TÜRKİYE CUMHURİYETİ
ÇAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

DİJİTAL VERİ HIRSIZLIĞI

TEZİ YAZAN
İslam Kurthan AÇIKBAŞ

Danışman: Prof. Dr. Mustafa Tevfik ODMAN
Jüri Üyesi: Dr. Öğr. Üyesi Tarık Polat İŞOĞLU
Jüri Üyesi: Dr. Öğr. Üyesi Mustafa ŞİMŞEK (Toros Üniversitesi)

YÜKSEK LİSANS TEZİ

MERSİN/ OCAK 2022

ONAY

T.C
ÇAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ' NE

20192030 numaralı öğrencimiz olan **İslam Kurthan AÇIKBAŞ** tarafından hazırlanan **"Dijital Veri Hırsızlığı"** başlıklı bu tez çalışması jüri üyeleri tarafından **oy birliği** ile **Kamu Hukuku** Anabilim Dalında **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Enstitü Müdürlüğünde Evrak Aslı İmzalıdır.

Tez Danışmanı- Jüri Başkanı Asıl Üye- Üniversite İçi :Prof. Dr. Mustafa Tevfik ODMAN

Enstitü Müdürlüğünde Evrak Aslı İmzalıdır.

Üniv. Dışı – Jüri asıl Üyesi :Dr. Öğr. Üyesi Mustafa ŞİMŞEK
(Mersin Toros Üniversitesi)

Enstitü Müdürlüğünde Evrak Aslı İmzalıdır.

Üniv. İçi – Jüri asıl Üyesi Dr. Öğr. Üyesi Tarık Polat İŞOĞLU

Yukarıdaki imzaların, adı geçen öğretim elemanlarına ait olduklarını onaylarım.

.....

18/04/2022
Doç. Dr. Murat KOÇ
Sosyal Bilimler Enstitüsü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'ndaki hükümlere tabidir.

İTHAF

Eşim, Kızım ve Türk Milleti'ne

ETİK BEYANI

Çağ Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

• Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,

• Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,

• Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,

• Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,

• Bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İslam Kurthan AÇIKBAŞ

TEŞEKKÜR

Her türlü desteğini bizden esirgemeyen, bizimle sürekli iletişim kurarak bizi motive eden Sayın Prof. Dr. Mustafa Tevfik ODMAN hocama, tezimin yazım sürecinde maddi ve manevi desteğini esirgemeyen, eşime ve aileme teşekkürler ederim.

ÖZET

DİJİTAL VERİ HIRSIZLIĞI

İslam Kurthan AÇIKBAŞ

Yüksek Lisans Tezi, Kamu Hukuku Anabilim Dalı
Tez Danışmanı: Prof. Dr. Mustafa Tevfik ODMAN
Ocak 2022, 152 sayfa

Dijital veriler, kullandığımız telefondan bilgisayarlara, akıllı saatlerimizden teknoloji içeren her eşyaya, oyuncaklardan sosyal aktivitelere kadar ve daha fazla alanda hayatımızda yer almış durumdadır. Dijital verilerin insan hayatındaki geniş çapta yer edinmesi, yeni suç tiplerini ve suç işleniş şekillerinin ortaya çıkmasına neden olmuştur. Toplumsal düzenin yapı taşı olan hukuk bilimi, bu değişim ve ilerleyişin karşısında kayıtsız kalamamış ve dijital verilerin temelini oluşturduğu bilişim alanında düzenlemeler yapılması ihtiyacını ortaya çıkarmıştır. Ancak, teknolojinin çok hızlı gelişmesi ve toplumun teknoloji karşısındaki ihtiyaçlarının ilerleyen zaman içinde hissedilmesi bilişim hukuku alanında, etkili bir yasal düzenlemenin yapılmasına engel olmuş, yapılan düzenlemeler de eksik veya mevcut düzenlemelere ekleme suretiyle yapılmıştır. Oluşan bu hukuki açık kısa zamanda hem ulusal hem de uluslararası alanda kendisini göstermiştir. Hem uluslar hem de uluslararası örgütler, oluşan bu açığı kapatmak ve bilişim suçlarıyla daha etkili mücadele etmek amacıyla girişimlerde bulunmuşlardır. Yine de bilişim hukuku alanındaki düzenlemelerin, teknolojik gelişmelere ilişkin düzenlemelerin gerisinde kaldığı ve yüzde yüz bir çözümün bulunamadığı görülmektedir. Bilişim hukuku alanındaki yasal düzenlemelerin kusursuz olmasını beklememekle birlikte, mevcut düzenlemelerinde yapılabilen ve yapılacak en etkin düzenleme olmadığını düşünmekteyiz. Bu nedenle; teknik bir alan olan bilişim hukukunun temelini oluşturan dijital verilerin, hem teknik hem de hukuk alanında adlandırılabilmesi için en basit haliyle teknik açıklamalar ve örnekler verilmiş, daha sonra dijital veri hırsızlığının temelini oluşturduğu ulusal düzenlemeler ile uluslararası düzenlemelerde yer alan farklı suç tipleri ele alınarak açıklanmış ve örnekler verilerek bilişim suçlarına konu dijital verilerin güvenliği için neler yapılabileceği anlatılmaya çalışılmıştır.

Anahtar kelimeler: Veri, dijital veri, bilişim suçları, veri hırsızlığı, bilişim hukuku.

ABSTRACT

DİJİTAL VERİ HIRSIZLIĞI

İslam Kurthan AÇIKBAŞ

Master Thesis, Department of Public Law
Thesis Supervisor: Prof. Dr. Mustafa Tevfik ODMAN
January 2022, 152 pages

Digital data takes place in many areas of our lives, from the phone to the computer, from smart watches to every item containing technology, from toys to social activites. The wide spread use of digital data in human lifes leads to the emergence of new crime types and forms of crime. Legal sience, which is the building block of the social order can not remain indiffrent to this change and progress anf reveals the need for regulations in the field of informatics, which is based on digital data. However, the development of technology and the fact that the society's needs against technology are felt more over time prevent effective legal regulations in the field of in formatics law and ensure that the regulations are made by adding them to the existing regulations. This gap in the legal field manifests itself in both national and international fields in a short time. Both national and international organizations are taking initiatives to close this gap and fight cyber crimes more quikly anf effectively. Despik this situations, it is seen that the regulations in the field of informatics law lag behind the regulations an technological developments and there is no definite solution.Although it is not expected that the legal regulations in the field of informatics law will be perfect, it is though that the legal regulations that can or will be made could be better. For this reason, in order to name the digital data that forms the basis of informatics law, which is a technical field, technical explanations and examples are given in a simple way, with diffrent types of crime in national and international regulations that form the basis of digital data theft, and digital data subject to cyber crimes are given. It is tried tı explain what can be done fort he security of the data.

Keywords: Digital data, cyber crimes, data, data theft, IT law

ÖN SÖZ

Dijital veriler, insan hayatının ve toplumun içerisinde yer edinmeye başlamasından itibaren değer kazanmaya başlamıştır. Dijital verilerin değer kazanması ve hayatın birçok noktasında maddi değere sahip unsurlar olması, suçluların dikkatini çekmiştir. Dijital veriler üzerinden para kazanılması, teknolojinin gelişmesi ve faillerin bulunmasının ve delillerin toplanmasının zorluğu nedeniyle cazip hale gelmiştir. Birçok fail bu nedenle, dijital verilerin çalınmasının doğrudan veya dolaylı olarak konu olduğu yeni suç tiplerini gerçekleştirmeye başlamıştır. Ancak, dijital verilerin kişilerin rızası ve izni olmadan çeşitli yol ve yöntemlerle ele geçirilmesi ve kullanılması eylemleri, bir tür hırsızlık olarak düşünülebilirse de bu konuda spesifik herhangi bir yasal düzenleme olmaması faillerin cezalandırılmaları yönünden büyük zorluklar yaratmaktadır. Dolayısıyla bu durum, bu tür fiillerin ve mevcut yasal düzenlemelerin yeterliliğini incelemeye ve bunun sonucunda ne gibi önlemler alınması ve değerlendirmeler yapılması gerektiğini araştırmaya yöneltmektedir.

Bu inceleme, araştırma ve değerlendirmeleri içeren Tez, dört ana bölümden oluşturulmuştur.

Tezin Birinci Bölümünde, teknik bir kavram olan dijital veri kavramı incelemeye alınmıştır. Dijital veri kavramı teknik bir kavram olduğu için daha iyi anlaşılması bakımından, dijital kavramının ve veri kavramının ne olduğu, dijital veri kavramına konu olan değerlerin neler olduğu açıklanmış ve sonrasında ise dijital verilerin çalınması yöntemlerinin teknik yönlerinin en bilinen şekilleri mümkün olduğunca teknik ayrıntıya girmeden ve örnekleme yapılarak anlatılmıştır.

Tezin İkinci Bölümünde, ulusal mevzuatımızda yer alan dijital veri hırsızlığının temeli olan bilişim suçlarıyla ilgili doğrudan ve dolaylı bağı olan suç tipleri açıklanmış ve bu suç anlatılırken öğretiden ve yargı kararlarından faydalanılmış, ilgili düzenlemelere eleştiriler getirilmiş ve bu eleştiriler uygulamadaki yargı kararları ile örneklendirilerek yasal düzenlemelerin yetersiz kaldığı noktalar tespit edilmeye çalışılmıştır.

Tezin Üçüncü Bölümünde, uluslararası hukukta yer alan ve dijital veri hırsızlığıyla bağlantılı düzenlemelerin tarihsel gelişim süreci incelenerek, bilişim hukukunda hangi gelişmelerin yaşandığı, gelişen teknoloji ile beraber mevcut yasal düzenlemelerdeki değişimlere neden ihtiyaç duyulduğu, uluslararası düzenlemeler ve

örneklerle incelenerek, bilişim hukukunun gelişimine nelerin etki ettiği tespit edilmeye çalışılmıştır.

Tezin Dördüncü ve son Bölümünde, dijital veri hırsızlığıyla mücadelenin nasıl olması gerektiği, teknik ve hukuki yönleriyle bilişim suçlarıyla mücadelede nelere dikkat edilmesi gerektiği, dijital verilerin nasıl korunabileceğine değinilmiş, bu çerçevede bireylerin ve devletlerin dijital veri hırsızlığıyla mücadeleyi en etkin şekilde nasıl yapabileceği anlatılmıştır.

İÇİNDEKİLER

İKİNCİ BÖLÜM
DİJİTAL VERİ HIRSIZLIĞI, DİJİTAL VERİ HIRSIZLIĞININ KONUSU OLAN BAŞLICA YASAL DÜZENLEMELER

ÜÇÜNCÜ BÖLÜM
DİJİTAL VERİ HIRSIZLIĞI İLE İLGİLİ ULUSLARARASI DÜZENLEMELER

KISALTMALAR

AB	**:** Avrupa Birliği
ABD	**:** Amerika Birleşik Devletleri
AK	**:** Avrupa Konseyi
AÜEHFD	**:** Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi
C. D.	**:** Ceza Dairesi
ATAD	**:** Avrupa Birliği Adalet Divanı
CDPC	**:** European Committee on Crime Problems
CHD	**:** Ceza Hukuk Dergisi
Convection +18	**:** Convention for the Protection of Individiuals with regard to Automatic Procesing of Personal Data
DEÜHFD	**:** Dokuz Eylül Üniversitesi Hukuk Fakültesi
DPC	**:** Data Protection Commission-Veri Koruma Komisyonu
EİK	**:** 5070 Sayılı Elektronik İmza Kanunu
ETS	**:** European Treaty Series
FESK	**:** 5846 Sayılı Fikir ve Sanat Eserleri Kanunu
GDPR	**:** General Data Protection Regulation
İst.	**:** İstanbul
KVKK	**:** 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanun
MALWARE	**:** Malicious software
s.	**:** sayfa
S.	**:** Sayı
TBMM	**:** Türkiye Büyük Millet Meclisi
TCK	**:** 5237 Sayılı Türk Ceza Kanunu
TDK	**:** Türk Dil Kurumu
TİK	**:** 5429 Sayılı Türkiye İstatistik Kanununun
TRT	**:** Türk Radyo ve Televizyon Kurumu
TUİK	**:** Türkiye İstatistik Kurumu
UKUSA	**:** Ukusa Agreement
USB	**:** Universal Serial Bus-Evrensel Seri Veri yolu
Vd.	**:** ve diğerleri
VERBİS	**:** Veri Sorumluları Sicili
Yrg.	**:** Yargıtay

EKLER LİSTESİ

GİRİŞ

İnsan evriminin en muhteşem yanı zekâsıdır. İnsanoğlunun milyonlarca yıl içerisinde hayatta kalma ve hayatını kolaylaştırmak için sarf ettiği gayret, insan zekâsının muhteşem bir evrim geçirmesine neden olmuştur. İnsanoğlunun çevresinde edindiği olgu ve çıkarımları veriler halinde, beyninde işleyerek ortaya çıkardığı bilgilerin sonucu olarak meydana gelen teknolojik gelişmeler, muazzam bir hız kazanmış ve teknoloji hayatımızın olmazsa olmazları arasına girmiştir.

İnsanoğlu gelişen teknoloji ile birlikte iş ve sosyal hayatını, dijital ortamlara taşımıştır. Böylece insan elindeki verileri hızlı, kaliteli ve hatasız şekilde işleyerek iş verimini arttırmış, sosyal hayatında etkileşimi kolaylaştırmış ve çeşitlendirmiştir. İnsanların hayatlarını dijital ortamlara taşımasıyla birlikte, dijital verilerin bazı suçlarda araç olarak kullanımı söz konusu olmaya başlamış ve bu suçlarla ilgili yasal düzenlemelerin yapılması gereği ortaya çıkmıştır.

Dijital ortamlarda yer alan kişisel verilerin, genelde tüzel kişilere, istisnai olarak da gerçek kişilere verildiği ve bu kişilerin dijital ortamlara işlediği kişisel verilerin, teknolojinin sağladığı imkan ve kolaylıklarla kötüye kullanılarak, veri sahibi kişilere maddi veya manevi açıdan zarar vermeye, bunun yanında veri sahibi dışındaki kişilere de kazanç sağlama gibi nedenler ile kullanılmaya başlandığı görülmektedir.

Dijital ortamlarda yer alan kişisel verilerin; veri sahibinin izni olmaksızın alınması ve kullanılması, hem veri sahiplerinin hem de üçüncü kişilerin mağduriyetine neden olmaktadır. Özellikle, sosyal medyadaki sahte profiller, hukuka aykırı şekilde elde edilen kişisel veriler ile parasal işlemlerin yapılması, ülkelerin sosyal medya sitelerinden sızdırılan kullanıcı profil analizlerinin seçim kampanyalarına hazırlık yapıldığı dönemlerde kullanılması gibi olaylar, gerçekte dijital ortamda hukuka aykırı biçimde elde edilen, kaydedilen veya başkalarına verilen veya ele geçirilen veri kullanımının ne kadar geniş çapta ve çeşitli şekilde olduğunu ortaya koymaktadır. Ancak, işlenen bu suçlara karşı etkili hukuki düzenlemelerin, teknoloji ile aynı hızda gelişemediği görülmektedir.

Genel, kapsamlı ve oluşabilecek sorunlar gözetilerek yasal düzenleme yapılmamış, sürekli olarak ortaya çıkan ihtiyaçlar doğrultusunda mevcut düzenlemelerin içerisinde kısım kısım veya yaşanılan sorunu kapsayan alanda yasal düzenlemeler yapılmıştır. Dağınık ve dar alanları kapsayan yasal düzenlemeler ise teknolojik gelişmeler karşısında çok sığ kalmış ve sınırlı çözümler olmaktan öteye gidememiştir.

Dijital alanda işlenen suçlara konu eylemlere ilişkin yeterli kapsamda yasal düzenlemelerin yapılmaması, hukuki boşlukların çok olması, dijital ortamda hareket eden faillerin suç işleme iradesini kamçılamakta ve onları suç işlemeye yöneltmektedir.

İnsanların iş ve sosyal hayatında teknolojik gelişmelerden yararlanması, toplum düzenini sağlayan hukuk sistemini de bu gelişmelere ayak uydurmaya yöneltmiştir. Teknolojinin araç olarak kullanıldığı suçlarda çeşitliliğin ve sayının artması, Türk Ceza Kanununda sınırlı sayıda yapılan yeni düzenlemelerin günün koşullarına uygun ve yeterli olup olmadığı konusunu tartışmaya açmıştır.

Belirtilen nedenlerden dolayı çalışmamda öncelikle konumla ilgili dijital veri kavramına ilişkin teknik bilgileri kısaca açıklama ve daha iyi anlaşılması için örneklemeye gidilmiş, kavramlar anlatılmıştır. Sonrasında konusunu dijital verilerin oluşturabileceği yasal düzenlemelere yer verilmiş ve yine örneklendirilmiştir. Çalışmamın devamında ülkemizdeki yasal düzenlemelere de etki eden karşılaştırılmalı hukuk kıyaslanarak uluslararası düzenlemeler incelenmiştir. Yapılan inceleme ile bilişim ve teknoloji ile ilgili yasal düzenlemelerin yapılması ihtiyacının kaynağı ve gelişimi tespit edilmeye çalışılmıştır. Yapılan tespitler, mevcut yasal düzenlemeler, içtihatlar ve öğreti görüşleri eşliğinde incelenmiştir.

Açıklanan kapsamda dört bölümden oluşan çalışmanın Birinci Bölümünde dijital veri kavramına yer verilerek incelenecektir. İkinci Bölümde bilişim suçlarının temelini oluşturan dijital veri hırsızlığı ve dijital veri hırsızlığı ile ilgili olabilecek yasal düzenlemeler üzerinde durulacaktır. Üçüncü Bölümde ise iç hukuku etkileyen karşılaştırılmalı hukuk tartışılacaktır. Çalışmanın Dördüncü ve Son Bölümünde bilişim suçlarıyla mücadelede bireylerin ve devletlerin neler yapabileceği ve nasıl bir hukuk düzenine ihtiyaç duyulduğu anlatılmıştır.

BİRİNCİ BÖLÜM

VERİ VE DİJİTAL KAVRAMLARI, VERİLERİN DİJİTAL ORTAMDA İŞLENMESİ, KİŞİLERİN DİJİTAL VERİLERİ KULLANMASI VE ÖNEMİ

1. Dijital Veri Kavramı

Dijital veri hırsızlığının, konusunu açıkça ortaya koyabilmek için, iki farklı kelimeden oluşan dijital veri kavramının anlamını açıklığa kavuşturmak gerekmektedir. Dijital veri, bir birini tamamlayan iki farklı kavramdan oluşmaktadır. Veri kavramının sıfatı niteliğinde bulunan dijital kavramı, çok geniş bir kullanım alanı olan veri kavramının teknoloji ve bilişim alanı içerisinde kullanılmak üzere bir çerçeve çizer. Çalışmamızın bu bölümünde veri ve dijital kavramlarını ayrı ayrı ele almak dijital veri kavramını daha iyi anlaşılmasını sağlayacaktır.

1.1. Veri

Köken olarak veri kavramı İngilizce *"data"* kelimesinden dilimize geçmiş olup, ham, gerçekleşmemiş enformasyon *"malumat"* parçacığına verilen ad olarak tanımlanmaktadır[1]. Data kelimesinin kökeni, Latincede "*Datum"* kelimesinden gelmektedir. Datum kelimesinin çoğulu anlamına gelen *"data"* kelimesi, verilen şey anlamına gelmektedir. Dilimizde de verilen şey *"veri"* olarak kullanılmaktadır[2]. Dijital verinin İngilizce karşılığı ise *dijital data*'dır.

Genel olarak *veri*; ham gerçek enformasyon parçacığına verilen addır. Veriler ölçüm, sayım, deney, gözlem ya da araştırma yolu ile elde edilmektedir. Ölçüm ya da sayım yolu ile toplanan ve sayısal bir değer bildiren veriler nicel veriler, sayısal bir değer bildirmeyen veriler de nitel veriler olarak adlandırılmaktadır.

Veri-data; incelenmek ve dikkate alınmak ve karar vermeye yardımcı olmak için kullanılan bilgiler, özellikle gerçekler veya sayılar veya bir bilgisayar tarafından saklanabilen ve kullanılabilecek elektronik formdaki bilgiler olarak da tanımlanır.

Verinin öğretide birden çok anlamı olduğu ve birden çok tanımlama yapıldığı görülmektedir. Kanun koyucu da veri kavramını; farklı yasal düzenlemelerde ve farklı tanımlamalarda kullanmıştır. 10.11.2005 Tarihli ve 5429 Sayılı Türkiye İstatistik

---

[1]Wikipedya**, Veri,** https://tr.wikipedia.org/wiki/Veri , e.t.: 30.08.2021.
[2] Gürol CANBERK, Şeref SAĞIROĞLU, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi**, 2006, Cilt:9, Sayı:3 https://dergipark.org.tr/, s. 166, e.t.: 30.08.2021.

Kanununun 2. maddesinde veri; anket veya idari kayıtlar yoluyla elde edilen nicel ve/veya nitel istatistiksel bilgiler şeklinde tanımlanmıştır[3]. 15.01.2004 Tarihli ve 5070 Sayılı Elektronik İmza Kanununda (EİK)[4] elektronik veri, elektronik, optik veya benzeri yollarla üretilen, taşınan ve saklanan kayıtları, 24 Mart 2016 Tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanunda (KVKK)[5] ise kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir[6].

Türk Dil Kurumu da veriyi birden fazla şekilde tanımlamıştır. Bir tanımında, *"Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli, biçimli gösterimi*[7]." olarak tanımlarken, diğer bir tanımlamada, *" bir araştırmanın bir tartışmanın, bir muhakemenin temeli olan, ana öğe muta, done."* açıklamasına yer vermiştir.

Çalışmanın konusu Bilişim Hukukuyla ilgili olduğu için, bu tanımlamalarda Bilişim Hukuku alanı ile ilgili olan verinin tanımının yapılması gerekmektedir. Veriyi en doğru şekilde; her türlü bilginin[8], bilgisayarda işlenebileceği, sonuçlar yaratabileceği ve gerektiğinde yeniden okunabilecek şekilde sayısal birimlere dönüştürülebilecek hali olarak tanılamak mümkündür[9].

Bu tanımı yaparken *"en doğru"* ifadesini kullanmamdaki neden; işlenebilecek bilgilerin, bilgisayarda işlenmesi ile sınırlı tutulmasıdır[10]. Çünkü günümüzde birçok teknolojik alet bilgisayar olmadığı halde, bilgiyi veri şekli ile depolayabilmektedir. Hafıza kartları, kredi kartları, harici depolama aygıtları bunlara örnektir. Bilgisayar olmadan da veriyi okuyabilen her hangi bir teknolojik aletle de bu veriler işlenebilmektedir. Türk Ceza Kanunun (TCK) Bilişim sistemine girme başlıklı 243. maddesinin 3. fıkrasında yer alan "*…sistemin içerdiği veriler yok olur veya değişirse,…"* şeklindeki düzenlemede yer alan *"veri"* kavramı; madde gerekçesinde

---

[3] 10.11.2005 Tarihli ve 5429 Sayılı Türkiye İstatistik Kanunu için bkz. **Resmi** Gazete, 18. Kasım2005, Sayı: 25997.

[4] 15.01.2004 Tarihli ve 5070 Sayılı Elektronik İmza Kanunu için bkz. **Resmi Gazete**, 23 Ocak 2004, Sayı: 25355.

[5] 24.04.2016 Tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanun için bkz. **Resmi Gazete**, 7 Nisan 2016, Sayı: 29677.

[6] Mehmet Can Karagöz, **Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemlerini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**, 1. Basım, İstanbul, Ekim 2020, On İki Levha Yayıncılık A.Ş., s. 27.

[7] **Türk Dil Kurumu Sözlüğünü,** https://sozluk.gov.tr/, e.t.: 30.08.2021

[8] Olgun Değirmenci, "**Bilişim Suçları**" Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı, İstanbul, 2002, S. 10.tez

[9] Murat Volkan Dülger, **Bilişlim Suçları ve İnternet İletişim Hukuku**, 8. Basım, Seçkin Yayınları, Ankara 2020, s. 76.

[10] Benzer görüş için bkz: *" Burada üzerinde durulması gereken bir başka nokta da verilerin yalnızca "bilgisayar verisi" olarak nitelendirilmesi hatalı olacaktır."* Dülger, s. 77.

"Sistem içindeki bütün soyut unsurlar fıkrada geçen veri teriminin kapsamındadır[11]*."* şeklinde açıklanarak geniş bir anlam katılmıştır[12].

En özet hali ile veriyi; bilişim sistemleri ile işlenebilen, kopyalanabilen, taşınabilen, depolanabilen, geri dönüştürülebilen, adlandırılabilen her türlü bilgi olarak tanımlamak mümkündür.

Gerek uluslararası hukukta gerekse ulusal hukukumuzda çok farklı kanunlarda ve farklı türlerde suç tiplerine konu olan ve Dijital veri hırsızlığı olarak değerlendirdiğim tüm fiillerin konusunu anlamlarını açıkladığım, ancak taşınır mal olup olmadığı tartışmaları halen süren dijital veriler oluşturmaktadır.

1.2. Dijital

Dijital terimi, Fransızca *"Digi"* ve *"tal"* kelimelerinden türemiştir. *"Digi"* Fransızcada sayısal anlamına gelmektedir. *"tal"* kelimesi ise Fransızcada *"ile ilgi"* anlamına gelmektedir[13]. Bu iki kelime birleşmesiyle dilimizde türeyen *"Dijital"* kelimesi *"sayı ile ilgili"* anlamına gelmekte olup, *"Sayısal"*[14] olarak tanımlanmaktadır. *"Sayısal"*, dijital kelimesi ile eş anlamlıdır.

Bilgilerin teknolojik aletler ile işlenmesi *"bit"*[15] adı verilen sayısal elektronik devre dizilimleri ile olmaktadır. Veriler bilgilerin sayısal birimlere dönüştürülmüş hali olarak tanımlamıştık. Bilgilerin dönüştürülmüş olduğu verilerin içerisinde bulunduğu ortam artık dijital bir ortam olacaktır. Bilgilerin veriler halinde işlenerek dijital ortama taşınması ile *"Dijital Veriler"* ortaya çıkmıştır.

Dijital veriler, çeşitli teknolojiler tarafından yorumlanabilen belirli makine dili sistemlerini kullanan diğer veri biçimlerini temsil eden bilgilerdir. Bu sistemlerin en temel olanı, karmaşık ses, video veya metin bilgilerini geleneksel olarak birler ve sıfırlar veya *"açık"* ve *"kapalı"* değerler olmak üzere bir dizi ikili karakterde depolayan ikili bir sistemdir. Dijital verilerin en güçlü yönlerinden biri, her türlü çok karmaşık analog girişin ikili sistemle temsil edilebilmesidir. Daha küçük mikroişlemciler ve daha büyük veri depolama merkezlerinin yanı sıra, bu bilgi

---

[11] Gerekçe için bkz. **TBMM, 22. Dönem, Yasama Yılı 2, Sıra Sayısı 664**, s. 640.
[12] Karagöz, s. 28.
[13] **Google Sözlük,** https://translate.google.com/ , e.t:10.09.2021.
[14] **Türk Dil Kurumu Sözlüğü,** https://sozluk.gov.tr/, e.t.: 30.08.2021.
[15] **Vikipedya, Bit,** https://tr.wikipedia.org/wiki/Bit_(bili%C5%9Fim), *"Programlamave haberleşmede, bir bit bilgi depolamave haberleşme veya bağlantının en küçük ve temel ünitesidir. Bir cihaz ya da fiziksel bir sistem tarafından depolanabilecek bilginin maksimum değeri normal olarak sadece 2 farklı şekilde bulunabilir. Bu durumlar genellikle (özellikle numerik veride) ikili sayılar 0 ve 1olarak yorumlanır."*e.t.: 10.09.2021.

yakalama modeli, işletmeler ve devlet kurumları gibi tarafların yeni veri toplama sınırlarını keşfetmelerine ve dijital bir ara yüz aracılığıyla daha etkileyici simülasyonları temsil etmelerine yardımcı olur[16].

En eski ilkel dijital veri tasarımlarından yeni, son derece sofistike ve büyük hacimli ikili verilere kadar, dijital veriler fiziksel dünyanın unsurlarını yakalamayı ve teknolojik kullanım için simüle etmeyi amaçlamaktadır. Bu, birçok farklı şekilde yapılır, ancak çeşitli gerçek dünya olaylarını yakalamak ve bunları dijital forma dönüştürmek için spesifik tekniklerle yapılır. Basit bir örnek, fiziksel bir sahnenin dijital bir görüntüye dönüştürülmesidir. Bu şekilde, yeni dijital veriler, fiziksel bir görüşü veya sahneyi kimyasal filme dönüştüren eski veri sistemlerine benzer. En büyük farklılıklardan biri, dijital verilerin görsel bilgileri bir bitmap'e veya pikselli bir haritaya kaydetmesidir; bu, her bit için belirli bir renk özelliğini kesin ve karmaşık bir ızgarada saklar. Bu basit ve temel veri aktarımı sistemi kullanılarak dijital görüntü oluşturuldu. Ses akışlarını dijital bir formda kaydetmek için benzer teknikler kullanılır[17].

Teknolojinin gelişmesi ile birlikte, bilgilerin veriler halinde işlenerek dijital ortama aktarımı kolaylaşmıştır. En basit hali ile örnek vermek gerekirse: telefon kamerası ile çekilen fotoğrafta, fotoğraf karesindeki görüntü, kamera vasıtasıyla telefonunuza aktarılıp, veri halinde telefon ekranına yansıtılması ile dijital bir veri elde edilmektedir. Bir ses kaydını; ses kayıt cihazı ile depolamak suretiyle, sesin işlenerek veriye dönüştürülmesi ve sonra da depolanarak dijital ortamda tutulması, dijital verilere örnek olarak gösterilebilir.

Bilgilerin dijital ortamlara aktarımının kolaylaşması ile birlikte kişilere ait dijital verilerin oluşturulması kolaylaşmış, ancak bu dijital verilerin oluşturulması kolaylaştıkça koruması ve muhafazası zorlaşmıştır. Oluşan ve toplanan dijital verilerin çeşitli bilişim programları sayesinde analizi ve incelenmesi kolaylamıştır. Binlerce veriyi saniyeler içerisinde analiz edebilen bilişim programları veri sahipleri hakkında çeşitli bilgilere kolayca erişmeyi mümkün kılmıştır.

1.3. Verilerin Dijital Ortama Taşınması

Bilgilerin elektronik ortamda işlenerek dijital verilere dönüştürülmesi, 1940'lı yıllara kadar dayanmaktadır. 1940-1959 yılları arasında Pensilvanya Üniversitesi Moore Elektrik Mühendisliği Okulunda bir grup bilim insanı, elektronik devrelere sahip, bilgi

[16]Techopedia Dijital Verileri Açıklıyor. https://tr.theastrologypage.com/digital-data e.t.: 23.01.2022.
[17] Dijital Veri Nedir? https://blog.ofix.com/dijital-veri-nedir/, e.t: 18.09.2021.

aktarımı yapabilen ilk teknolojik cihazı *"elektronik devrelere sahip ilk bilgisayarı"* üretmeyi başarmıştır[18].

Bu gelişmeyle birlikte, bilgilerin elektronik ortamlarda işlenmesi başlamış ve ilk dijital veriler oluşturulmuştur. Akabinde yapılan çalışmalar ile teknolojik gelişmeler hızlanmış, bununla beraber dijital verilerin kullanımı da kolaylaşmıştır. Dolayısıyla, gerçek ve tüzel kişiler, kendilerine ait bilgileri dijital ortamlara aktararak işlerinde verimi arttırmak, sosyal etkileşim de bulunmak, iletişimi kolaylaştırmak, reklamlarda strateji belirlemek, politikaların şekillenmesini sağlamak, para kazanmak gibi amaçlar ile hareket etmeye başlamıştır.

Dijital verilerin gerçek yaşamdaki kullanım yoğunluğu ve sıklığı; kültürel değişimlere, toplumun yapısal kökenlerine kadar etki de bulunmaktadır. Örnek vermek gerekirse:

-Sosyal medya kullanımı ile Twitter, İnstagram, Linked gibi sosyal medya araçlarında paylaşılan dijital veriler ile kitleleri etkileyebilir, yeni arkadaşlar edinebilir, iş arayabilirsiniz.

-Facetime, Zoom, Whatsapp gibi uygulamalarla dünyanın neresinde olursa olsun istediğiniz kişiler ile iletişim kurabilirsiniz.

-Kişisel banka kartları, sanal paralar ile yanınızda nakit para taşımadan, bir teknolojik cihazdan diğer bir teknolojik cihaza dijital verileri aktararak alışveriş yapılabilirsiniz.

-İnternette alışveriş için yapılan internet gezinmelerinin sonrasında, sürekli bakılan ürüne ilişkin reklam çıkmasının da dijital verilerin, analizi sonucu yapılan bir reklam çalışması olduğunu görebilirsiniz.

Kişilerin, kişisel verilerini[19] dijital ortamlara yüklemesi, kişisel verilerini dijital ortamlarda saklaması ve işlemesi günümüzde inanılmaz boyutlara ulaşmıştır. Verilerin günümüzde hangi boyutlara ulaştığına ve hayatımızın ne kadar önemli bir parçası haline geldiğine dair KirkBourne'un şu çarpıcı tespitlerine yer vermek isabetli olacaktır: İnsanlık tarihinin başlangıcından 2003 yılına kadar kayıt altına alınmış toplam bütün veri, beş milyar gigabayt *"exabayt"* civarında olarak tahmin

---

[18] Tunç Demircan, **Bilişim Alanında Suçlar**, 1. Basım, İstanbul Ekim 2016, Legal Yayıncılık, s. 10, atfen, Grolier International AmericanaEncylopedia, Sabah Yayınları, C. 3, İstanbul, s. 222.

[19] Mevzuat Bilgi Sistemi, **Kişisel Verilerin Korunması Kanunu,** https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5, 6698 Sayılı KVKK, 3.1/d maddesi, e.t: 02.09.2021.

edilmektedir. 2011 yılının başlangıcında, bu miktarda veri her iki gün içinde, 2013 yılında da her on dakikada üretilmiştir[20].

KirkBourne'un yaptığı bu tespitin üzerinden uzun bir süre geçtiği düşünüldüğünde, şu an bu rakamlar tahmin edilemez boyutlara ulaşmaktadır.

Bilgilerin elektronik aletler ile sanal ortamlara yüklenmesi ile sahip olunan dijital veriler, her geçen gün artmakta ve gelişen teknoloji ile de bunlara erişim ve kullanım kolaylaşmaktadır. Dijital verilerin aktarımının ve kullanımının kolaylaşması kadar bunların bilinçsizce kullanımı da artmaktadır.

Kişiler bilinçsiz olarak sanal ortamlara yükledikleri dijital verileri yaymakta, kendileri hakkında bilgi edinilmesinin kolaylaşmasına, kendilerine ait bu bilgilerin çeşitli şekillerde üçüncü kişilerin eline geçmesine sebep olmaktadır.

Sanal ortamların sağladığı anonimlik, tespit edilememe, bilgiye erişimdeki kolaylık, insanların iradesini kırma ve yanıltmanın kolay olması gibi faktörler ile bunlarla ilgili suç işlenmesini de kolaylaşmaktadır.

1.4. Dijital Ortamdaki Verilerin Güvenliğine İlişkin Sorunlar

Dijital veriler, bilgisayar virüsleri ve kötü amaçlı yazılımlar nedeniyle giderek büyüyen bir tehditle karşı karşıyadır. Çok sayıda, internette bireye ve kullanıcıya doğrudan veya dolaylı zarar veren birçok zararlı yazılım mevcuttur. Bu zararlı yazılımlar genel olarak *"Malware"* olarak adlandırılmaktadır. *"Malware"*; "Malicioussoftware"in kısaltılması olan virüsler, solucanlar, truva atları, trojanlar ve istenmeyen diğer kötü niyetli yazılımların genel adıdır[21].

Bilişim sistemi kullanıcılarının zararlı yazılımların yayılma tekniklerini bilmemesi, bu konuda kullanıcıların yeterli bilince sahip olmaması, her gün yeni sistemlerin ve zararlı yazılım tekniklerinin ortaya çıkması dijital verileri zararlı yazılımlara karşı çaresiz bırakmaktadır.

---

[20] Mesut Serdar Çekin, "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un BIG DATA (BÜYÜK VERİ) ve İrade Serbestisi Açısından Değerlendirilmesi" **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, 2016, Cilt 74, Sayı 2, s. 630, https://dergipark.org.tr/tr/pub/iuhfm/issue/28495/304076, e.t.: 02.09.2021;KirkBorne, Big Data, Small World: KirkBorne at TEDxGeorgeMasonU, https://www.youtube.com/watch?v=Zr02fMBfuRA

[21] **Zararlı Yazılımlar. (Virüs, Truva Atı, Solucan)** https://www.siberay.com/zararli-yazilimlar-virus-truva-ati-solucan, e.t: 18.09.2021.

1.4.1. Dijital Ortamdaki Verilere Karşı Gerçekleştirilen Suç Yöntemleri

Teknolojinin gelişmesi ile sürekli güncellenen bilişim sistemleri ve yazılımlar, kullanılan programlar her gün yeni bir suç yöntemini ortaya çıkarmaktadır. Bu nedenle dijital ortamdaki verilere karşı gerçekleştirilen yöntemlere ilişkin kesin bilgiler vermek doğru olmayacaktır. Ancak günümüzde dijital ortamdaki verilere karşı gerçekleştirilirken en sık kullanılan yöntemlerden bir kaç yöntemi teknik kısımlara girmeden, açıklamak gerekmektedir.

Zararlı yazılımların kişilere ait bilişim sistemlerini sızmaları sonucunda kişilerin bilişim sistemi içerisindeki dijital verilerinin kopyalayarak, veri sahibi gibi hareket etmesi veya veri sahibinin kişisel bilgileri ile üçüncü kişiler ile yaptığı iletişimi yasal olmayan şekilde öğrenebilmesi mümkündür. Bu durumda ayrıntısına aşağıda ayrıntısı ile değineceğimiz, Türk Ceza Kanununda (TCK)[22]yer alan bilişim sistemlerine ilişkin suçlar, özel hayatın gizliliği, kişisel verileri hukuka aykırı olarak kaydetme, yayma gibi suç tiplerinin failler tarafından gerçekleştirilmesinde kullanılmaktadır. Bilişim suçları ile mücadeleyi sağlamak ve yapılacak yasal düzenlemelerin tanımlamasını, unsurlarını, müeyyidesini belirlerken, bilişim suçlarında kullanılan yöntem ve sistemlerin failler tarafından nasıl kullanıldığını mümkün olduğunca iyi anlamak gerekmektedir.

1.4.1.1.Virüsler

Virüsler *"bilişim virüsleri"*, zararlı yazılımlar olarak nitelendirilmektedir[23].Virüsler kendilerini çeşitli yöntemler ile çoğaltıp, kopyalayarak başka sistemler üzerinde olumsuz etkiler yaratan yazılımlardır. Bu yazılımlar bilgisayar korsanı veya hacker denilen failler tarafından gerçekleştirilmektedir. Bu yazılımlar dijital verileri kopyalayabilmektedir. Dijital verilerin, rıza dışında üçüncü kişilerin kullanmasına, paylaşmasına sebep olabilmektedirler.

Örnek vermek gerekirse; 2016 yılı 21 Ekim tarihinde, tarihin en büyük siber saldırılarından biri gerçekleşmiştir. Amerika Birleşik Devletlerinde (ABD) gerçekleştirilen büyük çapta siber saldırıda Spotify, Netflix, WhatsApp, Amazon, PlayStation Network, TheVerge ve The New York Times gibi popüler internet sitelerinin / hizmetleri etkilenmiş sitelere giriş yapılamamıştır[24]. Bu siber saldırı ile ABD ile Rusya

[22]26.09.2004 Tarihli ve 5237 Sayılı **Türk Ceza Kanunu**, **Resmi Gazete** 12 Ekim 2004, Sayı: 25611.
[23] Karagöz, s. 98.
[24]WebTekno**, Dünyayı Yerinden Oynatan 21 Ekim Siber Saldırısı Hakkında Merak Edilenler**, https://www.webtekno.com/dunyayi-yerinden-oynatan-21-ekim-siber-saldirisi-hakkinda-merak-edilenler-h21469.html, e.t.: 01.12.2021.

arasında diplomatik krize neden olmuş ve ABD istihbaratına göre Amerika Birleşik Devletlerinde yapılan seçimin yönü Donald Trump lehine değişmiştir[25].

Gerçekleştirilen bu siber saldırılarda çeşitli yapılara sahip virüs dediğimiz zararlı yazılımlar kullanmıştır. Siber saldırıda kullanılan zararlı yazılımları ve bilişim sistemlerini anlamak, bilişim suçları ile mücadele etmenin temel noktasıdır.

1.4.1.2.Solucanlar

Solucanlar; bilgisayar ağları üzerinde hareket ederek kendisini bulunduğu bilişim sistemi içerisinde ve bir bilişim sisteminden diğerine kopyalayabilen bir yazılım türüdür. Solucanları, virüslerden ayıran en temel fark, bulundukları bilişim sistemine zarar vermeden de hareket edebilmeleri ve ağlar arasında hareket edebilme kabiliyetleridir[26].

Solucanlar, sürekli olarak diğer ağlara yayılma çabası içerisindedirler. Sahip olunan bilişim sisteminin ağ güvenliği zayıf ise rahat bir şekilde bu sistemi aşarak, üzerinde taşıdığı diğer zararlı yazımları bilişim sistemine bırakarak, diğer ağlara yayılmaya çalışmaya devam edebilirler.

Örneğin; bir solucan, e-posta adres defterindeki herkese kopyalarını gönderebilir ve sonra aynı şeyi gönderilen bilişim sistemleri içerisinde de yapabilir. Bu, domino etkisinin getirdiği yoğun ağ trafiği, iş yeri ağları ve internetin tümünü yavaşlatabilir[27]. Bu şekilde çok hızlı şekilde iletişim ağları ile bilgi sızıntısı olmaktadır.

1.4.1.3.Turuva Atı-Trojen Horse

Dijital verilerle ilgili olarak Truva Atı adı, Yunan Mitolojisindeki Truva Savaşından esinlenerek verilmiştir. Odysseus'un Truva surlarını aşmak için yaptırdığı tahtadan ata verilen addır. Truva atını iyi niyet olarak gören ve şehrin içine alan Truvalılar, atın içine saklanmış Akhalı askerlerin saldırısı ile yenilmişledir[28].

Truva Atı'nın çalışma mantığı da buna benzemektedir. Bilişim sistemine gönderilen veya yüklenmek istenen yararlı bir yazılımın içine gizlenen Truva Atı, yazılımın bilişim sistemine yüklenmesi ile bilişim sistemi içerisinde yer edinmektedir. Virüslerden ayıran

[25] BBC Türkçe, **2016 Gerçekleştirilen Siber Saldırılar**, https://www.bbc.com/turkce/haberler-38489376, e.t.: 01.12.2021.
[26] Dülger, **Bilişim Suçları**, s. 109; Karagöz, s. 102.
[27] Vikipedi, **Solucan Virüsü**, https://tr.wikipedia.org/wiki/Solucan_(vir%C3%BCs), e.t.: 10.09.2021.
[28] Vikipedi, **Truva Atı**, https://tr.wikipedia.org/wiki/Truva_At%C4%B1 , e.t.: 09.09.2021.

en temel özelliği, yaralı yazılımlar ile sisteme dahil olabilmeleridir. Bu sayede, bilişim sistemi sahibi farkında olmadan, bu yazılımı bilişim sistemine kurmuş olmaktadır.

Bilişim suçlarına konu birçok fiil, bu yazılım yoluyla gerçekleştirilmektedir[29]. Truva Atı bilişim sistemine girdikten sonra, bilişim sistemi içerisindeki dijital verileri kopyalayabilmekte, taklit ederek bilişim sistemi sahibinin davranışlarını sergileyebilmekte ve yaratıcısına bilişim sistemi içerisinde istediği gibi hareket etme kabiliyetini verebilmektedir.

Örneğin; bilişim sistemine yüklü kimlik ve kredi kartı bilgilerini çalmak için kullanılan tipik yazılım türüdür. Telefon ve tablet gibi uygulama indirilebilen bilişim sistemlerine uygulama ile birlikte inen ve kurulan, uygulamanın açılışını yavaşlatarak kendisini bu süre zarfında saklayan *"Trojandropper"* isimli Truva atı, diğer uygulamalar gibi hemen erişim izni istememektedir[30]. Bu sayede dikkat çekmemekte ve kendisini güvenlik programlarından da saklamaktadır. Uygun zamanı bekleyerek sıradan bir uygulama ile birlikte kendisi de erişim izni isteyerek sistem içerisindeki verileri yazılım sahibine veya belirlenen üçüncü kişilere aktarmaktadır.

1.4.1.4.Bukalemun

Bukalemun yazılımı, bilişim sistemine giriş şekliyle Truva Atına benzetmektedir. Ancak başarılı şekilde hazırlanmış Bukalemun yazılımlar, lisanslı yazılımları dahi başarılı şekilde taklit edebilmektedir[31].

Bukalemun yazılımları, bilişim sisteminin içine girip yerleştikten sonra, sistem içerisindeki tüm verileri toplamakta ve sonra kendi oluşturduğu gizli bir dosya içine kopyalamaktadır. Bu işlemleri yaptıktan sonra bilişim sistemi ekranına sistemin geçici süre ile kapatılacağı uyarısı ile sistemi kapatmaktadır[32].

Sistem kapandıktan sonra, Bukalemun yazılımını hazırlayan kişiye veya kişilere sistem içerisinde istediği verilere ulaşma imkanı tanımaktadır. Bu şekilde birçok veri hırsızlığı suçu işlenmektedir.

---

[29] Dülger, s. 104; ; Berrin Akbulut, **Bilişim Alanında Suçlar**, 2. Baskı, Ankara 2017, Adalet Yayınevi, s.79.
[30] Hürriyet, **Yakalanmamak İçin Gerçekmiş Gibi Davranan Truva Atı**, https://www.hurriyet.com.tr/teknoloji/yakalanmamak-icin-gercekmis-gibi-davranan-truva-ati-40652880 , e.t.: 01.12.2021.
[31] Karagöz, s. 105; Emine Doğan Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara, 1992, Doruk Yayınları, s. : 51; **Barış Emre Alp, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**, Ankara, 2018, Adalet Yayınevi s. 38.
[32] Dülger, s. 111,; Olgun Değirmenci/Caner Yenidünya, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, Legal Yayın evi, İstanbul, 2003, s. 104; Berrin Akbulut, **Bilişim Alanında Suçlar**, s.82.

Örneğin; Dünyanın en çok kullanılan arama sitesi Google' a ait tarayıcı olan Google Chrome internet tarayıcısının taklidini eden *"e- fast"* adında bir virüs tespit edilmiştir. Bu virüs yapısal olarak bukalemun virüsü özelliği taşımakta olup sisteme kendisini Google Chrome gibi tanıtarak Google Chrome tarayıcısının yerine geçmektedir. Kendisini tercih edilen tarayıcı olarak ayarlayarak kullanıcını fark etmeden tüm bilgilerini kaydetmekte ve kopyalamaktadır[33].

1.4.1.5.Salam Tekniği

Salam tekniği; özellikle para hareketlerine ilişkin bilişim sistemlerinde, hukuka aykırı şekilde yarar sağlama amacı ile kullanılan bir yazılım türüdür[34].

Salam yazılımı sızdığı banka ve benzeri sistemler içerisinde önemsiz derecede görülen miktarlarda, hesap sahibi ve bilişim sahibi sisteminin onayı olmadan emrinde olan kişinin belirlediği hesaplara para aktarımı yapmaktadır.

Salam tekniği genellikle Truva Atlarının içerisinde gizlenerek sisteme girmektedir[35]. Sisteme girdikten sonra harekete geçen Salam yazılımı kendisine verilen komutlar doğrultusunda, bilişim sisteminde yer alan hesaplarda ondalık oranında, çok az miktardaki hesapları yazılım sahibi lehine olacak şekilde yuvarlayarak, yuvarlanan kısımdaki miktarı yazılım sahibinin hesabına geçirmektedir.

Tespiti zor bir yazılım türü olması, aktardığı para miktarının mikro rakamlar olması, sistem içerisinde tespit edilinceye kadar failin çalınan miktarı kripto paralar veya takip edilemeyen ada ülkelere aktarılarak kullanmasını sağladığı için bilişim korsanlarının tercih ettiği bir sistemdir.

1.4.1.6.Fidye Yazılımı

Fidye yazılımları; Truva Atı, Bukalemun yazılımları gibi yazılımlar ile sistem içerisine girerek, bilişim sistemi sahibinin dosyalarını şifrelemeyi amaçlamaktadır. Fidye yazılımı genel olarak bilişim sahibine mail, yararlı bir link veya cazip bir reklam gibi sunulmaktadır. Bilişim sistemi sahibi bu linki açtığı zaman Fidye yazılımı bilişim sistemine dahi olur[36].

---

[33]Shifdelete, **Chrome'u Silen Zararlı Yazılım**, https://shiftdelete.net/chrome-silen-zararli-yazilim-efast-browser-64976, e.t.: 01.12.2021.
[34] Dülger, s. 105.
[35] Karagöz, s. 106. ; Levent Kurt, **Açıklamalı ve İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Tük Ceza Hukukundaki Uygulaması**, 1. Baskı, Ankara 2005, Seçkin Yayınevi s. 67.
[36] Dülger, s. 122.; Karagöz, s. 106.

Kripto paraların kullanımının artması ve takip edilmesinin zorlaşması, Fidye yazılım sahiplerinin istediği fidyelerin sistemi ele geçirilen kişiler için özellikle şirketler makul görülmesi ve yazılım sahiplerinin fidye ödendikten sonra şifreleri vermesi, bu saldırılara maruz kalanların fidye ödemeyi tercih etmesine sebep olmuştur. Bu durum Fidye yazılımını popüleştirmektedir.

Örneğin; ABD' de yüzlerce şirketin internet sitesine Rusya bağlantılı bir hacker grubu tarafından siber saldırı düzenlenmiştir. Düzenlenen saldırıda şirketlerin sitelerine erişimini engelleyen yazılım ile yetmiş milyon dolara karşılık gelecek şekilde fidye istemiştir. Saldırıyı üstlenen hacker grubu fidye yazılımını, gerçek bir güncelleme gibi gönderilen bir bildirim içerisine kamufle edilmiş zararlı yazılım sayesinde yerleştirdiğini bildirmiştir[37].

1.4.2. Teknolojinin Kullanımına İlişkin Sorunlar

Teknolojideki hızlı gelişmeler; bilişim sistemlerinin kullanımını her geçen gün kolaylaştıran yenilikler, dijital ortamdaki veri çokluğu, bununla birlikte gelen bilinçsiz kullanım, dijital verilere ilişkin suçlarda, suça konu eylemlere maruz kalmayı kolaylaştırmaktadır. Dolayısıyla, bu durumlarda pek sorun ortaya çıkmakta ve bu sorunların giderilmesi amacıyla da yeni teknikler geliştirilmeye çalışılmaktadır. Örneğin; telefonlardaki çocuk modları, internet yayıncılarının çocuklara özel kilitleri teknolojiyi kullanırken çocukların daha güvenli kullanmasına ve siber zorbalığa maruz kalmaması için geliştirilmiş bir yöntemdir.

1.4.2.1.Bilinçsiz İnternet Kullanımı

İnternet ortamı bilinmeyen bir deniz, bilişim sistemleri ise bu denizde yer alan gemiler gibidir. İnternetin hangi zamanlarda, hangi araçlarla kullanıldığına, gezinilen sayfalara, kullanılan linklere dikkat edilmez ise her an kullanıcılara zarar vermesi olasıdır.

Kaynağı bilinmeyen linklerin açılması, e-postalara gelen maillerin açılması, bilişim sistemlerini zararlı yazılımlara karşı koruyucu yazılımların kullanılmaması, kişisel alanlarda ve kişisel hesaplarda kullanılan şifrelerin basit algoritmalar içermesi, en büyük tehlikeler arasında yer almaktadır.

---

[37]DW MadeForMinds, **ABD Hacker saldırısı 70 Milyon Dolarlık Fidye Talebi**, https://www.dw.com/tr/abdde-hacker-sald%C4%B1r%C4%B1s%C4%B1-70-milyon-dolarl%C4%B1k-fidye-talebi/a-58165310, e.t.:01.12.2021.

Kaynağı bilinmeyen bu içeriklerin açılması ile birlikte, kullanılan bilişim sistemlerine giren zararlı yazılımlar, bilişim sistemlerini veya bilişim sistemlerinde yer alan verileri kullanarak, kullanımını engelleyerek, kopyalayarak mağduriyet yaşatabilmektedir.

İnternet ortamında sosyal medyalarda hiç kimse görmeyecek inancı ile yapılan yazışmalar, sosyal medyaya yüklenen kişisel bilgileri kısaca bilinçsiz şekilde veri paylaşmak, bilişim sistemine giren zararlı yazılımlar neticesinde ifşa olabilmekte, başkaları tarafından ele geçirilen kişi adına kullanılabilmektedir.

1.4.2.2.Koruyucu Yazılımların Kullanılmaması

Zararlı yazılımları önlemek üzere çok sayıda koruyucu yazılımlar vardır. Bu yazılımların; bilişim sistemine dışarıdan gelen tehditleri engellemek, yok etmek gibi görevleri bulunmaktadır. Koruyucu yazılımlar genel olarak Güvenlik Duvarı[38] ve Antivürs Programları [39] olmak üzere ikiye ayrılmaktadır.

Güvenlik duvarı, bilişim sistemine giren çıkan verilerin trafiğini kontrol eden genel bir koruyucu yazılımdır. Sistem içerine giren anormal ve hatalı gördüğü yazılımları tespit ederek bilişim sistemi sahibini uyarmakta ve kendisine verilen komuta göre şüphelendiği verilerin girişini engelleyebilmekte, yok edebilmekte veya karantina altına alabilmektedir.

Antivirüs programları ise daha özel ve gelişmiş yazılımlar olup bilişim sistemi içerisine giren belirli zararlı yazılımlara özgülenebilen bir yazılım türüdür.

İyi hazırlanmış bir Turuva Atı zararlı yazılımını, güvenlik duvarı fark edemeyebilmektedir. Ancak bilişim sisteminde yer alan ve Truva Atı veri tabanını tarayabilen bir Antivirüs bu yazılımı tespit edip engelleyebilmektedir.

Koruyucu yazılımlarda önemli olan, bu yazılımların güncel tutulması ve lisanslı [40]olmasıdır. Gelişen yazılım sistemleri ile her gün sayılamayacak kadar zararlı yazılım internet ortamına bırakılmaktadır. Koruyucu yazılımların da sürekli olarak güncel tutulması ve zararlı yazılımlara karşı önleyici görevini yerine getirmesi gerekmektedir.

---

[38]Vikipedi, **Güvenlik Duvarı,** https://tr.wikipedia.org/wiki/G%C3%BCvenlik_duvar%C4%B1, e.t.:13.09.2021.

[39] Bilişim Teknolojileri,**Antivirüs**, https://it.bilgi.edu.tr/tr/guvenlik/antivirus/, e.t.:13.09.2021.

[40] *"Üreticisi tarafından, kullanımına dair belge düzenleyen devlet makamı tarafından, belgelemeyi düzenlemeye yetkili kılınmış makamlar tarafından telifli olduğu belgelenmiş ise nesnenin kullanımı, geliştirilmesi, yeniden yapılandırılması, değiştirilmesi, alıntısının yapılabilmesi gibi hususları belirleyen belgeye yazılım lisansı denir."* Vikipedi, **Yazılım Lisansı**, https://tr.wikipedia.org/wiki/Yaz%C4%B1l%C4%B1m_lisans%C4%B1, e.t.:13.09.2021.

1.5. Dijital Verilerle Elde Edilen Bilgilere Olan Talep

İnsanlık varoluşundan bu yana birçok aşama geçirmiştir. Günümüzde ise insanlar bilgi çağında yaşamaktadır. Bilginin önemi, ekonomik ve küresel güç kazanımı başta olmak üzere birçok alanda artış göstermektedir.

Teknolojinin ve bilişim sistemlerinin gelişimi ile bilgiye erişme süresi ve yolları kısalmıştır. Bilişim sistemlerinin hızla gelişmesi ve bilişim sistemlerinin kullanımının yapay zeka[41] yazılımları ile kolaylaşması, depolama kapasitesinin artması ile birlikte kişilere ait bilgilerin dijital ortamlara aktarımında inanılmaz bir artış görülmüştür.

Kişisel verilerin dijital ortamlara yüklenmesine bu verilerin işlenmesi ile kişiler hakkında bilgi bankaları yapılmaya başlanmıştır. Bu verilerin çokluğu, özellikle şirketler ve devletler tarafından veri sahiplerinin rızasını alarak veya rızası dışında olmak üzere birçok amaçla kullanılır vaziyete gelmiştir. Bu amaçların başında reklamların yönelmesi gibi ekonomik faaliyetler, devletlerin politikasının belirlemesi ve verileri rıza dışı ele geçirenlerin çeşitli nedenlerle yarar sağlaması için kullanmaları gelmektedir.

1.5.1. Dijital Verilerin Reklam Amacıyla Kullanımı

> *"Reklam, 'insanları gönüllü olarak belli bir davranışta bulunmaya ikna etmek, belirli bir düşünceye yöneltmek, dikkatlerini bir ürüne hizmete, fikir ve kuruluşa çekmeye çalışmak, onunla ilgili bilgi vermek, ona ilişkin görüş ve tutumlarını değiştirmelerini veya belirli bir görüşü ya da tutumu benimsemelerini sağlamak amacıyla oluşturulan; iletişim araçlarından yer ya da süre satın almak yoluyla sergilenen ya da başka biçimlerde çoğaltılıp dağıtılan ve bir ücret karşılığı oluşturulduğu belli olan (diğer bir deyimle parasal destek sağlayan kişi ya da kuruluşların kimliği açık olan) duyuru'dur*[42] *"*

Reklamın tanımından da anlaşıldığı üzere kişiler üzerinde etki yaratmayı amaçlayan bir iletişim biçimidir. Kişiler üzerinde etki en şekilde nasıl yaratılır? Tabii ki, kişiler hakkında bilgi sahibi olur, edinilen bilgiler ile kişilerin ilgi alanına göre reklam yapılır. Kişiler hakkında bilgi sahibi olmak için en iyi yöntem, bilgiye ulaşmanın en kolay yöntemi olan dijital ortamlarda bulunan verilerin toplanmasıdır.

---

[41] Harun Pirim, "Yapay Zeka", **Yaşar Üniversitesi E Dergisi**, https://dergipark.org.tr/tr/pub/jyasar/issue/19113/202842, 2006, *"Yapay zeka bağımsız makineler-bu makineler insan olmaksızın kompleks işler yapabilir-inşa etmek için araştırma yapan bilişsel bilim dalıdır. Bu hedef makinelerin düşünmesini ve anlamasını gerektirir. Bu konuda akıl almaz ilerlemeler sağlanmışsa da hedefe bakıldığında hayal gibi gözükmektedir."* , e.t.:13.09.2021.

[42] Vikipedi, **Reklam**, https://tr.wikipedia.org/wiki/Reklam, e.t.: 14.09.2021

İnternet üzerinde Google internet sitesinde, örnek olarak verilmiştir, başka arama motorları da olabilir, alış-veriş yapmak için aranılan bir içeriğin veya araştırılan bir içeriğe ilişkin reklamların, internette gezinildiği sırada aniden görünmesinin sebebi, Google'ın yapay zekâsının arama yapan kişinin arama verilerinden yola çıkarak oluşturduğu algoritma ile reklam anlaşması yaptığı firmaların reklamlarını yönlendirmesidir.

Bu yöntemle hedefine daha etkili ve daha isabetli ulaşan bir reklam yapılmaktadır. İrlanda'nın Data Protection Commission-Veri Koruma Komisyonu-DPC tarafından yapılan bir araştırmada, kurumun baş politika sorumlusu Johnny Ryan tarafından Google'ın konum, arama geçmişi gibi verileri reklam verenleri ile paylaştığına ilişkin somut deliller ileri sürdüğü iddia edilmiştir[43].

1.5.2. Dijital Verilerin Politik Amaçlar İle Kullanımı

Devletler güçlerini arttırmak, iktidarlarını güçlendirmek ve halkı yönetmek için çeşitli yöntemlere başvurmuşlar ve başvurmaktadırlar. Bu yöntemlerden en önde gelenlerden biri de geçmişten günümüze kadar gelen bilgi toplamaları olmuştur. Bunlara örnek olarak; Osmanlı Döneminde padişahın, halkın arasına tebaadanmış gibi giyinerek karşıması, Teşkilatı Mahsusa gibi istihbarat teşkilatlarının kurulması gösterilebilir. Osmanlının yıkılış döneminde de Arabistan Yarım Adası'nda Arap toplumlarının Osmanlıdan kopması için çalışmalar gösteren İngiliz Ajan Thomas Edward Lawrence da[44] bilgi toplamak, toplumu analiz etmek ve isyan başlatmak için bu verileri kullanması yine somut örneklerdendir.

Gelişen teknoloji ve bilişim sistemleri ile toplum yapısı ve kültürler değişmeye başlamıştır. Kişilerin sosyal ilişkiler kurma ve kendilerini tanıtma yöntemleri dijitalleşmiştir ve bu değişim devam etmektedir. Değişen bu yapı ile birlikte, devletlerin kişiler hakkında bilgi toplama araçları ve yöntemleri de değişiklik göstermektedir. Devletler politikalarını belirlemek, güvenliğini sağlamak gibi nedenler ile kişilere ait dijital verilere, hukuki veya hukuka aykırı olarak da olsa erişmeye çalışmaktadır.

---

[43]Gündem Kıbrıs, **Google Tüm Kişisel Verilerimizi Sattı**, https://www.gundemkibris.com/teknoloji/google-tum-kisisel-verilerinizi-satti-h281173.html, e.t.: 17.09.2021.

[44]Salâhi R. Sonyel, **Lawrence Haşimi Araplarını Osmanlı İmparatorluğu'na Karşı Ayaklanmaları İçin Nasıl Aldattı (İngiliz Gizli Belgelerine Göre), Türk Tarih Kurumu**, https://www.ttk.gov.tr/belgelerle-tarih/lawrence-hasimi-araplarini-osmanli-imparatorluguna-karsi-ayaklanmalari-icin-nasil-aldatti-ingiliz-gizli-belgelerine-gore/, e.t.:17.09.2021.

Siyasi partilerin devletlerde iktidara gelme amacıyla kitlelerin oy davranışları ve tercihleri ile ilgili bilgi edinilmesi için yaptığı kamuoyu araştırmaları[45], kişisel verilere erişimin kolaylaşması ile bireyselleşmeye başlamıştır.

Amerika Birleşik Devletleri (ABD) Başkanı Obama, 2008 seçimlerinde, seçmenlerden toplanan verilere göre veri tabanı oluşturmuş ve sekizyüz farklı oy verme potansiyeline sahip grup belirleyerek bu gruplara yönelik mikro hedefleme yaparak bir seçim kampanyası yürütmüştür[46].

Bu seçim stratejisi, yasal olsa da tüm stratejiler bu şekilde değildir. Örneğin, bu durum gayri yasal *"Facebook–Cambridge Analytica veri skandalı"* olarak bilinen olayda yaşanmıştır. Bu olayda 2014 yılında yaklaşık elli milyon Facebook sosyal paylaşım sitesi kullanıcısının kişisel bilgilerinin, seçmenlerin fikirlerini politikalarda kullanmak için toplandığı ortaya çıkmıştır.

Kullanıcılara ait bu verilerin, şirketler tarafından satıldığı ve siyasetçiler tarafından satın alındığını ortaya çıkmış ve Facebook sosyal paylaşım sitesi bu durum üzerine özür dilemek zorunda kalmıştır[47].

1.5.3. Dijital Verilerin Suç İşlemeyi Kolaylaştırmak Amacıyla Kullanımı

Dijital ortamda işlenen suçların gün geçtikçe failler tarafından daha cazip hale gelmesinin temelin de kişilerin dijital platformda daha kolay şekilde yanıltılması ve iradelerinin kırılması, failin anonim şekilde suça konu eylemi gerçekleştirebilmesi ve bulunmasının zorluğu gibi nedenler bulunmaktadır. Her geçen gün gelişen teknoloji ise suça konu eylemlerin sürekli olarak değişmesine neden olmakta ve suç tiplerinin ve yapılarının anlaşılıp önlem alınmasını zorlaştırmaktadır.

Dijital ortamda suç işlenirken genellikle dört aşamadan geçilmektedir. Bilgi toplama, Sızma, Kalıcılığı Sağlama, İzleri Yok Etme'dir.[48] Özellikle, bilgi toplamak, bilişim sistemine girmek-sızmak, sistemde fark ettirmeden kalmak ve en son olarak da izleri silerek hareket etmek, dijital verilere karşı suç işlemeyi kolaylaştırmıştır.

---

[45] Ilgar Seyidov, " Büyük Verinin Gücü Adına: Siyasi Kampanyalarda Etkili Veri Kullanımı", **TRT Akademi**, https://doi.org/10.37679/trta.802534, e.t.: 17.09.2021.
[46] Seyidov, s. 39.
[47] Vikipedi, Facebook**–Cambridge Analytica veri skandalı**, https://tr.wikipedia.org/wiki/Facebook-Cambridge_Analytica_veri_skandal%C4%B1, e.t.:17.09.2017.
[48] Karagöz, s. 96.

1.5.3.1.Bilgi Toplama

Zararlı yazılımlar, dijital verilerin havuz haline getirilmesi ve bu verileri elde tutan şirketlerin bunları kar amaçlı kullanması, bilişim sistemine aşırı denebilecek dijital veri yüklenmesi, kişiler hakkında bilgi toplanmasını ve bu bilgilerin failler tarafından kullanılmasını kolaylaştırmıştır.

Bilgi toplama işlemi içinde, her gün yeni yöntemler ortaya çıkmaktadır. Örneğin *"Shodan"* adlı internet sitesi bilgi toplama işleminde, suç gerçekleştirmek isteyen failler tarafından veya bilişim güvenliği uzmanları tarafından da kullanılan, "Google" gibi tarayıcı niteliği taşıyan bir arama motorudur[49].

Shodan arama motorunun diğer arama motorlarından temel farkı, interneti açık olan bilişim sistemlerinin de taranabilir olmasıdır. Yani veri paylaşımınız bilinçli ya da bilinçsiz olarak internete açık ise shodan arama motoru ile yaptığınız bir arama işleminde verileri internete açık olan bilişim sistemlerine de erişiminiz mümkün olmaktadır.

1.5.3.2.Bilişim Sistemine Sızma

Kişilerin sürekli olarak bilgiye erişmek amacıyla bilişim sistemlerini kullanmaları ve bu kullanılmaları bilinçsizce gerçekleştirmeleri sonucu, zararlı yazılımların açık hedefi haline gelmeleri, bilişim sistemlerine sızmayı kolaylaştırmıştır.

Bilişim sistemine sızdıktan sonra, toplanan dijital veriler ile veri sahibinin zayıf yönleri tespit edilebilmekte veya iradesinin yanıltılması kolaylaşabilmektedir. Örnek vermek gerekirse, bilişim sistemine bir şekilde link tıklama veya yararlı olduğu düşünülerek yüklenen bir yazılımdan, zararlı yazılım ile her hareket yazılım sahibi tarafından izlenebilir. Daha sonra, bu veriler ile şantaj yapılabilir veya bilgiler aktarılıp güven oluşturularak dolandırıcılık suçu işlenebilir.

En çok karşılaşılan yöntemlerden biri; failin iletişim sistemleri ile mağdur ile bir araya gelmeden kurduğu iletişim üzerinden dolandırılmasıdır. Fail, mağdur hakkında çeşitli yollardan bilgi topladıktan sonra kendisini mağdurun etkilenebileceği şekilde konuşmalar gerçekleştirerek, çeşitli vaatler ile mağdurdan kazanç elde edilmesi yoluyla

[49] **Search Engine forthe internet of everythink,** https://www.shodan.io/ e.t. 17.09.2021.

olmaktadır. Burada fail mağduru etkilemek için mağdur hakkında bilgiyi bilişim sistemleri ve internet ortamı üzerinden edinmektedir[50].

1.5.3.3.Kalıcılık Sağlama

Sistem içerisine giren ve sürekli orada kalmak isteyen zararlı yazılım sahipleri, yarattıkları yazılımla sisteme fark edilmeden girip çıkmayı amaçlamaktadırlar. Böylece, sistemin güvenlik yapısı zararlı yazılımı fark edemediğinden buna engel olamamaktadır.

Bilişim sistemine sızan zararlı yazılım, istediği zaman bu sisteme girip istediği verileri alıp çıkabilecektir. Bu eyleme *"sisteme sahiplenme"* eylemi denilmektedir[51].Yukarıda değindiğimiz salam tekniği ile banka hesaplarının soyulması bu durumun en tipik örneklerindendir. Bu sistem de genellikle failin, mağdur üzerinden edindiği veriler ile veya mağdura fark ettirmeden mağdura ait bilişim sistemi üzerinden kendisine kazanç sağlamak amacı ile gerçekleştirilen bir yöntemdir.

1.5.3.4.İzleri Yok Etme

Zararlı yazılımların kodlanması da kendi içerisinde karakteristik bir yapıya sahiptir. Bu yapı, bilişim uzmanları tarafından incelenip zararlı yazılım sahibi hakkında bilgi verir[52]. Bu inceleme, zararlı yazılım sahibi faili tespit etmekte ve kriminal profilini çıkarmaya yaramaktadır. Bilişim sistemindeki bu izler, bir daha aynı tür saldırı olmaması için de tespit edilip engellenmeye çalışılmaktadır.

Bilişim suçlarına ilişkin failler, bu nedenle tespit edilmemek için çeşitli yöntemler izlemekte, yaratıkları zararlı yazılımları bu doğrultuda programlamaktadır. Bazı zararlı yazılım karşıtı yazılımlar, zararlı yazılımları engellemekle kalmamakta, izledikleri yolları da tespit etmeye çalışmaktadır.

Bu nedenlerle zararlı yazılım sahipleri, izlerini yok etmek için büyük çaba sarf etmekte ve zararlı yazılımların analizlerini ve takibini zorlaştıran kodlamalar yapmak veya sunucu değiştirmeye yarayan programlar kullanmaktadır.

---

[50] Hürriyet**, Her şey Yunanistan'dan gelen bir mesajla başladı! 1,2 derken 300.000 lirasından oldu**, https://www.hurriyet.com.tr/ekonomi/yunanistandan-turkiyeye-evlenme-vaadiyle-dolandiricilik-engelli-vatandasi-boyle-kandirdilar-41220628, e.t.:01.12.2021

[51]Hamza Elbahadır, **Hacking Interface,** 10. Baskı, İstanbul 2016, Kodlab Yayınevi, s. 225.

[52] İlker Kara, "Türkiye'de Zararlı Yazılımlar ile Mücadelenin Uygulama ve Hukuki Boyutunun Değerlendirilmesi", **Akademik Bakış Dergisi**, https://dergipark.org.tr/tr/pub/abuhsbd/issue/32946/366098, s. 91, e.t.: 17.09.2021.

En sık karşılaşılan yöntem olan sunucu değiştirmeye yarayan programlar özellikle kişilerin bulunduğu ülkede kamu otoritesi tarafından erişim engeli bulunan siteleri kullanmak için kullanılan yazılımlardır. Bu yazılımlar kullanılan internetin sinyalini yurt dışına göndererek oradaki sunucular aracılığı ile tekrar erişimi engellenen sitelere erişimi mümkün kılmaktadır. Örneğin; 20 Mart 2014 Tarihinde İstanbul Anadolu 5. Sulh Ceza Mahkemesinin 204/181 Sayılı kararı ile Twitter sosyal paylaşım sitesine erişim engellenmiştir[53]. Birçok kullanıcı bu engelin ardından Twitter sosyal paylaşım sitesine ulaşmak için çeşitli sunucu değiştirme programlar kullanmıştır. Kullanılan bu programlar ile bilişim sisteminin internete bağlandığı ağı ülke dışına yönlendirerek istenilen işlemleri yönlendirilen internet sitesi üzerinden yapılabilmektedir. Ağ bağlantılarının internet üzerinden çeşitli ülkelere ve farklı sunuculara yönlendirilmesi nedeni ile kullanıcının internet üzerinde gerçekleştirdiği işlemleri nereden gerçekleştirdiğinin tespit edilmesini engellemektedir. Failler internet üzerindeki ağ ayarlarını değiştirerek, gerçekleştirdikleri suça konu eylemlerden sonra bulunmayı neredeyse imkansız hale getirmektedir. Bu durum bilişim suçlarında failin belirlene bilirliği engellemektedir.

[53]Vikipedi, **Twitter'a Türkiye'den Erişim Engellemesi**, https://tr.wikipedia.org/wiki/Twitter%27a_T%C3%BCrkiye%27den_eri%C5%9Fimin_engellenmesi#cite_note-7, e.t.: 01.12.2021.

İKİNCİ BÖLÜM

DİJİTAL VERİ HIRSIZLIĞI, DİJİTAL VERİ HIRSIZLIĞININ KONUSU OLAN BAŞLICA YASAL DÜZENLEMELER

Çağdaş dünyada, veri hırsızlığı sanal dünyanın başlangıcından itibaren zaman zaman dijital dünyada gerçekleşen en büyük siber suçlardan biri haline gelmiştir. Dijital gelişmelerin hızlı büyümesiyle birlikte, dijital veri hırsızlığı sanal dünyayı ele geçirmiş ve sayısız kişi, şirket, kamu kurum ve kuruluşları profesyonel alanlarında bu saldırılara maruz kalmıştır. Buna karşın, digital verilerin hukuka aykırı bir şekilde ve değişik yöntemlerle ele geçirilmesi ve bunların farklı alanlarda farklı amaçlarla kullanılması ile ilgili olarak somut bir kavram geliştirilmemiş ve suç olarak düzenlenmemiştir. Gerek yabancı hukuklarda gerekse ulusal hukukumuzda bu yönde doğrudan bir düzenleme olmamasına karşın, genelde bu tür fiiller, *"veri hırsızlığı" veya "bilişim sistemlerinin araç olarak kullanıldığı suçlar "* olarak dillendirilmektedir. Bununla birlikte, genel olarak veri hırsızlığı, gizliliği tehlikeye atmak veya gizli bilgileri elde etmek amacıyla bilinmeyen bir kurbanın bilişim sisteminde, sunucularında veya elektronik cihazlarında depolanan dijital bilgilerin çalınması fiili olarak tanımlanabilmektedir[54]. Ancak dijital olmayan yani sanal ortam içerisinde yer almayan verilerin de var olduğu düşünüldüğün de " veri hırsızlığı " kavramı dijital olmayan verileri de kapsayacağından istenilen tanıma tam uymamaktadır. Burada " veri" den kastedilenin sanal ortamlarda yer alan dijital veriler olduğunu görülmektedir.

Yine, *"veri hırsızlığı"*nın, dolandırıcıların veya bilgisayar korsanlarının, herkese açık olarak paylaşılması amaçlanmayan belirli hassas ve özel bilgileri yasa dışı erişim yoluyla elde etmeleri şeklinde ortaya çıkan siber suçlar olarak da belirtildiği görülmektedir. Başka bir anlatımla, *"veri hırsızlığı"*, daha sonra etik olmayan bir şekilde kullanılan ve sonunda büyük kuruluşlara zarar veren bilgilerin çalınması anlamında da değerlendirilmektedir[55].

Diğer taraftan, veri hırsızlığı kavramı genel olarak sıklıkla kullanılmakla birlikte, verilerin değişik yöntemlerle ele geçirilmesi fiili, *"veri ihlali"* olarak da

[54] A DEFINITION OF DATA THEFT, https://digitalguardian.com/blog/what-insider-data-theft-data-theft-definition-statistics-and-prevention-tips, e.t.: 14/02/2022
[55] What Is Data Theft? **A Simple Explaination in 4 Points (2021)**, https://www.jigsawacademy.com/blogs/cyber-security/data-theft, e.t.: 14/02/2022

kullanılmaktadır[56]. Kanımca, bu tür fiillerin tümünü birden veri hırsızlığı kavramı altında toplayarak, yasal düzenlemelerin yapılması gerekmektedir. Bu nedenle, çalışmada kavram olarak *"veri hırsızlığı"* kullanılacaktır.

Değişik yöntemlerle ele geçirilen-çalınan bilgiler, kredi kartı numaraları veya banka hesapları gibi finansal bilgilerden sosyal güvenlik numaraları, ehliyet numaraları ve sağlık kayıtları gibi kişisel bilgilere kadar her şeyi içerebilmektedir. Bu nedenle, veri hırsızlığı tüm dünyada büyüyen bir sorun haline gelmiştir. Bir zamanlar sadece büyük işletmelerin ve kuruluşların sorunu olan veri hırsızlığı, günlük bilişim sistemi kullanıcıları için giderek büyüyen kişisel verilerin her alanına yayılan bir sorun olarak ortaya çıkmıştır. Dolayısıyla, veri hırsızlığı yalnızca küçük bir dijital suçu ifade etmemekte, aynı zamanda kimlik sahtekarlığı ve kimlik hırsızlığına da yol açabilecek suçlardan biri olarak da ortaya çıkmaktadır[57].

Veri hırsızlığının çoğu, şirket veri ihlalleri yoluyla gerçekleşmektedir. Ponemon Institute Raporu, ABD'ndeki tüm şirketlerin yüzde 43'ünün 2013'te en az bir veri ihlali yaşadığını belirlemiştir. Bazı veri ihlalleri, siber korsanlardan kaynaklanmaktadır. ABD'de 2016 yılında da yaklaşık 12,7 milyon kaydın açığa çıkmasına neden olan 450'den fazla veri ihlali yaşandığı ve tüm veri ihlallerinin yaklaşık yüzde 80'i çalışanların ihmalinden kaynaklandığı tespit edilmiştir.

İşletmeler ve kuruluşlar genellikle veri hırsızlığının hedefidir, ancak mağdur olanların çoğunluğu müşterilerdir. Örneğin, 2014 yılında ABD'de 56 milyondan fazla kişinin kredi kartı bilgileri Home Depot'ta çalınmıştır. Benzer bir sorun, Target'ta da yaşanmıştır. Bu bilgilerin daha sonra çoğu kurbanın haberi olmadan çevrimiçi mal satın almak için kullandığı *"Darknet"*te satıldığı öğrenilmiştir[58].

Diğer taraftan, nadiren karşımıza çıkabilen bir kriz olan COVID-19 salgının tüm dünyada hayatımıza girmesiyle birlikte, dijital dönüşüm de hızlanmıştır. Dolayısıyla kişilerin ve şirketlerin saldırı yüzeyleri de genişlemiştir. Bunun sonucu, dikkatler ve kaynaklar hayati öneme sahip güvenlik projelerinden uzaklaşarak sağlık sorunlarına yönelmiştir. ABD'de New York'da kurulu ve Dünyanın en büyük bilişim teknolojisi şirketi olan Uluslararası İş Makineleri-International Business Machines (IBM)

---

[56] Lillian Ablon ve Kathryn Kuznitsky, https://www.rand.org/blog/2016/10/digital-theft-the-new-normal.html, e.t.: 14/02/2022

[57] Katelyn Michaud, **What Is Data Theft?MPH, BSc Biochemistry**, https://safety-lovetoknow-com.translate.goog/personal-safety-protection/what-is-data-theft?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=sc

[58] Katelyn Michaud**, What Is Data Theft? MPH, BSc Biochemistry,** https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

tarafından yayımlanan Veri Sızıntısının Maliyeti, 2021 Raporuna göz atıldığında, salgın sürecinin veri ihlallerinin artmasında etkisi olduğu tespit edildiği görülmektedir. Bu bağlamda, ESET[59] uzmanları, 2020'den önceki son birkaç yılda da sızıntıların maliyetinde artış olduğunun altını çizmişlerdir. IBM tarafından yayımlana Rapora göre veri ihlali maliyetleri geçen yılın raporunda 3,86 milyon dolar iken, bu yıl bu maliyet %10 artarak 4,24 milyon dolar olmuştur. 50 ila 65 milyon tutarındaki *"mega ihlaller"* için ise, bu maliyet 2020 yılında 392 milyon dolar iken, %2 artışla 401 milyon dolar seviyesine gelmiştir. Rapora göre, çalıntı kullanıcı bilgileri ihlallerin en büyük nedenleri arasında yer almaktadır. Parolalar ve isimler de dahil olmak üzere, müşterilerin kişisel verileri, bu olaylarda ifşa olan en yaygın veri türlerinin ve ihlallerinin %44'ünü oluşturmaktadır[60].

Veri hırsızlığı ile ilgili olarak ortaya çıkan ihlaller ve etkilediği alanlarla maddi ve maddi olmayan varlılara verdiği zararlar göz önüne alınarak AB ve devletler tarafından yasal düzenlemelerin yapılmasına neden olmuştur. Bu bağlamda, veri hırsızlığı ile ilgili doğrudan ilk düzenleme, Lüsemburg tarafından yapılmıştır. Kanun koyucu, Lüksemburg Ceza Kanununda değişiklik yapan ve 25 Temmuz 2014 Tarihinde yayımlanan siber suçlara ilişkin 18 Temmuz 2014 Tarihli Kanunu kabul etmiş ve Kanun içeriğinde dijital veri hırsızlığına ilişkin yeni bir tanımlamayla suç oluşturulmuştur. Dolayısıyla, bu düzenlemenin, dijital veri hırsızlığının tanınmasına yönelik ilk adımı oluşturduğu ve bilgisayar sistemlerini korumayı, dijital verilere müdahale edilmesini veya müdahaleye teşebbüs edilmesini önlemeyi amaçladığı kabul edilmektedir. Ancak, dijital veri hırsızlığının bu şekilde tanınması, Lüksemburg hukukunda çok yeni bir olgu olduğundan, konuyla ilgili içtihatlar hala yetersiz olup, gerçek eğilimleri belirlemek zor olmaktadır. Kanunun yürürlüğe girmesinden önce, dijital verilerin hukuka aykırı olarak indirilmesini suç olarak kabul eden Lüksemburg Yargıtayı, Kanunun hırsızlık suçunu cezalandıran 461. maddesinin, hırsızlığa konu olan varlığın maddi ve maddi olmayan niteliği arasında ayrım yapmamış ve *"varlık"* terimini hem maddi hem de maddi olmayan varlıklara atıfta bulunarak

[59] **UEFI Tarayıcı**, ESET, güvenlik çözümüne Unified Extensible Firmware Interface'i (UEFI'yi) koruyan özel bir katman ekleyen ilk internet güvenlik sağlayıcısıdır. ESET UEFI Tarayıcı, UEFI gereksinimleri ile uyumlu önyükleme öncesi ortamın güvenliğini denetler ve standartların uygulanmasını zorlar. UEFI tarayıcı, firmware içerisindeki zararlı bileşenleri tespit edip bunları kullanıcıya bildirmek için tasarlanmıştır. https://www.eset.com/tr/about/technology/, e.t.: 14/02/2022.

[60] Şirketlerin Derdi Veri İhlali Kaynak:https://turk-internet.com/sirketlerin-derdi-veri-ihlali/, e.t.: 14/02/2022.

yorumlamıştır[61]. Buradaki varlık yorumlaması, kanaatimizce kapsayıcı bir kavram olması yönüyle doğru ancak terminolojik olarak doğru olmayan bir kavramdır. İhtiyaçlar doğrultusunda ortaya çıkan varlık teriminin, ihtiyaç duyulduğu yer bilişim sistemleri ve dijital dünya olduğu için kast edilenin açıkça yazılmasa da dijital veriler olduğu yorumlanabilmektedir. Dijital veri kavramının geniş ve kapsayıcı bir tanımı olmaması, yapılmasının zor olması Lüksemburg yasa koyucusunu "varlık " kavramı etrafında düzenleme yapmaya zorlamıştır[62].

Hukukumuzda da dijital veri hırsızlığının net bir tanımı olmamakla birlikte çeşitli suç tiplerine göre yorumlanmış bir kavramdır. Örneğin, Hırsızlık suçunun nitelikli hali olarak düzenlenen TCK madde 142/2-e de yer alan *"bilişim suçları aracılığı ile hırsızlık suçu"* düzenlemesinde, sadece bilişim sistemlerinin hırsızlık suçun da aracı olarak kullanılmasını düzenlemiştir. Ancak dijital ortamlarda yapılan diğer tüm eylemleri tanım dışı bırakan bir düzenlemedir. Çünkü temel hırsızlık suçuna bağlanmış ve nitelikli hali olarak düzenlenmiştir. Bu durumda ilgili düzenlemenin konusunu taşınır mal oluşturmaktadır. TCK'nın madde 243 ve devamında yer alan düzenlemeler incelendiğinde bölüm başlığı "*bilişim suçları*" olarak belirlenmişse de ilgili düzenlemeler de dijital verilere ilişkin bir açıklama yapılmamıştır. Bilişim sistemlerini hedef alan suç tipleri tanımlanmış ancak sistem içerisindeki dijital ortam da bulunan verilere ilişkin net bir tanım yapılmamıştır. Yoruma açık ve belirli tanımı olmayan düzenlemeler Ceza Hukukunun Kanuniliği ilkesinden dolayı faillere yasal düzenlemelerin arasından sıyrılma şansı vermiştir.

Dijital verilere ilişkin tanımlama da yaşanan eksiklik, Yargıtay içtihatlarında bilişim sisteminin ve verinin tanımını yapılarak giderilmeye çalışılmıştır. Örnekler üzerinden değerlendirme yapmak gerekirse; Yargıtay uygulamada verinin tanımını yaparken Avrupa Siber Suç Sözleşmesine atıf yapmıştır. Yapılan bu atıfta veriyi ; *"bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde islenmeye uygun nitelikteki her türlü bilgi "* olarak tanımlamış ve sözleşmenin iç hukukumuzda etkilediği 5651 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun da yer alan verinin tanımı olan , *"bilgisayar tarafından üzerinde*

[61] **Luxembourg: The theft of digital data–protection or restriction?** https://www.linklaters.com/it-it/insights/publications/financial-crime-update/financial-crime-update-december-2014/luxembourg-the-theft-of-digital-data--protection-or-restriction, e.t.: 14/02/2022.

[62]TITRE IX.- Crimes et délits contre les propriétés, https://sherloc.unodc.org/cld/uploads/res/document/lux/2014/criminal_code_of_luxembourg_html/cp_L2T09.pdf, e.t.: 11/02/2022.

işlem yapılabilen her türlü değer" olarak tanımlanmıştır[63]. Ancak 5651 sayılı kanun da verinin tanımı kanaatimizce eksik yapılmıştır. Çünkü verilerin bilgisayarla işleme zorunluluğu yoktur. Durmuş Tezcan'ın 1993 yılında yayınlanan bir makalesinde *"bilgisayar verileri"* ve *"mekanik (elle toplanan bilen) veriler"* olarak bir ayrım yapmıştır[64]. Yaptığı ayrım da her ne kadar "*bilgisayar verileri"* terimi kullanmış olsa da ilgili makaleye bakıldığında kastedilenin dijital ortamda yer alan veriler olduğu, "*mekanik veriler"* kavramının ise fiziki olarak kullanılabilen veriler olarak tanımladığı anlaşılmaktadır. Bu nedenle 5651 sayılı kanun da üzerinde işlem yapılabilen değerleri bilgisayar tarafından işlenebilmesi ile sınırlamak doğru olmayacaktır.

Yukarıda anlatıldığı üzere "veri" kavramını bilgisayarla veya bilişim sistemleri ile bağlamak veya sınırlamak doğru olmayacaktır. Veri, bilişim sistemleri ile dijital bir ortama aktarıldığı zaman artık fiziksel olmasa da bir değere sahip "*dijital veri"* olacaktır.

TCK'de madde 243 de düzenlenen *"Bilişim Sistemine Girme"* suçunun temelini oluşturan verinin tanımı kanun gerekçesinde yapılmıştır. Gerekçe de veri "*Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır."* şeklinde tanımlanmıştır[65]. Kanun gerekçesinde yer alan tanım aslında dijital verilere ilişkin yapılmış bir tanımdır. Çünkü dijital veriler ile ilgili net bir yasal düzenleme yapılmamıştır. Bu durum suçun konusuna ilişkin muğlak bir durum ortaya çıkarmaktadır. İlgili madde gerekçesinde yapılan tanım, ucu açık ve Ceza Hukukunda Yorum yasağına aykırı olacak şekilde yapılmıştır.

Bilişim sisteminin tanımını bilgisayar ile sınırlayacağımız gibi, dijital veri kavramını da sınırlayamayız. 5651 Sayılı kanunda verinin tanımında kullanılan ve veriyi işlemeye yarayan "bilgisayar " kavramı Yargıtay'ın yakın tarihli Ceza Genel Kurul Kararında değişmiştir[66]. İlgili karar 2021 tarihinde yayınlanmış olup,

"*Bilisim sistemi denince akla önce bilgisayar ve internet gelmekte ise de, bilisim sisteminin kapsamı çok genis olup, bilginin toplanmasında, islenmesinde,*

---

[63] Yargıtay 8. Ceza Dairesi, 2019/9478 E. 2020/15892 K. 23/09/2020 tarihli kararı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 23/02/2022.

[64] Yavuz Erdoğan, **Türk Ceza Kanun'da Bilişim Suçları**, Legal Yayın Evi, İstanbul Mart 2013 , s. 19; Durmuş Tezcan, Bilgisayar Karşısında Özel Hayatın Korunması, **Anayasa Dergisi,** Anayasa Mahkemesinin 29. Kuruluş Yıl Dönümü Nedeniyle Düzenlenen Sempozyumda Sunulan Bildiriler, Anayasa Mahkemesi Yayınları No: 21, 1993, S. 385

[65] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 243. Madde Gerekçesi,** https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 23/02/2022.

[66] Yargıtay Ceza Genel Kurulu 2018/51 E. 2021/68 K. 02/03/2021 Karar Tarihli, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 24/02/2022.

depolanmasında, aglar aracılıgıyla bir yerden bir yere iletilip kullanıcıların hizmetine sunulmasında kullanılan iletisim ve bilgisayarlar dâhil bütün teknolojileri kapsar."

şeklinde bir açıklama yapılmıştır. Artık Yargıtay verilerin işlenmesini bilgisayar teknolojisi ile sınırlı tutmamaktadır. Kanun da şekli düzenlemeler yer alsa da inanıyoruz ki bilişim sistemleri ile işlenen veriler ile somut veriler arasında ayrıma gidilmek zorunda kalınacak ve dijital veri kavramının tanımı netlik kazanacaktır. Kanun koyucu Lüksemburg kanun koyucusu gibi bilişim suçlarının temelini oluşturan dijital verileri korumak için bir tanıma ihtiyaç duyacak ve bilişim sistemlerinde yer alan varlıklar için bir tanım yapacaktır. Yürürlükte olan yasal mevzuatlarımızın dijital veri ve dijital verilerin konu olduğu suçlar noktasında anlam karmaşası içerisinde olduğu ve yetersiz kaldığı kabul edilmesi gerekmektedir. Bilişim ortamındaki her suç bilişim sistemlerine aktarılan ve dijitalleşen verilerin yer değiştirmesi ile meydana gelmektedir. TCK madde 141 düzenlenen Hırsızlık suçunun tanımındaki *"başkasına ait taşınır bir mal"* ın karşılığı bilişlim sistemlerinde dijital verilerdir. Bu nedenle bilişim suçlarının temelinde başkasına ait dijital bir verinin, veri sahibinin rızası dışında yer değiştirilmesi veya kullanılması söz konusudur. Bu nedenle bilişim suçlarının temelinde dijital verilerin hırsızlanması olduğunu kabul etmek gerekmektedir.

Tüm bu nedenlerle, dijital verilerin ve dijital verilerin konu veya aracı olduğu suçların çok çeşitli tanımlarının ve unsurlarının olması, dijital verilerle ilgili düzenlemeleri inceleme gereğine neden olmaktadır. Bu inceleme, güncel yasal düzenlemeler çok dağınık olsa da dijital verilerin, dijital veri hırsızlığına konu olan fiiller nedeniyle önemini bir kat daha artırmaktadır. Dolayısıyla, dijital veri hırsızlığı ile doğrudan ve dolaylı ilgili ve bağı olan ve dijital veri hırsızlığına konu olabilecek suç tiplerinin kanuni unsurları ile incelenip, doktrin görüşleri ve Yargıtay kararları çerçevesinde örneklerle açıklanması gerekmektedir.

2. Genel Olarak Dijital Veri Hırsızlığı

Açıklandığı üzere, dijital veri hırsızlığının kabul görmüş ve net bir tanımı bulunmamaktadır. Bunun nedenini, bilişim sistemine, sayısal dijital halinde yüklenen her türlü bilginin dijital veri niteliğine sahip olup, farklı yöntemlerle ele geçirilip kullanılmasıdır.

Dijitalleşen dünyada gelişen teknoloji ile bilgilerin dijital hallerde veri haline getirilerek depolanması, daha da kolay bir hal almıştır. Buda bilişim sistemleri içerisinde çok küçük alanlarda Evrensel Seri Veri yolu-Universal Serial Bus (USB)

bellek, bulut ağları gibi binlerce verinin kolaylıkla bir arada depolanmasını sağlamaktadır.

Bu depolanan dijital verilerin içeriği ne olursa olsun, dijital veri sahiplerinin rızaları dışında farklı şekillerde ele geçirilmesi; kanımca bir tür hırsızlık eylemi olarak değerlendirilmekte ve gerçekleştirilen hırsızlık eyleminin çeşitliliği ve içeriğinin genişliği, dijital veri hırsızlığının özel olarak incelenmesini gerektirmektedir.

2.1. Dijital Veri Hırsızlığı İle İlgili Yasal Düzenlemeler

Hukukun devinim sel bir bilim dalı olması nedeniyle, gelişen toplumsal ilişkilerin ortaya çıkardığı ihtiyaçları doğrultusunda şekillenmesini gerektirmektedir. Dijital verilerin hayatımıza yoğun şekilde girmesi ile birlikte, yasal düzenlemeler şekillenmeye başlamış, düzenlemelerin olmadığı alanlarda da suça konu eylemler, mevcut düzenlemeler etrafında anlamlandırılmaya çalışılmıştır. Birden fazla mevzuatta dağınık şekilde de olsa yapılan bu düzenlemeler, ihtiyaçlar doğrultusunda şekillendirilmiştir. Ancak, bu düzenlemelerin yeterli olup olmadığı, devinim içinde olan bu suçlar açısından tartışma konusu olmaktadır.

2.1.1. Dijital Veri Hırsızlığına Konu Olabilecek Türk Ceza Kanununda Düzenlenmiş Suç Tipleri

Hırsızlık, dolandırıcılık suçlarıyla fikri haklarla ilgili bilgilerin ele geçirilmesiyle ilgili düzenlemeler dışında, veri hırsızlığı diye tanımlanan suçlar, bilişim suçları, diğer bir anlatımla "siber suçlar" olarak TCK'da düzenlenmiştir. Bilişim suçları kavramı, gerçekte içeriğinde dijital veri hırsızlığını da barındırmaktadır. Zira, bu suçlar bilgisayar, tablet, cep telefonu gibi her türlü iletişim araçları kullanılarak verilerin ele geçirilmesine ve aktarılması suretiyle işlenebilmektedir.

Dijital veri hırsızlığı olarak adlandırdığım farklı yöntemler kullanılarak dijital verilerin ele geçirilmesi ve farklı alanlarda kullanılmasında, suçun konusunu genel olarak dijital varlığa sahip her şey oluşturmaktadır. Ancak günümüzde genellikle kişisel verilerin varlığı konuşulmakta ve kişisel veriler üzerine yasal düzenlemeler ve çalışmalar yapılmaktadır. Yargıtay 12. C. D. 20.10.2014 Tarihli ve 2013/24953 E., 2014/20322 K. Sayılı İlamında, *"...kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği,*

banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir." denilmektedir[67] . Diğer taraftan, uygulamada kişisel veri kişilerin; onuru, dini inançları, cinsel tercihleri, etnik kökeni, sabıka ve arşiv kayıtları, siyasi eğilimleri ve kişisel özel aktivitelere ilişkin bilgileri, mali varlığı, sahip olduğu hisseler ile hesapları, borçları, yaptığı alış verişleri, kredi kartlarına ilişkin verileri, sağlık bilgileri, e-postaları, adresleri veya şifreleri, kişilerin nerede ve kimlerle olduğu, şeklindeki bilgilerden oluştuğu kabul edilmektedir. Ancak dijital veriler kişisel verilerin de üstünde bir kavram olup, üst başlık niteliğindedir.

Gerek Yargıtay kararlarında gerekse uygulamada dijital veri hırsızlığı olarak, depolanan dijital verilerin içeriği ne olursa olsun farklı şekillerde de olsa veri sahiplerinin rızaları dışında, üçüncü kişiler tarafından ele geçirilmesi şeklinde tanımlamaya çalıştığım bu tanım, geniş bir tanımdır. Tanımdan da anlaşılacağı üzere, dijital veri kavramı, hem kamu hukuku hem de özel hukuk içerisinde çeşitli düzenlemelere konu olmuştur. Bununla birlikte, dijital veri hırsızlığı ile ilgili olan temel düzenlemeler, TCK'da yer almaktadır. Hızla gelişen teknolojiye ve bilişim sistemlerine ilişkin suç yapıları sürekli değişiklik göstermekte ve yenilenmektedir. Ancak, TCK'da geçerli olan *"suçta ve cezada kanunilik"* ve *"kıyas yasağı"* gibi ilkeler, bu tür suçlarla mücadeleyi zorlaştırmaktadır[68].Bu nedenle, dijital verilerin hırsızlığına ilişkin TCK'da yer alan düzenlemelerden daha etkin ve caydırıcı yasal düzenlemeler yapılması gerektiği düşünülmektedir. Bunun için de dijital veri hırsızlığının tanımı yapılmalı ve diğer düzenlemeler dijital veri hırsızlığı başlığı altında toplanmalıdır. Dijital veri hırsızlığının neden üst başlık olması gerektiğini daha iyi anlamak için TCK'da yer alan bilişim sistemi ile ilgili suç tipleri üzerinden açıklamalar yapmak yararlı olacaktır.

2.1.1.1. Konusu Bilişim Sistemleri Olan Düzenlemeler

TCK'da bilişim sistemleri ile ilgili suç olan temel normlar, TCK'nın 243-246. maddelerinde düzenlenmiştir. Bilişim sistemi; verilerin dijital ortamda yer aldığı ve

[67] LEGEALBANK Elektronik Hukuk Bankası, https://legalbank.net/ e.t.: 25/03/2022
[68] Demircan, s. 63.

otomatik işlemlere tabi tutulabildiği dijital sistemlerdir[69]. TCK'nın İkinci Kitabının Üçüncü Kısım Onuncu Bölümünde düzenlenen bu suç tiplerinin konusu, bilişim sistemleri ve bilişim sistemlerine yönelen eylemlerdir. Bilişim sistemlerine yönelen ve suç oluşturan eylemlerin hedefinde, genellikle bilişim sistemleri içerisinde yer alan dijital veriler olduğundan, yasal düzenlemelerde de bu çerçevede yapılmıştır.

2.1.1.1.1. Bilişim Sistemine Girme Suçu

765 Sayılı TCK'nın 525/a-1 maddesinde düzenlenmiş olan *"Verilerin ele geçirilmesi"* suçu yapılan eleştiriler sonunda, 5237 sayılı TCK ile birlikte *"Bilişim sistemine girme suçu"* olarak TCK'nın 243/1-2-3-4 maddesinde, *"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"*

şeklinde düzenlenmiştir.

Maddede geçen bilişim sistemi kavramı; verilerin saklanmasını, toplanmasını, işlenmesini, depolanmasını veya aktarılmasını sağlayan sistemlerin tümünü ifade etmektedir. Öğretide bu suç; *"izinsiz bilişim sistemine girme"*, *"yetkisiz erişim"* ve *hukuka aykırı erişim"* şeklinde tanımlanmaktadır[70].

"Verilerin saklanması, toplanması, işlenmesi, depolanması veya aktarılması" ifadesine bakıldığında buradaki verinin somut bir veri değil, dijital ortamda bulunan soyut veriler olduğu anlaşılmaktadır. Buradaki dijital verilerin saklanması, toplanması, işlenmesi, depolanması veya aktarılması aslında dijital veri sahibinin rızası dışında dijital verinin hareket ettirilmesidir.

Bir bilişim sistemine izinsiz girmek, yetkisiz erişmek ve hukuka aykırı erişim sağlamak için, failin, bilişim sistemi sahibinin bilişim sistemine girmek veya erişmek

[69] Ali Parlar/Mustafa Öztürk, **Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar**, 1. Baskı, Aristo Yayın Evi, İstanbul 2020, s. 26.
[70]Durmuş Tezcan/Mustafa Ruhan Erdem/R. Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, Güncellenmiş 16. Baskı, Seçkin Yayınları, Ankara, Eylül 2018, s. 1036.

için sahip olduğu dijital verileri (şifreler, kodlar vs.) bilişim sistemi sahibini rızası dışında kullanması ile olmaktadır. Bakıldığında hem tanımda hem de suça konu eylemde dijital verilerin rıza dışı kullanımı ve failin sağladığı bir yarar mevcuttur.

Başlangıçta üç fıkra halinde yapılan bu düzenlemeye daha sonra 24.03.2016 Tarihli ve 6698 Sayılı Kanunun çerçeve 30. maddesi ile eklenen 4. fıkra ile son halini alan 243. maddeye göre, bilişim sistemine girme suçunun konusunun, bilişim sisteminin bütünü veya bir kısmı olduğu anlaşılmaktadır. Suça konu eylem ise dört şekilde oluşmaktadır. Birincisi bilişim sistemine hukuka aykırı şekilde girilmesi, ikincisi orada kalmaya devam edilmesi ve üçüncüsü bu fiiller nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi, dördüncüsü ise bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerinin, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlenmesidir.

Görüldüğü üzere, maddede hukuka aykırılık özel olarak düzenlenmiştir. Bunun nedeni, failin sisteme hukuka aykırı bir şekilde girmesi ve orada kalmasıdır. Burada fail bilişim sistemi sahibinin kullanmış olduğu dijital verileri, sistem içerisinde kalmak için kullanmakta ve bilişim sistem içerisinde ise bilişim sistemi kullanıcısının sahip olduğu dijital verileri, dijital veri sahibi rızası olmaksızın erişmek ve kullanmak amacı gütmektedir. Zira, mevzuatımızda, bilişim sistemlerine yasal olarak girilmesine, orda kalınmasına ve hatta verilerin alınarak depolanmasına ilişkin hükümler bulunmaktadır. Örneğin, CMK'nın 134. maddesinde yer alan *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* ile 135. maddesinde düzenlenmiş olan *"İletişimin tespiti, dinlenmesi ve kayda alınması"* koruma tedbirleri bağlamında alınan kararlar doğrultusunda yapılan müdahaleler hukuka uygunluk sebebi olarak sayılmaktadır.

Bilişim sistemine girme suçunda fail, herkes olabilir. Burada failin bilişim sistemlerine hukuka aykırı şekilde girebilmesi, orada kalması ve bilişim sistemi üzerinde bilişim sisteminin sahibinin rızası dışında bilişim sistemine etki edebilmesi gerekmektedir.

Bilişim sistemlerini bilmeyen bir kimsenin bilişim sistemine girmesi mümkün olmayacağı gibi, bilişim sistemi içerisinde kalıp bilişim sistemine etki edemeyeceği için fail olmayacaktır. Bilişim sistemlerine ilişkin suçlarda, bilişim sistemlerine yasal olmayan şekilde girerek müdahale etmek, bilişim sistemi içerisinde kalan ve bilişim sistemine etki etmek bilgisayar üzerinde bir bilgi düzeyi gerektirdiği için bu kişilerle ilgili olarak öğretide hacker, siber terörist, korsan gibi ifadeler kullanılmaktadır.

Öğretide, bilişim sistemine hukuka aykırı müdahalede bulunan kişiler için temel bilgisayar bilgisi gerektirdiği için hacker, korsan, siber terörist kavramları kullanılır denilmişse de bu tanımda yer alan *"temel bilgisayar bilgisi"* kavramının, yetersiz olduğunu düşünmekteyim. Çünkü bilişim sistemleri, bilgisayar kavramının üzerinde ve daha geniş bir kavramdır. Örneğin, bilgi depolama cihazları da kendi içerisinde veriyi işleyerek depolar, ancak tam bir bilgisayar tanımını karşılamamaktır. Bu nedenle, bu tanımda yer alan *"temel bilgisayar sistemi"* kavramı yerine, doğrudan bilişim sistemi denilmesi kanımca daha doğru olacaktır.

Bilişim sistemine girme suçunda mağdur bilişim sistemi sahibi olabileceği gibi bundan zarar gören herkes olabilir. Mağdur gerçek veya tüzel kişi olabilir. Burada önemli olan mağdur konumunda bulunan kişilerin bilişim sisteminin sahibi olmasıdır.

Bilişim sistemine girme suçunun maddi unsurunu, bilişim sistemine hukuka aykırı olarak girilmesi veya hukuka uygun şekilde bilişim sistemine girilse dahi bilişim sistemi içerisinde bilişim sistemi sahibinin rızası dışında kalınması fiili oluşturmaktadır. Bu durum, genellikle bilişim sistemine, bilişim sistemi sahibinin rızasıyla girildikten sonra, zararlı yazılımlar sayesinde failin, çeşitli amaçlarla bilişim sistemi içerisinde kalması şeklinde olmaktadır. Bilişim sisteminin tamamına girilmesi şartı aranmamaktadır. Yani, bilişim sisteminin bir kısmına rıza dışı girmek veya orada kalmak da bu suçu oluşturabilmektedir. Sisteme girilmesinin sınırlandırılması genel olmasa bile, sistemde belirli yerler ile sınırlandırılmış ise ve fail sınırlandırılmış yere izinsiz giriş yaparsa da bu suç gerçekleşmiş olmaktadır[71].

Hukuka aykırı olarak bilişim sistemine girilmesi ile orada kalınmasına ilişkin fark, failin bilişim sistemine giriş şeklinden kaynaklanmaktadır. Hukuka aykırı olarak bilişim sistemine giren failin, bilişim sistemine girdiği mağdurun hiçbir şekilde rızası bulunmamaktadır. Ancak, failin orada kalması eylemi, mağdurun rızasıyla olmaktadır. Fakat failin mağdurun rızasıyla bilişim sistemine girdikten sonra, çıkması gerektiği zaman, herhangi bir şekilde kendisini bilişim sistemi dışında olduğunu mağdura inandırıp, bilişim sisteminde kalması sonucunda ortaya çıkan bir eylemi olmaktadır.

Bilişim sistemine girme suçunun manevi unsuru genel kasttır. Bu nedenle, failin bilişim sistemine girme veya bilişim sisteminde kalma kastıyla hareket etmesi gerekmektedir.

[71]Tezcan/ Erdem/Önok, s. 753.

Bilişim sistemine girme suçunda korunan hukuksal değer karma niteliklidir. Ancak korunan hukuki yarar temelin de bilişim sisteminin güvenliğidir. Bu nedenle, suçun oluşması için failin, bilişim sistemi içerinde hukuka aykırı olarak yer alması yeterli olmaktadır. Her ne kadar dijital verilerin çalınması, suçun oluşması için şart olmasa[72] da bu suçu gerçekleştiren faillerin amacı, genellikle bilişim sistemine hukuka aykırı olarak girerek veya çıkmayarak dijital verileri ele geçirmektedir. Mağdur bilişim sistemi sahibi olabileceği gibi bundan zarar gören herkes olabilir[73]. Mağdur, bilişim sistemi sahibinin yanı sıra bilişim sistemi içerisinde dijital verileri bulunan kişiler de olabilir.

Örnek vermek gerekirse; Yrg. 8. C.D. 06.05.2019 Tarihli ve 2017/24009 E.,2019/6266 K. Sayılı İlamına konu olan davada, Bayrampaşa Vergi Dairesinde gelir uzmanı olarak görev yapan sanığın görev ve yetkisi dışında, vergi dairesinin sistemine girerek çeşitli mükellefler hakkında sorgulama yapmasına ilişkin eyleminden yargılama yapılmıştır. Yargıtay, yeterli inceleme yapılmadan beraat kararı verildiğini belirterek kararı bozmuştur. Yargıtay'ın bu kararında, fail vergi dairesi memuru evrak kayıt sisteminde görevlendirilmiş, ancak görevi olmadığı halde mükellefler hakkında sorgulama yaptığı tespit edilmiştir. Failin, yetkisi olmadığı halde yetki alanının dışına çıkması ve kendisi için sınırlandırılan alanın dışında, vergi dairesinin bilişim sistemine girerek sorgulama yapması nedeniyle hakkında yargılama yapılmıştır. Ancak, yapılan yargılama sonunda, ilk derece mahkemesi beraat kararı vermiş, Yargıtay Ceza Dairesi ise ilk derece mahkemesinin kararını, sanığın mükellefleri sorgulama yetkisi olup olmadığı ve sorguladığı mükellefler hakkında düzenlenen sahte fatura olup olmadığı hususları kurumlara sorulmadan ve tespit edilerek dosyaya dahil edilmediğinden, eksik inceleme sonucu verilen beraat kararını bozmuştur. Failin buradaki eyleminin temelini mükelleflere ait dijital verilerin mükelleflerin bilgisi ve rızası dışında, hiçbir hukuka uygunluk sebebi olmaksızın kullanması oluşturmaktadır. Failin eylemi bilişim sistemine girme suçunu oluşturmuş olsa da aslında mağdurun dijital verilerinin rızası dışında kullanılması, bir yerden bir yere taşınması şeklinde gerçekleşmiştir. Dijital verilere yönelik bir hırsızlık suçunun suça konu eylemin de temelini oluşturduğu anlaşılmaktadır. Yargıtay kararında gerçekleşen suça konu eyleme ilişkin bilişim sistemine girme suçu aslında dijital veri hırsızlığının özel bir işleniş biçimi niteliğini kazanmıştır.

[72] Dülger, **Bilişim Suçları**, s. 239.
[73] Erdoğan, **Bilişim Suçları**, s. 121.

Yargıtay'ın bir diğer kararı ise 5. C. D'nin 30.04.2019Tarihli ve 2018/6722 E., 2019/4784 K. Sayılı İlamında yer alan sosyal medyayla ilgili kararıdır[74]. Karara konu olan davada sanık, eski nişanlısı olan katılanın sosyal medya hesabının (facebook) şifresini değiştirerek, (failin katılanın şifresini değiştirmesi katılanın şifresini oluşturan dijital verilerinin katılanın rızası dışında kullanılması ile oluşmaktadır.) katılanın sosyal medya hesabına girmiş ve katılanın bazı arkadaşlarına mesajlar atmıştır. İlk derece mahkemesi, bu davada sanık hakkında, bilişim sistemindeki verileri bozma, yok etme ve erişilmez kılma ve veri yerleştirme suçundan mahkumiyet hükmü tesis etmiştir. Ancak, 5. Ceza Dairesi, sanığın eyleminin hatalı değerlendirildiğini belirterek katılana ait facebook hesabının şifresini değiştirmek suretiyle bilişim sistemindeki verileri değiştirme suçuna ilişkin değerlendirilme yapılması gerektiği kanaatine varmıştır. Bu nedenle de sanığın eyleminin, TCK'nın 244/2 maddesinde düzenlenen bilişim sistemine erişimi engelleme, bozma, değiştirme suçunun oluştuğunun gözetilmesi gerektiği, ancak ilk derece mahkemesinin bu hususu gözetmeden TCK'nın 243/1 maddesine dayanarak mahkumiyet kararı vermesiyle hataya düştüğü vurgusunu yaparak ilk derece mahkemesinin kararını bozmuştur. Mevcut yasal düzenleme ile birlikte değerlendirildiği zaman Yargıtay'ın görüşü kanaatimizce daha doğrudur. Ancak yerel mahkemenin yanılgıya düşmesi, bilişim sistemlerine ilişkin somut ve genel bir düzenleme olmadığı için makul olarak görmekteyiz. İlgili kararda tartışmaya konu olan "Bilişim sistemine girme" suçu ile "bilişim sistemine erişimi engelleme, bozma, değiştirme" suçu için de gerekli olan bilişim sisteminin sahip olduğu dijital verileri rızası dışında kullanmak ve taşımak gereklidir. Bu nedenle aslında tartışılan iki suç tipinin temelini dijital veri hırsızlığını oluşturmaktadır. Tartışmaya konu suç tipleri arasında daha net ayrım yapabilmek için öncelikle dijital veri hırsızlığına ilişkin genel bir tanım yapmak, daha sonra suça konu dijital verinin değeri, kullanım şekli, suça konu eylemin dijital veri üzerindeki etkisi veya suçun işleniş tipine göre açık ve net şekilde sınıflandırmak, gerekmektedir. Bu sayede uygulamada ve suçların tasnifi ve sınıflandırılması kolaylaşacak daha istikrarlı kararlar çıkacaktır.

Bu iki karardan da anlaşılacağı üzere, aranması gereken husus sanığın kastı ve fiilinin niteliğidir. Yani failin dijital verileri kullanmaktaki amacı ve müdahale şekli suçun niteliğini belirlemede Yargıtay tarafından ayırıcı nitelik olarak belirlenmiştir. Sanık katılanın sosyal medya hesabına girmeyi mi amaçlamıştır yoksa katılanın kendi

[74]Parlar/Öztürk, s. 35.

sosyal medya hesabına erişimini engellemek kastıyla mı hareket etmiştir? Bu sorunun cevabı, fiillerin TCK'nın 243. maddesi kapsamında mı, yoksa 244. madde kapsamında olduğunu ortaya koyacaktır. İkinci kararda sanık, katılanın facebook sosyal medya hesabına girmekle kalmamış, katılanın hesabına erişimini de engellemiştir. Birçok bilişim sistemine girme eylemi, ayrıca sistem içerisinde veri değişikliğine veya sistemin kullanıcı tarafından engellemeyi de beraberinde getirmektedir. Bu ise failin kastının tespitini zorlaştırmaktadır.

Yargıtay'ın bu kararı; ilk derece mahkemesinin yanılsamasının nedeninin, hem konunun teknik olması hem de TCK'da bilişim sistemlerine ilişkin düzenlemelerin yetersizliği ve anlam kargaşası olduğunu ortaya koymaktadır. TCK'nın 243. maddesinde yer alan *"sistemin içerdiği veriler yok olur veya değişir"* düzenlemesi ile TCK'nın 244/2 maddesinde yer verilen *"bilişim sistemindeki verileri… yok eden, değiştiren…"* düzenlemesi arasında failin kastı dışında, bir fark olmadığı anlaşılmaktadır. Kanun koyucunun bu iki maddeyi düzenlerken oluşturduğu ayrım, sadece TCK'nın 243.maddesinde bilişim sistemine girilmesi ve verilere bir zarar gelmesi ile ilgilidir. Ancak, TCK'nın 244. Maddesinde, sanığın bilişim sistemine girdikten sonra, veriyi yok etme veya değiştirme eylemlerini gerçekleştirme kastının da bulunması gerekmektedir.

Bu yönüyle değerlendirildiğinde, dijital verilere ilişkin ayrıntılı ve tek kitapta toplanacak bir yasal düzenleme ihtiyacına ilişkin eleştirimin haklılığı görülmektedir. Tanımı yapılan suç tipi hangi şekilde gerçekleşirse gerçekleşsin dijital bir verinin veri sahibinin rızası dışında kullanılması ile gerçekleşmektedir. Bu nedenle Kanun koyucunun bilişim sistemleri ile ilgili olarak internette yer alan platformlara ilişkin daha somut bir tanımlama ve bu tanımlamalara ilişkin dijital veri hırsızlığı başlığı altında daha ayrıntılı düzenleme yapması halinde, uygulamadan kaynaklanan hatalar ortadan kalkabilecektir.

Cezanın indirilmesini gerektiren hal, 243/2 maddede *"Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilebilir. "*şeklinde düzenlenmiştir. Ancak, fıkrada geçen *"bedeli karşılığı yararlanılabilen sistemler"* in hangi sistemler olduğu konusu açıklık taşımamaktadır.

Bu fıkraya açıklık getirmek için öncelikle, *"bedeli karşılığı yararlanılabilen sistemlerin"* ne olduğunu anlamak gerekmektedir. İlgili maddenin gerekçesi, *"İkinci fıkraya göre, birinci fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen*

sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirmektedir[75]*."*şeklindedir. Gerekçenin herhangi bir tanımlamaya ve yeterli bir açıklamaya yer vermemesi nedeniyle, söz konusu fıkranın uygulanması bakımından bir dayanak oluşturmadığını düşünmekteyim. Bu gerekçede, hem kavramsal soru işareti hem de neden daha az ceza gerektiren bir durum olduğuna yer verilmemiştir. Oysa, bedeli karşılığı yararlanılabilen sistemler geniş bir kavramdır. Bu nedenle, *"bedeli karşılığı yararlanılabilen sistemler hakkında"* ifadelerinin ne anlama geldiğini, benzer düzenlemelerle kıyaslamak doğru olacaktır. Bu bağlamda, TCK'nın 163. maddesinde düzenlenen *"Karşılıksız Yararlanma Suçuna "*ilişkin maddenin gerekçesinde *"Otomatlar aracılığı ile sunulan ve bedeli ödendiği takdirde yararlanılabilen bir hizmetten ödeme yapmadan yararlanan kişiler ile telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan…*[76]*"* şeklinde bir tanımlama yapıldığı görülmektedir. TCK madde 243'de ise *"bedeli karşılığı yararlanılabilen sistemler"* belirlenirken düzenlemenin konusuna bakmakta fayda olacaktır. Düzenlemenin konusu bilişim sistemleri olduğu için bilişim sistemleri içerisindeki yani dijital ortamdaki *"bedeli karşılığı yararlanılabilen sistemler"* çerçevesinde yorumlanması gerekmektedir.

İlgili madde de geçen *"bedeli karşılığı yararlanılabilen sistemler*" tanımındaki sistemin bilişim sistemi olduğuna ve buradaki bedelin tanımının ne olduğunu belirlemek önemlidir.

Doktrinde bu tanımlama ile ilgili çeşitli noktalarda görüş ayrılıkları vardır. İlk görüş ayrılığı bedeli karşılığı yararlanabilen sistemin ne olduğudur. Bir takım görüşler belirli bir bedel karşılığı kullanılan bilişim sistemlerinin tamamının kapsanması gerektiğini iddia ederken, bir kısım görüşler de sadece dijital ortamda olan internet siteleri, bulutlar, ağlar gibi fiziki olmayan sistemlerin anlaşılması gerektiğini iddia etmektedir.

Kanaatimizce maddede kastedilen sistemlerin internet üzerindeki siteler olduğu konusunda bir tereddüt yoktur[77]. Çünkü burada verilen hizmetler tamamen elektronik ortamda yapılan hizmetlerdir[78]. Ancak internet kafeler gibi işletme şeklinde olan ve bilişim sistemlerinin kullanımını sadece fiziki olarak erişim imkanı sağlayan yerlerin bu

---

[75] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 243. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.:21.09.2021.
[76] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 163. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.:21.09.2021.
[77] Erdoğan, **Bilişim Suçları,** s. 148.
[78] Berrin Akbulut, **Bilişim Alanında Suçların Tarihi Gelişimi ve Bilişim Sistemlerine Girme,** 2. Basım, Adalet Yayınevi, Ankara 2017, s. 144.

düzenleme kapsamına girip girmediği tartışmalıdır. Yaygın olan ve bizim de katıldığımız görüşe göre internet kafelerde de kullanılan sistemlerin yani bilgisayarların bir çeşit bilişim sistemi olmasından dolayı bedeli karşılığı yararlanılabilen sistemlerde değerlendirmek doğru olacaktır[79]. Doktrin buradaki ayrımını genel olarak sistemin otomatik mi kullanıldığı yoksa manuel mi kullanıldığı noktasındaki tartışmalardan dolayı ayrıma gitmiştir[80]. Ancak tartışmanın konusunu bilişim sisteminin manuel kullanımımı yoksa otomatik kullanımımı olduğu noktasında taşımak çözüm oluşturmayacaktır. Çünkü bilişim sistemlerinin temelinde sistem içerisindeki dijital veriler yer almaktadır. Bilişim sisteminin otomatik veya manuel kullanımı dijital verinin kullanımıyla ilgilidir. İnternet kafeler, kişilerin dijital verilerini kullandığı alanlardır. Kişiler dijital verilerin kullanımını internet kafelerdeki bilişim sistemi aracılığı ile kullanmakta, veri yüklemekte verilerin yerini değiştirmektedir. İnternet kafelerin ticari işletmeler olduğu düşünüldüğünde bedeli karşılığı bilişim sisteminden yararlanılan bir yerdir.

Dijital gazeteler, internet yayınları, dijital dergiler, alışveriş sitelerinin bedeli karşılığı yararlanabilen sistemler içerisinde yer aldığı konusunda tartışmasızdır. Ancak dikkat edilmesi gereken nokta "*bedel*" tanımının ne olduğudur. Kavramsal olarak "*bedelin"* tanımının parasal değerle sınırlı tutmamak gerekmektedir. Çünkü bedel dijital veri olan her şey olabilir. Örneğin bazı siteler site kullanımı için her gün belli bir paylaşım sınırı koymakta, bazıları ise kendini kullandırmak için reklam gösterme şartı ortaya çıkarmaktadır. Ünlü video sitesi youtube reklamsız izlenmek için ücret talep etmekte, ancak ücretsiz kullanım için ise yayınladığı reklamları izletmektedir. Burada izlenilen reklamlar isteye reklam geliri getirmektedir. Yani reklam izlenmesi de aslında bir bedeldir.

"Bedeli karşılığı yararlanılabilen sistemler" kavramının tartışmalarına son vermek için kanaatimizce dijital veriler temelli bir yorum yapılmalıdır. Çünkü kavramda geçen *"sistem"* tanımının ne olduğu önemlidir. TCK madde 243'ün konusu bilişim sistemleri olduğu için buradaki sistemin dijital verilerin işlenebildiği, dijital verilerin kullanıldığı sistemler olması gerekmektedir. Bir kişi dijital verisini kullanmak, işlemek veya dijital bir veriden yararlanmak için kullandığı her sistem kanaatimizce ilgili tanımlama kapsamındadır.

[79] Dülger, **Bilişim Suçları**, S. 434.
[80] Akbulut, **Bilişim Alanında Suçların Tarihi Gelişimi**, s. 145.

TCK madde 243/2 de yer alan cezayı azaltıcı sebep olması kanaatimizce doğru değildir. Cezayı azaltıcı veya arttırıcı sebebin, yasal düzenlemenin korumayı amaçladığı hukuki yarara bakarak düzenlemek gerekmektedir. İlgili madde de korunan hukuki yarar bilişim sisteminin güvenliğidir. Bedeli karşılığında yararlanabilen de olsa ücretsiz de olsa amaç bilişim sisteminin güvenliğini korumak olduğu için ceza miktarında indirime gidilmesi kanaatimizce doğru olmayacaktır.

TCK'nın 243. maddesinde düzenlenen *"Bilişim Sistemine Girme"* suçunun nitelikli hali, 243/3maddesinde düzenlenmiştir. Cezayı arttırıcı neden, gerçekleşen eylemin sonucuna bağlanmıştır. Şayet, fail bilişim sistemine girmesi ile birlikte "*sistemin içerdiği veriler yok olur veya değişirse"* ağırlaştırıcı neden gerçekleşmiş olmaktadır. Ancak, burada failin kastının aranmadığı görülmektedir.

TCK'nın 243/4 maddesi 2016 yılında son halini almış ve*"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."* şeklindeki düzenlemiştir. Gelişen teknoloji ile birlikte bilişim sistemlerine girmeden, bilişim sistemleri içerisindeki verilere ulaşılabilmesi de mümkün olduğundan, bu şekilde bir düzenlemeye ihtiyaç duyulmuştur.

Bu yasal düzenleme, dijital verilerin korunması ile doğrudan bağlı olup, korunan hukuksal yarar, sadece bilişim sisteminin içeriği olmayıp aynı zaman da özel hayatında gizliliğidir[81].

Bu suçta fail ile ilgili özel şartlar aranmamış olsa da failin, bilişim sistemlerine girmeden bilişim sistemi içerisindeki veya bilişim sistemleri arasındaki veri nakillerini izlemeye yarayan teknik araçları kullanabilecek biri olması gerekmektedir. Mağdur ise bilişim sistemi içerisindeki veri sahibi herkes olabilecektir.

Suçun maddi unsurunu oluşturan fiil, failin veri aktarımını *"izlemesi"* dir. Failin veri aktarımını izlemesini, bilişim sistemine girmeden teknik araçlarla gerçekleştirmesi gerekmektedir. Suçun manevi unsuru ise failin, veri aktarımını izleme kastıdır.

TCK'nın 243. maddesindeki düzenlemenin ilk üç fıkrasının, dördüncü fıkra ile farklı olduğu, suçun unsurlarındaki unsurlardaki farklılıklara bakıldığında anlaşılmaktadır. 2016 yapılan bu değişiklik, bir ihtiyaçtan kaynaklanmasına karşılık, tabiri yerinde ise 243. maddeye iliştirilmiş bir görüntü vermektedir. Bu tarz düzenlemeler geçici nitelikte olup dijital verilere ilişkin ayrı bir yasal düzenlemeye duyulan ihtiyacı göstermektedir.

[81]Tezcan/ Erdem/Önok, s. 1002.

Madde geneline bakıldığında maddedeki tartışmalar ve anlam karmaşalarının temeli net ve somut kavram eksikliklerinden kaynaklanmaktadır. İlgili maddede bilişim sistemleri korunmak istenmiştir. Çünkü bilişim sistemleri dijital verileri işlemeye ve kullanamaya yarayan, verileri dijitalleştirme aracıdır. Fail bilişim sistemine girdikten sonra veya girip çıkmayarak, bilişim sistemi sahibinin dijital verilerini (kişisel veri olmasına gerek yoktur) kopyalayabilir, başka bir bilişim sistemine aktarabilir veya zarar verebilir. Bu eylemleri sınırlamak dijital dünyanın sınırı olmadığı için zordur. Biz bilişim sistemi içerisindeki eylemleri dijital veri hırsızlığı altında toplamanın yasal düzenlemedeki belirsizlikleri ortadan kaldıracağını düşünmekteyiz.

İlgili düzenlemede de bilişim sistemlerinin korunması ile aslında bilişim sistemi içerisindeki dijital verilerin en basit ve yalın hali ile hırsızlanarak zarar görmesini engellemenin yattığı anlaşılmaktadır.

2.1.1.1.2. Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu

TCK'nın 244. maddesinde,

"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", (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 beş bin güne kadar adlî para cezasına hükmolunur."

şeklinde düzenlenmiştir. Yapılan bu düzenleme ile bilişim sistemine karşı gerçekleştirilen suçla, verilere karşı gerçekleştirilen suç tiplerinin ayrı ayrı hüküm altına alındığı görülmektedir[82].

Maddenin gerekçesinde de bu durum,

> *"Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir. İkinci fıkrada, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde, verilecek cezanın artırılması öngörülmüştür.*
>
> *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*[83]*."*

Şeklin de açıklanmıştır.

Kanun koyucu düzenlediği bu madde ile hem Avrupa Birliği Siber Suçlar Sözleşmesine[84] paralellik[85] hem de toplumun bilişim sistemlerine ve bu sistemlerde işlenen verilere güvenmelerini sağlamaya çalıştığını ortaya koymaktadır[86]. Avrupa Siber Suçlar Sözleşmesinin *"Uluslar Arası Düzeyde Alınacak Önlemler"* başlıklı İkinci Bölümünün, Maddi Ceza Hukuku başlıklı Birinci Kısmında; *"Yasa Dışı Erişim, Yasa Dışı Müdahale, Verilere Müdahale, Sistemlere Müdahale, Cihazların Kötüye*

[82] Dülger**, Bilişim Suçları** s. 320.
[83] **TBMM 22. Dönem, Yasama Yılı 2, Sıra Sayısı 664**, s. 640 vd.
[84]Counsil Of Europa, **Convention on Cybercrime (ETS No. 185)**, https://rm.coe.int/1680081561, e.t.: 12.12.2021.
[85] Dülger**, Bilişim Suçları**, s.320.
[86] Karagöz, s. 154.

Kullanımı[87]*"*şeklindeki düzenlemelerinin gereği olarak 244. maddenin düzenlendiği anlaşılmaktadır.

Söz konusu maddede korunan hukuksal yararın, bilişim sisteminin kendisini ve bilişim sistemi içerisindeki dijital verilerin korumasını hedeflediği görülmektedir. Gerçekte bu düzenleme, dijital verilere ve bilişim sistemlerine ilişkin ayrı bir düzenlemeye duyulan ihtiyacı ortaya çıkarmaktadır.

Bilişim sistemleri, sistem içerisine yüklenen dijital veriler sayesinde işlem gerçekleştirdiği için bilişim sistemine verilebilecek zarar, ancak bilişim sistemi içerisindeki dijital veriler üzerinden, dijital verilerin, dijital veri sahibinin rızası dışında kullanılması veya failin oluşturduğu bilişim sistemi ile hedef alınan bilişim sistemi içerisindeki dijital verilerde yapılacak değişiklikler ile gerçekleşebilecektir.

TCK'nın 244.maddesindeki suç tipi Mala Zarar verme suçunun dijital ortamda işlenmiş hali olarak düşünülebilir. Ancak, bu suçun konusu bilişim sistemleri ve dijital veri olması yani elle tutulur somut bir eşya, suçun konusu olmadığı için ayrı bir düzenleme ile ele alınmıştır. Bu yönüyle ilgili düzenlemenin, mala zarar verme suçunun özel bir görünüm şekli olduğu düşünülebilir[88]. Dijital verilere zarar verme, bilişim sistemi sahibinin rızası dışında dijital verisini bir yerden başka yere taşınması veya yok edilmesi şeklinde iki temel başlık altında toplanabilir. İlk hal de dijital veri bilişim sistemi sahibinin rızası dışında bir yerden başka yere taşınacağı için dijital veri hırsızlığı ortaya çıkacaktır. İkinci halde ise failin bilişim sistemine girmek ve dijital verileri yok etmek için, hali hazırda bilişim sistemi sahibinin bilişim sistemine girmek için, sistem içerisindeki dijital verilerin yerini değiştireceği için yine dijital veri hırsızlığı ile karşılaşılmış olacaktır.

Bilişim sistemi fiziki anlamda bir mal veya eşya olmadığı için kanunilik ilkesi gereği, TCK madde 151'de düzenlenen "mala zarar verme " suçuna çok benzese de ayrıca düzenlenmiştir. Ancak doktrinde korunan hukuki değerlerin ne olduğu noktasın da farklı görüşler vardır. Doktrindeki görüş ayrılığının temel nedeni bilişim sistemlerindeki korunan değerlere net bir tanım yapılamamasıdır. Doktrindeki hakim olan görüş ise karma sistemli korunan hukuki değer görüşüdür. Bu görüş "bilişim sistemi sahibinin ve kullanıcısının maddi ve manevi değeri" olarak tanımlanabildiği

[87] T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, B.02.0.KKG.0.10/101-612/3607 Sayılı, 03.09.2012 Tarihli Kanun Tasarısı, https://www2.tbmm.gov.tr/d24/1/1-0676.pdf, e.t.: 12/11/2021.
[88]Tezcan/ Erdem/Önok,s. 1004.

gibi [89], genel anlamda iki ayrı korunan hukuksal değer üzerinde durulmaktadır. İlgili maddenin ilk fıkrasında sistemin çalışmasını ve sorunsuz kullanılmasını korumak isterken, ikinci fıkrasında veriler üzerinde tasarruf yetkisi bulunan kişilerin verilerini sorunsuz ve müdahalesiniz şekilde kullanması korunmaya çalışılmıştır[90].

Kanaatimizce bu ayrım failin kastına göre belirlenmelidir. Bilişim sistemlerinin fiziki teknolojik aletlerinin oluşan kısmına verilen zarar ile sanal ortamda oluşan dijital verilerin uğrayacağı zarar noktasında ayrıma gidilmelidir. Örneğin; bilgisayar, telefon, tablet gibi teknolojik aletler bilişim sistemidir. İçerisinde hiçbir dijital veri olmayan veya henüz bireysel kullanıma geçmemiş olan bir teknolojik aletin satıldığı mağazadan çalınması, mağazanın kundaklanması ile yanması gibi etkenlerden doğacak zarar ile bilişim sistemi sahibinin özele inmiş olması, yani bireysel kullanımda yer alan teknolojik aletin çalınması yönüyle korunan hukuki değer hususunda ayrım yapılmalıdır. Bir başka örnek ise, tartışan iki insandan birinin telefonunu tartışı kişinin alıp kırması sonucu, kırılan telefon sahibinin telefon içerisindeki dijital verilerinin gördüğü zarar ile telefon içerisindeki bilgileri almak için telefonun kırılarak içerisindeki hafıza depolamaya yarayan donanımların sökülüp alınması sonucu oluşan zarar bir tutulmamalıdır.

İlgili maddeyi mülkiyet hakkının korunduğu TCK madde 151'den ayıran temel nokta kanaatimizce bilişim sistemi içerisinde yer alan dijital verilerin varlığıdır. Dijital verilerin çalınması amacı ile bilişim sistemine zarar verilmesi amacı güden fail ile bilişim sistemine kullanılmasın diye veya veri kaybı yaşatmak için verilen fiziki zarar oluşturan eylem de ayrıma gidilmelidir. Yargıtay Ceza Genel Kurulu bir kararında "*sanık, bilisim sistemine zarar verme veya verileri yok etme, bozma, erisilmez kılma amacıyla hareket etmemektedir. Hedefi bilisim sistemi olmayıp, amacı bilişim sistemini kullanarak sikayetçinin bankadaki parasını çalmak, ele geçirmektir. Tamamıyla malvarlığına yöneliktir."* şeklindeki ifadesi ile suçun niteliğini belirlemede failin kastını irdelediği görülmektedir. Tabi 2009 tarihli bu karar verilirken fiziki olmayan dijital paralar dikkate alınmamıştır. İlgili karar bu yönüyle tartışmaya açık olsa da TCK madde 244'ü bilişim sistemlerin ilgilendiren diğer suç tiplerinden ayırırken nelere dikkat ettiği belirlemede yardımcı olmuştur[91].

---

[89] Erdoğan, s. 180.
[90] Akbulut, s. 181.
[91] Yargıtay Ceza Genel Kurulu, 17.11.2019. Tarihli ve 2009/11-193 E., 2009/268 K. Sayılı İlamı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 01.03.2022.

Genel anlamda kişilerin bilişim sistemlerine olan güveninin korunduğu düşünüldüğünde[92], kişileri asıl endişelendiren kişiselleşmiş bilişim sisteminin kullanımını (bilişim sistemi içerisindeki dijital verilerinin mahremiyetini) güvenli kılmaktır. Bireyler bilişim sistemlerine gelecek zarardan çok sistem içerisindeki dijital verilerinin çalınmasından endişe etmektedir. Bu nedenle dijital veri hırsızlığına ilişkin ayrı bir tanımlama yaparak ayırmak yaşanan tartışmalara son verecektir.

Söz konusu maddedeki suçlar maddi unsur açısından ele alındığında 2. ve 4. fıkralarında yer verilen *bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suçu* ile *bu fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması suçunun* doğrudan veri hırsızlığı ile ilgili olduğu anlaşılmaktadır.

2. fıkrada bilişim sisteminde yer alan verileri doğrudan etkileyen *"bozma, yok etme, değiştirme, engelleme, erişilmez kılma, sisteme veri yerleştirme, verileri başka yere gönderme"* şeklinde yedi farklı seçimlik hareketi, suça ilişkin eylem olarak sıralasa da yetersiz olduğu ve daha geniş bir kavram kullanılması gerekmektedir.

Zira, faillerin dijital verileri hedef alma yöntemleri her geçen gün değişik şekillerde yenilenmektedir. Bu yenilikler karşısında, dijital verilere yönelik suç oluşturan eylemleri sayma yoluyla-kaziustik metotlar belirlemenin etkili bir yöntem olmadığı açıktır. En basit şekliyle söz konusu maddede sayılan eylemler arasında, dijital verilerin kopyalanmasına ilişkin bir düzenleme bulunmamaktadır. TCK'nın 244/2 maddesinde suça konu eylemlerin kesin olarak sayılmasına karşın,*"... benzeri, ... verileri hedef alan,"* gibi ifadelere yer verilmemiş olması, dijital verileri kopyalan bir kişinin eyleminin suç sayılıp sayılmayacağı konusunda tartışma yaratmaktadır. Avrupa Birliği Siber Suçlar Sözleşmesinin 4. maddesinde yer alan *"Verilere Müdahale"* başlıklı kısmındaki, *"Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman,...*[93]*"* şeklinde düzenleme yapılmıştır. TCK'nın 244/2 maddesinde yer verilen düzenlemenin temelinde yer aldığını düşündüğümüz Avrupa Birliği Siber Suçlar Sözleşmesinin *"Bilgisayar Verilerinin ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişebilirliliğine"* ilişkin İkinci Bölümün Birinci Başlığını da

[92] Erdoğan, s.184,
[93] Murat Volkan Dülger, **Bilişim, Kişisel Verilerin Korunması ve İnternet İletişim Mevzuatı**, 7. Basım, Seçkin Yayınları, Ankara 2021, s. 41.

eleştirmek gerekmektedir. Çünkü, söz konusu hükümde, dijital veriler bilgisayar verileri ile sınırlandırılmıştır. Diğer bilişim sistemlerindeki dijital veriler, bu düzenlemenin kapsamı dışında bırakılmıştır. Avrupa Birliği Siber Suçlar Sözleşmesinin 23.11.2001 Tarihinde hazırlanmış olduğu düşünüldüğünde, dijital verilere karşı gerçekleştirilen ve suç sayılan eylemlere karşı, kanuni düzenlemelerin yetersiz kaldığı hususu, düşüncemi doğrulamaktadır.

Bu aşamada, TCK'nın 136. maddesinde düzenlenmiş olan *"kişisel verilerin korunmasına"* ilişkin hükümler akla gelmektedir. Ancak, bu maddede suçun konusunun, kişisel verilerle sınırlandırıldığı unutulmamalıdır. Bununla birlikte, dijital veriler kişisel veriler ile de sınırlı değildir. Dijital veriler, kişilere ilişkin veriler olabileceği gibi, kamu ve özel tüzel kişilerine ait veriler de olabilmektedir. Her ne kadar bu yönüyle, TCK'nın 244. maddesi yoruma açık olmasa da özellikle dijital verilere karşı yasa koyucunun yapacağı düzenlemeleri, istisnai olarak esnetmesi ve yargı mercilerine hareket etme alanı sağlaması gerektiği düşünülmektedir.

TCK'nın 244. Maddesindeki suça konu eylemlere bakıldığında TCK madde 136'da düzenlenen " kişisel verilerin korunması" suçuna ilişkin düzenleme ile kesiştiği düşünülebilir. Fail burada her iki suçtan sorumlu tutulabileceği gibi somut olayın gelişmesine göre ayrı ayrı da cezalandırılabilecektir. Dikkat edilmesi gereken husus failin eyleminin sonucudur.

TCK'nın 244. maddedeki düzenleme, içeriğinden de anlaşıldığı üzere eylemi gerçekleştirilen fail için belli bir özellik aramamaktadır[94].Bu suçta hukuka aykırılık unsuru, ilgilinin rızası ya da kanunun verdiği bir yetkinin kullanılması sonucu ortaya çıkmaktadır. Örneğin; İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda[95], içeriğinde belirli suçların oluşturduğu hususunda yeterli şüphe bulunan internet sitelerine erişiminin engellenebileceği kararının verilebileceği düzenlenmiştir[96].

2.1.1.1.3. Banka Ve Kredi Kartlarının Kötüye Kullanılması Suçu

Teknolojinin gelişmesiyle birlikte ortaya çıkan yeni sistemlere, bilişim sistemlerinin ve yazılımlarının da sürekli güncellenmesinin getirdiği yeniliklere kanunlarımızın

[94]Tezcan/ Erdem/Önok, s. 1005.
[95]04.05.2007 Tarihli ve 5651 Sayılı **İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**, **Resmi Gazete** 23.05.2007, Sayısı: 26530.
[96]Tezcan/ Erdem/Önok, s. 1005; Koray Doğan, Bilişim Suçları ve Yeni Türk Ceza Kanunu, **Hukuk ve Adalet Eleştiriler Hukuk Dergisi**, Y. 2, S. 6-7, s. 303, Ekim 2005.

uyarlanması gerekmektedir. TCK'nın 245. maddesi, yeni TCK ile birlikte gelen en gerekli düzenlemelerden birini oluşturmaktadır.

TCK'nın 245. maddesinde, banka ve kredi kartlarına yönelik suç oluşturan eylemlerle ilgili ayrı bir düzenleme yapılmıştır. Gelişen teknoloji ile birlikte fiziki cihazlarda, post makinesi, bankamatikler gibi kişilerin kartlarında bulunan dijital veriler kopyalanmakta, çoğaltılmakta ve elde edilen, çalınan veriler, hırsızlık ve dolandırıcılık gibi suçların işlenmesinde kullanılmaktadır[97]. Teknolojinin gelişmesiyle sanal kartlar ve internet üzerinden yapılan alışverişler artmış, kişiler sanal ortamlarda sanal kartlar oluşturmaya ve kart bilgilerini sanal ortamlara yüklemeye başlamışlardır. Kartların dijital ortamlara taşınması, zararlı yazılımlar ile kopyalanmasını ve üçüncü kişilerce kötü niyetli olarak kullanımı arttırmıştır[98].

Bu nedenlerle, banka ve banka kartlarının kötüye kullanılmasının konu olduğu ayrı bir düzenlemenin TCK'nın 245. maddesinde yapılması isabetli olmuştur. TCK'nın 245. maddesinde, ilk üç fıkrada üç farklı suç tipine verilmiştir. 1. fıkrada *"gerçek bir banka veya kredi kartının kötüye kullanılmasıyla hukuka aykırı yarar sağlama",* 2. fıkrada "*sahte banka ve kredi kartı üretme",* 3. fıkrada "*sahte banka veya kredi kartı kullanma suretiyle hukuka aykırı yarar sağlama"* suçları düzenlemiştir[99]. *Banka ve Kredi Kartlarının Kötüye Kullanılması* suçu olarak yapılan bu düzenlemede yer alan üç farklı suç tipi ilgili fıkralarda, her bir suç için ayrı ayrı maddi unsurlara yer verilerek suretiyle tanımlanmıştır.

Birinci fıkrada yer alan hükümde, failin banka kartını ne şekilde ele geçirdiğine bakılmaksızın, sadece ele geçirmiş olması veya elinde bulundurması gerekmektedir. Burada ele geçiriliş veya elinde bulundurulma şeklinin önemi yoktur. Fail, banka kartını her hangi bir hileli davranışla ele geçirmiş olabileceği gibi, kartı bulmuş veya kendisine verilen kartı iade etmemiş de olabilir. Fail bu eyleminden sonra, kendisine veya başkasına yarar sağlamasıyla birlikte, eylemini tamamlamış ve suçu gerçekleştirmiş olmaktadır. Bilişim suçlarında yapılan bu düzenleme, failin kastı noktasında TCK'da düzenlenen hırsızlık suçu ile çok benzerlik taşımaktadır. TCK'nın 141. maddesinde düzenlenen hırsızlık suçunun tanımında,*" ... kendisine veya başkasına*

---

[97] Ali Çağlar TINBEK, **Ümraniye'de ATM'lere Kart Kopyalama Düzeneği Yerleştiren Şüpheli Yakalandı.**, https://www.hurriyet.com.tr/gundem/umraniyede-atmlere-kart-kopyalama-duzenegi-yerlestiren-supheli-yakalandi-41774221, e.t. : 05.10.2021.

[98] **Sahte Alışveriş Sitesi Dolandırıcılığı : 16 Şüpheli Tutuklandı**, https://www.trthaber.com/haber/turkiye/sahte-alisveris-sitesi-dolandiriciligi-16-kisi-tutuklandi-529626.html, e.t.:05.10.2021.

[99] Dülger, **Bilişim Suçları**, s. 367.

bir yarar sağlamak maksadıyla ... " ifadelerine yer verilmek suretiyle, bu suçun özel kastla işlenebileceği belirtilmiştir. TCK'nın 245.maddesinde ise suçun gerçekleşmesi için failin kendisine veya bir başkasına yarar sağlaması aranmamış olup, suçun işlenebilmesi için genel kast yeterli görülmüştür. Bu iki suç, özellikle kast yönünden birbirinden ayrılmaktadır.

İkinci fıkradaki eylemler, başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek şeklinde, seçimlik hareketli suç olarak düzenlenmiştir. Görüldüğü üzere, failin eylemi seçimlik hareketlidir. Yani, fail bu eylemlerden birini veya birden fazlasını yapmak suretiyle söz konusu düzenlemedeki suçu gerçekleştirmiş olabilir. Bu eylemlerin bir veya birden fazlasının fail tarafından gerçekleştirilmesi, suçun oluşması için yeterli olup, bu durum sadece hakimin TCK'nın 61. maddesine göre, cezayı belirlediği sırada, asgari hadden uzaklaşarak ceza tayin etmesine etkili olacaktır.

Üçüncü fıkradaki düzenlemede ise maddi unsurlar arasında nedensellik bağı aranmaktadır. Burada failin bir banka veya kredi kartının sahtesini oluşturması veya mevcut kart üzerinde işlem yapması gerekmektedir. Failin bu eylem ile birlikte kendisine veya üçüncü kişilere yarar sağlaması ile suça ilişkin eylem ve nedensellik bağı tamamlanacak ve bu suç oluşmuş olacaktır. Burada dikkat edilmesi gereken husus, failin gerçek bir kişi üzerinden yola çıkarak, gerçek kişinin banka ve kart bilgilerini hedef alarak hareket etmiş olmasıdır.

Söz konusu kanuni düzenlemede korunan hukuksal yararın, kişilerin banka kartları ve banka kartları ile sahip olduğu değerler olduğu görülmektedir. Bununla birlikte, günümüzde artan kredi kartı ve banka kartı kullanımına ilişkin bankacılık sisteminin de korunduğu ve bu konuda ayrı bir başlık altında kanuni düzenlemenin yapıldığını söylemek mümkündür. Ancak odak noktamızın bireylerin banka ve kredi kartları ile sahip olduğu değerler olması gerekmektedir. Çünkü internet ile birlikte hızlı şekilde gelişen dijital verilerin finans ve ticarette kullanıldığı görülmektedir. Genel anlamda ilgili madde de korunan hukuksal değerin mal varlığı olduğu düşünülmektedir[100]. Yargıtay'ın kabul gören kararları da bu görüşü desteklemektedir[101]. Ancak burada bankacılık sisteminin ve teknoloji ile gelişen ticari yaşamın korunmaya çalışıldığı

[100] Dülger, **Bilişim Suçları,** s. 369.
[101] YCGK, 30/03/2010 tarihli ve 2010/11-17., 2010/65 K. Sayılı İlamı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 03/03/2022

unutulmamalıdır[102]. Özellikle fiziki olmayan maddi değere sahip dijital verilerin (indirim kuponları, kripto paralar, dijital değere sahip resimler v.b.) artması bankacılık sistemlerini asıl hedef haline getirmektedir. İlgili madde de yer alan maddi değerin tam olarak tanımlanmaması ve dijital verilerin maddi değer taşıyan bir kısmının olması, zamanla bizi dijital verilere ilişkin hırsızlıkların ayrı bir yerde ve alanda tanımlanması ihtiyacını doğuracaktır.

Söz konusu düzenlemeye ilişkin suçun faili, kart sahibi dışında herkes olabilir[103]. Dikkat edilmesi gereken husus, failin elinde bulundurduğu kredi kartı veya banka kartı bilgilerini ele geçirmiş kişi olmasıdır. Bu nedenle, fail banka kartı veya kredi kartı sahibinin rızasıyla verdiği kişi olamaz.

Bu suçta mağdur, banka ve kredi kartının sahibi olan kişidir. Banka kartını veya kredi kartını veren kurumun, mağdur olup olmadığı konusunda tartışmalar yapılmaktadır. Öğretide de kabul görüldüğü üzere, korunan hukuksal yararın banka kartı ve kredi kartı sahibinin, sahip olduğu mal varlığı olması nedeniyle, lafzi yorum yapılsa dahi banka kartı veya kredi kartını veren kurumun mağdur olacağından söz edilemeyeceğidir. Ancak, korunan hukuksal değerlerden birinin de bankacılık sistemine olan güvenin olması nedeniyle, bu yönüyle doğrudan olmasa da dolaylı olarak banka kartı veya kredi kartını veren kurumun da bundan zarar gördüğünü söylemek mümkün olabilmektedir.

Söz konusu düzenlemeye ilişkin suçun manevi unsuru kasttır. Failin genel kast içerisinde banka ve kredi kartlarını hedef alması ve bununla birlikte birinci ve üçüncü fıkrada kendisine veya başkasına yarar sağlama kastıyla hareket etmesi gerekmektedir.

TCK'nın 245. maddesinin dördüncü fıkrasında ise bu suçlara ilişkin cezasızlık sebepleri düzenlenmiştir. Buna göre üç durumda, ceza verilmesine yer olmadığı belirtilmektedir. Bunlar; haklarında ayrılık kararı verilmemiş eşlerden birinin zararına işlenmesi, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin zararına işlenmesi veya evlat edinen veya evlâtlığın zararına işlenmesi veya aynı konutta beraber yaşayan kardeşlerden birinin zararına işlenmesi halleridir.

TCK'nın 245. maddesinin beşinci fıkrasında ise mal varlığına karşı suçlara ilişkin etkin pişmanlık hükümlerine atıf yapılmaktadır. Söz konusu suçta korunan hukuki yararın banka kartı ve kredi kartları nedeniyle sahip olunan mal varlığı olduğu düşünüldüğünde, bu şekilde bir atfın yapılmasının yerinde bir atıf olduğu söylenebilir.

[102] Erdoğan, s.300.
[103] Tezcan/ Erdem/Önok, s. 1012.

Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarını da içeren bu suç tipinde içtihat farklılığını önlemek[104] ve uygulanabilirliğini kolaylaştırmak amacıyla düzenlenmiş olsa da asıl önemli nokta, suçun gerçekleşme şeklidir.

"Dijital veri hırsızlığı", bu suç tipinin işlenmesindeki temel yapı taşlarından birini oluşturmaktadır. Zira, banka kartları ve kredi kartlarının kopyalanabilmesi için kart içerisindeki dijital verilerin, bilişim sistemi araçlarıyla kopyalanıp alınması gerekmektedir. Faillerin, özellikle kart kopyalamak için kullandığı en bilinen yöntem, bankamatik gişelerine yerleştirilen kart kopyalamaya yarayan teknolojik sistemlerdir. Günümüzde bu sistem, geçmişte olduğu kadar olmasa da halen kullanılmamaktadır.

Günümüzde en çok kullanılan alışveriş yöntemi, sanal kartlarla yapılan alışverişitir. Sanal kart, internet ortamında yapılan alışverişlerde kullanılmak üzere geçerli olan ve üzerinde kartı çıkaran bankanın ve sistem sağlayıcı kuruluşun logosu bulunan bir kredi kartı çeşididir[105].

"Hepsiburada, gittigidiyor, trendyol, amazon, alibaba" gibi internet alışveriş siteleri; *"Google play, applestore"* gibi uygulama marketlerini milyonlarca kişi kullanmaktadır. Bu sitelerden alışveriş yapıldığı sırada, kredi kartlarının sadece bilgileri kullanılmakta ve bu sitelerin sistemlerine kredi kartı bilgileri yüklenmekte veya sanal kartlar kullanılmaktadır.

Uygulamada, fiziki olmayan veya fiziki olarak banka tarafından verilmiş kredi kartına bağlı olarak eşlenen veya bağımsız şekilde çalışan dijital kartları, hedef alarak başkalarına veya kendilerine yarar sağlayanlar, TCK'nın 245. maddesi kapsamında değerlendirilmektedir. Örneğin, internet bankacılığında kullanılan kartlar, fiziki kartlara karşılık gelen ve onlarla eşleşen kartlardır. Bir alışveriş sitesinde alış veriş yapıldıktan sonra, alışveriş sitesi kolay alışveriş için kart bilgilerini sisteme kaydetmektedir. Bu durumda fail, alışveriş sitesinin güvenlik duvarını aşarak sisteme kaydedilen kart bilgilerini alarak suçu işleyebilmektedir.

Ancak, burada faillerin bulunması ve sorumluluğun kimde olduğu noktasında sorunlar ortaya çıkmaktadır. Geçmiş yıllarda, banka ve kredi kartlarının kopyalanması çeşitli cihaz ve ekipmanla yapılırken günümüzde daha çok zararlı yazılımlar ile yapılmaktadır. Failler, kişilerin banka bilgilerini almak için bankaların sitelerinden

---

[104]Parlar/Öztürk, s. 91.
[105]Ferudun Kaya, **Türkiye'de Kredi Kartı Uygulaması**, https://www.tbb.org.tr/Dosyalar/Yayinlar/Dokumanlar/263.pdf, 2009, s. 81. e.t.: 06.10.2021

bunları birebir kopyalayabilmekte[106] veya güvenli olmayan alışveriş sitelerinde yapılan alışverişlerde, güvenlik açığı olabilmekte ve bu sayede siteye yüklenen zararlı yazılımlar ile alışveriş kartı sahibi kişilerin bilgilerini taklit ederek kendileri veya üçüncü kişiler için alışveriş yapabilmektedirler.

TCK'nın 245. maddesinde özellikle suçun işleniş şekli noktasında daha ayrıntılı düzenlemeler yapılması gerektiğini düşünmekteyim. Ancak, dijital veri hırsızlığına ilişkin yasal bir düzenlemenin olması ve TCK'nın 245. maddesinin de bu başlık altında tekrar detaylı düzenlenmesi hem uygulamayı rahatlatacak hem de faillerin ve suçtan sorumlu kişilerin belirlenmesinde kolaylık sağlayacaktır.

Yargıtay 8. Ceza Dairesi bir kararında

> *"Sanıklar ...ve ... hakkında Dolandırıcılık suçundan kurulan hükümlerin temyiz incelemesinde; Katılanlara ait kredi kartı bilgilerini ögrenip internet üzerinden farklı tarihlerde alısveris yapan sanıkların eylemlerinin bir bütün olarak TCK.nun 245/1 ve 43. maddelerindeki suçu oluşturduğu gözetilmeden, ayrıca dolandırıcılık suçundan mahkumiyet hükmü kurulması, ... bozulmasına"*

şeklinde verdiği kararında[107], her ne kadar faillerin eylemini TCK'nın 245/1 maddesi kapsamında değerlendirilmesi gerektiğine karar verse de ilgili karara konu olayda faillerin elinde 305 kişiye ait kredi kartı bilgileri ele geçirildiği karar içerisinde belirtilmiştir. 305 kişiye ait kredi kartı bilgilerinin, kart sahiplerinin elinden nasıl alındığına bakılmaksızın, 305 kişiye ait hesaplardan para harcamaya elverişli maddi değeri olan (dijital veri içeren) kredi kartlarının sadece TCK'nın 245/1 maddesi kapsamında cezalandırılması, oluşan zarar ile faillere uygulanan yaptırım arasında hakkaniyete uymayan fark olacaktır.

Yargıtay'ın ilgili kararından da anlaşılacağı üzere, bilişim suçlarına ilişkin düzenlemelerin kapsamlı ve detaylı olmaması nedeni ile yoruma açık kalması, Ceza Hukukunun temel ilkelerinden olan yorum yasağının ihlal edilmesine sebep olmaktadır.

2.1.1.1.4. Yasak Cihaz Ve Programlar

[106] **İnternet Dolandırıcılığı**, https://www.akbank.com/tr-tr/genel/akbankguvenlik/dolandiricilik.html, e.t.: 06.10.2021.
[107] Yargıtay 8. Ceza Dairesi, 11.02.2019. Tarihli ve 2018/6468 E., 2019/1826 K. Sayılı İlamı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 21.12.2021.

TCK'nın 245/A. maddesinde, doğrudan doğruya veri hırsızlığı diye tanımlanabilecek *"Yasak cihaz veya programlar"* başlığı altında, dijital verilerle ilgili yeni bir suç düzenlenmiştir. TCK'nın 245. maddesinden sonra gelmek üzere 24.03.2016 Tarihli ve 6698 Sayılı Kanunun Çerçeve 30. maddesi ile eklenen bu madde;

> *"(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."*şeklindedir.

Maddenin bu düzenlemesi incelendiğinde, zararlı yazılımlar ile bunları imal, ithal ve sevk etmeye, nakletmeye, depolamaya, kabul etmeye, satmaya, satışa arz etmeye, satın almaya, başkalarına vermeye veya bulundurmaya ilişkin bir düzenleme olduğu anlaşılmaktadır.

"Bir cihazdan" şeklinde ifade, suç işlemek amacıyla oluşturulmuş bilişim sistemleridir. Örneğin, güvenlik kartları, banka ve kredi kartları gibi içerisinde veri bulunduran dijital eşyaları kopyalamaya yarayan cihazlardır. Son zamanlarda oluşturulan ve telefonu kablosuz şekilde yaklaştığında kopyalayabilen cihazlarda bunlara örnek olarak gösterilebilir.

"*Bilgisayar programının, şifrenin veya sair güvenlik kodunun"* diye ifade edilenler ise zararlı yazılımlardır. Örneğin, bilişim sistemine bilinçli veya bilinçsiz şekilde kurulan zararlı yazılımlar ile bilişim sistemine yerleşen kopyalama programları gibi. Bu programlar bilişim sisteminde yer alan tüm hareketleri kaydedebilir. Kullanıcı farkında olmadan, zararlı yazılım sahibi veya zararlı yazılımda belirlenmiş şekilde üçüncü kişilere ulaştırılabilir. Keylogger[108] casus yazılımı en çok bilinen ve kullanılan casus yazılımdır. Bu yazılım; bilgisayarlarda bulunan klavye tuşlamalarının tamamını kaydeder ve böylece kişilerin şifreleri ile kullanıcı adlarını kopyalayan failler, bilişim sistemlerini ele geçirebilirler.

[108]**Klavye Dinleme Sistemi**, https://tr.wikipedia.org/wiki/Klavye_dinleme_sistemi, e.t.:05.10.2021.

En geniş anlamı ile açıkladığım zararlı yazılımlar ile bilişim cihazlarını kullanıma sunan ve kullanıma hazır hale getirilmesini sağlayan kişileri cezalandıran bir kanuni düzenleme olan TCK'nın 245/A maddesinin uygulanabilirliği oldukça zordur. Zira, internet arama motorlarına *"casus yazılım indir"* şeklinde bir yazı yazıldığında, o an birçok kullanıma uygun casus yazılım monitörde ortaya çıkmaktadır[109]. Bu nedenle, söz konusu zararlı program yazılımlarını oluşturan, satan, satışa arz eden, kopyalayan, depolayan, kabul eden, imal eden kişilerin tespit edilmesi neredeyse imkansızdır.

Dijital veri hırsızlığına ilişkin en temel yöntem, içerisinde zararlı yazılımların olduğu cihazların kullanıldığı TCK'nın 245/A maddesinde yer verilen ve belirtilen yöntemlerdir. Ancak bu maddenin genişletici yorum metoduyla geniş şekilde yorumlanması gerekmektedir. Zira, normal bir cep telefonu ile dahi casus yazılımlar kullanılabilmektedir. Ancak, telefondaki zararlı yazılım, bir bilgisayar programı olmayıp uygulamadır. Teknik anlamda uygulamalar; program olarak, telefonlarda bilgisayar olarak tanımlanabilse de bilgisayar ve bilgisayar programları ile failin belirtilen suçları işlemesi, telefon ve telefon programları ile suç işlenmesinden daha zordur. Bu nedenle, suça konu eylemin gerçekleşme şekline, işleniş kolaylığına ve etki alanına göre yasal düzenlemelerin genişletilmesi gerektiğini düşünmekteyim.

Söz konusu suçta korunan hukuksal yarar toplum güvenliği ve bununla birlikte kişilerin özel hayatı, mal varlığı ve haberleşme özgürlüğüdür. TCK'nın 245/A maddesinin düzenlemesi ile bilişim sistemlerinin güvenliği, kamu düzen ve güvenliğinin korunması amaçlanmıştır[110]. Failin bu suçta hedefi yasak cihaz ve programlar kullanılmak sureti ile üçüncü kişilere ait dijital verileri ele geçirmek olduğu anlaşılmaktadır. İlgili düzenlemeye bakıldığında failin asıl hedefinin üçüncü kişilerin dijital verilerini çalmak olduğunu söylemek doğru olacaktır. İlgili düzenleme ile failin dijital verileri çalmak için yasak cihaz ve program kullanılması cezalandırılmıştır.

Bu suçun konusunun, *"bir cihaz*" olarak ele alındığı düşünülse de bu kavramı geniş yorumlamak gerekmektedir. Çünkü; bilişim sistemlerine zarar vermek amacıyla yapılmış her türlü araç, gereç ve olgu, bu suçun konusunu oluşturabilecektir. Bu durum, yasal düzenlemenin bilişim suçlarına ilişkin yeterli şekilde düzenleme içermediğinden kaynaklandığını ortaya koymaktadır.

---

[109] **Casus yazılım indir**, https://www.google.com/search?q=casus+yaz%C4%B1l%C4%B1m+indir&oq=casus+yaz%C4%B1l%C4%B1m+indir&aqs=chrome..69i57j0i22i30l9.5509j0j4&sourceid=chrome&ie=UTF-8, e.t.:05.10.2021.

[110] Akbulut, s.349.

Bu suçun faili için belirli bir özellik belirtilmemiştir. Seçimlik hareketlerden bir veya birden fazlasını gerçekleştiren herkes fail olabilir. Burada mağdur ise kişiler ve toplumdur[111].

Söz konusu suçun maddi unsurunu oluşturan birden fazla fiil-hareket vardır. Bu fiilleri, bilişim sistemlerine ilişkin suçları işlemek amacıyla veya bilişim sistemlerini diğer yasal düzenlemelerdeki suçları araç olarak kullanmak suretiyle *"imal etmek, ithal etmek, sevk etmek, nakletme, depolamak, kabul etmek, satmak, satışa arz etmek, satın almak, başkalarına vermek, bulundurmak "*şeklindeki fiillerden birini gerçekleştiren kişi, bu suça ilişkin maddi unsuru yerine getirmiş olur. Failin seçimlik hareketlerinin sonucunda ayrıca bir suç işlenmesi gerekmez.

Söz konusu suçun oluşması için failin genel kastı yeterli olmaktadır. Ancak, gerçekleştirdiği fiil yönünden fail, suç işleme kastıyla hareket etmediğini, yanılsama veya aldatılma ile seçimlik hareketli suçlardan birini gerçekleştirdiğini iddia ediyorsa savunmamanın ispata ihtiyacı olmaması ilkesinin aksine, bunu ispatlamak yükümlülüğü faile düşecektir.

2.1.1.2. Bilişlim Suçları Aracılığıyla İşlenen Suçlar

Teknolojinin her alanda gelişmesi sadece hayatımızı kolaylaştırmamış, faillerin bilişim alanındaki suçlar dışında bir takım suçları işlemelerinde teknolojiyi araç olarak kullanarak, değişik türde suç işlemelerinin yollarını da açmış ve kolaylaştırmıştır.

Kişilerin yaşamlarını dijital ortamda sürdürmesi, dijital ortamda bulunarak kendilerini tanıtması, iş hayatını ve takibini kolaylaştırmak amacıyla hareket etmesi, faillerin hedefi haline gelmesine neden olmuştur.

Kişilerin dijital ortamdaki verileri toplanarak dolandırıcılık suçu için inandırıcılık ve güven sağlamakta araç olarak kullanılmış, casus yazılımlar ile iletişim verileri rıza dışı öğrenilmiş, habersiz kişisel bilgiler şantaj gibi suçlarda araç olarak kullanılmıştır. Örneğin, mağdurun kendisi veya yakınlarına ait kişisel bilgilerin çeşitli yollarla çalınmasıyla failin kendisini kamu görevlisi veya mağdurun bir yakını gibi tanıtarak çeşitli bahanelerle mağdurdan para istenmesi çok sık rastlanılan bir durundur [112].

[111] Parlar/Öztürk, s. 273.
[112] Emniyet Genel Müdürlüğü, **Sosyal Medya Dolandırıcılığı**, https://www.egm.gov.tr/sosyal-medya-dolandiriciligi, e.t.: 12.12.2021

2.1.1.2.1. Türk Ceza Kanununda Dijital Veri Hırsızlığına Konu Olabilecek Mal Varlığına Karşı Suçlar

Mal varlığına karşı işlenen suçların temelinde, failin kolay şekilde mal edinme ve kazanma amacı vardır. Bilişim teknolojilerinin gelişmesi ile de sanal ortama geçen mal varlıkları kolay hedef halini almıştır. Aynı zaman da bilişim araçları kullanılarak kişilerin hileli bir şekilde kandırılması ve mal varlığı üzerindeki hâkimiyetlerine müdahale edilmesi kolaylaşmıştır. Bu nedenle, bilişim suçlarının mal varlığına ilişkin suçlar adı altında, ayrı bir düzenleme yapılması gerekmektedir.

2.1.1.2.1.1. Bilişim Sistemlerinin Kullanılması Yoluyla İşlenen Hırsızlık Suçu

Dijital veri hırsızlığını anlamak için TCK'nın 243.maddesi ile devamında yer alan bilişim suçlarının yanında, TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunun unsurlarına da değinmek gerekmektedir. Çünkü, bilişim teknolojileri her iki durumda, suçun temel unsurları arasında yer almaktadır.

Hırsızlık suçunda korunan hukuki değer zilyetliktir. TCK'da zilyedin rızası olmadan başkasına ait taşınır malın alınmasından söz edilmektedir[113].TCK'ya göre hırsızlık suçunun oluşması için taşınır bir mal olması gerekmektedir. Malın bulunduğu yerden alınmasıyla birlikte, malın üzerindeki zilyetliğinde kaybedilmesi gerekmektedir. Taşınır malın zilyedinin hakimiyet alanından çıkarılarak failin hakimiyet alanına alınmasıyla, zilyedinin taşınır mal üzerindeki hâkimiyetinin sonlandırılarak fiil tamamlanmış olmaktadır. Üzerinde zilyet olunan suça konu eşyanın ise taşınır olması gerekmektedir.

TCK'nın 142/2-e maddesinde, hırsızlık suçuna konu eylemin, bir bilişim sistemi aracılığıyla işlenmesi veya bilişim sistemlerinin sağladığı kolaylıkla işlenmesi gerekmektedir. Ayrıca, failin kastının da bilişim sistemlerini kullanarak hırsızlığı gerçekleştirmek olması gerekmektedir. Bilişim sistemleri, fail için amaç veya hedef değil sadece araçtır. 142/2-e maddedeki suçun manevi unsuru failin kastıdır. Failde, zilyedin taşınır mal üzerindeki zilyetliğini, zilyedin rızası dışında sonlandırma kastı vardır[114].

Söz konusu suçta parasal değeri olan, ancak fiziki değeri olmayan dijital verilerin çalınması durumunda, hangi madde hükümlerinin uygulanacağı sorunu ortaya çıkmaktadır? Zira, dijital verilerin taşınır mal olup olmadığı tartışmalıdır.

---

[113] Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, 11. Baskı, Yetkin Yayın Evi, Ankara 2016, s. 373.
[114] Soyaslan, s. 378.

Hırsızlık suçunun nitelikli halleri incelendiğinde, genel olarak suçun işlenme şekli, işlenmesini kolaylaştıracak durumlar, malın bulunduğu yer, tahsis amacı ve malın değeri dikkate alınarak nitelikli hallerin belirlendiği görülmektedir. Hırsızlık suçunun nitelikli hallerinin yer verildiği TCK'nın 142/2-e maddesinde, *"Bilişim sisteminin kullanılması suretiyle,* "şeklinde bir ifadeye yer vermek suretiyle, hırsızlık suçunda bilişim sisteminin araç olarak kullanılması nitelikli hal olarak kabul edilmiştir. Ancak, madde gerekçesinde, *"Fıkranın (e) bendine göre; hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi, daha ağır ceza ile cezalandırılmayı gerektiren bir nitelikli unsur oluşturmaktadır."* denilmesine karşın, suçun bilişim sistemleri kullanılarak ne şekilde işleneceği hususuna herhangi bir açıklık getirilmemiştir. Bunun sonucu olarak parasal değeri olan, ancak üzerinden fiilen zilyet olunamayan ve bilişim sistemleri içerisinde dijital varlıkların bir yerden başka bir yere gönderilmesi durumunda ne olacağı sorusuna net bir cevap olmadığı için, failin eylemi yoruma açık bırakılmıştır.

Örneğin; Türkiye'de 2000'li yılların başından itibaren çok kullanılan dijital oyunlar, internetin yaygınlaşmasıyla internet üzerinden oynayan sayısını arttırmış ve bu oyunların maddi değeri inanılmaz boyutlara ulaşmıştır.

Bir kişinin yüksek tutarlarda maddi değeri olan bir oyun karakterinin, kişinin bilişim sistemine girilerek bir yerden başka bir yere taşınması durumunda ne olacaktır ?

Yargıtay bu konudaki içtihatlarında, sosyal hesapları bilişim sistemi olarak yorumlamakta ve karar vermektedir. Yargıtay 8. Ceza Dairesi, sanal oyun hesabına rıza dışı girilerek oyun hesaplarının çalındığına ilişkin yapılan yargılamada, mağdurun oyun hesabına link üzerinden girilerek yapılan oyun karakterinin failin hesabına aktarılmasını, TCK'nın 243 maddesi kapsamında değerlendirmiştir[115]. Ancak burada failin mağdurun oyun hesabına girmesi dışında, sanal ortam da değeri olan ve karşılığında gerçek para ile hesap edilebilen, dijital değerler vardır. Ve bu değerlerin mağdurun hesabından failin hesabına aktarılması yani gerçek değere sahip dijital bir varlığın başka failin zilyetliğine devredilmesi cezasız kalmıştır.

Kanımca, bu karar yerinde bir karar değildir. Zira, güncel bir örnek vermek gerekirse en popüler oyunlardan olan Pub-G oyunun yüz bin Türk lirasından fazla

[115]Yargıtay 8. Ceza Dairesi, 25.05.2017 Tarihli ve 2017/897 E. 2017/6019 K. Sayılı İlamı, https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/, e.t: 02.12.2021.

değerde olanlarının piyasada satışı mevcuttur[116]. Bu nedenle, kişiler için bu denli değer taşıyan dijital karakterin dijital ortamdaki zilyetliğinin, failin veya bir üçüncü kişinin bilişim sistemine, mağdurun rızası dışında aktarımını TCK'nın 243 ve devamı maddelerince değerlendirmek doğru olmayacaktır. Kripto paralar da henüz kabul edilmiş bir para birimi olmamasına karşılık, maddi değeri olan dijital verilerdir. Dolayısıyla, kripto paraların bir yerden başka yere malikinin rızası dışında örnek verdiğimiz Yargıtay kararında olduğu gibi, TCK'nın 243 ve devamı maddeleri kapsamında değerlendirilmesi de doğru olmayacaktır.

Katıldığım görüş, dijital değeri olan varlıkların her ne kadar fiilen zilyetliği mümkün olmasa da kabul etmemiz gereken bir dijital zilyetliği söz konusudur. Dijital veriler suçun konusu yönünden kanunilik ilkesi gereği TCK'nın 141. maddesi ve devamında düzenlenen hırsızlık suçunun tanımına uymasa da dijital ortamda paraya dönüştürülebilen varlıklar olarak bu suç değerlendirilebilir. Dolayısıyla, bilişim sistemleri aracılığıyla gerçekleşen eylemler olduğu için de dijital verilerin dijital malikinin rızası dışında aktarımı ve el değiştirmesine ilişkin eylemlerin, TCK 142/2-e maddesi kapsamında değerlendirilmesi gerektiğini düşünmekteyim. Ancak, bu durumun kanunilik ilkesinin istisnası olarak görülmesi gerekmektedir. Aksi halde, gelişen teknolojik ve dijital gelişmeler karşısında, TCK'nın yetersiz kalması gündeme gelecektir[117]. Netice itibariyle TCK'da yer alan yasal düzenlemelerin yetersizliği ve dijital verileri temel alan bir yasal düzenleme ihtiyacı olduğuna ilişkin düşüncemin haklılığı görülmektedir.

Bilişim sistemlerinin kullanarak hırsızlığın gerçekleştirilmesi, daha kolay bir yöntem olarak görülmektedir. Yargıtay, internet cep bankacılığı aracılığıyla, kişinin rızası dışında ve hukuka aykırı biçimde para transferlerini nitelikli hırsızlık olarak kabul etmektedir. Örneğin, failin mağdurun internet bankacılığı şubesindeki hesabını kırarak kendi hesabına para aktarması fiilini, Yargıtay Ceza Genel Kurulu, 17.11.2009 Tarihli ve 2009/11-193 E., 2009/268 K. Sayılı İlamında TCK'nın 142/2-e kapsamında değerlendirmiştir[118]. Bu kararda; faillerin bir kurumun internet bankacılığına kurumun rızası dışında girerek, kendi nam ve hesaplarına gönderilen paranın sonucu olarak oluşan eylemin niteliğinin TCK'nın142/2-emaddesikapsamında mı yoksa 244. maddesi

[116] Game Satış, **Old Joker Hesap**, https://www.gamesatis.com/pubg-mobile-hesap-satisi/oldjoker-hesap-172126, e.t.:01.12.2021.
[117] Ersan Şen, **Kripto Para Çalınır mı?** https://www.haber7.com/yazarlar/prof-dr-ersan-sen/1948163-bitcoin-calinir-mi, e.t.: 12.11.2021.
[118] Yargıtay Ceza Genel Kurulu 17.11.2009 Tarihli ve 2009/11-193 E., 2009/268 K. Sayılı İlamı, https://rayp.adalet.gov.tr/resimler/552/dosya/2009-19328-06-202113-58.pdf, e.t.: 11.10.2021

kapsamında mı değerlendirileceği konusu üzerindeki tartışmaya ilişkindir. Yargıtay Ceza Genel Kurulu değerlendirmesinde, dijital verilerin maddi bir karşılığı olduğu ve mağdurun maddi mal varlığında gerçekleştirilen transfer sonucu bir azalma olduğu için faillerin eylemlerinin, TCK'nın 142/2-e maddesi kapsamında değerlendirilmesi gerektiği sonucuna varılmıştır.

Bilişim sistemlerine ilişkin suçlar, her ne kadar TCK'nın 243. Maddesi ile devamı maddelerde düzenlenmiş olsa da, bilişim sistemlerinin nitelikli ve özel hallerinin olduğu bilişim sistemleri ile bağlantılı suçlarda, belirlenen bağlantılı suç tipi üzerinde durulması gerektiği, aynı Yargıtay kararı ile de kabul edilmiştir. Yargıtay'ın bu kararının suçun tipiklik unsurunun dışına çıktığı iddiası ile eleştiren doktrin görüşleri de mevcuttur. Bu görüşe göre TCK madde 244/4 ile TCK madde 142/2 maddesinin ayrımı yararın elde edildiği andır. Bu görüş ilgili Yargıtay kararını paranın bir hesaptan çıkıp internet bankacılığı üzerinden bir başka hesaba aktarılması ile suçun tamamlandığını bu aşamada ise ilgili suçun tipiklik unsuru nedeni ile TCK madde 244/4 'den yorumlanması gerektiği savunulmuştur[119]. Görüş ayrılıklarının temel sebebinin dijital verilerin çalınmasına ilişkin net ve mümkün olduğunca somut düzenlemeler yer alamaması yer almaktadır. Bankadaki para fiziki olarak var olmadığı için TCK 142 de düzenlenen hırsızlık suçunun tanımına tam olarak uymasa da var olan bankadaki değer aslında yer değiştirebilir parasal değeri olan bir dijital veridir. Dijital verinin çalınması ayrı bir düzenleme ile ele alınsaydı söz konusu tartışma olmayacaktır.

TCK'nın 142/2-e maddesinde, *"Bilişim sisteminin kullanılması suretiyle,"* ifadesi kullanılmıştır. TCK'nın 141. maddesinde düzenlenen hırsızlık suçunun konusunun taşınır mallar olması nedeniyle madde içerisinde anlam kargaşasına yer verdiği görülmektedir. Bilişim sisteminde yer alan verilerin taşınır mal olup olmayacağı tartışma konusu olmaktadır. Bir görüşe göre bilişim sistemleri aracılığıyla gerçekleştirilen hırsızlık suçunun konusunu veri oluşturduğundan, verinin de taşınır mal olmaması nedeniyle anılan suçun uygulama olanağının bulunmadığıdır[120]. Farklı görüş ise dijital verinin hırsızlık suçuna konu olması sorunu ile hırsızlık suçuna konu olan malların taşınabilir olması sorununun ayrı konular olması nedeniyle, hırsızlık suçunun bilişim sistemleriyle işlenemeyeceği anlamına gelmediği yönündedir[121]. Dülger bu

[119] Erdoğan, s. 289.
[120] Veli Özer Özbek, "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", **DEÜHFD**, Prof. Dr. Ünal Narmanlıoğlu'na Armağan, C. 9, Özel Sayı: 2007, s. 1058.
[121] İsa Başbüyük, "Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerin Araç Olarak Kullanılması Suretiyle İşlenmesi", **CHD**, Yıl: 5, S.: 14. Aralık 2010, s. 157-164.

konuda, hırsızlık suçunun temel halinin somut nesneler olarak görüldüğü ve bu nedenle de 142/2-e maddesinin ayrı bir madde olarak düzenlenmesi gerektiği yorumunu yapmaktadır[122]. Bu yoruma kısmen katılmak mümkündür. Zira, dijital veri hırsızlıklarına ilişkin düzenlemelerin ayrıca bir arada ele alınması ve daha ayrıntılı bir şekilde düzenlenmesi gerekmektedir. Ancak, TCK'nın 142/2-e maddesinde, hırsızlık suçunun konusu yerine, işleniş şekli tanımlanmış, başka bir anlatımla, gerçekleştirilen fiilde bilişim sistemlerinin kullanılması nitelikli hal olarak düzenlenmiştir. Sonuç olarak dijital verilerinde bilişim sistemleri aracılığıyla taşınabilen bir şey olduğu söylenebilir. Bunun en somut örneği, içerisinde maddi değeri olan bir dosyanın, dosyanın bulunduğu bilişim sisteminin sahibinin rızası olmadan, bilişim sistemine girilerek mail atılması ve elde edilmesi kanımca bu suçu oluşturacaktır.

Bu tartışmaları sonlandırmak ve uygulamada tereddüt yaratmamak için dijital verilere ilişkin suç tiplerinin ayrıca düzenlenmesinin yerinde olacağını düşünmekteyim.

Fıkrada yer verilen *"Bilişim sistemlerinin kullanılması suretiyle…"*ifadesi ile kanun koyucunun neyi kastettiği de açık değildir. Çünkü bilişim sistemlerini, hırsızlık suçunu işlemek amacıyla çok geniş alanlarda kullanmak mümkündür. Dülger'in belirttiği gibi bilişim sistemindeki verilere ilişkin bir kullanım mı, yoksa bilişim sistemlerini fiilen kullanmak mı kastedilmektedir? Örneğin, kişinin ev alarm sistemi bir bilişim sistemidir. Zararlı yazılımlar ile ev alarm sistemini kapatarak veya etkisiz hale getirerek hırsızlık suçu işlendiğinde de bu kapsamda mı değerlendirme yapılacaktır? Kanımca bu durumda fiilin, 142/2-e madde kapsamında değerlendirilmesi gerekir. Çünkü, kanun maddesi açık şekilde hırsızlık suçunun bilişim sistemini kullanarak işlenmesini nitelikli hal kapsamına almıştır.

Söz konusu düzenlemede korunan hukuksal yarar mal varlığı dolayısıyla mülkiyet hakkıdır. Fail açısından ise yasal düzenlemede özel bir şart aranmadığı için bu suçun faili herkes olabilecektir. Suçun konusu, bilişim sisteminin kullanılması suretiyle hırsızlık olduğundan, bu suçla mal varlığında azalma veya mal varlığında değer kaybı olan herkes, bu suçun mağduru olabilir. Ancak, bankaların dahil olduğu suçlamalarda, mağdurun banka mı yoksa bankada hesabı bulunan kişiler mi olduğuna dikkat edilmelidir. Bu konunun tespiti için bankalar ile hesap sahipleri arasındaki sözleşmelere bakılması gerekmektedir.

[122] Dülger, s. 493.

Suçun konusunu, maddi değeri olan her türlü veri oluşturabilecektir. Bilişim sisteminde yer almayan, yer alsa bile sürekli olarak bilişim sisteminde yer almadığı için eylem gerçekleşirken sistem ile bağı olmayan veriler, bu suçun konusunu oluşturmayacaktır. En basit açıklamayla bilişim sistemine bağlı olmayan bir hard disk içindeki verinin ele geçirilmesi amacıyla gerçekleştirilen hırsızlık suçu, bu suçun konusu olmayacaktır. Ayrıca TCK'nın 244/2-e maddesine göre, bu verilerden haksız yarar sağlanmış iseTCK'nın244/4 maddesi uygulanacaktır[123]. Buradaki önemli fark, hırsızlık suçunda bilişim sistemin kullanılmış olmasıdır.

Örneğin, kamu kurumlarının bilişimine sahte bilgiler girerek (tapu kaydı gibi) bu kayıt sayesinde kurumdan hububat parasının alınması durumunda, ilk akla gelen suç tipi hırsızlık olsa da maddi değer taşıyan bir varlığın yer değiştirmesi değil de daha çok failin kendisine hukuka aykırı veriler ile menfaat sağlaması vardır. Bu durumda, eylemin TCK'nın 243. maddesi ve devamı maddeleri çerçevesinde değerlendirilmesi daha doğru olacaktır[124].

Yargıtay 13 . Ceza Dairesinin bir kararında failin müştekiye ait banka hesabındaki parayı, internet bankacılığına yasal olmayan şekilde girerek kendisine para göndermek şeklinde gerçekleştirdiği eylemi, ilk derece mahkemesinin TCK'nın 243. ve devamı maddeleri kapsamında değerlendirilmesini yerinde bulmamıştır[125]. Failin eyleminin, TCK'nın 142/2-e maddesi kapsamında değerlendirilmesine karar vermiştir. Bu davada Yargıtay 13. Ceza Dairesinin, failin kastına bakarak değerlendirme yaptığı görülmektedir. Failin kastının veri aktarımı olmadığı, kendisinin mal varlığında artış sağlama amacıyla hareket ettiğini belirtmiştir. Kanımca, hırsızlık suçunun manevi unsuru olan failin mağdurun mal varlığını azaltmaya yönelik kastının olup olmadığına bakmış ve yorumlamıştır. Bu değerlendirme çerçevesinde, katıldığım görüş çerçevesinde, dijital değeri olan verilerin yer değiştirmesinde sanığın kastına ve verinin maddi karşılığı olup olmadığına bakılarak karar verilmesi gerekmektedir.

Anılan suça konu eylemin, temel hırsızlık suçundan farkı, eşya üzerinde zilyet olan kişinin, eşya üzerindeki hâkimiyetini sonlandıracak eylemin, bilişim sistemi üzerinden ve sanal ortamda yapılmasıdır. Bilişim sisteminde gerçekleştirilen eylemin sonucunda, zararın niteliğine bakılmaksızın zilyedin hakimiyet alanından çıkıp failin zilyetliğine geçtiği an suç tamamlanmış olmaktadır.

---

[123] Dülger, s. 495.
[124] Soyaslan, s. 388.
[125] Yargıtay 13. Ceza Dairesi 10.10.2013 Tarihli ve 2012-14783 E., 2013-28348 K. Sayılı Kararı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 16.12.2021

Failinin eylemini TCK'nın 243. maddesi ve devamı hükümlerine göre değerlendirmek suçun manevi unsuruna bakılmaksızın yapılan bir değerlendirme olacaktır.

TCK'nın 142/2-e maddesinde failin özel kastı vardır. Failin özel kastı, aynı zaman da TCK'nın 243. maddesi ve devamında yer alan bilişim suçları ile TCK'nın 142/2-e maddesinde yer alan hırsızlık suçunda, bilişim suçlarının araç olarak kullanılmasına ilişkin yasal düzenlemenin farkını belirlemektedir. Açıklanan Yargıtay Kararının da görüşü bu yöndedir. Failin özel kastı arandığı için de olası kasttan söz etmek mümkün olmayacaktır.

TCK'nın madde 142/2-e maddesinde yer alan düzenlemede, özel hukuka aykırılığa yer verilmemiş olup suçun unsuru olarak failin, işlenen fiile hukuk düzeni tarafından cevaz-izin verilmemiş olmasını bilmesi yeterli görülmüştür. Zira fiilin, hukuk düzeni ile çatışma ve çelişki içinde olması yeterlidir.

2.1.1.2.1.2. Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenen Dolandırıcılık Suçu

Bilişim sistemlerinin araç olarak kullanılmasıyla işlenen suçların türü her geçen gün artmaktadır. Bilişim sistemleri sayesinde, sahte belge düzenleme, para aklama, vergi kaçırma, banka dolandırıcılığı gibi suçlar ortaya çıkmıştır[126]. Bilişim teknolojilerinin gelişmesiyle ortaya çıkan dijitalleşme ve beraberinde gelen dijitalleşmenin ve teknolojinin öğrenilme zorluğu, kişilerin bilişim teknolojileri yoluyla sergilenen hileli davranışların inandırıcılığını ve kişilerin bu davranışlara aldanmasını kolaylaştırmıştır.

TCK'nın 158/1-f maddesi dolandırıcılık suçunun, *"Bilişim sistemlerinin,...araç olarak kullanılması suretiyle,"* işlenmesi halini, nitelikli dolandırıcılık suçu olarak düzenlemiştir.

Madde gerekçesinde,

> *"Dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi de, birinci fıkranın (f) bendinde bu suçun bir nitelikli unsuru olarak kabul edilmiştir. Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi*

[126] Parlar/Öztürk, s. 287.

açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir."

açıklamasına yer verildiği görülmektedir. Ancak, gerekçede suçun maddi unsurunu oluşturan hareket-fiilin ne şekilde gerçekleştirileceğine ilişkin herhangi bir açıklama yer almamaktadır. Dolayısıyla, suçun ne şeklide işleneceği konusu tamamen uygulayıcıların yorumuna bırakılmıştır.

Dolandırıcılık suçunun bilişim sistemleri aracılığıyla işlenmesinin kanımca iki aşaması vardır. İlk aşama mağdurun kişisel bilgilerinin, yani failin mağduru aldatmaya yönelik eylemi için gerekli bilgilerin, dijital veriler aracılığıyla temin edilmesi ve elde edilen bilgilerin mağduru aldatmak için kullanılmasıdır. Fail, TCK'nın 158/1-f maddesindeki dolandırıcılık suçuna ilişkin eylemi gerçekleştirmek amacıyla mağduru aldatmaya yönelik bilgileri (genel de dijital ortamlarda elde edilen verilerdir) temin eder.

Söz konusu düzenleme ile korunan hukuksal yarar mal varlığıdır. Her hangi bir mal üzerinde hâkimiyete sahip herkes, bu suçun mağduru olabilir. Ancak, burada mağdurun hakimiyeti altındaki eşyayı kaybetmesinde, failin hileli bir davranışta bulunarak yanıltmış olması gerekmektedir.

Dolandırıcılık suçunda fail, her hangi bir kimse olabilir. Dolandırıcılık suçunun oluşabilmesi için failin, *"hileli davranışlarla bir kimseyi aldatmış olması"* aranmıştır. Bir kişiyi aldatmak, hileli davranışların inandırıcılığı ile ilgilidir. Dolayısıyla, hileli davranışların inandırıcı olması için failin karşısındaki insanın güvenini kazanması gerekmekte ve ona güven duyabileceği şeylerden bahsetmelidir. Fail, mağdura güven vermek için mağdurun özel bilgilerini mağdura karşı kullanır. Bu bilgilerde genellikle mağdurun haberi olmadan bilişim sistemleri aracılığıyla elde edilen bilgilerdir.

TCK'nın 158/1 maddesine göre maddi unsur yönünden, failin hileli davranışlarda bulunması ve aldatma eyleminin sonucunda, failin kendisine veya bir başkasına haksız yarar sağlama kastının olması gerekmektedir. Ayrıca, hileli davranışların mağduru aldatmaya elverişli olması aranmaktadır. Dolayısıyla, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen dolandırıcılık suçunda, bilişim sistemlerinin yapısı gereği, mağdurun kandırılmasına yönelik eylemleri gerçekleştirmek kolaylaşmış

bulunmaktadır. Dolandırıcılık suçunda da hırsızlık suçunda olduğu gibi failin özel kastı bulunması gerekmektedir.

Günümüzde yaşanan bilişim sistemleri aracılığıyla işlenen suçlardan en sık rastlananlar; mağdurun kişisel bilgilerinin faile beyan edilmesi suretiyle para istenmesi veya zararlı yazılımlar ile ele geçirilen sosyal medya hesaplarından, hesap sahibinin arkadaşlarına karşı, asıl hesap sahibi gibi hareket edilerek para gönderilmesinin sağlanmasıdır. Dolayısıyla bir kişinin bilişim sisteminin, zararlı yazılımlar ile ele geçirilerek alınan kişisel bilgilerinin, daha sonra kişinin kendisine karşı telefonla veya bir başka iletişim cihazı ile ulaşan ve kendisini devlet adına görevli gibi tanıtan ve çeşitli şekilde para isteyen kişiler çok artmıştır. Emniyet Genel Müdürlüğü, bu konu ile ilgili sık sık uyarıda[127]bulunsa da kandırılarak parası alınan çok sayıda kişinin olduğu gözlemlenmektedir. Fail; bu kişilere, kendisini polis olarak tanıtıp, adresi, ailesi ve mesleği ile ilgili bilgileri, Türkiye Cumhuriyeti Kimlik Numarası gibi özellikleri söylemek suretiyle kişilerin inanmasını sağlamaktadır.

Yine sosyal medyadan ele geçirilen hesap sahibinin arkadaşlarına, mesaj atarak para isteyen failler, hedef aldığı kişiye yazmadan önce ele geçirdiği hesap sahibi ile mağdur arasındaki ilişkiyi anlamak için tarafların profillerini ve mesajlaşmalarını incelemekte ve böylece çok geniş bilgiye sahip olmaktadırlar.

Failin, mağdurun sosyal medya hesabına girerek çıkmaması, bilişim suçlarına ilişkin hükümler çerçevesinde değerlendirilmelidir. Ancak, failin sosyal medya hesabı üzerinden mağdur ve arkadaşları arasındaki ilişkileri gözeterek, mağdurun arkadaşlarını yanıltmaya yönelik girişimlerde bulunmak suretiyle kendisine veya üçüncü kişilere kazanç sağlaması durumunda, failin eylemi, TCK'nın 152/1-f maddesi kapsamında değerlendirilmektedir.

Örnek verilen her iki durumda da, dolandırıcılık suçunda mağdurun aldatılması, bilişim sistemlerindeki kişilere ait dijital verilerinin kullanılması kolaylığından kaynaklanmaktadır. Bu tür davranışlar, mağdurların aldatılması ve faillerin tespit edilememesi bakımından sıklıkla tercih edilen bir yöntem olmuştur.

Dolandırıcılık suçunda bilişim sistemlerinin, kredi veya banka kurumlarının araç olarak kullanılması nitelikli hal olarak değerlendirilmiştir. Nitelikli dolandırıcılık

[127]**Sizi arayarak kendisini polis, savcı, hakim olarak tanıtıp adınız…**, https://www.egm.gov.tr/gocmenhudut/sizleri-telefonla-arayarak-kendilerini-polis-asker-veya-savci-olarak-tanitip-adiniz, e.t.: 16.10.2021

suçunu işlerken failin, mağdura ait bilişim sistemine karşı gerçekleştirdiği suçtan dolayı, ayrıca TCK'nın 244/4 maddesine göre, ceza verilmeyecektir[128].

TCK'nın 158/1-f maddesindeki düzenlemenin temelinde, dolandırıcılık suçunun bilişim sistemleri aracılığıyla daha kolay şekilde işlenebilir olması bulunmaktadır[129]. TCK madde 244/4 ile TCK madde 158/1-f arasındaki ayrım üzerinde durmakta fayda vardır. Buradaki temel ayrım TCK madde 244/4'ün meydana gelen suç unsuru eylemin TCK'da karşılığı olmadığı durumlarda uygulanması gerekliliğidir. Bu ayrımın tespiti için failin bilişim sistemine müdahalesi ile yararın kendiliğinden mi ortaya çıktığını yoksa üçüncü bir kişinin araya girmesi ile menfaat elde ettiğini belirlemek gerekmektedir[130] . Daha basit anlatımla fail bilişim sistemine müdahale ettiğinde yarar müdahalenin sonucu olarak kişi değil de bilişim sisteminin aldatılması sonucu yarar sağlandı ise TCK madde 244/4, ancak bilişim sistemine yapılan müdahale ile üçüncü kişinin iradesi etkilendi ise TCK madde 158/1-f maddesi kapsamında değerlendirilecektir.

Yargıtay'ın bir kararında failin hareketlerinin gerçek bir kişiye yönelik olması gerektiği vurgulanmıştır[131]. Yargıtay bir başka kararında *"Sanık katılanın nüfus cüzdanındaki bilgilerle kendi fotoğrafını yapıştırdığı bir nüfus cüzdanı düzenlemiş, bankada bu nüfus cüzdanıyla hesap açtırarak katılanın hesabındaki paraları sahte nüfus cüzdanıyla açmış olduğu hesaba aktarıp parayı çekmiştir. Sanık eyleminin paranın sanığın açtırdığı hesaba intikaline kadar katılana yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle bilişim alanında suçu oluşturduğunun gözetilmesi gerekir. "* demiştir. Karardan da anlaşılacağı üzere suçun vasfını belirlemede eylemin kime yöneltildiğine bakılmıştır.

TCK madde 244/4 ile TCK madde 158/1-f düzenlemelerinin cezai müeyyideleri arasında çok fazla fark vardır. Suçun niteliği ve korunan yararın bu farkı oluşturduğu düşünülse de kişilerin mal varlığını daha güvenli şekilde muhafaza etmek amacı ile dijital verilere dönüştürerek (bankadaki paranın dijital veri olması gibi) saklanması korunan mal varlığının değerini azaltmayacağı gibi kişilerin bilişim sistemine olan güvenini sarsmaktadır. Ayrıca dijital platformların kendi içlerinde algoritmaları, yapay zekaları ve güvenlik protokolleri vardır. Failin bu güvenlik sistemlerini aşarak dijital

[128] Parlar/Öztürk, s. 288.
[129] Tezcan/ Erdem/Önok, s. 778; Mahmut Koca/ İlhan Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, 5. Baskı, Adalet Yayın Evi, Ankara, 2018, s. 702.
[130] Erdoğan, s. 273.
[131] Yargıtay 11. Ceza Dairesi, 12/10/2009 tarihli ve 2008/11060 E., 2009/11936 K. Sayılı İlamı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 15/02/2022.

verileri çalması için özel bir beceri gerekmektedir. Bu nedenle biz kanun koyucunu yaptığı düzenlemeyi eksik buluyoruz. TCK madde 144/4 düzenlenirken oluşan açığı TCK madde 158/1-f kapatmayacak, tam tersine faillerin kurutuluşuna imkan sağlayacaktır.

TCK 158/1-f maddesinin mağduru her hangi bir gerçek kişidir. Daha somut haliyle mağdur, mal varlığına sahip olan herkes olabilir[132]. Bazı durumlarda Fail, kamu tüzel kişilikleri veya özel tüzel kişiliklerinin bilişim sistemlerine girerek veya oluşturulan sahte evraklar ile (banka kartları, resmi kurum evrakları) oluşturulan sahte kimliklerle veya evraklarla hareket ederek, kendilerine veya üçüncü kişilere menfaat sağlayabilirler. Bu durumda failin eyleminden zarar gören ve hileli davranışa maruz kalan gerçek kişi olmadığı için TCK 158/1-f maddesindeki dolandırıcılık suçunun nitelikli hali gerçekleşmeyecektir. Burada failin gerçekleştirdiği eylem özel bir suç kapsamına girmiyorsa TCK'nın 243.maddesi ve devamı maddelerince yargılanmaları gerekmektedir[133].

Bu nedenle, mağdurun veya suçtan zarar gören üçüncü kişilerin, dolandırıcılık suçunda araç olarak kullanılmak üzere çalınan dijital verilerine ilişkin düzenleme olmaması, dolandırıcılık suçunun nitelikli hali arasında sıkışıp kalması, kişilerin mağduriyetini arttıracak niteliktedir.

2.1.1.2.2. Türk Ceza Kanununda Dijital Veri Hırsızlığına Konu Olabilecek Özel Hayata Ve Özel Hayatın Gizli Alanına Karşı Suçlar

Teknolojinin getirdiği yenilikler ile bilişim sistemlerinin fotoğraf, video, ses gibi verileri kaydederek dijital veriler haline getirilmesi kolaylaşmıştır. Anayasa tarafından korunan ve kişilerin çekirdek hakları kapsamında kaldığı kabul edilen özel hayatları ve kişilerin *gizli-mahrem* diyebileceğimiz alanlarına ilişkin bilgiler, istekleri dışında yayılabilmekte ve mağduriyetlerine yol açabilmektedir.

Özellikle, kişilerin sosyal medya üzerinden yapılan konuşmalarının ifşası, ses kayıtlarının çıkması, sosyal bir ortamda konuşulanların kişilerin rıza dışı paylaşılması, ünlülerin ailesi veya eşi ile paylaştığı fotoğrafların ele geçirilerek halka açık sosyal platformlarda paylaşılması, çok büyük mağduriyete yol açmaktadır.

[132] Tezcan/ Erdem/Önok, s. 753. Koca/Üzülmez, s. 688.
[133]Soyaslan, s. 434.

Bilişim sistemine yüklenen her bilgi, dijital bir veri kabul edildiğinde, bu alan da yer alan suç tiplerinin dijital veri hırsızlığı ile bağlı olduğu şüphesiz bir gerçek olarak karşımıza çıkmaktadır. Dolayısıyla, TCK'nın İkinci Kitabının İkinci Kısım, Dokuzuncu Bölümünde yer alan *özel hayata ve hayatın gizli alanına karşı suçlar* yönünden dijital veri hırsızlığı ile ilgilerini ortaya koymak gerekmektedir.

2.1.1.2.2.1. Haberleşmenin Gizliliğini İhlal Suçu

*Haberleşmenin gizliliğini ihlal "*başlıklı TCK'nın 132. maddesi,

"Madde 132- *(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır.*

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. ***(Ek cümle: 2/7/2012-6352/79 md.)*** *İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.*

(4) ***(Mülga: 2/7/2012-6352/79 md.)"*** şeklindedir.

TCK'nın Özel Hayat ve Hayatın Gizli Alanına karşı Suçlar başlıklı Kısmında 132. maddede yapılan düzenleme ile özel hayatın anayasal ve uluslararası anlaşmalar ile güvence altına alınmasından bağımsız olarak ayrıca ceza hukuku açısından da güvence altına alınarak haberleşmenin dokunulmazlığının koruma altına alındığı ifade edilebilir.

Maddenin gerekçesi;

"MADDE 132-Madde metninde, kişiler arasındaki haberleşmenin gizliliğinin ihlâli suç olarak tanımlanmaktadır.

Söz konusu suç, belirli kişiler arasındaki haberleşmenin içeriğinin öğrenilmesiyle işlenmektedir. Kişiler arasındaki haberleşmenin ne suretle yapıldığının suçun oluşumu açısından önemi yoktur. Bu haberleşme, örneğin mektupla, telefonla, telgrafla, elektronik posta yoluyla yapılabilir. Bu suç açısından önemli olan, haberleşmenin belirli kişiler arasında

yapılmasıdır. Söz konusu suçu, bu haberleşmenin tarafı olmayan kişi işleyebilir.

Haberleşmenin gizliliğinin sadece dinlemek veya okumak suretiyle ihlâl edilmesi, bu suçun temel şeklini oluşturmaktadır. Ancak, bu gizlilik ihlâlinin, haberleşme içeriklerinin yani konuşulanların veya yazılanların kayda alınması suretiyle yapılması, bu suçun nitelikli şekli olarak tanımlanmıştır. Örneğin telefon konuşmalarının ses kayıt cihazıyla kayda alınması hâlinde, suçun bu nitelikli hâli gerçekleşmektedir.

Maddenin ikinci fıkrasında, kişiler arasındaki haberleşme içeriklerinin hukuka aykırı olarak ifşa edilmesi, ayrı bir suç olarak tanımlanmıştır. Haberleşme içerikleri hukuka uygun bir şekilde veya birinci fıkrada tanımlanan suçun işlenmesi suretiyle öğrenilmiş olabilir. İkinci fıkrada tanımlanan suç, haberleşme içeriklerinin ifşasıyla, yayılmasıyla, yani yetkisiz kişilerce öğrenilmesinin sağlanmasıyla oluşur. Fıkra metninde bu ifşanın hukuka aykırı olması açıkça vurgulanmıştır.

Maddenin üçüncü fıkrasında, kişinin kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa etmek suretiyle haberleşmenin gizliliğini ihlâl etmesi ayrı bir suç olarak tanımlanmıştır. Bu suçun oluşabilmesi için, ifşanın alenen yapılması gerekir. Bu bakımdan, örneğin kişi kendisine gönderilen mektubu gönderenin bilgisi ve rızası dışında bir başkasına okutması hâlinde, bu suç oluşmayacaktır.

Dördüncü fıkrada, kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ikinci veya üçüncü fıkralara göre verilecek cezanın belli oranda artırılması öngörülmüştür.[134] ”

şeklindedir.

Maddenin gerekçesinde, korunan temel unsurun kişiler arasındaki haberleşme olduğu anlaşılmaktadır[135]. Haberleşmeden amacın, kişiler arasında kurulan her türlü iletişimin olduğudur. Burada dikkat edilmesi gereken husus, tarafların gerçekleştirilen haberleşmenin üçüncü kişilerin duymalarını ve öğrenmelerini istememesidir. Bu

[134] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 132. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.:21.12.2021.
[135] Tezcan/ Erdem/Önok, s. 620.; Soyaslan, s. 334.

bakımdan, kişisel nitelik taşımayan haberleşmeler, bu suçun konusunu oluşturmamaktadır.

Kişiler arasındaki iletişimin gelişen bilişim teknolojileri ile birlikte artması, casus yazılım ve programlarında teknoloji ile birlikte paralel bir gelişme göstermesi bu suçun işlenmesini kolaylaştırmıştır.

Söz konusu yasal düzenlemede fail, gizliliği ihlal edilen haberleşmenin tarafları dışındaki herkes olabilir. Mağdur ise ihlal edilen haberleşmenin taraflarıdır.

Bilişim teknolojilerinin gelişmesi ile birlikte, kişilerin iletişim şekilleri de değişmiştir. Özellikle, internet aracılığıyla dünyanın neresinde olursa olsun kişilerin kolaylıkla iletişim kurması sağlanmıştır. Kişiler arasında iletişimi sağlayan işaretler, yazımlar ve sesler bilişim sistemlerine dâhil oldukları anda, bir dijital veriye dönüşmekte ve karşı tarafa iletilmektedir. Karşı tarafın bilişim sistemi, gönderilen bu dijital verileri toplamakta ve anlaşılabilecek şekilde iletmektedir.

Gelişen teknolojiye paralel olarak gelişen casus yazılımlar, bu iletişimi sağlayan dijital verilerin usulsüz ve hukuka aykırı bir biçimde kaydedilmesini, kopyalanmasını ve çoğaltılmasını kolaylaştırmıştır. Bugün üçüncü kişiler taraf olmamalarına karşın, kişiler arasındaki iletişim, çok basit programlar ile [136]elde edebilmekte ve bunlar hakkında bilgi sahibi olabilmektedirler.

TCK'nın 132. maddesinde düzenlenen suç tipinde, failin fiilini gerçekleştiriş şekli önemlidir. Örneğin, iki kişi arasındaki konuşmayı duyarak alenen ifşa eden kişi ile mağdurlardan birinin veya birkaçının bilişim sistemine girerek taraflar arasındaki konuşmayı metin olarak yayan kişinin, mağdurların mağduriyetine etkisi aynı değildir.

Bu düzenlemede, bir diğer temel sorun haberleşmenin içeriğinin ne kadar gizli olduğunu belirlemektedir. Örneğin, kişinin sosyal medya hesabında yaptığı bir gönderinin altına yapılan yorumları, kişi isteğine göre sadece sosyal medya hesabındaki kişilerin okumasına da izin verebilir ya da herkese açık şekilde yorum yapılmasına da izin verebilir. Ancak, kişi sosyal medya hesabı herkese açık olduğu zaman yapılan bir yorumu kayda alan fail, daha sonra sosyal medya hesap sahibi kişinin sosyal medya hesabını arkadaşı dışındakilere gizlediği zaman, kayda alınan yorumun ifşasının suçu oluşturup oluşturmayacağı yoruma açıktır.

Kanımca, yorum yapıldığı zaman yorumun kamuya açık olması nedeniyle, kişinin yapılan haberleşmeyi herkesin okumasına rıza gösterdiği varsayılabilir. Sonradan

yorumların kapatılması, söz konusu haberleşmenin içeriğini özele dönüştürmeyecektir. Dolayısıyla, bilişim sistemlerinden ve sosyal medya platformlarının kullanımından kaynaklı bir karmaşa vardır. Bu nedenle, dijital verilere ilişkin ayrı bir yasal düzenleme olmadığı için, yaşanabilecek bu tür eylemlerin bir karşılığı da bulunmamaktadır.

2.1.1.2.2.2. Kişiler Arasındaki Konuşmaların Dinlenmesi Ve Kayda Alınması Suçu

TCK'nın *Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması* başlıklı 133. maddesi;

> *"Madde 133- (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.)*
>
> *(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.*
>
> *(3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dört bin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."* şeklindedir.

Maddenin birinci fıkrasında, kişiler arasındaki aleni olmayan konuşmalar korunan hukuki yarardır. Korunan hukuki yararın *"konuşma"* şeklindeki iletişim olması gerekmektedir. Konuşma, karşılıklı olarak gerçekleştiği için korunan hukuksal yararın yüz yüze yapılan görüşmelerin olduğu ifade edilebilir[137]. Kişiler arasındaki yüz yüze konuşmanın korunmasındaki amaç, kişilerin kaydedilme korkusu olmadan, serbestçe konuşmaları ve kendilerini ifade edebilmelerini sağlamak ve konuşmanın doğallığını korumaktır[138]. Bu bakımdan, gerçekleşen konuşmanın ise aleni olmaması gerekmektedir. Konuşmanın aleni olup olmadığına ilişkin tespiti, maddenin gerekçesinde belirlenmiştir. Maddenin gerekçesinde "*konuşmanın başkaları tarafından*

[137] Tezcan/ Erdem/Önok, s. 632.
[138] Koca/Üzülmez, s. 528., atfen, **Kindhauser**, BT I, (2), s. 28, kn. 1; **Lackner/Kühl**, (25), s. 201, kn. 1; Lalft, BT II, (8), s. 93.

ancak özel gayret gösterilerek duyulabilecek olması halinde" yapılan konuşmanın aleni olmayacağı belirtilmiştir[139]. Failin, tarafların konuşmalarını bir aletle dinlemesi veya ses alma cihazı ile kaydetmesi ile eylemi gerçekleştirmesi gerekmektedir[140].

Bu suçun mağdurları, konuşmanın taraflarıdır. Mağdurlardan birinin konuşmanın kayda alınmasında rızasının olmaması, suçun oluşması için yeterlidir. Maddenin gerekçesinde de konuşmanın taraflarından birisinin rızasının olması durumunda dahi eylemi suç olmaktan çıkartmayacağı belirtilmiştir.

Maddenin ikinci fıkrasında *"aleni olmayan söyleşiler"* suçun konusunu oluşturmakta ve bu yönden kişinin özel hayatı korunmaya çalışılmaktadır. Dolayısıyla, suçun koruduğu yarar özel hayatın gizliliğidir. Söyleşiden neyin kast edildiği madde gerekçesinde açıklanmamıştır. Korunan hukuki değer olan söyleşi ile neyin kastedildiğini tanımlamak ve anlamak, suça konu eylemi belirlemek bakımından önemlidir.

Türk Dil Kurumuna göre söyleşinin üç tür anlamı vardır. İlki arkadaşça, dostça, karşılıklı sohbet, hasbihal; ikincisi belli bir konuda belli bir alanla ilgili bilgilendirme toplantısı; üçüncüsü ise edebiyatta bir yazı türüdür[141]. Öğretide de 133. maddenin birinci fıkrasında, *"konuşma"* ifadesi kullanırken ikinci fıkrasında *"söyleşi"* ifadesinin kullanılması eleştirilmiştir. Maddenin gerekçesinde, kişiler arasındaki aleni olmayan konuşmaların, söyleşiye katılan kişilerden biri tarafından diğerlerinin rızası olmadan kayda alınmasını suç olarak tanımlanmak istenildiği anlaşılmaktadır. İkinci fıkranın, birinci fıkradan farklı olarak en az üç kişinin arandığı, hem maddenin gerekçesinde hem de yasal düzenlemeye ilişkin metinden anlaşılmaktadır[142].

Açıklanan her iki madde de kişiler arasındaki konuşmaların ve söyleşilerin gizliliği korunmaya çalışılmıştır. Ancak, suça konu eylem olarak birinci fıkrada konuşmaların *"bir aletle dinlenmesi veya kayıt cihazı ile kayda alınması"* suç oluşturan eylem olarak kabul edilmesine karşın, ikinci fıkrada sadece *"ses alma cihazı ile kayıt yapma"* eylemi, suç unsuru olarak kabul edilmiştir. Kanun koyucunun neden bu şekilde bir suça konu bakımından eylem farklılığına gittiği anlaşılmamaktadır.

Maddenin üçüncü fıkrasında ise birinci ve ikinci fıkralarında kaydedilen verilerin ifşa edilmesi cezalandırılmıştır. Maddenin gerekçesinde, bir ve ikinci fıkralarda

---

[139] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 133. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.:21.12.2021.
[140] Soyaslan, s.: 339.
[141] **Türk Dil Kurumu**, Söyleşi ne demek? https://sozluk.gov.tr/, e.t.: 18.12.2021.
[142] Koca/Üzülmez, s. 530.

tanımlanan suçların işlenmesi suretiyle elde edildiği bilinen veya böylece elde edildiği kabul edilebilecek olan bilgilerden yarar sağlanması veya bunların başkalarına verilmesi veya bunlardan diğer kişilerin bilgi edinmelerini temin edilmesi, suç olarak tanımlanmıştır[143]. Gerekçeden de anlaşıldığı üzere, birinci ve ikinci fıkradaki suça konu olan konuşma ve söyleşilerin, kişilere ait kişisel bir veri olarak tanımladığı yorumu yapılabilecektir.

Yapılan bu düzenleme de suçun maddi unsurunu, kişiler arasındaki özel olan, aleni olmayan konuşmaların, konuşmayı kaydetme ve dinlemeye yarayan özel bilişim sistemleri ile dinlenilmesi veya kayda alınması oluşturmaktadır[144].

133. maddenin her üç fıkrasındaki suça konu eylemler, sırf hareket suçu niteliğindedir. Eylemlerin gerçekleştirilmesi teknolojik sistemlerin kullanılması ile kolaylaşmaktadır.

Casus ses kayıt ve dinleme sistemlerine günümüzde çok rahat bir şekilde ulaşılabilmektedir. Örneğin, dünyanın en çok kullanılan Amazon alışveriş sitesinde, yüz metre uzaktan dinleme yapabilme yeteneğine sahip ses toplama cihazı, çok cüzi rakamlara alınabilecek durumdadır[145]. Bunun yanında, bilgisayar faresi şeklinde ortam dineleme cihazları[146] gibi cihazlarda piyasada satılmaktadır. Kişiler arasındaki konuşmalar ve söyleşiler sadece cihazlarla değil, suçun mağduru olan kişilerin bilişim sistemlerine yerleştirilen zararlı yazılımlarla da kaydedilebilmektedir. Örneğin, kişinin telefonuna indirdiği masum olarak görülen uygulamalar ile bilişim sistemine giren zararlı yazılımlar, söz konusu uygulama ile birlikte mikrofona erişim izni alabilmektedir. Bunun sonucunda fail, mağdurun bilişim sistemini kendi adına kullanabilmektedir. Bu yönüyle de ilgili düzenleme dijital verilerin konusu alanına girmektedir.

---

[143] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 133. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.:21.12.2021.
[144] Parlar/Öztürk, s. 416.
[145] Amazon.com, **Ses Toplama Tabağı**, https://www.amazon.com.tr/Doorslay-Parabolik-Kulakl%C4%B1kl%C4%B1-Amplifikat%C3%B6r%C3%BC-G%C3%B6zlemleme/dp/B09JC438TB/ref=asc_df_B09JC438TB/?tag=trshpngglede-21&linkCode=df0&hvadid=510230748607&hvpos=&hvnetw=g&hvrand=18398987926831585567&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9056866&hvtargid=pla-1464483206851&psc=1, e.t.: 20.12.2021.
[146] **Lazımbana.com, Mouse Şeklinde Ortam Ses Dinleme Cihazı,** https://www.lazimbana.com/mouse-seklinde-ortam-ses-dinleme-cihazi-ev-isyeri-guvenlik-ses-dinleme-cihazi-p-807496, e.t.: 20.12.2021.

Burada konuşmaların ve söyleşilerin kaydedilmesi veya dinlenmesine yarayan bilişim aletleri, bu kişisel verileri kaydederken veya dinlenmesini sağlarken dijital verilere dönüştürebilmektedir. Bu bağlamda faillerin konuşmaları ve söyleşileri kaydetmesi veya dinlemesi dijital verileri oluşturacaktır. Konuşma ve söyleşilerin dijital veri olduktan sonra gerçekleşen her eylem dijital verilere karşı gerçekleştirilmiş bir eylem niteliğindedir. TCK'nın 133. maddesi, aleni olmayan konuşma ve söyleşilerin kaydedilmesini, dinlenmesini cezalandırılmış, dijital veri haline gelen konuşmaların ve söyleşilerin ifşa edilmesini ayrı bir düzenleme olarak kabul etmemiş aynı madde içerisinde düzenlemiştir. Kanımca, üçüncü fıkranın ayrı bir kanun içerisinde bilişim sistemleri ve dijital veri hırsızlığı ile ilgili hükümlerle birlikte değerlendirilmesi, anlam karmaşasının önüne geçecek ve bütünlük sağlayacaktır.

Yargıtay 12. Ceza Dairesinin,

"Maddi gerçeğin kuşkuya yer bırakmayacak şekilde belirlenebilmesi, suç vasfına ve suçun unsurlarının oluşup oluşmadığına ilişkin tereddütlerin giderilmesi amacıyla; şikayete konu 5 adet video kaydının denetime olanak verecek şekilde ayrı ayrı çözümü yaptırılarak, kaydedilen konuşmaların kimler arasında geçtiği, içeriği, sanığın konuşmaların tarafı mı dinleyici konumunda mı olduğu, kayda alınan konuşmaların özel bir gayret gösterilmeksizin başkaları tarafından da duyulabilen aleni konuşmalar olup olmadığı hususları açıklığa kavuşturularak, toplanan tüm deliller birlikte değerlendirilip, sanığın hukuka aykırı hareket etme bilinciyle davranıp davranmadığı da irdelenmek suretiyle hukuki durumunun takdir ve tayini gerektiği gözetilmeksizin, "...Sanığın görüntü ve ses kaydı yapılan alanda çalışan ve dolayısıyla bu konuşmaların tarafı olan bir kişi olduğu..." biçimindeki yetersiz gerekçelere ve eksik incelemeye dayalı olarak sanık hakkında TCK'nın 133/2. madde ve fıkrasındaki kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçundan dolayı mahkumiyet kararı verilmesi,"

kararında[147] TCK madde 133'ün maddesi içerisinde yer alan failin eyleminin ilgili maddenin hangi fıkrasında değerlendirildiğini belirlemek incelenmesi gereken kriterleri açıklamıştır.

İlgili karara göre; konuşmanın tarafları ve failin dinleyicimi yoksa konuşmaya taraf mı olduğu dolayısıyla failin ilgili maddenin hangi fıkrasından sorumlu tutulması açısından önemlidir. Konuşmanın içeriği önemlidir çünkü suça konu eylemin yani madde içerisindeki korunan hukuki değerin belirlenmesi ilgili madde de hangi fıkra kapsamına değerlendirileceği açısından önemlidir. Suça konu dinlemenin de aleni olup olmadığının tespitinin gerekliliği de suçun maddi unsuru açısından önemlidir. İlgili karara göre değerlendirilmesi gereken bir başka unsur failin kastının ne olduğudur. Çünkü, karara konu olan TCK'nın 133. maddesinde düzenlenen suç tipinde failin kastı aranmaktadır.

2.1.1.2.2.3. Özel Hayatın Gizliliğini İhlal Suçu

TCK'nın *Özel hayatın gizliliğini ihlal*' başlıklı 134. Maddesi;

(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.

(2) ***(Değişik: 2/7/2012-6352/81 md.)*** *Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.* "

şeklindedir.

Kişilerin özel hayatları, Anayasa ile güvence altına alınmış en temel haklarındandır. Ancak, kişilerin kendi özel hayatlarını bilişim sistemleri ile dijital veriler halinde dijital platformlara taşınması, faillerin açık hedefi hallerine gelmelerine neden olmuştur.

Kişilerin kullandığı bilgisayar, telefon gibi özel araçlarının kameraları, gerekli tedbirler alınmaz ise uzaktan erişim ile casus birer kameraya dönüşebilmektedir[148]. Bu durumda; mağdurun evi, iş yeri gibi özel alanında yer alan görüntüler, fail tarafından ele geçirilmiş ve mağdurun özel hayatı ihlal edilmiş olmaktadır. Görüldüğü üzere,

[147] Yargıtay 12. Ceza Dairesi 26.06.2019 Tarihli ve 2018/8316 E., 2019/7741 K. Sayılı Kararı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 27.12.2021

[148]**Web Kamera Çekimleri Yapan Pro Klavye Casus Programı,**https://www.hoverwatch.com/tr/web-kamerayla-cekilen-resimler, e.t. :16.10.2021.

kişilerin özel hayatlarını dijital ortama yükleyerek dijital veri haline getirmesi, kişinin özel hayatına ilişkin gizliliğinin ihlali yine dijital verilerin bir şekilde çalınması ile olmuştur.

134. madde; Anayasanın 20. maddesinde düzenlenen *"Özel Hayatın Gizliliği"* başlıklı madde ile tanınan temel hakkı güvence altına almak için getirilmiş bir düzenlemedir[149]. Anayasanın 20.maddesinde, kişilerin özel hayatına ve aile hayatına saygı gösterilmesi hakkına sahip olduğu; özel hayatına ve aile hayatına dokunulamayacağı belirtilmektedir.

TCK'nın134. maddesinde ise korunması amaçlanan Anayasa maddesinin ihlali durumunda, ihlal eden faili cezalandırıcı bir yaptırım ön görülmüştür.

TCK'nın134. maddesi, özel hayattın sınırlarını belirlememiş olsa da maddenin gerekçesinde, özel hayatın sınırları, *"gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam"* olduğu belirlenmiştir[150]. Korunan hukuki değer özel hayat ve aile hayatının dokunulmazlığıdır[151].

Bu düzenlemede fail herkes olabilir. Ancak, TCK'nın 137. maddesinde düzenlenen suçun nitelikli halinde, fail için özel şartlar belirtilmiştir. Buna göre, şayet özel hayatın gizliliğini ihlal eden fail kamu görevlisi ise ve görevinin verdiği yetkiyi kötüye kullanılmak suretiyle suçu işliyorsa veya fail, belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle suçu işliyorsa suçun nitelikli hali ortaya çıkmaktadır. Bu suçun mağduru herkes olabilmektedir.

Suçun konusu ise kişiler arasındaki haberleşme, konuşma, söyleşi ve kişisel veri niteliğindeki bilgiler dışında kalan özel hayat alanına ait tüm faaliyetler olarak nitelendirilebilir. Burada kişiler arasındaki haberleşme, konuşma, söyleşi ve kişisel veri niteliğindeki bilgiler ise TCK'da ayrıca suç olarak düzenlendiği için ayrı değerlendirilmesi gerekmektedir.

134/1 maddesinde, özel hayata ilişkin görüntü veya seslerinin kayda alınması ağırlaştırıcı sebep olarak düzenlenmiştir. Failin özel hayatı sadece görüntü veya sesle kayıt altına alması suçun oluşması için yeterlidir. Suç seçimlik hareketli eylem içeren

---

[149] 18.10.1982 Tarihli ve 2709 Sayılı **Türkiye Cumhuriyeti Anayasası, Resmi Gazete**, 9 Kasım 1982, Sayı:17863.

[150] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 134. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 21.12.2021.

[151] Koca/Üzülmez, s. 542.

bir suç tipi olduğu için, failin hem görüntü hem ses alması durumunda tek suç işlenmiş sayılacaktır[152].

134/2 maddesinde, özel hayata ilişkin görüntü ve seslerin hukuka aykırı olarak ifşa edilmesi suç olarak düzenlenmiştir. Maddede hukuka aykırılığın özel olarak belirtilmesi önemli bir noktadır. Çünkü, kayıt altına alınan görüntü veya sesin hukuka uygun olması, kaydedilen verilerin yayımlanmasının hukuka uygun olacağı anlamına gelmeyecektir[153].

Bu fıkrada maddi unsur; görüntü ve seslerin kamuya duyurulması veya aleni hale getirilmesi veya bu verilere erişim hakkı olmayan kişilere bilgilerin erişime açılmasıdır[154].

Anılan maddede, özel hayatın görüntülü veya sesli olarak kayda alınması suçun oluşması için yeterlidir. Mağdurun bu kayıtları sildirmesi, fail için cezasızlık sebebi olmamaktadır.

Maddeye göre, özel hayatın gizliliğinin ihlalinde, suçun ağırlaştırıcı ve nitelikli hallerinde bilişim sistemleri ve teknoloji ile doğrudan bağlantı olduğu görülmektedir. Özellikle, gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi hali ve ifşası bilişim sistemleri ve teknoloji ile olmaktadır. Öyle ki; kişinin bilgisayarına yerleştirilen bir casus program ile kişinin rızası dışında bilgisayarın kamerası çalıştırılarak kişinin özel hayatı görüntülenebilmekte veya kayda alınabilmektedir[155].

Bilişim sistemlerinin veya teknolojilerin dahil olduğu suçlarda, sadece 134. madde dikkate alınarak yapılan suçlama, eksik olacak ve anlam karmaşasına yol açacaktır. Örneğin; bir kişinin sosyal medya hesabını kanuna aykırı şekilde ele geçirerek, kişiye ait özel görüntülerin paylaşılması durumunda failin, TCK'nın 243. maddesi ile devamı maddelerinden mi yargılanacağı, yoksa TCK'nın 134. ve devamı maddelerden mi yargılanacağı sorun yaratmaktadır. Bu konuya ilişkin ayrıntılı yorum, TCK'nın 135.maddesinde düzenlenen Kişisel Verilerin Kaydedilmesi ve 136. maddesinde düzenlenen Verileri Hukuka Aykırı Olarak Verme ve Ele Geçirme Suçunu inceledikten sonra yapılacaktır.

---

[152]Soyaslan, s. 344.
[153] Tezcan/ Erdem/Önok, s. 643.
[154]Soyaslan, s. 345.
[155] Ayşe Arman, **Bu Röportajı Okuduktan Sonra Kameranızı Kapatacaksınız,** https://www.hurriyet.com.tr/bu-roportaji-okuduktan-sonra-bilgisayarinizin-kamerasini-yara-bandiyla-kapatacaksiniz-23369267, e.t.: 22.12.2021.

2.1.1.2.2.4. Kişisel Verilerin Kaydedilmesi Suçu

Kişisel verilerin kaydedilmesi suçu TCK'nın 135. maddesinde düzenlenmiştir. *"Kişisel verilerin kaydedilmesi"* başlıklı 135. Madde

> *"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.*
>
> *(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."*

şeklindedir.

Bu düzenleme, kişisel verilerin hukuka aykırı olarak kaydedilmesini suç saymıştır. Korunan hukuki yarar özel hayat ve hayatın gizli alanı ve özel olan kişisel verilerdir[156]. Mağdurun ve failin herkes olabileceği bu düzenlemede, suçun maddi unsuru verilerin kaydedilmesidir.

Verilerin ne şekilde ve nereye kaydedildiğinin önemi yoktur. Yani fail, mağdur hakkında fiziki belgeler veya dokümanlarda tutmuş olabilir veya dijital ortama kayıt altına almış da olabilir. Bu durumun, mevcut düzenlemede suçun oluşması bakımından bir farkı yoktur. Ancak, dijital ortama atılan her bilginin, dijital bir veri özelliği kazanması, suçun mağdur üzerinde yaratacağı etkiyi etkileyecektir.

Kişisel verilerin kaydedilmesi suçu, kişinin bilişim sistemine girilmesi suretiyle gerçekleştiği zaman, ortaya TCK'nın 243. maddesinde düzenlenen *"hukuka aykırı olarak bilişim sistemine girme veya kalma"* suçu gündeme gelecektir. Burada faile ayrıca, TCK'nın 243. maddesinden ceza verilmeyecektir. Çünkü, bilişim sistemine girme ve kalma ile 243.maddededüzenlenen suçun,135. maddedeki suçun oluşması için gerçekleştirilen bir geçit suçudur. Ancak fail, mağdurun bilişim sistemi içerisindeki kişisel bilgileri kaydetmesi durumunda, TCK'nın 135. maddesindeki düzenleme karşısında bu suçtan da yargılanacaktır. Failin burada bilişim sistemi içerisinde ele geçirdiği kişisel verileri yayması durumunda, TCK'nın 136. maddesinde yer verilen verileri hukuka aykırı olarak verme veya ele geçirme suçu oluşacaktır.

[156]Soyaslan, s. 349.

Kanun koyucu bu düzenlemenin gerekçesinden de anlaşılacağı üzere, kişisel verileri korumayı aynı zamanda Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 Tarihinde imzaladığı veKişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında BireylerinKorunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokolün onaylanmasının uygun bulunduğuna dair kanunu onaylayarak[157], *Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmenin* ilgili hükümlerini iç hukukta geçerlilik tanımayı amaçlamıştır[158].

Gerçek kişi ile ilgili her türlü bilgi, kişisel veri olarak kabul edilmektedir[159]. Teknolojinin gelişmesi ile birlikte, bilgi işleme sistemleri büyük hız kazanmıştır. Özellikle devletler, özel şirketler gibi birçok bireyin bir arada bulunduğu yerlerde, bireylerin bilgileri belli amaçlarla kayıt altına alınarak işlenmekte ve işlenen bilgiler ile hayatın kolaylaştırılması veya bireylere hem sosyal hem de iş hayatında kolaylık sağlanması amaçlanmaktadır.

Örneğin, şirketler çalışanlarının sigorta girişleri için vatandaşlık numaralarını almakta ve kaydetmekte, sosyal medya kullanıcıları doğum tarihleri, hobileri, ilgi alanları gibi kişisel bilgilerini sosyal medya platformlarına kaydetmektedir.

TCK'nın 135. maddesi, kişilerin kaydedilen verilerinin, kullanım amacı dışında kaydedilmesini önlemek için getirilmiş bir düzenlemeyi içermektedir. Kaydedilen kişisel verilerin bilişim sistemlerine yüklendiği anda, dijital veri olması ve dijital veri haline gelen bu kişisel verilerin veri sahibinin rızası dışında kaydedilmesi veya kopyalanması TCK'nın 135. maddesinin konusunu oluşturmakta ve ayrıca kişilerin dijital verileri de çalınmış olmaktadır.

Her en suretle olursa olsun kişisel verilerin rıza gösterilen şartlar dışında kaydedilmesi, TCK'nın 135. maddesinin kapsamına girmekle birlikte, bu verilerin dijital ortamlarda kayda geçirilmesi, suçun işlenmesini kolaylaştırmakta ve fail/faillerin bulunmasını da zorlaştırmaktadır.

---

[157] 20 Nisan2016 Tarihli ve 6705 Sayılı, **Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun** için bkz. **Resmi Gazete**, 5 Mayıs 2016, Sayı: 29703.

[158] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 135. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 21.12.2021.

[159] Parlar/Öztürk, s. 531.

2.1.1.2.2.5.Verileri Hukuka Aykırı Olaraka Verme Veya Ele Geçirme Suçu

Verileri hukuka aykırı olarak verme veya ele geçirme suçu;

TCK'nın136. maddesinde,*(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.*

(2) ***(Ek:17/10/2019-7188/17 md.)*** *Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır."*

şeklinde düzenlenmiştir.

Bu düzenleme, TCK'da yer alan Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlıklı kısmına ait son suç tipidir. Bu düzenleme ile kişisel verilerin başkasına verilmesi ve ele geçirilmesi suç olarak belirlenmiştir. 136. maddede korunan hukuki yarar, TCK'nın 135. maddesinde olduğu gibi özel hayat ve özel hayat kapsamına giren kişisel verilerdir[160].

Söz konusu suçun faili, gerçek kişidir. Fail gerçek kişi olsa da gerçekleştirilen eylemler, tüzel kişiler lehine yapılabilir. Mağdur ise hem gerçek hem de tüzel kişi olabilir.

Suçun maddi unsurunu, verilerin verilmesi, yayması veya ele geçirilmiş olması eylemleri oluşturmaktadır. Failin, veriyi hukuka aykırı mı yoksa hukuka uygun olarak mı ele geçirdiğinin bir önemi olmayacaktır. İlgili maddenin gerekçesi incelendiğinde, kişisel verilerin ayrı bir suç olarak düzenlendiğine vurgu yapılmıştır[161].

Suçu oluşturan eylem, seçimlik hareketli bir eylemdir. Failin, verileri başkasına verme, ele geçirme veya yayma eylemlerinden birini gerçekleştirmesi, suçun oluşması için yeterlidir. Bu üç eylemin de ne şekilde gerçekleştiğinin (fiziki olarak, dijital ortamda başkasına verilebilir, ele geçirilebilir veya yayılabilir) önemi olmayacaktır. Dolayısıyla, bu suç serbest hareketli bir suçtur.

Suçun manevi unsuru genel kasttır. Fail, mağdura ait kişisel verileri isteyerek veya yanlışlıkla ele geçirdi ise de yanlışlıkla olduğunu bile bile başkasına vermesi, yayması, manevi unsur açısından suçun oluşumu için yeterlidir.

---

[160]Soyaslan, s. 353.

[161] Sinerji Hukuk Yazılımları, **Türk Ceza Kanunu 135. Madde Gerekçesi**, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.:21.12.2021.

Bir kişinin bilişim sistemine girilerek elde edilen dijital verilerin, ele geçirilmesi suçunda TCK'nın 243. maddesinde düzenlenen *"hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu"* şartlarının da gerçekleşmesi mümkündür. Ancak, 243. maddede düzenlenen suç tipi, TCK'nın özel hayatın gizliliği ve özel hayatın gizli alanına karşı suçların gerçekleştirilmesinde araç olarak kullanılmaktadır. Bu nedenle, fail ilgili düzenlemede yer alan eylemleri gerçekleştirdiğinde; sadece 136. madde kapsamında cezalandırılacaktır[162].

TCK'nın 132. ve devamında düzenlenen özel hayatın gizliliği ve özel hayatın gizli alanına karşı suçların nitelikli halleri, 157. maddede düzenlenmiştir. Nitelikli haller düzenlenirken özel hayatın gizliliği ve özel hayatın gizli alanına karşı suçlar ile korunan hukuki değerlere ilişkin eylemlerin, suçu kolaylaştıran halleri olarak düzenlendiği görülmektedir. Bu haller, kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesidir.

Dijital veri hırsızlığına ilişkin ayrı bir düzenlemenin yer almamasının getirdiği kargaşayı ortaya koyan ve en somut örneklerden biri deTCK'nın132. maddesi ile devamında yer alan özel hayatın gizliliği ve özel hayatın gizli alanına karşı suçların düzenleniş şeklidir. Kişiler arası konuşmanın ve söyleşilerin cihazlarla kaydedilmesi veya dinlenmesi, toplanan verilerin dijital bir veriye dönüşmesine sebep olmaktadır. Ayrıca, bu suç tiplerinin bilişim sistemlerine girilerek gerçekleştirilmesi durumunda, çok farklı büyük çapta etkileri olduğu görülmektedir. Yani, bir kişinin bilgisayar sistemine girerek hem görüntülü hem de sesli kayıt yaparak bunu aynı zaman da yayımlaması mümkündür. Bu şekilde gerçekleşen bir eylemin, mevcut düzenlemeye göre hangi suç kapsamında değerlendirileceğine ilişkin somut bir hüküm yoktur. Bu durum uygulamada kargaşaya yol açmaktadır.

TCK'da bilişim suçları ile ilgili düzenlemelerin; sürekli ihtiyaca göre benzediği suç tipleri arasında düzenlendiği ve suça konu eylemlere ilişkin tanımlamalarda teknik eksiklikler olduğu, bununda sıklıkla anlam karmaşasına yol açtığı görülmektedir. Bu durumu, Yargıtay Ceza Genel Kurul Kararı ile örneklendirmek gerekirse[163],karara konu olayda; sanık olan köşe yazarının, mağdurun fotoğrafını köşe yazısına koymak için mağdurun bilgisi olmadan çektiğini, sonradan da mağdurun fotoğrafını bir arkadaşlık

[162]Soyaslan, s. 356.
[163] Yargıtay Ceza Genel Kurulunun 17.06.2014 Tarihli ve 2012/12-1510 E., 2014/331 K. Sayılı İlamı, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#, e.t.: 19.12.2021.

sitesine yüklediğini, mağdurun çocuklu ve evli olduğunu, mağdurun erkek arkadaşı aradığına ilişkin asılsız açıklama ile oluşturulan sahte hesabın mağdurun öğrenmesine kadar olan sürede iki gün boyunca sitede kaldığı, sonrasında sanığın mağdurdan özür dileyerek hesabı sildiği belirtilmiştir. İlk derece mahkemesi,*"Özel hayatın gizliliğinin ihlali"* suçundan açılan davada, bu suç üzerinden mahkumiyet kararı vermiştir. Ancak, Yargıtay Ceza Genel Kurulu oyçokluğuyla bu olayda gerçekleşen eylemin, TCK'nın 134/2 maddesinde düzenlenen özel hayatın gizliliği suçunun değil, 136. maddesinde düzenlenen verileri hukuka aykırı olarak yayma suçunun oluşacağına karar vermiştir.

Yargıtay Ceza Genel Kurulu, ilgili kararı verirken TCK'da suç konusu olan *"kişisel veri"* kavramının tanımı olmadığı için o tarihte yürürlüğe girmemiş olan Kişisel Verilerin Korunması Kanunu taslağı, Avrupa İnsan Hakları Sözleşmesine, 28.01.1981 Tarihli ve 108 Nolu Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Uluslararası Sözleşmesi gibi ceza hukuku ile ilgili olmayan, ancak tanımlardaki yaşanan kargaşa nedeniyle açıklama yapmak zorunda kaldığı hususları, öğretiye de atıf yaparak kişisel verileri tanımlamaya çalışmıştır.

Söz konusu Karar, dijital verirleri temel alan bir bilişim suçlarına kanuna duyulan ihtiyacı ortaya koymaktadır. Çünkü, sürekli ortaya çıkan yeni durumlar karşısında, mevcut yasal düzenlemelerin içerisinde düzenlemeler yaparak oluşturulan hükümler, bilişim suçları alanını tutarsız, karmaşık bir alana çevirmeye devam etmektedir. Bu durum, ceza hukukunun kanunilik ilkesine de ağır darbe vurmaktadır.

2.1.2. Dijital Veri Hırsızlığı İle İlgili Türk Ceza Kanunu Dışında Yer Alan Düzenlemeler

Bilişim hukuku alanında dijital veri hırsızlığına ilişkin özel ve ayrıntılı bir düzenleme olmaması, bilişim hukukunun ve buna bağlı olarak dijital veri hırsızlığının etki alanına giren birden çok konu olması nedeniyle, dijital veri hırsızlığına konu olabilecek düzenlemeler dağılmıştır. Bu düzenlemelerin en önemlisini, Fikir ve Sanat Eserleri Kanununda (FSEK) yer alan hükümler oluşturmaktadır.

2.1.2.1. Fikri Ve Sanat Eserleri Kanunda Yer Alan Konusu Dijital Veri Hırsızlığını İlgilendiren Düzenlemeler

Teknolojinin ve dijital platformların gelişmesi ile birlikte, toplumda bu gelişmelere uyum sağlamaya başlamıştır. Toplumun uyum sağlaması, yeni fikri hakların ortaya

çıkması, fikri haklarla ilgili bloggerlik[164], içerik üretici gibi yeni mesleklerin doğmasına yol açmıştır. Müzik, sinema, yazarlık gibi alanların ise dijital platformlara taşınmasına sebep olmuştur.

Dolayısıyla, ortaya çıkarılan eserlerin çeşitli amaçlar ile eser sahibinin rızası dışında kullanımı teknoloji ile birlikte yaygınlaşmıştır. Bir dönemin korsan kasetleri ile başlayan bu eylemler, yerini saniyeler içerisinde binlerce kopya yaratılmasına bırakmıştır.

Dijital ortamlarda yer alan fikri ve sınai eserlerin, eser sahibinin rızası dışında kullanılmasının temelinde, dijital veri halini alan bu fikri ve sınai eserlerin çalınarak kullanılması yatmaktadır. Bu nedenle, fikri ve sınai eserlerin eser sahibi dışında kullanılması ile dijital veri hırsızlığı yakından ilgilidir.

Kanun koyucu, FESK'te[165] konusu ve eylem çeşitliliği yönünden iki tür ayrıma tabi tutmuştur. Birinci kısımda manevi, mali ve bağlantılı haklara tecavüz, ikinci kısımda ise koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri ilgili konular düzenlenmiştir.

2.1.2.1.1. Manevi, Maddi Ve Bağlantılı Haklara Tecavüz Suçu İle Dijital Veri Hırsızlığının İlişkisi

FSEK ile ülkemizde kişilerin emek sarf ederek ortaya çıkardığı düşün ile sanat ürünlerinin *"eser"* kavramı ile tanımlanarak koruma altına alınması amaçlanmıştır[166]. FSEK'te yer alan ceza konularının ilki, 71. maddede düzenlenmiştir.

71. maddede manevi, mali ve bağlantılı haklara ilişkin konular ayrıntılı bir şekilde ayrı ayrı açıklanarak yer verilmiştir.

71. madde, *"1. Manevi, mali veya bağlantılı haklara tecavüz*

Madde 7 1 Bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek:

> *1. Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair*

[164]Blogger, web sitelerine uygun yazı ve içerik sağlayan kişilere verilen addır.
[165] 05.12.1951 Tarihli ve 5846 Sayılı **Fikir ve Sanat Eserleri Kanunu**, **Resmi Gazete**, 13 Aralık 951, Sayı: 7981.
[166] Dülger, **Bilişim Suçları**, s. 538.

şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur.

2. Başkasına ait esere, kendi eseri olarak ad koyan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hâlinde, hapis cezasının üst sınırı beş yıl olup, adlî para cezasına hükmolunamaz.

3. Bir eserden kaynak göstermeksizin iktibasta bulunan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

4. Hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır.

5. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır.

6. Bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

Bu Kanunun ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına hükmolunur.

Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir."

şeklindedir.

FSEK'nın 71. maddesi ile hak sahibinin manevi, maddi ve bağlantılı hakları korunması amaçlanmıştır. Maddede ayrıntılı şekilde yer alan düzenlemede, fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakların ihlali, altı farklı kategoride sıralanmıştır.

İlgili düzenlemede korunan hukuki yarar, hak sahibinin fikir ve sanat eseri üzerindeki mali, manevi ve bağlantılı haklarının korunmasıdır. Hak sahibinin fikri ve eseri ile maddi gelir elde etmesi mali hak, hak sahibinin manevi ve mali haklarına zarar vermemek kaydıyla komşu hak sahipleri ile filmlerin ilk tespitini gerçekleştiren film yapımcılarının sahip oldukları haklar bağlantılı hak, manevi hak ise hak sahibinin ortaya çıkardığı fikir ve eserin hak sahibinde ortaya çıkardığı ve hak sahibine kazandırdığı duygu durumudur.

Bu düzenlemeye konu suç oluşturan eylemlerin, geniş bir yelpazeye sahip olduğunu ve en geniş tanımlamayla hak sahibinin rızası dışında fikir ve eser üzerinde gerçekleştirilen her türlü eylemin suç kapsamına alındığı anlaşılmaktadır. İlgili düzenlemede, mağdur fikir ve eser sahibidir. Fikir ve eser sahibi, ortaya çıkardığı fikir ve eserin tüm haklarını, üçüncü kişiye devrederse o zaman suçun mağduru fikir ve eser üzerindeki hak sahibi olacaktır. Fail ise hak sahibinin rızası dışında fikir ve eser üzerinde tasarrufta bulunan herkes olabilir. Suçun oluşumu yönünden failin genel kast ile hareket etmesi yeterlidir.

Teknoloji ile gelişen sistemlerde eser sahipleri artık eserlerini; yazılı, sesli, görüntülü yollarla eserlerini işleyerek kamuya sunmaktadır. Şarkıcıların besteleri kendi platformlarında veya *"youtube"* gibi video platformlarında, yazarlar eserlerini *"bloglar"* içerisinde yayımlayabilmektedirler.

Eser sahiplerinin eserlerini dijital platformlarda işlemesi, eserlerin dijital birer dijital veri halini alması, suç işleme veya daha özel ifade ile bu eserler üzerinden haksız kazanç sağlamak isteyenlerin hedefi haline gelmiştir.

Failler çeşitli şekillerde elde ettikleri başkalarına ait eserleri, anonim yollarla halka sunabilmektedir. Bu sayede, kendilerine ve üçüncü kişilere yarar sağlayabilmektedir.

Günümüzde, bu eylemlerin gerçekleşme şeklinin nerede ise tamamı dijital ortamlarda ve dijital yollarla olmaktadır. Eserlerin casus kamera ve yazılımlarla kayda alınması veya eserin oluşturulduğu platformlara zararlı yazılımlar ile sızdırılması sonucu gerçekleştirilen bir alenileşme söz konusu olmaktadır. Ortaya çıkan ve bir şekilde dijital ortama aktarılan eserin-dijital verinin, çalınarak alenileştirilmesi ile suça konu eylemler gerçekleşmiş olmaktadır.

71. maddede yer alan ve maddi haklara yönelik eylemler de vardır. Bu eylemlerin gerçekleşmesine de bilişim sistemleri büyük etki etmektedir. Bu eylemlerle amaç, eser üzerinden maddi kazanç elde etmektir.

Örnek vermek gerekirse; eserin çoğaltılması suça konu en temel eylem şeklidir. Çoğaltma ile kast edilen ortaya çıkarılan eserin ekonomik getiri amacıyla herkese ulaştırılması için sayılarının arttırılmasına yarayan ve bilişim sistemleriyle yapılan teknik işlemlerin tümüdür[167].

Bu eylem ile eser sahibinin maddi geliri elde edeceği geliri, fail eser üzerinden elde etmektedir. En çok rastlanan örneği, halka arz edilmeyen korsan kitaplar ve film yayınlarıdır. Yayımlanmamış bir filmin veya sadece sinema ortamında yayımlanan bir filmin, korsan internet sitelerinde yayımlanarak, izleyicilerin sinemaya gitmemesi veya satın alarak filmi izlemeye ihtiyaç duymaması sonucu ortaya çıkan bir kazanç kaybı söz konusudur.

Eserin, failin kendisi tarafından çoğaltılmış kopyasının satışa çıkarılması, eserin kiralama veya kamuya ödünç verilmesi suretiyle yayılması da maddi haklara yönelik gerçekleştirilen ve suç barındıran bir eylemdir. Eserin çoğaltılması ile benzerlik gösteren bu eylemlerin farkı; eserin, eser sahibinin elinden rızasıyla çıkması, ancak daha sonra rızası dışında çoğaltılması ve yayılmasıdır.

Eserin veri ağı iletim ağı üzerinden yayılması ve yayımlanmasına aracılık edilmesi, maddi haklara yönelik gerçekleştirilen bir eylemdir. Suç, fikir ve sanat eserlerinin radyo, televizyon, uydu ve kablo gibi telli telsiz yayın yapan kuruluşlar ile internet gibi sanal ağlar aracılığıyla halka arz edilmesi ile gerçekleşmektedir[168].

Bu durumda, esere ait dijital verilerin üçüncü kişiler tarafından çalınması ve istenildiği gibi eser üzerinden haksız menfaatler elde edilmesi kaçınılmaz olmaktadır. Bu nedenle,71. maddedeki düzenlemeye konu korunan hukuki yarar bakımından, eylemlerin tek bir madde içinde oluşturulmasından ziyade, düşünceme göre ayrı bir kanunda ayrı bir kısımda ayrıntılı şekilde ele alınması daha doğru olacaktır.

2.1.2.1.2. Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri İle Dijital Veri Hırsızlığı İlişkisi

FSEK'nın*"2. Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri***"**

Madde 72- (Değişik: 23/1/2008-5728/139 md.) Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla

[167] Dülger, **Bilim Suçları,** s. 548; Mustafa Albayrak, **Fikir ve Sanat Eserleri ile Markalar Aleyhine İşlenen Suçlar**, Ankara 2003, Adil Yayınevi, s. 23.
[168] Dülger,**Bilişim Suçları** s. 550; Yılmaz Yazıcıoğlu, **Fikri Mülkiyet Hukukundan Kaynaklanan Suçlar**, İstanbul 2009, XII Levha Yayıcılık, s. 303.

oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır. "

İlgili düzenlemede dijital ortamda yer alan eserlerin, eser sahibinin rızası dışında kullanımını engellemeye yönelik alınan tedbirleri etkisiz bırakmak için gerçekleştirilen eylemleri kapsamaktadır. Koruyucu programlardan kastedilen eser sahibinin rızası dışında eserin kullanımını engelleyen yararlı yazılımlardır[169]. Bu yazılımlar dijital veri hırsızlığını başta olmak üzere bilişim suçlarına konu olan eylemlerin engellenmesi amacı ile kullanılmaktadır.

Örnek vermek gerekirse internet sitelerinde yer alan bazı yazıların kopyalanamaması veya indirilememesi bu programlar sayesinde olmaktadır. Uydu alıcılarına takılan ve şifre çözücü diye adlandırılan, üyelik isteyen kanalları ücretsiz izlemenize yarayan aletler bu programları etkisiz kılmaktadır. Bilişim sisteminize atılan ver dijital verilerinizi kopyalayan zararlı yazılımlar bu programlar sayesinde engellenmektedir.

İlgili düzenlemede korunan hukuki değer koruyucu programlarmış gibi anlaşılsa da asıl korunan hukuki değer yine fikir ve sanat eseridir. Çünkü amaç fikir ve sanat eserinin korunmasına engelleyen programların etkisiz kılınmasının önüne geçmektir.

2.1.2.2. Elektronik İmza Kanununda Düzenlenen Bilişim Suçları İle Dijital Veri Hırsızlığının İlişkisi

Teknolojinin gelişmesi ile birlikte bilişim sistemleri, hem ticari hem de iş alanında hem de hayatımızda önemli yerler edinmeye başlamıştır. Özellikle, ticarette uzun mesafelerde yapılan ve yürütülen ticari işlerde, kamu alanında yürütülecek olan işlerde kullanılan e-devlet sisteminin temelinde, elektronik imza kullanılmaktadır[170].

5070 Sayılı EİK3.maddesinde Kanunda geçen kavramların tanımlamaları yapılmıştır. Buna göre, elektronik imza, *"Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi"*, elektronik veri ise "*Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları,"* şeklinde tanımlanmıştır. Özetle elektronik imza, dijital ortamda yer alan kişiye özel kodlamalar olarak tanımlanabilmektedir.

[169] En iyi antivürüsler, **En iyi Anti Virüs**, https://eniyiantivirusler.com/top10, et.: 23.12.2021.
[170] Dülger,**Bilişim Suçları,** s. 560.

Elektronik imza o kadar önemlidir ki fail, kişinin elektronik imzasını oluşturan elektronik veriler ile kopyalanmış bir e-imza ile e-devlet sistemine girerek kişi hakkında her türlü veriyi elde edebilmekte ve kullanabilmektedir. İşte bu durumu engellemek için EİK'nın 16. maddesi ve elektronik imza ile aynı nitelikte olan elektronik sertifikayı korumayı amaçlayan 17. maddesi düzenlemiştir.

Fail tarafından elektronik imza oluşturmak için ister söz konusu veriler elde edilsin, verilsin, kopyalansın, imza kopyalama araçları üretilsin veya yeni elektronik imza oluşturulsun, isterse birkaç eylem birlikte gerçekleştirsin yine de bu suçu işlemiş olmaktadır[171]. Bu eylemler, EİK'nın 17. maddesinde düzenlenen elektronik sertifikalarda sahtekarlık suçu açısından da geçerlidir.

Bu suç tiplerinde suçun konusu tamamen dijital verilerdir. Ancak, bu dijital verilerin özel bir yanı vardır. Bu dijital verilerin özelliği, kişiler arasında güvenilirliği yüksek anlamlandırılan dijital birer mühürdür. Bu nedenle, bu dijital verilerin korunması, diğer birçok dijital verilerden daha önemlidir.

Kanun koyucu elektronik imzada sahteciliğin cezasının üst sınırını üç yıl hapis cezası olarak belirlerken, sertifika sahteciliğinin üst sınırını beş yıl olarak belirlemiştir.

Kanun koyucu EİK'da elektronik sertifkayı,*"Elektronik sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı,"*şeklinde tanımlamıştır.

Tek bir elektronik imza ile tek bir kişinin sistemine erişme imkanı varken, elektronik sertifika ile imza doğrulama verilerini çeşitli kimlik bilgilerine bağlayarak birçok kişinin kişisel bilgisine ulaşılabilmektedir. Bu durumda, oluşacak zarar daha geniş ve etkili olmaktadır.

Kanun koyucunun bu kadar korunması önem arz eden bir konuyu, ayrı bir kanun içerisinde düzenlemiş olsa da kanımca uygulanan yaptırımlar bakımından, korunan hukuki değer ile bağdaşmamaktadır. Elektronik imzaların kullanım alanı o kadar geniştir ki, verebileceği zarara ve suça konu eylemlerin gerçekleşme şekline göre, yaptırımların çeşitlendirilmesi gerektiği düşünülmektedir.

Dijital verilerin bu denli geniş alanda kullanılması, geniş uygulama alanı yer edinmesine neden olmuştur. Ancak, parçalı şekilde düzenlenen ve dijital verilerin hırsızlığının konu olduğu bu yasal düzenlemeleri tek çatı altında ve daha ayrıntılı şekilde düzenlemenin; hem uygulanırlığını hem de etkinliğini ile caydırıcılığını arttıracak nitelikte olacağını düşünmekteyim.

---

[171] Dülger, **Bilişim Suçları**, s. 567; Ali Karagülmez, **Bilişim Suçları ve Soruşturma–Kovuşturma Evreleri**, 5. Basım, Ankara, 2014, Seçkin Yayıncılık, s. 189,190.

ÜÇÜNCÜ BÖLÜM

DİJİTAL VERİ HIRSIZLIĞI İLE İLGİLİ ULUSLARARASI DÜZENLEMELER

Gelişen dünyada insanların yaşantılarını oluşturan çerçevenin sınırları genişlemektedir. İnsanların işleri, sosyal hayatları, eğitimleri gibi insan hayatına etki eden faktörler, ülke sınırlarını aşmakta ve bu sınır tanımayan gelişmeler gün geçtikçe daha da artmaktadır. Sınır tanımayan konular, her gün genişlemekte ve sadece insan hayatı ile sınırlı kalmamakta, ayrıca devletlerin politikaları, partilerin propagandaları gibi toplum düzenini ilgilendiren ilişkilerin de ülke sınırlarının dışına çıkmasına neden olmaktadırlar.

Ülkelerin fiziki sınırlarının; artık sadece insanların fiziki seyahatlerini engelleyen veya seyahatlerinin kontrol edilmesini sağlayan sınırlar olması dışında, herhangi bir özelliği kalmamıştır. Gelişen teknolojinin getirisi olarak verilerin, dünyanın her yerine saniyeler içerisinde ulaşabilir olması, birçok alanda da küreselleşme ve uluslararası birlikteliklerin kurulması zorunluluğunu doğurmuştur.

Küreselleşen toplum ve insan ilişkilerinde, kişilerin ve eşyaların hareketlerinin uluslararası platformda rahatlıkla hareket edebilir duruma gelmesi ve sınır ötesi hizmet veriminin kolaylaşması ve dijital verilerin kolay bir şekilde sınır ötesine aktarılabilir olması, sınır aşan suçları da beraberinde getirmiştir[172].

İnsan hayatının ve toplumsal yaşamın küreselleşmesi işlenen suçlara ilişkin küreselleşmeyi de beraberinde getirmektedir. Bunun sonucunda ise sınır aşan yeni suçlar meydana gelmeye başlamıştır. Teknolojik, ekonomik ve politik gelişmemeler ile birlikte küreselleşmenin ortaya çıkması, özellikle organize suç örgütlerinin sınır aşan bir niteliğe bürünmesine sebep olmuştur[173].

Suç işlemenin uluslararası platforma taşınmasından en çok etkilenen alanlarından biri de dijital veri hırsızlığıdır. Bunun temelini, dijital ortamda sınırların tamamen ortadan kalkması nedeniyle, denetimin hiç yapılamaması veya zor olması ve zararlı yazılımlar, suça konu bilişim sistemleri, bilişim sistemlerine yüklenen verilerin yoğunluğu ve benzeri şekildeki suçun unsurlarındaki hızlı değişimlerin getirdiği iz bırakmama ve anonimleşme durumları oluşturmaktadır.

---

[172]UlrichSieber, **Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku,** Editör: Feridun Yenisey/Salih Oktar/Zehra Başer Doğan, Seçkin Yayınevi, Ankara, 2021, s. 40.

[173]Merve Erdem/Gürkan Özocak, **Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği,** https://ab.org.tr/ab17/bildiri/110.pdf ,s. 1, e.t.: 27.10.2021.

3. Dijital Veri Hırsızlığı İle Mücadelede Uluslararası İşbirliği

Bilişim suçlarında verilerin transferinin de sınırların olmaması, faillerin bulundukları yerden dünyanın her hangi bir noktasına etki edebilecek şekilde eylemler gerçekleştirebiliyor olması, doğrudan ve dolaylı olarak bilişim suçları ile mücadeleyi uluslararası boyuta taşımıştır.

Bilişim suçlarında, failin suç işlediği yerin failin bulunduğu yerden farklı ülke sınırları içerisinde olması, eylemin yapıldığı ülke ile etkisinin görüldüğü ülkelerde farklılıklar olması, gerçekleşen eyleme ve yasal düzenlemelere ilişkin tanımlarda farklılıklar meydana gelmesi, uygulanacak ceza ve ceza usul hukuku hükümlerinde farklılık olması, bu suçlarla mücadeleyi zorlaştırmaktadır.

Bilişim suçlarında, suçun unsurlarına ilişkin ve uygulanacak olan yasal düzenlemelerdeki bu farklılıklardan dolayı, bilişim suçları ile mücadele ederken ülkeler birçok sorun yaşamaktadır. Bu nedenle, devletlerin özellikle bilişim suçları açısından uluslararası alanda işbirliği yapmaları, ihtiyacın ötesine geçmiş zorunlu bir işbirliği noktasına gelmiştir. Bu bakımdan, Avrupa ülkeleri başta olmak üzere, diğer dünya ülkeleri bilişim suçlarına karşı mücadelede ortak adımlar atmaya başlamışlardır.

3.1. Dijital Veri Hırsızlığı İle Mücadelede Uluslararası İşbirliğinin Önemi

Bilişim suçları ile mücadelenin zorlukları, bu suçlarla doğrudan bağlantılı olan dijital veri hırsızlığı ile ilgili zorlukları da beraberinde getirmektedir. Bilişim suçları ile mücadeledeki zorluklar birkaç noktada toplanabilir.

1.Bilişim suçlarının analiz ve çözümlemesinde yaşanan zorluklara bağlı olarak, bu suçlarla mücadelede, kaynakların kullanımı sorunu ortaya çıkmaktadır. Ayrıca, bu suçlar ile siber suçların failler yönünden, gittikçe popüler olması nedeniyle, suçların işleniş biçimleri yönünden de, şablonların çıkartılması imkansız hale gelmektedir.[174]. Bu bağlamda, faillerin bulunması için kullanılacak teknolojilerin nedenli gelişmiş olması gerektiği, hangi bilişim suçlarında ne kadar ve hangi vasıfta insan gücü harcanacağı gibi suçlarla mücadelede kullanılan kaynakların kullanımı noktasında da sorunlar yaşandığı görülmektedir.

Ülkelerin kendi sınırları içerisinde karşılaştıkları bilişim suçu tiplerini ve bu suç tiplerine ilişkin verileri ve analizlerini birbirleriyle paylaşmaları, benzer suç tipiyle ilk

[174]Murat Önok, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi , Prof. Dr. Nur Centel'e Armağan**, https://dergipark.org.tr/tr/pub/maruhad/issue/48280/623844, s. 1232, e.t.: 26.10.2021.

defa karşılaşan diğer ülkelerin kaynaklarını, doğru şekilde kullanarak, bu suçlara karşı daha etkili mücadele yapılmasını sağlayacaktır.

2.Bilişim suçları ile mücadelede bir diğer sorun, ceza muhakemesinde görev alan kişi, makam ve mercilerin, bilişim suçlarıyla ilgili teknik bilgilerinin yeterli derece olmamasından kaynaklanmaktadır.

Kolluk kuvvetlerinin, bilişim suçlarına ilişkin konularda, delil toplama aşamasında bulunmaları ve bilişim suçları büro amirliği gibi daha özel alanlarda çalışmaları sonucu, teknik bilgiye yargı makamlarından daha çok sahip oldukları görülmektedir. Ancak, özellikle yargının işleyişinde yer alan savcılar ile hakimlerin, bilişim ve siber suçlar konusunda teknik bilgi eksikliği nedeniyle, suçların soruşturulması ve kovuşturulması noktasında, kimi aksaklıkların yaşandığına ve hataların yapıldığına sıklıkla karşılaşılmaktadır.

3.Bilişim suçları ile mücadelede bir başka önemli sorun da maddi ceza hukukundaki tanımlamaların ve suçların kanuni unsurlarının, farklı ülkelerin hukuklarındaki tanımlarla uyum içinde yeknesak biçimde olmamalarının ortaya çıkardığı istikrarsız uygulamalardır[175].

Maddi hukukta ortaya çıkan bu farklılıklar ve belirsizlikler bilişim suçları ile mücadeleyi zorlaştırmaktadır. Ancak, ülkelerin etkili bir işbirliği ile maddi hukuklarında uyumlu ve tutarlı düzenlemeler yapmaları halinde, sürekli kendisini yenileyen bilişim suçlarına karşı, daha etkili bir yok izlenebilmesi mümkün olacaktır.

4.Bilişim suçları ile mücadelede en çok karşılaşılan sorunlardan bir diğeri ise suça ilişkin eylem ile neticenin farklı ülke sınırları içerisinde yer almasıdır. Örneğin, bir siber saldırı, dünyanın her hangi bir noktasından başka bir noktasına yapılabilmektedir. Terör propagandaları, terör örgütleri tarafından tek bir yerden aynı anda dünyanın birçok noktasına ulaştırılabilmektedir. Gerçekten fail ile mağdur arasında sınır farklılıklarının olması, devletlerin egemenlik eşitliği ilkesi karşısında zorluklar çıkarmaktadır. Dolayısıyla, hangi devletin yasalarının uygulanacağının sorununu ortaya çıkmaktadır. Her devletin egemenliğine dayanarak kendi kanunlarını uygulamak istediği durumda, uluslararası işbirliğinin önemi daha da artmaktadır. Bu bakımdan, özelikle soruşturmaya ilişkin uyumlaştırılmış uniform kanunların yapılması, bilişim suçlarına ilişkin eylemlerin ve faillerinin tespitini kolaylaştıracaktır.

---

[175]Önok, s. 1233; Hasan Sınar, Galatasaray Üniversitesi Yayınları **Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme, Prof. Dr. Çetin Özek Armağanı**, İstanbul, 2004, s. 766; Dülger, **Bilişim Suçları,** s. 103.

5. Failler tarafından suçların, bilişim yoluyla işlenmesinin tercih edilmesinin en önemli nedenlerinden biri de faillerin ve faillere ulaşmakta kullanılan delillerin zorluğunda yatmaktadır.

Bilişim suçlarına ilişkin faillerin ve delillerinin tespitine ilişkin zorluğun temelinde, internet üzerinden anonim şekilde birçok eylem yapılabilmesinin olanaklı olmasıdır. Bilişim sistemlerinin kullanımının sürekli olarak değişmesi, yeni yöntem ve sistemlerin oluşturulması, bilişim sistemlerine ilişkin suçlarda faillerin tespitine yarayan delillerin fark edilerek toplanmasını zorlaştırmaktadır. Bu suçlara ilişkin delilleri toplamanın zorluğunun yanında, delillerin toplanmasında ülkeler arasındaki uygulanan delil toplama usullerine ilişkin farklılıkların da olması, soruşturmaları zorlaştırmaktadır[176]. Faillerin tespiti ve delillerin hızlı ve kaybolmadan toplanması için bilişim suçları ile mücadelede ülkelerin uyumlu yasal düzenlemeler ve kendi aralarındaki protokoller yapmak suretiyle birlikte çalışmalarının önemi gün geçtikçe artmaktadır.

6.Bilişim suçlarında özellikle dijital veri hırsızlığında, failler kısıtlı maddi imkanlar ile topluma, kurum ve kuruluşlar ile kişilere çok büyük zararlar verebilmektedirler. Ancak, bu suçlarla mücadele ederken lojistik harcamalar, personel masrafları, kullanılan teknik sistemler ile zarar verilmiş olan bilişim sistemleri veya zarar gören dijital veriler göz önüne alındığında, çok büyük oranda maddi kayıplar olabilmektedir. Daha somut bir örnek ile anlatmak gerekirse bilişim suçlarının verdiği zararı, bir inşaat yapımı için işçilerin emekleri, malzemeler, ustaların sanatları, harcanan malzeme paraları ve harçların tek bir dinamitle patlatılarak kullanılmaz hale gelmesi gibi düşünülebilir. Ülkelerin işbirliği içerisinde koordineli şekilde hareket etmeleri, maddi kayıpların ve harcamaların azalmasına yardımcı olacaktır.

7. Bilişim suçları ile mücadeleyi zorlaştıran ve en çok karşımıza çıkan durumlardan biri, bilişim suçlarına ilişkin hiç yasal düzenleme yapmayan ya da yeterli düzenlemeye sahip olmayan ülkelerin varlığıdır.

Yasalarında bilişim suçlarının suç olarak düzenlemesi yeterli olmayan veya hiç düzenleme bulunmayan ülkeler, bilişim suçlarını gerçekleştiren failler tarafından kaçış noktası olarak görülmektedir. Öğretide yer verildiği üzere, bilişim suçları ile

[176]Önok, s.1236.

mücadelenin Dünya çapında yapılması gerekliliğinin kabul edilmiş olmasının[177]nedeni de failler için kaçış ve ele geçirilememe bakımından, yasalarında bilişim suçlarıyla mücadeleye ilişkin yeterli düzenlemelere sahip olmayan ülkelerin varlığıdır. Bu ülkelerle uluslararası alanda işbirliği yapılmalı ve iç düzenlemelerinde, bilişim suçlarına ilişkin düzenlemeler yapmaları veya var olan bilişim suçlarına ilişkin düzenlemelerinin uluslararası alanda kabul görmüş temel kriterlere getirilmesi sağlanmalıdır. Bu şekilde bilişim suçu faillerinin saklanmasını ve işledikleri suçlara ilişkin delillerin karartılmasını engellemek daha kolaylaşacak ve mümkün olabilecektir.

Ülkelerin bilişim suçlarına ilişkin işbirliği, bilişim suçlarına ilişkin ortak tanımlar yapmak, devletlerarasındaki bilişim suçlarına ilişkin düzenlemelerde uyumluluğu sağlamak, bilişim suçları ile mücadelede diğer ülkeler ile uyumlu olacak şekilde ceza usul hukuku kurallarına uyum sağlamak noktasında toplanmaktadır[178].

Dijital veri hırsızlığının konusunun maddi varlığa yönelik olması özellikle sanal mal varlıklarının arttığı bu dönemde, sanal mal varlıklarını, faillerin hedefi haline getirmiştir. Örnek vermek gerekirse, Dünyada en çok kullanılan kripto para birimi olan *"Bitcoin"* adlı sanal paranın, 2021 yılı Haziran ayındaki işlem hacmi yaklaşık 1.7 trilyon dolardır[179]. Bu hacimdeki bir para piyasası, devletlerin de dikkatini çekmiş ve devletler bu nedenle kripto paralara ilişkin düzenlemeler yapma ihtiyacı hissetmiştir. Örnek olarak, El Salvador *"Bitcoin"* kripto parasını kabul eden ilk ülke olmuştur[180]. Bunun yanında birçok ülke, kripto paraların kaynağının bilinmemesi ve takip edilememesi nedeniyle, kripto parayı kara para aklama yeri olarak kabul etmektedirler. Yasa dışı yollarla kazanılan parayı ifade eden kara paraların[181], kripto paralar aracılığıyla rahatça hareket edebiliyor olması, devletlerin rahatsız olduğu bir konu haline gelmiştir.

Özellikle, konusu ekonomi olan suçların temelini oluşturan kara paraların taşınması, saklanması, kullanımı devletlerin sıkı denetimine tabi tutulmasına karşın, kripto para kullanımı ile birlikte kara paraların aklanmasının önü açılmış olmaktadır. Kripto

---

[177]Önok, s. 1236; Esposito, G. (2004), "TheCouncil of Europe Convention on cyber-crime: a revolutionaryinstrument?", in Broadhurst, R. (Ed.), Proceedings of the 2nd AsiaCyberCrimeSummit, CentreforCriminology: University of Hong Kong, Hong Kong, s. 54'ten naklen Broadhurst s.412.

[178] Erdem/Özocak, **Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği**, https://ab.org.tr/ab17/bildiri/110.pdf ,s. 3, e.t.: 27.10.2021.

[179]BigPara, **Piyasa Hacmi 1.7 Trilyon Dolarda! İşte Son Gelişmeler**, https://bigpara.hurriyet.com.tr/haberler/bitcoin-haberleri/piyasa-hacmi-17-trilyon-dolarda-iste-son-gelismeler_ID1470152/, e.t.: 27.10.2021.

[180]**BBC, Bitcoin: El Salvador, kripto parayı resmi para birimi olarak kabul eden ilk ülke oldu.** https://www.bbc.com/turkce/haberler-dunya-58474009, e.t.: 25.10.2021.

[181] Kara Para, **Türk Dil Kurumu Sözlük**, https://sozluk.gov.tr/, e.t.:25.10.2021.

paralar; kara paraların kullanımı ve aklanması dışında, vergi kaçırma gibi insanlar ve ülkeleri de etkileyen alanlarda da kullanılmaya başlamıştır. Kripto paraların bu şekilde kullanılması, devletleri kripto paralara karşı önlem ve tedbirler almaya zorlamıştır. Örneğin, Çin Hükümeti, kripto paraların para birimi olmadığını ve geleneksel para ile piyasalarda bulunmamasını ve gezmemesi gerektiğini belirtmiştir[182].

Kripto paraları tehdit olarak görerek tedbir almaya çalışan bir diğer örnek ülke ise ABD'dir. Bilişim suçları faillerinin, fidye yazılımları-zararlı yazılımlarla gerçek ve tüzel kişilerin dijital verileri çalınarak veya dijital verilerin bilişim sistemi içerisinde kullanılması engellenerek kişilerden fidye istemeleri, istenilen fidyenin ise kripto para borsalarından olan *"Suex"* adlı bir borsa üzerinden yapılması nedeniyle, ABD bu durumu engellemek amacıyla harekete geçmiştir. ABD, *"Suex"* borsasının sekiz adet fidye olayında, suçun işlenmesini kolaylaştırdığı gerekçesiyle ABD'yi ilgilendiren kurum ve kuruluşlar ile çalışmasını yasaklamıştır[183]. Kripto paraların güncel bir konu olması ve olmaya devam etmesi nedeniyle, bu örnekleri çoğaltmak mümkündür.

Uluslararası suçlarda, bilgi aktarımın ve haberleşmenin yine dijital veriler üzerinden yapılması, özellikle örgütlü suçlarda talimatların bilişim sistemleri üzerinden veri aktarımı suretiyle gerçekleştirilmesine imkân sağlamaktadır. Teknolojinin ve veri kodlamanın çok hızlı bir şekilde geliştiği her gün, yeni yöntemlerin türediği bilişim dünyasında, bilişim suçlarına ilişkin konularda ülkelerin işbirliği yapma ihtiyacı ve zorunluluğu kendiliğinden ortaya çıkmaktadır. Bu nedenlerle, ülkeler ortak şekilde çeşitli düzenlemeler oluşturma gayreti içine girmişler ve düzenlemeler yapmışlardır.

3.2. Dijital Veri Hırsızlığına Konu Olabilecek Türkiye'yi De Etkileyen Uluslararası Düzenlemeler

Bilişim suçları çok geniş bir alanı kapsamaktadır. Ancak, bilişim suçlarının temelinde bilişim ortamındaki dijital verilerin hukuka aykırı bir biçimde ele geçirilmesi, nakledilmesi, başkalarına aktarılması, verilmesi veya işlenmesi fiilleri yer almaktadır. Bilişim suçlarının temelinde, dijital veri hırsızlığı olduğu için çalışma, dijital veri hırsızlığı üzerine yoğunlaşmaktadır. Bilişim suçlarını engellemek, dijital veri

[182] NTV, **Çin'den Kripto Para Açıklaması,** https://www.ntv.com.tr/ekonomi/cinden-kripto-para-aciklamasi,1rCQCR82MkucGsNG1HW61w, e.t.: 26.10.2021.
[183]HaberTürk, **ABD Hazine Bakanlığından Kripto Para Borsasına Yaptırım**, https://www.haberturk.com/abd-den-kripto-yaptirimi-abd-hazine-bakanligi-ndan-flas-karar-kripto-para-haberleri-3198422-ekonomi, e.t.:26.10.2021.

hırsızlığının önüne geçmek ve gerçekleştirilen suçlara daha hızlı müdahalelerde bulunmak için ülkeler arasında uluslararası düzenlemeler yapılmış ve kabul edilmiştir.

Bu sayede, ülkeler taraf oldukları veya kabul ettiklerini ilan ettikleri bilişim suçlarına ilişkin düzenlemeler ile iç hukuklarını uyumlaştırmaya çalışmıştır. Örneğini bunlardan en önemlisi Avrupa Birliği Siber Suçlar Sözleşmesidir.

3.2.1. Avrupa Birliği Siber Suçlar Sözleşmesi

Avrupa Birliği Siber Suçlar Sözleşmesi[184], bilişim suçlarını konu alan ilk sözleşme niteliğini taşımaktadır[185]. Sözleşme, *"Avrupa Birliği Siber Suçlar Sözleşmesi"* olarak tercüme edilse de Sözleşmenin uygulanmasına ilişkin kanun tasarında *"Sanal Ortamda İşlenen Suçlar Sözleşmesi"* olarak anıldığı için Sözleşme hukukumuzda bu adıyla yer almaktadır[186].

Avrupa Birliği, 1990'lı yıllarına sonunda gelişen teknoloji ile birlikte, suç tiplerinde de teknolojilerin kullanılmaya başladığını ve doğrudan ve dolaylı şekilde teknoloji ile bağlı suçların gerçekleştirildiği fark etmeye başlamıştır. Bu durum, suç sorunlarıyla ilgilenen Avrupa Komitesinin dikkatini çekmiştir.

Sözleşmenin başlangıcını, Suç Sorunlarına İlişkin Avrupa Komitesinin, Avrupa Konseyine 1996 yılında siber suçlara ilişkin uzman bir komite kurması tavsiyesinde bulunmasına dayanmaktadır[187].Avrupa Konseyi Bakanlar Komitesi, bu tavsiye üzerine 1997 yılında *"Siber-Uzay Suçları Uzmanlar Komitesini"* kurmuştur[188]. Komitenin adından da anlaşılacağı üzere Siber-Uzay Suçlarını inceleyen bir komite kurulmuştur. Komitenin isminde sadece *"Siber"* kavramının yer almayıp aynı zaman da *"Uzay"* kavramına da yer verilmesinden dolayı, siber suçlara konu olan teknolojilerin yeni gelişmeye başlaması ve ortaya çıktığı dönemin *"Uzay Çağı"*[189] olarak nitelenen bir zaman dilimine gelmesinden kaynakladığını düşündürmektedir. Siber-Uzay Suçları

[184]**Avrupa Birliği Siber Suçlar Sözleşmesi** Türkçe metni için bkz. https://www.bg.org.tr/Doc/AvrupaBirligiSiberSuclarSozlesmesi.doc e.t.: 05.12.2021.
[185] Karagöz, **Bilişim Sistemlerine Giriş**, s. 128; Yavuz Erdoğan, s. 67.
[186] T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, B.02.0.KKG.0.10/101-612/3607 sayılı, 03.09.2012 Tarihli Kanun Tasarısı, https://www2.tbmm.gov.tr/d24/1/1-0676.pdf, e.t.:04.11.2021.
[187] Cahit Aliusta/Recep Benzer, Avrupa Siber Suçlar Sözleşmesi Ve Türkiye'nin Dahil Olma Süreci, **Uluslar Arası Bilgi Güvenliği Dergisi**, Cilt:4, No:2, s. 37, 2018, https://dergipark.org.tr/tr/pub/ubgmd/issue/43240/512829, e.t.: 07.11.2021; Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi, Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt: LIX, Sayı: 1-2, 2001, s. 3-10.,https://dergipark.org.tr/tr/download/article-file/95984, e.t.:13/01/2022.
[188]Aliusta/Benzer, s. 37; Council of Europe, Explanatory Report totheConvention on Cybercrime, https://rm.coe.int/16800cce5b, e.t.: 13/01/2022.
[189]Vikipedi, **Uzay Çağı**, https://tr.wikipedia.org/wiki/Uzay_%C3%87a%C4%9F%C4%B1, e.t.:10.11.2021.

Uzmanlar Komitesi, dört yıl süren çalışmaları sonucunda "*Sanal Ortamda İşlenen Suçlar Sözleşmesinin"* taslağını hazırlamışlar ve Budapeşte, 23.11.2001 yılı Kasım ayında ülkelerin imzasına sunulmuştur. Yeterli imzanın toplanması ile 1 Temmuz 2004 yılında yürürlüğe girmiştir[190].

Türkiye bu Sözleşmeyi (Sanal Ortamda İşlenen Suçlar Sözleşmesi) 10.11.2010 Tarihinde Strazburg'da imzalamış ve 22.04.2014 Tarihli ve 6533 Sayılı Uygun Bulma Kanunu ile kabul edilmiş ve 31.05.1963 Tarihli ve 244 Sayılı Kanunun 3. maddesine göre, Bakanlar Kurulunun 2014/6656 Sayılı Kararı ile onaylanması uygun bulunmuştur[191].

Sözleşme giriş kısmı hariç toplam dört bölümden ve kırk sekiz maddeden oluşmaktadır. Birinci Bölüm içerisinde tanımlamalara, İkinci Bölümde ulusal düzeyde maddi ve usul hukukuna ilişkin hükümlere, üçüncü bölümde uluslararası iş birliği için hükümlerine, dördüncü bölümde ise yürürlük ve çekincelere ilişkin hükümlere yer verilmiştir[192].

Yürürlüğe giren bu Sözleşmede, toplumu siber suçlara karşı koruyabilmek için öncelikle ortak bir ceza hukuku politikasının uygulanmasının gerektiği vurgulanmaktadır. Ortak bir ceza politikasının belirlenmesiyle birlikte, siber suçlarla mücadele için gerekli mevzuatların kabul edilerek ve uluslararası işbirliğinin daha kolay ve uyumlu şekilde sağlanması hedeflenmektedir. Bu sayede, siber suçlar ile yapılan uluslararası mücadelede ortaya çıkan ulusal mevzuat farklılıkları minimize edilmiş olacaktır.

Sanal Ortamda İşlenen Siber Suçlar Sözleşmesinin Giriş Kısmında, sözleşme ile ulaşılmak istenen amacın[193]:

-Bilişim alanına konu olabilecek suç tiplerine ilişkin tanımlamaların ve düzenlemelerin, taraf devletlerin yasal mevzuatlarında birbirleriyle uyumlu hale getirilmesini,

-Siber suçların ve elektronik delil içeren diğer suçların soruşturma ve kovuşturmaya ilişkin uygulanacak olan uygulamaya ilişkin ulusal usul hukuku kurallarının sözleşme ile tekelleşmesini,

-Bilişim alanına konu olacak suçların soruşturulması ve kovuşturulmasına ilişkin yeknesaklaşmayı sağlayarak uluslararası işbirliğinde bu suçlara ilişkin hızlı karar alma,

[190] Karagöz, s. 128.
[191] Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun için bkz. **Resmi Gazete**, 2 Mayıs 2014, Sayı: 28988. Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasına İlişkin Bakanlar Kurulu Kararı için bkz. **Resmi Gazete**, 9 Ağustos 2014, Sayı:29083
[192] Karagöz, s. 129.
[193] Aliusta/Benzer, s. 38; Önok, s. 1236.

hızlı harekete geçme ve güncel suç yöntemlerine ilişkin bilgi paylaşılmasını sağlamak, olduğu görülmektedir.

Sözleşme ile ulaşılması amaçlanan konular göz önüne alındığında, sadece bilişim suçlarına ilişkin suç tiplerini değil elektronik ortamda oluşturulan ve bilişim suçları ile bağlantılı suç tiplerine ilişkin delillerin toplanmasının da Sözleşmeye konu edildiği görülmektedir.

Elektronik ortamda oluşan veya oluşturulan deliller, faillerin bulundukları ülkenin sınırları dışında suç işlemeye teşvik eden bir durum olarak karşımıza çıkmaktadır. Suç işleme kastı ile hareket eden fail veya failler, suçu gerçekleştirecekleri ülke ile suça hazırlık yaptıkları ülkenin farklı olmasından faydalanmak istemektedir.

Bu duruma,*"Linked"* adlı iş hayatı sosyal paylaşım sitesinin 500 milyon kullanıcısının verilerinin çalınması olayı somut bir örnek olarak gösterilebilir[194]. Yaşanılan bu olayda 500 milyon kişisinin kullanıcı kimlikleri, isimleri, e-posta adresleri, telefon numaraları, cinsiyet bilgileri ve bu kişilerin diğer sosyal medya profillerine verilen linklere kadar çalındığı ve açık arttırma ile satıldığı öğrenilmiştir. Bu olayda, faillerin kişisel verileri birden çok site üzerinden ve farklı ülkelerden hareket ederek çaldıkları tespit edilmiştir. Failler dijital veri hırsızlığı yaparken bıraktıkları dijital izlerin takibinin ve toplanmasının zor olması amacıyla farklı ağlardan ve farklı bilişim sistemleri üzerinden eylemlerini gerçekleştirmişlerdir.

Son yıllarda artan terör propagandaları da bilişim sistemleri üzerinden dijital ağlar aracılığı ile yapılmaktadır. Terör örgütleri bilişim sistemleri üzerinden sanal ağlar yardımıyla maddi yardım, katılım çağrıları, gündem olma gibi amaçlar ile propaganda yapmaktadırlar. Bu propagandalar, her ne kadar bilişim suçu oluşturmasa da propaganda aracı olarak kullanılan yazılı, sesli ve görüntülü materyaller birer suç delili olduğu için bu delillerin toplanmasında uluslararası işbirliği önem kazanmaktadır. Bu nedenle, Sanal Ortamda İşlenen Suçlar Sözleşmesi konusu bilişim olan suçlarla birlikte dijital materyallerin kullanıldığı suçlara karşı mücadelede de işbirliğini içermektedir.

Siber Suçlarla Mücadele Sözleşmesi, siber suçlarla mücadelede işbirliği yaparken bir dengeden söz etmiştir. Siber suçlarla mücadele edildiği sırada, bireyin her hangi bir müdahale olmaksızın düşünme, düşündüklerini ifade etme, her tülü bilgi ve düşünceyi

[194]Linkeden: **500 Milyon Kullanıcının Verileri Çalındı, Açık Artırmada Satışa Çıkarıldı**, https://www.cumhuriyet.com.tr/haber/once-facebook-sonra-linkedln-milyonlarca-kullanicinin-kisisel-verileri-calindi-1826667, e.t.:12.11.2021.

sınırsızca arama, iletişim haklarını ve insanların temel hak ve özgürlüklerini gözeterek bir denge kurulması gerektiği vurgusu yapılmıştır[195].

Bilişim sistemleri ve sosyal ağalar ile kurulan iletişimin artması, kişiler arasındaki iletişimin alenileşmesini kolaylaştırmıştır. Kişiler arasındaki iletişimin suç unsuru içerip içermediğinin tespiti veya suç unsuru aranırken karşılaşılan özel verilerin korunması veya temel hak ve özgürlüklere giren kısımların ihlal edilmemesi arasında, ince bir çizgi bulunmaktadır. Bu ince çizginin aşılmaması için Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesinin Giriş Kısmında, siber suçlarla mücadele ile ilgili işbirliği yapılırken ulusal yasalarda yapılan düzenlemelerde, 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Konveksiyonu, 1966 Birleşmiş Milletler Uluslararası Sivil ve Siyasi Haklar Sözleşmesi ve diğer insan hakları ile ilgili sözleşmelerin dikkate alınmasındaki önemi vurgulamıştır.

3.2.1.1.Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesi Sistematiği

Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesi, Giriş Kısmı hariç toplam dört bölüme ayrılmıştır. Sözleşmenin dört bölümünün teknik, ceza ve yargısal konular ile işbirliğine ilişkin konuları düzenlendiği görülmektedir. Birinci Bölümde, bilgisayarla ilgili bir takım teknik tanımlara yer verilmiştir. İkinci Bölüm, kendi içerisinde üç kısma ayrılmış ve ulusal düzeyde, maddi ve usul hukukuna ilişkin hükümler düzenlenmiştir. Üçüncü Bölümde ise uluslararası platformda hukuksal işbirliğine ilişkin hükümlere ve Dördüncü ve son bölümde de Sözleşmenin yürürlüğüne ve çekincelere ilişkin hükümlere yer verilmiştir[196].

3.2.1.1.1.Avrupa Konseyi Siber Suçlar Sözleşmesinin Birinci Bölümü

Sözleşmenin Birinci Bölümünde 1. maddesinde Sözleşmenin amacına yönelik olarak tanımlara yer verilmiştir. Bu tanımlarda,

a. ""Bilgisayar Sistemi", bir program çerçevesinde, otomatik veri işlemi yapan bir veya birden fazla birbirine bağlı veya ilgili cihaz ve cihaz grupları; b. "Bilgisayar verisi", bir bilgisayar sisteminin belli bir fonksiyonu yerine getirmesini sağlayan uygun programları içeren, bir bilgisayar sistemi içinde işlem yapmaya uygun bir formda bilgi veya konsept ve bilgilerin sunumu; c. "Servis Sağlayıcı": i. Servis kullanıcılarının bir bilgisayar sistemi aracılığıyla, iletişim kurabilmelerini sağlayan herhangi kamu veya özel bir oluşum, ve ii. Bu tip bir iletişim servisi veya böyle bir servisin kullanıcıları adına, bilgisayar verisi işleyen veya saklayan herhangi bir oluşum; d. "Veri Trafiği",

[195] T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, B.02.0.KKG.0.10/101-612/3607 Sayılı, 03.09.2012 Tarihli Kanun Tasarısı, https://www2.tbmm.gov.tr/d24/1/1-0676.pdf, e.t.: 12.11.2021.
[196] Karagöz, s. 129.

iletişimin, orijinini, gideceği noktayı, tarih, zaman, boyut, süre veya temel servis tipini belirterek, o iletişimin bir zincirini oluşturan bir bilgisayar sistemi aracılığıyla yapılan bir iletişimle ilgili herhangi bir bilgisayar verisi,"

anlamına geldiği belirtilmektedir.

Ancak, anılan tanımların hem kavramsal olarak hem de içerik olarak yeterli olmadığı düşüncesindeyim. Zira, kavramlar tanımlarken dijital sistem olarak sadece bilgisayarların tanımlanması, Sözleşmede en önemli eksik noktayı oluşturmaktadır. Çünkü bilişim sistemleri, bilgisayar kavramının çok üzerinde bir kavram olup dijital veriler de sadece bilgisayarlarda işlenmemekte veya saklanmamaktadır. Diğer taraftan, *"Hizmet sağlayıcı ve trafik bilgileri"*, kavramlarında da bilgisayar aracılığıyla ve bilgisayar sistemleri ile işlenen verilerden söz edilmiştir. Oysa, siber suçların işlenmesinin bilgisayarla sınırlı olmaması ve bilişim sistemlerinin, bilgisayarı da kapsayan çok üst bir kavram olması nedeniyle bilgisayar kavramı yerine, bilişim sistemleri kavramı kullanılması konuyu açıklamaktan ve tanımlamaktan uzak kalmaktadır.

Ayrıca, Sözleşmede siber saldırılara ilişkin tanımlarda da eksiklik olduğu görülmektedir. Bunun en somut örneği ise, Sözleşmenin adında geçen *"siber suç"* kavramı dahi tanımlanmamış olmasıdır. Bunun yanı sıra, zararlı yazılımlar, hacker-bilişim sistemi korsanları gibi bilişim sistemlerinde yer alan ve siber suçlara konu olan kavramlara da yer verilmemiştir. Oysa bu kavramların her ülke düzenlemeleri ve uygulayıcılar açısından yoruma müsait olmayacak şekilde yapılmış olması ve böylece yeknesaklığın sağlanmış olması gerekirdi.

3.2.1.1.2.Avrupa Konseyi Siber Suçlar Sözleşmesinin İkinci Bölümü

Sözleşmenin İkinci Bölümün de, Ulusal Boyutta Alınacak Önlemler başlığı altında düzenleme yapılmıştır. Bu Bölüm, kendi içerisinde üç Kısma ayrılmış olup, Kısım I– Maddi Ceza Hukuku; Kısım II–Usul Hukuku; Kısım III- Yargı Yetkisinden oluşmaktadır.

Birinci Bölümde, ulusal hukuk sistemlerinde maddi ceza hukukunda düzenlenmesi öngörülen suç tiplerine yer verilmiştir. Bu suç tipleri sıralanırken bilişim suçlarını doğrudan ilgilendiren suç tiplerine öncelik verilmiş, devamında ise bağlantılı suçlara yer verilmiştir.

TCK'da *"Bilişim Alanında Suçlar"* başlığı altında yer verilen 243-246 maddelerindeki suçların düzenlenmesinin kaynağını, Avrupa Konseyi Siber Suçlar Sözleşmesinin İkinci Bölümü oluşturmaktadır. Sözleşmenin bu Bölümünde düzenlenen ve doğrudan bilişim suçları ile ilgili konuları düzenleyen maddeler, iç hukukumuzda doğru bir şekilde üç madde altında toplanmıştır. Bilişim sistemleri aracılığı ile işlenen suçlar ise iç hukukumuzda aracı kılınan suç tipleri arasında nitelikli hal olarak ayrıca düzenlenmiştir. TCK'nın 158/1-f maddesinde bilişim sistemleri kullanılarak işlenen dolandırıcılık suçunu düzenlenirken, 226. maddesinde çocuk pornografisi, FSEK'nın 71. maddesinde ise telif haklarına ilişkin suç tipleri yer verilmiştir[197].

İkinci Bölümün Birinci Kısmında yer alan suç tipleri, kendi içerisinde beş başlık altında toplanmıştır.

Birinci Başlıkta bu suçlar; "*Bilgisayar Veri Ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulunmasına Yönelik Suçlar "*başlığı altında; *"Yasadışı Erişim, Yasadışı Müdahale, Verilere Müdahale, Sistemlere Müdahale, Cihazların Kötüye Kullanımı* "şeklinde sıralanmıştır.

İkinci Başlıkta "*Bilgisayarla İlişkili Suçlar"* başlığı altında, *"Bilgisayarla İlişkili Sahtecilik Fiilleri, Bilgisayarla İlişkili Sahtekârlık Fiilleri"* olarak açıklanmış ve Üçüncü Başlıkta, " *İçerikle İlişkili Suçlar"* başlığı altında; "Çocuk Pornografisiyle İlişkili Suçlar" olarak düzenleme yapılmıştır.

Dördüncü başlıkta "*Telif Hakları ve Benzer Hakların İhlaline İlişkin Suçlar"* başlığı altında; *"Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar"* düzenlenmiştir. Bu konu ile ilgili somut bir örnek vermek gerekirse facebook, instagram gibi video ve müzikli içerik paylaşılabilen sosyal medyalara müzikli bir video yüklenildiğinde, *"Ülkenizde bu şarkı telif hakkı kapsamındadır"* şeklinde bir uyarı yapılmaktadır. Bu uyarıda yer alan *"Ülkenizde"* ifadesinin kullanılmasının nedeni, Türkiye'nin taraf olduğu sözleşmelerden kaynaklı telif hakları yönünden sorumluluğun olduğudur.

Beşinci Başlıkta, "*İlave Yükümlülükler ve Yaptırımlar"* başlığı altında; *"Teşebbüste Bulunmak ve Yardım ya da Yataklık Etmek"* eylemleri, *"Kurumsal Yükümlülükler"*, *"Yaptırım ve Önlemler"* düzenlenmiştir. Bu Başlıkta, İkinci kısımda düzenlenen suç tiplerinin, iç hukukta işlenmesi halinde gerekli yasal işlemlerin yapılması konusunda bir düzenleme yapıldığı görülmektedir.

[197] Karagöz, s. 130.

Sözleşmenin İkinci Bölümünün İkinci Kısmında, usul hukukuna ilişkin düzenlemeler yapılmıştır. İkinci Kısımda kendi içerisinde beş başlık altında düzenlenmiştir.

Birinci Başlıkta, "*Genel Hükümler"* başlığı altında; *"Usul hükümlerinin kapsamı, Şartlar ve Önlemler "*ile ilgili hükümlere yer verilmiştir.

İkinci Başlıkta,*"Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması"* başlığı altında *"Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması, Trafik Bilgilerinin Korunmasının Kolaylaştırılması ve Kısmen Açıklanması"* ile ilgili düzenleme yapılmıştır.

Üçüncü Başlıkta, "*Üretim Talimatı"* başlığı altında hükme yer verilmiş, Dördüncü Başlıkta, "*Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konulması"* başlığı altında, delillerin toplanmasına ilişkin düzenlemelere yer verilmiştir.

İlk dört başlıkta yer alan suçlara ilişkin delillerin toplanmasıyla ilgili olan maddelerin uygulanabilmesi için bilişim suçunun veya bilişim sistemleri ile bağlantılı suçun gerçekleşmiş olması gerekmektedir. Bu maddelerde, suça ilişkin dijital verilerin güvenli şekilde toplanıp saklanması ile bu dijital verilere ulaşılmasının kolaylaştırılmasına ilişkin düzenlemelerin iç hukuka alınmasına yönelik hükümlerin yer aldığı görülmektedir.

Beşinci Başlıkta, "*Bilgisayar Verilerini Gerek Zamanlı Olarak Toplanması"* başlığı altında, *"Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması, İçerikle İlgili Bilgilere Müdahale Edilmesi"* düzenlenmiştir.

Bu Başlıktaki düzenlemenin, veri trafiğinin gerçek zamanlı olarak toplanmasındaki amacın, gerçekleşmekte olan veya gerçekleşmesi muhtemel suçların tespitine ilişkin hükümler olduğu anlaşılmaktadır. Birçok bilişim suçunun tespiti için suçun gerçekleşmeye başladığı zaman, suça konu dijital verilerin takibi ve izlenmesi ile suçun engellenmesi ve fail/faillerin tespiti büyük önem taşımaktadır. Bu nedenle, Sözleşmenin bu kısmında, Sözleşmeye taraf ülkelerin, oluşan bu veri trafiğini gerçek zamanlı olarak, teknik imkânlarını kullanmak suretiyle toplamaları ya da kaydetmeler için gerekli yasal düzenlemelerin yapmaları gereği üzerinde durulmaktadır.

İkinci Bölümün Üçüncü Kısmında, *"Yargı Yetkisine*" ilişkin düzenlemeler yer almaktadır. Bu düzenleme ile yargı yetkisi açısından bir karmaşanın olmaması ve her hangi bir ulusal hukuk sisteminde uygulanan cezai yargı yetkisinin kapsam dışı bırakılmaması amaçlanmaktadır.

3.2.1.1.3. Avrupa Konseyi Siber Suçlar Sözleşmesinin Üçüncü Bölümü

Sözleşmenin Üçüncü Bölümünde, uluslararası işbirliği yapılırken uygulanacak genel ilkeler ve uygulanacak özel hükümler üzerinde durulmuştur. Üçüncü Bölümün Birinci Kısmında, düzenlenen genel ilkeler kendi içerisinde dört başlığa ayrışmıştır. Bu başlıklar sırasıyla, *" Uluslararası İşbirliğine İlişkin Genel İlkeler, İadeye İlişkin Genel İlkeler, Yardımlaşmaya İlişkin Genel İlkeler, Uluslararası Anlaşmaların Bulunmadığı Durumlarda Gelen Yardım Taleplerine İlişkin Usuller"*dir.

Sözleşmenin Üçüncü Bölümünün teması, 23. Maddedeki Temel İlkeler Kısmında belirlenmiştir. Devletlerarasındaki adli yardımlaşmanın en geniş ve etkili şekilde sağlanması için mümkün amacıyla uyumlu şekilde birlikte çalışılması, bu birlikteliğin bilişim suçları ile beraber elektronik ortamdaki diğer suç tiplerini ve elektronik ortamdaki suçlara konu delilleri de kapsayacak şekilde olması gerektiği vurgulanmıştır. Adli yardımlaşmanın Sözleşmenin öngördüğü şekilde yerel ve uluslararası anlaşmalar uyarınca yapılması gerektiğine de değinilmiştir.

Bu bağlamda, Üçüncü Bölümün devamında adli yardımlaşmaya ilişkin maddelerde, adli yardımlaşmanın uyum içerisinde istikrarlı şekilde uygulanması ve yürütülmesi için gerekli düzenlemelere yer verilmiştir. Bunlar iadeye ilişkin hükümler ve adli yardımlaşmaya ilişkin genel ilkeler ile Sözleşmenin kapsamadığı, ancak uluslararası adli yardımlaşmanın gerekliliğine ilişkin düzenlemelerdir.

Sözleşmenin Üçüncü Bölümünün İkinci Kısmında, dijital ortamda yer alan delil niteliği taşıyan ve adli yardımlaşmaya konu olabilecek verilerin elde edilip saklanmasına ilişkin düzenlemelere yer verilmiştir. Bu hükümlerde belirtilen amaç, veri trafiğinde yer alan veya dijital ortama yüklenmiş ve suça ilişkin bir verinin, silinmeden, çıkartılmadan ve kaybolmadan önce, tespit edilerek muhafaza altına hızlı şekilde alınmasını sağlamaktadır. Bununla birlikte, saklanan bu verilerin hızlı şekilde Sözleşme kapsamında üye devletlerin erişmesine açılması ve bu konuda yardımcı olunması da kararlaştırılmıştır.

3.2.1.1.4. Avrupa Konseyi Siber Suçlar Sözleşmesinin Dördüncü Bölümü

Avrupa Konseyi Siber Suçlar Sözleşmesinin Final Provizyonları-Son Hükümler başlıklı Dördüncü Bölümünde, Sözleşmeye taraf olunması, Bölgesel Uygulama Sözleşmenin Üyelere Etkisi, Deklarasyonlar, Rezervasyonlar, İhtilafların Çözümlenmesi, Sözleşmenin tabiiyeti, Sözleşmeden ayrılma konuları gibi Sözleşmeye ilişkin genel hükümler ve şartlar düzenlenmiştir.

Avrupa Konseyi Siber Suçlar Sözleşmesi, içerik bakımından eksik yönleri bulunsa da en kapsamlı ve doğrudan siber suçlarla mücadeleyi konu alan bir sözleşme niteliği taşımaktadır. Bu nedenledir ki, TCK'da yer alan bilişim suçlarına ilişkin düzenlemeler ile diğer maddelerde ve özel kanunlarda yapılan düzenlemeler, bu Sözleşme esas alınarak yapılmış ve güncelleştirilmiştir.

3.2.2. AB 95/46/EC Sayılı Veri Koruma Direktifi

Kişisel verilerin korunmasına ilişkin ulusal düzenlemelerin başlangıç noktası olarak 1970 yılında Almanya, 1973 yılında İsveç, 1974 yılında ise ABD'de hazırlanan yasa metinleri olarak görülmektedir[198]. Kişisel verilerin korunmasına ilişkin yasal düzenlemelerin uluslararası alana taşınması,28.01.1981 Tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ile gerçekleştirilmiştir.

1980'li yılların sonlarına doğru kişisel verilerin işlenmesi daha spesifik olarak yorumlanmış ve insanların özel hayatına ilişkin verilerden ayrı şekilde ele alınmaya başlanmıştır. Gelişmiş ülkelerin ekonomik ve siyasal politikalarında kişisel verilerin korunmasına ilişkin benzer hukuki düzenlemelere yer verilse de[199] 1980'li yılların sonlarında ortaya çıkan internet ve yeni bilişim sistemleri ile geniş ağlar kurulmuş, kişisel verilerin işlenmesi hızlanmış, bununla beraber kişisel verilerin elektronik ortamda kullanımı artış göstermiştir.

Ulusal mevzuatlarında kişisel verilerin korunmasına ilişkin düzenleme yapan devletlerin, internet ağı büyüyen ve hızlanan veri trafiğini kontrol etmesi ve uyum içerisinde çalışması zorlanmış ve uyumsuzluklar yaşanmasına ve kişisel verilerin korunmasına ilişkin çalışmalarda sorunlar ortaya çıkmaya başlamıştır. Bu nedenle, AB kişisel verilerin dolaşımına ilişkin bir çerçeve çizmek istemiş ve 20 Şubat 1995 Tarihli ve 95/46/EC Sayılı AB Veri Koruma Direktifini yürürlüğe koymuştur[200]. Bu Direktif taraf devletlerin kişisel verilerin korunmasına ilişkin yapılacak düzenlemeler için bir

---

[198] Council of Europe, **Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi**, https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf, ; Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler Ve Türk Hukuku Bakımından Değerlendirilmesi**, T.C. Kalkınma Bakanlığı Çalışma Raporu 6, Yayın No:2968, Yayın Tarihi :2017, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf, e.t.:16.11.2021.

[199] Akıncı, s. 3; İkbal Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara, Turhan Kitabevi, 2010, s. 3.

[200] **European Data ProtectıonSupervısor, Directive 95/46/EC,** https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, **e.t.: 25.12.2021.**

çerçeve niteliğinde kabul edilmiştir. Belirtmek gerekir ki, 20 Şubat 1995 Tarihinde kabul edilen Direktifin üye ülkeleri doğrudan bağlayıcı niteliği olmayıp tavsiye niteliğinde hazırlanmış bir düzenlemedir[201].

95/46/EC Sayılı AB Veri Koruma Direktifi, üye devletlerin veri güvenliğine ilişkin iç hukuktaki düzenlemelerinde uyum sağlanmasını ve üye ülkeler arasındaki veri trafiğinin güvenli şekilde işlemesini amaçlanmaktadır. 2000'li yıllarda internet kullanımının artarak devam etmesi, internet aracılığı ile sanal ortamlarda bilişim sistemleri aracılığıyla erişimin artması, beraberinde veri akışının ve trafiğinin hızlanmasına neden olmuştur. Teknolojideki devrim niteliğindeki gelişmelerin yaşanması ve veri trafiğindeki hızlanma nedeniyle, üye ülkelerin hukuk sistemlerindeki veri koruma hükümleri arasında, uyum bozulmuş ve ihtiyaçları karşılayamayacak düzeylere gelmiştir.

95/46/EC sayılı AB Veri Koruma Direktifinin yeni gelişmeler karşısında çizdiği çerçevenin yetersiz kalması, AB'nin amacı olan kişisel verilere ilişkin üye devletlerarasındaki uyumun sağlanması bakımından geride kalmasına neden olmuştur.

Direktifin yetersiz kalması nedeniyle, ortaya çıkan ihtiyaçlar doğrultusunda veri güvenliğinin sağlanması amacıyla üye devletlerin veri korumaya ilişkin düzenlemelerini mümkün olduğunca kapsayacak şekilde bir veri koruma tüzüğü hazırlanmıştır[202]. Hazırlanan veri koruma tüzüğü, 2016 yılı Mayıs ayında *"Avrupa Birliği Genel Veri Koruma Tüzüğü"* olarak kabul edilmiştir[203]

3.2.3. 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğünün (GDPR) Ortaya Çıkması

95/46/EC sayılı AB Veri Koruma Direktifi, bilişim alanındaki gelişmeler karşısında yetersiz kalmış ve bu nedenle, taraf devletlerarasında olması planlanan veri korumasına ilişkin ortak bir politika sağlanamamıştır.

Bilişim sistemindeki değişiklikler ve ortaya çıkan sorunlar karşısında, her devletin yeni çıkan sorunların, 95/46/EC Sayılı AB Veri Koruma Direktifinin dışında kalan alanlarda olması karşısında, yeni düzenlemeler yapmalarına neden olmuştur.

---

[201] Akıncı,s. 6.

[202] Murat Volkan Dülger, Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması, **Yaşar Hukuk Dergisi**, https://dergipark.org.tr/tr/pub/yhd/issue/52537/807628, C. 1, S. 2, Temmuz 2019, s. 71, e.t.: 19.11.2021.

[203] **Avrupa Birliği Genel Veri Koruma Tüzüğü (GPDR)**, Avrupa Birliği Bakanlığı Çevirisi, https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf, e.t.: 25.12.2021.

Devletlerin bağımsız şekilde veri korumasına ilişkin düzenlemeler yapması, ülkelerarası dolaşan veri trafiğinde güvenlik zafiyeti yaratmaya başlamış ve 95/46/EC Sayılı AB Veri Koruma Direktifinin amacı olan veri korumasına ilişkin ortak düzenlemelerin yapılması imkânsız hal almıştır. Hem bilişim sistemlerinde yeni kavramlar ve yeni ihlal şekillerinin ortaya çıkması hem de yargı sistemlerinin bilişim sistemlerini içerisine alan kararları, Veri Koruma Tüzüğünün (General Data ProtectionRegulation, GDPR) Özellikle bireyleri de kapsayacak şekilde düzenlenmesine sebep olmuştur.

Örnek vermek gerekirsek Avrupa Adalet Divanı (ATAD)'ın Google–İspanya Kararı litaratüre, " Unutulma Hakkı " olarak girecek kavramın çıkış noktası olmuştur[204]. Bu Karara göre İspanya vatandaşı MarioCosteja kendisi hakkında 1998 yılında yapılan bir haberin Google arama motorundan kaldırılmasını talep etmiştir. Bu talebi karşılık bulamayınca, Google İspanya ve Google Inc.'ye karşı hukuki süreç başlatmıştır. Bu davada, ATAD'ın verdiği karar ile arama motorlarını ve internet veri sağlayıcılarını, veri kontrolörü olarak saymış, kişilerin ise çevrim içi verilerinin üzerindeki kontrolüne değinmiştir.

ATAD Kararı, GDPR'nin düzenlenmesine etki eden kararlardan biri olmakla birlikte, aynı zamanda 95/46/EC Sayılı AB Veri Koruma Direktifinin, eskidiğinin ve yeni kavramlar ile yeni olgular göz önüne alınarak yeni bir düzenleme yapılması gerekliliğini gösteren en somut karar niteliğini taşımaktadır.

Ortaya çıkan karmaşadan dolayı, AB Komisyonu 25 Ocak 2012 Tarihinde 95/46/EC Sayılı AB Veri Koruma Direktifinde köklü değişiklikler içeren bir önerinin hazırlığını bitirmiş ve yayımlamıştır[205].

Gelişen teknoloji ile birlikte kişilerin verilerinin dijital ortamlarda otomatik işlemelere tabi tutulması, kişilerin verilerin trafiği hakkında yeterli bilgi sahibi olmaması, veri işleyen sistemlerin kişilerden aldığı rızanın usulen olması gibi nedenler, kişilerin dijital ortamlarda işlenen verilerinin güvenliğini tehlikeye düşürmüştür.

---

[204] Akıncı, s. 9, atfen, Karar C-131/12, Google Spain SL ve Google Inc. vAgenciaEspañola de Protección de Datos (AEPD) ve MarioCostejaGonzález, Adalet Divanı (Grand Chamber) of 13 Mayıs 2014, ECR [2014] 317, parag. 32-41.

[205] Proposalfor a Regulation of the European Parliamentand of the Council on the protection of individuals with Regard to theprocessing of personal dataand on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, C-7-0025/12, http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdfe.t.: 17/01/2022.

Verilerinin güvenliğini tehlikeye düşüren en somut örneği kişilerin, *"onayla, kabul ediyorum"* gibi uygulama indirdikleri veya bir internet sitesini kullandıkları sırada, gösterdikleri rızalara ilişkin şartların okumamasıdır. Her ne kadar kişiden usulen rıza veya onay alınsa da kişilere ilişkin veri paylaşımının bir kamu sorunu olması ve beraberinde birçok suça konu olabilmesi nedeniyle, taraf devletlerin kişilerin merkezde olduğu bağlayıcı, veri paylaşımını ayrıntılı şekilde düzenleyen bir metne ihtiyaç duyulmuştur.

Verilerin korunmasına her geçen gün daha çok ihtiyaç duyulması ve 95/46/EC Sayılı AB Veri Koruma Direktifinin yetersiz kalması nedeniyle, 2011 Yılı Haziran ayında ve 95/46/EC sayılı AB Veri Koruma Direktifinin yeniden düzenlenmesi gündeme gelmiştir[206]. 2012 yılında AB Komisyonu değişiklik teklifi hazırlamış, 12 Mart 2014 Tarihinde Avrupa Birliği Veri Toplama Tüzüğünün taslağı kabul edilmiştir. 25 Mayıs 2018 tarihinde de uygulamaya geçilmiştir.

Avrupa Birliği Genel Veri Koruma Tüzüğü, 95/46/EC Sayılı AB Veri Koruma Direktifinden farklı olarak bireyleri merkez alacak şekilde ve üye ülkeleri doğrudan bağlayacak şekilde düzenlenmiştir. AB direktifleri, üye ülkeleri doğrudan bağlayıcı bir niteliği sahip olmamakla birlikte, üye ülkeleri yönlendirici ve tavsiye niteliğinde kararlardır. Üye devletler direktiflerdeki ilkeleri zaman içerisinde, iç hukuklarında uygulamaları gerekir. AB Bakanlar Konseyi tarafından çıkarılan tüzükleri ise AB direktiflerinden farklı olarak tüm üye ülkeleri kapsayıcı ve doğrudan uygulanabilir niteliğe sahiptir[207].

AB'nin 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ile veri korumasına ilişkin düzenlemeyi direktif yerine tüzük olarak düzenlemesi ile verilerin korunmasına zaman içerisinde daha çok önem verdiğini göstermektedir.

Verilerin korunmasına ilişin köklü değişikliklerin yapılması ihtiyacı, verilerin dijital ortamlarda işlenmesi ve dijital ortamlarda oluşan veri trafiğinin artması sebep olmaktadır. Gelişen teknoloji ile birlikte bilişim sistemlerindeki gelişmelerin ve verilerin dijital boyuta taşınması, *"dijital veri"* kavramının öne çıkmasına sebep olmuştur.

---

[206] Dülger, **Avrupa Birliği GDPR**, s. 85, atfen, ComprehensiveApproach on Personal Data Protection in theEuropeanUnion, June 2011, https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-dataprotection_en

[207] **Mehmet Nuri Tapan**, "Avrupa Birliği (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri: Avrupa Adalet Divanı", **Türkiye Barolar Birliği Dergisi**, S. 3, Y. 1998 (s. 971-1020), s. 993 vd. http://tbbdergisi.barobirlik.org.tr/m1998-19983-879, e.t.: 03/01/2022.

Toplumdaki düzeni ve refahı sağlanmasını amaçlayan devletler ve uluslararası kuruluşlar gerçekleşen teknoloji devrimi karşısında, toplumun düzenini sağlamak için oluşturdukları hukuki düzenlemelerle aynı hızla karşılık vermeye çalışmışlardır. Buna en somut örnek, Avrupa Birliği Siber Suçlar Sözleşmesinde *"Veri Trafiği"* nden her hangi bir bilgisayar verisi" olarak söz ederken, GDPR' de kişisel verilerin işlenmesinde otomatik sistemlerden, dosyalama sistemlerinden ve bu sistemlerin parçası olan araçların kullanılmasından bahsedilmiştir[208]. İki metnin hazırlanmasında yaklaşık on yıllık bir süre olmasına karşın, verilerin sadece bilgisayar üzerinden işlenmeyeceği anlaşılmış ve bilişim sistemlerini kapsayıcı bir ifadeye yer verilmiştir.

95/46/EC Sayılı AB Veri Koruma Direktifinin niteliğinin tüzük olarak değiştirilerek ve merkeze kişisel verilerin alınarak GDPR'nin hazırlanmasının temelinde, bilişim sistemlerinin hızla gelişmesi ve bilişim sistemlerine yüklenen kişisel verilerin kontrol altına alınarak toplumsal düzenin dijital ortamda da sağlanmaya çalışıldığını görülmektedir.

3.2.3.1. 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Hakkında Genel Bilgiler

GDPR'nin uygulama alanı gelişen bilişim sistemleri ve verilerin işlendiği alanlar dikkate alınarak belirlenmiştir. Uygulama alanı, GDPR'nin 2. maddesinde düzenlenmiş olup bu maddeye göre GDPR'nin uygulama alanı;

> *"Tüzük, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesine ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesine uygulanır."* şeklinde belirlenmiştir.

Anılan maddenin son kısmı olan *" ... amaçlanan araçlarla işlenmesine uygulanır."* şeklinde düzenlenerek uygulama alanı kısıtlanmıştır. Maddeden de anlaşılacağı üzere, Tüzük kapsamındaki fiillerin, sayılan araçlarla işlenmesi durumda Tüzük uygulama alanı bulacaktır. Bu hüküm uyarınca, fiillerin otomatik araçlarla işlenmesi, otomatik araçlar haricinde bir dosya depolama sisteminin parçası ile işleme tabi tutulması, bir

[208] **T.C. Dış İşleri Bakanlığı Avrupa Birliği Başkanlı, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) çevirisi**, https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf, e.t.: 29.11.2021.

dosyalama sisteminin parçasını oluşturması amaçlanan araçlar ile işlenmesi durumunda uygulanacaktır.

Maddenin devamında ise; *"kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkin makamlar tarafından kişisel verilerin işlenmesinde uygulanmaz.* "denilmek suretiyle, istisnalara yer verilmiştir. Maddenin istisnaları incelendiğinde, suçların önlenmesi ve ceza yargılaması ile infaz süreçlerinin istisna olarak tutulduğu anlaşılmaktadır. Bu durumda, 2016/680 Sayılı Adli ve Kolluk Teşkilatınla Verilerin Korunmasına ilişkin Direktif uygulanacaktır[209]. GDPR içerisinde kolluk teşkilatının faaliyetlerinin nasıl olacağı noktasında bir düzenleme yer almamaktaydı. Bu açığı kapatmak için Avrupa Konseyi 2016/680 Sayılı Adli ve Kolluk Teşkilatınla Verilerin Korunmasına ilişkin Direktif' ni yürürlüğe koymuştur. Avrupa Birliği Genel Veri Koruma Tüzüğüne paralel olarak düzenlenen 2016/680 sayılı bu Direktif, kolluk küveti bağlamında kişisel verilerin korunması ile ilgili olarak ayrıntılı bir sistem kurmakla birlikte, kamu güvenliğini ilgilendiren veri işlemenin özelliklerini de dikkate almıştır[210].

GDPR niteliği itibariyle üye devletleri doğrudan kapsamaktadır. Tüzüğe taraf olmak isteyen üçüncü ülkeler ise veri koruma bakımından güvenilir ülke statüsünde ise taraf olabilmektedirler. Bu koşullar iç hukukumuzda yer alan 6698 Sayılı Kişisel Verilerin Korunması Kanununun temelini oluşturmaktadır. Türkiye, 6698 Sayılı Kanun ile verilerin korunması bakımından güvenilir bir ülke statüsünde yer almıştır.

95/46/EC Sayılı AB Veri Koruma Direktifi, veri korumasına ilişkin genel bir çerçeve çizmiş olmasına karşılık, GDPR, daha geniş kapsamlı bir uygulama alanı bulmuştur. Ancak, teknolojik gelişmelerin getirdiği değişimler ile kişisel verilerin rıza dışı kullanımı GDPR'nin kişisel verilere ilişkin ayrıntılı düzenlemelere yer vermesine neden olmuştur. Verilerin dijitalleşmesiyle ortaya çıkan yeni kavramlar ve teknik kısımların anlaşılması kolay olmamıştır. Bu durum, GDPR'nin uzun kabul sürecinin nedenini oluşturmaktadır.

GDPR'nin de 95/46/EC Sayılı AB Veri Koruma Direktifi ile aynı esaslar üzerine kurulduğu görülmektedir. Bu esaslar, kişilere ait işlenen verilerin korunmasına ve bu verilere ait trafiğin güvenli şekilde olmasına yöneliktir. Gelişen teknoloji ile birlikte

[209] Dülger, **Avrupa Birliği GDPR,** s. 94.
[210] Christos Giakoumopoulos/ Giovanni Buttarelli/ Michael O'Flaherty**, Handbook on European data protection law 2018 edition**, https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf, e.t.: 02/01/2022.

yaşanan somut olgulardan da yola çıkarak yapılan çalışma ile oluşturulan GDPR ile yaşanan gelişmeler dikkate alınarak daha birey merkezli bir düzenleme yapılmıştır. Yaşanan gelişmeler neticesinde GDPR'nin üç temel konu üzerinde durduğu görülmektedir. Bunlar; kişisel verilerin ve veri sahiplerinin daha etkin korunması, veri işleyenler ile veri kontrolörlerinin sorumluluklarının artırılması ve uygulanma alanı bakımından daha güçlü düzenlemeler yapılmasıdır[211].

GDPR verilerin işlenmesi ile ilgili olarak 5. Maddesinde, bazı temel unsurlara yer vermiştir. Bu unsurlar; kişisel verilerin şeffaf ve dürüstlük kuralına uygun olarak işlenmesi, kişisel verilerin sadece meşru amaçlar ile toplanması, kişisel verilerin gerektiği kadar işlenmesi, kişisel verilerin doğru şekilde işlenmesi, kişisel verilerin amacına uygun süreler ile tutulması, verilerin güvenli ve gizlilik içerisinde işlenmesi ve veri kontrolörünün belirlenen hususlar çerçevesinde sorumlu tutulmasıdır.

GDPR'nin, sadece kişisel verileri temel alması, insanların kişisel olmayan yani kamuya açık platformlarda paylaştıkları verileri dışarıda bırakması açısından kanımca, bir güvenlik açığı oluşmaktadır. GDPR'nin ceza hukukundan çok özel hukuk temelli düzenlendiği görülmektedir. Kişisel verilerden ziyade, dijital verileri kapsayan bir düzenlemenin gerekliliği 95/46/EC Sayılı AB Veri Koruma Direktifinden GDPR'ye geçiş de hissedilmiştir. Çünkü 95/46/EC Sayılı AB Veri Koruma Direktifi kişisel verilerin dijital alanda işlenmesi ile yetersiz kalmış ve GDPR' ye ihtiyaç duyulmuştur. Peki kişisel olmayan ancak dijital veri niteliği taşıyan diğer verilerin nasıl kullanılacağına dair ayrıntılı bir düzenleme mevcut değildir.

Kişilere ait veri dolaşımının bilişim teknolojileri ve internetin gelişimi ile kontrol edilemediği ve bunun sonucunda yapılan bahsi geçen düzenlemeler kişisel veriler ile sınırlı olduğu için hızlı bir şekilde yeni olaylar ve olgular karşısında yetersiz kalacağı aşikardır. Dijital verilere ilişkin geniş çapta ve ayrıntılı bir düzenleme olmaması, her on yılda bir yeni yasal düzenleme ihtiyacını ortaya çıkaracaktır.

3.2.4. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (CONVECTION 108+)

Teknoloji ile birlikte gelişen dijitalleşme 21. Yüz Yılın başlarında, bilişim sistemlerini içeren teknolojik aletlerin boyutlarının küçülmesi ve erişiminin kolay

[211] Akıncı, s. 19.

olması nedeniyle, dijital ortamlara veri aktarımı hızlanmış aynı zaman da veri trafiğinin hareketliği de takip edilemez derecede artmıştır.

TUİK'in verilerine göre Türkiye'de 2009 yılında bireysel internet kullanımı oranı %38.1, internete erişimi olan hane miktarı %30, internetten ürün sipariş oranı ise %4 iken, 2020 yılında bu oranlar; internetin bireysel kullanımı %79, internete erişimi olan haneler %90.7, internetten ürün siparişi oranı ise %36,4 seviyelerine gelmiştir[212].

Hanelerin internet kullanımı, hane içerisindeki bireylerin bilişim sistemlerine yüklenen dijital verilerin artışı anlamına gelmektedir. Bireysel internet kullanımının artması ise insanların teknolojiyi ve interneti hayatlarında ne kadar çok yer edindiğinin bir göstergesidir. Bilişim sistemine yüklenen dijital verilerin en önemli kanıtı ve aynı zaman da suça konu olan kısmı ise internet ortamında yapılan alışverişlerdir. Bu nedenle, bu oranların da nerede ise dokuz kat arttığı görülmektedir. İnternet alışverişi yapabilmek için dijital ortama yüklenen alışveriş bilgileri, kişisel bilgiler ile birlikte en çok çalınan dijital veriler arasında yer almaktadır.

Kullanılan internetin daha hızlı hale gelmesi adına bilişim sistemleri tarafından dijital ortamda bulunan kişisel veriler bilişim sistemleri tarafından kaydedilmeye başlanmıştır. Kaydedilen bu veriler çoğu zaman kişilerin rızası dışında otomatik olarak işlenmeye başlanmıştır. Kişisel verilerin otomatik olarak işleme tabi tutulmamasından neyin kastedildiği kanunlarda yer alamamaktadır. ConventionfortheProtection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), (Convection 108+)[213], ülkemizin taraf olduğu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinde ve KVKK'da *"otomatik işleme"* tanımının yer almaması büyük bir kanuni eksikliktir. Otomatik işleme tabi tutulan kişisel verilerin nasıl ve ne tür bir işlemle karşı karşıya kaldığını anlatmak adına ilk önce otomatik olarak verilerin işlenmesini izah edeceğiz.

Otomatik olarak veri işleme; dijital ortamda bulunan veriyi, bilişim sistemleri aracılığı ile bilişim sistemi içerisine yerleştirilen ve önceden çeşitli algoritmalar ile programlanmış yazılımlar tarafından kendiliğinden işlenmesi veya kullanılmasıdır. Daha basit tabir ile Otomatik Veri İşleme; Bilgisayar, telefon, saat vb. işlemci sahibi

---

[212]**Türkiye İstatistik Kurumu Haber Bülteni**, Hane Halkı Bilişim Teknolojileri Kullanım Araştırması, https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-Information-and-Communication-Technology-(ICT)-Usage-in-Households-and-by-Individuals-2020-33679, Yayın Tarihi: 25 Ağustos 2020, Sayı: 22679, e.t.: 18.11.2021.

[213]Counsil of Europa, **ConventionfortheProtection of IndividualswithregardtoAutomaticProcessing of Personal Data (ETS No. 108)**, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019AP0142&rid=1, e.t.:25.12.2021.

cihazlar tarafından yerine getirilen, yazılım veya donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyeti olarak ifade edilebilir[214].

Verilerin otomatik işlenmesine ilişkin yasal ihtiyaç devletlerin, vatandaşlarına ait bilgilerin kayıtlarının tutulması, aktarılması, analizi, yok edilmesi gibi işlemler veri sahibi olan kişilerin aleyhine kullanılması tehlikesini gözetmesi ve bu nedenle yasal düzenleme yapma ihtiyacı hissetmesi ile başlamıştır. Verilerin otomatik işleme tabi tutulmasının yasal zemine tabi olmasıyla hedeflenen ise yani korunması istenen husus insanların temel anayasal hakları olmuştur.

Avrupa Konseyi (AK) kişisel verilerin otomatik işleme tabi tutulmasını kontrol altına almak ve kişisel verileri otomatik işleme sırasında hak ihlalleri olmaması için Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesini 28 Ocak 1981 Tarihinde imzaya açmış ve 1 Ekim 1985 tarihinde ilgili sözleşme yürürlüğe girmiştir. Avrupa Konseyi dışındaki üye ülkeler için de imzaya atılan bu sözleşme ülkemiz tarafından 28 Ocak 1981 tarihinde imzalanmıştır. İmzalanan sözleşmenin amacı her üye ülkede yaşan gerçek kişilerin din, dil, ırk, mezhep, düşünce ve inancına bakmaksızın kişisel niteliğe sahip verilerinin otomatik işleme tabi tutulması sırasında özel yaşama dair haklarını güvence altına alınmasıdır. Kırk yedi ülke sözleşmeye taraf olmuş, ülkemiz dışındaki kırk altı ülke ise onaylayıp yürürlüğe koymuştur. Türkiye onaylayıp yürürlüğe koymayan tek ülkedir[215].

Bilişim teknolojilerindeki gelişmeler ile kişisel verilerin dijitalleşmesindeki artış ve bu verilerin gelişmiş programlar ile saniyeler içerisinde sayılamayacak derecede otomatik işleme tabi tutulması karşısında Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi yetersiz kalmaya başlamıştır. Bu nedenle 18 Mayıs 2018 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilen Convetion +108 olarak bilinen protokol ile güncellenmiştir.

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin temelinde de Dijital Verilerin yer aldığını ve sözleşmeye konu dijital verilerin de veri sahibinin rızası dışında tabi tutulduğu işlemler sırasında gerçekleşecek hak ihlallerinin önlenmesi amaçlanmıştır. Aslında korunmak istenilen amacın bir nevi

[214]Verbis Online, **Otomatik Veri İşleme ve Otomatik Olmayan Veri İşleme**, https://verbis.online/otomatik-veri-isleme-ve-otomatik-olmayan-veri-isleme/, e.t.:26.12.2021.
[215] Dülger, **İnternet İletişim Mevzuatı**, s. 505-506.

dijital ortamdaki kişisel verilerin hırsızlanması olduğu da söylenebilir. Çünkü kişilere ait verilerin kişinin rızası dışında kullanımı hırsızlık suçuna benzetilebilecektir.

Otomatik veri işlemeyi somutlaştırmak gerekirse; Google arama motorunda satın almak için aradığınız bir ürünü, alışveriş sitesi dışında da gezerken Google tarayıcısı karşınıza çıkardığında, aslında Google sizin alışveriş ihtiyacınızı algoritmaları sayesinde analiz edip işleyerek aradığınız ürün için reklam veren müşterilerinin ürünlerini sizin karşınıza çıkarmaktadır. Burada ürüne duyduğunuz ihtiyacınız kişisel veriniz, Google'ın armanızı kaydederek analiz etmesi otomatik şekilde işlenen veri kaydınız, Google arama motorunun reklam anlaşması yaptığı ve sizin ürünlerinizi satan firmanın reklamını karşınıza çıkarması ise bir dönüttür. Google burada kişisel verinizi kullanarak reklam anlaşması yapmakta ve kazanç sağlamaktadır. Sosyal paylaşım siteleri de reklam için en çok kişisel veri toplayan sanal ağlardır. Sosyal paylaşım sitelerinin kişisel verilerin üçüncü kişiler ile paylaşımıyla ilgili yapılan bir analizde Instagram sosyal paylaşım sitesinin %79 oranla üçüncü kişiler ile reklam için veri paylaşımı yaptığı bu oranı Facebook %57, Linked %50, Youtube %43 oranla takip ettiği görülmüştür[216]. Dünyada toplamda 4,55 milyar sosyal medya kullanıcısı olduğu düşünüldüğünde ne kadar büyük bir veri trafiği olduğunu ve dijital verilerin ne kadar savunmasız kaldığı görülmektedir[217].

[216]HaberTürk, **Verilerimizi reklam için en çok paylaşan sosyal ağ hangisi?** https://www.haberturk.com/iste-kisisel-bilgilerimizi-en-cok-satan-sosyal-ag-haberler-3016427-teknoloji, e.t.:26.12.2021.

[217]**WebTekno, Dünyada Toplam Kaç Milyar İnternet ve Sosyal Medya Kullanıcısı Olduğu Açıklandı**, https://www.webtekno.com/kac-milyar-internet-sosyal-medya-kullanicisi-oldugu-aciklandi-h116978.html, e.t.: 25.12.2021.

DÖRDÜNCÜ BÖLÜM

DİJİTAL VERİ HIRSIZLIĞINA KARŞI ALINMASI GEREKEN VE ALINABİLECEK ÖNLEMLER

Dijital verilerle ilgili uluslararası ve ulusal düzenlemelerdeki eksikliğin zaman içerisinde mümkün olduğunca giderildiği, bilişim suçları alanında dijital veri hırsızlığı temelli geniş kapsamlı ve ayrıntılı bir yasal düzenleme yapıldığı kabul edilebilir. Ancak, bu düzenlemelerin dijital verilerin çalınması veya kişilerin rızaları dışında kullanımını engellemek için yeterli midir? Bu soruya kanımca hayır cevabı vermek gerekir. Çünkü; dijital veriler hayatın her alanına girmiş ve bu nedenle de bilişim suçları çok geniş alanlara yayılmış, faillerin sürekli gelişme gösterdiği yeni yöntemler ve stratejiler geliştirmelerine imkan sağlamıştır.

Dijital verileri anlamadan, dijital verilerin kişisel verilerin üzerinde bir alan olduğunu kabul etmeden, sanal varlıklarında her ne kadar fiziki varlığı olmasa da insan yaşamasında maddi değeri olabileceğini kabul etmeden, dijital verilere karşı gerçekleştirilen suçlarda ortaya çıkan kaybın, boyutlarını ön görmeden dijital verilere karşı işlenen suçlar ile mücadele etmek imkansız olacaktır. Bu nedenle, öncelikle dijital verilerin önemi, insan hayatındaki varlığı kabul edilmelidir.

Dijital veri hırsızlığı ile mücadele de en temel sorun kavram ve tanım karmaşasıdır. Bilişim suçlarının 1960'lı yıllarından itibaren Amerika'da çıkmaya başlaması ilk olarak Amerika doktrinlerinde yaygın olarak kullanılmaya başlayan "computer –crime" (bilgisayar suçu) kavramı ile başlamıştır. Bilişim suçlarının çıkış noktasında kullanılan bilgisayar suçu kavramı, dijital verilerin en çok işlendiği araç olan bilgisayar ile kullanılması ile daha da pekişmiş ve "bilgisayar suçu" kavramının yaygınlaşmasına neden olmuştur. Zaman içerisinde bilgisayar dışında dijital veri işleyen ve bilişim sistemlerine sahip teknolojik aletler çıkınca "bilgisayar suçu" kavramı yetersiz kalmaya başlamıştır. Yaşanan bu kavram yetersizliği sorunu AKSSS ve BM metinlerinde "siber suçlar" kavramı kullanılmaya başlamasına neden olmuştur. Ancak siber suçların bilişim sistemleri arasındaki suçları tanımlaması kullanılan kavramın sınırlanmasına neden olmuştur. Daha sonra çeşitlenen bu kavramlar "internet suçları, bilişim suçları, siber zorbalık, bilgisayarla ilgili suçlar" ortaya çıkmıştır. Ancak

en genel tanımını "bilişim suçları" kavramı oluşturmaktadır. Çünkü teknoloji ile ilgili tüm suçlarda bilişim sistemleri aracı olarak kullanılmakta ve hedef alınmaktadır[218].

Bilişim suçlarına ilişkin genel bir tanım yapmak, bilişim suçları ile mücadeleyi ortak ve genel bir tanım olması nedeni ile suç sınıflandırmasında ve uluslararası yardımlaşmanın sağlanmasını kolaylaştırmıştır.

Bilişim suçlarının araç olduğu veya hedef alındığı suçlara ilişkin eylemlerin temeli olan dijital verilerin failler tarafından kullanılmasına ilişkin net bir tanım olmaması da aynı anlam karmaşasına yol açmaktadır.

4.1. Dijital Veri Hırsızlığı İle Mücadele

Sosyal bir varlık olan insanın diğer insanlar ile etkileşim de bulunması insan doğasının gereğidir. Suçların temelinde yatan esas neden, insanlar arasındaki etkileşimdir. İnsanlar birbirleriyle etkileşim içerisinde olduğu için sorunlar ve uyuşmazlıklar ortaya çıkmaktadır. Hukuk sistemlerinin temel amacı ise insanların etkileşiminden ortaya çıkan sorunları, düzenlendikleri belli kurallar ile sistematik şekilde çözmek ve sosyal hayatın en sorunsuz şekilde işlemesini sağlamaktır.

İnsanlar, çeşitli bilişim sistemleri ile evlerinden çıkmadan, diğer insanlar ile etkileşimde bulunmaya başlamıştır. Dijital ortamın sağladığı anonimlik ise insanların etkileşimleri sırasında etkileşim de bulunduğu insana karşı suç barından davranışlar sergilemesini kolaylaştırmıştır. Anonimliğin getirdiği kimlik belirsizliği, farklı kimlikle hareket etme, kısıtlı erişilebilirlik, ulaşılmanın zorluğu, özellikle içinde suç işleme isteği barındıran insanlara cesaret vermiş ve suç işlemeyi kolaylaştırmıştır.

Bireylere ait dijital verilerin rıza dışı ele geçirilip kullanılması, dijital ortamda işlenen suçların en temel noktasıdır. Çünkü, bir kişi dijital ortamda var olmak için bilişim sistemleri aracılığıyla dijital verileri kullanmak zorundadır. Örnek vermek gerekirse; telefon dolandırıcılığında, failin mağdurdan bilgi almasında veya daha önce ele geçirdiği bilgiyi mağdurla paylaşarak mağdurun iradesini kırma çalışmasında, mağdurun rızası dışında kullanılan dijital verileri vardır. Dolayısıyla, en basit durumda mağdurun telefon numarası dahi bir dijital veridir. Mağdurun telefon numarasının rızası ve bilgisi dışında ele geçirilmesi, dijital bir verinin çalınması anlamına gelmektedir.

Başka bir örnek vermek gerekirse; en çok karşılaşılan sosyal medya suçlarından biri de failin zararlı yazılımlarla mağdurun verilerini ele geçirerek veya mağdurun kendi

[218] Erdoğan, s.46.

rızasıyla sosyal platformlara yüklediği ancak rızası dışında bu verilerin kullanılması suretiyle oluşturulan sahte hesaplar ile mağdur adına hareket edilmesi veya mağdurun ele geçirilen dijital verileri ile mağdur gibi hareket edilerek verilerin hukuka aykırı şekilde kullanılması suretiyle ortaya çıkmaktadır. Böylece fail, mağdur üzerinden kendisi anonim olacak şekilde suç içeren eylemler gerçekleştirebilmektedir.

Örneklerden de anlaşılacağı üzere, bir birine çok benzeyen ancak teknik ve eylemsel bakımından, bir birinden tamamen farklı suç tipleri, *"Bilişim Alanında Suçlar*" başlıklı Bölümde yer alan TCK'nın 243.ve devamı maddelerindeki, düzenlemeler kapsamında değerlendirilerek yaptırımlar uygulanmaktadır. Ancak, verilen örneklerde ise doğrudan bilişim sistemleri ile olmayıp, sosyal medya hesapları üzerinden suçlar işlenmektedir. Dolayısıyla, fail mağdurun bilişim sistemine girmeden de söz konusu suçları işleyebilmektedir. Kanun koyucunun konusu bilişim sistemi olan bir suç tipinde bilişim sistemi ile ilgisi olmayan ve tamamen sanal dünyada var olan sosyal medya platformunu, bilişim sistemi olarak kabul etmesi, yasal düzenleme açısından gerçekçi bir yaklaşım değildir.

TCK'nın 243. maddesinin gerekçesinde bilişim sistemi; *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir."* şeklinde manyetik bir sistem olarak tanımlanmıştır. Buna karşılık, sosyal medya ise bilgi paylaşımı yapılan bir medya sistemidir[219]. İki kavramda bir birinden tamamen farklıdır. Yargıtay içtihatlarında ise sosyal hesaplarını, bilişim sistemi olarak yorumlamakta ve kararlarını bu doğrultuda vermektedir.

Örnek vermek gerekirse; Yargıtay 8. Ceza Dairesi, mağdurun sanal oyun hesabına link üzerinden rıza dışı girilerek hesaplarının çalındığına ilişkin bir davanın yargılamasında, oyun karakterinin failin hesabına aktarılmasını TCK'nın243. maddesi kapsamında değerlendirmiştir[220]. Yargıtay 8. Ceza Dairesi söz konusu kararında; failin mağdurun bilgisayar sistemine zararlı yazılımlar ile erişerek şifresinin mağdurun rızası dışında alındığı yorumunu yapmış olsaydı, eyleminin TCK'nın 243.maddesi kapsamında değerlendirmesi uygun olabilecekti. Ancak failin, direkt olarak mağdurun zararlı yazılımlar sayesinde, oyun hesabına girmiş olması, internet ortamında olan ve bilişim sisteminin sadece erişmek için aracı kullanıldığı bir platformda gerçekleşmesi

[219]Vikipedi, **Sosyal Medya**, https://tr.wikipedia.org/wiki/Sosyal_medya, e.t.: 27.11.2021.
[220] Yargıtay 8. Ceza Dairesi, 25.05.2017 Tarihli ve 2017/897 E., 2017/6019 Karar Sayılı İlamı, https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/, e.t: 02.12.2021.

nedeniyle, eyleminin, bilişim sistemine karşı gerçekleştirilen bir suç olarak yorumlanması doğru değildir. Çünkü, karar içeriğinden de anlaşıldığı üzere, oyun karakteri failin hesabına aktarılmış olup, dijital verileri çalınmıştır. Maddi değeri çok yüksek olabilen bir oyun karakterinin, mağdurun hesabından failin hesabına aktarılması kanımca hırsızlık suçunu oluştururken, Yargıtay tarafından sadece bilişim sistemlerine karşı gerçekleştirilen bir suç gibi yorumlanması, dijital veri hırsızlığını ve bilişim sistemlerini konu alan bir düzenleme olmamasından kaynaklanmaktadır.

Söz konusu olayda, mağdurun sosyal ağ içerisinde maddi değere sahip ve maliki olduğu bir dijital varlığın yani verinin, failin hesabına yasa dışı yolla aktarılmasının, TCK'nın 141. maddesi ve devamında düzenlenen hırsızlık suçunu oluşturacağı kanısındayım.

Ceza hukukunun temel ilkelerinden olan ve TCK'nın 2/3. maddesinde, düzenlenen *"Suçta ve Cezada Kanunilik İlkesi"*, açıkça kıyas ve yorum yasağı getirmiştir. Verilen örneklere ilişkin suç tiplerinde, genel hüküm niteliğinde düzenlemeler yapıldığından, bu hükümlerin yorumlanmasıyla hüküm kurulması, teknik terimlere yabancılık çekilen bir hukuk alanında anlam karmaşasına ve eylemlerin niteliğinin tespitinde ve suçun konusunda yanılmalara ve dolayısıyla, tesis edilen hükümde duraksamalara neden olacaktır.

4.2. Dijital Verilerin Hırsızlığı İle İlgili Ayırıntılı Ve Tek Bir Yasal Düzenleme İhtiyacı

Ülkemizde bilişim alanında yer alan düzenlemeler, dağınık bir durumdadır. Özellikle, bilişim hukukunun hem kamu hukuku hem de özel hukuku kapsayan bir alan olması, bilişim hukukunu ayrı bir hukuk dalı olmaya doğru yöneltmektedir. Örneğin; internet üzerinden yapılan e-imzalı bir sözleşmede, e-imzanın sahte olarak oluşturulması, bir kamu hukuku sorunu iken, atılan imzadan dolayı doğacak sorumluluk bir özel hukuk uyuşmazlığı olarak ortaya çıkmaktadır. Elektronik İmza Kanununun (EİK) 13. maddesinde, imza atanın hukuki sorumluluğuna ilişkin *"Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir."* şeklinde düzenleme yapılırken cezai boyutu için *"Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır. "şeklinde düzenleme yapmıştır.*

İlk başta aynı kanun içerisinde yapılan düzenleme doğruymuş gibi görülse de sahte elektronik imza oluştururken kullanılan veriler, KVKK' da tanımlanan kişisel veri dışında kalan ve mağduru yanıltıcı özelliğe sahip bir yapıya sahiptir. Dolayısıyla, TCK'da düzenlenen dolandırıcılık suçunun hileli davranış unsurları da mevcuttur. Sonuçta, elektronik imza taklit edilerek mağdura karşı gerçekleştirilen bir hileli davranış ve nedensellik bağı içinde failin kendisine veya haksız kazanç sağlamak istediği üçüncü kişinin lehine bir davranış vardır. Sahte olarak düzenlenen ve kullanılan e-imza ile özel hukuk hükümleri, EİK uyarınca alınmış bir e-imza ise KVKK ve TCK'da yer alan hükümlerin uygulanması söz konusu olacaktır. Bu farklı hükümler, uygulanacak yasal düzenleme ve izlenecek yol bakımından hem uygulayıcıları hem de tarafların delillerin toplanması ve eylemlere ilişkin hukuki niteleme yapılması noktasında, zor duruma düşürmekte ve yapılan yargılamada da hata oranını arttırmaktadır.

İnternet, hemen hemen toplumun tamamına yayılmış olan ve modern insanın ise iş, eğitim ve sosyal yaşamanın tam ortasında yer alan bir teknolojidir. Sadece insanın değil devletlerin de siyasi, politik, askeri vb. düzenine doğrudan etki eden bir olgu halini almıştır. Her toplumun kendine özgü bir sosyal düzeni ve gelişmişliği vardır. Sosyal düzeni sağlayan hukuk sistemleridir. Teknoloji ve gelişen bilişim sistemleri, çağımız sosyal düzenin ayrılmaz bir parçası konumundadır. Ancak, bu konu ile ilgili doğrudan yasal düzenlemeler yapılması yerine, ülke olarak hem teknolojiyi ve bilişim sistemlerini hem de teknoloji ve bilişim ile ilgili hukuk sistemlerini göz önüne alarak iktibas yoluyla düzenleme yapılmaktadır. Yabancı toplumların kendi ihtiyaçlarına göre şekillenen bilişim teknolojilerini ve hukukunu, toplumun ve hukuk düzeninin ihtiyaçlarına uygun olarak geliştirmeyip dışarıdan ithal ettiğimiz zaman, bilişim hukuku sistemi içerisindeki hatalar kaçınılmaz olmaktadır[221].

Gelişen teknoloji ve bilişim sistemleriyle ilgili yapılan düzenlemelerin yeterince günün koşullarına ve geleceği de kapsayacak şekilde ayrıntılı yapılmaması, genel yasa maddeleri ile çeşitli kanunlarda dağınık şekilde ek maddeler halinde düzenleme getirilmesi, bilişim sistemleri ve teknoloji ile ilgili alanda yapılması gereken hukuki çalışmaları kısır bir döngüye çevirmiştir.

Özellikle ülkemizin de örnek aldığı ve uyumlaştırdığı AB tarafından temel esasları ve ilkeleri belirlenen düzenlemelerin, sadece insanlara ait özel veriler üzerinden

[221] Dülger, **Bilişim Suçları**, s. 580.

yapılması, internet ve bilişim sistemleri açısından çok fazla uygulama sorunlarının çıkmasına sebep olmuştur. Dolayısıyla bu durum, bilişim hukukunda çok büyük hukuksal açıklar meydana getirmektedir.

İç hukukumuzda bilişim suçlarına ilişkin düzenlemeler çok dağılmıştır. Yine Amerika'da Bilgisayar Sahtekarlığı ve Bilgisayarın Kötüye Kullanılması Kanunu, Çocuk Pornografisinin Önlenmesi Kanunu, İletişim Ahlakı kanunu, Elektronik Haberleşmenin Gizliliği Kanunu, Kimlik Hırsızlığının Önlenmesi Kanunu gibi genel kanunların yanı sıra 47 eyalette ayrıca mevzuatlar vardır[222].

Bu kadar fazla kanun ihtiyacı bilişim suçlarının bir temele dayandırılamaması olmasından kaynaklanmaktadır. Halbuki bilişim suçlarını temelinde yer alan bilişim sistemlerinin var olması için olmazsa olmaz olan dijital verilerdir. Daha önce de izah ettiğimiz üzere bilişim suçları, bilişim sistemi içerisindeki dijital verilerin, veya bilişim sistemine dışarıdan bir başka bilişim sistemi tarafından oluşturulan zararlı dijital veriler yollanması ile gerçekleşmektedir. Her iki kavramda da temel olarak dijital verilerin hırsızlanması ile eylem gerçekleşmektedir.

Bilişim sistemlerini ve dijital verileri konu alan ayrıntılı bir yasal düzenlemeyi tek bir yasal düzenleme halinde toplamak sürekli ve hızlı gelişen bilişim sistemleri ve veri trafiğine ilişkin suçlarla mücadelenin daha etkili olmasını sağlayacaktır.

İnternette ve bilişim sisteminde yer alan her türlü olgu, bir veri olarak yer almaktadır. Bu nedenle, internet ortamında ve bilişim sistemleri aracılığıyla işlenen her türlü suçun konusunu dijital veriler oluşturmaktadır. Dijital verilerin sahibinin rızası dışında gelişen suç tiplerini, dijital verilere ilişkin gerçekleştirilmiş bir hırsızlık suçu olarak ifade etmek, anlaşılması bakımından kolay bir tanımlama olacak, ancak yine de yetersiz kalacaktır. Zira, internetin ve bilişim sistemlerinin temelinde, dijital verilerin bulunması ve bilişim sistemleri ile ilgili suçların işlenmesinde de verilerin çalınması veya dijital veri sahibinin rızası dışında kullanılması olduğundan, dijital verileri genel anlamda düzenleyen bir yasa ihtiyacı ortaya çıkmaktadır.

4.3. Bilişim Suçlarıyla Mücadelede Alınması Gereken Önlemler

Zararlı bir olgu ile mücadele edebilmek için öncelikle zararlı olgunun niteliklerinin farkında olmak gerekmektedir. Bu nedenle, öncelikle bilişim suçlarıyla mücadele etmenin zorluğunun farkındalığına varmak gerekmektedir.

[222] Erdoğan, s.56.

Bilişim suçları ile mücadelenin klasik suçlarla mücadele etmekten zor olmasını birkaç başlık altında sıralayabilmek mümkündür. Bunlar bilişim teknolojilerinin sürekli gelişen bir alan olması; her gün yeni suç metotları ve yöntemlerinin bulunması; bilişim suçlarının soyut olan dijital veriler sayesinde gerçekleştirilmesi; faillerin takibinin ve belirlenmesinin zor olması; bilişim sistemi kullanıcılarının bilişim sistemlerini basit ve bilinçsiz şekilde kullanması şeklindeki nedenler, bilişim suçları ile mücadeleyi zorlaştırmaktadır.

Bilişim sistemlerinin kendi özelliğinden kaynaklanan zorlukların yanı sıra, kolluk kuvvetlerinin ve yasa uygulayıcılarının bilişim sistemlerinin teknik sistemlerini anlamakta zorlanmaları ve bilişim sistemlerini kullanmadaki yeterli donanıma sahip olunmamaları, soruşturma ve kovuşturmanın yapılmasını zorlaştırmaktadır[223].

Siber suçlarla mücadelenin en etkili yöntemi siber saldırıya maruz kalmamaktadır. Siber saldırıya maruz kalmamak veya siber saldırıda veri ve sistem kayıpları olmaması için bir takım önlemler alınabilir. Alınan güvenlik önlemlerinin amacı, sadece dijital veri güvenliği olmamalıdır. Alınan güvenlik önlemindeki amaç, bilişim sisteminin sorunsuz ve sürekli çalışması, bilişim sistemine sızmaları ve yetkisiz erişimlerin engellenmesi, sistemde bulunan verilerin yok olmasının veya çalınmasının önlenmesi olmalıdır.

4.3.1. Bilişim Sistemlerinin Güvenliğini Sağlamaya Yönelik Yazılımlar

Bilişim sistemlerine yetkisiz erişimin engellenmesi ve virüs olarak adlandırılan zararlı yazılımların sisteme sızmasını engellemek için en çok kullanılan yöntem, *"firewall"* adı verilen güvenlik duvarıdır[224]. Firewall yazılımı ile birlikte sisteme yüklenen anti virüs adı verilen zararlı yazılımları ve yetkisiz erişimleri engelleyici faydalı yazılımlar, bilişim sistemine ve bilişim sistemi içerisinde yer alan dijital verilerin korunmasında önemli rol oynamaktadır. Faydalı olan anti virüs yazılımları bilişim sistemine dışarıdan gelen verileri süzgeçten geçirerek içerisinde saklanan zararlı yazılımları tespit ederek bilişim sistemine girmesini engeller veya bilişim sistemi içerisine bir şekilde girmiş olan zararlı yazılımları tespit ederek bilişim sistemi sahibini uyarır. Kendisine verilen komut doğrultusunda tespit ettiği zararlı yazılımı yok edebilir,

[223] Dülger, **Bilişim Suçları**, s. 626.
[224]Vikipedi, **Güvenlik Duvarı**, https://tr.wikipedia.org/wiki/G%C3%BCvenlik_duvar%C4%B1, e.t.:26.12.2021.

karantinaya alabilir veya zararlı yazılımın geldiği verinin bilişim sistemine girmesini engelleyebilir[225].

Yararlı olan Firewall ve diğer anti virüs yazılımları kullanılırken dikkat edilmesi gereken husus, yararlı yazılımların güncel tutulmasıdır. Bilişim sistemine karşı gerçekleştirilen saldırılar için kullanılan zararlı yazılımlar sürekli olarak kendilerini yeniledikleri veya failleri tarafından yeniden yazıldıkları için mevcut olan yararlı yazılım sisteme giren yeni zararlı yazılımı fark etmeyebilmektedir. Bu nedenle, yararlı yazılım oluşturan şirketler sürekli olarak kendilerini güncelleyerek ortaya yeni çıkan zararlı yazılımlarla mücadele yöntemleri bulmaya çalışmaktadırlar.

4.3.2. Bilişim Sistemlerinin Siber Güvenliği

Özellikle resmi veya özel kurum ve kuruluşların bilişim sistemlerinin çalıştırılmasını veya yönetilmesini, kurum veya kuruluş içerisindeki görev dağılımında görevlendirilen personel yapmaktadır. Bilişim sistemlerinin güvenliği,*"CM/CybersecurityManagement"* olarak bilinmekte ve Türkçe 'ye siber güvenlik olarak çevrilmektedir. Siber güvenlik, günümüzde tek başına bir güvenlik disiplini oluşturmaktadır. Bir sistemin siber güvenliğini sağlamak için yeterli ve özgün güvenlik protokolleri oluşturularak bu protokollerin yeterli ve yetkin personel tarafından uygulanması gerekmektedir.

Bilişim sisteminin güvenliği için gerekli tüm adımlar atılmış olsa da tamamen güvenli bir bilişim sisteminin kurulmasından söz etmek mümkün değildir. Çünkü, bilişim sistemleri her an yeni ve güncel siber saldırı yöntem ve metotlarıyla karşı kalabilmektedir. Ancak, bilişim alanında güvenlik tedbirleri alındığı sırada, kesin olmayıp en iyi ya da makul güvenlik sağlamaya çalışıldığı göz önüne alınmalıdır. Bilişim suçlarını engellemek ve siber saldırılarla mücadele edebilmek için bireysel ve kurumsal olan bilişim sistemi sahiplerini, bilişim sistemlerini kullanma konusunda ve kendi bilişim sistemlerinde sağlayabilecekleri güvenlik engellerini oluşturmaları bakımından, yeteri kadar bilinçlendirmek gerekmektedir.

4.3.3. Bilişlim Sisteminin Açıklarının Yasal Şekilde Tespit Edilmesi

Bünyesinde çok fazla dijital veri barındıran kamu ve özel tüzel kişilikleri, aldıkları siber güvenlik önlemlerini test etmek amacıyla alanında uzman kişilerden destek

[225]Yusuf Uzunay, **Dijital Saldırılar, Emniyet Güçleri Açısından Önemi ve Korunma Yolları**, PBD, Ankara, C.5, S. 2, 2003, s. 138., https://app.trdizin.gov.tr/makale/TXpNd05qWT0=/dijital-saldirilar-emniyet-gucleri-acisindan-onemi-ve-korunma-yollari, e.t.:25/01/2022.

almaktadırlar. Son zamanlarda, bir iş dalı olarak ortaya çıkan bilişim güvenliği uzmanı kişiler, siber güvenliği test edilmesi istenilen bilişim sistemine yapılabilecek gerçek bir saldırıyı taklit ederek, gerçekleştirilebilecek bir siber saldırıda faillerin, bilişim sisteminin hangi noktalarına ulaşabileceğini ve verebilecekleri zararları tespit etmeye çalışmaktadırlar[226].

Yapılan tespitler ile bilişim sisteminin güvelik duvarındaki ve diğer teknik alanlarındaki zayıf noktalardan elde edilen veriler incelenerek, tespit edilen zayıf noktalara karşı ne şekilde önlemler alınabileceği hakkında çözümler üretilmekte ve uygulanmaktadır. Bundan sonra, bilişim sisteminde tespit edilen güvenlik zaafları kapatılarak sisteme tekrar kontrollü bir siber saldırı uygulanmakta ve bilişim sisteminin alınan yeni önlemlerden sonra, siber saldırıyı fark edip engelleyip engellemeyeceği tespit edilmektedir. Amaç, bilişim sistemine yapılan gerçek bir saldırıyı bilişim sistemine zarar vermeden engelleyip durdurmaktır[227].

Bilişim sistemine yapılan kontrollü sahte saldırı çok etkili bir yöntem olmasına rağmen, içinde büyük riskler barındırmaktadır. Bu riskler, kontrollü saldırıyı gerçekleştiren bilişim uzmanları yönünden, TCK'nın 243 ve 244. maddelerinde düzenlenen suçlara ilişkin eylemleri gerçekleştiriyor olmaları ve bilişim sistemi sahibinin üçüncü kişiler tarafından bilinmesi istenilmeyen dijital verileri ifşa edilmesi ve teste tabi tutulan verilere zarar verilmesi riskleridir.

Bilişim uzmanları tarafından gerçekleştirecekleri kontrollü saldırı ile TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme suçu oluşmayacaktır. Çünkü, madde içerisinde yapılan düzenlemede suça konu faili tanımlarken *" bilişim sistemine hukuka aykırı olarak giren veya orada kalan "* kişi olarak tanılamaktadır. Bilişim sistemine işlem yapmak için rızayla girildiğinden, bilişim uzmanları yönünden hukuka uygunluk sebebi vardır. Ancak, bilişim uzmanı sisteme girdikten sonra, bilişim sahibinin rızası dışında bilişim sistemi içerisinde kalmaya devam ederse suç işleme kastı oluşacağından cezasızlık sebebi ortadan kalkacaktır.

Bilişim uzmanları yönünden risk oluşturan diğer bir düzenleme TCK'nın 244. maddesinde yer verilen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçudur. Bilişim uzmanı, bilişim sistemine kontrollü saldırı düzenlerken verilerin zarar görme riskine karşı bilişim sistemi sahibi rıza gösterse de 244. maddede, 243. maddede olduğu gibi hukuka uygunluk sebebi yoktur. 244. maddede yer alan bu eksiklik

[226] Dülger, **Bilişim Suçları**, s. 629.
[227] Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, s. 79.

uygulamada sorun yaratabilecek niteliktedir. Çünkü, 244. maddedeki suç soruşturulması ve kovuşturulması şikayete bağlı olmayan ve re'sen soruşturulan gereken bir suç tipidir. Her ne kadar bilişim sistemi sahibinin rıza açıklaması hukuka uygunluk sebebi olarak gösterilse de ceza hukukundaki yorum yasağı nedeniyle sağlıklı bir uygulama yapılamamaktadır[228]. Bu durum, ülkemizdeki bilişim hukuku alanında dijital veri hırsızlığı temelli bir kanuni düzenlemenin eksik olduğu düşünce ve görüşümü desteklemektedir.

Bilişim uzmanları söz konusu riskleri en aza indirmek için bilişim sistemi sahibi ile saldırının ne şekilde olacağını, hangi dijital verileri hedef alacağını, saldırının riskinin neler olduğunu, ne kadar süreceğini, oluşan hasarın ne kadar sürede düzeltileceğine ilişkin bilgilendirici bir sözleşme yapmak zorundadırlar. yapılan bu sözleşme ile bilişim sahibinin tam ve uygun rızası alınmaktadır.

4.3.4. Devletlerin Bilişim Sistemlerinin Güvenliği İle İlişkisi

Bilişim suçlarının gerçekleşmesini önlemek amacıyla bireysel olarak alınabilecek önlemlerin yanı sıra, bilişim suçlarıyla mücadelede devletlere de hem kendi içlerinde hem de uluslararası işbirliği noktasında, önemli görevler düşmektedir. Özellikle, devletlerin bilişim suçlarıyla mücadeleyi gerçekleştiren ve bilişim suçlarını kovuşturan birimleri oluşturması ve eğitmesi, sosyal ağların ve internet ortamının denetlemesinin gerekliliğiile bilişim suçlarıylane şekilde mücadele edileceği konusunda, gerekli ve yeterli tedbirleri alması gerekmektedir. Bilişim suçlarına ilişkin hukuki düzenlemelerin tekel olması, bir başka önemli konuyu oluşturmaktadır.

4.3.4.1. Bilişim Suçları İle Mücadelede Devletlerin Uluslararası İşbirliğinin Önemi

Dijital verilerin dolaşımında fiziki bir sınır ve kontrol mekanizmasının olmaması, dijital verilerin saniyeler içerisinde dünyanın her köşesine iletilebilir olması, bilişim suçlarıyla mücadelenin en temel sorunları arasındadır. Ayrıca, faillerin dünyanın her hangi bir noktasından, dünyanın başka bir noktasında istediği şekilde suç teşkil eden eylemleri gerçekleştirebiliyor olması, ceza muhakemesinin uygulanmasında, gerçekleşen suçların tanımlanması sorununu yaratmaktadır. Bilişim sitemleri üzerinden gerçekleştirilen hukuka aykırı eylemlerin nereden ve kim tarafından gerçekleştiğinin

[228] Karagülmez, **Bilişim Suçları**, s. 92,93.

tespitinin çok zor veya mümkün olmaması da bilişim suçlarıyla mücadelede ayrı bir sorundur[229].

Bilişim suçlarıyla mücadelede en kapsamlı düzenleme, *"Avrupa Siber Suç Sözleşmesi"*dir. Sözleşme ile ceza muhakemesine ilişkin net ve somut hükümlerin taraf devletlere yüklediği sorumluluklar, suçlara ilişkin delillerin toplanması, yeni yöntemlerin fark edilerek önlemler alınması, faillerin takibi ve yakalanmasında önemli katkı sağlamıştır.

4.3.4.2. Devletlerin Bilişim Suçları İle Mücadele Eden Birimlerini Eğitmesi

Bilişim hukukunu anlamak ve yorumlayabilmek için hukuk bilgisinin yanında teknik bilgi de gerekmektedir. Teknik bilgi; delillerin toplanması, bilişim suçlarına konu eylemlerin yorumlanması ve etkilerini anlamak bakımından önemlidir. Bu nedenle, devletlerin bilişim suçlarıyla mücadele eden birimlerine gerekli eğitimleri vermesi ve bilişim suçlarına ilişkin uzmanlık alanları oluşturması gerekmektedir.

Uygulamada eğitilmesi gereken kolluk ve adli birimlerde görevli personeldir. Bilişim suçlarıyla polisiye yöntemlerle etkili bir mücadele gerçekleştirebilmek için ilgili kolluk birimlerinin suça konu bilişim sistemleri hakkında en az failler kadar bilgi birikimine ve düzeyine sahip olması gerekmektedir[230]. Aksi halde, bilişim hukuku alanındaki fail her zaman kolluktan bir adım önde olacaktır. Kolluk kuvvetinin eğitilmesi, özellikle suçun önlenmesine katkı sağlayacağı gibi adil bir yargılama için de soruşturmanın sağlıklı yürütülmesi için gereklidir.

Soruşturma ve kovuşturmada, savcı ve hakimlerin de bilişim sistemleri hakkında yeterli bilgi birikimine ve donanımına sahip olması gerekmektedir. Çünkü, savcının bilişim suçlarına ilişkin delillerin hızlı ve çabuk tespiti için vermesi gereken talimatı, bilişim sistemleri hakkında bilgi sahibi olmayan bir savcının vermesi mümkün değildir. Bu durum, hali hazırda takibi ve elde etmesi zor olan bilişim sistemindeki delillerin, fail tarafından yok edilmesi için faile zaman kazandıracaktır. Kovuşturmada ise failin bilişim suçuna ilişkin eyleminin yorumlanması önemli olduğu için kovuşturmayı gerçekleştiren hakimin, suça konu bilişim sistemi hakkında yeterli bilgi ve donanıma sahip olması gerekmektedir. Bilişim sistemi hakkında yeterli bilgi ve donanıma sahip

[229] Dülger, **Bilişim Suçları**, s. 636; Uğur Özüdoğru, Siber Suçlarla Mücadele Yöntemleri: Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri, Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, Aralık, 2011, s. 56. https://afyonluoglu.org/PublicWebFiles/Reports-TR/Uzmanlik_Tez/BTK/siber/2011%20Aral%C4%B1k%20Siber%20Su%C3%A7lar%20ve%20M%C3%BCcadele%20Y%C3%B6ntemleri.PDF, e.t.: 09.11.2021.
[230] Dülger, **Bilişim Suçları**, s. 632; Değirmenci, **Bilişim Suçları**, s. 110.

olmayan bir hakimin, dosyaya ilişkin yorum yapması ve dolayısıyla adil kararlar vermesi zorlaşacaktır.

4.3.4.3. Devletlerin Bilişim Suçları İle Mücadele İçin Yasal Düzenlemeler Yapması

Bilişim sistemleri ile işlenen suçlarla mücadelenin en etkin şekilde yapılması ve kalıcı olması için, bilişim suçları ile mücadele ederken insanların temel hak ve özgürlüklerine zarar verilmemesi için bilişim bu suçların ve diğer yasal düzenlemelerin dikkatle hazırlanması gerekmektedir.

Bilişim sistemlerinin kaynağı olan toplumsal sorunlar üzerinde kanun düzenlemenin zor yanı ise bilişim hukukunun hem kamu hukukunu hem de özel hukuku içine alan karma bir yapıya sahip olmasıdır. Bilişim hukuku ile kanun düzenlemesinin zor yanı olan, karma hukuk düzenlemeleridir. Ülkemizde aslında tek bir hukuksal alan olan bilişim hukukuna ilişkin düzenlemelerin farklı kanunlarda ve bölümlerde düzenlenmesi, konunun karmaşıklığına neden olmuştur. Bilişim hukukuna ilişkin düzenlemelerde ortaya çıkan bu karmaşıklık, özellikle bilişim suçlarına ilişkin olan ve çeşitli kanunlarda yer alan düzenlemelerin farklı olmasından kaynaklanma ve bu da uygulama çelişkili kararların ve sorunların çıkmasına sebep olmaktadır.

Oysa, Dünyada bilişim suçlarını ayrı bir kanun olarak düzenleyen hukuk sistemleri vardır. Anglo-Sakson hukuk sitemine tabi olan İngiltere, İrlanda ve ABD bilişim suçları ile ilgili ayrı bir kanun düzenlemişlerdir[231]. Kanımca da ülkemiz hukuk sistemi açısından, bilişim suçları ile ilgili olarak ayrı özel bir kanuni düzenleme yapılması gerekmektedir.

4.3.4.4. Devletlerin Sanal Ortamları Ve İnternet İletişimini Denetlemesi

Siber saldırıların ve bilişim suçlarının önlenmesi amacıyla suçun kaynağı olan sanal ortamların ve faillerin iletişim kurduğu internet iletişim ağlarının denetlenmesi ihtiyacı ortaya çıkmıştır. Sanal alanların denetlenmesinin getirdiği risk ise demokratik toplumun olmazsa olmazı, haberleşme hak ve özgürlüğü, özel hayatın gizliliği, mahremiyeti ve iletişim özgürlüğü gibi ilkelerin ihlal edilme ihtimalidir.

Sosyal ağlar üzerinde yapılan etkileşimlerin ve iletişimin çoğu genellikle ikili veya belli bir grup arasındaki diyaloglardır. Bu diyalogların suç unsuru olup olmadığının bilinmesi nerede ise imkansızdır. Ancak, başta olmak terör suçları üzere, faillerin

[231] Özüdoğru, **Bilişim Suçları**, s. 39.

kullandığı yöntemler, özellikle takibi güç olan sanal iletişim sistemleri üzerinden gerçekleştirilmektedir. Devletler iletişimin tespitini, erişim sağlayıcıları aracılığıyla veya gayri resmi olan ağlar arasındaki veri akışını analiz eden bilişim sistemleri ve yazılımlar üzerinden yapabilmektedir. Bu nedenle, iletişim ağını denetlerken temel hak ve özgürlerin özüne dokunmadan gerçekleştirmek güç olmaktadır[232].

Devletlerin sanal ortamları denetlemesini, sadece ikili veya bir grup arasındaki haberleşme olarak sınırlandırmamak gerekmektedir. İnternet ortamında paylaşılan ve suç içeren veya suçta araç olarak kullanılan her veri devletin denetlemek istediği alana girmektedir.

Devletlerin egemenlik alanı, sanal ortamların denetlenmesi açısından bir başka sorun teşkil etmektedir. Zira, bir internet yayımının, bir sosyal gönderinin veya paylaşımın etki alanı, içerik sağlayıcının bulunduğu ülkenin sınırlarını rahatlıkla aşabilmektedir. İçerik sağlayıcının suç teşkil eden eyleminin, hangi hukuka göre değerlendirileceği sorununun yanında, erişim sağlayan ülkelerin bir kısmında bu eylemelerin suç oluşturduğu kabul edilirken aynı eylemler, içerik sağlayıcının bulunduğu ülkede suç teşkil etmeyebilmektedir. Buna benzer egemenlik alanına ilişkin sorunların yaşandığı durumlarda, uluslararası işbirliğinin önemi tekrar gündeme gelmektedir.

Devletlerin sanal ortamları ve iletişimi denetlemeyi istemesi ve bu konuda düzenleme yapması, kimi zaman temel hak ve özgürlüklerin korunmasının önüne geçmektedir. Genellikle gayri resmi olarak gerçekleştirilen bu denetimlerde, denetimi gerçekleştirilen devletler internet ortamında aktarılan veri trafiğinin tamamını denetleyebilen bilişim sistemleri oluşturmuşlardır. Bu projelerden en çok ses getireni ifşa edilmiş ve gizli bir program olan *"Echelon"* adlı projedir[233].

Echelon projesi ifşa edilince, devletlerin sanal ortamlara müdahaleleri ve internet iletişimi üzerinden denetim sağlamaları, öğrenilmiş ve bunu önemi de çıkmıştır. Bu nedenle, Echelon projesi hakkında bilgi verme gereği duyulmuştur. Echelon projesinin temelleri 1947 yılında UKUSA (Ukusa Agreement) anlaşması ile atılmıştır[234]. Echelon projesi ile ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda devletlerinin istihbarat servislerinin oluşturduğu, dünya üzerindeki iletişimi denetlemek için oluşturulmuş,

---

[232] Berfu Salıcı/İsmail Güneş, "**İnternet Güvenlik ve Denetim: Masumiyet Yitiriliyor Mu?",**https://avesis.cu.edu.tr/yayin/2f0b03d4-b0c4-42c6-acd0-705411713d2a/internette-guvenlik-ve-denetim-masumiyet-yitiriliyor-mu, s. 234, e.t.: 14.04.2004

[233]Vikipedi, **Echelon**, https://tr.wikipedia.org/wiki/ECHELON, e.t.: 27.12.2021.

[234]Wikipedia, **UsukaAgreement**, https://en.wikipedia.org/wiki/UKUSA_Agreement, e.t.: 28.12.2021.

resmi olarak kabul edilmeyen bir projedir[235]. Proje sayesinde telefon, cep telefonu, elektronik postalar, gibi veri iletişim ağlarında aktarılan verilerin tamamı denetlenebilmektedir. Echelon projesinde kullanılan bilişim sisteminde dakikada iki milyon, günde ise üç milyar telefon görüşmesinin dinlendiği belirtilmektedir[236]. Echelon projesindeki sistem aynı anda uydu, internet ağları, radyo sinyalleri gibi dünya üzerindeki tüm iletişim ağlarını özel sistemi sayesinde toplayarak, sözlük adı verilen bir filtreleme sisteminden geçirmekte ve uzmanlar tarafından belirlenen anahtar sözcükler sayesinde istenilen alanda takip yapılabilmektedir.

ABD resmi olarak Echelon projesini kabul etmese de proje Avustralya ve Yeni Zelanda gibi ülkeler tarafından kabul edilmiştir. Projenin, UKUSA anlaşması ile kabul edilen taraf devletlerin ulusal güvenliğinin korunması amacıyla gerçekleştirildiği iddia edilse de projenin ulusal güvenlik amacını aştığı ve sivil ulaşım ve kişisel iletişim sistemlerinin de denetlendiği ve endüstriyel casuslukta kullanıldığı ifade edilmektedir[237].

Ülkemizde sanal ortam ve internet iletişiminin denetlenmesi ilgili yasal düzenleme, "*5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*dur. Kanunun amacı, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir. Kanun tümü itibariyle bu mücadeleyi içerik, yer ve erişim sağlayıcıları üzerinden yapmayı hedeflemiş ve ilgili düzenleme ile içerik sağlayıcılara, yer sağlayıcılara, erişim sağlayıcılara ve toplu kullanım sağlayıcılara sorumluluk yüklemiştir.

5651 Sayılı Kanunun 8. maddesindeki düzenlemeyle TCK'da yer alan; intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama suçlarıyla ilgili olarak içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilebileceği düzenlenmiştir. Bu düzenleme kabul edilebilir niteliktedir. Ancak, 8/A maddesinde,

---

[235] Dülger, **Bilişim Suçları**, s. 635., Atfen, Alp Tekin Ocak, "**Denetim Toplumu: Gözetleniyoruz**", Çev: Tekin Memiş, AÜEHFD, Erzincan, C.VS. 1-4, 2001, s. 324.
[236]Dülger, **Bilişim Suçları**, s. 635, atfen, Mehmet Özcan, "Siber Terörizm ve Ulusal Güvenlik", İnternet ve Hukuk, Der: Yeşim M. Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 301-340.
[237]Dülger, **Bilişim Suçları**, s. 635, atfen, Salıcı/Güneş, İnternet Medya ve Denetim; Ocak, Denetim Toplumu, s. 42.

"*Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması"* gerekçeleri ile *"Cumhurbaşkanlığı veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi ile içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebileceği*" düzenlenmiştir.

Sanal ortamların kullanımında ve internet iletişimin ağlarında kişilerin temel hak ve özgürlerinin geniş alan kapsadığı; temel hak ve özgürlüklere ilişkin alanın, bilişim suçlarıyla mücadele edilirken çakışabileceği hususuna dikkat edilmesi gerekmektedir. İnternetin bir iletişim ağı olduğuna ve iletişim hakkının temel haklar arasında olduğuna göz önüne alındığında, kişilerin iletişiminin denetlenmesinin ve kısıtlanmasının mahkeme kararı ile olması gerekirken, ilgili düzenleme ile mahkeme tarafından yapılması gereken erişimin engellenmesi,*"Bilgi Teknolojileri ve İletişim Kurumu Başkanı"*na verilmiştir. Aynı şekilde, düşünce ve fikir özgürlüğünün en çok kullanıldığı alanlardan olan sosyal ağlarda yer alan bir içeriğin mahkeme kararı ile kaldırılması gerekirken ilgili düzenleme ile bu yetkinin,*"Bilgi Teknolojileri ve İletişim Kurumu Başkanına"*da verilmesi, hukuk devletinin ilklerine aykırı olmaktadır.

Bilişim sistemlerine ilişkin temel bir mevzuatın olmaması sıkıntısı, bu düzenlemede de açıkça görülmektedir. Bilişim sistemlerine ve dijital verilere ilişkin hem özel hem de kamu hukuku alanlarının ülkemizde çok dağınık şekilde düzenlenmesi, demokratik ve adil yargılamayı engellemekte, ayrıca bilişim suçlarıyla mücadeleyi de zorlaştırmaktadır.

SONUÇ

İnsanlar birkaç yüzyıl önce temel ihtiyaçları olmadığı zaman çaresiz hissederken artık çaresizlik hissi elektriğimiz, internetimiz, bilişim sistemlerimiz olmadığı zamanlarda hissedilmeye başlanmıştır. İnsanların maddi gücünün çok üstünde bedeller ödeyerek teknolojik cihazlar alması; sanal ortamda dokunamadığı, tadamadığı, koklayamadığı şeyler için maddi harcamalar yapması, sağlığından dahi vazgeçmesi teknolojinin ve bilişim sistemlerinin insan hayatına ne kadar etki ettiği, insan hayatında ne kadar geniş yer kapladığının göstergesidir.

İnsan hayatındaki bu gelişmelere toplumun hızla ayak uydurması mümkün olmamıştır. İnsanların teknoloji ve bilişim sistemlerine bilgisiz ve kontrolsüz şekilde ulaşma çabası, toplumsal ilişkileri sarsmaya başlamış ve insanların temel haklarına kadar dokunabilen mağduriyetlerin doğmasına yol açmıştır.

Toplumun düzenini sağlamakla görevli olan otoriteler olan devletler, uluslararası örgütler ve kuruluşlar bilişim sistemleri ve teknoloji ile beraber gelen sosyal düzensizliği önlemek ve kontrol altına almak için insanların mağduriyetlerinden yola çıkarak önlemler almaya başlamışlardır. Bilişim sistemleri ile doğrudan veya dolaylı şekilde yaşanan olayları analiz etmişlerdir. Elde ettikleri bulgular doğrultusunda yapılan kanuni düzenlemelerin ise yeni bir kanun düzenlemesinden çok mevcut yasalara uyumlaştırma yoluyla veya mevcut yasalar arasına kapsamı çok sınırlı olan birkaç yeni madde ekleyerek çözüm bulmaya çalışılmışlardır.

Yapılan çalışmalar teknolojinin ve bilişim sistemlerinin gelişme hızı karşısında etkili olamamış, sanal ağ üzerindeki dijital veriler katlanarak artmış, dijital verileri tehdit eden unsurlarda aynı şiddet ve derece ile artmaya devam etmiştir. Toplumsal düzeni sağlayan yasa koyucu otoritelerin yaşanan olaylardan yola çıkarak kanuni düzenleme yapması, sistemin her zaman en az bir adım geriden gelmesine sebep olmuştur. Bilişim sistemlerine karşı gerçekleştirilen ve bilişim sistemleri içerisindeki kişi verileri hedefleyen faillerin her gün yeni yöntemler bulması, kanun koyucu otoritelerin bilişim suçları ile mücadele etmesini neredeyse imkansız bir noktaya getirmiştir.

Kanun koyucu otoritelerin yürürlüğe koydukları yasal düzenlemeleri, hissedilen ihtiyaçlar doğrultusunda geliştirildiği ve şekillendirildiği için doğası gereği karma bir hukuk bilimi olan dijital verilerin kaynağını oluşturduğu bilişim hukuku karışık bir hal almıştır. Kişilere ait verilere ilişkin ayrıntılı bir çalışmanın geçmişten günümüze

yapılırken, bilişim suçlarına ilişkin düzenlemeler daha geri planda kalmıştır. Halbuki her iki yanda da sanal ortama yüklenmiş ve dijitalleşmiş veriler düzenlenmek istenen sorunun kaynağını oluşturmaktadır.

Kişisel verilerin hukuka aykırı şekilde alınması, kullanılması, yer değiştirilmesi ve benzeri hareketlerin, bilişim hukukuna ilişkin düzenlemelerden ayrı düşünmemek gerekmektedir. Çünkü; sanal ortamda bulunan her türlü bilgi dijital bir veridir. Kişisel veriler, kişilere özgülenebilen veriler olarak kabul görüldüğü için, kripto para gibi sahibi olan ve maddi değere sahip dijital veriler gündeme geldiğinde maalesef yapılan hukuki düzenlemeler çaresiz kalmaktadır. Yaşanan çaresizlik durumun içerisinde her devlet kendi hukuki düzenlemesini yapmaya çalışmakta bu durumda ise sınır tanımayan suçlar olan bilişim suçları ile mücadelede, hukuksal bütünlüğün sağlanamaması ile sonuçlanmaktadır. Bu durumda devletler çeşitli anlaşmalarla ve uluslararası örgütlerle bilişim suçlarına karşı ve kişisel verilerin korunması ile ilgili olarak daha geniş kapsama alanına ve daha geniş hukuki içerik barındıran düzenlemeler yapmaya başlamıştır. Devletlerin hem ulusal hem de uluslararası hukukta, bilişim suçları ve kişisel verilere ilişkin düzenlemelerde hukuksal birlik ve bütünlük çabası, aslında dijital verileri konu olan tek ve geniş kapsamlı bir kanuni düzenleme olması gerektiğine ilişkin düşünce ve görüşlerimi desteklemektedir.

Sanal ortama yüklenen her türlü bilgi ya tüzel ya da gerçek kişi tarafından yüklendiği için aslında sahibi var olan verilerdir. Bu verilerin sanal ortama yüklendiği an dijital veri statüsüne kavuşması hukuki düzenlemeye tabi tutulması gereken konunun, kişisel veriler değil, dijital veriler olması gerektiğini ortaya koymaktadır. Aynı durum, bilişim suçları için de geçerlidir. Bilişim suçları sanal ortama yüklenen verileri–dijital verileri konu almaktadır.

Kanun koyucu otoriteler, dijital verilerle ilgili tek ve geniş kapsamlı bir yasal düzenleme yaptığında, yapılan yasal düzenlemenin temeli hem kişisel veriler, hem de bilişim suçlarına ilişkin konular olacağı için anlamsal ve sistematik bütünlük sağlanır. Devletlerin dijital veri temelli geniş ve kapsamlı bir hukuki düzenleme yapması, hem devletlerarası uyumu kolaylaştırır, hem de gerçekleşen eylemlere ve kişisel veri ihlallerine karşı uygulanacak hukuki düzenleme belirlenmiş olur.

Bu çerçevede, öncelikle bilişim hukukunun temelinde yer alan dijital veri olgusu kabul edilmeli ve olabildiğince geniş tanımlanmalıdır. Nasıl gelecek yıllara ilişkin teknolojik gelişmelerin tahminleri yapılıyorsa, dijital verilerin kapsamı ve bilişim hukuku için de aynı çalışmalar yapılıp hazırlanabilen en geniş kapsamlı hukuki

düzenlemenin çalışması yapılmalıdır. Bu sayede kapsayıcı ve ön görülebilir bir hukuki düzenleme ortaya çıkar. Tek çatı altında düzenlenen hukuki düzenlemeler sayesinde ulusal ve uluslararası hukukta, istikrarlı ve uyumlaştırılabilir yasalar sayesinde bilişim suçları ile mücadele etkili ve adil, kişisel verilerin korunması da daha güvenli hale gelmiş olur.

Bu bağlamda, konunun bölgesel düzenlemeler yerine, uluslararası alanda ele alınarak düzenlenmesi, hukuki ve bağlayıcılık bakımından çok daha etkili olacağı düşünülmektedir. Dolayısıyla, tüm ülkeleri tehdit eden ve büyük zararlara neden olan dijital verilerin hukuka aykırı olarak ele geçirilmesi, üçüncü kişilere verilmesi, kişilere ve devletin güvenliğine karşı suçlarda kullanılması ve siber suçlarla mücadele için Birleşmiş Milletler nezdinde yapılacak bir konferansta kabul edilecek çok katılımlı bir sözleşme düzenlenmesi ve bu sözleşme ile tüm ülkeleri sözleşme hükümleri çerçevesindeki yükümlülüklerini takip ve denetlemek için bir merkez oluşturulması ihtiyacı her geçen gün artmaktadır.

Bu şekilde uluslararası bir düzenleme yapılması, bu düzenlemeye taraf olan devletlerin de uniform-tek tip düzenleme yapmalarına ve böylece birlikte mücadele edilmesi ve uygulamada çıkan/çıkacak sorunların ve uyuşmazlıkların aynı kural ve yöntemlerle çözümlenmesi imkanını sağlayabilecektir.

KAYNAKÇA

KİTAPLAR

Ahmet Yavuz Uşaklıoğlu, **Dijital Hukuk,** Seçkin Yayınevi, 2021.

Ali Karagülmez, **Bilişim Suçları ve Soruşturma–Kovuşturma Evreleri,** Seçkin Yayınevi, Ankara 2014.

Ali Parlar, & Mustafa Öztürk, **Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar,** Aristo Yayın Evi, İstanbul 2020.

Emine Doğan Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Doruk Yayınevi, Ankara 1992.

Berrin Akbulut, **Bilişim Alanında Suçlar,** Adalet Yayınevi, Ankara 2017.

Barış Emre Alp, **Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**, Adalet Yayınevi, Anakara 2018.

Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**. Yetkin Yayınevi, İstanbul 2016.

Durmuş Tezcan, Mustafa Ruhan Erdem, & Murat Önok, (2017). **Teorik ve Pratik Ceza Özel Hukuku,** Seçkin Yayınevi, Ankara 2017.

Eşref Barış Börekçi, **Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu (TCK M. 136),** On İki Levha Yayınevi, İstanbul 2020.

İlhan Üzülmez & Mahmut Koca, **Türk Ceza Hukuku Özel Hükümler,** Adalet Yayınevi, Ankara 2018.

İkbal Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Turhan Yayınevi, Ankara 2010.

Levent Kurt, **Açıklamalı ve İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Hukukundaki Uygulaması,** Seçkin Yayınevi, Ankara 2005.

Mahmut Koca & İlhan Üzülmez, **Türk Ceza Hukuku Özel Hükümler,** Adalet Yayınevi, İstanbul 2018.

Mehmet Can Karagöz, **Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemlerini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**. On İki Levha Yayınevi, İstanbul 2020.

Mustafa Albayrak, **Fikir ve Sanat Eserleri ile Markalar Aleyhine İşlenen Suçlar**, Adil Yayınevi, Ankara 2003.

Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku,** Seçkin Yayınevi, Ankara 2020.

Murat Volkan Dülger, **Bilişim, Kişisel Verilerin Korunması ve İnternet İletişim Mevzuatı,** Seçkin Yayınevi, Ankara 2021.

Olgun Değirmenci&Caner Yenidünya, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,** Legal Yayınevi, İstanbul 2003.

Süleyman Yılmaz, **Bilişim Hukuku Güncel Sorunlar II**. Yetkin Yayınevi, İstanbul 2021.

Tunç Demircan, **Bilişim Alanında Suçlar,** Legal Yayınevi, İstanbul 2016.

Yılmaz Yazıcıoğlu, **Fikri Mülkiyet Hukukundan Kaynaklanan Suçlar**, XII Levha Yayıncılık, İstanbul 2009.

Ulrich Sieber, (Editörler) Feridun Yenisey, Salih Oktar, & Zehra Başer Doğan, B**ilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku (Yazarın Seçilmiş Makalelerinden),** Seçkin Yayınevi, Ankara 2021.

Yavuz Edoğan, **Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile),** Legal Yayınevi, İstanbul 2013.

TEZLER

DEĞİRMENCİ Olgun, **Bilişim Suçları Yayınlanmamış Yüksek Lisans Tezi,** Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul 2002.

ORTA Mesut, **Bilişim Suçlarında Adli Analiz**, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Konya 2015.

ÖZÜDOĞRU Uğur, **Siber Suçlar ve Mücadele Yöntemleri: Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri**, Bilişim Teknolojileri ve İletişim Kurumu, Bilişim Uzmanlığı Tezi, İstanbul 2011.

PALLI Hayati, **Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları,** Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Kayseri 2008.

YAZICIOĞLU Recep Yılmaz, **Bilgisayar Suçları Sosyolojik, Kriminolojik ve Hukuki Boyutları ile**, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul 1997.

MAKALELER

AKINCI Ayşe Nur, "Avrupa Birliği Genel Veri Koruma Tüzüğünün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi Çalışma Raporu–6", **Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü 2968 Numaralı Yayını,** 2017, http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf

BAŞBÜYÜK İsa, **Cağdaş Hukukçular Dergisi, "**Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerin Araç Olarak Kullanılması Suretiyle İşlenmesi", 2010.

BENZER Recep, & ALİUSTA Cahit, "Avrupa Birliği Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", **Uluslararası Bilgi Güvenliği Dergisi**, 2018, https://dergipark.org.tr/tr/pub/ubgmd/issue/43240/512829

BULUT İpek Çimen, "Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları", **Anadolu Üniversitesi Sosyal Bilimler Dergisi**, 2019, https://dergipark.org.tr/tr/pub/ausbd/issue/55241/758041

CANBERK Gürol, & SAĞIROĞLU Şeref, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi**, 2006, https://dergipark.org.tr/tr/download/article-file/384578

ÇEKİN Mesut Serdar, "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un BIG DATA (BÜYÜK VERİ) ve İrade Serbestisi Açısından Değerlendirilmesi" , **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,** 2016, https://dergipark.org.tr/tr/pub/iuhfm/issue/28495/304076

DOĞAN Koray, "Bilişim Suçları ve Yeni ve Türk Ceza Kanunu", **Hukuk ve Adalet Eleştiriler Hukuk Dergisi,** 2005.

DÜLGER Murat Volkan, "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması", **Yaşar Hukuk Dergisi**, 2019, https://dergipark.org.tr/tr/pub/yhd/issue/52537/807628

ERDEM Merve & ÖZOCAK Gürkan, "**Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği"**, https://ab.org.tr/ab17/bildiri/110.pdf

GIAKOUMOPOULOS Christos, BUTTARELLI Giovanni & O'FLAHERTY Michael, "Handbook On European Data Protection Law 2018 Edition" https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf,

İÇEL Kayıhan, "Avrupa Konseyi Siber Suç Sözleşmesi, Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, 2001, https://dergipark.org.tr/tr/download/article-file/95984

KARA İlker, "Türkiye'de Zararlı Yazılımlar ile Mücadelenin Uygulama ve Hukuki Boyutu", **Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi**, 2015, https://dergipark.org.tr/tr/pub/abuhsbd/issue/32946/366098

KAYA Ferudun, " Türkiye'de Kredi Kartı Uygulaması**", Türkiye Baralar Birliği Yayınları,** https://www.tbb.org.tr/Dosyalar/Yayinlar/Dokumanlar/263.pdf,

ÖNOK Murat, **"**Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadele Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırma Dergisi**, 2013. https://dergipark.org.tr/tr/pub/maruhad/issue/48280/623844

ÖZBEK Veli Özer, "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,** 2007.

PİRİM Harun, "Yapay Zeka", **Yaşar Üniversitesi E Dergisi,** 2006, https://dergipark.org.tr/tr/pub/jyasar/issue/19113/202842

SALICI Berfu & GÜNEŞ İsmail, "İnternet Güvenlik ve Denetim: Masumiyet Yitiriliyor Mu?", **Akademik Bilişim 2003 Konferasında Sunulan Bildiri,** 2003. https://avesis.cu.edu.tr/yayin/2f0b03d4-b0c4-42c6-acd0-705411713d2a/internette-guvenlik-ve-denetim-masumiyet-yitiriliyor-mu

ŞEN Erhan, "Kripto Para Çalınır mı" **Haber7 Sitesi** https://www.haber7.com/yazarlar/prof-dr-ersan-sen/1948163-bitcoin-calinir-mi,

SINAR Hasan, "**Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme"** Galatasaray Üniversitesi Yayınları, 2004.

TABAN Mehmet Nuri, , "Avrupa Birliği (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri: Avrupa Adalet Divanı", **Türkiye Barolar Birliği Dergisi,** 1998. http://tbbdergisi.barobirlik.org.tr/m1998-19983-879

UZUNAY Yusuf, "Dijital Saldırılar, Emniyet Güçleri Açısından Önemi ve Korunma Yolları", **Polis Bilimleri Dergisi,** 2003. https://app.trdizin.gov.tr/makale/TXpNd05qWT0=/dijital-saldirilar-emniyet-gucleri-acisindan-onemi-ve-korunma-yollari

YAZICIOĞLU Yılmaz, "Yeni Türk Ceza Kanundaki Bilişim Suçları Genel Değerlendirmesi", **Yedi Tepe Üniversitesi Hukuk Fakültesi Dergisi**, 2005, https://yeditepe.edu.tr/sites/default/files/hukuk_dergi/II-2.pdf

SÖZLÜKLER

Türk Dil Kurumu Sözlüğü, https://sozluk.gov.tr

Google Sözlük, https://translate.google.com/

Tureng Sözlük, https://tureng.com/tr/turkce-ingilizce/tuareg

Zargan Sözlük, https://www.zargan.com/tr

İNTERNET KAYNAKLARI

A DEFINITION OF DATA THEFT, https://digitalguardian.com/blog/what-insider-data-theft-data-theft-definition-statistics-and-prevention-tips.

ABLON Lillian / KUZNİTSKY Kathryn , Digital Theft: The New Normal https://www.rand.org/blog/2016/10/digital-theft-the-new-normal.html.

AKBANK, İnternet Dolandıcılığı, , https://www.akbank.com/tr-tr/genel/akbankguvenlik/dolandiricilik.html

Avrupa Birliği Genel Veri Koruma Tüzüğü (GPDR**),** Avrupa Birliği Bakanlığı **Çevirisi,** https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-T%C3%BCrk%C3%A7e-%C3%87eviri-AB-Bakanl%C4%B1%C4%9F%C4%B1.pdf,

Bilişim Teknolojileri,Antivirüs, https://it.bilgi.edu.tr/tr/guvenlik/antivirus/

Counsil Of Europa, Convention on Cybercrime (ETS No. 185) , https://rm.coe.int/1680081561.

Counsil of Europa, ConventionfortheProtection of Individuals with regardto Automatic Processing of Personal Data (ETS No. 108), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019AP0142&rid=1.

Dergi Park, https://dergipark.org.tr/

Emniyet Genel Müdürlüğü, https://www.egm.gov.tr/.

ERDEM Murat/ÖZOCAK Gökhan, "Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslar Arası İşbirliği" https://ab.org.tr/ab17/bildiri/110.pdf ,s. 1,

European Data Protectıon Supervısor, Directive 95/46/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

Güncel Kanunlar, https://www.mevzuat.gov.tr.

Haber Sitesi, https://www.bbc.com/turkce/.

Haber Sitesi, https://www.hurriyet.com.tr/teknoloji/.

Haber Sitesi, https://www.dw.com/tr/.

Haber Sitesi, https://www.gundemkibris.com/teknoloji/.

Haber Sitesi, https://www.trthaber.com/.

Haber Sitesi, https://www.haber7.com.

Haber Sitesi, https://www.ntv.com.tr.

Haber Sitesi, https://www.haberturk.com.

INTRODUCTION, What Is Data Theft? A Simple Explaination in 4 Points (2021), https://www.jigsawacademy.com/blogs/cyber-security/data-theft.

LEGEALBANK, Elektronik Hukuk Bankası, https://legalbank.net/arama

Luxembourg: The theft of digital data–protection or restriction**?** https://www.linklaters.com/it-it/insights/publications/financial-crime-update/financial-crime-update-december-2014/luxembourg-the-theft-of-digital-data--protection-or-restriction.

KAYA, F., "Türkiye'de Kredi Kartı Uygulaması", https://www.tbb.org.tr/Dosyalar/Yayinlar/Dokumanlar/263.pdf.

KirkBorne, Big Data, Small World: KirkBorne at TEDxGeorgeMasonU, https://www.youtube.com/

Online Oyun Satış Sitesi, Game Satış, https://www.gamesatis.com/pubg-mobile-hesap-satisi/oldjoker-hesap-172126,

SEYİDOV, I., "Büyük Verinin Gücü Adına: Siyasi Kampanyalarda Etkili Veri Kullanımı". TRT Akademi, https://doi.org/10.37679/trta.802534.

SONYEL, S. R., " Lawrence, Haşimi Araplarını Osmanlı İmparatorluğu'na Karşı Ayaklanmaları İçin Nasıl Aldattı (İngiliz Gizli Belgelerine Göre)", https://www.ttk.gov.tr/belgelerle-tarih/lawrence-hasimi-araplarini-osmanli-imparatorluguna-karsi-ayaklanmalari-icin-nasil-aldatti-ingiliz-gizli-belgelerine-gore/.

MICHAUD Kately, What Is Data Theft? MPH, BSc Biochemistry, https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft.

Şirketlerin Derdi Veri İhlali Kaynak: https://turk-internet.com/sirketlerin-derdi-veri-ihlali/.

Sinerji Hukuk Yazılımları, https://www.sinerjimevzuat.com.tr/kullaniciGiris.jsf?dswid=6640#

Shodan Web Tarayıcı, https://www.shodan.io/

Vikipedia, Özgür Ansiklopedi**,** https://tr.wikipedia.org.

Verbis Online, Otomatik Veri İşleme ve Otomatik Olmayan Veri İşleme, https://verbis.online/otomatik-veri-isleme-ve-otomatik-olmayan-veri-isleme/.

Yargıtay Resmi İnternet Sitesi, https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/

T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, https://www2.tbmm.gov.tr/d24/1/1-0676.pdf,

Teknoloji Sitesi "Web Tekno", https://www.webtekno.com.

Türk Tarih Kurumu, https://www.ttk.gov.tr/

UEFI Tarayıcı, https://www.eset.com/tr/about/technology.

TITRE IX.- Crimes et délits contre les propriétés, https://sherloc.unodc.org/cld/uploads/res/document/lux/2014/criminal_code_of_luxembourg_html/cp_L2T09.pdf.

Webtekno, https://www.webtekno.com/

KANUNLAR

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (04.05.2007 Tarihli ve 5651 Sayılı), **Resmi Gazete**, 23 Mayıs 2007, S.26530.

Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun (02.05.2014 Tarihli ve 28988 Sayılı), **Resmi Gazete**, 9 Ağustos 2014, S.29083.

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır aşan Veri Akışına İlişkin Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun (20.06.2016 Tarihli ve 6705 Sayılı), **Resmi Gazete**, 5 Mayıs 2016, S.29703.

Fikir ve Sanat Eserleri Kanunu (05.12.1951 Tarihli ve 5846 Sayılı), **Resmi Gazete,** 13 Aralık 1951, S.7981.

Türkiye Cumhuriyeti Anayasası (18.10.1982 Tarihli ve 2709 Sayılı)**, Resmi Gazete**, 9 Kasım 1982, S.17863.

Elektronik İmza Kanunu (15.01.2004 Tarihli ve 5070 Sayılı), **Resmi Gazete**, 23 Ocak 2004, S.25355.

Türk Ceza Kanunu (26.09.2004 Tarihli ve 5237 Sayılı), **Resmi Gazete**, 12 Kasım 2014, S.25611.

Türkiye İstatistik Kanunu (10.11.2005 Tarihli ve 5429 Sayılı), **Resmi Gazete**, 18 Kasım 2005, S.25997.

Kişisel Verilerin Korunması Hakkındaki Kanun (24.04.2016 Tarihli ve 6698 Sayılı), **Resmi Gazete**, 7 Nisan 2016, S.29677.

YARGI KARARLARI

Yrg. 11. C. Dai' nin 12.10.2009 Tarihli ve 2008/11060 E. ve 2009/11936 K. Sayılı İlamı.

Yrg. C. Gnl. Krl.' nin 17.11.2009 Tarihli ve 2009/11-193 E. ve 2009/268 K. Sayılı İlamı.

Yrg. C. Gnl. Krl.' nin 30.03.2010 Tarihli ve 2010/11-17 E. ve 2010/65 K. Sayılı İlamı.

Yrg. 13. C. Dai' nin 10.10.2013 Tarihli ve 2012/14783 E. ve 2013/28348 K. Sayılı İlamı.

Yrg. C. Gnl. Krl' nin 17.06.2014 Tarihli ve 2012/12-1510 E. ve 2014/331 K. Sayılı İlamı.

Yrg. 8. C. Dai' nin 25.05.2017 Tarihli ve 2017/897 E. ve 2017/6019 K. Sayılı İlamı.

Yrg 12. C. Dai' nin 26.06.2019 Tarihli ve 2018/8316 E. ve 2019/7741 K. Sayılı İlamı.

Yrg. 8. C. Dai' nin 11.02.2019 Tarihli ve 2018/6468 E.ve 2019/1826 K. Sayılı İlamı.

Yrg. 8. C. Dai' nin 23.09.2020 Tarihli ve 2019/9478 E. 2020/15892 K. Sayılı İlamı.

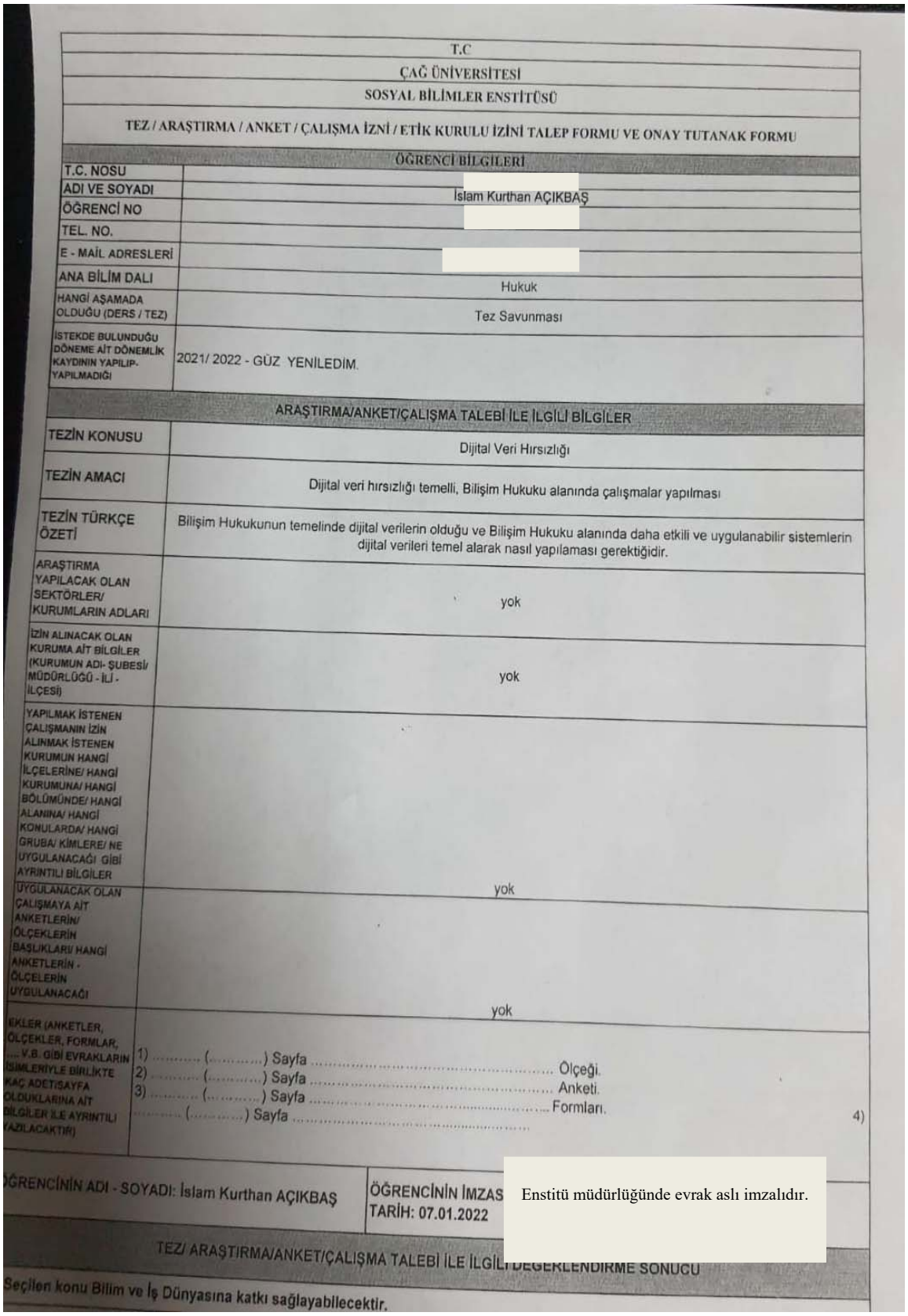
Yrg. 13. C. Dai' nin 08.01.2020 Tarihli ve 2019/9265 E. ve 2020/258 K. Sayılı İlamı.

Yrg. 8. C. Dai' nin 15.12.2021 Tarihli ve 2020/18328 E. ve 2021/ 22899 K. Sayılı İlamı.

Yrg. C. Gnl. Krl.' nin 02/03/2021 Tarihli ve 2018/51 E. ve 2021/68 K. Sayılı İlamı.

EKLER

EK A. Etik Kurulu Onay Belgesi



T.C
ÇAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ / ARAŞTIRMA / ANKET / ÇALIŞMA İZNİ / ETİK KURULU İZİNİ TALEP FORMU VE ONAY TUTANAK FORMU

ÖĞRENCİ BİLGİLERİ

T.C. NOSU	
ADI VE SOYADI	İslam Kurthan AÇIKBAŞ
ÖĞRENCİ NO	
TEL. NO.	
E - MAİL ADRESLERİ	
ANA BİLİM DALI	Hukuk
HANGİ AŞAMADA OLDUĞU (DERS / TEZ)	Tez Savunması
İSTEKDE BULUNDUĞU DÖNEME AİT DÖNEMLİK KAYDININ YAPILIP-YAPILMADIĞI	2021/ 2022 - GÜZ YENİLEDİM.

ARAŞTIRMA/ANKET/ÇALIŞMA TALEBİ İLE İLGİLİ BİLGİLER

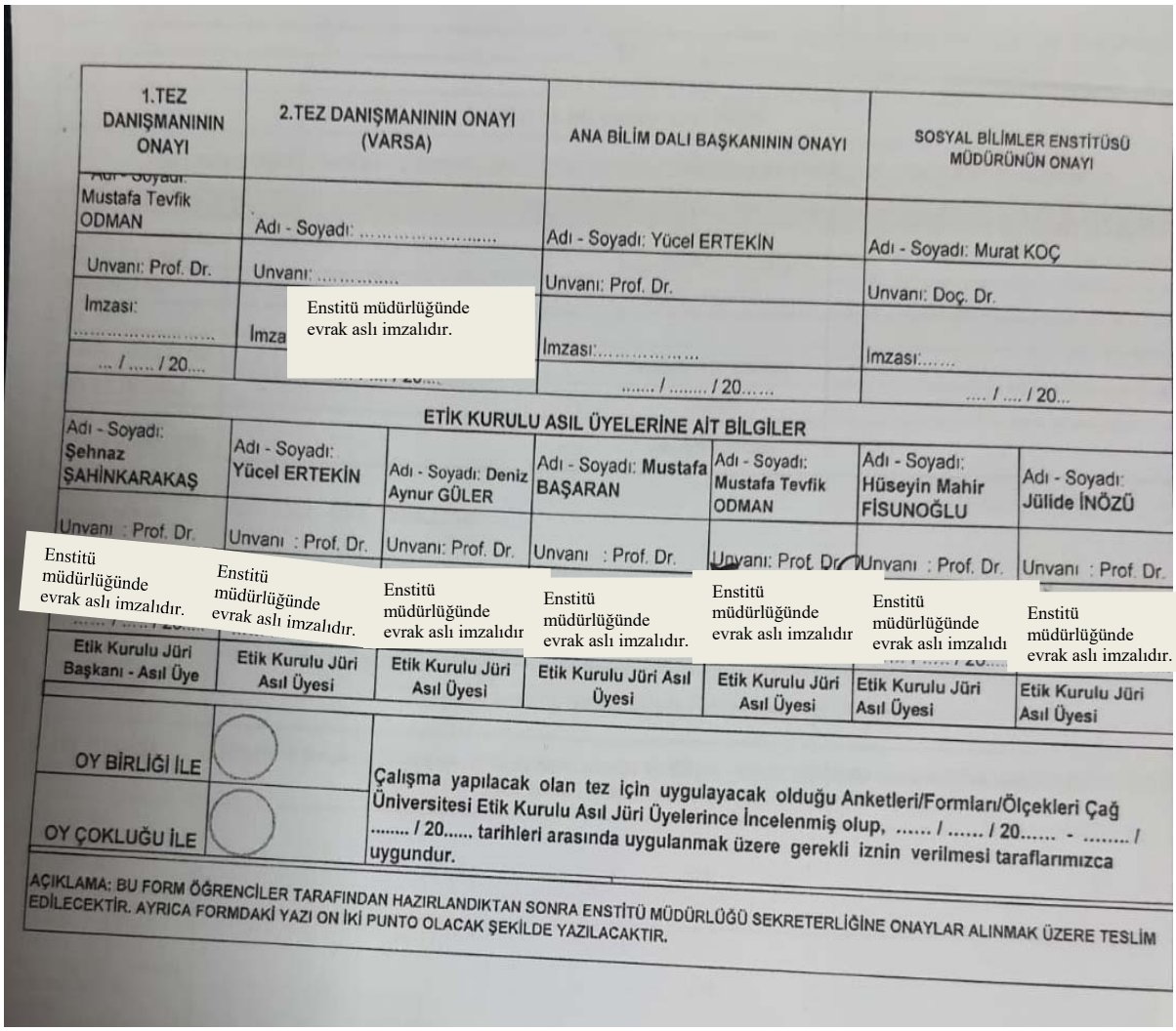
TEZİN KONUSU	Dijital Veri Hırsızlığı
TEZİN AMACI	Dijital veri hırsızlığı temelli, Bilişim Hukuku alanında çalışmalar yapılması
TEZİN TÜRKÇE ÖZETİ	Bilişim Hukukunun temelinde dijital verilerin olduğu ve Bilişim Hukuku alanında daha etkili ve uygulanabilir sistemlerin dijital verileri temel alarak nasıl yapılaması gerektiğidir.
ARAŞTIRMA YAPILACAK OLAN SEKTÖRLER/ KURUMLARIN ADLARI	yok
İZİN ALINACAK OLAN KURUMA AİT BİLGİLER (KURUMUN ADI- ŞUBESİ/ MÜDÜRLÜĞÜ - İLİ - İLÇESİ)	yok
YAPILMAK İSTENEN ÇALIŞMANIN İZİN ALINMAK İSTENEN KURUMUN HANGİ İLÇELERİNE/ HANGİ KURUMUNA/ HANGİ BÖLÜMÜNDE/ HANGİ ALANINA/ HANGİ KONULARDA/ HANGİ GRUBA/ KİMLERE/ NE UYGULANACAĞI GİBİ AYRINTILI BİLGİLER	yok
UYGULANACAK OLAN ÇALIŞMAYA AİT ANKETLERİN/ ÖLÇEKLERİN BAŞLIKLARI/ HANGİ ANKETLERİN - ÖLÇEKLERİN UYGULANACAĞI	yok
EKLER (ANKETLER, ÖLÇEKLER, FORMLAR, ... V.B. GİBİ EVRAKLARIN İSİMLERİYLE BİRLİKTE KAÇ ADET/SAYFA OLDUKLARINA AİT BİLGİLER İLE AYRINTILI YAZILACAKTIR)	1) ..... (.....) Sayfa ..... Ölçeği. 2) ..... (.....) Sayfa ..... Anketi. 3) ..... (.....) Sayfa ..... Formları. ..... (.....) Sayfa ..... 4)

ÖĞRENCİNİN ADI - SOYADI: İslam Kurthan AÇIKBAŞ
ÖĞRENCİNİN İMZAS
TARİH: 07.01.2022

Enstitü müdürlüğünde evrak aslı imzalıdır.

TEZ/ ARAŞTIRMA/ANKET/ÇALIŞMA TALEBİ İLE İLGİLİ DEĞERLENDİRME SONUCU

Seçilen konu Bilim ve İş Dünyasına katkı sağlayabilecektir.



1.TEZ DANIŞMANININ ONAYI	2.TEZ DANIŞMANININ ONAYI (VARSA)	ANA BİLİM DALI BAŞKANININ ONAYI	SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRÜNÜN ONAYI
Adı - Soyadı: Mustafa Tevfik ODMAN	Adı - Soyadı:	Adı - Soyadı: Yücel ERTEKİN	Adı - Soyadı: Murat KOÇ
Unvanı: Prof. Dr.	Unvanı:	Unvanı: Prof. Dr.	Unvanı: Doç. Dr.
İmzası:	İmza	İmzası:.....	İmzası:.....
.. / ..... / 20....	..... / 20....	..... / ..... / 20.....	.... / .... / 20...

Enstitü müdürlüğünde evrak aslı imzalıdır.

ETİK KURULU ASIL ÜYELERİNE AİT BİLGİLER

Adı - Soyadı: **Şehnaz ŞAHİNKARAKAŞ**	Adı - Soyadı: **Yücel ERTEKİN**	Adı - Soyadı: **Deniz Aynur GÜLER**	Adı - Soyadı: **Mustafa BAŞARAN**	Adı - Soyadı: **Mustafa Tevfik ODMAN**	Adı - Soyadı: **Hüseyin Mahir FİSUNOĞLU**	Adı - Soyadı: **Jülide İNÖZÜ**
Unvanı : Prof. Dr.	Unvanı : Prof. Dr.	Unvanı: Prof. Dr.	Unvanı : Prof. Dr.	Unvanı: Prof. Dr.	Unvanı : Prof. Dr.	Unvanı : Prof. Dr.
Enstitü müdürlüğünde evrak aslı imzalıdır.	Enstitü müdürlüğünde evrak aslı imzalıdır.	Enstitü müdürlüğünde evrak aslı imzalıdır	Enstitü müdürlüğünde evrak aslı imzalıdır.	Enstitü müdürlüğünde evrak aslı imzalıdır	Enstitü müdürlüğünde evrak aslı imzalıdı	Enstitü müdürlüğünde evrak aslı imzalıdır.
Etik Kurulu Jüri Başkanı - Asıl Üye	**Etik Kurulu Jüri Asıl Üyesi**	**Etik Kurulu Jüri Asıl Üyesi**	**Etik Kurulu Jüri Asıl Üyesi**	**Etik Kurulu Jüri Asıl Üyesi**	**Etik Kurulu Jüri Asıl Üyesi**	**Etik Kurulu Jüri Asıl Üyesi**

OY BİRLİĞİ İLE	◯	**Çalışma yapılacak olan tez için uygulayacak olduğu Anketleri/Formları/Ölçekleri Çağ Üniversitesi Etik Kurulu Asıl Jüri Üyelerince İncelenmiş olup, ... / ..... / 20..... - ..... / ..... / 20..... tarihleri arasında uygulanmak üzere gerekli iznin verilmesi taraflarımızca uygundur.**
OY ÇOKLUĞU İLE	◯	

AÇIKLAMA: BU FORM ÖĞRENCİLER TARAFINDAN HAZIRLANDIKTAN SONRA ENSTİTÜ MÜDÜRLÜĞÜ SEKRETERLİĞİNE ONAYLAR ALINMAK ÜZERE TESLİM EDİLECEKTİR. AYRICA FORMDAKİ YAZI ON İKİ PUNTO OLACAK ŞEKİLDE YAZILACAKTIR.

EK B. Çağ Üniversitesi Etik Kurul İzin İstek Yazısı

T.C.
ÇAĞ ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

Sayı : E-23867972-050.01.04-2200000236 11.01.2022
Konu : Bilimsel Araştırma ve Yayın Etiği Kurulu Kararı Alınması Hk.

REKTÖRLÜK MAKAMINA

İlgi: 09.03.2021 tarih ve E-81570533-050.01.01-2100001828 sayılı Bilimsel Araştırma ve Yayın Etiği Kurulu konulu yazınız.
İlgi tarihli yazınız kapsamında Üniversitemiz Sosyal Bilimler Enstitüsü bünyesindeki Lisansüstü Programlarda halen tez aşamasında kayıtlı olan **İslam Kurthan AÇIKBAŞ, Emine NALÇACI AKBABA** isimli öğrencilerimize ait tez evraklarının "Üniversitemiz Bilimsel Araştırma ve Yayın Etiği Kurulu Onayları" alınmak üzere Ek'lerde sunulmuş olduğunu arz ederim.

Doç. Dr. Murat KOÇ
Sosyal Bilimler Enstitüsü Müdürü

Ek : 2 Adet öğrenciye ait tez evrakları listesi.

EK C. Tez Etik İzin Yazısı

T.C.
ÇAĞ ÜNİVERSİTESİ
Rektörlük

Sayı : E-81570533-044-2200000402 17.01.2022
Konu : Bilimsel Araştırma ve Yayın Etiği
Kurul İzni Hk.

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : a) 11.01.2022 tarih ve E-23867972- 050.01.04-2200000236 sayılı yazınız.
b) 10.01.2022 tarih ve E-23867972- 050.01.04-2200000183 sayılı yazınız.

İlgi yazılarda söz konusu edilen Dilek Williams, İslam Kurthan Açıkbaş ve Emine Nalçacı Akbaba isimli öğrencilerimizin tez evrakları Bilimsel Araştırma ve Yayın Etiği Kurulunda incelenerek uygun görülmüştür.

Bilgilerinizi ve gereğini rica ederim.

Prof. Dr. Ünal AY
Rektör