bilgi.zone/dijital-dunyada-60-saniye/* (Erişim Tarihi: 24.03.2018)

BTK-BilgiZone, 2018c, Dijital Oyunların 6 Zararı, *https://bilgi.zone/dijital-oyunlarin-6-zarari/* (Erişim Tarihi: 28.07.2018)

CANATA Fatih, 2016, 5651 Sayılı Kanun Kapsamında İnternet Düzenlemeleri ve Düşünce-İfade Özgürlüğü Üzerine Bir Değerlendirme, Türk Kütüphaneciliği, Cilt: 30, Sayı: 2 (s.185-205)

CLOUGH Jonathan, 2010, Principles of Cybercrime, Cambridge University Press

CORPUS, 2018, Corpus Web Mevzuat ve İçtihat Programı, CD Medya Yazılım ve İçerik Geliştirme

CoE (Council Of Europe), 2001a, Convention on Cybercrime, European Treaty Series – No. 185, Budapeşte

CoE, 2001b, Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapeşte, *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b* (Erişim Tarihi: 11.05.2018)

CoE, 2018a, Chart of signatures and ratifications of Treaty 185, *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=3v48WmgI* (Erişim Tarihi: 27.04.2018)

CoE, 2018b, https://www.coe.int/en/web/cybercrime/tcy, (Erişim Tarihi: 17.07.2018)

CoE, 2018c, Cybercrime Convention Committee (T-CY) - Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, *https://rm.coe.int/t-cy-2018-23-protoprov-draft-public-text-v1/16808c498f*, (Erişim Tarihi: 17.07.2018)

CoE, 2018ç, Towards a Protocol to the Budapest Convention: Further Consultations, *https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-budapest-convention-further-consultations*, (Erişim Tarihi: 17.07.2018)

CYBERMAG, 2017, Siber Güvenlik Dergisi, Yerel Süreli Yayın, Dumat Ofset Matbaacılık Ltd. Şti., Ankara

CYBERMAG, 2018, "Yılın En Popüler Siber Suçu: Cryptojacking", *https://www.cybermagonline.com/yilin-en-populer-siber-sucu-cryptojacking* (Erişim Tarihi: 22.06.2018)

ÇAKMUT YENERER Özlem, 2016, Cinsel Şiddet Mağduru Çocuk Kavramı ve Türk Ceza Kanunu'nun Çocuğa Yönelik Cinsel Şiddet Düzenlemelerine Genel Bakış, T.C. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt: 22 Sayı: 1 (s.35-51)

ÇAM Ali Rıza, 2015, Adli Kolluk ve Bilişim, On İki Levha Yayıncılık, Yayın No: 556, İstanbul

ÇARKACIOĞLU Abdurrahman, 2016, Kripto Para Bitcoin, Araştırma Raporu, Sermaye Piyasası Kurulu – Araştırma Dairesi

ÇEKEN Hüseyin, 2004, Amerika Birleşik Devletlerinde Siber Suçlar, *http://archiv.jura.uni-saarland.de/turkish/HCeken.html* (Erişim Tarihi: 03.09.2018)

ÇEKİÇ, Burak, 2006, İnternet Aracılığı ile İşlenen Suçlar, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Anabilim Dalı, Kamu Hukuku Bilim Dalı, İstanbul

DEĞİRMENCİ Olgun, 2005, 2004 Türk Ceza Kanunu'nun Bilişim Suçları Açısından Değerlendirilmesi, Türkiye Barolar Birliği Dergisi, Sayı: 58

DEĞİRMENCİ Olgun, 2014, Ceza Hukukunda Yanılma Kavramı ve Hukuka Uygunluk Nedenlerinde Yanılma, Türkiye Barolar Birliği Dergisi, Sayı: 110

DEIBERT Ronald, PALFREY John, ROHOZINSKI Rafal, ZITTRAIN Jonathan, 2008, Access Denied: The Practice and Policy of Global Internet Filtering, The MIT Press, Massachusetts

DEMİR Ömer, ARIÇ Mehmet, POLAT Halil, 2015, Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar, Adalet Yayınevi, Ankara

DIŞİŞLERİ BAKANLIĞI, 2018, Avrupa Konseyi - Uluslararası Örgüt Künyesi, *"http://www.mfa.gov.tr/avrupa-konseyi_.tr.mfa"* (Erişim Tarihi: 10.05.2018)

DOĞAN Koray, 2010, Neticesi Sebebiyle Ağırlaşmış Suç, Doktora Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı

DOĞAN Ramazan, 2014, 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Adalet Yayınevi, Ankara

DOĞU Ali Haydar, 2016, Bilişim Hukuku - Bilgi ve İletişim, Ekin Basım Yayın Dağıtım, Bursa

DÜLGER Murat Volkan, 2005, 5237 Sayılı YTCK'da Kastın Unsurları ve Türleri - Özellikle Olası Kastın Değerlendirilmesi, Hukuk ve Adalet Eleştirel Hukuk Dergisi, Yıl: 2 Sayı: 5

DÜLGER Murat Volkan, 2014, Suçların Birleşmesine İlişkin Tanımlar - Sorunlar ve Çözüm Önerileri, Leges Ceza Hukuku Dergisi. Yıl: 1, Sayı: 1 (s.4-87)

DÜLGER Murat Volkan, 2015, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara

DÜLGER Murat Volkan, 2016, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, Sayı: 3 (2), Güz (s.101-167)

DÜLGER Murat Volkan, 2017, Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması, Türkiye Adalet Akademisi Dergisi, Yıl: 8, Sayı: 31 (s.141-258)

DW, 2017, German Army Launches New Cyber Command, *https://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517* (Erişim Tarihi: 01.09.2018)

EBEM Şeriban, 2013, Kamu Bilişim Sistemleri Açısından Bulut Bilişimin Teknik, Yönetim ve Hukuki Boyutlarıyla İncelenmesi: Bilgi Teknolojileri ve İletişim Kurumu İçin Öneriler, Teknik Uzmanlık Tezi, Ankara

EKER Umut Ö., 2006, Türk Ceza Hukukunda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu, Türkiye Barolar Birliği Dergisi (Sayı 62)

ENCYCLOPAEDIA BRITANNICA, 2018, *www.britannica.com/topic/modus-operandi* (Erişim Tarihi: 19/04/2018)

ERCAN İsmail, 2008, Ceza Hukuku Genel Hükümler & Özel Hükümler, İkinci Sayfa Basım Yayım Dağıtım, İstanbul

ERDAĞ Ali İhsan, 2010, Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda), Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt. XIV, Sayı. 2, Ankara

ERDOĞAN Yavuz, 2010, Bilişim Sistemine Girme ve Kalma Suçu, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 12, Özel S. (s.1363-1433)

ERDOĞAN Yavuz, 2011, Türk Ceza Kanunu'nda Bilişim Sistemini Engelleme Bozma Verileri Yok Etme veya Değiştirme Suçu, Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Anabilim Dalı, Kamu Hukuku Bilim Dalı, İstanbul

ERDOĞAN Yavuz, 2012, Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle), Legal Yayıncılık, İstanbul

ERGÜN İsmail, 2008, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara

ERGÜN OKUYUCU Güneş, 2013, Banka Veya Kredi Kartlarının Kötüye Kullanılması, T.C. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Özel Sayı Prof. Dr. Nur CENTEL'e Armağan, Cilt: 19 Sayı: 2 (s.1065-1086)

ERMAN Ragıp Barış, 2006, Yanılmanın Ceza Sorumluluğuna Etkisi, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı

ERTAŞ Şeref, 2006, Eşya Hukuku, Seçkin Yayıncılık, Ankara

GÖKPINAR Mahmut, 2008, Ceza Sorumluluğunun Temeli: "Kast", Türkiye Barolar Birliği Dergisi, Sayı 79 (s.198-233)

GÖKTÜRK Neslihan, 2014, Türk Hukuku'nda Suçların İçtimaı, Ceza Hukuku ve Kriminoloji Dergisi, Cilt: 2, Sayı: 1-2 (s.31-60)

GÖZÜŞİRİN Mesih, 2011, 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları Ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi, Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Güvenlik Bilimleri Anabilim Dalı

GÜL Ahmet, 2016, Doğrudan - Dolaylı Bilişim Suçları, Seçkin Yayıncılık, Ankara

GÜNDOĞAN ÖZER Çiğdem, 2013, Will Facebook Remember You Forever: The Right To Be Forgotten On Social Networks Within The Privacy Framework, LLM in Internet Law, University of Essex, School of Law

GÜROCAK İsmail, 2010, Bilişim Sistemine Girme Suçu (TCK m. 243), *http://www.ismailgurocak.av.tr/makale/B%C4%B0L%C4%B0%C5%9E%C4%B0M%20S%C4%B0STEM%C4%B0NE%20G%C4%B0RME%20SU%C3%87U-%C4%B0SMA%C4%B0L%20G%C3%9CROCAK.pdf* (Erişim Tarihi: 22.07.2018)

HAFIZOĞULLARI Zeki, KURŞUN Günal, 2007, Türk Ceza Hukukunda Örgütlü Suçluluk, Türkiye Barolar Birliği Dergisi (Sayı 71)

HAFIZOĞULLARI Zeki, ÖZEN Muharrem, 2009, Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar, Ankara Barosu Dergisi, Yıl: 67, Sayı: 4 (s.9-22)

HAFIZOĞULLARI Zeki, ÖZEN Muharrem, 2016, Türk Ceza Hukuku Özel Hükümler - Topluma Karşı Suçlar, US-A Yayıncılık, Ankara

HAVUZ Serdar, 2007, Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği, Yüksek Lisans Tezi, Genelkurmay Başkanlığı, Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü, Uluslararası İlişkiler Anabilim Dalı, İstanbul

HELPGUIDE, 2018, Bullying and Cyberbullying-How to Deal with a Bully and Overcome Bullying, *https://www.helpguide.org/articles/abuse/bullying-and-cyberbullying.htm*, (Erişim Tarihi: 02.09.2018)

HENKOĞLU Türkay, 2017, Veri Koruma Kanununun Getirdikleri, Journal of Current Researches on Social Sciences (JoCReSS), Vol:7, Issue:2, *http://dergipark.gov.tr/download/article-file/359655* (Erişim Tarihi: 15.08.2018)

IC3, 2017, FBI Internet Crime Complaint Center - Internet Crime Report, *https://pdf.ic3.gov/2017_IC3Report.pdf* (Erişim Tarihi: 03.09.2018)

İLBAŞ Çığır, 2009, Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi, Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü

JLT, 2018, Japanese Law Translation - Penal Code (nr.45) - Act on Prohibition of Unauthorized Computer Access (nr.128), *http://www.japaneselawtranslation.go.jp/* (Erişim Tarihi: 04.09.2018)

KADİR Mohammed Rizgar, 2010, The Scope and the Nature of Computer Crimes Statutes – A Critical Comparative Study, German Law Journal - Vol. 11, No: 6

KALKINMA BAKANLIĞI, 2017, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Çalışma Raporu - 6, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü, Bilgi Toplumu Dai.Bşk.lığı

KAN Çiğdem, 2009, Sosyal Bilgiler Eğitiminde Küresel Vatandaşlık, Pamukkale Üniversitesi, Eğitim Fakültesi Dergisi, Sayı 26, 2009, s. 25-30

KARAGÜLMEZ Ali, 2014, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, Seçkin Yayıncılık, Ankara

KARAKEHYA Hakan, 2009, Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu, Türkiye Barolar Birliği Dergisi (Sayı 81)

KASPERSKY, 2016, "Fidye yazılımı hakkında bilmeniz gereken her şey" *https://www.kaspersky.com.tr/blog/ransomware-faq/2613/* (Erişim Tarih: 23.04.2018)

KASPERSKY, 2017, "Çocukları Siber Zorbalıktan Korumanın 5 Yolu" *https://www.kaspersky.com.tr/about/press-releases/2017_cocuklari-siber-zorbaliktan-korumanin-5-yolu* (Erişim Tarihi: 02.09.2018)

KAYA Ahsen, BİLGİN Umut Erdar, MOLLAOĞLU Abdullah, KOÇAK Aytaç, EKİN Özgür Aktaş, 2013, Türkiye Genelinde Bilişim Yolu ile İşlenen Dolandırıcılık Suçu: 16 Olgu, NWSA-Social Sciences, ID: 2013.8.3.3C0111 (s.101-105) *http://dergipark.gov.tr/download/article-file/187057* (Erişim Tarihi: 14.08.2018)

KAYA Yasin, 2016, Bulut Bedelli Adli Bilişim, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku

KAYMAZ Seydi, 2012, 5237 Sayılı Türk Ceza Kanununa Göre İştirak Halinde İşlenen Suçlarda Nitelikli Hallerin Diğer Suç Ortaklarına Geçişi Sorunu, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C: 16, Sayı: 2 (s.117-167)

KETİZMEN Muammer, 2008, Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara

KILIÇOĞLU Ahmet, 2006, Sınai Haklarla Karşılaştırmalı Fikri Haklar, Turhan Kitabevi, Ankara

KIZILTAN Burak Mehmet, 2007, 5237 sayılı Türk Ceza Kanununda Bilişim Sistemine Girme Sistemi Engelleme ve Bozma Suçları, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul

KOCA Mahmut, ÜZÜLMEZ İlhan, 2014, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara

KOÇAK Hüseyin, DANDİN Ali Nazmi, 2017, Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri, Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi / Cilt 19, Sayı: 1, s.137-152

KPMG, 2017, Cybercrime Survey Report – Insights and Perspectives, *https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf* (Erişim Tarihi: 19.04.2018)

KULEVSKA, Sanna (2013), The Future of Your Past: A Right to be Forgotten Online, *https://www.lumendatabase.org/blog_entries/521* (Erişim Tarihi: 18.08.2018)

KURT Levent, 2005, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulamalar, Seçkin Yayıncılık, Ankara

KÜLTÜR BAKANLIĞI, 2018, Ticaretle Bağlantılı Fikri Mülkiyet Anlaşması, *http://www.telifhaklari.gov.tr/Ticaretle-Baglantili-Fikri-Mulkiyet-Anlasmasi-TRIPS* (Erişim Tarihi: 07.08.2018)

KÜZECİ Elif, 2010, Kişisel Verilerin Korunması, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku (Genel Kamu Hukuku) Anabilim Dalı

KVKK, 2018, 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Yayınları, *https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf* (Erişim Tarihi: 15.08.2018)

LEVIN Avner, ILKINA Daria, 2013, International Comparison of Cyber Crime, Ryerson University, Privacy and Cyber Crime Institute

MAHMUTOĞLU Fatih Selami, 2005, Kusurluluk Prensibi Açısından Azmettirenin Ceza Sorumluluğu, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 63, S. 1-2

MARİAN Omri, 2013, Kripto Para Birimi Üstün Vergi Cenneti mi?, (çev.) Sedef Pelin Gürlek Keleş, 2016, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LXXIV, Sayı: 2, Legal Yayıncılık A.Ş., İstanbul (s.919-930)

McQUADE Samuel C., 2009, Encyclopedia of Cybercrime, Greenwood Press, Westport/Connecticut

MERAN Necati, Yeni Türk Ceza Kanununda Sahtecilik - Malvarlığı - Bilişim Suçları işe Ekonomi ve Ticaret Alanında Suçlar, Seçkin Yayıncılık, Ankara

MERKİ Duygu, 2009, Bileşik Suç, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku (Ceza Hukuku) Anabilim Dalı, Ankara

NACAR Fatma Burcu, 2010, Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları, Yüksek Lisans Tezi, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Avrupa Birliği Anabilim Dalı, Ankara

NATSUI Takato, 2003, Cybercrimes in Japan: Recent Cases Legislations Problems and Perspectives,
http://cyberlaw.la.coocan.jp/Documents/netsafepapers_takatonatsui_japan.pdf
(Erişim Tarihi: 04.09.2018)

NCA (National Crime Agency), 2018, National Strategic Assessment of Serious and organised Crime, İngiltere,
http://www.nationalcrimeagency.gov.uk/publications/905-national-strategic-assessment-for-soc-2018/file (Erişim Tarihi: 20.07.2018)

ODTÜ, 2005, *http://www.internetarsivi.metu.edu.tr/tarihce.php* (E.Tarih:07.03.2018)

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

ÖNOK Murat, 2013, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlara Mücadelede Uluslararası İşbirliği, T.C. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Özel Sayı Prof. Dr. Nur CENTEL'e Armağan, Cilt: 19 Sayı: 2

ÖZBEK Veli Özer, 2007a, Neticesi Sebebiyle Ağırlaşmış Suçlar, Ceza Hukuku Dergisi, Sayı: 4, Seçkin Yayıncılık, s.223-246

ÖZBEK Veli Özer, 2007b, Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245), Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 9, Özel Sayı

ÖZEN Muharrem, BAŞTÜRK İhsan, 2011, Bilişim - İnternet ve Ceza Hukuku, Adalet Yayınevi, Ankara

ÖZGENÇ İzzet, 2014, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık

ÖZGENÇ İzzet, ÜZÜLMEZ İlhan, GÖKTÜRK Neslihan, 2012, Ceza Hukukuna Giriş, T.C. Anadolu Üniversitesi Yayını No: 2476, Eskişehir

ÖZTÜRK Bahri, Erdem Mustafa Ruhan, 2007, Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara

ÖZTÜRK Özgür, 2009, E-Postalarda Spam Sorunu ve Çözüm Önerileri, Bilişim Uzmanlığı Tezi, Ankara

PALLI Hayati, 2008, Türk Hukukunda Ve Mukayeseli Hukukta Bilişim Suçları, Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı

PARLAR Ali, 2011, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara

PASSERI Paolo, 2018, *https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/* (Erişim Tarihi: 19.04.2018)

PICOTTI Lorenzo, 2012, Preparatory Colloquium Section II Report of XIXth International Congress of Penal Law, *http://www.aidpitalia.org/docs/Verso%2019%20Congresso%20AIDP/Sect%20II%20AIDP%20-%20Italy%20Report%20Picotti.pdf* (Erişim Tarihi: 03.09.2018)

PLAGEMANN Gottfried, YENİSEY Feridun, 2015, Alman Ceza Kanunu (Strafgesetzbuch-StGB), Beta Yayınları, İstanbul

REDSTOR, 2018, "Cyber-crime Court To Be Set Up In London", *https://www.redstor.com/news/cyber-crime-court-be-set-london* (E.Tarih:20.07.2018)

SAMSUNG, 2017, Siber Zorba Olma, *https://www.samsung.com/tr/sosyal-sorumluluk/siber-zorba-olma/* (Erişim Tarihi: 02.09.2018)

SARIASLAN Halil, 2012, Yeni Dünya Düzeninin Temel Belirleyicileri Ve Ülkelerin Buna Uyumu, Ankara Barosu Uluslararası Hukuk Kurultayı, 10-14 Ocak 2012 - 3. Cilt, Ankara, s.145-151

SINAR Hasan, 2001, İnternet ve Ceza Hukuku, Beta Yayıncılık, İstanbul

SÖNMEZ Yağmur, 2018, Günümüz İnternet Ortamında Bilişim Suçları ve Türkiye'deki İnternet Haber Sitelerine Yansıması, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İletişim Bilimleri Bilim Dalı, İstanbul

STATISTA, 2018a, "Apple's Services Revenue by Product Category From 2011 to 2020" *https://www.statista.com/statistics/742847/apple-services-revenue-by-product-category/* (Erişim Tarihi: 28.03.2018)

STATISTA, 2018b, Video Game Industry – Statistics & Facts, *https://www.statista.com/topics/868/video-games/* (Erişim Tarihi: 28.07.2018)

STATISTA, 2018c, Customer Preferred Gaming Platforms According To Gaming Companies Worldwide 2016, *https://www.statista.com/statistics/608933/gaming-companies-customer-preferred-gaming-platforms-worldwide/* (Erişim Tarihi: 28.07.2018)

STATISTA, 2018d, Number of Cybercrime Related Consultations in Japan from 2012 to 2017, *https://www.statista.com/statistics/746985/japan-number-of-reported-cyber-crimes/* (Erişim Tarihi: 04.09.2018)

STM, 2018, Siber Tehdit Durum Raporu (Ocak-Mart), *https://www.stm.com.tr/documents/file/Pdf/siber-tehdit-durum-raporu-ocak-mart-2018.pdf*

ŞEN Ersan, 2012, Hırsızlık Suçları, Ankara Barosu Dergisi, Yıl: 70, Sayı: 2012/3 (s.319-357)

ŞIRACI Sertel, 2016a, Oyunlarda Yaşanan Hukuksal Sorunlar, *https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/oyunlarda-yasanan-hukuksal-sorunlar.html* (Erişim Tarihi: 28.07.2018)

ŞIRACI Sertel, 2016b, Yasak Program ve Cihazlar Zararlı Yazılım, https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zararli-yazilim-imal-etme-bulundurma-sucu.html (Erişim Tarihi: 03.08.2018)

ŞİMŞEK Oğuz, 2008, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayıncılık

TANERİ Gökhan, 2016, Temel Cezanın Belirlenmesi, Ankara Barosu Dergisi, Yıl: 74, Sayı: 2016/3 (s.127-161)

TANRIKULU Cengiz, 2014, Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve El Koyma, Adalet Yayınevi, Ankara

TAŞDEMİR Kubilay, 2001, Uygulamada Bilişim Suçları, Panel - Bilişim Suçları, T.C. Adalet Bakanlığı Hâkim ve Savcı Adayları Eğitim Merkezi Başkanlığı, Ankara

TAŞKIN Şaban Cankat, 2008, Bilişim Suçları, Beta Yayıncılık, İstanbul

TAŞKIN Şaban Cankat, 2016, İnternete Erişim Yasakları, Seçkin Yayıncılık, Ankara

TBMM, 2004, TBMM Mevzuat Bilgi Sistemi, http://mevzuat.tbmm.gov.tr/mevzuat/faces/kanunmaddeleri?_adf.ctrl-state=14uyxbaeyu_4&pkanunlarno=24110&pkanunnumarasi=5237 (Erişim Tarihi: 28.07.2018)

TBMM, 2012a, Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu

TBMM, 2012b, Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676)

TBMM, 2016a, TBMM Mevzuat Bilgi Sistemi, 5237 Sayılı TCK'nın Gerekçeleri, *https://mevzuat.tbmm.gov.tr/mevzuat/faces/kanunmaddeleri?pkanunlarno=24110&pkanunnumarasi=5237* (Erişim Tarihi: 17.05.2018-27.08.2018)

TBMM, 2016b, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, Yasama Dönemi: 26, Yasama Yılı: 1, Sıra Sayısı: 117, https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf (Erişim Tarihi: 27.07.2018)

TDK, 2018a, Türk Dil Kurumu Ana Sayfası - Bilim ve Sanat Terimleri Ana Sözlüğü, *http://www.tdk.gov.tr/index.php?option=com_bilimsanat&arama=kelime&guid=TDK.GTS.5aeb89330f4688.55088498* (Erişim Tarihi: 29.01.2018)

TDK, 2018b, Türk Dil Kurumu Ana Sayfası - Güncel Türkçe Sözlük, *http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5a821ca2237b15.93387259* (Erişim Tarihi: 12.02.2018)

TOGED, 2014, Bilgisayar Oyunlarının Faydaları, *http://www.toged.org/bilgisayar-oyunlarinin-faydalari/* (Erişim Tarihi: 28.07.2018)

TOROSLU Nevzat, FEYZİOĞLU Metin, 2008, Ceza Muhakemesi Hukuku, Savaş Yayınevi, Ankara

TOROSLU Nevzat, 2009, Ceza Hukuku Genel Kısım, Savaş Yayınevi, Ankara

TUFANOĞLU İshak, 2014, Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçları, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, İstanbul

TULUM İsmail, 2006, Bilişim Suçları ile Mücadele, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Isparta

TURABİ Selami, 2012, Kusurluluk ve Kusurluluğu Etkileyen Haller, Türkiye Barolar Birliği Dergisi, Sayı: 102 (s.267-292)

TURAN Metin, KÜLCÜ Özgür, 2014, Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi, Türk Kütüphaneciliği, Cilt: 28, Sayı: 1 (s.18-46)

TURAN Metin, 2016, Bilişim Hukuku, Seçkin Yayıncılık

TURAN Metin, 2017, Alman Bilişim Hukuku, Adalet Yayınevi, Ankara

TURHAN Meltem, 2010, Siber Güvenliğin Sağlanması, Dünya Uygulamaları Ve Ülkemiz İçin Çözüm Önerileri, Bilişim Uzmanlığı Tezi, Ankara

TURHAN Oğuz, 2006, Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), Planlama Uzmanlığı Tezi, Ankara

UÇAR Hüdaverdi, 2014, 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Yüksek Lisans Tezi, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı - Ceza ve Ceza Usul Hukuku Bilim Dalı, Ankara

UNCTAD, 2018, Cybercrime Legislation Worldwide, *https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx* (Erişim Tarihi: 03.09.2018)

UNICEF, 2017, The State of the World's Children 2017-Children in a Digital World *https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf* (Erişim Tarihi: (01.09.2018)

US-CERT, 2016, "Ransomware What It Is and What To Do About It?" *https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf* (Erişim Tarihi: 23.04.2018)

UYSAL Kemal, 2010, Comparison Of The Copyrıght Law In Turkey With the EU Acquıs Communautaire In The Framework Of Full Harmonization, Yüksek Lisans Tezi, Marmara Üniversitesi Avrupa Birliği Enstitüsü, Avrupa Birliği Hukuku Anabilim Dalı

ÜNAL Osman Gazi, 2011, Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve El Koyma, Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ceza ve Ceza Usul Hukuku Anabilim Dalı, Ankara

WEBER, M. Amalie, 2003, The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal, Volume 18 – İssue 1 – Article 28 *https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj* (Erişim Tarihi: 09.05.2018)

WIPO, 2018, Inside WIPO - What is WIPO, *http://www.wipo.int/about-wipo/en/* (Erişim Tarihi: 07/08/2018)

YARGITAY, 2018, Emsal Karar Arama, *https://emsal.yargitay.gov.tr/BilgiBankasiIstemciWeb/GelismisDokumanAraServlet*

YAYCI Esra, 2007, Bilişim Suçları, Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı - Ceza ve Ceza Usulü Hukuku Bilim Dalı, Ankara

YAZICIOĞLU Yılmaz, 2001, Bilgisayar Ağları Marifetiyle İşlenen Suçlar: Sanal Suçlar, Panel - Bilişim Suçları, T.C. Adalet Bakanlığı Hâkim ve Savcı Adayları Eğitim Merkezi Başkanlığı, Ankara

YENİDÜNYA Ahmet Caner, DEĞİRMENCİ Olgun, 2003, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, İstanbul

YERDELEN Erdal, 2014, Mütemadi (Kesintisiz) Suç - *Dauerverbrechen*, Türkiye Adalet Akademisi Dergisi, Yıl: 5, Sayı: 18

YETİM Servet, 2014, Siber Suçlar Yargılama Yetkisi ve Yeni Bir Model Önerisi, Türkiye Adalet Akademisi Dergisi, Yıl: 5, Sayı: 17 (s.177-230)

YILMAZ Çetin, 2018, Türk Ceza Hukukunda Dolandırıcılık Suçu, Yüksek Lisans Tezi, Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı

YILMAZ Sacit, 2010, Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu, Türkiye Barolar Birliği dergisi, Sayı: 87 (s.262-298)

YILMAZ Sacit, 2011, 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanında Suçlar, Türkiye Barolar Birliği Dergisi, Sayı: 92 (s.62-100)

YOKUŞ SEVÜK Handan, 2009, Haberleşmenin Gizliliğini İhlal Suçu, Dicle Üniversitesi Hukuk Fakültesi Dergisi, Sayı: 12-13 (s.159-195)

ZDNET, 2018, "Cyber crime: Under-reporting of attacks gives hackers a green light, say police", *https://www.zdnet.com/article/cyber-crime-under-reporting-of-attacks-gives-hackers-a-green-light-say-police/* Erişim Tarihi: (20.07.2018)

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

14/09/2018

Burak Cesur AKÖZ

ÖZGEÇMİŞ

1986 yılında Ankara'da doğdu. İlk, orta ve lise öğrenimini İstanbul, İzmir ve Ankara illerinde tamamladı. 2005 yılında Başkent Üniversitesi Hukuk Fakültesi'nde başladığı eğitimini 2009 yılında dördüncülükle bitirdi. Ankara Üniversitesi Hukuk Fakültesi Özel Hukuk Anabilim Dalı'nda tezli yüksek lisans eğitimine devam etmektedir. 2010-2011 yılları arasında Ankara Barosu bünyesinde tamamladığı staj programı sonrasında avukatlık ruhsatını almış, 2011 yılı Aralık ayında Kültür ve Turizm Bakanlığı'nda uzman yardımcısı sıfatıyla kamudaki görevine başlamıştır. 2013 yılı Aralık ayından bu yana Bilgi Teknolojileri ve İletişim Kurumu'nun çeşitli birimlerinde (Teknik Düzenlemeler Dairesi Başkanlığı, Hukuk Müşavirliği, Tüketici ile İlişkiler Müdürlüğü) görev almış olup, Kurumdaki görevini Bilişim Uzman Yardımcısı olarak sürdürmektedir. Evli ve bir çocuk babasıdır.