

# YAŞAR HUKUK DERGİSİ YAŞAR LAW REVIEW

---

CİLT 1  
VOLUME

SAYI 2  
ISSUE

TEMMUZ 2019  
JULY

---



**YAŞAR**  
ÜNİVERSİTESİ

**SAHİBİ**

**(Yaşar Üniversitesi Rektörlüğü adına)**

Prof. Dr. Ali Nazım SÖZER

**YAYIN KURULU BAŞKANI (EDİTÖR)**

Prof. Dr. Halide Gökçe TÜRKÖĞLU

**YAYIN KURULU**

Prof. Dr. Sevilay UZUNALLI

Prof. Dr. Fevzi DEMİR

Prof. Dr. Timur DEMİRBAŞ

Prof. Dr. Mustafa Ruhan ERDEM

Prof. Dr. Ayşe HAVUTÇU

Prof. Dr. Meral SUNGURTEKİN ÖZKAN

**İNGİLİZCE EDİTÖR**

Öğr. Gör. David BRODY

**EDİTÖR YARDIMCILARI**

Araş. Gör. Muzaffer KARAASLAN

Araş. Gör. Çağrı AVCIOĞLU

**DANIŞMA KURULU**

Prof. Dr. Aydın ZEVKLİLER

Prof. Dr. Haluk BURCUOĞLU

Prof. Dr. Şeref ERTAŞ

Prof. Dr. İsmail KIRCA

Prof. Dr. Ünal NARMANLIOĞLU

Prof. Dr. Ayşe ODMAN BOZTOSUN

Prof. Dr. Işıl ÖZKAN

Prof. Dr. Hasan PULAŞLI

Prof. Dr. Fazıl SAĞLAM

Prof. Dr. Oğuz SANCAKDAR

Prof. Dr. Oruç Hami ŞENER

Prof. Dr. Durmuş TEZCAN

Prof. Dr. Yıldırım ULUER

Prof. Dr. Veliye YANLI

**YAŞAR HUKUK DERGİSİ**  
CİLT 1 SAYI 2 TEMMUZ 2019

**İÇİNDEKİLER**

HAKEMLİ MAKALELER <sup>1</sup>

BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI 6

*Prof. Dr. Berrin AKBULUT*

KONKORDATODA ALACAKLILAR KURULU 47

*Prof. Dr. Meral Sungurtekin ÖZKAN*

AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ BAĞLAMINDA KİŞİSEL  
VERİLERİN KORUNMASI 71

*Doç. Dr. Murat Volkan DÜLGER*

CRYPTOLOCKER; BİR FİDYE VİRÜSÜNÜN CEZA HUKUKU AÇISINDAN ANALİZİ

*Doç. Dr. Olgun DEĞİRMENCİ 175*

YILLIK ÜCRETLİ İZİN 205

*Av. Mustafa TUGAY*

---

<sup>1</sup> Makaleler, yazarların akademik unvanı ve adlarına göre sıralanmıştır.

VELAYET DAVALARINDA ÇOCUKLARIN DURUŞMA SALONUNDA DİNLENMESİNE  
İLİŞKİN HAKİM, AVUKAT VE UZMAN GÖRÜŞLERİ 248

*Umut Haydar COŞKUN, Ayşe Dolunay SARICA, Yeliz COŞKUN*

#### MAKALELER

CEZA MUHAKEMESİNDE BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE  
KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA (CMK M. 134) 271

*Prof. Dr. Cumhuri ŞAHİN*

BİLİŞİM SUÇLARINDA ULUSLARARASI ADLİ YARDIMLAŞMA 287

*Prof. Dr. Durmuş TEZCAN*

YARGITAY KARARLARI IŞIĞINDA DOĞRUDAN BİLİŞİM SUÇLARI (TCK. 243 VE 244 )

*Nevzat ÖZSOY 296*

**YAŞAR LAW REVIEW**  
VOLUME 1, ISSUE 2, JANUARY 2019

**CONTENTS**

ARTICLES (Refereed) <sup>2</sup>

MISUSE OF DEBIT CARDS OR CREDIT CARDS 6

*Prof. Dr. Berrin AKBULUT*

BOARD OF CREDITORS IN THE CONTEXT OF PROTECTING THE INTERESTS OF  
CREDITORS IN COMPOSITION WITH CREDITORS PROCEEDINGS 47

*Prof. Dr. Meral Sungurtekin ÖZKAN*

PERSONAL DATA PROTECTION UNDER GENERAL DATA PROTECTION REGULATION  
IN EUROPEAN UNION 71

*Doç. Dr. Murat Volkan DÜLGER*

CRYPTOLOCKER: ANALYSIS OF A RANSOM VIRUS IN TERMS OF CRIMINAL LAW

*Doç. Dr. Olgun DEĞİRMENCİ* 175

ANNUAL PAID LEAVE 205

*Av. Mustafa TUGAY*

---

<sup>2</sup> Articles are ordered according to the academic titles and names of the authors.

JUDGE, LAWYER AND SPECIALİST OPINIONS ON CHILD HEARING IN CUSTODY  
LAWSUITS 248

*Umut Haydar COŞKUN , Ayşe Dolunay SARICA , Yeliz COŞKUN*

ARTICLES

SEARCH, COPY AND SEIZURE IN THE COMPUTERS, COMPUTER PROGRAMMES AND  
DATABASES UNDER CRIMINAL PROCEDURAL LAW 271

*Prof. Dr. Cumhuri ŞAHİN*

JUDICAL ASSISTANCE IN CYBERCRIME 287

*Prof. Dr. Durmuş TEZCAN*

DIRECT CYBERCRIMES IN THE LIGHT OF SUPREME COURT DECISIONS 296

*Nevzat ÖZSOY*

## **BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI<sup>3</sup>**

*Prof. Dr. Berrin AKBULUT*

### **ÖZET**

Banka veya kredi kartlarının kötüye kullanılması fiilleri, banka ve kredi kartlarında yaşanan gelişmelerin ve kötüye kullanılmaların sonucu olarak TCK'nın 245. maddesinde düzenlenen bir suç şeklidir. İlk defa 5237 sayılı Kanunla mevzuatımıza girmiş bir hükümdür.

Bankamatik kartlarının kötüye kullanılması fiillerinin hangi suç kapsamında nitelendirileceği konusunda zaman içinde tartışmalar yaşanmıştır. Kanun koyucu özel düzenlemeye kavuşturmak suretiyle problemleri ortadan kaldırmak istemiştir. Ancak yapılan düzenleme, bankamatik kartlarıyla ilgili tartışmaları sona erdirmemiş, yeni tartışmalar ve problemler ortaya çıkarmıştır.

245. madde 5 fıkradan oluşmaktadır. Maddede üç ayrı suç tipine yer verilmiştir. İlk üç fıkroda suçlar, son ik fıkroda ise şahsi cezasızlık nedeni ve etkin pişmanlık hükmü düzenlenmiştir. İncelemede 245. madde de düzenlenen her bir suç tipi unsurlarıyla açıklanacak, yaşanan problemler ve eksiklikler belirtilecek, yeri geldikçe yargı kararlarına değinilecektir.

**Anahtar kelimeler:** banka kartı, kredi kartı, sahtecilik, internet, yarar sağlamak, şahsi cezasızlık nedeni.

### **MISUSE OF DEBIT CARDS OR CREDIT CARDS**

#### **ABSTRACT**

The acts of misuse of debit or credit cards are a form of crime issued in article 245 of Turkish Penal Code as a result of the developments and misuse of bank and credit cards. This clause was first entered into our legislation by the Law No. 5237.

There has been some debate over for which crime to consider about misuse of debit cards. The legislator wanted to eliminate the problems by enacting a special rule. However, the arrangement did not stop discussions about debit cards, and new debates and problems arose.

---

<sup>3</sup> ORCID: <https://orcid.org/0000-0001-8045-2784>

Article 245 consists of 5 paragraph. Three different types of crime are included in the article. The first three paragraph regulate the crimes, the last two paragraph regulate the reason for personal impunity and effective remorse. In the study, each type of crime will be explained with the elements of the crime, and the problems and deficiencies will be indicated and the judicial decisions will be mentioned.

Key words: debit card, credit card, forgery, internet, benefit, reason for personal impunity.

## I. GENEL OLARAK

Bilişim alanında yaşanan gelişmeler, bir çok alanda olduğu gibi ceza hukukunu da işlenen suçlar nedeniyle etkilemiştir. Bilişim suçları kavramı ortaya çıkmış, bilişim hukuku veya bilişim ceza hukukunun ayrı bir hukuk dalı olup olmadığı tartışılmaya başlanmıştır. Bilişim alanının, bilişim suçları konusunda ceza hukukunu etkilediği gelişmelerden biri de banka veya kredi kartları ile bunların kötüye kullanılması fiilleridir. Bu kartlar para yerine kullanılmaya başlanmış ve temsil ettiği miktarlar nedeniyle suçun konusu haline gelmişlerdir. Ancak mevcut düzenlemelerin daha ziyade maddi bünyeye sahip ekonomik değerleri koruması, belgelerde yapılan sahteciliği cezalandırmaları, banka veya kredi kartlarının kötüye kullanılması fiillerinin hangi suç kapsamında nitelendirileceği tartışmalarını doğurmuş ve kanunilik ilkesi gereğince ülkeler mevzuatlarında değişikliğe gitmiştir. Türkiye ise, banka veya kredi kartlarının kötüye kullanılması fiilleri için 1 Haziran 2005 tarihli 5237 sayılı Kanunun 245. maddesinde özel düzenleme yapma yolunu tercih etmiştir. Bu suç mülga 765 sayılı TCK'da ayrı bir suç tipi olarak özel düzenlemeye kavuşturulmamıştır. Dolayısıyla da banka veya kredi kartlarının kötüye kullanılması fiillerinin hangi suç kapsamında nitelendirileceği 765 sayılı Kanun döneminde uygulamada farklı içtihatlarla konu olmuştur<sup>4</sup>. Banka veya kredi kartlarının kötüye kullanılmasının bağımsız suç olarak hükme bağlanması çalışmalarına ilk defa 2000 Tasarısında (m. 349) rastlamaktayız. Daha sonra 2003 Tasarısında da hükme (m. 350) yer verildiğini görmekteyiz. Ancak Tasarıdaki düzenleme 5237 sayılı Kanunda değişikliklerle kanunlaştırılmıştır. Gerekçede duraksamaları ve içtihat farklılıklarını önlemek için banka veya kredi kartlarının kötüye kullanılması fiillerinin bağımsız suç haline getirilmesinin uygun bulunduğu belirtilmiştir.

Banka veya kredi kartlarının kötüye kullanılması, TCK'nın Toplum Karşı Suçlar Başlığını Taşıyan Üçüncü Kısımın Bilişim Alanında Suçlar ismini taşıyan onuncu bölümünde düzenlenmiştir. Kanun koyucu bu bölümde yer alan suçları korunan hukuki değere göre ilgili bölümlere

---

<sup>4</sup> Ayrıntılı bilgi için bkz.: Akbulut, Berrin, Bilişim Alanında Suçlar, 2. Baskı, Ankara 2017, s. 270 vd.



yerleştirmemiş, farklı hukuki değerleri koruyan suçları aynı bölümde düzenlemiştir. Bu şekilde düzenleme kanunun sistematiğine aykırı olduğu gibi<sup>5</sup>, suçların koruduğu hukuki değer ve mağdur açısından da sorun yaratmaktadır. Suçların ayrı bir bölümde düzenlenmesinin diğer bir sakıncası da bilişim alanında yaşanan gelişmelerin zamanla ceza hukukunu çok daha fazla etkilemesi ve mevcut hükümlerin değiştirilmesi veya ilave hükümler konulması durumunda birkaç suçun ayrı bir bölümde bilişim alanında suçlar ismiyle düzenlenmesinin mantığının kalmamasıdır. Kalmaya devam etse bile hükümlerin uygulanmasında sorun yaşanacaktır. Örneğin şu an bile bilişim sistemlerinin kullanılması suretiyle hırsızlık (m. 142/2-e), 244. madde, 245. madde arasında sorun yaşanmaktadır. Ayrıca mevzuatımızda başka kanunlarda ve TCK'nın başka bölümlerinde de bilişim araçlarıyla işlenen suçlar bulunmaktadır. Keza mevcut suçların işlenmesinin bilişim araçlarıyla gerçekleştirilmesi de ceza hukukunda değişikliğe gidilmesi sonucunu doğurmakta ve doğuracaktır. Örneğin sanal ortamda oynanan oyunlar aracılığıyla çocukların ölümlere sürüklenmesi (intihara yönlendirme, öldürme suçu), insansız araçların karayolunda veya hava yolunda kullanılmalarından doğan, yapay zekanın kullanıldığı diğer alanlarda yaşanacak sorunlar (izin verilen risk alanı gibi) ceza hukukunda değişikliğe gidilmesi sonucunu doğuracaktır. Tüm dünyada olduğu gibi ülkemizde de Mavi Balina ve benzeri oyunlar çocukların ölümüne yol açmakta ve TCK'nın 84/4. maddesi kapsamına giren bir durum söz konusu olmaktadır. Belirtilen oyunlarda kusur yeteneği olmayan çocuklar veya kusur yeteneği bulunan çocuklar tehdit kullanmak suretiyle intihara mecbur bırakılmaktadır. Dolayısıyla da bu fiilleri işleyen kişilerin öldürme suçundan sorumlu tutulmaları gerekmektedir. TCK'nın 84. maddesinde intihara yönlendirmeye ilgili hükümde ve öldürme suçuna ilişkin düzenlemede (TCK m. 82) değişikliğe gidilerek ağlar aracılığıyla veya kitle iletişim araçlarıyla suçların işlenmesinin cezanın daha fazla verilmesini gerektiren nitelikli hal sayılması uygun olacaktır. 84. maddenin 3. fıkrasında alenen intiharı teşvik suçu yer almaktaysa da bu yalnızca teşvikle ilgili olup azmettirmeyi veya intihar kararını kuvvetlendirmeyi ve dolaylı failliği kapsamamaktadır. Ayrıca 82. maddede de buna ilişkin bir düzenleme bulunmamaktadır. Dolayısıyla bazı suçları ayrı bölümde düzenlemek yerine, korunan hukuki değere göre ilgili bölüme yerleştirmek hem kanunun sistematiğine hem de meydana gelecek gelişmeleri karşılamak

---

<sup>5</sup> Düzenlendiği yerin gözden geçirilmesine ilişkin olarak bkz.: **Özbek, Veli Özer**, “Banka veya Kredi Kartlarının Kötüye Kullanılması suçu (TCK m. 245)”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 9, Özel Sayı 2007, s. 1022; **Yılmaz, Sacit**, “Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu”, TBB, Sayı 87, 2010, s. 267; **Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker**, Türk Ceza Hukuku, Özel Hükümler, 13. Baskı, Ankara 2018, s. 999. İsbetli olduğuna ilişkin olarak bkz.: **Karagülmez, Ali**, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara 2005, s. 200.

açısından daha uygun olacaktır. Bilişim Alanında Suçlarda olduğu gibi ekonomi, sanayi ve ticarete ilişkin suçlarda da aynı tercih yapılmış, belli bir alana ilişkin olmaları nedeniyle bazı suçlar dokuzuncu bölümde düzenlenmiştir. 1987 Öntasarısını hazırlayanlar başka bölüme yerleştiremeyen suçların 9. Bölümde düzenlendiğini belirtmişlerdir<sup>6</sup>. Ancak o dönemde de bu tercihe eleştiriler yöneltmiştir<sup>7</sup>. Bilişim suçlarının ilgili bölüme yerleştirilememesinin söz konusu olmadığı belirtilmelidir.

Kanunun düzenlemesine getirilecek eleştirilerden bir tanesi de benzer nitelikteki fiillerin farklı bölümlerde ve maddelerde düzenlenmesi ve farklı cezaların öngörülmesi nedeniyle hükümler arasında fiillerin haksızlık içerikleriyle uyumlu olmayan belirlenmelerin yapılmış olmasıdır. Bir bilişim sitemindeki verileri değiştirmek, silmek altı aydan üç yıla kadar (kamu kurum ve kuruluşlarına ait bir bilişim sistemi üzerinde işlenmesi yarı oranında artırmak suretiyle) hapisken (TCK m. 244/2-3), özel belgede sahtecilik 1 yıldan 3 yıla kadar hapis cezasıdır (TCK m. 207). Sahte banka veya kredi kartı üretmek ise üç yıldan yedi yıla kadar hapis cezası gerektirmektedir (TCK m. 245/2). Yine internet aracılığıyla bir hesaptan başka bir hesaba para havale edildiğinde Yargıtay'ın kabul ettiği şekilde TCK m. 142/2-e uygulandığında 5 yıldan 10 yıla kadar hapis cezası verilebilmekte, banka veya kredi kartını kullanmak suretiyle para alındığında ise kişinin cezası 3 yıldan 6 yıla kadar hapis ve beşbin güne kadar adli para cezasıdır. Arabanın anahtarını alarak arabayı (500.000 TL'lik) çalan kişi yalnızca hırsızlık suçundan sorumlu olurken (örneğin 5 yıldan 10 yıla kadar hapis cezasıyla m. 142/2-h), banka kartını çalarak (5 yıldan 10 yıla kadar hapis cezasıyla m. 142/2-h) bankamatikten para (2000 TL) çeken (3 yıldan 6 yıla kadar ve adli para cezasıyla) kişi hem hırsızlık suçundan hem de banka veya kredi kartların kötüye kullanılması suçundan (8 yıldan 16 yıla kadar hapis cezasıyla) sorumlu olmaktadır.

Banka veya kredi kartlarının kötüye kullanılması başlığını taşıyan 245. maddede 3 ayrı suç düzenlenmiştir. Birincisi, banka veya kredi kartlarının kötüye kullanılması suçu (f. 1), ikincisi sahte banka veya kredikartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçu (f. 2), üçüncüsü ise sahte banka veya kredi kartını kullanarak yarar sağlamak suçudur (f. 3). Maddede yer

---

<sup>6</sup> **Dönmezer, Sulhi**, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 41.

<sup>7</sup> Bu şekilde tercihin doğru olmadığına ilişkin olarak **Yarsuvat, Duygun**, “Kamuya Gerekli Şeylerin Yokluğuna Sebepiyet Vermek Gıda Maddeleriyle Kamuya Gerekli Madde ve Eşyanın Noksanlığına Sebepiyet Vermek Suçları”, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 63. Aynı bölümde düzenlenmesinin yerindeliği hakkında bkz.: **Cihan, Erol**, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 77; **Erman, Sahir**, “Devletin Ekonomik İtibarını Sarsma Açığa Atılan İmzanın Kötüye Kullanılması Hileli Taksirath İflas”, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 39.

alan diğer iki fıkroda (4 ve 5. fıkroda) ise 1. fıkroda düzenlenen suçla ilgili şahsi cezasızlık nedenine ve etkin pişmanlık hükmüne yer verilmiştir. Kanun koyucunun farklı hukuki değerleri koruyan suçları aynı maddede düzenlemesi de uygulamada ve doktrinde mağdur ile korunan hukuki değer açısından sorun yaratmaktadır. Bu şekilde bir düzenlemenin kanun yapma tekniği açısından da doğru bir tercih olmadı söylenmelidir. Ancak kanun koyucu başka maddelerde de aynı yönde tercihte bulunmaktadır. Mümkün olduğunca kanun koyucunun farklı suçları farklı maddede düzenlenmesi yolunu tercih etmesi gerekir.

Maddenin 2. fıkrasındaki suç, 1 Haziran 2005 tarihinde yürürlüğe giren ilk şeklinde bulunmamaktaydı. O zaman 245. madde düzenlemesi iki fıkradan oluşmakta ve bu fıkralarda şu anki 245. maddenin 1. ve 3. fıkralarındaki suçlar düzenlenmekteydi. 29.06.2005 tarihinde 5377 sayılı Kanunla yapılan değişiklikle ayrı bir suç olarak ikinci fıkra eklenmiş, 2. fıkradaki suç 3. fıkraya alınmış ve 4. fıkroda şahsi cezasızlık nedeni düzenlenmiştir. 245. maddede 6.12.2006 tarihinde bir değişiklik daha yapılmış ve etkin pişmanlık hükmü eklenerek madde bu günkü halini almıştır.

## II. BAŞKASINA AİT BANKA VEYA KREDİ KARTIYLA YARAR SAĞLAMAK SUÇU

### A. KORUNAN HUKUKİ DEĞER

TCK'nın 245. maddesinin 1. fıkrasında düzenlenen başkasına ait banka veya kredi kartıyla yarar sağlamak suçu, malvarlığına ilişkin bir suç olup, bireysel malvarlığını korumaktadır. TCK'nın 245. maddesinin 4. ve 5. fıkrası da bu suçun malvarlığına karşı suç olduğunu ortaya koymaktadır<sup>8</sup>.

<sup>8</sup> **Koca, Mahmut/Üzülmez, İlhan**, Türk Ceza Hukuku, Özel Hükümler, 5. Baskı, Ankara 2018, s. 887, 888; **Yılmaz**, s. 266; **Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, Murat**, Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 16. Baskı, Ankara 2018, s. 1054; **Soyaslan, Doğan**, Ceza Hukuku, Özel Hükümler, Güncelleştirilmiş 11. Baskı, Ankara 2016, s. 656; **Artuk, M. Emin/Gökçen, Ahmet/Yenidünya, A. Caner**, Ceza Hukuku, Özel Hükümler, 15. Baskı, Ankara 2015, s. 896; **Karagülmez**, s. 199; **Gül, Ahmet**, Doğrudan Dolaylı Bilişim Suçları, Ankara 2016, s. 119; **Özbek/Doğan/Bacaksız/Tepe**, s. 999. Ayrıca kişilere duyulan güven (**Artuk/Gökçen/Yenidünya**, s. 896; **Yılmaz**, s. 266), kamuya duyulan güven (**Gül**, s. 119; **Özbek/Doğan/Bacaksız/Tepe**, s. 999), bankacılık sistemine ve ticari yaşama duyulan güven (**Tezcan/Erdem/Önok**, s. 1054; **Özbek**, s. 1022; **Özbek/Doğan/Bacaksız/Tepe**, s. 999), banka ve kredi kartlarının kötüye kullanılmasının önlenmesi (**Koca/Üzülmez**, s. 888), ekonomik yapının sağlıklı işleminin (**Karagülmez**, s. 199) korunduğu da belirtilmektedir. Bazı yazarlar bu suçun daha çok malvarlığına karşı işlenen suç izlenimi verdiğini, ancak düzenlendiği yer itibarıyla bunun anlamsızlaştığını, korunan yararın kamu güveni ve bilişim alanı olduğunun söylenebileceğini belirtmektedirler. Korunan hukuki değer hem malvarlığı, hem de kamu güveni olması kabul edildiğinde karma nitelik taşıdığı, ancak asıl korunan hukuki değer bilişim alanı ve bu alanın güvenliği olduğu belirtilmektedir: **Özbek**, s. 1022, 1025; **Özbek/Doğan/Bacaksız/Tepe**, s. 999, 1000). Bazı yazarlar ise bilişim sistemlerinin düzgün işleminin ilişkin toplumsal menfaat, kamu güveni, kişilere ait malvarlığına ilişkin menfaat gibi çeşitli hukuki varlık veya menfaatleri ihlal ettiğini belirtmekle beraber, suçun hukuki konusunun bilişim sistemlerinin düzgün işlemindeki topluma ait menfaat olduğunu kabul etmektedirler: **Okuyucu-Ergün, Güneş**, "Banka veya

Madde gerekçesinde, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasının, bu yolla çıkar sağlanmasının önlenmesi ve faillerinin cezalandırılması için 245. maddenin kaleme alındığı ifade edilmiştir

## B. SUÇUN UNSURLARI

### 1. Maddi Unsur

#### -Fail ve Mağdur

Suçun faili, herhangi bir kimse olabilir<sup>9</sup>. Hamili olduğu banka veya kredi kartını kullanarak yetki aşımı yapan kişinin fiili suç oluşturmamakta ve 245. madde kapsamına girmemektedir. Banka veya kredi kartı hamili<sup>10</sup>, kartını kötüye kullanmak suretiyle kendisine veya başkasına çıkar sağlamışsa veya banka kartı veya kredi kartını kaybettiği ya da çaldığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanmışsa veya başkasına kullanırmışsa m. 245/1 oluşmaz. 5464 sayılı Banka Kartları ve Kredi Kartları Kanununda yer alan suçlar gerçekleşecektir<sup>11</sup>.

Banka veya kredi kartının kullanılması suretiyle çıkar sağlanması gerektiğinden, bu çıkar nedeniyle hesabında azalma veya borç gözüken banka ve kredi kart hamili olan kişi suçun mağdurudur<sup>12</sup>. Kart düzenleme yetkisine sahip bankalar ve diğer kuruluşlar kartın mülkiyetine sahip olup<sup>13</sup> suçun mağduru değildir<sup>14</sup>. Yargıtay, banka veya kredi kartının veya kart bilgilerinin kart hamiline tesliminden önce ele geçirilerek yarar sağlanması durumunda suçun mağdurunun kartın verilmesi gereken kişi değil, banka (tüzel kişi olması nedeniyle bunu malik veya ortak olarak anlamak gerekir) olduğunu, kartın tesliminden sonra ise adına kart düzenlenen kişinin mağdur olduğunu kabul etmektedir<sup>15</sup>. Yargıtay bu belirlemeyi Banka Kartları ve Kredi Kartları Kanununun

---

Kredi Kartlarının Kötüye Kullanılması (Abuse of Bank or Credit Cards)", Prof. Dr. Nur Centel'e Armağan, 2013, C. 19, S. 2, s. 1067.

<sup>9</sup> Özgü suç olduğuna ilişkin olarak bkz.: **Tezcan/Erdem/Önok**, s. 1064.

<sup>10</sup> Kart hamili, banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişiyi ifade etmektedir (5464 sayılı Banka Kartları ve Kredi Kartları Kanunu, m. 3/j).

<sup>11</sup> Bkz.: **Tezcan/Erdem/Önok**, s. 1054, 1055; **Koca/Üzülmez**, s. 892; **Özbek**, s. 1033.

<sup>12</sup> **Tezcan/Erdem/Önok**, s. 1055; **Yılmaz**, s. 267; **Koca/Üzülmez**, s. 890; **Özbek/Doğan/Bacaksız/Tepe**, s. 1005. Mağdurun toplum olduğuna, kart hamilinin suçtan zarar gören olabileceğine ilişkin olarak bkz.: **Okuyucu-Ergün**, s. 1068. Mağdurun banka ve finans kurumu olduğuna ilişkin olarak bkz.: **Soyaslan**, s. 656; **Gül**, s. 121.

<sup>13</sup> Banka veya kredi kartını çıkaran banka veya diğer kuruluşun mağdur olup olamayacağı doktrinde tartışmalıdır. Mağdur olacağını kabul edenler olduğu gibi (**Özbek/Doğan/Bacaksız/Tepe**, s. 1005; **Özbek**, s. 1029) suçtan zarar gören olabileceğini belirtenler de bulunmaktadır (**Okuyucu-Ergün**, s. 1068; **Tezcan/Erdem/Önok**, s. 1055; **Yılmaz**, s. 268; **Koca/Üzülmez**, s. 890).

<sup>14</sup> "aynı kişiye ait farklı bankalardan verilmiş iki adet kredi kartını değişik zamanlarda kullanması suçunun mağduru adına kredi kartı düzenlenen kişi olması nedeniyle eylemin TCK 245/1 ve 43'e uyan suçu oluşturacağı", 8. CD, 04.07.2018, E. 2017/18974, K. 2018/8273. Ayrıca bkz.: 8. CD, 27.01.2016, E. 2015/14834, K. 2016/969, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.05.2016). 8. CD, 25.01.2016, E. 2015/9775, K. 2016/949, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.01.2017); CGK, 18.10.2011, 166-213, **İlhan ve Diğerleri**, s. 1228.

<sup>15</sup> "Banka ya da finans kuruluşları tarafından üretilen, banka veya kredi kartlarının ya da kart bilgilerinin, kartın hamile tesliminden önce ele geçirilerek menfaat temin edilmesi halinde, suçun mağduru ilgili banka olup; kullanım ve

(5464 sayılı Kanun) 15. maddesi gereğince yapmaktadır. Ancak TCK'nın 245. maddesinin 1. fıkrasında kartın kendisine verilmesi gereken kişinin rızası dışında kullanılması veya kullandırılması arandığından, bu halde de mağdurun adına kart düzenlenen kişi olduğunu kabul ediyoruz<sup>16</sup>. Kartı çıkaran banka ve diğer kuruluşlar ise suçtan zarar gören durumundadırlar.

#### **-Konu**

Başkasına ait banka veya kredi kartıyla yarar sağlamak suçunun konusu, malvarlığına ilişkin herhangi bir değerdir<sup>17</sup>. Ekonomik değeri olan şeyler suçun konusunu oluşturur. Doktrinde bazı yazarlar ise suçun konusunun banka veya kredi kartları olduğunu belirtmektedir<sup>18</sup>. Ancak banka veya kredi kartları, suçun konusu olmayıp fiil aracıdır. Fiil aracı, failin suçu işlemek için kullandığı araçtır<sup>19</sup>.

#### **-FİİL**

Türk Ceza Kanununun 245/1. madesi, “başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa” düzenlemesini içermektedir. Dolayısıyla suçun oluşması için başkasına ait banka veya kredi kartının kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın kullanılması veya kullandırılması ve yarar sağlanması gerekir.

Suçun oluşması için banka veya kredi kartının hem kullanılması veya kullandırılması, hem de yarar sağlanması gerektiğinden, m. 245/1 çok hareketli suç niteliği taşımaktadır. Kullanma veya kullandırtma hareketleri seçimlik olarak sayıldığından herhangi birinin gerçekleştirilmesi suçun oluşması için yeterlidir.

Suçun oluşması için kullanılan veya kullandırılan banka veya kredi kartının başkasına ait olması gerekir. Başkasına ait olmak şartı arandığından kişinin kendisine ait banka veya kredi kartını kullanması halinde, başkasına ait olmak şartı gerçekleşmeyeceğinden m. 245/1 oluşmaz. Başkasına verilip kullandırılması halinde, kullanan açısından başkasına ait kart şartı oluşmakla birlikte, kart hamilinin rızası bulunduğundan yine m. 245/1 gerçekleşmeyecektir.

---

*sağlanan çıkar miktarı, kastın yoğunluğu, suçların işleniş biçimleri gözetilerek TCK.nun 3 ve 61. maddeleri uyarınca alt sınırdan uzaklaşmak suretiyle ve kart sayısı gözetilerek zincirleme şekilde TCK.nun 245/1 ve 43. madde ve fıkraları uyarınca cezalandırılmasına karar verilmesi gerekirken, yazılı şekilde kart sayısının mahkumiyet hükmü kurulması yasaya aykırıdır”, 8. CD, 18.01.2016, E. 2015/14822, K. 2016/441, www.kazanci.com.tr (E.T.23.04.2016). 8. CD, 27.06.2016, E. 2016/1579, K. 2016/8464.*

<sup>16</sup> Özbek/Doğan/Bacaksız/Tepe, s. 1005; Koca/Üzülmmez, s. 890.

<sup>17</sup> Konunun yarar olduğuna ilişkin olarak bkz.: Koca/Üzülmmez, s. 891.

<sup>18</sup> Özbek, s.1025; Özbek/Doğan/Bacaksız/Tepe, s. 1002; Tezcan/Erdem/Önok, s. 1055.

<sup>19</sup> Gropp, Walter, Strafrecht, Allgemeiner Teil, 3. Auflage, Berlin Heidelberg 2005, s. 147.

Başkasına ait banka veya kredi kartının kullanılması veya kullandırılması fiillerinin rıza olmaksızın gerçekleştirilmesi gerekir. Kart hamilinin rızasının bulunması suçun oluşmasını engelleyecektir. Buradaki rıza, tipikliğe ilişkin rıza niteliğindedir. Dolayısıyla kast, kişinin rızasının bulunmadığını da kapsamalıdır.

Banka veya kredi kartının kullanılması veya kullandırılması gerekmektedir<sup>20</sup>. Kartın kullanılması, kartın hamiline sağladığı hizmetlerden yararlanmayı ifade etmektedir. Kullandırtma ise, kartın sağladığı hizmetlerden yararlanmayı başkası aracılığıyla gerçekleştirmeyi belirtmektedir. Kullandırtmanın şekliyle ilgili kanunda herhangi bir belirleme yapılmamıştır. Dolayısıyla herhangi bir şekilde kullandırtarak yarar sağlanmışsa m. 245/1'deki suç oluşacaktır. Azmettirmek, cebir veya tehdit kullanmak ya da hatadan yararlanmak suretiyle kullandırtmak sağlanabilir. Aslında belirtilen durumlarda ya azmettirme ya da dolaylı faillik hükümleri gereğince kişinin cezalandırılması yoluna gidilecekken, kanun koyucunun bu düzenlemesi gereğince kullandırtan kişi fail olarak sorumlu tutulmaktadır<sup>21</sup>. Kullanan kişi hakkında ise cebir veya tehdit etkisiyle kullanmışsa kusurunun bulunmaması nedeniyle ceza verilmesine yer olmadığı kararı verilecek, azmettirilmişse iştirak kuralları gereğince fail olarak sorumlu tutulacak, hata içindeyse (kastı ortadan kaldıran hatada TCK. m. 30 gereğince fiilin taksirli şekli bulunmadığından) sorumlu tutulmayacaktır. Ancak cebir veya tehdit kart hamiline uygulanmış ve hamilin cebir veya tehdit ile örneğin bıçak zoruyla bankamatikten para çekip vermesi sağlanmışsa<sup>22</sup> yağma suçu söz konusu olacaktır. Ele geçirilen veya elinde bulundurulmuş kart söz konusu olmadığından m. 245/1'in uygulanması söz konusu olmayıp yalnızca yağma suçu gerçekleşmektedir. Silah kullanılması veya diğer nitelikli hallerin gerçekleşmesi halinde m. 149 gereğince sorumluluk tayin edilecektir.

Banka kartının veya kredi kartının ne olduğu Banka Kartları ve Kredi Kartları Kanunu m. 3'e göre belirlenecektir. Banka kartı, mevduat hesabı veya özel carî hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kartı ifade etmektedir (Banka Kartları ve Kredi

---

<sup>20</sup> “Emekli aylığını çekmek için ATM önüne gelen katılanın kendisine yardım etmesini istediği sanığın, katılana ait kart ile başka bir kartı el çabukluğu ile değiştirip katılıandan kart şifresini öğrendiği, işlem yaparken ATM cihazının kartı yuttuğunu söyleyip katılanı banka şubesine gönderdiği, görevlinin ATM cihazı içerisinden başka birisine ait kartı çıkarttığı ve katılanın hesabını kontrol ettiğinde 550,00 TL olan parasının çekilmiş olduğunu fark ettiği olayda, sanığın suça konu bankamatik kartını hakimiyetine geçirip kullanmak şeklindeki eylemi ile birlikte TCK. 245/1 maddesinde düzenlenen banka ve kredi kartlarının kötüye kullanılması suçunun maddi unsurlarından olan başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçirme veya elinde bulundurma koşulunun gerçekleştiği, sanığın katılana ait hesaptan suça konu kartı kullanarak para çekmek suretiyle haksız menfaat temin edildiği ve TCK. 245/1. maddesinde düzenlenen banka ve kredi kartlarının kötüye kullanılması suçunun tamamlandığına yönelik kabulde bir isabetsizlik görülmemiştir”, 15. CD, 13.4.2017, E. 2017/3801, K. 2017/9251.

<sup>21</sup> Koca/Üzülmüş, s. 894.

<sup>22</sup> Helmann, Uwe, “Der praktische Fall - Strafrecht: Überfall am Geldautomaten”, JuS, 1996, Heft 6, s. 522 vd.; Tezcan/Erdem/Önok, s. 1057.

Kartları Kanunu m. 3/d). Bu tanımlamaya göre banka kartı, mevduat hesabı ve özel cari hesabı bulunan kişilere verilen kart niteliği taşımaktadır. Hesapları kullanmak dışında diğer bankacılık işlemlerden yararlanmayı da sağlamaktadır. Para yatırma, para çekme, mal ve hizmet alımlarının bedelini ödeme, hisse senedi alım satımı gibi işlemler yapılabilmektedir. Kredi kartı, nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını belirtmektedir (Banka Kartları ve Kredi Kartları Kanunu m. 3/e). Kredi kartları kullanıcıya kredi limiti çerçevesinde üye işyerlerinde mal ve hizmet alımı yapmasına imkan tanımakta, nakit çekme hizmeti vermektedir. Limitin aşılması kullanıma imkanı olmakla beraber faiz uygulanması yoluna gidilmektedir (5464 sayılı Kanun m. 9). Çıkarılan sanal kartlar da kredi kartları niteliğinde olup, m. 245/1 kapsamındadır.

Banka veya kredi dışındaki diğer elektronik kartların kullanılmasında m. 245/1 uygulanmaz. TCK m. 244/4'ün şartlarının gerçekleşmesi şartıyla bu fıkranın uygulanması yoluna gidilecektir. Örneğin manipülasyon yapılmak suretiyle haksız çıkar sağlanmışsa m. 244/4 uygulanacaktır. PayPal Nakit Kart, İninal Kart, Passolig Kart gibi kartların kullanılmasında, bu kartlar Banka veya Kredi Kartları Kanununa göre banka veya kredi kartı sayılmadığından bu kartlarla ilgili gerçekleştirilen fiiller TCK m. 245/1 kapsamında değildir<sup>23</sup>. Başkasının kartının internetten yapılan alışverişlerde rıza dışı kullanılması durumunda m. 244/4 kapsamında değerlendirme yapmak gerekmektedir. Yargıtay'ın görüşü (söz konusu kartlarla ilgili olmamakla beraber) bu gibi durumlarda m. 142/2-e'nin uygulanması yönündedir. Kanun koyucunun kartlar konusunda özel düzenleme yapma yolunu tercih ediyorsa tüm kartları içeren düzenleme yapması gerekmektedir. Aksi takdirde farklı maddelerin ve cezaların uygulanması devreye girmektedir. Yargıtayın görüşü kabul edildiğinde banka veya kredi kartı olmayan kartlarda kişinin cezası 5 yıldan 10 yıla kadar hapis cezası olurken, banka veya kredi kartıyla yarar sağladığında 3 yıldan 6 yıla kadar hapis cezası ve adli para cezasıyla cezalandırılmaktadır. Kartlar konusunda farklı kanun hükümlerinin uygulanması imkanının ortadan kaldırılması ve suçun banka ve kredi kartlarıyla işlenmesinin nitelikli hal olarak düzenlemesi gerekmektedir.

Banka veya kredi kartının ele geçiriliş veya elinde bulunduruş şekli önemli değildir. Kanun koyucu bunu 245/1. maddede “her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse” ifadesiyle belirtmiştir. Çalınan, bulunan veya hata sonucu ele geçirilen, rıza ile verilen<sup>24</sup>,

---

<sup>23</sup> Aksi görüş **Gül**, s. 120.

<sup>24</sup> “Oluşa, katılanın beyanına, suça sürüklenen çocuğun savunmasına ve tüm dosya kapsamına göre; katılanın yanında çalışan sanığa kredi kartını ve şifresini vermesinin ardından suça sürüklenen çocuğun kart ile aldığı şifreyi kullanarak

kartın iptal ettirilmesi için verilen, rızası dışında alınıp, kullanıldıktan sonra geri bırakılan<sup>25</sup> veya kartın hamiline teslim edilmesi için elde bulundurulan kartlar her ne suretle olursa olsun ele geçirilen veya elinde bulundurulan kart niteliğindedir. Bankamatik kartlarının rıza ile verilip, yetki sınırının aşılması durumunda, kart hamilinin belirli bir miktar çekmesi için verdiği, ancak anlaşılan miktarın üzerinde kullanıldığı veya alışverişler yapıldığı veya veriliş amacının dışında farklı zamanlarda nakit çekilmesinde yararlanıldığı gibi olaylarda fiil m. 245/1 kapsamındadır<sup>26</sup>.

Kart hamilinin hileli davranışlarla para çekme konusunda kandırılıp banka veya kredi kartıyla tasarrufta bulunulması durumunda dolandırıcılık suçunun<sup>27</sup> gerçekleştiği kabul edilmektedir<sup>28</sup>. Burada hile para çekilmesi için kullanılmıştır. Fiil soyut yalanın dışındaysa dolandırıcılık suçu açısından değerlendirme yapılmalıdır. Kanunumuza göre aynı zamanda her ne suretle olursa olsun ele geçirilen kart olduğundan ve bu kartın kullanılması suretiyle yarar sağlanması da gerçekleştiğinden m. 245/1 de ihlal edilmiştir. Sorun suçların içtimaı (fikri içtima) kapsamında çözümlenmelidir.

Yargıtay bir olayda m. 245/1'in ve dolandırıcılık suçunun gerçekleşmediğini, hırsızlıktan hüküm kurulması gerektiğini kabul etmiştir. Yargıtay'a göre, "*maaşını çekmek amacıyla ATM cihazına gelen mağdurun banka kartını cihaza yerleştirip, şifresini yazdıktan sonra işlem*

---

*yarar sağlaması eyleminin TCK'nın 245/1. madde ve fıkrasında tanımlı suçu oluşturduğu gözetilmeden, yazılı şekilde TCK'nın 155/2. madde ve fıkrası uyarınca uygulama yapılması*", 8. CD, 15.06.2016, E. 2015/10794, K. 2016/7952.

<sup>25</sup> Kullanıldıktan sonra geri bırakılan kartlarla ilgili olarak bkz.: **Wessels, Johannes/Hillenkamp, Thomas**, (Çev.: Yener Ünver), "Hırsızlık ve Güveni Kötüye Kullanma Suçları", Malvarlığına Karşı Suçlar ve Ekonomik Suçluluk, Karşılaştırmalı Güncel Ceza Hukuku Serisi 9, Prof. Dr. Eric Hilgendorf'a Armağan, Ankara 2009, s. 65 vd.

<sup>26</sup> "*Sanık, katılanın kendisine ait işyerine alışveriş yapması için rızasıyla verdiği kredi kartıyla değişik zamanlarda kendisi için birden fazla nakit çekme ve nakit çekmeye teşebbüs etmiştir. Kartın birden fazla kullanılması sebebiyle banka veya kredi kartlarının kötüye kullanılması suçu sebebiyle verilecek cezadan zincirleme suç hükümleri uyarınca artırım yapılması gerekir*", 8. CD, 10.03.2015, E. [2014/28835, K. 2015/13337, www.kazanci.com \(E.T.02.02.2017\)](#).

<sup>27</sup> "*Oluşa, katılanın beyanına, sanıkların savunmalarına ve tüm dosya kapsamına göre; Suç tarihinde katılan ...'nun cep telefonuna "düzenli kredi kartı ödemelerinizden dolayı 1000 TL indirim kazandınız ...'i arayarak bu indirimi gerçekleştirin" şeklinde mesaj gönderilmesi üzerine katılanın ... Pazarlama ve ... İletişim Turizm Pazarlama şirketinin kimliği tespit edilemeyen satış elamanı ile ürün satışına ilişkin telefon görüşmesi yaptığı, satış elamanın piyasa değeri 200 TL olan iki adet cep telefonu ve mini uydu alıcısını 2000 TL'ye katılana satarak, katılanın kredi kartından para çekimini gerçekleştirdiğinin anlaşıldığı olayda, katılanın ... kredi kartı ile ilgili istenen tüm bilgileri satış elamanına rızası ile vermesi ve satışların da 3D güvenli sistem ile yapıldığının 13.12.2013 tarihli ... yazısı ile sabit olması karşısında, sanıkların eyleminin TCK.nun 157 maddesinde tanımlı Dolandırıcılık suçunu oluşturacağı gözetilmeden, suç vasfında yanılığa düşülerek yazılı şekilde TCK.nun 245/1. madde ve fıkrasında tanımlanan banka veya kredi kartlarının kötüye kullanılması suçundan mahkumiyetine hükmedilmes,"yasaya aykırıdır: 8. CD, 9.1.2017, E. 2016/8611, K. 2017/11.*

<sup>28</sup> **Cramer/Perron-Schönke/Schröder**, 2010, § 263 a, kn. 42; **Tröndle, Herbert/Fischer, Thomas**, Strafgesetzbuch und Nebengesetze, 53. Auflage, München 2006, § 263 a, kn. 13; **Dreher, Eduard/Tröndle, Herbert**, Strafgesetzbuch und Nebengesetze, Kommentar, 47., neubearbeitete Auflage des von Otto Schwarz begründeten Werkes, München 1995, § 263 a, kn. 8; **Hecker, Bernd**, "Die Strafbarkeit des Ablistens oder Abnötigens der persönlichen Geheimnummer", JA, 1998, Heft 4, s. 301; Farklı düşünce için bkz.: **Erdem, Mustafa Ruhan/Özbek, Veli Özer**, "Ceza Hukuku Açısından Bankamatiklerin Kötüye Kullanılması", İzmir Barosu Dergisi, 1997, s. 76.



menüsünün ekrana yansıdığı aşamada yardım etme bahanesiyle mağdurun yanına gelen sanığın, mağdurun talebi doğrultusunda hesapta bulunan para miktarına bakma bahanesiyle hesaptan 800 liranın çekilmesi amacıyla işlemler yaptıktan sonra, hesapta para bulunmadığını söyleyip, mağdurun gerçekten hesabında para bulunup bulunmadığını kontrol amacıyla yan tarafta bulunan diğer ATM cihazına geçmesini fırsat bilerek ATM cihazının verdiği 800 TL'yi alarak olay yerinden kaçması şeklinde gerçekleşen somut olayda; suça konu bankamatik kartının mağdur tarafından makinaya yerleştirilip işlemlere başlanması ve kartın sanığın eline hiçbir şekilde geçmemiş olması nedeniyle, 5237 sayılı TCK'nın 245. maddesinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun, başkasına ait banka veya kredi kartının her ne suretle olursa olsun ele geçirilmesi veya elde bulundurulması şartı gerçekleşmemiştir. Diğer taraftan, sanığın hesapta para bulunmadığı şeklindeki beyanı dolandırıcılık suçunun hileli davranış unsurunu oluşturacak nitelikte bulunmayıp, soyut yalandan ibarettir. Zira mağdurun o an hesabını kontrol ederek para olup olmadığını anlama imkanı bulunmaktadır. Öte yandan suça konu paranın mağdurun rızasıyla teslimi de söz konusu değildir. Dolayısıyla, banka veya kredi kartlarının kötüye kullanılması ve dolandırıcılık suçlarından her ikisinin de unsurları itibarıyla oluşmadığı göz önünde bulundurulduğunda, sanığın eyleminin hırsızlık suçunu oluşturduğu yönündeki özel dairenin bozma kararı doğrudur”<sup>29</sup> şeklinde belirleme yapmıştır. Ancak bu karara katılmıyoruz. Görüşümüze göre burada m. 244/4'ün uygulanması gerekmektedir. Çünkü TCK m. 244/2 çerçevesinde gerçekleştirilen bir fiille çıkar sağlanması söz konusudur. Ayrıca kartın rıza ile alınıp kendisine verilen yetkinin dışında kullanıldığında kişinin, 3 yıldan 6 yıla kadar ceza ile cezalandırılması söz konusuysa verilen karardaki olayda bilişim sisteminin kullanılması suretiyle eylem gerçekleştirildiğinden 5 yıldan 10 yıla kadar ceza verilmesi söz konusu olacaktır<sup>30</sup>. Yargıtay

<sup>29</sup> CGK.08.04.2014 gün ve 1368-179, İlhan ve Diğerleri, s. 837. Aynı yönde “Oluşa ve dosya kapsamına göre; para çekmek için bankamatik kartını ATM cihazına yerleştiren ve şifresini giren katılanla sohbet eden sanığın gizlice ATM cihazının para çekme tuşuna basıp, katılan uzaklaştıktan sonra çekilen tutarı alması şeklinde gelişen eyleminde, sanığın suça konu kredi kartını ya da kart bilgilerini ele geçirmiş olmaması sebebiyle TCK'nın 245/1. maddesinde düzenlenen suçun unsurlarının bulunmadığı, eylemin TCK'nın 141/1. maddesinde düzenlenen “hırsızlık” suçunu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi yasaya aykırı olup”, 8. CD, 17.6.2015, E. 2014/37160, K. 2015/19397, www. kazanci.com (E.T.23.01.2017).

<sup>30</sup> “Sanıklar hakkında Banka veya kredi kartlarının kötüye kullanılması suçundan kurulan hükümlerin incelenmesinde; sanıkların ilk olarak ATM'den para çekmek amacıyla gelen ve kimliği tespit edilemeyen bir şahsa ait banka kartını kurdukları özel düzenek sayesinde ele geçirmeye çalışırken polisçe yakalanma korkusu ile olay yerinden kaçmaları; yine aynı gün ... Bankasının ... Bulvarındaki ATM cihazına kurdukları özel düzenekle mağdurun kartını sıkıştırıp almaya çalışırken polisçe yakalanmaları, şeklinde gerçekleşen eylemlerinin iki ayrı hırsızlığa teşebbüs suçunu, sonraki tarihte .ilinde ATM'den para çekme amacıyla gelen şikayetçiye ait banka kartını kurdukları özel düzenek sayesinde çalmaktan ibaret eylemlerinin, hırsızlık suçunu oluşturacağı gözetilmeden, TCK'nun 245/1. ve 35. maddeleri uyarınca hüküm kurulması hukuka aykırıdır”, 8. CD, 4.4.2013, E. 2012/37255, K. 2013/10817. “Şikayetçinin para çekmek için gittiği ATM'de kartıyla işlem yapmak üzere şifresini girdiği, para çekme bölümüne sanığın yerleştirdiği düzenek

kartın kullanıldığı benzer bir olayda fail tarafından kartın kullanılması nedeniyle eylemin m. 245/1 kapsamında olduğunu nitelendirmiştir: “*Sanığın olay tarihinde emekli maaşını çekmek üzere ATM’ye giden şikayetçiye yardım etme bahanesiyle banka kartını alıp ATM’ye sokarak şikayetçinin söylediği şifreyi girdiği, para çekme işlemi yaptıktan sonra ATM’den çıkan kartı şikayetçiye iade ederek hesapta yalnızca 30 TL olduğunu söylediği, şikayetçinin emekli maaşını henüz çekmediğini, hesapta para olması gerektiğini söylediği üzerine ise şikayetçiyi bankaya yönlendirerek ATM’den çıkan 550 TL’yi alması şeklinde gerçekleşen eylemde suç vasfını TCK’nın 245/1. madde ve fıkrasında düzenlenen başkasına ait banka veya kredi kartının kötüye kullanılması olarak belirleyen mahkemenin takdir ve uygulamasında bir isabetsizlik görülmemiştir*”<sup>31</sup>.

Banka veya kredi kartının kullanılması veya kullandırılmasının fiziki kullanmayı mı ifade ettiği, yoksa ele geçirilen kart numarasının ve şifresinin internet üzerinden kullanılarak yarar sağlamasını da mı kapsadığı tartışmalıdır<sup>32</sup>. Herşeyden önce belirtilmelidir ki, banka veya kredi kartlarının kötüye kullanılması suçu, banka veya kredi kartlarıyla ilgili özel bir düzenlemedir. Ayrıca 5464 sayılı Kanunun 3. maddesi, fiziki varlığı olmayan kart numarasını da kredi kartı olarak tanımlamaktadır. Dolayısıyla sadece fiziki kullanımlarda değil, diğer kullanımlarda da m. 245/1’in uygulanacağını kabul ediyoruz. TCK m. 244/4’ün uygulanması ancak başka bir suçun kapsamına

---

*nedeniyle para ve kartını alamadığı, bankanın kapalı olması ve orada bulunan yardım bahanesiyle yaklaşan sanıkla beraber şikayetçinin şifreyi tekrar girip yine işlem yapamaması üzerine oradan uzaklaşması sonucu sanığın ATM’den çıkan parayı alıp uzaklaştığı, şikayetçinin daha sonra kartını banka görevlilerinden teslim aldığı anlaşılmalı, sanığın şikayetçinin kartını alıp kullanmaya yönelik hareketi bulunmayıp hedefinin sadece ATM’deki paraya yönelik olduğu, menkul mal niteliğinde olan paranın zilyedin rızası dışında alıkonulması nedeniyle hırsızlık suçunu oluşturacağı gözetilmeden, uygulama alanı bulunmayan TCK’nın 245/1. maddedeki suçtan mahkumiyete hükmedilmesi” bozmaya konu olmuştur, 8. CD, 08.04.2015, E. 2014/33365, K. 2015/15858, **Gül**, s. 127.*

<sup>31</sup> 8. CD, 16.04.2018, E. 2017/17930, K. 2018/4266.

<sup>32</sup> Doktrinde bazı yazarlar banka veya kredi kartının ATM, POS (Point Of Sale) cihazı gibi makinelerden geçirilerek fiziki kullanımlarında m. 245/1’in uygulanacağını, kart numarasının ve şifresinin internet üzerinden alışverişlerde kullanılması halinde m. 245/1’in gerçekleşmeyeceğini belirtmektedirler. Kanundaki kartın kullanılması veya kullandırılması ifadesi, fiili kullanımları kastetmektedir: **Koca/Üzülmüş**, s. 895; **Tezcan/Erdem/Önok**, s. 1057; **Ekinci, Mustafa/Esen, Sinan**, Anlatımlı ve Gerekçeli Yeni Türk Ceza Kanununda Yer Alan Hırsızlık Yağma Güveni Kötüye Kullanma Dolandırıcılık Hileli ve Taksirli İflas Karşılıksız Yararlanma Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Ankara 2005, s. 373; **Özbek/Doğan/Bacaksız/Tepe**, s. 1008, 1009 (yazar m. 244/4’teki başka suç oluşturmama ibaresi nedeniyle m. 245/1’in de uygulanmasının mümkün olduğunu söylemektedir); **Özbek**, s. 1032, 1033 (Yazar m. 245’in uygulanmayacağını belirtmekle beraber kredi kartının banka kartından farklı olarak “basılı kart veya fiziki varlığı bulunmayan kart numarası” şeklinde tanımlanması nedeniyle m. 245/1 açısından kredi kartının fiziksel olarak kullanılmasının zorunlu olmadığı sonucu çıktığını da ifade etmektedir). Bu durumda m. 244/2-3 veya m. 244/4 (**Özbek/Doğan/Bacaksız/Tepe**, s. 1008; **Özbek**, s. 1032), somut olayın işleniş şekline göre hırsızlık, dolandırıcılık veya m. 244/4’ün uygulanması gerektiği ifade edilmektedir (**Koca/Üzülmüş**, s. 895; **Ekinci/Esen**, s. 373). Bazı yazarlar ise maddenin yalnızca fiziki kullanımları kapsamadığını, aynı zamanda kart bilgilerinin kullanılarak yarar sağlanmasının da m. 245/1 kapsamında olduğunu benimsemektedirler. Buna gerekçe olarak da 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 3. maddesi hükmü ileri sürülmektedir: **Yılmaz**, s. 274; **Karagülmez**, s. 211; **Okuyucu Ergün**, s. 1071, 1072. Aynı yönde **Mahmutoğlu, Fatih Selami**, “Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, İÜHF, 2013, C. LXXI, S. 1, s. 872.

giremeyen hallerde söz konusu olduğu için sorunun m. 245/1 çerçevesinde çözümlenmesi gerektiği düşünmekteyiz. Yargıtay da yalnızca fiziki kullanımlarda değil şifre ve kart numarasının kullanılarak internette işlem yapılması durumunda da m. 245/1'in uygulanacağını kabul etmektedir<sup>33</sup>.

### -Yarar Sağlamak

Başkasına ait banka veya kredi kartıyla yarar sağlamak suçunun oluşması için, suçun isminden de anlaşıldığı gibi yararın sağlanması gerekmektedir. Yarar, kartın ve kart bilgilerinin kullanılması suretiyle elde edilmiş olmalıdır<sup>34</sup>. Kart kullanılmakla veya kullandırılmakla beraber, yarar elde edilememişse m. 245/1'de düzenlenen suç tamamlanmış olmaz. Ayrıca kartın kullanılması veya kullandırılması ile sağlanan yarar arasında bağlantı bulunmalıdır. Yarar sağlanması suçun aynı zamanda bir zarar suçu olduğunu göstermektedir.

Yarar, failin kendisine sağlanabileceği gibi, başkasına da sağlanabilir. Yararın mutlaka fiilen elde edilmiş olması gerekmez. Yarar, üzerinde tasarruf edebilir duruma gelmiş ise suç tamamlanmış demektir. Örneğin, ATM'de parayı kendi hesabına havale etmiş olması yeterli olup, yararın sağlanması için paranın çekilmiş olması gerekmez<sup>35</sup>

Yararın ekonomik nitelikte olması gerekir. Ekonomik nitelikte olmayan yararlar m. 245/1 kapsamına girmez.

<sup>33</sup> “Mağdurların sahip oldukları kredi kartlarının kendi başvuruları sonucu üretildiği ve teslim olunduğu mağdur beyanlarından anlaşılmakta ise de, sanıkların tespit edilemeyen şekilde kart bilgilerini ele geçirerek kullandıkları sabit olup, kart kullanımı için fiziksel varlık gerekmiyip bilgilerin kullanılması halinde de eylem mağdur sayısınınca TCK'nın 245/1. maddesindeki suçu oluşturacağı gözetilmeden suça konu kartların üretiminde sanıkların iştiraki olmadığından bahisle suç vasfında yanılıgı sonucu yazılı şekilde hüküm kurulması”, 8. CD, 27.06.2016, E. 2016/1579, K. 2016/8464; “Başkasına ait kredi kartının kötüye kullanılması suretiyle yarar sağlama suçunun oluşabilmesi için 5464 sayılı Yasanın 3. maddesi uyarınca kartın fiziken kullanılmasını gerekmiyip kart bilgilerinin kullanılması yeterli olduğu cihetle, sanığın müşteriye ait kredi kart bilgileriyle değişik zaman ve yerlerde alışveriş yapmasından ibaret eylemlerinin banka ve kredi kartlarının kötüye kullanılması suçunu oluşturduğu ve TCK'nın 245/1, 43. Madde ve fıkraları gereğince cezalandırılmaları gerektiği gözetilmeden, suç nitelenmesinde yanılıgı ile hırsızlık suçunu oluşturduğundan bahisle yazılı şekilde hüküm kurulması”, 8. CD, 24.02.2016, E. 2015/11830, K. 2016/2167. “Sanığın, katılan ...'in ele geçirdiği kart bilgilerini kullanarak alışverişler yapması şeklinde gerçekleşen eyleminin küll halinde, TCK.nun 245/1. maddesindeki suçları oluşturacağı gözetilmeden”, 8. CD, 19.11.2018, E. 2017/24012, K. 2018/12886. Aynı yönde 8. CD, 05.03.2017, E. 2018/333, K. 2018/2385.

<sup>34</sup> Yararın bu suretle elde edilmediği olaylarda suç oluşmayacaktır: “Şikayetçinin para çekmek için gittiği ATM'de kartıyla işlem yaptığı sırada sanığın yardım bahanesiyle şikayetçinin yanına geldiği, işlemi devralarak ATM'den müşterinin istediği parayı ve kartı şikayetçiye verip sonrasında çekmiş olduğu parayı el çabukluğuyla aldığı, şikayetçinin kartla birlikte ATM'den ayrıldığı anlaşılma; sanığın, şikayetçinin kartını alıp kullanmaya yönelik hareketi bulunmayıp hedefinin sadece ATM'deki paraya yönelik olduğu, menkul mal niteliğinde olan paranın zilyedinin rızası dışında alıkonulması sebebiyle eylemin hırsızlık suçunu oluşturacağı gözetilmeden, uygulama alanı bulunmayan TCK.nun 245/1. madde ve fıkrasında tanımlanan banka veya kredi kartlarının kötüye kullanılması suçundan mahkumiyetine hükmedilmesi hatalıdır.”, 8. CD, 21.4.2016, E. 2016/1437, K. 2016/5453.

<sup>35</sup> Özbek, s. 1034; Özbek/Doğan/Bacaksız/Tepe, s. 1009, 1010; Koca/Üzülmez, s. 896; Tezcan/Erdem/Önok, s. 1057, 1058.

## 2. Manevi Unsur

Kasten işlenen bir suçtur. Taksirle işlenmesi söz konusu değildir. Kastın suçun kanuni tanımında yer alan unsurları kapsamı gerekir. Bu çerçevede failin kullandığı veya kullandırttığı şeyin banka veya kredi kartı olduğunu, başkasına ait olduğunu, bu kişinin rızasının bulunmadığını, kartın kullanılması suretiyle kendisine veya başkasına yarar sağladığını bilmelidir. Rızasının bulunması kast kapsamına dahil olduğundan suç doğrudan kastla işlenebilir<sup>36</sup>.

## 3. Hukuka Aykırılık

Rıza dışında (rıza tipiklik içinde düzenlendiğinden) diğer hukuka uygunluk nedenleri bu suçta gerçekleşebilir<sup>37</sup>. Örneğin velayet veya vesayet hakkı nedeniyle mallar üzerinde tasarruf yetkisi bulunan kişinin ATM'den para çekmesi sahip olduğu hakkın sınırları içinde kalmak şartıyla hukuka aykırılık teşkil etmez.

## C. TEŞEBBÜS

Başkasına ait banka veya kredi kartıyla yarar sağlamak suçunun tamamlanması için yarar sağlamak gerektiği için failin elinde olmayan nedenlerle yararı sağlayamadığı hallerde suç teşebbüs halinde kalmıştır. Fail kartı kullanmak için hareket etmesine rağmen yine elinde olmayan nedenlerle hareketini tamamlayamazsa suç yine teşebbüs aşamasında kalmıştır. Örneğin şifrenin yanlış girilmesi veya cihazın kartı alıkoymasına nedeniyle<sup>38</sup> veya ATM'den para çekerken failin yakalanması gibi durumlarda suç teşebbüs aşamasında kalmıştır.

Kart ele geçirilmekle birlikte kullanılmasına başlanmamışsa (kullandırılan kişi açısından da kullanmaya başlaması), örneğin ele geçirilen kart düşürülmüş veya kaybedilmişse m. 245/1'de düzenlenen suçun icra hareketleri başlamadığı için cezalandırma söz konusu olmayacaktır<sup>39</sup>. Bu

---

<sup>36</sup> Olası kastla işlenebileceğine ilişkin olarak bkz.: **Özbek**, s. 1035.

<sup>37</sup> **Koca/Üzülmez**, s. 897. Aksi görüş **Özbek/Doğan/Bacaksız/Tepe**, s. 1010. Hakkın kullanılmasının hukuka uygunluk nedeni olmadığına ilişkin olarak bkz.: **Tezcan/Erdem/Önok**, s. 1059.

<sup>38</sup> “müştekinin daha önceden sanığa işle ilgili olarak alışveriş yapması için verdiği bankamatik kartını sanığın müştekiye geri vermeyerek para çekmek amacıyla bu bankamatik kartını kullanarak hesaba bağlı telefon numarası ile bu kartın şifresini değiştirdiği/müştekinin müdahale etmesi sonucu kartın iptal edilerek atm cihazı tarafından kartın alıkonulduğu ve sanığın para çekemediği - eylemin bir bütün halinde banka kartlarının kötüye kullanılmasına teşebbüs suçunu oluşturacağı”, 13. CD, 1.6.2016, E. 2015/6014, K. 2016/10363.

<sup>39</sup> **Özbek/Doğan/Bacaksız/Tepe**, s. 1015; **Koca/Üzülmez**, s. 898; **Okuyucu Ergün**, s. 1071; **Özbek**, s. 1031; “Banka kartı henüz sanıkların hakimiyet alanına girmeden şikayetçi tarafından geri alınması nedeniyle kartın henüz ilgilinin rızasına aykırı olarak kullanılmasına veya kullandırılmasına yönelik davranışlarda bulunmadığından, TCK'nın 245/1. maddesindeki banka veya kredi kartlarının kötüye kullanılması suçunun icrai hareketlerine başlanmadığı ve bu suçun yalnızca hazırlık hareketleri gerçekleştirildiği görülmektedir. Ancak o ana kadar gerçekleşen ve banka veya kredi kartlarının kötüye kullanılması suçunu henüz oluşturmayan eylemin, hırsızlık suç tipine uyduğu ve tamamlanamaması nedeniyle teşebbüs aşamasında kaldığı kabul edilmelidir”, CGK.04.03.2014 gün ve 1439-104, **İlhan ve Diğerleri**, s. 837.

durumda yalnızca bağımsız suç teşkil eden ele geçirilmeden ceza verilecektir<sup>40</sup>.

Suçun icrasına elverişli hareketlerle başlanmaması durumunda teşebbüs söz konusu olmayacaktır. Yargıtay bir kararında çalıntı ihbarı üzerine iptal edilen kartın bankamatikte kullanılmaya çalışılırken ATM’de el konulduğu olayla ilgili olarak işlenemez suçun bulunduğunu kabul etmiştir<sup>41</sup>.

## D. İŞTİRAK

İştirakin ve iştirak şekillerinin gerçekleşmesi mümkündür. İştirake ilişkin TCK’nın 37 vd. maddeleri çerçevesinde değerlendirme yapılacaktır.

Ele geçirmenin bağımsız suç teşkil ettiği durumlarda bu suçun ve m. 245/1’in işlenmesine katılan kişiler iştirak kuralları gereğince her iki suçtan da sorumlu olacaktır. Ancak yalnızca fiillerden birine katılmışsa, diğerine manevi de olsa katkı sağlamamışsa herkes kendi fiili çerçevesinde sorumlu tutulacaktır.

## E. İÇTİMA

Başkasına ait banka veya kredi kartıyla yarar sağlamak suçu zincirleme suç şeklinde işlenebilir<sup>42</sup>.

---

<sup>40</sup> Koca/Üzülmez, s. 898. Yargıtay’a göre, “sanıkların ATM’den işlem yapmak isteyen mağdura yardım edeceklerinden bahisle kredi kartını alıp işlem yaptıktan sonra para olmadığını söyleyerek mağdurun kartı yerine başka bir kart vermeleri eyleminin TCK.nun 141/1. maddesinde düzenlenen hırsızlık suçunu oluşturduğu gözetilmelidir”, 8. CD, 28.4.2017, E. 2016/4520, K. 2017/4723.

<sup>41</sup> 8.CD, 27.03.2018, E. 2018/1757, K. 2018/3390; 8. CD, 04.10.2017, E. 2017/7700, K. 2017/10852.

<sup>42</sup> “5237 Sayılı TCK.nun 245/1. madde ve fıkrasında düzenlenen başkasına ait banka veya kredi kartını kötüye kullanmak suçunun mağduru kart sahibi olan gerçek ya da tüzel kişiler olduğu, aynı kişiye ait birden fazla banka veya kredi kartının değişik tarih ve zamanlarda kullanılması halinde, kart sayısına göre bağımsız ayrı suçlardan bahsedilemeyeceği, kart ve kullanım sayısı ile yarar miktarına göre TCK.nun 3 ve 61. maddeleri uyarınca temel ceza ile zincirleme suç hükümleri sebebiyle cezada yapılacak artırım oranının değerlendirilmesi gerektiği gözetilerek, somut olayda; sanıkların, aynı banka tarafından mağdura tahsis edilen iki bankamatik kartı ile değişik zamanlarda para çekme ve harcama yapma şeklindeki eylemlerinin TCK.nun 245/1, 43. maddelerine uyan tek suç oluşturacağı gözetilmeden, sanıklar hakkında yazılı şekilde iki ayrı suçtan hüküm kurulması”, 8. CD, 25.01.2016, E. 2015/9775, K. 2016/949, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.01.2017); “Sanık, katılanın kendisine ait işyerine alışveriş yapması için rızasıyla verdiği kredi kartıyla değişik zamanlarda kendisi için birden fazla nakit çekme ve nakit çekmeye teşebbüs etmiştir. Kartın birden fazla kullanılması sebebiyle banka veya kredi kartlarının kötüye kullanılması suçu sebebiyle verilecek cezadan zincirleme suç hükümleri uyarınca artırım yapılması gerekir”, 8. CD, 10.03.2015, E. 2014/28835, K. 2015/13337, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.01.2017). Yargıtay zincirleme suçta tek suçun oluştuğunu kabul etmekle birlikte, biz zincirleme suçta birden fazla suçun gerçekleştiğini kabul ettiğimizden bu görüşü kabul etmiyoruz.

Yargıtay, kartın kısa zaman aralıkları içinde kullanılması durumunda zincirleme suçun uygulanmayacağını, tek fiil bulunduğunu kabul etmektedir<sup>43</sup>.

Banka veya kredi kartının çalıandıktan sonra bankamatikte kullanılması durumunda m. 245/1'in özellikle hırsızlık suçuyla olan ilişkisi oldukça tartışmalıdır. 5237 sayılı Kanunun 245/1. maddesinde yer verilen "her ne suretle olursa olsun" ibaresi yaşanan tartışmada rol oynamaktadır. Kartın ele geçirilmesinin hırsızlık, dolandırıcılık, güveni kötüye kullanma, yağma gibi başka suçları oluşturup oluşturmayacağı üzerinde durulmaktadır. Bazı yazarlar, kartın ele geçirilmesi ile başkasına ait banka veya kredi kartıyla yarar sağlamak suçu arasında tüketen-tüketilen norm ilişkisi olduğunu, yalnızca banka veya kredi kartıyla yarar sağlamak suçundan cezalandırılması gerektiğini belirtmektedirler<sup>44</sup>. Bazı yazarlar, m. 245/1 için kartın ne şekilde ele geçirildiğinin bir önemi olmadığını, hırsızlık suçunun başkasına ait banka veya kredi kartıyla yarar sağlamak suçunun unsuru konumunda olduğunu, ayrıca ceza verilemeyeceğini ifade etmektedirler. Ayrıca bu yazarlar kartın ele geçirilmesi için işlenen suç (hırsızlık, dolandırıcılık gibi) ile m. 245/1 arasında fikri içtima ilişkisinin de uygulanacağını belirtmektedirler<sup>45</sup>. Bazı yazarlar ise, fıkra da geçen her ne olursa olsun ele geçiren veya elinde bulduran ifadesiyle, herhangi bir suç işlenmek suretiyle ele geçirilen kartlar kastedildiği gibi, herhangi bir suç işlemeksizin mağdurun rızasıyla verdiği kartın buldurulmasının da girdiğini, açıkça suç ismi zikredilmediği için bileşik suçun bulunmadığını, bu nedenle kartı ele geçirmek için işlenen suçtan ve m. 245/1'den ayrı ayrı ceza vermek gerektiğini kabul etmektedirler<sup>46</sup>. Yargıtay da bu son görüş çerçevesinde değerlendirme yapmakta ve banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi durumunda oluşabilecek hırsızlık, yağma<sup>47</sup>,

---

<sup>43</sup> "sanığın aynı kişiye ait farklı bankalardan verilmiş iki adet kredi kartı ile aynı gün aynı ATM'den çok kısa zaman aralıklarıyla para çekmesinden ibaret eyleminde "değişik zamanlarda" koşulu gerçekleşmediğinden TCK.nun 43. maddesinin uygulanma olanağının bulunmadığı gözetilmeden yazılı şekilde hüküm kurulması, Yasaya aykırı, sanığın temyiz itirazları bu itibarla yerinde görülmüş olduğundan", 8. CD, 11.10.2018, E. 2018/5960, K. 2018/10773. Aynı kartın biri saat 15.48, diğeri 15.51'de olmak üzere iki alışveriş yapılan olayda zincirleme suçun uygulanmasını hukuka aykırı görmüş (11. CD, 03.11.2008, E. 2008/13771, K. 2008/11018, Özbek/Doğan/Bacaksız/Tepe, s. 982), aynı kişiye ait birden fazla banka veya kredi kartının değişik tarih ve zamanlarda kullanılması halinde, kart ve kullanım sayısı ile yarar miktarına göre TCK.nun 3 ve 61. maddeleri uyarınca temel ceza ile zincirleme suç hükümleri sebebiyle cezada yapılacak artırım oranının değerlendirilmesi gerektiğini belirtmiştir (8. CD, 25.01.2016, E. 2015/9775, K. 2016/949, www.kazanci.com.tr (E.T.23.01.2017).

<sup>44</sup> Tezcan/Erdem/Önok, s. 1063.

<sup>45</sup> Karagülmez, s. 203 vd.

<sup>46</sup> Özbek, s. 1043; Özbek/Doğan/Bacaksız/Tepe, s. 1017, 1018; Koca/Üzülmez, s. 900-902; Okuyucu Ergün, s. 1074; Taner, Fahri Gökçen, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu Bir Bileşik Suç mudur?", AÜHFD, 2007, C. 56, S. 2, s. 80.

<sup>47</sup> "Yakındanan yağmaladıkları ve zorla şifrelerini söyledikleri üç ayrı bankaya ait kredi kartlarını, iki gün içerisinde kullanarak bankomatlardan para çeken ve alışveriş yaparak kendilerine haksız yarar sağlayan sanıkların eylemlerinin, yağma suçundan ayrı olarak şikayetçinin farklı bankalara ait krdi kartlarını hukuka aykırı kullanması ayrı ayrı 5237 sayılı TCK'nın 245/1. maddesinde öngörülen banka ve kredi kartlarının kötüye kullanılması suçlarını da oluşturduğu

güveni kötüye kullanma, dolandırıcılık gibi suçlar ile banka veya kredi kartlarıyla yarar sağlamak suçu arasında gerçek içtimanın uygulanması ve failin her bir suçtan ayrı ayrı cezalandırılması gerektiğini kabul etmektedir<sup>48</sup>. Biz de kanunda ifade edilen her ne suretle ele geçirilirse geçirilsin ibaresinden yola çıkarak, hukuka aykırı veya hukuka uygun ele geçirilmesi önemli olmaksızın bu kartların kullanılarak veya kullandırılarak yarar sağlanması durumunda m. 245/1'in uygulanacağını, ayrıca kartın ele geçirilmesi suç teşkil ediyorsa bundan da ceza verilmesi gerektiğini benimsiyoruz. Ancak bu durumda belirtilmelidir ki cezanın miktarı önemli boyutlara ulaşmaktadır. Örneğin arakadaşının kredi kartını yurttaki dolabından çalan kişinin ayrıca bu kartı kullanarak 1000 TL çekmesi durumunda hırsızlıktan beş yıldan on yıla kadar hapis (TCK m. 142/2-h) ve TCK m. 245/1'den üç yıldan altı yıla kadar hapis cezası ile cezalandırılacaktır.

Yargıtay, kart numarasının ve şifrenin hile ile ele geçirilip internet ortamında kullanılarak yarar sağlanması olayının küll halinde m. 245/1 kapsamında olduğunu kabul etmektedir<sup>49</sup>. Küll halinde m. 245/1'in oluştuğunun kabulünün doğru olmadığını düşünüyoruz. Zira kartın rıza dışında alınmasında hırsızlığın ve kartın kullanılması durumunda da m. 245/1'in uygulanmasını kabul eden Yargıtay'ın, kart bilgilerinin ele geçirilerek yarar sağlanmasında ise yalnızca m. 245'den hüküm kurması adil olmayan sonuç doğurmaktadır. Kişisel verilerin ele geçirilmesi suçu açısından ayrıca değerlendirme yapılması gerekmektedir. Yargıtay, daha önce ele geçirdikleri internet bankacılık şifresinin kullanılarak başkasının hesabından kendi hesabına havale yapan kişilerin eylemiyle ilgili olarak da değerlendirme yapmamış, TCK m. 142/2-e'den sorumluluk tayin edilmesi gerektiğini kabul etmiştir<sup>50</sup>. Dolayısıyla Yargıtay'ın uygulamasının aynı olduğu söylenebilir. Daha önce de

---

*ve bu suçlardan da mahkumiyetlerine karar verilmesi gerektiği gözetilmeden, nitelendirmede yanlıya düşülerek yazılı gerekçe ile beraatlerine hükmedilmesi"*, 8. CD, 09.03.2009, E. 2008/10669, K. 2009/4966.

<sup>48</sup> CGK,04.03.2014, E. 2012/11-1439, K. 2014/104, **Gül**, s. 171.

<sup>49</sup> "Sanığın, katılan ...'in ele geçirdiği kart bilgilerinin kullanarak alışverişler yapması şeklinde gerçekleşen eyleminin küll halinde, TCK'nun 245/1. maddesindeki suçları oluşturacağı gözetilmeden ayrıca aynı Yasanın 136. maddesiyle de hüküm kurulması, yasaya aykırı, sanığın temyiz itirazları bu itibarla yerinde görülmesi olduğundan hükmün bu sebepten dolayı", 8. CD, 19.11.2018, E. 2017/24012, K. 2018/12886. "müdahili telefonla arayıp bir bankadan aradığını ve banka görevlisi olduğunu, kredi kartından çekilen kart ücretinin iadesi için kart bilgilerinin gerektiğini söyleyen ve müdahilden bu şekilde temin ettiği kart numarası, son kullanma tarihi ve güvenlik numarası bilgilerini mail order sistemiyle kullanarak bir mağazadan alışveriş yapan sanığın eyleminin bir bütün olarak banka ve kredi kartlarının kötüye kullanılması suçunu oluşturduğunu gözetilerek 5237 sayılı TCK'nın 245/1. madde ve fıkrası uyarınca cezalandırılması ile yetinilmesi gerekirken yazılı şekilde iki ayrı suç olarak kabulüyle ayrıca dolandırıcılık suçundan da hüküm kurulması yasaya aykırı olup hükmün bu nedenle bozulması gerekmektedir", 8. CD, 13.06.2012, E. 2012/11116, K. 2012/20386, **Gül**, s. 137.

<sup>50</sup> CGK, 17.11.2009, E. 2009/11-193, K. 2009/268, www.kazanci.com (E.T. 12.12.2016). Aynı yönde "İnternet ortamında tanıştığı sanığın, kendisini avukat olarak tanıtp güven duygusu verdiği katılanı telefon ile arayarak Akbank ve Halk Bankası'ndaki hesap bilgilerinin alıp internet ortamında EFT'ler yaparak Yapı Kredi Bankası Kırıkkale Şubesindeki hesabına 19.06.2012 ve 20.06.2012 tarihlerinde toplamda 10.800 TL para yatırıldığı, bu paranın büyük bir çoğunluğunun sanık tarafından çekildiği, kalan kısmını çekmeye gittiğinde polislerce yakalandığından bahisle açılan davada; sanık, tanıştığı bir şahsın hesabının icralık olması nedeniyle kullanmadığını, havaleler geldiğinde

belirtildiği gibi her iki örnek karşılaştırıldığında faile birinde 3 yıldan altı yıla kadar hapis cezası, diğerinde beş yıldan on yıla kadar hapis cezası uygulanmaktadır.

Türk Ceza Kanununun 245/1. maddesinde düzenlenen başkasına ait banka veya kredi kartıyla yarar sağlamak suçu TCK m. 244/4'de yer alan suça göre özel düzenlemedir. Şartları gerçekleşmişse m. 245/1, aksi durumda bilişim sisteminin kullanılarak yarar sağlanmasında m. 244/4 uygulanacaktır. Ayrıca TCK. m. 244/4'deki başka suç oluşturmaması ibaresi nedeniyle m. 245/1 asli norm niteliği taşımaktadır<sup>51</sup>.

## F. ŞAHSİ CEZASIZLIK SEBEBİ

Ceza Kanunumuzun 245. maddesinin 4. fıkrasında başkasına ait banka veya kredi kartıyla yarar sağlamak suçuyla ilgili şahsi cezasızlık sebebine yer verilmiştir. TCK m. 245/4. fıkarda, *“Birinci fıkrada yer alan suçun; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz”* şeklinde düzenleme yapılmıştır. Düzenleme belirtilen akrabalık ilişkisinin bulunması halinde kişiye ceza verilmeyeceğini düzenleyerek şahsi cezasızlık nedeninin

---

*borçları nedeniyle el konulacağını, bu nedenle bir hesap numarasına ihtiyaç duyduğunu ve karşılığında ücret ödeyeceğini söylemesi üzerine Yapı Kredi Bankası'ndaki hesap numarasını ve kartını verdiğini, bankadan 6000 lira çekip bu kişiye verdiğini, daha sonra kartını istediğini, oyaladığını, daha sonra hesabını kontrol için gittiğinde hesabında bloke olduğundan bahisle banka yetkililerinin polis çağırıp yakalattığını, havalelerin ne şekilde geldiğini bilmediğini, suçla ilgisi olmadığını savunması karşısında, katıldan internette tanıştığı şahısla görüntülü, sesli ve yüzyüze görüşmeler yapıp yapmadığı sorulup, yapmışsa sanıkla yüzleştirilmesi, yapmamışsa katılanın suç tarihindeki MSN kayıtlarının ilgili şirketten istenmesi, katılanın internette görüştüğü kişi tarafından arandığı anlaşılan telefon hattının Hasan Özçelik adına olduğu, bununla ilgili HTS raporu istendiği ancak CD olarak gönderilen raporun çözümlenmesinin yapılmadığı ve hat sahibinin dinlenmediği anlaşılacakla CD şeklindeki HTS raporunun çözümlenmesinin yapılması, raporda görüşme veya para çekme sırasında bulunduğu baz istasyonlarının da belirlenmesi, hat sahibinin CMK.nun 48. maddesi uyarınca tanık sıfatıyla dinlenmesi, kabul etmediği takdirde hatta ilişkin sözleşme ve eki belgeler getirtilip, ekinde resimli belge bulunduğu takdirde sanık ve katıldan sorulması, sözleşme ve eki belgelerinde bulunan yazı, rakam ile imza yönünden hat sahibi ve sanık açısından inceleme yapılması, bankalarda EFT'ler sırasında kullanılan IP numaraları getirtilip hangi hatta bağlı olduğunun saptanması, Yapı Kredi Bankası'nın yazı cevabında 6000 liranın bankadan çekildiği, diğer miktarların ATM'lerden çekildiğinin bildirildiği, ancak hesap hareketlerinde, şubeden para çekiminin görülmediği, gelen EFT'lerin kuyumcularda yapılan alışverişlerde harcandığı görülmekle, ilgili kuyumculardan alışverişlere ait belgelerin istenmesi, sliplerde imza olduğu takdirde imza incelemesi yaptırılması, kuyumcuların tanık sıfatıyla dinlenmeleri, Yapı Kredi Bankası'ndan 6000 liranın çekildiğine dair dekontun istenmesi, üzerindeki imzanın da incelenmesi, sanığın hesabında başka EFT'ler de görülmekle hakkında benzer soruşturmalar olup olmadığı araştırılıp sübutu halinde eylemin TCK.nun 142/2-e maddesi kapsamında değerlendirilmesi gerektiği dikkate alınarak sonucuna göre hukuki durumunun tayin ve takdiri gerekirken eksik inceleme ile yazılı şekilde hüküm kurulması, yasaya aykırıdır”*, 8, CD, 15.02.2017, E. 2015/13216, K. 2017/1393.

<sup>51</sup> Koca/Üzülmöz, s. 903.



ceza verilmesini engelleyen nitelikte olduğunu ifade etmiştir. Cezada indirim yapılmasını gerektiren şahsi cezasızlık nedenine m. 245/4'te yer verilmemiştir<sup>52</sup>.

Hükmün uygulanması nedenlerinden biri haklarında ayrılık kararı verilmemiş eşlerden birinin zararına işlenmesidir. Bu neden için TMK hükümlerine göre eşler hakkında mahkemece ayrılık kararının verilmemiş olması, evliliğin devam ediyor olması gerekir. Dolayısıyla hüküm evliliği sorunsuz devam eden eşler için uygulanabileceği gibi, sorun nedeniyle boşanma davası devam eden, ancak ayrılık kararı verilmeyen eşler için de ve henüz boşanma davası açılmamış ancak ayrı yaşayan eşler (ayrılık kararı verilmemiş) için de uygulanabilecektir. Evlilik resmi evlilik olarak kabul edildiğinden birlikte yaşam veya imam nikahlı birliktelik hükmün uygulama alanının dışında kalmaktadır. Fiilin işlendiği sırada ayrılık kararının verilmemiş olması gerekir. Sonradan verilmiş olması veya fiilin işlenmesinden sonra evliliğin gerçekleşmesi önemli değildir<sup>53</sup>.

Hükmün uygulanması nedenlerinden diğeri, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın zararına işlenmesidir. Altsoy ve üst soyun veya bu derecedeki kayın hısımlığının uzaklığı önemli değildir. Torunun torunu da fiili işlediğinde şahsi cezasızlık nedeni uygulanacaktır. Kayın akrabalık açısından fiilin işlendiği esnada evliliğin devam devam edip etmemesi gerektiği doktrinde tartışmalıdır<sup>54</sup>. Evlat edinen ilişkisi kanunla kurulmuş akrabalık ilişkisidir. Bunlardan biri diğerrinin zararına m. 245/1. maddedeki suç işlediğinde şahsi cezasızlık nedeninden yararlanacaktır.

Hükmün uygulanma nedenlerinden sonuncusu aynı konutta beraber yaşayan kardeşlerden birinin zararına işlenmesidir. Aynı konutta yaşıyor olmak şartıyla aynı anne babadan olmak gerekmemektedir. Ebeveynlerin daha önceki evliliklerden olan çocukların da aynı konutta yaşıyor olmak şartıyla kardeş kapsamına girdiği belirtilmektedir<sup>55</sup>.

Fiilin işlendiği esnada böyle bir neden varsa suç işleyen kişi bilmese bile uygulanır. Örneğin annesi olduğunu bilmeden banka kartını kullanarak para çeken kişi hakkında 4. fıkra

---

<sup>52</sup> Diğer gerekçelerin yanında ceza da indirim yapılmasının gerektiren şahsi cezasızlık nedenine ilişkin olarak da Anayasa Mahkemesine başvurulmuş, ancak Anayasa Mahkemesi itirazı yerinde görmemiştir. Zira cezada indirim yapılmasını gerektiren bir neden ceza siyasetine bağlı olarak yasa koyucunun takdirindedir. Bkz.: Anayasa Mahkemesi Kararı, 05.03.2009, E. 2006/123, K. 2009/43, R.G.S. 27246, 2 Haziran 2009, <http://www.resmigazete.gov.tr/eskiler/2009/06/20090602-9.htm> (E.T.02.02.2017).

<sup>53</sup> Bkz.: **Tezcan/Erdem/Önok**, s. 855.

<sup>54</sup> Bazı yazarlar evliliğin devam etmesi gerektiğini ararken (**Dönmezer, Sulhi**, Kişilere ve Mala Karşı Cürümler, 16. Bası, İstanbul 2001, s. 610), bazı yazarlar evlilik sona erse bile şahsi cezasızlık nedeninin uygulanacağını kabul etmektedirler (**Tezcan/Erdem/Önok**, s. 855).

<sup>55</sup> **Tezcan/Erdem/Önok**, s. 856.

hükmü uygulanacaktır. Şahsi cezasızlık sebebinde düşülen hata failin ceza sorumluluğunu etkilememektedir.

### G. ETKİN PİŞMANLIK

Türk Ceza Kanununun 245. maddesinin 5. fıkrasında, başkasına ait banka veya kredi kartıyla yarar sağlamak suçuna ilişkin etkin pişmanlık hükmüne yer verilmiştir. Bu fıkra göre “Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır”. Hükümle TCK m. 168’e yollama yapılarak bu hükmün uygulanması kabul edilmiştir<sup>56</sup>.

TCK m. 168 gereğince, başkasına ait banka veya kredi kartlarıyla yarar sağlamak suçu tamamlandıktan sonra ve fakat bu nedenle hakkında kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde, verilecek ceza üçte ikisine kadar indirilecektir. Etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi halinde, verilecek cezanın yarısına kadar indirilecektir. Kısmen geri verme veya tazmin halinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranması gerekmektedir. Etkin pişmanlık hükmü cezanın indirilmesini sağlamaktadır. Ceza verilmesini engelleyen bir neden değildir<sup>57</sup>.

### H. YAPTIRIM

Başkasına ait banka veya kredi kartıyla yarar sağlamak suçunun cezası üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasıdır<sup>58</sup>. Kanun koyucu TCK m. 245/1’de yarar

---

<sup>56</sup> Bu hüküm 6 Aralık 2006’da maddeye eklenmiştir. Hükümde etkin pişmanlık hükmüne yer verilmemesi diğer gerekçelerle birlikte Anayasaya aykırık nedeniyle Anayasa Mahkemesine götürülmüşse de, Anayasa Mahkemesi tarafından karar verilmeden önce kanun koyucu tarafından maddeye eklenmiş, Anayasa Mahkemesi de 2009 yılında verdiği kararda etkin pişmanlık itirazını redetmiştir: Anayasa Mahkemesi Kararı, 05.03.2009, E. 2006/123, K. 2009/43, R.G.S. 27246, 2 Haziran 2009, <http://www.resmigazete.gov.tr/eskiler/2009/06/20090602-9.htm> (E.T.02.02.2017).

<sup>57</sup> Kısmi ödeme halinde de etkin pişmanlık hükümleri mağdurun rızasıyla uygulanabilecektir. Yargıtay da verdiği bir kararda etkin pişmanlık hükümlerinin değerlendirilmesini istemiştir: “Sanık tarafından katılana ait kredi kartı hesabına, yapılan harcamaların bir süre düzenli olarak ödenmesi ve bu ödemelerin banka tarafından gönderilen ekstrelerde de yer alması karşısında sanığın soruşturma aşamasında kısmi ödemede/iadede bulunduğu anlaşıldığından, katılandan kısmi ödeme sebebiyle etkin pişmanlık hükmünün uygulanmasına rızası olup olmadığı sorulup sonucuna göre sanık hakkında etkin pişmanlık hükümlerinin uygulanıp uygulanmayacağı tartışılarak sanığın hukuki durumunun takdir ve tayini gerektiği gözetilmeden, eksik incelemeyle yazılı şekilde hüküm kurulması”nın yasaya aykırılık oluşturduğunu belirtmiştir: 8. CD, 19.06.2014, E. 2014/14750, K. 2014/15689, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.15.02.2017).

<sup>58</sup> Türk Ceza Kanununun m. 245/1’de öngörülen ceza miktarı için Anayasa Mahkemesine müracaat edilmiştir. Başvuruda m. 245/1’de öngörülen ceza miktarının aynı kanunda benzer eylemler için düzenlenen hükümlerde öngörülen cezalarla karşılaştırıldığında Anayasaya aykırı olduğu belirtilmiştir. Zira kanunda m. 245/1 için 3 yıldan 6 yıla kadar bir hapis cezası öngörülürken, bir bilişim sisteminin işleyişini engellemek, bozmak suretiyle ya da verileri yok etmek, erişilmez kılmak ya da sisteme veri yerleştirmek suretiyle ve kendisi ya da başkasına yarar sağlamak şeklinde gerçekleşen eyleme 2 yıldan 6 yıla kadar hapis cezası öngörülmektedir (m. 244/4). Yine hırsızlığın vasıflı hali olan, kamu kuruluşlarından

sağlamak suretiyle ekonomik kazanç sağlandığından hapis cezasının yanında adli para cezasının verilmesini de öngörmüştür. Adli para cezasının üst sınırı belirtilmiş alt sınırı ifade edilmemiştir. Alt sınır TCK'nın 52. maddesi gereğince 5 gün olarak kabul edilecektir. TCK'nın 246. maddesi gereğince TCK'nın 245. maddesinin 1. fıkrasında yer alan suçun tüzel kişi yararına işlenmesi durumunda TCK'nın 60. maddesinde yer alan güvenlik tedbirleri uygulanacaktır.

## I. SORUŞTURMA VE KOVUŞTURMA

Resen takip edilen bir suçtur. Görevli mahkeme, Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanununun 11. ve 12. maddeleri gereğince asliye ceza mahkemesidir. Yetkili mahkeme ise CMK m. 12 gereğince suçun işlendiği yer mahkemesidir. Suçun işlendiği yer ise TCK m. 8'e göre belirlenecektir. Buna göre 245. maddenin 1. fıkrasında yer alan kullanma veya kullandırmanın gerçekleştirildiği yer ile yararın sağlandığı yer mahkemeleri yetkili mahkemedir. Fiil bankamatiklerin kullanılması ve POS cihaz yardımıyla işlendiği takdirde kullanma veya yararın sağlandığı yer çoğunlukla aynı yerdir. Ama internet üzerinden fiil işleniyorsa kişinin beden olarak bulunduğu yer ile hareketin açığa çıktığı yer de suçun işlendiği yer olacaktır. Suçun oluşması için yararın da sağlanması gerektiğinden sağlandığı yer de suçun işlendiği yer, dolayısıyla bu yerdeki mahkeme de yetkili mahkemedir. Ülke içinde işlenen suçlarda zincirleme suç veya teşebbüs söz konusuysa CMK m. 12/2 gereğince yetkili mahkeme belirlenecektir. Suç yabancı ülkede işlenmiş ve Türkiye'de yargılama yapılmasının mümkün olduğu hallerde yetkili mahkeme CMK m. 14 gereğince belirlenecektir. Olayda şahsi cezasızlık sebebi varsa Cumhuriyet savcısı takdir yetkisi çerçevesinde kamu davasını açmayabilecektir (CMK m. 171).

---

hırsızlık, bina dan, kilitli yerlerden, ulaşım araçlarından, açıkta bırakılmış eşya lar ile ilgili hırsızlık hallerinde bile ceza 2 yıldan 5 yıla kadar hapis cezasıdır. Bunun da m. 245/1'in sanıkları aleyhine bir eşitsizlik, demokratik toplumda olması gereken adil bir dengenin bulunmaması sonucunu doğurduğu belirtilerek Anayasanın 10 uncu maddesindeki eşitlik ve 2 nci maddesindeki demokratik hukuk devleti ilkelerine aykırı olduğu, demokratik bir toplumda uygun görülebilecek bir dengenin atılı suçun cezasında bulunmadığı sonucuna varıldığı belirtilerek Anayasa Mahkemesine başvurulmuştur. Anayasa Mahkemesi ise, banka ve kredi kartlarının hukuka aykırı olarak kullanılması suretiyle çıkar sağlayanlar hakkında üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası öngören kurala, Türk Ceza Kanununun bilişim alanında suçlara ilişkin bölümünde yer verildiğini, bundan, kartın bağlı bulunduğu hesap sahibinin malvarlığı yanında kişisel verilerinin de hukuki koruma kapsamında olduğunun anlaşıldığını, kurala korunmak istenen hukuki yarar, suçun niteliği ile öngörülen cezanın tür ve miktarı gözetildiğinde kuralda yer alan cezanın adaletsiz ve ölçüsüz olduğundan söz edilemeyeceğini belirterek kuralın Anayasaya aykırı olmadığına karar vermiştir: Anayasa Mahkemesi Kararı, 05.03.2009, E. 2006/123, K. 2009/43, R.G.S. 27246, 2 Haziran 2009, <http://www.resmigazete.gov.tr/eskiler/2009/06/20090602-9.htm> (E.T.02.02.2017).

### III. SAHTE BANKA VEYA KREDİ KARTI ÜRETMEK, SATMAK, DEVRETMEK, SATIN ALMAK VEYA KABUL ETMEK SUÇU

#### A. GENEL OLARAK

Türk Ceza Kanununun 245/2. maddesi teknolojik gelişmelerin ortaya çıkardığı imkanların, ödeme alanında yarattığı etkinin sonucudur. TCK'ya 08.07.2005 tarihli 5377 sayılı Kanunla eklenmiştir. 5237 sayılı Kanun yürürlüğe girmeden önce 5237 sayılı TCK'da ve 765 sayılı Kanunda böyle bir düzenleme bulunmamaktaydı. 765 sayılı TCK'da (m. 525/c) verilerde sahtekârlık suçu düzenlenmişti. Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tâbi tutan bir sisteme verileri veya diğer unsurları yerleştirmek veya var olan verileri, diğer unsurları tahrif etmek gerektiği için banka veya kredi kartlarında sahtecilikle ilgili fiillere bu hükmün uygulanma imkanı bulunmamaktaydı. Yargıtay kredi kartı ve onunla ilgili sahtecilikleri özel belgede sahtecilik olarak kabul ediyordu<sup>59</sup>. 5237 sayılı Kanunda verilerde sahteciliğin düzenlenmemesi ve banka veya kredi kartlarının, belgede sahtecilik suçu anlamında belge sayılmasının kanunilik ilkesine aykırılık oluşturması kanun koyucuyu düzenleme yapmaya yöneltmiştir<sup>60</sup>.

Ceza Kanunumuzda banka veya kredi kartlarıyla ilgili düzenleme yapılmakla beraber, ödeme yapmakta kullanılan diğer kartlarda sahtecilikle ilgili bir düzenleme bulunmamaktadır. Bunun bir eksiklik olduğu belirtilmelidir. Nitekim doktrinde TCK'da var olan mevcut düzenlemelerin (sahtecilik suçlarının, karşılıksız yararlanma suçunun) diğer kartlarda yapılan sahtecilikleri kapsamayacağı, ayrı bir düzenlemeye ihtiyaç bulunduğu belirtilmektedir<sup>61</sup>.

#### B. KORUNAN HUKUKİ DEĞER

Türk Ceza Kanununun 245/2. maddesinde düzenlenen suç, özel sahtecilik suçu niteliğinde bir fiildir<sup>62</sup>. Kamu güvenine karşı işlenen suç niteliği taşımaktadır. Kanun koyucu m. 245/2'de, başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmeyi, bunları satmayı, devretmeyi, satın almayı veya kabul etmeyi suç haline getirmiştir. Belirtilen fiiller sahte banka veya kredi kartı üretilmesi ve üretilen kartlarla ilgili bazı davranışları içermektedir. Bu nedenle Ceza Kanunumuzun 245/2. maddesinde düzenlenen sahte banka veya kredi kartı üretmek,

---

<sup>59</sup> Özbek/Doğan/Bacaksız/Tepe, s. 1020.

<sup>60</sup> Düzenlemenin nedeninin, banka veya kredi kartlarının, belgede sahtecilik suçu anlamında belge sayılmasının kanunilik ilkesine aykırılık oluşturacağı düşüncesi olduğuna ilişkin olarak bkz.: Tezcan/Erdem/Önok, s. 1058.

<sup>61</sup> Özbek/Doğan/Bacaksız/Tepe, s. 1020, dipnot 148.

<sup>62</sup> Soyaslan, s. 664; Koca/üzülmez, s. 905; Özbek/Doğan/Bacaksız/Tepe, s. 1020.

satmak, devretmek, satın almak veya kabul etmek suçuyla korunan hukuki değer, ödeme aracı olarak kullanılan banka veya kredi kartlarının işlerliği ve güvenilirliğidir<sup>63</sup>.

Kanun koyucu TCK m. 245/2'de düzenlenen suç ile sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartlarının kullanılması suretiyle yarar sağlama suçunun hazırlık hareketleri niteliğindeki fiilleri bağımsız suç haline getirmiştir<sup>64</sup>. Bu özelliği nedeniyle soyut tehlike suçu niteliği taşımaktadır. Belirtilen hareketlerin yapılması banka veya kredi kartlarının kullanıldığı ödeme ilişkileri açısından yüksek soyut tehlike oluşturmaktadır<sup>65</sup>.

### C. SUÇUN UNSURLARI

#### 1. Maddi Unsur

##### -Fail ve Mağdur

Herhangi bir kişi suçun faili olabilir.

Fıkra da sayılan bazı fiiller çok failli suç niteliği taşımaktadır. Satmak-satın almak, devretmek-kabul etmek hareketlerinde, bir tarafta satan diğer tarafta satın alan, bir tarafta devreden diğer tarafta kabul eden kişi bulunmaktadır.

Suç, sahtecilik suçu niteliğinde olduğundan topluma karşı işlenen suçlardandır. Ayrıca bazı fiiller açısından TCK m. 245/2'nin çok failli suç olduğu gözden uzak tutulmamalıdır<sup>66</sup>. Suçun oluşması için fıkra da belirtilen hareketlerin yapılması yeterli olup, sahte kartın kullanılması gerekmemektedir. Sahte olarak üretilen kartın kullanılması 3. fıkra da ayrı bir suç olarak düzenlenmiştir. Kullanılma aranmadığı için hesap sahibinin veya bankanın zarar görmesi gerekli değildir<sup>67</sup>.

Yargıtay da suçun mağdurunun banka veya finans kurumu olduğunu benimsemektedir. Aynı bankaya ait sahte kartların üretilmesi durumunda tek fiilin bulunduğunu kabul etmektedir<sup>68</sup>. Ancak

---

<sup>63</sup> Tröndle/Fischer, § 152 a, kn. 2; Sternberg-Lieben-Schönke/Schröder, 2010, § 152 a, kn. 1. Doktrinde bu suçla korunan hukuki değer konusunda, bazı yazarlar karma nitelikte olduğunu (Özbek, s. 1045; Özbek/Doğan/Bacaksız/Tepe, s. 1019), bazı yazarlar birden fazla yararın korunduğunu (Okuyucu-Ergün, s. 1067, 1076), bazı yazarlar ise kamunun bu kartların gerçek olduğuna yönelik güveni olduğunu belirtmektedirler (Koca/Üzülmez, s. 904).

<sup>64</sup> Koca/Üzülmez, s. 904.

<sup>65</sup> Bkz.: Tröndle/Fischer, § 152 a, kn. 2. TCK m. 245/2'de düzenlenen suçun neticesi harekete bitişik suç olduğuna ilişkin olarak bkz.: Özbek/Doğan/Bacaksız/Tepe, s. 1022.

<sup>66</sup> Bazı yazarlar, banka ya da finans kuruluşu yanında, sahte kartın ilişkilendirildiği banka hesabı sahibinin de suçun mağduru olduğunu belirtmektedirler (Özbek, s. 1046). Bazı yazarlar, suçun mağdurunun banka veya finans kurumu olduğunu kabul etmektedirler (Tezcan/Erdem/Önok, s. 1062; Özbek/Doğan/Bacaksız/Tepe, s. 1020; Okuyucu-Ergün, s. 1076; Gül, s. 150).

<sup>67</sup> Koca/Üzülmez, s. 905.

<sup>68</sup> "Başkasına ait banka hesabıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi TCK.nun 245/2. maddesinde; sahte banka veya kredi kartını kullanarak kendisine veya bir başkasına yarar sağlanması ise anılan maddenin 3. fıkrasında birbirinden bağımsız ve ayrı ayrı suçları

suçun kamu güvenine karşı işlenen suç niteliğinde olması nedeniyle Yargıtay'ın belirlemelerine katılmamaktayız.

#### -Konu

Türk Ceza Kanununun 245/2. maddesinde düzenlenen suçun konusu banka veya kredi kartlarıdır. Bu kartların başkalarına ait banka hesaplarıyla ilişkilendirilerek çıkarılmış sahte kartlar olması gerekir<sup>69</sup>. Başkalarının hesaplarıyla ilişkilendirilmeden sahte kartın üretilmesi veya bu kartların satılması, devredilmesi, satın alınması veya kabul edilmesi m. 245/2'i oluşturmayacaktır<sup>70</sup>. Bu durumda 2. fıkra anlamında sahte bir karttan söz edilemeyecektir<sup>71</sup>. Başkalarına ait hesapla ilişkili olmayan sahte banka veya kredi kartlarının kullanılarak bir kişinin aldatılması suretiyle yarar sağlanmasında dolandırıcılık suçu oluşacaktır<sup>72</sup>.

#### -Fîil

Suçun oluşturan hareketler banka veya kredi kartını *üretmek, satmak, devretmek, satın almak veya kabul etmek* olarak belirtilmiştir. Hareketler seçimlik olarak belirtildiğinden her hangi birinin yapılması suçun oluşması için yeterlidir<sup>73</sup>. Hareketlerden bir kaçının yapılması (örneğin hem üretip

---

*oluşturduğu, bankaya ait gerçek bir kredi kartının manyetik şerit bilgilerinin kopyalanarak sahte bir kredi kartı üretmesi ve bu kartı kullanmak suretiyle yarar sağlaması halinde suçtan zarar görenin ilgili banka olduğu, kartları gerçeğe aykırı olarak üretilen banka sayısınca TCK.nun 245/2. maddesiyle aynı bankanın birden fazla kartının değişik zamanlarda kopyalanması durumunda 43. maddesinin, sahte olarak üretilen kartların alışverişte kullanılması halinde ise, banka sayısınca TCK.nun 245/3. maddesiyle aynı bankaya ait birden fazla kart ile veya bir kart ile değişik zamanlarda para çekilmesi veya harcama yapılması halinde ise TCK.nun 43. maddesi uyarınca uygulama yapılması gerektiği, somut olayda da katılan... 'a ait gerçek kredi kartlarının manyetik şerit bilgilerinin kopyalanarak sahte kredi kartlarının üretilmesi ve bu kartları kullanmak suretiyle yarar sağlaması mahkemece gerekçeli kararda belirtildiği halde, eylemlerin küll halinde TCK.nun 245/3. maddesi kapsamındaki suçları oluşturacağı kabulüyle uygulama yapılması, yasaya aykırıdır": 8. CD, 10.02.2016, E. 2015/15546, K. 2016/1315, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.04.2016). Daha önceki bir kararında banka sayısınca suçun işlendiğini kabul etmekle beraber 43. maddenin uygulanması gerektiğini belirtmiştir: 8. CD, 21.05.2015, E. 2014/32263, K. 2015/17388, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.04.2016).*

<sup>69</sup> Belgede sahtecilik fiillerindeki kandırıcılık kabiliyeti kavramına benzediğine ilişkin olarak bkz.: **Özbek**, s. 1048.

<sup>70</sup> Başkalarının hesaplarıyla ilişkilendirilmeden üretilen banka veya kredi kartlarının veya bunlarla ilgili gerçekleştirilen diğer fiillerin özel belgede sahtecilik suçunun unsurlarını oluşturması halinde m. 207 gereğince cezalandırılabilceği belirtilmektedir. Bu görüşe göre suçun oluşması için bu banka veya kredi kartının kullanılması gerektiği, dolayısıyla da başkalarının hesaplarıyla ilişkili olmayan banka veya kredi kartını üretmenin suç teşkil etmeyeceği kabul edilmektedir: **Koca/Üzülmez**, s. 905.

<sup>71</sup> **Özbek/Doğan/Bacaksız/Tepe**, s. 1022.

<sup>72</sup> **Koca/Üzülmez**, s. 907.

<sup>73</sup> Fıkra da sayılan hareketler açısından doktrinde bazı eleştiriler yöneltilmektedir. Birinci eleştiri, sayılan hareketlerin aynı cezaıyla cezalandırılmasının doğru olmadığı yönündedir. Kartın sahte olarak üretilmesiyle bu kartın kabul edilmesinin aynı haksızlık içeriğine sahip olmadığı, bu nedenle sahte kartların satın alınması ve kabul edilmesinin parade sahtecilik veya kıymetli damgada sahtecilik suçunda olduğu gibi daha az cezalandırılması gerektiği belirtilmektedir (**Koca/Üzülmez**, s. 906 ve dipnot 172). Kanun koyucunun bazı fiillerde (TCK'nın m. 197/2, TCK m. 282/2) bu değerlendirmeyi yapması söz konusu olmakla birlikte bazı fiillerde (TCK m. 165, TCK m. 174/1, TCK m. 245/A) böyle bir tercihi bulunmamaktadır. İkinci eleştiri, bulundurma da cezalandırılan bir hareket olarak fıkra da yer alması yönündedir. Bu görüş, kabul etmenin bulundurmaya da içermekle birlikte kabul etmek kavramının çok geniş içeriğe sahip olması nedeniyle kanuniliğe uygun görünmediğini ifade etmektedirler. Üzerinde banka veya kredi kartı bulunan herkesin kabul etmekten dolayı sorumlu olacağını dile getirmektedirler. Bu görüşe göre ayrıca fıkra da üretmek

hem de satılması) durumunda konu aynı olmak şartıyla tek fiil ve tek suç söz konusu olacak, ancak hareketlerden bir kaçının yapılması temel cezanın belirlenmesinde dikkate alınacaktır.

Üretmek, banka veya kredi kartının tamamen sahte olarak oluşturulmasını ifade ettiği gibi, var olan bir banka veya kredi kartında değişiklik yapılarak bunun sahte kart haline dönüştürülmesini de karşılamaktadır<sup>74</sup>. Sahte olarak üretilen kartların banka veya kredi kartı olması gerekir. Sanal kartın oluşturulması durumunda da m. 245/2 oluşacaktır<sup>75</sup>.

Gerçeğe aykırı beyan ve belgelerle ilgili banka veya finans kurumuna başvurup kart çıkartılmasının m. 245/2 kapsamına girdiği Yargıtay tarafından kabul edilmektedir<sup>76</sup>. Yargıtay 5464

kelimesinden sonra bilerek kelimesi de eklenmelidir. Her iki kavramın ilave edilmesi suretiyle tesadüflerin cezalandırılmasının önlenilebileceği belirtilmektedir (Özbek/Doğan/Bacaksız/Tepe, s. 1022).

<sup>74</sup> Soyaslan, s. 664; Tezcan/Erdem/Önok, s. 1058. “Değişik bankalara ait kredi kartlarının manyetik şerit bilgilerini kopyalayarak elde ettikleri kart bilgileri ile üretilen sahte kartların bağlı oldukları bankalar sayısınca cezalandırılacağı, aynı bankanın birden fazla kartının değişik zamanlarda kopyalanması halinde 43. maddesinin uygulanacağı dikkate alınarak”, 8. CD, 22.10.2018, E. 2018/9086, K. 2018/11316.

<sup>75</sup> Aynı yönde Gül, s. 145.

<sup>76</sup> “Sahte oluşturulan nüfus cüzdanla kredi kartı başvurusu yapmak suretiyle sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi 5237 Sayılı T.C.K.nun 245/2. maddesinde, sahte banka veya kredi kartını kullanarak kendisine veya bir başkasına yarar sağlanması ise, anılan maddenin 3. fıkrasında düzenlenen birbirinden bağımsız ve ayrı ayrı suçları oluşturduğu cihetle; sanık M. Y.’in askerlik görevini ifa eden kayınbiraderi katılan M. Y. kimlik bilgilerine göre üzerinde sanık M. Y.’in resmi bulunan sahte bir nüfus cüzdanı düzenlettirip bu nüfus cüzdanıyla adına Denizbank’tan iki ayrı, hsbc Bank, Asya Katılım Bankası ve Finansbank’tan birer kredi kartı başvurusunda bulunup bu şekilde temin ettikleri toplam beş adet kredi kartını alıp kullandıklarından bahisle açılan davada, sanıklar T. B. H. Y.’in soruşturma safhasında “sanıklar M.’la T. Kocamustafapaşa’da ortak bir işyeri çalıştırmakta olup sanık M.’nin akrabası olması sebebiyle zaman zaman işyerlerine gidip gelen sanık H. Y., sanık M.’nin işyerinde olmadığı sırada, ortağı olan sanık T. bana bir zarfın içinden çıkardığı katılana ait kimlik bilgilerine göre düzenlenmiş ancak sanık M.’nin resmi yapışık olan bir nüfus cüzdanını gösterdiğini, “bu ne biçim nüfus cüzdanı” diye sorduğunda, sanık M.’nin bu nüfus cüzdanıyla muhtelif bankalara başvurup ve M. Y. adına kredi kartları aldığını ve kullandığını söylediği, bu sırada sanık M. Y.’in, sanık H.’ya bir bankadan 5000 TL kredi çektirip taksitlerini ödemediği, bu sebeple borcu olduğu, işyerlerine tekrar gittiğinde, ortağı sanık T. işyerindeydi, sohbet esnasında suça konu 5 adet kredi kartını vermek istediğini ve herhangi bir şey olursa tanıklık yapmasını söylediği, alacağını alamadığı için borcunu ödemezse bu kredi kartlarıyla hakkında şikayetçi olacağını söylemek ve kredi kartlarını koz olarak kullanmak düşüncesiyle sanık T.’ün verdiği 5 adet kredi kartını alıp evine götürdüğünü ve sakladığını, 16.9.2009 günü güvenlik görevlileri gelip olayı sorduklarında anlatıp ve kitapların altına sakladığı 5 adet kredi kartını teslim edildiğini”, mahkeme huzurunda ise katılana vermek üzere sanık T. B. tarafından sanık H. Y.’a verildiğine dair savunmaları ve aradaki çelişkilerin giderilmemesi, diğer sanık M. Y.’in ise suçu kabul etmeyip diğer sanıkların işlemiş olabileceğini savunması,

İlgili bankalardan Denizbank’tan gelen belgeler üzerinde imza yönünden yapılan inceleme sonucu alınan kriminal raporda; gerek katılan, gerekse sanıklara aidiyetinin saptanamadığının belirtilmesi, diğer bankaların belgeleri üzerinde inceleme yapılmaması, şikayetçi hsbc bankasının belgeleri gönderdiği belirtilmişse de dosyada rastlanmaması, gerek katılan Finansbank gerekse şikayetçi Denizbank’ın hesap ekstrelerinde kontür alımları olduğunun anlaşılması karşısında, öncelikle şikayetçi HSBC bankasının sahte olarak düzenlettirilip kullanıldığı iddia olunan kredi kartına dair sözleşme ve ekleriyle birlikte harcama belgelerinin de istenilip gerek sanıkların gerekse katılanın suç tarihinden önce resmi dairelerde mevcut bulunan imza ve yazı örnekleri getirilip tüm bankalara ait belgelerde inceleme yaptırılması, hesap ekstrelerinde görülen kontür alımı yapılan telefon numaralarının kimlere ait olduğu araştırılıp diğer alışveriş yerlerinin sahipleri de dinlenerek sonucuna göre sanıklar T. B. H. Y.’la birlikte katılan Finansbank’a yönelik atılı suçu fikir ve eylem birliğiyle işleyip işlemedikleri belirlendikten sonra suçun sübutu halinde, sanık M. Y.’in fotoğrafı yapıştırılmak suretiyle elde edilen nüfus cüzdanını kullanıp sözleşmeler imzalayarak, kredi kartları alma eylemlerinin banka sayısınca T.C.K.nun 245/2., 43 ve her bir bankaya ait birden fazla kartın değişik zamanlarda üretilmesi halinde de kendi içerisinde zincirleme şekilde T.C.K.nun 245/2., 43. madde ve fıkralarında;

sayılı Banka Kartları ve Kredi Kartları Kanununun 37/2. maddesinde düzenlenen suçun<sup>77</sup>, kredi kartı sözleşmesinin düzenlenip kartın üretilmesi aşamasına kadar uygulanacağını, sözleşme düzenlenip sahte kartın üretilmesinden sonra ise TCK'nın m. 245/2'nin uygulanacağını kabul etmektedir<sup>78</sup>. Ayrıca belgede sahtecilik suçunun uygulanmasını kabul etmemektedir<sup>79</sup>. Burada sorun sahte belgelerle başvurarak kartın çıkarılmasında, dolaylı failliğin gerçekleşip gerçekleşmediğidir. Eğer dolaylı faillik kabul edilirse o zaman sahte belgelerle başvurup kartın çıkarılması durumunda sahte kart üretme fiili gerçekleşmiştir. Dolaylı failliğin gerçekleşeceğini düşünüyoruz. Zira banka görevlisinin araç olarak kullanması suretiyle sahte belge üretilmektedir. Ayrıca sahte belge vermek suretiyle fail, m. 37/2'yi de gerçekleştirmiştir. Tek fiille hem m. 37/2, hem de m. 245/2 gerçekleştirildiğinden fikri içtima kuralları gereğince fail yalnızca m. 245/2'den sorumlu olacaktır. Dolandırıcılığın ise oluşmadığını düşünüyoruz. Zira kredi kartı çıkarmak için

---

*kartları değişik zamanlar- da kullanarak alışveriş yapmak suretiyle yarar sağlaması halinde ise, aynı Kanunun 245/3., 43. madde ve fıkralarındaki birbirinden bağımsız ayrı ayrı suçları oluşturacağı dikkate alınarak hükümler kurulması gerekirken, eksik incelemeye dayanarak dört bankaya yönelik sahte kredi kartı üretmek ve kullanmak şeklinde gerçekleşen eylemler küll halinde değerlendirilerek, zincirleme suretiyle işlenen T.C.K.nun 245/3. maddesi uyarınca karar verilmesi yasaya aykırıdır”, 8. CD, 21.05.2015, E. 2014/32263, K. 2015/17388, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.04.2016). 8. CD, 02.03.2015, E. 2014/27246, K. 2015/12807. Aynı yönde 8. CD, 18.02.2015, E. 2014/26299, K. 2015/12123; 8. CD, 30.03.2015, E. 2014/28809, K. 2015/15294; 8. CD, 03.02.2015, E. 2014/38108, K. 2015/2265, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.22.02.2017); 8. CD, 31.05.2017, E. 2017/932, K. 2017/6373.*

<sup>77</sup> Banka Kartları ve Kredi Kartları Kanununun 37. maddesinin 2. fıkrası, “kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler” hükmünü içermektedir.

<sup>78</sup> “5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 37/2. maddesinde yer alan “kredi kartı, üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar, sözleşme imzalamak amacıyla sahte belge ibraz edenler” şeklindeki düzenlemenin sözleşmenin imzalanmasını da kapsayacak aşamaya kadar uygulanabileceği, kredi kartı sözleşmesinin düzenlenmesinden sonra kartın üretilmesi halinde 5237 sayılı TCK'nun 245/2. maddesindeki suçu oluşturacağını gözetilmemesi...yasaya aykırıdır”, 11. CD, 08.05.2013, E. 2011/10450, K. 2013/7470, “5237 Sayılı Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları”, [www.taa.gov.tr/.../alper-yukselen-bikirli-yargitay-8-ceza-dairesi-uyesi-c2F5ZmF8Nzh](http://www.taa.gov.tr/.../alper-yukselen-bikirli-yargitay-8-ceza-dairesi-uyesi-c2F5ZmF8Nzh) (E.T.03.03.2017); 8. CD, 27.03.2018, E. 2017/17576, K. 2018/3373; 8. CD, 25.04.2018, E. 2017/22393, K. 2018/4692.

<sup>79</sup> Doktrinde ise farklı belirlemeler bulunmaktadır. Bazı yazarlar, sahte belgelerle başvurularak kredi kartı çıkartılması durumunda, sahte bir kartın bulunmadığı, banka veya finans kuruluşu tarafından düzenlenen gerçek bir kart bulunduğunu, bu kart kullanılmak suretiyle yarar sağlanması durumunda nitelikli dolandırıcılık suçunun oluşacağını belirtmektedirler (Soyaslan, s. 664. Bazı yazarlar da sahte kartın bulunmadığını belirtmektedirler: Meran, Necati, Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara 2005, s. 382; Karagülmez, s. 215). Bazı yazarlar ise, sahte resmi belgenin kullanılması sonucunda kartın üretilmesinin sağlanması halinde hem resmi belgede sahtecilik suçunun hem de m. 245/2'nin oluştuğunu, her iki fiilden de ceza verilmesi gerektiğini belirtmektedirler. Belgenin özel belge olması halinde ise, 5464 sayılı Kanunun 37. maddesinde düzenlenen suçun özel belgede sahtecilik suçunu özel şekli olduğunu, sahte özel belgeyle başvurularak sahte kartın üretilmesi durumunda m. 245/2'nin oluşacağını, ayrıca m. 37/2'den ceza verilmeyeceğini belirterek özel belgenin kullanılması durumunda Yargıtay gibi değerlendirmede bulunmaktadır (Gül, s. 146, 147). Bazı yazarlar sahte müracaatlar ile başvurularak kartın çıkartılması durumunda m. 245/2'nin gerçekleşeceğini benimsemektedirler (Artuk/Gökçen/Yenidünya, s. 900). Bazı yazarlar ise, kredi kartı sözleşmesi düzenlenmesi amacıyla sahte belge ibraz edilmesi durumunda Banka Kartları ve Kredi Kartları Kanununun 37/2. maddesinin, sahte bilgilerle sözleşmenin düzenlenmesinden sonra kartın üretilmesi durumunda ise TCK m. 245/2'den sorumluluğun doğacağını belirtmektedirler (Mahmutoğlu, Bilişim Alanındaki Suçlar, s. 873).



sahte belge ibraz etmek bağımsız suç olarak m. 37/2’de düzenlenmiştir. Belgede sahtecilik suçunun gerçekleşip gerçekleşmediğine gelince m. 37/2’deki seçimlik hareketler iki farklı konu üzerinde gerçekleştirilmektedir. Birincisi kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerinde yapılan sahtecilik, ikincisi ise kullanılan başka sahte (sahtecilik yapılan kredi kartı veya üye işyeri sözleşmesinde veya eki belgeleri değil) belgedir. Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerinde yapılan sahtecilik açısından özel belgede sahtecilik suçunun özel şekli olduğu söylenebilir de sözleşme imzalamak amacıyla sahte belge ibraz etmek açısından aynı şeyin geçerli olmadığı belirtilmelidir. Dolayısıyla sahtecilik yapılan belgenin kullanılması açısından hem 5464 sayılı Kanununun 37/2. maddesi, hem de özel belge ise TCK’nın 207. maddesi, resmi belge ise TCK’nın 204. maddesi gerçekleştirilmiştir. Ancak TCK m. 212 hükmü burada da geçerli olmalıdır. Dolayısıyla Yargıtay’ın küll halinde TCK m. 245/2’in gerçekleştiği kararına katılmıyoruz. Yazılanlardan da anlaşıldığı üzere sahte belge ibraz etmek suretiyle kredi kartı çıkarılmışsa fail hem m. 245/2’den hem de özel belge veya resmi belgede sahtecilik suçundan sorumlu tutulmalıdır.

Satmak, bir değer karşılığında banka veya kredi kartının alıcıya verilmesidir.

Devretmek, banka veya kredi kartı üzerindeki mülkiyeti veya hakkı başkasına geçirmektir. Süreli veya süresiz olabilir. Bedel karşılığında yapılmamaktadır.

Satın almak, bir bedel karşılığında banka veya kredi kartını kendine mal etmektir.

Kabul etmek, bedelsiz olarak verilen banka veya kredi kartını almaktır. Bağış yoluyla veya başka şekilde verilebilir. Süreli veya süresiz olabilir.

## 2. Manevi Unsur

Kasten işlenebilen suçtur. Suçun oluşması için failin başkalarının hesaplarıyla ilişkilendirilmiş sahte banka veya kredi kartı ürettiğini, sattığını, devrettiğini, satın alan veya kabul eden kişinin de başkalarının hesaplarıyla ilişkilendirilmiş sahte banka veya kredi kartını satın aldığını veya kabul ettiğini bilmesi gerekmektedir. Failin bilmemesi durumunda m. 30/1 çerçevesinde hata hükümleri uygulanacak ve sorumlu tutulmayacaktır.

TCK m. 245/2’de suçun taksirli şekline yer verilmemiştir. Herhangi amaç veya saik de aranmamıştır. Bilerek gibi bir ifadeye de yer verilmemiştir<sup>80</sup>. Dolayısıyla hem doğrudan hem de olası kastla suçun işlenmesi mümkündür.

---

<sup>80</sup> Üretmek fiili dışında bilerek kavramına yer verilmesi gerektiği noktasında bkz.: **Özbek/Doğan/Bacaksız/Tepe**, s. 1023.

### 3. Hukuka Aykırılık

TCK m. 245/2’de yer alan suç, topluma karşı işlenen suçlardan olduğundan meşru savunma, ilgilinin rızasının uygulanması söz konusu olmayacaktır. Hakkın kullanılması ve görevin ifasının gerçekleşmesi de mümkün görünmemektedir<sup>81</sup>.

### D. TEŞEBBÜS

Teşebbüs mümkün olabilir. Ancak TCK m. 245/2’deki suç, soyut tehlike suçu niteliğinde olduğundan hareketin başlamasıyla tamamlanması arasında sürenin söz konusu olduğu hallerde teşebbüs gerçekleşebilir. Örneğin failin satarken yakalanması durumunda teşebbüs söz konusu olacaktır. Yine sahte kart üretilirken failin yakalanması halinde de suç teşebbüs aşamasında kalacaktır<sup>82</sup>. Yargıtay, kart bilgileri ele geçirilmekle birlikte kartın oluşturulmadığı hallerde kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçunun gerçekleştiğini kabul etmektedir. Buna karşılık kart oluşturulmuşsa kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçundan cezalandırmayı benimsememektedir<sup>83</sup>. Yine Yargıtay sahte belgelerle kredi kartı için başvurulup, belgenin sahte

<sup>81</sup> Koca/Üzülmez, s. 907; Özbek/Doğan/Bacaksız/Tepe, s. 1023.

<sup>82</sup> Yargıtay TCK m. 245/A yürürlüğe girmeden önce gerçekleşen bir olayla ilgili verdiği kararda manyetik şerit bilgilerin i kopyalamak ve şifrelerini elde etmek için ATM’ye düzenek yerleştirme eylemini hazırlık hareketi saymıştır. Yargıtay’a göre, “Sanığın kartın sıkışmasını sağlamak için bilişim sisteminin bir parçası olan ATM’ye yerleştiği düzenegi çıkarırken yakalandığının anlaşılması karşısında; eyleminin TCK.nun 245/2. maddesinde düzenlenen sahte banka veya kredi kartı üretme suçunun hazırlık hareketi niteliğinde olması, sanığın sahte kart üretimine yönelik her hangi bir faaliyette bulduklarının belirlenememesi, ancak cihazda işlem yapan sanığın katılan bankanın ATM cihazına yerleştiği düzenekle, işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmeye çalışmaktan ibaret eyleminin TCK.nun 136. maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturduğu gözetilmeden suç vasfında yanılıya düşülerek yazılı şekilde hüküm kurulması, yasaya aykırıdır”, 8. CD, 04.05.2017, E. 2016/10604, K. 2017/5010.

<sup>83</sup> “Sanığın.... Kebap Salonu isimli işyerinde garson olarak çalıştığı, mağdurlar ... ve ...’a ait kredi kartlarının kopyalandığı yönünde bankalardan gelen ihbar üzerine mağdurların adı geçen işyerine gelerek, işyeri sahibine kredi kartlarının kopyalandığını bildirmeleri nedeniyle suç tarihinde işverence yapılan araştırmada sanığın pantolonun cebinden siyah renkli el içine sığabilecek büyüklükte kredi kartını kopyalamaya yarayan cihazın ele geçirildiği, sanığın, çalıştığı lokantada yemek yiyen mağdurların kredi kartlarını kopyalamak suretiyle, sahte kredi kartı ürettikleri ve oluşturulan sahte kredi kartlarını kullanmak suretiyle kendilerine yarar sağladıkları iddiası ile TCK.nun 245/2, 245/3. maddeleri ile cezalandırılması talebiyle kamu davası açılan somut olayda; sanığın üzerinde kopyalanmış kart ele geçmemiş olması karşısında; suça konu kredi kartlarının bağlı olduğu bankalardan hesap özetlerinin istenmesi ve bankalardan sorulması suretiyle, mağdurlara ait kartlarla harcama yapılıp yapılmadığı, sanıkta ele geçen ve dosya arasında bulunan kopyalama cihazı üzerinde bilirkişi incelemesi yaptırılarak, herhangi bir bilgi bulunup bulunmadığı araştırılarak, mağdurlara ait kart bilgileri kopyalanarak bir kart oluşturulması halinde suçtan zarar görenin ilgili banka olduğu dikkate alınarak, suça konu kredi kartları gerçeğe aykırı olarak üretilen banka sayısınca TCK.nun 245/2. maddesi ile ve aynı bankanın birden fazla kartının değişik zamanlarda kopyalanması durumunda aynı yasanın 43. maddesinin uygulanması, bu kartların kullanılması halinde ise, banka sayısınca TCK.nun 245/3. maddesi ile aynı bankaya ait birden fazla kart ile veya bir kart ile değişik zamanlarda para çekilmesi veya harcama yapılması halinde ise TCK.nun 43. maddesi uyarınca uygulama yapılması, harcama yapılmadan kartların bloke olması halinde TCK.nun 245/3 maddesine teşebbüs suçundan uygulama yapılması gerektiği, mağdurlara ait kart bilgileri kopyalanarak bir kart oluşturulmaması halinde ise ele geçirilen kopyalama cihazında bilgi bulunması halinde eyleminin mağdur sayısınca TCK.nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme, bulunmaması halinde ise kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırma ile yazılı şekilde hüküm kurulması”, 8. CD, 08.10.2018, E. 2018/6171, K. 2018/10436.

olduğunun anlaşılması nedeniyle kart talebinin reddedildiği olayda, kart üretilmediğinden dolayı 245/2'nin gerçekleşmediğini, 5464 sayılı Kanunun 37/2. maddesinin gerçekleştiğini kabul etmektedir<sup>84</sup>.

## E. İŞTİRAK

İştirak şekilleri gerçekleşebilir. Dolaylı faillik, müşterek faillik ve şeriklik söz konusu olabilir.

Satmak-satın almak veya devretmek-kabul etmek çok faili suç niteliğinde olduğundan hareketlerden biri yapıldığında her iki fail de cezalandırılacaktır. Örneğin satma fiilinde satın alan kişi de m. 245/2'den sorumlu tutulacaktır.

Sahte kartın üretilmesinde kullanılan bir cihazın temin edilmesinde ise TCK m. 245/A gerçekleşecektir. Aynı zamanda cihazı temin eden kişi m. 245/2'ye yardım eden konumunda olacaktır. Cihazı veren kişi m. 245/A'nın faili olduğundan failliğin şerikliğe üstünlüğü ilkesi gereğince m. 245/A'dan sorumlu olacaktır.

## F. İÇTİMA

TCK m. 245/2'deki suçta zincirleme suç kuralları uygulanabilir. Failin farklı zamanlarda sahte banka veya kredi kartı üretmesi halinde zincirleme suç gerçekleşmiştir. Seri halde çok sayıda banka veya kredi kartının üretilmesi veya satılması veya kabul edilmesi halinde tek fiil ve tek suç bulunmaktadır. Ancak Yargıtay, sahte banka kartının üretilmesinde kartların aynı bankaya veya farklı bankaya ait olmasına göre ayırım yapmaktadır. Farklı farklı bankaya ait kartların üretilmesi durumunda banka sayısınca suçun oluştuğunu kabul etmektedir. Ancak aynı bankaya ait çok sayıda banka veya kredi kartının üretilmesinde ise zincirleme suç kurallarının uygulanmasına karar vermektedir<sup>85</sup>.

Failin sahte olarak ürettiği veya satın aldığı veya kabul ettiği sahte kartı kullanarak yarar sağlaması durumunda tek suçtan mı sorumlu tutulması gerektiği, yoksa ayrı ayrı mı cezalandırılması gerektiği doktrinde tartışmalıdır. Bazı yazarlar yalnızca yarar sağlama suçunun düzenlendiği TCK m. 245/3'den hüküm kurulması gerektiğini, ayrıca m. 245/2'den ceza verilmemesi gerektiğini belirtmektedirler<sup>86</sup>. Sadece m. 245/3'den sorumluluk tayin edilmesi gerektiğini belirten yazarlardan bazıları geçit suç bulunduğunu ifade etmektedirler<sup>87</sup>. Bizim de

---

<sup>84</sup> 8. CD, 11.12.2017, E. 2017/17537, K. 2017/14072; 8. CD, 27.03.2018, E. 2017/17576, K. 2018/3373.

<sup>85</sup> 8. CD, 10.02.2016, E. 2015/15546, K. 2016/1315, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.04.2016); 8. CD, 21.05.2015, E. 2014/32263, K. 2015/17388, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.04.2016).

<sup>86</sup> Tezcan/Erdem/Önok, s. 1063.

<sup>87</sup> Soyaslan, s. 668.

görüşlerine katıldığımız bazı yazarlar ise, hem TCK m. 245/2'den, hem de TCK m. 245/3'den sorumluluk tayin edilmesi gerektiğini, yani gerçek içtimanın uygulanması gerektiğini kabul etmektedirler. Tek fiil olmadığından fikri içtimanın uygulanamayacağını, suçlar aynı olmadığından zincirleme suç kurallarının gerçekleşmediğini ifade etmektedirler<sup>88</sup>. Yargıtay da hem sahte kartın üretilip hem de yarar sağlanmasında iki ayrı suçun oluştuğunu, failin TCK m. 245/2'den ve TCK m. 245/3'den ayrı ayrı cezalandırılması gerektiğini benimsemektedir<sup>89</sup>.

TCK m. 245/2 yanında m. 245/3'ün gerçekleştirildiği olaylarda ayrı ayrı cezalandırma kabul edilmekle birlikte, düzenlemeye eleştiri de yöneltilmektedir. Her iki maddeden ceza verilmesi halinde ceza alt sınırdan tayin edilse bile 7 yıl gibi bir cezanın söz konusu olduğu bunun da yüksek olduğu belirtilmektedir. TCK m. 245/3'deki düzenlemenin TCK m. 245/2'nin nitelikli hali olarak düzenlenmesi gerektiği ifade edilmektedir. Bu şekilde daha adil cezalandırmanın söz konusu olabileceği ileri sürülmektedir<sup>90</sup>. Kanaatimizce cezalar arasındaki orantısızlığın giderilmesi ve sahtecilik suçlarıyla uyumlu hale getirilmesi gerekmektedir.

Fail m. 245/A kapsamında bir cihazı ürettikten sonra ayrıca sahte kart üretiminde kullanmışsa, hem m. 245/A'dan hem de m. 245/2'den sorumlu olacaktır.

## G. YAPTIRIM

Türk Ceza Kanununun 245. maddesinin 2. fıkrasındaki suçun cezası, üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası olarak öngörülmüştür. Kanun koyucu, satmak suretiyle kazanç da sağlandığından hapis cezasının yanında adli para cezasının verilmesini de

<sup>88</sup> **Koca/Üzülmez**, s. 908; **Karagülmez**, s. 219-220; **Yılmaz**, s. 280; **Özbek/Doğan/ Bacaksız/Tepe**, s. 1024; **Özbek**, s. 1050; **Gül**, s. 152. Bu görüşü savunan yazarlardan bazıları, TCK m. 245/3'ün TCK m. 245/2'nin ağırlatıcı nedeni olarak düzenlenmesi gerektiğini ileri sürmektedirler: **Özbek**, s. 1050; **Özbek/Doğan/Bacaksız/Tepe**, s. 1024.

<sup>89</sup> “Sanıklar hakkında aynı zaman diliminde katılana karşı benzer suçlar işledikleri iddiasıyla açılmış davaların olduğu anlaşılmalı; başkasına ait banka hesabıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi TCK'nın 245/2. maddesinde, sahte banka veya kredi kartını kullanarak kendisine veya bir başkasına yarar sağlanması ise anılan maddenin 3. fıkrasında birbirinden bağımsız ve ayrı ayrı suçları oluşturduğu, bankaya ait gerçek bir kredi kartının manyetik şerit bilgilerinin kopyalanarak sahte bir kredi veya banka kartı üretilmesi ve bu kart kullanılarak yarar sağlanması halinde suçtan zarar görenin ilgili banka olduğu, aynı bankaya ait birden fazla kartın kopyalanması durumunda 245/2,43., sahte olarak üretilen kartların alışverişte kullanılması halinde ise, banka sayısınca 245/3. maddesi ile aynı bankaya ait birden fazla kart ile veya bir kart ile değişik zamanlarda para çekilmesi veya harcama yapılması halinde ise 43. maddesi uyarınca uygulama yapılması gerektiği dikkate alınarak, sanıklar hakkında başka benzer eylem nedeniyle davalar açılıp açılmadığı araştırılıp, yargılanmakta olduklarının anlaşılması halinde, suç tarihleri gözetilerek mükerrer cezalandırılmalarının önlenmesi bakımından sanıklar hakkında açılan davaların birleştirilmesi, aksi halde incelenerek bu davayı ilgilendiren delillerin onaylı örneklerinin dosyaya konulduktan sonra tüm delillerin birlikte değerlendirilerek sanıkların hukuki durumunun takdir ve tayini gerektiği gözetilmeden yazılı biçimde hükümler kurulması bozmayı gerektirmiştir”, 8. CD, 05.11.2018, E. 2017/25362, K. 2018/12171; 8. CD, 15.10.2018, E. 2016/10134, K. 2018/10888; 8. CD, 18.02.2015, E. 2014/26299, K. 2015/12123, T. 18.2.2015, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T. 23.01.2017).

<sup>90</sup> **Özbek/Doğan/Bacaksız/Tepe**, s. 1024; **Özbek**, s. 1050; **Yılmaz**, s. 296; **Koca/Üzülmez**, s. 866 (bileşik suç şeklinde düzenlenmesi gerektiği belirtilmektedir).

öngörmüştür. Adli para cezasının üst sınırı belirtilmiş alt sınırı öngörülmemiştir. Alt sınır TCK'nın 52. maddesi gereğince 5 gün olarak kabul edilecektir.

TCK'nın 246. maddesi gereğince yararına suç işlenen tüzel kişi hakkında de TCK'nın 60. maddesindeki güvenlik tedbirleri uygulanacaktır

## H. SORUŞTURMA VE KOVUŞTURMA

Türk Ceza Kanununun 245. maddesinin 2. fıkrasında yer alan suç, resen takip edilen suçlardandır. Görevli mahkeme, Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 11. ve 12. maddeleri gereğince asliye ceza mahkemesidir. TCK m. 245/2, soyut tehlike suçu olduğundan harekete göre suçun işlendiği yer ve yetkili mahkeme belirlenecektir. Buna göre 245. maddenin 2. fıkrasında yer alan seçimlik hareketlerinin gerçekleştirildiği yerde bulunan mahkeme yetkili mahkemedir. Farklı yerlerde gerçekleştirilmişse seçimlik hareketlerin gerçekleştirildiği yer mahkemeleri yetkili olacaktır. Ülke içinde işlenen suçlarda zincirleme suç veya teşebbüs söz konusuysa CMK m. 12/2 gereğince yetkili mahkeme belirlenecektir. Suç yabancı ülkede işlenmiş ve Türkiye'de yargılama yapılmasının mümkün olduğu hallerde yetkili mahkeme CMK m. 14 gereğince belirlenecektir.

## IV. SAHTE BANKA VEYA KREDİ KARTINI KULLANARAK YARAR SAĞLAMAK SUÇU

### A. KORUNAN HUKUKİ DEĞER

Sahte banka veya kredi kartını kullanarak yarar sağlamak suçu, Türk Ceza Kanununun 245. maddesinin 3. fıkrasında, “*sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır*” hükmüyle düzenlenmiştir. Kanun koyucu başkalarına ait banka veya kredi kartının kullanılarak yarar sağlanmasını bağımsız suç olarak düzenlediği gibi (TCK m. 245/1), sahte olarak oluşturulmuş veya üzerinde sahtecilik yapılmış banka veya kredi kartının kullanılmasını da ayrı bir suç olarak hükme bağlamıştır. Kanun koyucu sahte kartların kullanılarak 3. kişilere zarar verilmesini, bu yolla yarar sağlanmasını engellemek istemiştir. Dolayısıyla korunan hukuki değer kişilerin malvarlığıdır<sup>91</sup>. Diğer hukuka aykırı yarar sağlamaya

---

<sup>91</sup> Doktrinde TCK'nın 245. maddesinin 3. fıkrasında düzenlenen suçun, kişilerin malvarlığını korumakla beraber başka değerleri de koruduğu belirtilmektedir. Bazı yazarlar, ağırlıklı olarak malvarlığının korunmakla beraber, aynı zamanda sahte kartların piyasada kullanılmasının önlenmesi suretiyle bu kartların doğruluğuna ilişkin güvenin de korunduğunu kabuletmektedirler (Koca/Üzülmez, s. 909). Bazı yazarlar, sahte banka veya kredi kartını kullanarak yarar sağlamak suçunun belirtilen bu iki değer yanında bilişim alanının güvenliğinin sağlanması olduğunu da ifade etmektedirler

ilişkin bilişim suçlarında olduğu gibi sahte banka veya kredi kartının kullanılarak yarar sağlanması suçunda da fail, kendisine veya başkasına yarar sağlamak suretiyle kişilerin malvarlığında zarara neden olmaktadır. Suçun cezasının hapis cezası yanında onbin güne kadar adli para cezası olarak öngörülmesi de bu sonucu desteklemektedir.

## B. SUÇUN UNSURLARI

### 1. Maddi Unsur

#### -Fail ve mağdur

Sahte banka veya kredi kartını kullanarak yarar sağlamak suçunun faili 3. fıkarda bir özelleştirmeye gidilmediğinden herhangi bir kimse olabilir. Fail, 2. fıkarda düzenlenen sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçunu da işlemiş olabilir. Ancak fail, 2. fıkradaki suçu gerçekleştiren kişi dışında başka bir kişi de olabilir<sup>92</sup>.

TCK'nın 245/3. maddesinde düzenlenen suç için, sahte banka veya kredi kartının kullanılması suretiyle yarar sağlanması gerektiğinden, bu yarar nedeniyle malvarlığında azalma olan kişi suçun mağduru olacaktır<sup>93</sup>. Eğer sahte kart bir hesaba bağlantılı olarak kullanılıyorsa malvarlığında azalma olan kişi, adına sahte kart düzenlenen kişidir (kart hamilidir). Ancak bu şekilde bir yarar sağlanmıyorsa hayali hesaplarla yarar sağlanıyorsa banka veya finans kuruluşunun

---

(Özbek, s. 1052). Bazı yazarlar da benzer belirleme yapmakta, korunana değer birden fazla olduğunu, bilişim sistemlerinin düzgün işlemesine ilişkin toplumsal menfaat, kamu güveni, kişilere ait malvarlığına ilişkin değerlerin korunduğunu kabul etmektedirler (Okuyucu-Ergün, s. 1067. Korunan hukuki değer karma nitelikte olduğuna ilişkin olarak ayrıca bkz.: Meran, 378, 379).

<sup>92</sup> Yargıtay da TCK'nın 245. maddesinin üçüncü fıkrasında yazılı sahte kartın kullanılarak çıkar sağlanması suçunun oluşması için, 2. fıkarda kabul edilen suçun işlenmesinin zorunlu olmayıp üretme, satın alma veya kabul etmenin dışında bir başka yolla kartın edinilmesi, örneğin sahte kartın bulunması üzerine kullanımı suretiyle de çıkar sağlanmasının olanaklı olduğunu ifade etmektedir, 8. CD, 18.02.2015, E. 2014/26299, K. 2015/12123, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.22.03.2017). “Sahte banka veya kredi kartı üretme, kabul etme ve sahte oluşturulmuş banka veya kredi kartı ile ATM cihazından para çekme ya da alışı veriş yapma eylemlerinin mağduru, kredi ya da banka kartını üreten banka veya finans kuruluşu olması nedeniyle; sanığın, F. K. 'ya ait nüfus cüzdanı fotokopisiyle katılan F...Bank'tan sahte kredi kartı çıkartmak eyleminin bir bütün halinde TCK.nun 245/2., 43. maddelerine uyan suçu oluşturduğu ve bu kartlarla değişik zamanlarda harcama yapmaktan ibaret eyleminin ise yine TCK.nun 245/3. ve 43. maddesine uyan suçu oluşturduğu gözetilmeden, eylem kül halinde değerlendirilerek TCK.nun 245/1. maddesinden hüküm kurulması suretiyle eksik ceza tayini yasaya aykırıdır”, 8. CD, 09.02.2015, E. 2015/1107, K. 2015/4706, [www.kazanci.com.tr](http://www.kazanci.com.tr) E.T.22.03.2017).

<sup>93</sup> Türk Ceza Kanununun 245. maddesinin 3. fıkrasında düzenlenen sahte banka veya kredi kartını kullanarak yarar sağlamak suçunun mağdurunun kim olduğu doktrinde tartışmalıdır. Bazı yazarlar suçun mağdurunun, failin yarar nedeniyle malvarlığı zarara uğrayan kişi olduğunu belirtmektedirler. Bunun kart hamili veya bankanın malikleri veya başka bir kişi olmasına ilişkin bir belirleme yapmamaktadırlar (Koca/Üzülmez, s. 909). Bazı yazarlar ise, somut olayın koşullarına bakılarak mağdurun belirlenmesi gerektiğini, sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartının kullanılması suretiyle banka veya kredi kuruluşunun mu yoksa ilgili kişinin mi yoksa her ikisinin mi malvarlığında bir azalma olduğuna bakılmak suretiyle suçtan zarar görenin belirlenmesi yoluna gidilmesi gerektiğini belirtmektedir (Okuyucu-Ergün, s. 1080). Bazı yazarlar ise, suçta sahte, hayali hesaplara bağlı olarak üretilen kartlar söz konusu olduğundan bu suçun mağdurunun banka ya da finans kurumu olduğunu ifade etmektedirler (Özbek, s. 1053). Bazı yazarlar ise suçun mağdurunun kart hamili olduğunu ifade etmektedirler (Özbek/Doğan/Bacaksız/Tepe, s. 1029; Gül, s. 123; Tezcan/Erdem/Önok, s. 1061).

malik veya ortakları ya da alışveriş yapılan kişiler mağdur olacaktır<sup>94</sup>. Yargıtay, suçun mağdurunun kredi ya da banka kartını üreten banka veya finans kuruluşu olduğunu kabul etmektedir<sup>95</sup>.

### **-Konu**

Sahte banka veya kredi kartını kullanarak yarar sağlamak suçunun konusu, malvarlığına ilişkin ekonomik değerdir. Doktrindeki bazı yazarlar sahte banka veya kredi kartını kullanarak yarar sağlamak suçunun konusunun sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartları olduğunu ifade etmektedirler<sup>96</sup>. Ancak daha önce de belirtildiği gibi banka veya kredi kartları, suçun konusu olmayıp fiil aracı niteliğindedir.

### **-Fiil**

Türk Ceza Kanununun 245/3. maddesindeki suçun oluşması için hem sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartının kullanılması, hem de yarar sağlanması gerektiğinden, söz konusu suç çok hareketli suç niteliği taşımaktadır. Suçun oluşması için yarar sağlanması da gerektiğinden m. 245/3'deki suç, aynı zamanda bir zarar suçudur.

Suçun oluşması için yarar sağlamada kullanılan kartın, sahte olarak oluşturulmuş veya üzerinde sahtecilik yapılmış bir kart olması gerekmektedir. Fıkra da belirtildiği gibi, banka veya kredi kartı tamamen sahte bir kart şeklinde oluşturulabileceği gibi, var olan bir banka veya kredi kartının içerik olarak değiştirilmesi şeklinde veya banka veya kredi kartları üzerindeki kabartma numaralarının kesilerek değiştirilmesi suretiyle veya gerçek kartların manyetik şeritlerine farklı bir bankaya ait kart bilgisinin kopyalanması yoluyla da gerçekleştirilebilir. Sahte kart gerçek bir hesapla ilişkilendirilmek suretiyle gerçekleştirilebileceği gibi, tamamen hayali kişiler adına açılmış bir hesapla ilgili bilgilerin kullanılması suretiyle de üretilebilir<sup>97</sup>. Fıkra da gerçek bir hesapla ilişkilendirilmesine ilişkin belirleme yapılmadığından hayali isimlere çıkartılan kartla da suçun işlenmesi mümkündür.

Doktrindeki bazı yazarlar “sahte olarak oluşturulan” ifadesinin, kartın alınması sırasında sahte olarak verilen kullanıcı bilgileri, gerçeğe aykırı kişisel bilgilere dayalı olarak düzenlenen kartları ifade ettiğini kabul etmektedirler. Dolayısıyla da bu kartların kullanılması durumunda

---

<sup>94</sup> Krş.: **Özbek**, s. 1053.

<sup>95</sup> “*sanıkların bir bankaya ait gerçek bir kredi kartının manyetik şerit bilgilerinin kopyalanarak sahte bir kredi kartı üretmesi ve bu kartı kullanmak suretiyle yarar sağlamaları halinde suçtan zarar görenin ilgili banka olduğu*”, 8. CD, 15.10.2018, E. 2016/10134, K. 2018/10888; 8. CD, 05.11.2018, E. 2017/25362, K. 2018/12171; 8. CD, 12.05.2015, E. 2014/29393, K. 2015/17026, [www.kazanci.com](http://www.kazanci.com) (E.T.22.03.2017).

<sup>96</sup> **Özbek**, s. 1052; **Özbek/Doğan/Bacaksız/Tepe**, s. 1026; **Artuk/Gökçen/Yenidünya**, s. 902.

<sup>97</sup> **Koca/Üzülmez**, s. 910. Aksi görüş için bkz.: **Karagülmez**, s. 215.

TCK'nın 245. maddesinin 3. fıkrasındaki suçun oluşacağını benimsemektedirler<sup>98</sup>. Bazı yazarlara göre ise, TCK'nın 245. maddesinin 2. fıkrasında yer alan “sahte oluşturulan veya üzerinde sahtecilik yapılan kart” kavramının bizzat kartın fiziki yapısına yönelik sahtecilik ile gerçek kart üzerinde sahtecilik yapmayı ifade ettiğini, gerçek dışı bilgilerle bankadan kart alınmasında gerçek bir kartın bulunduğunu, sahte bir kartın bulunmadığını, dolayısıyla bu kartın kullanılarak yarar sağlanmasında m. 245/3'ün oluşmayacağını kabul etmektedirler<sup>99</sup>. Daha önce de belirttiğimiz gibi başkalarına ait bilgilerin kendisine aitmiş gibi kullanılarak kart çıkartılmasında m. 245/2 gerçekleşecektir. Yargıtay'ın da kabul ettiği gibi bu kartın kullanılarak yarar sağlanmasında TCK m. 245/2 gerçekleşeceği gibi, TCK m. 245/3'de oluşacaktır<sup>100</sup>. Hayali isimlerle ve buna ilişkin

<sup>98</sup> Bu görüşü savunan yazar için bkz.: **Karagülmez**, s. 214, dipnot 230. Aynı yönde **Özbek/Doğan/Bacaksız/Tepe**, s. 1027.

<sup>99</sup> **Karagülmez**, s. 215. Bazı yazarlar bu durumda m. 245/3 değil, dolandırıcılık veya 5464 sayılı Kanunun 37/2. maddesi gereğince cezalandırılacağını belirtmektedirler: **Tezcan/Erdem/Önok**, s. 1059.

<sup>100</sup> “Somut olayda sanığın, katılanın rızası ve bilgisi olmaksızın kimlik bilgilerine göre düzenlenmiş kredi kartını alıp harcama yaparak T.C.K.nun 245/3. maddesinde belirtilen sahte banka veya kredi kartını kullanmak suçunun yanında, T.C.K.nun 245/2. maddesinde düzenlenen sahte banka veya kredi kartını üretirme suçu da olduğu halde, fikri içtimadan bahisle yazılı şekilde tek hüküm kurulması yasaya aykırıdır”, 8. CD, 18.02.2015, E. 2014/26299, K. 2015/12123, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.03.2017). “Sahte oluşturulan nüfus cüzdanla kredi kartı başvurusu yapmak suretiyle sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi 5237 Sayılı T.C.K.nun 245/2. maddesinde, sahte banka veya kredi kartını kullanarak kendisine veya bir başkasına yarar sağlanması ise, anılan maddenin 3. fıkrasında düzenlenen birbirinden bağımsız ve ayrı ayrı suçları oluşturduğu cihetle; sanık M. Y.'in askerlik görevini ifa eden kayınbiraderi katılan M. Y. kimlik bilgilerine göre üzerinde sanık M. Y.'in resmi bulunan sahte bir nüfus cüzdanı düzenlettirip bu nüfus cüzdanıyla adına Denizbank'taniki ayrı, hsbc Bank, Asya Katılım Bankası ve Finansbank'tan birer kredi kartı başvurusunda bulunup bu şekilde temin ettikleri toplam beş adet kredi kartını alıp kullandıklarından bahisle açılan davada, sanıklar T. B. H. Y.'in soruşturma safhasında “sanıklar M.'la T. Kocamustafapaşa'da ortak bir işyeri çalıştırmakta olup sanık M.'nin akrabası olması sebebiyle zaman zaman işyerlerine gidip gelen sanık H. Y., sanık M.'nin işyerinde olmadığı sırada, ortağı olan sanık T. bana bir zarfın içinden çıkardığı katılana ait kimlik bilgilerine göre düzenlenmiş ancak sanık M.'nin resmi yapışık olan bir nüfus cüzdanını gösterdiğini, “bu ne biçim nüfus cüzdanı” diye sorduğunda, sanık M.'nin bu nüfus cüzdanıyla muhtelif bankalara başvurup ve M. Y. adına kredi kartları aldığını ve kullandığını söylediği, bu sırada sanık M. Y.'in, sanık H.'ya bir bankadan 5000 TL kredi çektiyip taksitlerini ödemediği, bu sebeple borcu olduğu, işyerlerine tekrar gittiğinde, ortağı sanık T. işyerindeydi, sohbet esnasında suça konu 5 adet kredi kartını vermek istediğini ve herhangi bir şey olursa tanıklık yapmasını söylediği, alacağını alamadığı için borcunu ödemezse bu kredi kartlarıyla hakkında şikayetçi olacağını söylemek ve kredi kartlarını koz olarak kullanmak düşüncesiyle sanık T.'un verdiği 5 adet kredi kartını alıp evine götürdüğünü ve sakladığını, 16.9.2009 günü güvenlik görevlileri gelip olayı sorduklarında anlatıp ve kitapların altına sakladığı 5 adet kredi kartını teslim edildiğini”, mahkeme huzurunda ise katılana vermek üzere sanık T. B. tarafından sanık H. Y.'a verildiğine dair savunmaları ve aradaki çelişkilerin giderilmemesi, diğer sanık M. Y.'in ise suçu kabul etmeyip diğer sanıkların işlemiş olabileceğini savunması, İlgili bankalardan Denizbank'tan gelen belgeler üzerinde imza yönünden yapılan inceleme sonucu alınan kriminal raporda; gerek katılan, gerekse sanıklara aidiyetinin saptanamadığının belirtilmesi, diğer bankaların belgeleri üzerinde inceleme yapılmaması, şikayetçi hsbc bankasının belgeleri gönderdiği belirtilmişse de dosyada rastlanmaması, gerek katılan Finansbank gerekse şikayetçi Denizbank'ın hesap ekstrelerinde kontür alımları olduğunun anlaşılması karşısında, öncelikle şikayetçi HSBC bankasının sahte olarak düzenlettirilip kullanıldığı iddia olunan kredi kartına dair sözleşme ve ekleriyle birlikte harcama belgelerinin de istenilip gerek sanıkların gerekse katılanın suç tarihinden önce resmi dairelerde mevcut bulunan imza ve yazı örnekleri getirtilip tüm bankalara ait belgelerde inceleme yaptırılması, hesap ekstrelerinde görülen kontür alımı yapılan telefon numaralarının kimlere ait olduğu araştırılıp diğer alışveriş yerlerinin sahipleri de dinlenerek sonucuna göre sanıklar T. B. H. Y.'la birlikte katılan Finansbank'a yönelik atılı suçu fikir ve eylem birliğiyle işleyip işlemedikleri belirlendikten sonra suçun sübutu halinde, sanık M. Y.'in fotoğrafı yapışırılmak suretiyle elde edilen nüfus cüzdanını kullanıp sözleşmeler imzalayarak,



belgelerle hesap açtırılıp, kart çıkartılarak kullanılmasında da TCK m. 245/3'deki suç işlenecektir. Ancak bu durumda TCK m. 245/2'in gerçekleşmesi söz konusu olmayacaktır.

Kullanma fiili için, kartı sahte olarak oluşturan veya üzerinde değişiklik yapan kişinin bu ürettiği kartı bizzat kendisinin kullanması gerekmez. Daha önce de belirtildiği gibi başkalarının banka hesaplarıyla ilişkilendirilmeden üretilen sahte banka veya kredi kartları suç oluşturmamaktadır. Bu kartların başkasına verilerek kullandırılması durumunda iştirak hükümleri çerçevesinde sorumluluk tayin edilecektir. Ancak başkalarının hesaplarıyla ilişkilendirilerek üretilen sahte banka veya kredi kartının aynı zamanda yarar sağlamada da kullanılması halinde fail hem 245. maddenin 2. fıkrasındaki suçu hem de 3. fıkrasındaki suçu gerçekleştirmiş olacaktır. Ancak üçüncü fıkra yazılı sahte kartın kullanılarak çıkar sağlanması suçunun oluşması için, 2. fıkra kabul edilen suçun işlenmesi zorunlu değildir. Örneğin sahte kartın çalınması veya bulunması üzerine kullanılarak yarar sağlanması durumunda 3. fıkradaki yarar sağlama suçu oluşacaktır. TCK'nın 245. maddesinin 2. fıkrasında yazılı suçun oluştuğundan sözedilemeyecektir. Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartını üreten, satan, devreden kişinin, kartı satın alan kişinin bu kartı kullanarak yarar sağlaması fiiline iştirak iradesi yoksa, kartı üreten, satan, devreden kişinin satın alanın kullanmasına iştirak ettiği ve 3. fıkradaki suçu işlediği söylenemeyecektir. Uygulamada failerin yakalanmamak için kopyaladıkları sahte kartları farklı kişilere kullandırdıkları, yakalanan kişilerin kopyalama eylemine katılmadıkları, kartı alıp sadece işlem yaptıkları, ancak bu durumda kartı kabul etmenin söz konusu olduğu, dolayısıyla TCK m. 245/2'in gerçekleştiği, ayrıca yarar sağlama suçunun (m. 245/3) oluştuğu belirtilmektedir<sup>101</sup>.

Sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartları ATM'lerde, üye işyerlerindeki alışverişlerde, internette yapılan alışverişlerde kullanılabilir.

Suçun oluşması için yararın sağlanması şarttır. Yarar, ekonomik nitelikte olmalıdır. Ekonomik nitelikte olmayan yararlar da TCK m. 245/3 uygulanmaz. Yarar sağlanması ile sahte banka veya kredi kartının kullanılması arasında bağlantı bulunmalıdır. Yarar, failin kendisine

---

*kredi kartları alma eylemlerinin banka sayısınca T.C.K.nun 245/2., 43 ve her bir bankaya ait birden fazla kartın değişik zamanlarda üretilmesi halinde de kendi içerisinde zincirleme şekilde T.C.K.nun 245/2., 43. madde ve fıkralarında; kartları değişik zamanlar- da kullanarak alışveriş yapmak suretiyle yarar sağlaması halinde ise, aynı Kanununun 245/3., 43. madde ve fıkralarındaki birbirinden bağımsız ayrı ayrı suçları oluşturacağı dikkate alınarak hükümler kurulması gerekirken, eksik incelemeye dayanarak dört bankaya yönelik sahte kredi kartı üretmek ve kullanmak şeklinde gerçekleşen eylemler küll halinde değerlendirilerek, zincirleme suretiyle işlenen T.C.K.nun 245/3. maddesi uyarınca karar verilmesi, yasaya aykırıdır”, 8. CD, 21.05.2015, E. 2014/32263, K. 2015/17388, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.23.03.2017).*

<sup>101</sup> Gül, s. 153.

sağlanabileceği gibi, başkasına da sağlanabilir. TCK'nın 245. maddesinin 3. fıkrasında “kendisine veya başkasına yarar sağlayan” ifadesiyle bu husus açıkça dile getirilmiştir. Yararın mutlaka fiilen elde edilmiş olması gerekmez. Yarar, üzerinde tasarruf edebilir duruma gelmiş ise suç tamamlanmış demektir. Örneğin, bir kişinin kendi adına hesap açıp, daha sonra bu hesaba başka hesaplardan sahte banka veya kredi kartını kullanmak suretiyle para transferi yapması durumunda suç tamamlanmıştır. Gidip bankadan bu paraları alması gerekmez<sup>102</sup>.

## **2. Manevi Unsur**

Kasten işlenebilen bir suçtur. Failin m. 245/3'deki suçtan sorumlu olması için kullandığı kartın banka veya kredi kartı olduğunu, bu kartların sahte olduğunu, banka veya kredi kartını kullanmak suretiyle kendisine veya bir başkasına yarar sağladığını bilmelidir.

Olası kastla da işlenebilir. Taksirle işlenmesi söz konusu değildir.

## **3. Hukuka Aykırılık**

TCK'nın 245. maddesinin 3. fıkrasında düzenlenen sahte banka veya kredi kartını kullanarak yarar sağlamak suçu açısından herhangi bir hukuka uygunluk nedenin gerçekleşmesi söz konusu değildir.

## **C. TEŞEBBÜS**

Sahte banka veya kredi kartı kullanarak yarar sağlamak suçuna teşebbüs mümkündür. Suçun oluşması için sahte oluşturulmuş veya üzerinde sahtecilik yapılmış kartın kullanılması suretiyle yarar sağlamak gerektiğinden, kartın kullanılmasına rağmen yararın elde edilemediği hallerde suç teşebbüs aşamasında kalmıştır. Örneğin ATM'den para çekmek isterken failin yakalanması halinde suç tamamlanamamıştır.

Sahte kartın üretilmesi veya bilgilerin ele geçirilmesi suça teşebbüs edildiğini göstermez. Zira suçun oluşması için kartın kullanılması ve yararın elde edilmesi gerekmektedir. Bu durumda TCK m. 245/2 veya TCK m. 136 gerçekleşebilir.

Teşebbüs mümkün olduğundan yarar sağlanıncaya kadar gönüllü vazgeçme hükümleri uygulanabilir. İştirak halinde işlenip işlenmemesine göre TCK m. 36 veya m. 41 uygulanabilecektir.

## **D. İŞTİRAK**

İştirak açısından bir özellik göstermemektedir. İştirak şekilleri gerçekleşebilir ve TCK'nın 37 vd. maddeleri uygulanabilir.

## **E. İÇTİMA**

---

<sup>102</sup> Soyaslan, s. 666.

Sahte banka veya kredi kartı kullanarak yarar sağlamak suçunun zincirleme suç şeklinde işlenmesi mümkündür. Mağdur aynı olmak şartıyla sahte kartla değişik zamanlarda yarar sağlanması halinde zincirleme suç kuralları uygulanacaktır. Aynı kişi adına farklı bankalara ait birden fazla sahte banka veya kredi kartlarının değişik zamanlarda kullanılması halinde de zincirleme suç gerçekleşecektir. Ancak Yargıtay sahte kartların yarar sağlamada kullanılmasında mağduru banka olarak kabul ettiğinden aynı bankaya ait sahte kartın değişik zamanlarda kullanılmasında<sup>103</sup> veya aynı bankaya ait birden fazla sahte kartın kullanılarak yarar sağlanmasında<sup>104</sup> zincirleme suç hükümlerini uygulamaktadır. Farklı bankalara ait sahte banka veya kredi kartlarının kullanılarak yarar sağlanmasında zincirleme suçu kabul etmemektedir<sup>105</sup>.

Türk Ceza Kanununun 245. maddesinin 3. fıkrası yardımcı norm şeklinde düzenlenmiştir. Kanun koyucu söz konusu fıkra bu "fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde" ifadesiyle ortaya koymuştur. Dolayısıyla gerçekleştirilen eylem, daha ağır cezayı gerektiren başka bir suç oluşturduğunda yardımcı norm TCK m. 245/3 uygulanmayacak, daha ağır cezayı gerektiren asıl norm uygulanacaktır. Doktrinde akla gelen suçlardan birinin dolandırıcılık<sup>106</sup>, diğerinin özel belgede sahtecilik suçu<sup>107</sup> olduğu belirtilmektedir. Ancak sahte kartların kullanılarak yarar sağlanmasında özel belgede sahtecilik suçunun oluşmayacağını ifade etmeliyiz. Dolandırıcılık suçunun oluşabileceğini, ancak nitelikli şeklinin cezasının bile TCK m. 245/3'deki cezadan az olması nedeniyle dolandırıcılık suçunun değil, sahte banka veya kredi kartı kullanarak yarar sağlama suçunun uygulanacağı belirtilmiştir. Dolandırıcılık suçunun yardımcı norm

<sup>103</sup> "Sanığın, başka bir kişiye ait nüfus cüzdanına kendi resmini yapıştırıp, bu nüfus cüzdanıyla bankaya müracaat ederek kredili mevduat hesabı başvuru formu imzalayıp bankaya sahte banka kartı ürettirmesi eyleminin kül halinde banka veya kredi kartlarının kötüye kullanılması ve zincirleme suç hükümlerine ilişkin maddelere uyduğu gözetilmelidir", 8. CD, 02.03.2015, E. 2014/27246, K. 2015/12807; "Sanığın başkasına ait kimlik bilgilerini kullanarak katılan bankadan kredi kartı alarak değişik zamanlarda birden çok kez kullanmak eyleminin TCK.nun 245/2, 245/3, 43. maddelerinde düzenlenen suçları ayrı ayrı oluşturacağı gözetilmeden yazılı şekilde resmi evrakta sahtecilik suçundan açılan davada beraatine karar verilip, TCK.nun 245/3. maddesinden kurulan hükümde tayin edilen cezanın TCK.nun 43. maddesi gereğince arttırılmaması, yasaya aykırıdır", 8. CD, 03.02.2015, E. 2014/36395, K. 2015/2260, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.22.03.2017).

<sup>104</sup> "Sahte banka veya kredi kartı üretme, kabul etme ve sahte oluşturulmuş banka veya kredi kartı ile ATM cihazından para çekme ya da alışveriş yapma eylemlerinin mağduru, kredi ya da banka kartını üreten banka veya finans kuruluşu olması nedeniyle, kartı çıkaran banka sayısınca ve aynı bankaya ait birden fazla sahte kart kullanılması halinde ise, kendi içerisinde zincirleme şekilde T.C.K.nun 245/2. ve 245/3. madde ve fıkralarında düzenlenen suçların oluşacağı", 8. CD, 12.05.2015, E. 2014/29393, K. 2015/17026, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.22.03.2017).

<sup>105</sup> "kartları değişik zamanlar- da kullanarak alışveriş yapmak suretiyle yarar sağlaması halinde ise, aynı Kanunun 245/3., 43. madde ve fıkralarındaki birbirinden bağımsız ayrı ayrı suçları oluşturacağı dikkate alınarak hükümler kurulması gerekirken, eksik incelemeye dayanarak dört bankaya yönelik sahte kredi kartı üretmek ve kullanmak şeklinde gerçekleşen eylemler kül halinde değerlendirilerek, zincirleme suretiyle işlenen T.C.K.nun 245/3. maddesi uyarınca karar verilmesi isabetsizdir", 8. CD, 21.05.2015, E. 2014/32263, K. 2015/17388, [www.kazanci.com.tr](http://www.kazanci.com.tr) (E.T.22.03.2017).

<sup>106</sup> Özbek/Doğan/Bacaksız/Tepe, s. 1030; Koca/Üzülmez, s. 911.

<sup>107</sup> Özbek/Doğan/Bacaksız/Tepe, s. 1030.

niteliğinde olduğu söylenmiştir<sup>108</sup>. Ancak 24.11.2016 tarihinde 158. maddede yapılan 6763 sayılı değişiklikle dolandırıcılık suçunun nitelikli şeklinin kapsamına giren bazı hallerde hapis cezasının alt sınırı m. 245/3'deki suçun cezasıyla aynı olmuş, 158. maddeye 24.11.2016 tarihinde 6763 sayılı Kanunla eklenen eklenen 3. fıkrayla da bazı hallerde nitelikli halin cezasının m. 245/3'den fazla şekilde belirlenmiştir. Bu fıkraya göre, "bu madde ile 157 nci maddede yer alan suçların, üç veya daha fazla kişi tarafından birlikte işlenmesi hâlinde verilecek ceza yarı oranında; suç işlemek için teşkil edilmiş bir örgütün faaliyeti çerçevesinde işlenmesi hâlinde verilecek ceza bir kat artırılır".

Failin hem m. 245/3'ü hem de 245/2'yi ihlal etmesi halinde sorumluluğun ne şekilde belirleneceği daha önce de belirtildiği gibi tartışmalı olup, daha önceki açıklamalara bakılmalıdır.

Fail m. 245/A kapsamında bir cihazı ürettikten, bunu sahte kart üretmede kullanmış, ayrıca bu sahte kartı kullanarak yarar sağlamışsa hem m. 245/A'dan hem de m. 245/2'den hem de m. 245/3'den ayrı ayrı sorumlu olacaktır.

#### **F. YAPTIRIM**

Türk Ceza Kanununun 245. maddesinin 3. fıkrasındaki suçun cezası, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası olarak öngörülmüştür. Kanun koyucu yarar sağlamak suretiyle ekonomik kazanç sağlandığından hapis cezasının yanında adli para cezasının verilmesini de öngörmüştür. Adli para cezasında alt sınır öngörülmediğinden alt sınır TCK'nın 52. maddesi gereğince 5 gün olarak kabul edilecektir.

Suçun tüzel kişi yararına işlenmesi halinde haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur (TCK m. 246). Kanun koyucu, TCK'nın 245. maddesinin 1. fıkrası için kabul ettiği şahsi cezasızlık sebebi ile etkin pişmanlık hükümlerinin uygulanmasını TCK m. 245/3 için kabul etmemiştir.

#### **G. SORUŞTURMA VE KOVUŞTURMA**

Türk Ceza Kanununun 245. maddesinin 3. fıkrasında yer alan suç, resen takip edilen suçlardandır. Görevli mahkeme, Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 11. ve 12. maddeleri gereğince asliye ceza mahkemesidir. Yetkili mahkeme ise 245. maddenin 3. fıkrasında yer alan kullanmanın gerçekleştirildiği yer ile yararın sağlandığı yer mahkemeleridir. İnternet üzerinden failin işlendiği hallerde kişinin beden olarak bulunduğu yer ile hareketin açığa çıktığı yer de suçun işlendiği yer olacaktır. Ülke içinde işlenen suçlarda zincirleme suç veya teşebbüs söz konusuysa CMK m. 12/2

---

<sup>108</sup> Özbek/Doğan/Bacaksız/Tepe, s. 1030. TCK m. 245/3'ün uygulanması gerektiğine ilişkin olarak bkz.: Koca/Üzülmez, s. 870.

gereğince yetkili mahkeme belirlenecektir. Suç yabancı ülkede işlenmiş ve Türkiye’de yargılama yapılmasının mümkün olduğu hallerde yetkili mahkeme CMK m. 14 gereğince belirlenecektir.

### SONUÇ

TCK’nın 245/1. maddesinde başkasına ait bir banka veya kredi kartını, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak yarar sağlanması cezalandırılmıştır. Düzenleme yalnızca banka veya kredi kartlarıyla ilgili yapılmıştır. Bunun eksiklik olduğu belirtilmelidir. Yalnızca banka veya kredi kartlarıyla değil, tüm kartlarla ilgili düzenleme yapma yolunun tercih edilmesi gerekir. Uygulamada TCK m. 244/4’ün, hırsızlığa ilişkin TCK m. 142/2-e’nin ve TCK m. 245/1’in tatbik edilmesinde sorun olduğunu düşünmekteyiz. Kontör yüklemeye veya diğer kartların (telefon kartları gibi) kullanılmasıyla çıkar sağlamaya m. 244/4 uygulandığında 2 yıldan altı yıla kadar hapis cezası söz konusu olacakken, internet aracılığıyla havale yapılmasına 142/2-e uygulandığında 5 yıldan 10 yıla kadar hapis cezası verilebilecektir. Ayrıca bilişim sistemi aracılığıyla haksız çıkar sağlamada beşbin güne kadar adli para cezası verilmesi gerekirken hırsızlık suçunda adli para cezasının uygulanması söz konusu değildir. Banka veya kredi kartını kullanmak suretiyle para alındığında ise kişinin cezası 3 yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasıdır (TCK m. 245). Ancak bir hesaptan başka bir hesaba para aktarmak suretiyle fiil işlendiğinde 5 yıldan 10 yıla kadar hapis cezasının verilmesi söz konudur. Uygulamada yaşanan bu sorunun giderilmesi için düzenlemede değişikliğe gidilmesi gerektiğini düşünmekteyiz.

Türk Ceza Kanununun 245/2. maddesinde düzenlenen sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçu açısından da düzenlemenin yalnızca banka veya kredi kartlarıyla ilgili olması eleştirilmelidir. Kullanılan diğer kartlarla ilgili de sahtecilik fiilinin düzenlenmesi gerekir. Aslında kanunumuzda verilerde sahtecilikle ilgili düzenleme yapılması gerekir. Bunun dışında cezalardaki problem bu suç açısından da bulunmaktadır. Özel belgede sahtecilik suçuyla m. 245/2 ve 244/2 arasında sorun bulunmaktadır.

Türk Ceza Kanununun 245. maddesinin 3. fıkrasında hükme bağlanan sahte banka veya kredi kartını kullanarak yarar sağlamak suçunda, sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak cezalandırılmaktadır. Failin hem m. 245/3’ü hem de 245/2’yi ihlal etmesi halinde sorumluluğun ne şekilde belirleneceği tartışmalıdır. Biz failin her iki fiilden ayrı ayrı cezalandırılması görüşüne katılmaktayız.

## KAYNAKÇA

**Akbulut, Berrin**, Bilişim Alanında Suçlar, 2. Baskı, Ankara 2017.

**Artuk, M. Emin/Gökçen, Ahmet/Yenidünya, A. Caner**, Ceza Hukuku, Özel Hükümler, 15. Baskı, Ankara 2015.

**Cihan, Erol**, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 77.

**Dönmezer, Sulhi**, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 41.

**Dönmezer, Sulhi**, Kişilere ve Mala Karşı Cürümler, 16. Bası, İstanbul 2001.

**Dreher, Eduard/Tröndle, Herbert**, Strafgesetzbuch und Nebengesetze, Kommentar, 47., neubearbeitete Auflage des von Otto Schwarz begründeten Werkes, München 1995.

**Ekinci, Mustafa/Esen, Sinan**, Anlatımlı ve Gerekçeli Yeni Türk Ceza Kanununda Yer Alan Hırsızlık Yağma Güveni Kötüye Kul-lanma Dolandırıcılık Hileli ve Taksirli İflas Karşılıksız Yararlanma Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Ankara 2005.

**Erdem, Mustafa Ruhan/Özbek, Veli Özer**, “Ceza Hukuku Açısından Bankamatiklerin Kötüye Kullanılması”, İzmir Barosu Dergisi, 1997, s. 58 – 86.

**Erman, Sahir**, “Devletin Ekonomik İtibarını Sarsma Açığa Atılan İmzanın Kötüye Kullanılması Hileli Taksiratlı İflas”, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 25-36.

**Gropp, Walter**, Strafrecht, Allgemeiner Teil, 3. Auflage, Berlin Heidelberg 2005.

**Gül, Ahmet**, Doğrudan Dolaylı Bilişim Suçları, Ankara 2016.

**Hecker, Bernd**, “Die Strafbarkeit des Ablistens oder Abnötigens der persönlichen Geheimnummer”, JA, 1998, Heft 4, s. 300-306.

**Helmann, Uwe**, “Der praktische Fall - Strafrecht: Überfall am Geldautomaten”, JuS, 1996, Heft 6, s. 522-529.

**Karagülmez, Ali**, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara 2005.

**Koca, Mahmut/Üzülmez, İlhan**, Türk Ceza Hukuku, Özel Hükümler, 5. Baskı, Ankara 2018.

**Mahmutoğlu, Fatih Selami**, “Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, İÜHFİM, 2013, C. LXXI, S. 1, s. 857-889.

**Meran, Necati**, Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar, Ankara 2005.

**Okuyucu-Ergün, Güneş**, “Banka veya Kredi Kartlarının Kötüye Kullanılması (Abuse of Bank or Credit Cards)”, Prof. Dr. Nur Centel’e Armağan, 2013, C. 19, S. 2, s. 1065-1086.

**Özbek, Veli Özer**, “Banka veya Kredi Kartlarının Kötüye Kullanılması suçu (TCK m.245)”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 9, Özel Sayı 2007, s. 1019-1063.

**Özbek, Veli Özer/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker**, Türk Ceza Hukuku, Özel Hükümler, 13. Baskı, Ankara 2018.

**Schönke, Adolf/Schröder, Horst/Lenckner, Theodor/Cramer, Peter/Stree, Walter**, Strafgesetzbuch, Kommentar, 28., neubearbeitete Auflage von Eser, Albin/Heine, Günter/Perron, Walter/Sternberg Lieben, Detlev/Eisele, Jörg/Bosch, Nikolaus/Hecker, Bernd/Kinzig, Jörg/Schittenhelm, Ulrike, München 2010.

**Soyaslan, Doğan**, Ceza Hukuku, Özel Hükümler, Güncelleştirilmiş 11. Baskı, Ankara 2016.

**Taner, Fahri Gökçen**, “Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu Bir Bileşik Suç mudur?”, AÜHFD, 2007, C. 56, S. 2, s. 75-81.

**Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, Murat**, Teorik ve Pratik Ceza Özel Hukuku, Güncellenmiş 16. Baskı, Ankara 2018.

**Tröndle, Herbert/Fischer, Thomas**, Strafgesetzbuch und Nebengesetze, 53. Auflage, München 2006.

**Wessels, Johannes/Hillenkamp, Thomas**, (Çev.: Yener Ünver), “Hırsızlık ve Güveni Kötüye Kullanma Suçları”, Malvarlığına Karşı Suçlar ve Ekonomik Suçluluk, Karşılaştırmalı Güncel Ceza Hukuku Serisi 9, Prof. Dr. Eric Hilgendorf’a Armağan, Ankara 2009, s. s. 15-75.

**Yarsuvat, Duygun**, “Kamuya Gerekli Şeylerin Yokluğuna Sebebiyet Vermek Gıda Maddeleriyle Kamuya Gerekli Madde ve Eşyanın Noksanlığına Sebebiyet Vermek Suçları”, Ekonomik Suçlar ve Ceza Kanunu Öntasarısı Sempozyumu (17-18 Nisan 1987), İstanbul 1987, s. 63-73.

**Yılmaz, Sacit**, “Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu”, TBBD, Sayı 87, 2010, s. 262-298.

## KONKORDATODA ALACAKLILAR KURULU <sup>109</sup>

**Prof. Dr. Meral Sungurtekin ÖZKAN**

### **Anahtar kelimeler :**

alacaklı- borçlu menfaat dengesi-iflas- konkordato-ölçülülük ilkesi- kamu yararı- alacaklılar kurulu-iyileştirme

### **ÖZET**

Ticari yaşamda özellikle son yıllarda sıkça yaşanan adi olsun malvarlığının terki suretiyle olsun konkordato süreçlerinde, alacaklıların menfaatlerinin hukuk devleti ilkesi doğrultusunda korunması da en az borçlu menfaatlerinin korunması kadar önem taşır hale gelmiştir. Bu sebeple alacaklıların menfaatlerinin korunmasıyla doğrudan bağlantılı olan alacaklılar kurulu, yapısal ve işlevsel olarak ele alındığı gibi; hukuki niteliği, yükümlülük ve yetkileri ile sorumluluğu bakımından da ele alınarak değerlendirilmiştir. Kaynak İsviçre İİK' na ve zaman zaman da Alman Acz Kanununa(InsO) değinilmiştir. Konkordato, alacaklının ve borçlunun yararını gözettiği gibi kamunun da yararını gözetmek durumunda olan ve iflasa benzemekle beraber; ona oranla özel ve daha hafif bir cebri icra türü, kollektif bir tasfiye usulüdür. Gerek adi konkordatoda gerekse malvarlığının terki suretiyle konkordatoda, İcra ve İflas Kanunumuz alacaklılar kuruluna dair ayrıntılı denilebilecek düzenlemeleriyle, bu süreçte alacaklı- borçlu menfaat dengesini temin amacına uygun davranarak kamu yararını da gözetken bir tavır sergilemiştir.

### **BOARD OF CREDITORS IN THE CONTEXT OF PROTECTING THE INTERESTS OF CREDITORS IN COMPOSITION WITH CREDITORS PROCEEDINGS**

#### **Keywords:**

Balance between the interests of creditor – debtor, bankruptcy, composition with creditors, principle of proportionality, public interest, board of creditors, restoration.

#### **Abstract**

---

<sup>109</sup> ORCID: <https://orcid.org/0000-0001-7159-0421>



In commercial life, especially in a process of composition with creditors, protecting the interests of the creditors in accordance with the rule of law principle is as important as protecting the interests of the debtor.

Because of this reason, in order to examine this issue, the board of creditors is addressed in terms of its structure, functions, legal nature, powers and responsibilities. Similar institutions that are regulated in Swiss Debt Enforcement and Bankruptcy Code and German Insolvency Code are also analyzed.

It should not be overlooked that composition of creditors is a collective liquidation procedure as bankruptcy in which the interests of creditor, debtor and public. However, composition of creditors procedure is also a special and lighter type of compulsory enforcement than bankruptcy.

In every type of composition of creditors, it is important and necessary to act in a manner in which a balance between the interests of creditors and the debtor is created and public interests are protected by regulating the board of creditors in a detailed way in Debt Enforcement and Bankruptcy Code.

## GİRİŞ

Ekonomik yaşam ve hukuk içiçe geçmiş kavramlar olarak birbirine karşılıklı etkide bulunur. Ekonomik gidişata bağlı olarak iflasların gündeme gelişi, bunların da toplumsal yaşamda işsizlik başta olmak üzere ekonomik durgunluğa bağlı olarak bazı psikososyal sorunlar ortaya çıkardığı bir gerçektir. Bu negatif toplumsal etkilerin ortaya çıkmasının önlenmesini de sağlayabilmek adına konkordato denilen özellikle adi konkordato dediğimiz kurum, 7101 sayılı kanunla, İİK'nun adi konkordatoya dair hükümleri değişikliğe uğratarak vadesi gelmiş borçlarını ödeyemeyen ya da ödeyememe tehlikesi altında bulunan borçluların yararlanabileceği bir kurum olarak yeniden düzenlenmiştir. Ekonomi ile hukuk kuralları ilişkisi, konu bağlamında özel önemdedir. Bu anlamda hukuk kuralları getirilirken piyasalardaki arz- talep dengesinin temini, alacaklı/lar- borçlu menfaat dengelemesinin gerçekleştirilmesi, kamu yararının sağlanması gibi hususlar yasa koyucunun dikkate almak durumunda olduğu temel hususlardır. Ekonomik problemlerin çözümü ekonomik alandaki tedbir ve yapısal değişikliklerle sağlanacak olup; hukuk ancak bazı olumsuz etkileri bertaraf etmeye kısıtlı olarak yardımcı olabilir. Dolayısıyla hukuk, ancak evrensel bazı hukuk ilkelerini göz ardı etmeksizin, ekonomiye dair sıkıntıların yarattığı sorunların aşılması konusunda kurallar getirerek bir ölçüde katkı sağlayabilir. Bu makale,

konkordato konusunda getirilmiş yasal düzenlemelerle yapılmış değişiklikleri 4949 sayılı kanunla malvarlığının terki suretiyle konkordatoda düzenlenmiş olan vey akın zamanda da 7100 sayılı kanunla adi konkordatoda yasal zemine kavuşturulmuş olan **alacaklılar kurulunu**, varlık ve işlevini bu bakış açısıyla irdelemektedir.

## I. KONKORDATO HAKKINDA GENEL BİLGİ

Konkordatonun tanım ve amacı ortaya konulduktan sonra alacaklılar kurulu üzerinde çalışmak daha yerinde olacaktır. Zira konkordatonun ne olduğu ve hukuki niteliği saptandıktan sonra, organ olarak alacaklılar kurulunun amaç ve işlevinin ne olduğunun belirlenmesi, çok daha anlaşılır olmasını sağlayacaktır. Konkordato, alacaklının ve borçlunun yararını gözettiği gibi kamunun da yararını gözetmek durumunda olan, iflasa benzemekle beraber ona oranla özel ve daha hafif bir cebri icra türü ve kollektif tasfiye usulüdür<sup>110</sup>. Olumsuz oy kullanan alacaklılar bakımından da bağlayıcılığı bulunması ve mutlaka resmi organların katılımının gerekmesi, keza konkordatonun kısmen veya tamamen feshinin İcra ve İflas Kanununda düzenlenmiş olması da onun bir cebri icra kurumu olduğunu ve cebri icra ilkelerinin göz önünde bulundurulmak gerekliliğini ortaya koyar<sup>111</sup>.

Konkordato, vadesi geldiği halde ödeyememe durumunda olan ya da vadesinde ödeyememe tehlikesi altında bulunan herhangi bir borçlunun, vade verilmek veya tenzilat yapılmak ya da her ikisi de kullanılarak borçlarını ödeyebilmek için uygun koşullar altında yeniden yapılandırılabilmesi, mali durumunu düzeltebilmesi ya da iflasa tabi bir borçlu ise, olası bir iflastan kurtulabilmesine imkan sağlayan, iflasa oranla özel ve kollektif bir icra iflas hukuku kurumudur. Borçlunun bir proje ile yapmış olduğu teklif, İİK. m.302’deki nitelikli çoğunluk teşkil eden

---

110 Türk – İsviçre hukuklarında baskın olan bu görüşe göre tek başına alacaklılar çoğunluğunun iradelerinin diğer taraftan borçlunun iradesi veya mahkeme kararı yeterli değildir. İflasa alternatif olan konkordatoda alacaklılar ile borçlunun çıkarları ile kamu yararı gözetilir. Konkordatonun hukuki niteliği için ayrıntılı bilgi için **ÖZTEK, S.** Yeni Konkordato Hukuku, 2. Bası, 2019, s. 140 (**BUDAK, A.C., TUNÇ YÜCEL, M., KALE, S., YEŞİLOVA, B., ERCAN, I.** İcra ve İflas Hukukunda Malvarlığının Terki Suretiyle Konkordato, Konya 2008, s. 157 vd.; Esasen değişik konkordato tanımları için bkz. **PEKCANİTEZ, H./ERDÖNMEZ, G.** : 7101 sayılı Kanun Çerçevesinde Konkordato, 2018, s. 7 vd., 4-5 **POSTACIOĞLU, İ.** Konkordato, İstanbul 1965, s.12, **KURU, B.** İcra Ve İflas Hukuku Elkitabı, 2. Bası 2013, s. 1444; **YILDIRIM, M.K./DEREN YILDIRIM, N.** İcra ve İflas Hukuku, İstanbul 2015, s. 504, **PEKCANİTEZ/ATALAY/SUNGURTEKİN ÖZKAN/ÖZEKES,** İcra ve İflas Hukuku, Dersi kitabı, 5. Bası İstanbul 2018, s. 441, **TANRIVER, S.** Konkordato Komiseri, Ankara 1993, s.6-7; **UYAR, T.** Yeni Konkordato Hukuku, Ankara 2019, s. 13

111 ERCAN, s.160; Ayrıca bkz. **TAŞPINAR AYVAZ, S.** Adi konkordato hakkında İcra ve İflas Kanununda yapılan değişiklikler, **BATIDER**, Aralık 2003, C.XXII, S.2, s.49-50; **TANRIVER/DEYNEKLİ,** Konkordatonun Tasdiki, Ankara 1996, s. 29 : “kanunda öngörülen belirli şartların yerine getirilmesi halinde borçlunun vadesi geldiği halde ödeyemeyen veya vadesinde ödeyememe tehlikesi altında bulunan herhangi bir borçlu, vade verilmek veya indirim yapılmak suretiyle borçlarını ödeyebilmek veya muhtemel bir iflastan kurtulmak için sunulan bir proje ile başlayan kendine özgü bir cebri icra kurumudur”

alacaklılar tarafından kabul edilerek yetkili mahkemece tasdik olunarak, iflasa tabi bir borçlu ise, olası bir iflastan da kurtulabildiği bu süreçte, borçlu karşısında alacaklılar menfaati/lerinin korunması, hukuk devleti olmanın kaçınılmaz bir gereğidir. Bu amaca hizmet edecek kurumlardan biri belki de en önemlisi de alacaklılar kuruludur.

Malvarlığının terki suretiyle konkordato ise, değişik türleri bulunmakla beraber; borçlunun, alacaklılarına terk ettiği malvarlığının (kısmen ya da tamamıyla terk etmiş olabilir) paraya çevrilmesi suretiyle borçlarının ödenmesinin sağlandığı bir kollektif tasfiye usulü olup; iflasa oranla etkileri daha hafif bir cebri icra kurumudur<sup>112</sup>. Malvarlığının terki suretiyle konkordato, alacaklılarla tasfiye anlaşması şeklinde olabileceği gibi yeni şirket kurarak<sup>113</sup> ya da malvarlığının üçüncü bir kişiye devri suretiyle gerçekleştirilebilir<sup>114</sup>. Adi konkordato ve malvarlığının terki suretiyle konkordato arasındaki farklılıkları ortaya koymanın, alacaklılar kurulunun işlevini tespit noktasında da önemli olabilecektir.

Malvarlığının terki suretiyle konkordatoda, adi konkordatodan farklı olarak konkordatoyu talep eden borçlunun tacir olması, tacir sayılması vs. yani iflasa tabi kişi olması gereklidir. Adi (tenzilata yönelik) konkordato talebi bakımından baştan bir teklif söz konusu olduğu için bu teklifin borçlunun kaynakları ile orantılı olması önem taşır. Oysa malvarlığının terki suretiyle konkordato, baştan talepte bulunanın teklifiyle başlamadığından, talepte bulunan iflasa tabi borçlunun kaynakları ile orantılı olması da gerekmez<sup>115</sup>. Bu tür konkordatoda, malvarlığının tümü ya da bir kısmını iflasa tabi borçlu, alacaklılarına terk etmekte ve bunlar alacaklıları tarafından paraya çevrilerek elde edilen miktardan alacaklılar, alacaklarını tahsil etmektedirler. Dolayısıyla borçların ne kadarının karşılanacağı başlangıçta belli değildir. Bu yüzden adi konkordatonun aksine borçlunun malvarlığı üzerinde tasarruf etme yetkisi tamamen kalkmaktadır; alacaklılarına geçmektedir<sup>116</sup>. Alacaklıların alacaklarına ne oranda kavuşacakları hususundaki belirsizliğin bir dengeleyicisi olarak borçlunun malvarlığı üzerinde tasarruf etme yetkisinin alacaklılarına geçmesi

---

112 Malvarlığının terki suretiyle konkordato ile de borçlunun malvarlığının kısmen veya tamamen tasfiyesi sonucu doğduğundan, iflasın daha hafif bir hali olarak ifade edilmektedir. **WIDMER**, "Der Nachlassvertrag, eine Rechtswohlthat Festschrift 100 Jahre SchKG, Zürich 1989, S.391, 395; ayrıntılı bilgi için bkz. **ERCAN**, s. 165-169. Tasdik aşamasına kadar adi konkordato hükümlerine tabi olmakla beraber, tasdikten sonrası iflasa benzer nitelik arz etmektedir. Ancak İİK'nda tasfiyenin nasıl yapılabileceği düzenlenmiştir.

113 **ERCAN**, s. 111-121

114 **ERCAN**, s. 121-127.

115 Diğer farklar hakkında bkz. **ERCAN**, s. 142-143.

116 Tasfiye anlaşması şeklinde olan malvarlığının terki suretiyle konkordato, daha ziyade iflasa benzediğinden, adi konkordatodan farklılık çok daha barizdir. Burada amaç borçlunun malvarlığının paraya çevrilmesi suretiyle alacaklılara en yüksek oranda ve hızlı biçimde alacaklarını temindir. Sıra cetveli çerçevesinde dağıtım yapılacaktır. İmtiyazlı olup olmadıklarına göre alacaklıların alacaklarına kavuşacaktır. Malvarlığının terki suretiyle konkordatoda, borçludan çok alacaklılar korunmaktadır(**ERCAN**, s. 129 vd.)

söz konusudur. Bu suretle bir menfaat dengelemesi de yapılmıştır. Alacaklılar da bu tasarruf etme yetkisini, seçtikleri tasfiye memurları eliyle kullanırlar. Tasfiye memurları, ihale- satış-satış ilanları vs. ile ilgili olarak İİK hükümleriyle bağlı değildir<sup>117</sup>.

Adi konkordatoda da, borçlu menfaatlerinin korunmasının yanında alacaklıların menfaatlerinin de ölçülülük ve hukuk devleti ilkelerinden ödün verilmeksizin temininin amaçlandığı ifade edilmelidir. Öğretide<sup>118</sup>, “yeni konkordato hukuku borçlunun menfaatleri ile alacaklıların menfaatleri arasında daha iyi bir denge kurmaya gayret eden ve hakime de mühlet kararı verirken genel ve hatta bölgesel ekonomik yararı gözetme imkanı veren bir yolda ilerlemektedir ve halihazır durumda gelişimini tamamladığını söylemek de mümkün değildir” ifadesine rastlamaktayız.

## **II. ALACAKLILAR KURULUNUN HUKUKİ DAYANAĞI, AMACI VE NİTELİĞİ**

### **A. ALACAKLILAR KURULUNUN HUKUKİ TEMELİ VE KONUYLA İLGİLİ DÜZENLEMELER**

İcra ve İflas Kanunu, gerek adi konkordato; gerekse malvarlığının terki suretiyle konkordatoda, alacaklılar kuruluna dair ayrıntılı denilebilecek düzenlemelerle, süreçte alacaklı- borçlu menfaat dengesini temin amacına uygun olarak, hem ismen hem de yapısal ve işlevsel olarak alacaklılar kurulunu düzenlemiş; bu suretle kamu yararını da gözetten bir tavır sergilemiştir. Konkordatoda alacaklılar kurulunun oluşturulması bakımından Türk- İsviçre hukuklarındaki hükümlerden geçici mühlet verilmesi esnasında alacaklılar kurulunun sürece dahil edilmesi söz konusu değildir<sup>119</sup>.

Konkordatoyu iflas sürecinden ayırıştıran en temel husus, iflasta alacaklarını tamamen elde edememiş olan alacaklıların bakiyeyi bilahare elde edebilme imkanına (İİK.m. 255) konkordatodaki durumun aksine sahip olmalarıdır. Konkordatoda, bakiyeyi elde edebilmek bakımından takip vs. yolları kullanabilmek mümkün değildir. Bu yüzden alacaklıları konkordato sürecine çok daha etkin olarak dahil etmek, onların aktif ve sorgulayan konumda olmalarını sağlamak ve güçlü kılınmaları, özellikle konkordatonun salt tasfiye prosedürü olmadığı; yeniden yapılandırma amacıyla da başvurulabildiği düşünüldüğünde gereklidir.

Türk hukukunda iflasta bir alacaklılar kurulunun düzenlenmemiş olduğu bunun da esasen bir eksiklik olarak değerlendirilmesi gerektiği yönündeki düşüncemizi de yeri gelmişken paylaşmakta yarar görmekteyiz.

---

117 Ayrıntılı bilgi için **ERCAN**, s. 53-140

118 İcra ve İflas Kanununda Değişiklikler üzerinde çalışan Bilim Komisyonunun Başkanı olan Sayın Prof. Dr. ÖZTEK’ in editörlüğünde hazırlanmış Yeni Konkordato Hukuku, **ÖZTEK**, s. 141, dn. 14 civarı

119 **BÖRÜ, L.** “Adi Konkordatoda Alacaklılar Kurulu”, İnÜHD C. IX, S.2, 2018 s. 346 vd.

7101 sayılı Kanunla yapılan değişiklikler öncesi, ne adi konkordatoda ne iflas ertelemesinde alacaklılar kurulu bulunmaktaydı. 7101 sayılı Kanunla getirilinceye kadar adi konkordatoda ve iflas ertelemesinde alacaklılar kurulunun bulunmayışı, ciddi bir eksiklikti. Yasa koyucu da bu eksikliği saptayarak varlığı gerekli bu organı düzenlemiştir<sup>120</sup>. Türk kanun koyucusunun ilk olarak malvarlığının terki suretiyle konkordatoda 4949 sayılı kanun değişiklikleriyle hukuk sistemimize m. 309a ile düzenleme yaparak soktuğu bu özel organın<sup>121</sup>, adi konkordatoda yarı resmi bir organ olarak yasal zemine kavuşturulmuş olması, olumlu ve önemli bir adım olmuştur. Ancak alacaklılar kurulunun oluşturulması, Türk- İsviçre hukuklarında geçici mühlet verilmesi esnasında değil; kesin mühlet verilirken planlanmış ve düzenlenmiştir<sup>122</sup>. Alacaklılar kurulu, 7101 sayılı kanunla özellikle 289 vd. maddelerde ve “Konkordato Komiserliği ve Alacaklılar Kuruluna Dair Yönetmelik”<sup>123</sup> m.21-24 ile düzenlenmiştir. Adi konkordatoda alacaklılar kurulu, kural olarak mahkemenin takdiri ile kesin mühlet verilirken oluşturulmaktadır. Yani kural olarak ihtiyari bir organdır.

Adi konkordato sürecinde mahkemece, malvarlığının terki suretiyle konkordatoda ise, alacaklılar toplanmasında oluşturulan alacaklılar kurulu, alacaklı/lar menfaatlerinin korunmasında önemli bir rol oynar.

Kaynak İsviçre İİK. m. 237, iflas tasfiyesine ilişkin hükümlerinde alacaklılar kurulunu düzenlemiştir; bu yolla iflas idaresi karşısında alacaklıların menfaatlerinin korunması amacıyla birinci alacaklılar toplantısı tarafından belirlenen bir organ olarak alacaklılar kurulunu vazetmiştir. Alacaklılar toplantısı iflas sürecinin başında ( Birinci) ve bir de sonunda ikinci alacaklılar toplantısı olarak mevcut olup; alacaklılar kurulu bulunması halinde, alacaklıların iflas idaresi ile çok daha iyi koordine olacağı ve çalışacağı bir gerçektir.

Alman Ödeme Güçlüğüne bağlı Külli Takip Kanunu’nda da 22.paragraftaki şartların bulunması halinde geçici alacaklılar kurulu dahi oluşturularak ödeme güçlüğüne dayalı külli takip sürecinin başında alacaklılara yeniden yapılandırmaya mı yoksa tasfiyeye mi gidileceği ya da borçlunun malvarlığının devrine mi gidileceği konusunda söz hakkı verilmiş bulunmaktadır. Esasen Almanya’da 2000 yılından beri yürürlükte olan Ödeme Güçlüğüne bağlı Külli Takip

---

120 İflas sürecinde alacaklıların, alacaklarını bilahare tahsil imkanının (m.255) bulunmakta olması sebebiyle, alacaklılar kurulunun bulunmayışı bir dereceye kadar katlanılabılır bir durum olarak değerlendirilebilir.

121 Tasfiye memurları ile birlikte, **konkordato hakkında karar veren alacaklılar tarafından alacaklılar kurulu** seçilmekte ve asliye ticaret mahkemesinin onayı ile göreve başlamaktadır.

122 BÖRÜ, s. 346 vd.;

123 RG **30.01.2019, S. 30671** Bu yönetmeliğin 25.maddesi ile **2/6/2018 tarihli 30439 sayılı RG’ de** yayımlanan Konkordato Komiserinin Niteliklerine Dair Yönetmelik **yürürlükten kaldırılmıştır.**

Kanunu (InsO) ile konkordato hükümleri kaldırılmış olduğundan külli takip planı söz konusu fonksiyonu yerine getirmektedir.

Çalışma konumuz konkordatoda alacaklılar kurulu ise de, kanımızca İİK' nunda değişiklikler yapılırken iflas sürecinde de alacaklılar kuruluna dair yasal düzenleme getirilmesi isabetli olurdu. Alacaklılar menfaatinin korunması ve alacaklı(lar)- borçlu menfaat dengesinin temini ve ölçülülük ile hukuk devleti ilkeleri, iflas sürecinde de alacaklılar kurulunun varlığını kabulü haklı kılmaktadır.

### **B. ALACAKLILAR KURULUNUN AMACI VE HUKUKİ NİTELİĞİ**

Konkordato borçluya sunulmuş çok önemli bir fırsat olmakla beraber; alacaklıların, tenzilat konkordatosunda alacaklarının bir kısmından vazgeçtikleri ya da vade konkordatosunda, alacağın tahsilini süreye yaydıkları düşünüldüğünde, alacaklıların haklarının korunmasının ve borçlular tarafından konkordato müessesesinin amacı dışında ve kötü niyetle kullanımının önlenmesi gereği anlaşılır. Her iki konkordato türünde de alacaklılar kurulu, alacaklı menfaatlerinin konkordato süreci boyunca korunması bakımından önemli bir role sahiptir.

Malvarlığının terki suretiyle konkordatoda alacaklılar kurulunun temel fonksiyonu, tasfiye memurlarının işlemlerini denetlemek olup; özel bir organ niteliğindedir. Bu kurul, tasfiye memurlarının paylaştırmaya ilişkin kararları hakkında yapılan itirazları inceler. Bu konuda verdiği kararlara karşı şikâyet yoluna başvurulabilir(m. 309/ç, II). Alacaklılar kurulu; paraya çevirmenin usûlü ve zamanını tasfiye memurlarının teklifi üzerine karara bağlar (m. 309/e, II). Tahsili güç ya da ihtilafli alacaktan, iptal davasından, borçlu veya çalışanlarına karşı sorumluluk davasından, alacaklılar kurulu vazgeçebilmektedir. Bu durumu bildirerek alacaklıları haberdar ederek bu iddiaların takibini 245. maddeye uygun olarak alacaklılara devretmeyi teklif edebilir<sup>124</sup>.

Alacaklılar kuruluna dair 7101 sayılı Kanunla getirilmiş yeni düzenlemeler, adi konkordato ile ilgili olup söz konusu değişikliklerle (İİK. m. 289/IV) ve ardından çıkarılmış bulunan Yönetmelikle, alacaklılar kurulu adi konkordato bakımından düzenlenmiştir. Malvarlığının terki suretiyle konkordatoda ise, daha önce 4949 sayılı kanunla zaten alacaklılar kuruluna dair düzenleme getirilmişti. 7101 sayılı Kanunla adi konkordatoda da konu düzenlenince, alacaklılar kurulu her iki tür konkordatoda da yasal zemine sahip hale gelmiş oldu.

---

124 Konkordato tasfiyesinin bir yıldan fazla sürmesi hâlinde ise, tasfiye memurları tarafından her yılın en geç aralık ayı sonuna kadar düzenlenen yıllık cetvel ve raporları, alacaklılar kurulu inceler; takip eden yılın şubat ayı sonuna kadar da alacaklıların incelemesine hazır bulundurulmak üzere, tasdik için ticaret mahkemesine gönderir. Tasfiye memurlarının verdiği cetvel ve raporu inceleyerek gerektiğinde, görülen eksikliklerin tamamlanmasını da alacaklılar kurulu tasfiye memurlarından isteyebilmektedir.

Konkordato ile mülkiyet hakkına müdahalede bulunulduğu düşünüldüğünde, hukuk devletinde temel haklara müdahalenin ancak kanunla ve ölçülülük ilkesine uygun olarak söz konusu olabileceği gerçeği çerçevesinde konuya yaklaşılması gereği de anlaşılır. “Konkordato kurumu, hem alacaklıların hem de borçlunun menfaatlerini temin eder şekilde işletilmelidir”. Temel hakka müdahalenin gerekli, elverişli, orantılı ve hakkaniyete uygun olmasını ifade eden ölçülülük ilkesi, alacaklıların temel haklarına (vade ya da tenzilat veyahut da her ikisi suretiyle) müdahalenin, bu ölçütlere uygun olarak gerçekleşip gerçekleşmediğinin gerektiğinde yargı organınca da denetlenebilir olmasını gerektirir. Nitekim adi konkordatoda ihtiyari organ olarak karşımıza çıkan alacaklılar kurulunun teşekkül ettirilip ettirilmeyeceği kararı mahkemece verilirken bu da dikkate alınması gereken hususlardandır. Kesin mühletin verilmesinin alacaklıların alacaklarına kavuşmaları bakımından doğuracağı risk ya da gecikme kurulun teşekkülünün ne denli gerekli olduğunu gösterir<sup>125</sup>

Alacaklılar kurulunun, yetkilerinin ve işleyişinin yasal olarak düzenlenmiş olması ve bu çerçevede hayata geçip geçmediği, bunun yargısal kontrolü, hukuk devleti ilkesinin de bir gereğidir. Bu kurula süreçte yer verilmesi konusundaki düzenleme bir taraftan; diğer İİK. m. 334 ile borçlunun konkordato müessesesini kötüye kullanması halinde, hakkında uygulanabilecek cezai yaptırım diğer taraftan keza m. 290 ile alacaklılar kurulu ve konkordato komiserinin görevlerinin ve sorumluluğunun ayrıntılı düzenlenmiş olması, konkordatoda alacaklı(lar)- borçlu menfaat dengelemesinin hukuk devleti ilkesine uygun olarak gerçekleştirilmesi amacı ve kurumun kötüye kullanımının engellenmesine dair önemli düzenlemelerdir. Zaten İcra ve İflas Kanununda kısmen ve tamamen fesih halleri düzenlenmiş olduğuna göre birkaç cümle önce ifade ettiğimiz hususların çok da önemli olmadığı kanımızca söylenemez. Zira konkordato kurumunun sadece borçlunun menfaatine hizmet eder şekilde algılanıp uygulama kazanmasının daha sürecin başından başlanarak önüne geçilmelidir.

İcra ve İflas Kanunundaki konkordato ile ilgili düzenlemelere bakıldığında, kanun yollarının bazı hallerde kapalı olduğu dikkati çeker. İİK. m. 293 ile, kesin mühlet talebinin kabulü ile mühletin kaldırılması talebinin reddine dair kararlara karşı kanun yolunu kapalı tutmuştur. Esasen alacaklılar kurulu vasıtasıyla konkordato sürecinde alacaklıların menfaatlerinin korunmasının amaçlandığı düşünüldüğünde kesin mühlet verilmesi ve kesin mühletin kaldırılması taleplerinin reddine dair kararlara karşı kanun yoluna başvurulabilmesi beklenirdi. Zira alacaklı

menfaatlerinin kesin mühletin kaldırılmasını, gerektirebileceği unutulmamalıdır.. Kesin mühletin kaldırılmasında hukuki yararı bulunan alacaklılar kurulunun bu kaldırma talebinin reddi kararına karşı kanun yoluna gidebilmesi gerekirdi. Öte taraftan aynı maddenin 2.fikrasında, konkordato talebinin reddi hakkındaki karara karşı borçlunun istinaf yoluna başvurabileceği belirtilmiştir. Ancak istinaf incelemesi sonucunda, “BAM’ nin verdiği karar ise kesindir” şeklinde düzenleme getirilmiştir. Kesin mühletin kaldırılması talebinin mahkemece reddi üzerine<sup>126</sup>, bu ret kararına karşı kanun yoluna gidilemeyeceğinin belirtilmesi, mahkemenin 291.madde çerçevesinde alacaklılar kurulunu davet ettikten sonra bu kararı verdiği düşünülse bile, konkordato talebi reddedilen borçlunun 10 gün içinde istinaf yoluna gidebildiği(m. 293/II) yasayla düzenlendiğine göre, istinaf imkanının her iki tarafa da eşit olarak sunulması uygun olurdu denilerek eleştirilebilir. Keza konkordato komiserini denetleyen alacaklılar kurulunun mahkemeden komiserin değiştirilmesini gerekçeli raporla istemesi halinde, borçlu ve komiser dinlendikten sonra mahkemece kesin karar verilmesi de alacaklılar kurulunun buna karşı kanun yoluna başvuramaması da alacaklı menfaatlerinin süreç boyunca korunması ilkesi ile ilgili samimiyeti şüpheli hale getirmektedir<sup>127</sup>.

### III. ALACAKLILAR KURULUNUN TEŞEKKÜLÜ

Hukukumuzda, Yönetmelikle getirilmiş alacaklılar kurulunun oluşturulmasının zorunlu olduğu hallerden söz edilmelidir. Bu haller dışında Türk hukukunda kurulun oluşturulması mahkemenin takdirindedir Kurul oluşturulmasının zorunlu olduğu haller, Yönetmelikte düzenlenmiştir. Kurulun varlığının zorunlu olduğu haller, konkordatonun, alacaklıların mülkiyet temel hakkına müdahale niteliğinden ötürü sınırlı olarak ve kanunla düzenlenmek gerekirken; sınırlı olarak ancak Yönetmelikle “en az üç alacaklı sınıfının söz konusu olduğu halde, alacaklı sayısı 250’den fazla ise ya da alacak miktarı 125 milyon liranın üzerinde ise, zorunlu olarak alacaklılar kurulu oluşturulur” şeklinde düzenlenmiştir.

İsviçre kanun koyucusu ise alacaklılar kurulunun teşekkülünü emreden somut durumları ortaya koymak yoluna gitmemiş; “şartların gerektirmesi halinde” ifadesini kullanarak alacaklılar

---

126 -ki bu konudaki karar alacaklıların menfaatlerini doğrudan ilgilendirmektedir- . Oysa alacaklılar kurulu buna karşı kanun yoluna gidebilme imkanına sahip olsaydı, söz konusu karar değiştirilerek alacaklıların menfaatlerinin korunmasının yasa koyucu tarafından gerçekten önemsendiği ve alacaklılar kurulunun etkin kılındığı düşünülebilirdi.

127 Benzer görüş için bkz. PEKCANİTEZ /ERDÖNMEZ, s. 82



kurulu teşekkülünün kural olmaması, istisna olarak bırakılmasını uygun bulmuştur. Şartları yoksa, mahkeme alacaklılar kurulu teşkili yoluna gitmeyecektir<sup>128</sup>.

Türk-İsviçre hukuklarında mahkemenin alacaklılar kurulu oluşturması, kural olarak kesin mühlet kararı verilmesiyle aynı zamana denk gelir. Mahkeme, somut olaydaki konkordatonun kapsam, önem ve karmaşıklığından yola çıkarak alacaklılar bakımından verilmek gereken kararların etkisini ve olası süresini hesaba katarak alacaklılar kurulu ile ilgili kararı vermelidir. Zira süreçte alacaklıların durumunu etkilemesi söz konusu olan kararlar, ne kadar yoğunsa, sürecin doğru yönetimi alacaklıların malvarlıklarını ne kadar kuvvetle ilgilendirmekteyse, alacaklılar kurulu vasıtasıyla konkordato sürecine etkin şekilde dahil olup işbirliği yapmak da, alacaklı menfaatleri ve kamu yararı bakımından o kadar önemli hale gelir. Para trafiğinin ve mevcudun durumu, tüm hesaplar ve belgelerin tetkiki ile tespit edilebildiğinden alacaklılar kurulunda bu işlerden anlayan kişi/kişiler bulunmalıdır. Bu suretle etkin ve verimli çalışan bir kurul söz konusu olabilir<sup>129</sup>.

Alacaklılar kurulu oluşturulması kararı, kesin mühlet kararıyla kural olarak aynı zamana denk gelmekle beraber, devam etmekte olan kesin mühlet içinde de ilgili şartlar değişmiş ve kurul tayini anlamlı olacaksa, bu zaman diliminde de ilk kez alacaklılar kurulu teşekkül ettirilebilir<sup>130</sup>. Mahkeme takdirinde olan hususlar, plan harici alacaklılar kurulunda genişlemeye gidilmesi ya da kurulu daraltma(küçültme) ya da şahıslarda değişiklik yapmak da olabilir. Uygun sebebin varlığı halinde görevden alma da ağırlıklı görüşe göre mahkemenin takdirindedir; ancak istisna kalmalı ve önemli sebebe dayanmalıdır. Ayrıca komiserin alacaklılar kurulunun teşkili hususunda dilekçe verip veremeyeceği de tartışmaya açık bir konudur. Bir görüşe göre<sup>131</sup> komiserin alacaklılar kuruluna şahıs tayinine dair dilekçe verme yetkisi bulunmaz.

Tüm alacaklılar kurulu üyeleri ya da bir kısmının yeniden belirlenmesi veya görevden alınması, devam etmekte olan kesin mühlet sürecinde de söz konusu olabilir. Alacaklılar kuruluna

---

128 İsviçre’de ilk kesin mühlet verilmesi esnasında daha ziyade alacaklılar kurulu teşekkülü söz konusudur (Art. 295a) İİK. m. 295a, kesin mühlet esnasında alacaklılar kurulunun teşekkül ettirilmesi gerekip gerekmediği hususundaki kararın, mahkemenin takdirinde olduğunu belirtmektedir (JAEGER, Kom. S. 1644, Rdnr.9) Ayrıca bkz. JAEGER, S.1663

129 JAEGER, Rdnr.13

130 JAEGER, S.1692, Rdnr. 6-7. İsviçre’de mühlet kararı verilirken, mahkeme, mühletin hedefinin iyileştirme mi yoksa tasfiyesi mi olduğu çerçevesinde, alacaklılar kurulunun teşekkül ettirilip ettirilmeyeceğine karar verir. İsviçre hukuk öğretisinde amaç değişikliğinin de mümkün olduğu belirtilmektedir. Amaç değişikliği konusunda borçlunun ve konkordato komiserinin mahkemeyi talep aranmaksızın bilgilendirmesi gerekir. Konkordato bakımından şartların yerine getirilmiş olup olmadığı ve buna göre kesin mühlet kararının verilebilmesi bakımından konkordatonun başanya ulaşmasının mümkün olduğunun anlaşılması gerekmektedir. Şartları bulunmamaktaysa, İsviçre’de kesin mühlet verilmesi kararına karşı konulabilmektedir (krş. İsv. İİK.m. 295b).

131 JAEGER, Kom. S.1702, Rdnr. 8

ilişkin olarak sonradan şahıs sayısının artışı ya da bu kurulu küçültmek veya şahıs değişimi gerçekleştirmek mahkemenin takdirindedir. Şüphesiz bu yönde bir ihtiyaç da söz konusu olabilir. Mahkemenin teşekkül ettirilmiş alacaklılar kurulunu tamamlayıp tamamlayamayacağı görevden alıp alamayacağı meselesi Kanunda düzenlenmiş değildir. Ancak mahkemenin geniş takdiri çerçevesinde uygun sebep bulunmak kaydıyla, kurulu görevden alması istisnaen de olsa mümkündür<sup>132</sup>.

Kesin mühlet esnasında mahkeme kendiliğinden alacaklılar kurulu teşekkülüne dair meseleyi tetkik eder. Uygulamada ise, bu konuyla ilgili olarak sürece dahil olanların, talepte bulunması ile mahkeme konu üzerinde çalışır. Talep sahibi olarak münferit alacaklılar veya alacaklı grupları görülür. Bu talebin borçludan ya da komiserden (tasfiyeciden ya da yöneticiden de) de gelmesine engel olan bir yasal düzenleme bulunmamaktadır. Mahkemenin alacaklılar kurulu teşekkül ve tayin kararına karşı gidilebilecek hukuki bir imkan bulunmamaktadır. Oysa kaynak İsviçre hukukunda, borçlu veya alacaklıların ZPO 319 anlamında hukuki imkana sahip bulunduğu (m. 295a/1 ve 295c) dikkati çekmektedir<sup>133</sup>. Hukukumuzda da kaynak İsviçre hukukunda olduğu gibi karara karşı itiraz ve sonuç vermemesi halinde de istinaf yoluna gidilebilmesi gerekirdi. Özellikle kurulun teşekkül tarzından menfaati haleldar olan alacaklı veya alacaklı sınıfı başta olmak üzere komiser ve duruma göre borçlu dahi böyle bir imkana sahip olmalıdır. 7101 sayılı Kanunda Kaynak kanunda olduğu gibi karara karşı konulabilmesine dair düzenleme getirilmeliydi<sup>134</sup>.

Alacaklılar kurulunun oluşturulması bakımından yetkinin Asliye Ticaret mahkemesinde olduğu anlaşılmalı beraber; özellikle yönetmelikte belirtilen halde “en az üç alacaklı sınıfının söz konusu olduğu halde alacaklı sayısı 250’den fazla ise ya da alacak miktarı 125 milyon liranın üzerinde ise” zorunlu olarak alacaklılar kurulu oluşturulur. Mahkeme, alacaklı sınıflarını hakkaniyet çerçevesinde tespit eder. Kurul oluşturulurken komiserin de görüşünün alınacağı kanunda düzenlenmiştir. Sadece konkordato komiserinin görüşünün alınacağı Kanunda(m. 289/IV) belirtildiğine göre alacaklı sınıfını temsil edecek olan şahsın belirlenmesi aşamasında temsil olunacak alacaklı kategorisinin görüşünün alınmayacağı sonucuna ulaşılmaması gerekir. Her bir alacaklı sınıfını temsil etmek üzere kurula üye (temsilcisi) belirlenirken örneğin «bankalar»

---

132 Bu şekilde görevden alma, sadece alacaklılar kurulu atamanın doğru olduğu şartların artık bulunmadığı; yani bugün olsa mahkeme alacaklılar kurulu teşekkül ettirmeyeceği durumların varlığını mutlaka gerektirmez. Alacaklılar kurulu teşekkülü hk.bkz. **JAEGER**,Rdnr. 10-12

133 Beschwerde imkanına sahip olduğu. Buna başvuruda miktar bakımından bir sınırlama da yoktur(**JAEGER**, Rdnr.9)

134 Alacaklılar kurulunun teşekkülü kararı, Asliye Ticaret Mahkemesince verildiğinden, İİK’ nun icra mahkemesi kararlarına karşı istinaf yolunu düzenleyen 363 vd.maddeleri uygulama alanı bulamaz.

kategorisini temsil edecek olanı tespitinde bu kategori alacaklılarından fikir alınması için mahiyetine uygun düşer. Kuruldakilerin sayısı 7'yi aşamayacaktır(m. 289/IV). Üç veya beş de olabilir<sup>135</sup>.

Esasen alacaklı sınıfları kanunla sayılmış olmadığından her somut olayda farklı sınıflar olma olasılığı bulunmaktaysa da hemen hemen tüm konkordato süreçlerinde işçiler (çalışanlar), bankalar ve mal temin edenler(tedarikçiler) bulunur. Kanunda alacaklılar kurulunda farklı alacaklı sınıflarının ve varsa rehinli alacaklıların HAKKANİYETE uygun olarak temsil edileceğinden söz edilmektedir. 289.maddenin III. fıkrasında konu ayrıntılı olarak düzenlenmiş ise de mahkemenin kurulun teşekkülü hususundaki kararına karşı gerek alacaklılar gerek komiserin gidebileceği hukuki imkandan söz edilmemiştir. 7101 sayılı Kanunla değişiklikler düzenlenirken Kaynak Kanundaki gibi öncelikle itiraz ve bu itiraz üzerine Mahkemenin kararına karşı da istinaf yolu açık tutulması uygun olurdu.

#### IV. ALACAKLILAR KURULUNUN GÖREVE BAŞLAMASI VE SÜREÇTE ROLÜ

Adi konkordatoda olsun, malvarlığının terki suretiyle konkordatoda olsun; alacaklıların menfaatlerinin de dikkate alınması, konkordatoda alacaklıların güçlendirilmesi, konkordato müessesesinin mülkiyet hakkına müdahale olduğu gerçeğine uygun olarak hukuk devleti ilkesi ve ölçülülük ilkesi çerçevesinde konuya yaklaşıldığının ve esasen bunun hukuk devleti ilkesi yönünden gerekli de olduğunun kanun koyucu tarafından anlaşıldığının göstergesidir.

Alacaklılar Kurulunun teşekkülü, adi konkordatoda, konkordato konusunda yetkili ve görevli olan asliye ticaret mahkemesinin kararıyla olur. İcra ve İflas Kanununun 289. maddesi gereğince **kesin mühlet kararıyla** beraber ya da en geç 2004 sayılı Kanunun 299 uncu maddesi uyarınca **alacaklıların alacaklarını bildirmesi** ve aynı Kanunun 300 üncü maddesi gereğince **de borçlunun alacaklılar hakkındaki beyanı alındıktan sonra, yedi alacaklıyı geçmemek,** herhangi bir ücret takdir edilmemek<sup>136</sup> ve tek sayıda olmak kaydıyla konkordato komiserinin de görüşü de alınarak Asliye ticaret mahkemesi tarafından alacaklılar kurulu *oluşturulabilir* (Yön. m. 21). Yani alacaklılar kurulu zorunlu değil; ihtiyari bir konkordato organıdır. Hukuki nitelikleri büyük ölçüde birbirine benzer olan alacaklılar, aynı alacaklı sınıfında yer alır. Yönetmeliğin

---

135 İsviçre hukukunda Alacaklılar kurulunun üye sayısı ile ilgili Yönetmelik bulunmamakta uygulamada 3 veya 5 üyeden oluştuğu, kararlarını basit çoğunlukla aldığından tek sayıda olmasının uygun olacağı belirtilmektedir **BÜRĞİ, U.** Art. 237, S.1047, Rdnr.27. İsviçre hukukunda alacaklılar kurulunun sadece konkordatoda değil; iflas sürecinde de oluşturulabileceğinin unutulmaması gerekir. S.1048 vd.'nda iflasta alacaklılar kuruluna dair açıkla-malara yazar yer vermiştir. **JAEGER,** Rdnr.10-13

136 İsviçre'de GebV SchKG m.55' kıyasen uygulayarak mahkeme götürü ücret tespit edebilmektedir(**JAEGER,** Rdnr.24: Bunu yaparken mahkeme, üyelerin görecekları için zorluk derecesini, meşguliyetlerinin çerçevesini ve sürecin ağırlığını(büyükliğini) dikkate almaktadır. Bu ücretler, bilahare iflas söz konusu olursa masa borcu olarak ödenmektedir(Rdnr. 24).

ifadesiyle hukuki nitelik itibarıyla birbirinden farklı olan alacaklı sınıfları ve varsa rehinli alacaklılar, alacaklılar kurulunda hakkaniyete uygun biçimde temsil edilir. *Rehinli alacaklılar, rehinin kıymetini karşılayan miktardaki alacakları bakımından ayrı bir sınıf olarak kabul edilir.* En az üç alacaklı sınıfın bulunması kaydıyla, alacaklı sayısının iki yüz elliye veya alacak miktarının yüzyirmibeş milyon Türk Lirasını aşması halinde alacaklılar kurulunun oluşturulması zorunludur(Yön.m.22)<sup>137</sup>.

Malvarlığının terki suretiyle konkordatoda ise alacaklılar tasfiye memurlarını ve alacaklılar kurulu üyelerini seçer(m. 309a/II). Esasen bir önceki “kurulun teşekkülü” başlığı altında konu incelenmişti.

İyileştirme amacına da hizmet edebilen konkordato müessesesi, iflasların önlenmesi ve mümkün merteye sosyal ve ekonomik bakımlardan iflasların sebebiyet vereceği yıkıcı etkilerin engellenmesini de sağlama yönünde bir işleve sahiptir. Bu işleve gölge düşürecek tarzda alacaklı/lar menfaatinin göz ardı edildiği bir süreç olarak yaşanması, ticari hayatta zincirleme olarak konkordato ve iflasların yaşanması sonucunu yaratabilir. “Konkordato Komiserliği ve Alacaklılar Kuruluna Dair Yönetmelik ” teki (m. 21-24’teki) düzenlemelerle ve 7155 sayılı kanunla özellikle konkordato komiseri konusunda getirilmiş hükümler ve konkordato başvurusunda bulunurken aranan belgelere dair değişikliklerle bu engellenmeye çalışılmıştır.

Adi konkordatoda en erken kesin mühlet kararıyla birlikte, Asliye Ticaret mahkemesi alacaklılar kurulunun teşekkülüne karar verebilmektedir. Geçici mühlet esnasında alacaklılar kurulu teşekkül ettirilmemektedir. Kaynak kanun bakımından da İsviçre’de Ocak 2014’te yürürlük kazanan revizyondan sonra dahi geçici mühlet esnasında alacaklılar kurulu teşekkülü öngörülüş değildir. Zira sürecin bu erken aşamasında kural olarak mahkemenin ne alacaklılar kurulunun gerekliliğini karara bağlaması ne de bunun kimlerden teşekkül edebileceğini tespiti mümkündür. Kesin mühlet kararıyla ya da bilahare 299 uncu maddesi uyarınca alacaklıların alacaklarını bildirmesi ve aynı Kanunun 300 üncü maddesi gereğince borçlunun alacaklılar hakkındaki beyanı alındıktan sonra, teşekkül ettirilebilen alacaklılar kurulu bu konuda verilmiş mahkeme kararıyla görevine başlar.

---

137 Kaynak hukuk olarak İsviçre hukukunda, Konkordato ile ilgili hususlarda konkordato mahkemesi, konkordato komiseri tayin ederken icabında alacaklılar kurulu da teşekkül ettirebilmekte(m. 295a) ve her ikisinin de iznine ihtiyaç gösteren işlemlere(m. 298/II) karar verebilmektedir.

Malvarlığının terki suretiyle konkordatoda ise, alacaklılar kurulu, tasfiye memurları ile birlikte, konkordato hakkında karar veren alacaklılar tarafından seçilmekte ve asliye ticaret mahkemesinin onayı ile göreve başlamaktadır.

Gerek İsviçre'deki Revizyonla gerek ülkemizde 2018 Martında yasalaşan düzenlemelerle güdülen amaç, adi konkordato sürecinde alacaklıların konumunu (durumunu) güçlendirmektir. Esasen gerek Avrupa gerekse ABD'de yeniden yapılandırmaya ilişkin mevzuat değişikliklerine bakıldığında hem iflas sürecinde hem de konkordato sürecinde hatta yeniden yapılandırma sürecinde alacaklıların süreçlere katkı ve etkide bulunma haklarının artırıldığı; alacaklılar toplantısı dışında alacaklılar kurulunun ayrı bir organ olarak oluşturulduğu da dikkat çekmektedir<sup>138</sup>.

Nitekim malvarlığının terki suretiyle konkordatoda da alacaklılar kurulu ve tasfiye memurları ilişkisi ve özellikle tasfiye anlaşması şeklindeki malvarlığının terki suretiyle konkordatoda alacaklıların yararının korunmasının ön planda tutulmuş olmasından ötürü, Kanunda açıkça tasfiye memurlarına verilmiş yetkiler hariç, boşluk bulunan durumlarda alacaklılar kurulunun yetkili olduğunun kabul edilebileceği belirtilmiştir<sup>139</sup>.

## V. ALACAKLILAR KURULUNUN İŞLEVİ

Denetim organı olduğu göz ardı edilmemek gereken alacaklılar kurulu, gerek konkordato sürecini gerek konkordato komiserini denetler. Ancak bizzat sürecin gidişatına dair işlemler yapamaz. Konkordato borçlusu ile alacaklılar kurulu arasında direkt bir ilişki bulunmaz. Talepleriyle ilgili partneri konkordato komiseridir. Geçmiş tecrübeler, mühlet aşamasında borçlunun geleceğine dair yol haritasını ortaya koyan kararların- bilhassa iyileştirme veya tasfiye hususunun karara bağlanabilmesi- söz konusu olabilmesi sebebiyle alacaklıların, alacaklılar kurulu eliyle sürece iştirak etmesinin menfaatlerinin korunması bakımından hayati önemde olduğunu göstermiştir. Kesin mühlet içinde borçlunun malvarlığının özünün en iyi biçimde muhafaza edilmesi gereği açıktır. Zira adi konkordatoda, halihazır mühlet süresi boyunca borçlu hala önemli aktivitelerde bulunabilmektedir. Zaruri ve ivedi tasarrufları söz konusu olabilen borçlu karşısında alacaklıların haklarının güvence altında tutulması gereksinimi, borçlunun malvarlığının korunmasını temin etmelerini gerektirir. Bu ise, alacaklılar kurulunun türlü denetim ve gözetim faaliyetlerinde bulunması ile sağlanabilir. Kesin mühlet verilirken ya da sonrasında mahkeme

---

138 Hukukumuzda da **TANRIVER** tarafından alacaklılar toplantısından başka alacaklılar kurulunun oluşturulması önerilmiştir( Konkordato Komiseri, Ankara 1993, s.28)

139 **ERCAN**, s. 184-185

tarafından oluşturulmuş alacaklılar kurulunun görevlerine bakıldığında, en önemlisinin konkordato komiserinin gözetimi ve denetimi olduğu görülür.

Alacaklılar Kurulu, konkordato komiserine sürecin sağlıklı yürütmesi ve zarara uğramamaları için düzeltici önerilerde bulunabilir. Yapıcı eleştiriler getirebilir. Komiser de alacaklılar kurulunu düzenli olarak sürecin gidişatı ile ilgili bilgilendirir. Denetim işlevine karşın kurul şikayet mercii değildir<sup>140</sup>. Kurulun denetim işlevini yerine getirişinin kapsam, tarz ve işleyişi biçimi, somut konkordato sürecine bağlı olarak değişiklik gösterdiği gibi, alacaklılar topluluğunun ilgili menfaatlerine göre yön ve içerik kazanır. Küçük basit konkordato süreçlerinin aksine komplike ve geniş kapsamlı süreçlerde alacaklılar çok daha yüksek düzeyde denetim gerçekleştirmek durumundadır<sup>141</sup>.

Malvarlığının terki suretiyle konkordatoda da, alacaklılar kurulunun en önemli görevi tasfiye memurlarını denetlemektir. (m. 309/ç). Tasfiye memurlarının **borçlunun mallarının idaresini ve paraya çevirmeyle ilgili tüm işlemlerini konkordato tasfiyesi boyunca kurul denetler**. Bu bakımdan kapsamlı bir inceleme yetkisine sahip ve ihtiyaç duyduğu tüm bilgi ve belgelere kolayca ulaşabilir durumda olmalıdır. Kanun gereği karar vermeye yetkili olduğu konularda tasfiye memurlarına talimat da verebilir<sup>142</sup>.

## VI. ALACAKLILAR KURULUNUN ÇALIŞMA USULÜ VE SORUMLULUĞU

Alacaklılar Kurulu, teşkiliyle birlikte, bizzat bir çalışma genelgesi ortaya koyabilir ve bir başkan ve başkan vekili seçebilir<sup>143</sup>. Kurul üyelerinin görev dağılımı, başkanın kim olduğu, toplantı aralıkları, karar ittihazı, zapta geçirilmesi, toplanmama sebepleri gibi sürece dair diğer hususları da bu çalışma genelgesinde düzenlemek uygun olur. Kanımızca Komiser ve Kurul ile ilgili Yönetmelikte bunlara dair açıklık getirilmek gerektiğine dair düzenleme getirilmesi isabetli olurdu.

Adi konkordatoda, mahkeme tarafından alacaklılar kurulu teşekkül ettirildikten sonra, kurulun her ay en az bir defa toplanacağı ve kararlarını oyçokluğu ile alacağı<sup>144</sup> da (m.289)

---

140 Kanton şikayet mercilerine İsv.İİK.m.17 vd. çerçevesinde başvurulabileceği belirtilmektedir ( **JAEGER**, Rdnr.14 141 **JAEGER**, Rdnr. 15

142 **ERCAN**, s. 279. Kurulun tasfiye memurları üzerinde disiplin yetkisi bulunmamaktadır. Bu yetki icra mahkemesindedir.

143 Uygulamada kurul kendisi Organisationsreglement ile üyelerin görev dağılımı, başkanın kim olduğu toplantı aralıkları, karar ittihazı, zapta geçirilmesi, toplanmama sebepleri gibi sürece dair diğer hususları da düzenler(**JAEGER**, Rdnr.23) .Ayrıca bkz. **SARISÖZEN**, S. İcra- İflas ve Konkordato Hukukundaki Yenilikler, 3. Bası, Ankara 2019, s. 159

144 Kurul üyelerinin sadece temsil ettikleri alacaklı grubunun değil; tüm alacaklıların menfaatlerini aynı oranda gözetme koruma yükümlülüğü dolayısıyla eşit oy hakkına sahip olarak oy çokluğuyla karar almaları kanımızca doğaldır.

belirtmiştir. Bu toplantıların yapılması ve kurulun etkin çalışması, alacaklılar ile borçlu menfaatlerinin süreç boyunca dengede olması bakımından önemlidir.

Alacaklılar kurulu oturumlarında komiser de hazır bulunur. Hukukumuzda m. 289/IV’ teki “Komiser toplantıda hazır bulunarak alınan kararları toplantıya katılanların imzasını almak suretiyle tutanağa bağlar” açık ifadesi karşısında, alacaklılar kurulunun münferit oturumlarını tamamen veya kısmen komiser olmaksızın gerçekleştirmek imkanının bulunduğunu söylemek güçtür<sup>145, 146</sup>.

İstemesi halinde veya alacaklılar kurulunun talebi üzerine veya bir kurul üyesinin talebi üzerine komiser bilgi verir<sup>147</sup>.

Şüphesiz alacaklılar kurulu aktif çalışmıyorsa, kanunen her ay en az bir defa yapmakla yükümlü olduğu toplantısını örneğin yapmamaktaysa, komiserin, alacaklılar kurulunu, yasa gereği yapmaları gereken toplantıya zorlayabilip zorlayamayacağı tartışmaya açık olmakla beraber; komiserin alacaklılar kurulunun dikkatini her ay bir kere toplantı yapmak şeklindeki yasal yükümlülüğe çekebilmesine imkan bulunduğunu söyleyebilmek 289/IV<sup>148</sup>’ teki ifadeden ulaşılması zor bir husustur. İleride alacaklılar kurulunun ve üyelerinin sorumluluğunun gündeme gelebilme olasılığına binaen komiserin söz konusu aylık toplantıların gerçekleştirilmediği hususunu tespit tutanağı tanzimi ile belgelendirmesinin uygun olacağı, 289/IV’ teki ifadeden çıkarılabilecek bir sonuçtur.

Düzenli aralıklarla kurulun konkordatonun gidişatı hakkında komiserce bilgilendirilmesi komisere düşen bir görev ise de, komiserin genel bir himaye yükümlülüğü bulunduğu sonucu çıkarılamaz.

İİK. m. 290 /II, e gereğince komiser, alacaklılar kurulunu konkordatonun seyri hakkında düzenli aralıklarla bilgilendirmekle de yükümlü kılınmıştır. Dolayısıyla alacaklılar kurulunun komiserden bu yükümlülüğü çerçevesinde davranmasını talep yetkisi kanunen bulunmaktadır. 290/II, f bendi gereğince de talepte bulunan alacaklılara konkordatonun seyri ve borçlunun güncel mali durumu hakkında komiser bilgi vermekle yükümlüdür. Kurul üyelerinin bütün alacaklıların haklarını aynı oranda savunmaları, sadece temsilcisi oldukları alacaklı grubunun menfaatlerini

---

145 İsviçre hukukunda bunun mümkün olması gerektiği hakkında **HUNKELER**, Kurzkommentar SchKG 2.Auflage 2014, S.1393, Rdnr. 18

146 Önemli işlemlere ilişkin e-mail, faks ya da telekonferansla bilgilendirme ve danışma (istişare etme) mümkündür. Acil durumlarda sirküler yoluyla alınmış kararlar da esasen mümkün olabilmelidir (**HUNKELER**, S. 1393-1394)

147 Bu iyiniyetli bir istişari faaliyet olarak ifade edilir (**HUNKELER**, S. 1394)

148 “Kurul her ay en az bir kere toplanır ve komiser toplantıda hazır bulunarak alınan kararları katılanların imzasını alarak tutanağa bağlar”

koruma amaçlı faaliyette bulunmamaları lazımdır<sup>149</sup>. Kurulun sorumluluğu bakımından İİK. m. 5'in uygulanması olanağı bulunmamaktadır. Alacaklılar Kurulu, cebri icranın atipik bir organıdır. Bir taraftan kamu hukuku, diğer taraftan özel hukuk fonksiyonu bulunan kurulun üyeleri resmi (amtlich) pozisyonadadır ve sır saklamakla yükümlüdür. Kurulun üyeleri, temsilcisi oldukları alacaklıların değil; aksine tüm alacaklıların hatta sürece dahil tüm bileşenlerin menfaatlerini korumak durumundadır., Yükümlülüklerini ihlal etmeleri halinde, bundan bir zarar ortaya çıkarsa, alacaklılara karşı haksız fiil hükümleri çerçevesinde sorumlu olacaklardır; ama İİK. m. 5 uygulama alanı bulmayacaktır.<sup>150</sup>

Alacaklılar kurulu, görevlerini gereği gibi yapmadığı, yetkileri bulunduğu ve engelleyebilecekleri halde engellemedikleri alacaklı/ lar zararlarından ötürü haksız fiil kurallarına göre sorumludurlar. Mahkemece belli özelliklere sahip kişilerden ve Yönetmelikle<sup>151</sup> aranan özelliklere uygun kişiler arasından atanmış olan konkordato komiseri için bile m. 290'ın iflas idaresinin sorumluluğuna dair İİK. m. 227/IV'e yollama yaptığı düşünüldüğünde alacaklılar kurulu bakımından m. 5'in uygulama alanı bulmasının mümkün olmadığı netleşir. Bu sebeple sorumluluk bakımından İİK.m.5 uygulanamaz; ancak Borçlar Kanununun haksız fiil hükümlerine göre alacaklılar kurulu sorumlu olabilir.

## VII. ALACAKLILAR KURULUNUN HAK VE YÜKÜMLÜLÜKLERİ

### 1. Alacaklılar Kurulunun Yükümlülükleri

Periyodik olarak kanunen her ay en az bir defa toplanır

Komiserin faaliyetlerine nezaret eder(m. 290/VI).

Genellikle kanunda her ay en az bir kere toplanacağı belirtilmiş olan kurulun bu periyodik toplantılarında bilgilendirmede bulunur. Kurul toplantılarının hangi aralıklarla gerçekleşeceği, tasfiye konkordatosuna oranla hummalı ve zamansal baskının söz konusu olduğu adi konkordatoda daha da önem kazanır. Komiserin davetiyle ya da alacaklılardan birinin bir başka deyişle kurul üyelerinden birinin insiyatifıyla toplantı gerçekleştirilmesi söz konusu olur. Toplantı öncesinde komiserin kurul üyelerini yazılı olarak ön bilgilendirmede bulunur; döküman gönderir. Toplantıda da sözlü olarak bunları tamamlar, soruları yanıtlar. Toplantılar dışında komiser, kurulun yazılı sorduğu hususlara e-mail, faks ya da telekonferans yöntemiyle bilgilendirerek de katkı sağlar.

---

149 PEKCANITEZ/ERDÖNMEZ, s. 80 (Bizim de katıldığımız kurul üyelerinin bağımsızlıkları bakımından konkordato talep eden borçluyla hiçbir ilişkilerinin olmaması şeklindeki yazarlara ait görüşten de bahsedilmelidir).

150 HUNKELER, Rdnr.24-25, JAEGER, Rdnr.26

151 RG. **30.01.2019, S. 30671**



Aslında kesin mühletin başlangıcında alacaklılar kurulu ve komiserin, standartlaştırılmış ve basit bir karşılıklı iletişim konusunda anlaşmış olması önemlidir<sup>152</sup>.

Komiserin gerektiğinde değiştirilmesini gerekçeli rapor tanzim ederek mahkemeden talep edebilecek olan denetim organı niteliğindeki alacaklılar kurulunun komiserle iyi bir iletişim içinde olması çok önemlidir.

Kanunun belirttiği hallerde mahkemeye görüş bildirmekle(m. 289/IV, m. 291/II, m. 292/son c. 297/II) de kurul yükümlüdür.

Örneğin kesin mühletin kaldırılarak borçlunun iflasına karar verilmesi öncesinde mahkeme alacaklılar kurulunu davet ederek dinleyecektir. Bu konuda kurulun görüş ve taleplerini mahkemeye sunabilmesi, borçlunun mali durumunun iyileştirilmesi olasılığı kalmamışsa daha fazla takip yasaklarının devam etmesinin alacaklıların zararına olması sebebiyle son derece yerinde bir düzenlemedir. Kanunda alacaklılar kurulunu davet etmek zorunda olduğu, diğer alacaklıları dinleyip dinlememekte takdir yetkisi bulunduğu düzenlenmiş olduğundan kurulun teşekkülünün ne denli önemli olduğu izah gerektirmeyen bir husustur<sup>153</sup>

Komiserin konkordato ile ilgili işlemlerine dair şikayet yoluna başvurmak(m.290/III) 290.maddede kıyasen uygulanacak hükümler arasında şikayetle ilgili 16.madde de(8,10,11 ve 21 ve 359.maddeler) sayılmış olduğundan mümkündür. Kurul da münferit alacaklılar da komiserin işlemleri bakımından şikayet yoluna gidebilir. Zaten kurulun konkordato komiserinin görevden alınarak bir başkasının komiser olarak atanmasını mahkemeden talep hakkı bulunduğu da düşünüldüğünde, şikayet yoluna gidebileceği de rahatlıkla ortaya çıkar.

## **2.Alacaklılar Kurulunun Hak ve Yetkileri**

Konkordato komiserinin denetimi ve gözetimi konusunda yetkili olmak, alacaklılar kuruluna komisere genel anlamda talimat vermek yetkisi sunmaz. Komiserin ne zaman hangi şekilde bilgi vereceği hususu alacaklılar kurulunun tek tarafı olarak belirleyebileceği bir husus değildir.

Komiserin faaliyetlerini yeterli bulmazsa, mahkemeden komiserin değiştirilmesini gerekçeli bir raporla isteyebilir. Komiserin değiştirilmesini talep hakkı kurulca kullanıldığında, mahkeme borçluyu ve komiseri dinledikten sonra kesin olarak karar vermektedir<sup>154</sup>. Kanımızca kanun yolunun açık olması, alacaklı(lar)-borçlu menfaat dengelemesi bakımından isabetli

---

152 JAEGER, Rdnr.16; HUNKELER, Rdnr. 17 ff. Ayrıca bkz. UYAR, s.54; SARISÖZEN, s. 158

153 Benzer şekilde görüş için PEKCANITEZ/ERDÖNMEZ, s. 82

154 Bu yetkinin ne kadar etkin kullanılabileceğinin belirsiz olduğu yönündeki görüş için bkz. PEKCANITEZ/ERDÖNMEZ, s. 82.

olacaktır. Çalışmasının tatminkar olmadığını gerekçeli raporla alacaklılar ortaya koymuş olmakla beraber; mahkemeye yapılan komiser değişikliği talebi kabul edilmemişse, mahkemenin bu kararına karşı kanun yoluna gidilebilmesi gerekir. Aksi takdirde ciddi menfaat zedelenmesi olduğu halde mahkemenin komiseri değiştirmemiş olmasından zarar gören alacaklılar, onun kusurlarıyla verdiği zarardan sorumlu olması sebebiyle ( m. 290'ın iflas idaresinin sorumluluğuna dair m.227'ye yaptığı atıf) adli yargıda tazminat davası açabileceklerdir. Ceza hukuku bakımından ise komiser, memur sayıldığından bu çerçevede sorumlu olacaktır. Bunlar maalesef gecikmiş ve pek de fazla işe yarar olmayan yaptırımlardır. Oysa mahkemenin ret kararı üzerine istinaf mahkemesine kurul kararı taşıyabilse oradan komiserin değiştirilmesine dair karar alabilse sürece çok daha etkin bir katılımından söz edilebilirdi.

Kanundan, Kurulun düzenli aralıklarla konkordatonun gidişatı hakkında komiserden bilgilendirilme talebinde bulunma yetkisi olduğunu m. 290/e'den çıkartmak mümkündür. Hatta kurulun münferit üyelerinin de komiserden konkordatonun gidişatı ve borçlunun güncel mali durumu hakkında bilgi verilmesini istemek yetkisi vardır.

Alacaklılar kurulu, Komisere tavsiyelerde de bulunabilmek yetkisine sahip kılınmıştır. (m.290/son f<sup>155</sup>). Ayrıca konkordato sürecinde borçlunun yapmış olduğu işlemlere dair evrak inceleme, gerektiğinde komiserden bilgi talep etme hakkı da kurula tanınmıştır. Kurulun komiseri denetleme yetkisi özel öneminden ötürü aşağıda ayrı başlık altında incelenecektir.

### **3. Komiserin Faaliyetinin Denetlenmesi Yetkisi**

Alacaklılar kurulu komiseri gözetimi altında bulundurur ve konkordato sürecinde ona danışır, onunla istişare içinde bulunur. Bu kurul, tüm alacaklıların menfaatlerini temsil eder. Komiserin işlemlerinin ve yaptığı işlerin tüm bu alacaklıların çıkarlarını gözetip gözetmediği ve aldığı kararların alacaklı(lar) menfaatlerine uygunluğunu güvence altında tutar şekilde kurulun denetim yetkisinin bulunduğundan söz edilebilmesi için, komiser değişikliği talebinin mahkemece reddi halinde bunu istinafa götürebilmesi gerekirdi<sup>156</sup>.

Kurul komiseri denetler(m. 290/VI krş. İsv. İİK.m. 295a/II). Denetimin kapsamı, biçimi ve yöntemi somut sürece bağlıdır. Alacaklıların tümünün ilgili menfaatlerine göre denetimin içeriği düzenlenmelidir. Kapsamlı ve karmaşık konkordato sürecinde ya da alacaklılar bakımından büyük yayılımı olanlarda küçük basit olanlara oranla alacaklıların komiseri denetimi daha yüksek düzeyde gerekir ve haklılık kazanır.

---

155 Krş. İsv. İİK.m. 295a

156 Aynı yönde görüş için bkz. PEKCANITEZ /ERDÖNMEZ, s.82-83

Komiser de düzenli olarak sürecin gidişatı ile ilgili alacaklılar kuruluna bilgi vermek durumundadır. Bunun süreç boyunca bu şekilde olması gerekir. Hangi sıklıkta ve ne biçimde komiser ve alacaklılar kurulunun ilişki içinde bulunacağı, somut olayın şartlarından ortaya çıkar. Alacaklılar kurulu, komisere (m. 290/son f.krş. İsv.İİK.m. 295a/II gereğince) tavsiyelerde bulunabilir<sup>157</sup>.

Hukukumuzda m.290'nın, alacaklılar kurulunun komisere genel talimat verme yetkisi bulunduğu sonucunu çıkarmayı sağlayacak ya da en azından tartışılmasını mümkün kılacak bir ifade taşımadığı açıktır.

İsviçre'de "Alacaklılar kurulu" nun, komisere hangi hareket tarzı ve hangi kararı doğru gördüğünü bildireceği ve ondan da bunu bekleyeceği yani alacaklılar kurulu ve komiserin birbirine bağlı, koordine çalışacakları belirtilmiştir<sup>158</sup>. «Komiser sonunda farklı karar verdiği takdirde, alacaklılar kurulu bunu iptal ettirebilir veya yargıca durumu bildirebilir» denilmektedir. Mahkeme, sürmekte olan konkordatoda gerekirse, komiseri azledebilir ve bir yenisini atayabilir. (krş. M. 295/I). Sadece acil durumlarda yukarıda belirtilen usul gereğince verilmiş talimatlar, komiserce takip edilmek gerektiğinden bu yapılmadığında kayıplar da ortaya çıkabilecektir. İşbirliği içinde faaliyet göstermeyen komiserin değiştirilmesi önerisinde kurul bulunulabilecektir.

Komiserin kararlarına karşı alacaklılar kurulunun bağımsız bir veto hakkı bulunmamaktadır; İsviçre'de konkordatodaki alacaklılar kurulunun yetkilerinin, iflastaki alacaklılar kurulundan çok daha az olduğu görülür.

İİK. m. 297 gereğince borçlunun mahkemenin izni dışında mühlet kararından sonra rehin tesis edebilmesi, kefil olabilmesi, taşınmaz ve işletmenin devamlı tesisatını kısmen dahi olsa devredebilmesi ve takyit edebilmesi ve ivazsız tasarrufta bulunabilmesi mümkün değildir. Rehin tesis edebilmesi, kefil olabilmesi, taşınmaz ve işletmenin devamlı tesisatını kısmen dahi olsa devredebilmesi ve takyit edebilmesi ve ivazsız tasarrufta bulunabilmesi hususlarında karar yetkisi mahkemeye aittir.

---

<sup>157</sup>İsviçre'de Revizyon Tasarı taslağında alacaklılar kurulunun komisere talimat verebileceği de belirtilmişti. Daha sonradan komisyonda bu husus değişikliğe uğratılmıştır. Bu değişiklik açıkça haksızdır ve sisteme uygun değildir eleştirisine uğramıştır. Alacaklılar kurulu, denetim kurulu olarak üst kuruldur ve doğrudan müdahale gerekli ise, bunu tespit edebilmesi gerektiği öğretide (**HUNKELER** 295a Rdnr. 19, son) belirtilmiştir. Kaynak İsviçre hukuku bakımından, kanunun açık ifadesi karşısında bağımsız bir talimat verme hakkının yasa koyucu tarafından kurula tanınmadığı da şüphesizdir. Mahkemelerden de, alacaklılar kurulunun komisere bağlayıcı nitelikte talimatlar verebilmesini mümkün kılan bir anlayış beklenemez.

<sup>158</sup> **HUNKELER**, Rdnr.20

Aksi halde yapılan işlemler hüküm ifade etmemektedir. İşlemler hakkında karar vermeden önce, mahkeme, komiser ve alacaklılar kurulunun görüşünü almak zorundadır<sup>159</sup>.

## SONUÇ

Adi konkordatoda ve malvarlığının terki suretiyle konkordatoda alacaklılar kurulunun ele alındığı bu çalışmada, bir taraftan alacaklılar kurulunun tanıtımı amaçlanmış; diğer taraftan da kurulun yapısı, işlevi, yükümlülükleri, yetkileri, çalışma usulü ile sorumluluğu ortaya konmuştur. Kurulun işlevselliğinin alacaklı(lar)/borçlu menfaatlerinin dengede tutulması bakımından çok önemli olduğu zira konkordato sürecinin alacaklısının örneğin tedarikçinin diğer bir ticari ilişkide borçlu statüsünde olabileceği unutulmamalıdır. Ticari hayatın düzen ve denge içinde gidebilmesi bakımından, mevcut konkordato sürecinde menfaatleri korunmak gereken alacaklı, diğer bir hukuki/ticari ilişkide eş zamanlı borçlu konumunda olabilir. Bu alacaklı(lar) konkordatodan ağır şekilde zarar görecektir olursa, kendisi de borçlarını ifa edemeyecek ve zincirleme olarak onun da konkordatoya gitmesi ya da iflas etmesi gibi olasılıklar yaşanacaktır. Bu da sosyoekonomik bakımdan istenmeyen sıkıntılı durumlar yaratacaktır.

Özellikle mahkemenin alacaklılar kurulu teşekkülü ile ilgili kararına karşı gidilebilecek kanun yolu olmaması, keza 293.madde ile mühletin kaldırılması talebi reddedildiğinde, karara karşı kanun yoluna gidilememesi ve de alacaklılar kurulunun komiserin değiştirilmesi talebinin mahkeme tarafından reddi kararına karşı kanun yolunun kapalı tutulması, konkordato sürecinde alacaklılar kurulunun etkinliğini, işlevselliğini ne yazık ki ciddi anlamda örselemektedir<sup>160</sup>. Kurulun teşekkülünden sonra çalışması ile ilgili yasal düzenlemeler kanımızca yeterli olmaktan uzaktır. Yönetmelikte çok daha ayrıntılı düzenleme getirilmesi umulurdu. Keza alacaklılar kurulunun sorumluluğu da düzenlenmiş değildir. Ancak bu durum, yetkilerini kullanmamış ve zarar doğmasına sebebiyet vermiş olan alacaklılar kurulunun, en azından Borçlar Kanunu genel hükümleri dairesinde sorumluluğunun doğmayacağını düşündürmez. Doğal olarak İİK.m.5'in burada tatbiki mümkün olmayacağından BK' nun haksız fiil hükümlerine göre sorumluluğu söz konusu olacaktır. Kanımızca alacaklılar kurulunun gerek İİK. m. 289/IV; gerek 290 ile adi konkordato bakımından da yasal zemine kavuşmuş olması, Yönetmelikle bazı hususlara yer verilmiş olması -malvarlığının terki suretiyle konkordatoda zaten 4949 sayılı Kanunla yapılan

---

159 Bu hükmün karşılığı olan İsv. İİK.m. 298/II'ye göre ise, borçlu onaya tabi hukuki işlemler akdetmek istediği hallerde III. fıkrayla alacaklılar kuruluna karar yetkisi sunmaktadır. Mahkeme yerine gerekli onayı alacaklılar kurulu vermektedir(Ayrıntılı bilgi için bkz. **JAEGER**, Rdnr.19-21; **HUNKELER**, Rdnr.22)

160 Benzer görüş için bkz. **PEKCANITEZ/ERDÖNMEZ**, s. 82.

değişikliklerle konu düzenlenmişti- önemli bir adım olarak düşünölmekle beraber; yeterli olduğunu söylemek oldukça güçtür. Hukuk devleti ilkesi ile ölçölölük ilkesi konkordatoda alacaklı/lar-borçlu menfaat dengelemesinin sağlanmasını gerektirdiğinden yapılan düzenlemelerin çok daha somut ve ayrıntılı şekilde örneğın çalışma usulü, karar yetersayısı ve sorumluluğı düzenlenmelidir.

### KISALTMALAR

Art.	: Artikel
BAM	: Bölge Adliye Mahkemesi
bkz.	: bakınız
BK	: Borçlar Kanunu
c.	: cümle
C.	: Cilt
f.	: fıkra
İİK	: İcra ve iflas Kanunu
InsO	: Insolvenzordnung
İNÜHD:	İNönü Üniversitesi Hukuk Fakültesi Dergisi
Kom.	: Kommentar
krş.	: karşılaştırınız
m.	: madde
Rdnr	:Randnummer
S.	: Sayı ya da Seite
s.	: sayfa
SchKG	: Schuldbtreibungs-und Konkurs Gesetz
vd.	: ve devamı
vs.	: ve saire
Yön.	: Yönetmelik
ZPO	: Zivilprozessordnung

**KAYNAKÇA**

- BÖRÜ, L.** : “Adi Konkordatoda Alacaklılar Kurulu”, İnÜHD C. IX, S.2, 2018 s. 346 vd.
- ERCAN, I.** : İcra ve İflas Hukukunda Malvarlığının Terki Suretiyle Konkordato, Konya 2008.
- HUNKELER, D.** : Kurzkomentar SchKG 2.Auflage Basel 2014
- JAEGER,** : Kommentar zum Bundesgesetz über SchKG, Zürich, Basel, Genf 2017
- KURU, B.** : İcra ve İflas Hukuku Elkitabı, 2.Bası 2013.
- ÖZTEK,S. /BUDAK,A.C.,/TUNÇ YÜCEL, M, /KALE,S. ,/YEŞİLOVA,B.)** : Yeni Konkordato Hukuku,2. Bası, 2019.
- PEKCANITEZ, H./ERDÖNMEZ, G.** : 7101 sayılı Kanun Çerçevesinde Konkordato, 2018.
- PEKCANITEZ/ATALAY/SUNGURTEKİN ÖZKAN/ÖZEKES,** : İcra ve İflas Hukuku, Dersi kitabı, 5.Bası İstanbul 2018.
- POSTACIOĞLU, İ.** : Konkordato, İstanbul 1965.
- SARISÖZEN, S.** :İcra- İflas ve Konkordato Hukukundaki Yenilikler, 3. Bası, Ankara 2019
- TANRIVER, S.** : Konkordato Komiseri, Ankara 1993.
- TANRIVER/DEYNEKLİ,** : Konkordatonun Tasdiki, Ankara 1996.
- TAŞPINAR AYVAZ, S.** : Adi konkordato hakkında İcra ve İflas Kanununda yapılan değişiklikler, BATIDER, Aralık 2003, C.XXII,S.2,s. 49 vd.
- UYAR, T.** : Yeni Konkordato Hukuku, Ankara 2019.
- WIDMER,** : “Der Nachlassvertrag, eine Rechtswohltat Festschrift 100 Jahre SchKG, Zürich 1989.
- YILDIRIM, M.K./DEREN YILDIRIM, N.** : İcra ve İflas Hukuku, İstanbul 2015

## AVRUPA BİRLİĞİ GENEL VERİ KORUMA TÜZÜĞÜ BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI

Doç. Dr. Murat Volkan Dülger<sup>161,162</sup>

### ÖZET

Bireylerin temel hak ve hürriyetlerini ilgilendirilen kişisel veriler hakkında zaman içinde farkındalık oluşmuş ve bu çerçevede ulusal ve ulusüstü düzenlemeler yapılmıştır. Bu çerçevede kabul edilmiş en geniş kapsamlı ve en güncel düzenleme 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğüdür (Tüzük ya da GDPR). 95/46/EC sayılı Direktif bilişim teknolojilerinin günümüzdeki kadar gelişmiş olmadığı bir dönemde kabul edilmiş olup, amaçlarından biri olan AB ülkelerinde kişisel verilerin korunması hukukunda yeknesaklığı da sağlayamamıştır. Bu durum, AB veri koruma normlarının yeniden düzenlenmesi gereğini ortaya çıkarmıştır ve bu ihtiyaçtan hareketle Mayıs 2016'da Avrupa Birliği Genel Veri Koruma Tüzüğü kabul edilmiştir. İlk bakışta Tüzüğün genelinde fark edilebilen ve onu önceki düzenlemelerden ayıran en önemli farklılık, Tüzüğün AB'de kişisel verilerin korunması hukukunun yeknesaklaştırılması amacıyla oldukça ayrıntılı ve etkili bir sistem kurma çabasıdır. Tüzük, bu hedeften yola çıkarak hem tamamen yeni düzenlemelere yer vermiş, hem de daha önceden var olan düzenlemeleri daha somut ve detaylı olarak düzenlemiştir. Bu doğrultuda öncelikle Tüzüğün bölgesel kapsamı artırılmış ve belirli hallerde Tüzüğün AB dışındaki ülkelere de uygulanabilir olduğu öngörülmüştür. Kişisel verilerin korunması hukukunun gelişiminin ve ilgili düzenlemelerin analiz edilmesi ve Tüzüğün kabul edilmesinin arka planının anlaşılması, ayrıca Tüzüğün detaylıca incelenmesi amacıyla makale iki ana bölüme ayrılmıştır. Bu doğrultuda, 1. Bölüm'de kişisel verilerin korunması hakkının yer aldığı başlıca uluslararası düzenlemelere yer verilecektir. 2. Bölüm'de ise Tüzüğün kapsamı, getirdiği yenilikler, düzenlediği ilkeler, haklar ve yükümlülükler ile kurduğu sistem incelenecektir.

**Anahtar Kelimeler:** GDPR, kişisel veri, veri koruma hukuku, Avrupa Birliği, Genel Veri Koruma Tüzüğü, KVKK.

### ABSTRACT

---

<sup>161</sup> İstanbul Aydın Üniversitesi Hukuk Fakültesi, Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku öğretim üyesi.

<sup>162</sup> ORCID: <https://orcid.org/0000-0003-4034-5436>



The awareness on personal data which relates to basic rights and freedoms raised over time and national and international legal legislations have been adopted correspondingly. European Union General Data Protection Regulation numbered 2016/679 is the most broad in scope and most up-to-date legal text on the matter. The Directive numbered 95/6/EC, adopted in a context where information Technologies weren't as developed as today, failed its principal mission: ensuring uniformity and consistency between data protection laws of member states of European Union. This lead to the occurrence of the need for regulating European data protection law all over again. Based on this need, European General Data Protection Regulation was adopted on May 2016. The most outstanding novelty and difference on the general overview of The Regulation is that The Regulation aims to build a circumstantial and effective system in order to harmonize data protection law in the Europe. Based on this aim, The Regulation engage both creation of entirely new rules and remodeling of existing ones with a more circumstantial and comprehensive approach. In this direction, first the territorial scope of The Regulation was extended and it is provided that The Regulation can be applicable to the countries outside European Union within certain circumstances. This article was divided into two main parts in order to first analyze the development of personal data protection law, related legislations and background of the adoption of The Regulation and then examine the provision of The Regulation in detail. Accordingly, main international texts disposing right to personal data protection are presented in the First Part. The scope of The Regulation, the novelties brought by and the principles, rights and obligations disposed in The Regulation are examined in the Second Part.

**Keywords:** GDPR, personal data, data protection law, European Union, General Data Protection Regulation, KVKK.

## GİRİŞ

Günümüzde en çok duyulan kavramlardan ikisi kişisel verilerin korunması ve yapay zekâ teknolojileridir. Teknolojinin hızla gelişerek her geçen gün hayatlarımıza yeni bir şey kattığı bu dönemde, neredeyse her bireyin kişisel verileri, bireylerin üzerlerinde çeşitli kontrol seviyelerine sahip olduğu işlemlere konu oluyor. İnsanlar kimi zaman kendi istekleri ile verilerini paylaşırlarken, kimi zaman “okudum, anladım” seçeneğine al el acele tıklayıp bunu gerçekleştiriyorlar; kimi zaman ise hiç haberleri olmadan verileri kendileri dışındaki kişilere ulaşıyor. Bu durum, kişisel verileri kullanarak nöral sinir ağları sistemiyle büyük bir hızla gelişen

yapay zekâ teknolojilerine kaynak sağlarken, bir yandan da gözetim toplumunun oluşmasına ve bireylerin sürekli kontrol altında tutulmasına yol açıyor.

Zamanla hakkında bilinçlenme oluşan bir konu olan kişisel veri, bireylerin temel hak ve özgürlükleri ile çok yakından ilgili olması sebebiyle pek çok riski de içinde barındırmakta. Bu nedenle bu alanın yasal düzeyde düzenlenmesi gerekliliği doğmuş ve kişisel verilerin korunması hususu ulusal ve uluslararası seviyede çeşitli belgelerde işlenmiştir. Bu çerçevede kabul edilmiş en geniş kapsamlı ve en güncel düzenleme 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğüdür (Tüzük ya da GDPR).

Kişisel verilerin korunması hukukunun gelişiminin ve ilgili düzenlemelerin analiz edilmesi ve Tüzüğün kabul edilmesinin arka planının anlaşılması, ayrıca Tüzüğün detaylıca incelenmesi amacıyla makale iki ana bölüme ayrılmıştır. Bu doğrultuda, 1. Bölüm’de kişisel verilerin korunması hakkının yer aldığı başlıca uluslararası düzenlemelere yer verilecektir. 2. Bölüm’de ise Tüzüğün kapsamı, getirdiği yenilikler, düzenlediği ilkeler, haklar ve yükümlülükler ile kurduğu sistem incelenecektir.

## **§ 1. Kişisel Verilerin Korunması Hakkı**

Kişisel verilerin korunması hakkı aslında geçmişten beri var olan, fakat günümüzde çok hızlı değişen ve gelişen teknoloji ile birlikte daha görünür hale gelen, önemi artan ve kapsamı genişleyen bir haktır. Bu hak, başlı başına bağımsız bir hak veya diğer bazı hakların bir parçası olarak, yarım asır önce düzenlenmiş belgeler ile dahi korunmaya çalışılmıştır.

Makalenin I. Bölümünde, kişisel verilerin korunması hakkının farklı dönemlerde farklı uluslararası organizasyonlar tarafından nasıl değerlendirildiği, ardından da bu hakkın uluslararası mahkemelerce nasıl yorumlandığı incelenecektir.

### **I. Kişisel Verilerin Korunması Hakkının Gelişimi**

Kişisel verilerin korunması hakkı, uzun bir süre “özel hayatın gizliliği” veya “özel ve aile hayatına saygı” başlıkları altında değerlendirilmiştir. Zamanla bu hakların kapsamlarının birbirinden farklılığı kabul edilmiş ve “kişisel verilerin korunması hakkı” temel haklar içerisinde, ayrı ve bağımsız bir hak olarak değerlendirilmeye başlanmıştır. Gerçekten de birbiriyle çok yakından ilgili olan bu iki hak, gerek içerikleri, gerek devletlere yükledikleri yükümlülükler düşünüldüğünde tam olarak örtüşmemektedir. Örneğin; özel hayatın gizliliği hakkı genel itibarıyla devletlerin bireylerin özel hayatına müdahalesinin yasaklanması nosyonunu korurken, kişisel verilerin korunması hakkı ona kıyasla daha aktif, kişisel verilerin işlenmesi söz konusu olduğunda ilgili bireylerin menfaatlerini korumak amacıyla denetim ve denge sistemlerinin kurulmasını içeren

bir haktır.<sup>163</sup> Kişisel verilerin korunması hakkının gelişimi ve kapsamının tam olarak anlaşılabilmesi için, bu hakkı içeren uluslararası düzenlemelerin incelenmesi faydalı olacaktır.

#### A. OECD

Ekonomik İş Birliği ve Kalkınma Teşkilatı (OECD), 23.09.1980 tarihinde *Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler*'i (OECD Rehber İlkeleri) kabul etmiş ve böylelikle kişisel verilerin korunması ile ilgili uluslararası alanda adım atan ilk kuruluş olmuştur.<sup>164</sup> Söz konusu ilkeler bağlayıcılık taşımamaktadır ve tavsiye niteliğindedir.<sup>165</sup> Yumuşak hukuk kuralı (soft law) olarak nitelendirilen bu kuralların her ne kadar kâğıt üzerinde ve doğrudan bir bağlayıcılığı olmasa da, bunların ülkelerin çoğu tarafından benimsenmesi halinde, ilgili alanda temel başvuru kaynağı olmaktadır<sup>166</sup>. Nitekim OECD'nin Rehber ilkeleri de bu niteliğe ulaşmıştır.

Rehber ilkeler, sekiz temel prensipten oluşur: (1) *Veri toplamının sınırlı olması ilkesi*, (2) *Veri niteliği ilkesi*, (3) *Amacın belirli olması gerektiği ilkesi*, (4) *Kullanımın sınırlandırılması ilkesi*, (5) *Veri güvenliği ilkesi*, (6) *Açıklık ilkesi*, (7) *Bireyin katılımı ilkesi*, (8) *Hesap verme zorunluluğu ilkesi*.

OECD ilkelerinin günümüzde yetersiz kalmasının sebebi, bu ilkelerin teknolojinin şimdiki kadar gelişmiş olmadığı, örneğin; bireylerin sosyal medya hesaplarından kendilerine dair pek çok bilgiyi ve görseli dünyanın her yerinde erişime açık olarak paylaşmadıkları bir dönemde kabul edilmiş olmasıdır. Gelişen teknoloji ve artan internet kullanımı, ilkelerin yayınlandığı zamanda öngörülemeyen yeni riskler ortaya çıkarmıştır.<sup>167</sup> Ayrıca, ilkelerin asıl düzenlenme amacının üye devletlerin ekonomik alanda geliştirilmesi amacından kaynaklanması da bireylerin kişisel verilerinin korunmasının tüm boyutlarıyla incelenmemesine sebep olmuştur.<sup>168</sup>

Bağlayıcı olmamasına rağmen üye devletler kişisel verilerin korunması hukuku alanındaki düzenlemelerinde OECD İlkeleri'ni göz önünde bulundurarak hareket etmiştir.<sup>169</sup>

---

<sup>163</sup> **Christos Giakoumopoulos/Giovanni Buttarelli/Michael O'Flaherty**, Handbook on European Data Protection Law, Publications Office of the European Union, Luxembourg, 2018, s. 19.

<sup>164</sup> **Murat Volkan Dülger**, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019, s. 30.

<sup>165</sup> **Hüseyin Murat Develioğlu**, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul, 2017, s. 7.

<sup>166</sup> Yumuşak hukuk kuralı hakkında ayrıntılı bilgi için bkz: **Andrew T. Guzman/Timothy L. Meyer**, International Soft Law, Journal of Legal Analysis, Volume 2, Issue 1, Spring 2010, s. 171–225.

<sup>167</sup> **Develioğlu**, s. 7.

<sup>168</sup> **Dülger**, s. 50.

<sup>169</sup> **Dülger**, s. 51.

## **B. Birleşmiş Milletler**

### **1. İnsan Hakları Evrensel Beyannamesi**

10 Aralık 1948 tarihinde kabul edilen İnsan Hakları Evrensel Beyannamesinde kişisel verilerin korunması hakkı ayrı bir hak olarak düzenlenmemiştir. Fakat bu durum hakkın korunmasız bırakıldığı anlamına gelmemektedir. Beyannamenin 12. maddesinde hiç kimsenin özel hayatı, ailesi, meskeni veya yazışması konularında keyfi müdahaleye, şeref ve şöhretine karşı tecavüzlere maruz bırakılmayacağı ve herkesin bu karışma ve tecavüzlere karşı kanun yoluyla korunmaya hakkı olduğu<sup>170</sup> belirtilmiştir. Birleşmiş Milletler, kişisel verilerin korunmasını özel yaşamın gizliliği kapsamında değerlendirmiştir.

### **2. Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme**

Kişisel verilerin korunması hakkı, 23 Mart 1976 tarihinde yürürlüğe giren *Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme*'de; hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemeyeceği ve onuru veya itibarının hukuka aykırı saldırılara maruz bırakılmayacağı, ayrıca herkesin bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahip olduğunun düzenlendiği "*mahremiyet hakkı*" altında değerlendirilmiştir.<sup>171</sup> Örneğin, BM İnsan Hakları Komitesi mahremiyet hakkının incelendiği 16. genel yorumunda; kamu otoritelerinin, özel kişi veya kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgi toplanması veya saklanması hukuki düzenlemeye tabii olması gerektiğini belirtmiştir.<sup>172</sup>

### **3. Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler**

Yukarıda belirtildiği üzere, Birleşmiş Milletler, kişisel verilerin korunması hakkını özel hayatın gizliliği altında değerlendirmektedir. Bununla birlikte, gelişen teknoloji ve bilgisayar kullanımının yaygınlaşması, *Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler*'in (BM Rehber İlkeleri) yayınlanması gerekliliğini doğurmuştur.<sup>173</sup> Söz konusu ilkeler, doğrudan kişisel verilerin korunması hakkına ilişkin ilk Birleşmiş Milletler düzenlemesi olması sebebiyle büyük önem arz etmektedir.<sup>174</sup> İlgili kılavuzda aşağıdaki ilkeler

---

<sup>170</sup> UN General Assembly, Universal Declaration of Human Rights, 10 Aralık 1948, 217 A (III), m. 12.

<sup>171</sup> UN General Assembly, International Covenant on Civil and Political Rights, 16 Aralık 1966, United Nations, Treaty Series, vol. 999, p. 171, m. 17.

<sup>172</sup> UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 Nisan 1988, s. 10.

<sup>173</sup> **Dülger**, s. 53.

<sup>174</sup> **Dülger**, s. 53.

düzenlenmiştir: “*Hukuka uygunluk ve dürüstlük ilkesi*”, “*doğruluk ilkesi*”, “*amacın belirliliği ilkesi*”, “*ilgili kişinin verilerine erişim hakkının bulunması ilkesi*”, “*verilerin güvenliği ilkesi*”, “*ayrımçılık yasağı ilkesi*”, “*denetim ve yaptırım ilkesi*”, “*sınır ötesi veri akışı ilkesi*”.

Söz konusu prensipleri düzenlemek suretiyle BM Rehber İlkeleri, üye ülke mevzuatlarında yer alması gereken asgari standartları belirlemeyi amaçlamıştır.<sup>175</sup>

## **C. Avrupa Konseyi**

### **1. 108 No’lu Kişisel Verilerin Otomatik İşleme Tabii Tutulması Karşısında Bireylerin Korunması Sözleşmesi**

1960’lı yıllarda bilişim teknolojilerinin ortaya çıkması ile birlikte bireylerin kişisel verilerinin korunmasını sağlamak için daha detaylı düzenlemelere ihtiyaç duyulmaya başlandı. Bu gereksinimi karşılamak amacıyla Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde 108 No’lu Kişisel Verilerin Otomatik İşleme Tabii Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 No’lu Sözleşme)<sup>176</sup> imzalandı. Bu sözleşme, kişisel verilerin korunması alanında bağlayıcı nitelikteki ilk uluslararası sözleşme olması nedeniyle büyük önem arz eder. Sözleşme, bireyleri kişisel verilerinin işlenmesine bağlı olarak ortaya çıkabilecek zararlardan korumanın yanı sıra, sınırlararası veri akışlarını düzenlemeyi hedefler.<sup>177</sup>

108 No’lu Sözleşme, kamu sektöründe ve özel sektörde gerçekleştirilen her türlü veri işleme faaliyetine uygulanır. Buna yargı ve emniyet teşkilatının veri işlemesi de dahildir<sup>178</sup>. İleride bahsedileceği üzere, bu yönüyle Avrupa Birliği Genel Veri Koruma Tüzüğü’nden farklılaşmaktadır. Çünkü Tüzük, yargı ve emniyet teşkilatı tarafından gerçekleştirilen veri işleme faaliyetlerini kapsam dışı bırakmıştır.

Bu sözleşme ile birlikte, otomatik işlemeye konu olan kişisel verilerin “*adil bir biçimde ve yasal yoldan elde edilip işlenmesi*”, “*belirli ve meşru amaçlar için kaydedilmesi ve bu amaçlara aykırı kullanılmaması*”, “*kaydedilmelerinin amaçlara uygun ve yerinde olması ve aşırı olmaması*”, “*doğru olmaları ve gerektiğinde güncellenmeleri gerektiği*”, “*ilgili kişilerin kimliklerini belirlemeye, kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde imkan verecek bir biçimde saklanması*” prensipleri düzenlenmiştir.<sup>179</sup> Ek olarak, iç hukukta uygun

---

<sup>175</sup> Develioğlu, s. 10.

<sup>176</sup> Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 Ocak 1981, ETS 108 (Convention 108).

<sup>177</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 24.

<sup>178</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 24.

<sup>179</sup> Convention 108, m. 5.

güvenceler sağlanmadıkça özel veri kategorilerinin, yani bireylerin ırksal kökenlerini, siyasi düşüncelerini, dinlerini veya diğer inançlarını ortaya koyan kişisel veriler ile sağlık veya cinsel hayatları ve ceza mahkumiyetleriyle ilgili kişisel verilerin, otomatik işleme tabi tutulamayacağı açıkça belirtilmiştir.<sup>180</sup>

108 No’lu Sözleşmede ele alınmış bir diğer husus ise, bireylerin kendileri ile ilgili olarak saklanan kişisel verileri öğrenme ve gerektiğinde bunları düzeltirme, eğer veriler sözleşmede belirtilmiş ilkelere vücut veren iç hukuk hükümlerinin ihlali suretiyle işlenmiş ise bunları sildirtme hakkıdır.<sup>181</sup>

Sözleşmede belirlenmiş haklar, 9. madde uyarınca, yalnızca (a) taraf devletin kanunlarında öngörülmüş olması ve (b) demokratik bir toplumda (i) devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi veya (ii) ilgili kişinin veya başkasının hak ve özgürlüklerinin korunması için gerekli bir önlem oluşturması hallerinde sınırlanabilecektir.<sup>182</sup> Ayrıca, sözleşme, taraf devletler arasında kişisel verilerin serbest aktarımını öngörürken, yasal düzenlemelerin bu sözleşme ile getirilen seviyede bir koruma sağlamadığı devletlere veri aktarılmasına bazı sınırlamalar getirmektedir.<sup>183</sup>

Bir diğer önemli nokta ise, 108 No’lu Sözleşme AİHM’in yargı yetkisi altında olmasa da, AİHS’in 8. maddesi (özel ve aile hayatına saygı hakkı) kapsamında inceleme yaparken, mahkeme, bu sözleşmeyi dikkate almış ve sözleşmede belirlenmiş prensipler ışığında bu hakka bir müdahale olup olmadığına karar vermiştir.<sup>184</sup>

2001 yılında, 108 No’lu Sözleşme’deki eksiklikleri gidermek için bir adım atılarak, bu sözleşmeye ek niteliğindeki *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol* kabul edilmiştir.<sup>185</sup> Bu kapsamda Ek Protokol, taraf olmayan devletlere sınıraşan veri akışı ve yerel denetleyici makamlarının kurulmasının zorunluluğu konularını düzenlemiştir.<sup>186</sup>

## 2. 108 +

18 Mayıs 2018 tarihinde kabul edilen *Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapılmasına Daire Protokol*’ün (108+) imzalanması

---

<sup>180</sup> Convention 108, m. 6.

<sup>181</sup> Convention 108, m. 8.

<sup>182</sup> Convention 108, m.9.

<sup>183</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 25.

<sup>184</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 25.

<sup>185</sup> **Dülger**, s. 56.

<sup>186</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 26;

ile 108 No’lu Sözleşme modernize edilmiş ve bilişim teknolojilerinin getirdiği yeniliklere uyum sağlanması, dijital alanda gizliliğin korunmasının pekiştirilmesi ve sözleşmenin takip mekanizmalarının güçlendirilmesi hedeflenmiştir.<sup>187</sup> Ek Protokol, 108 No’lu Sözleşmenin önemli prensiplerini tekrar teyit ederek sabitleştirmiş, ayrıca veri işleyen kişilerin sorumluluklarını ve hesap verebilirliklerini artırmış ve bireylere yeni haklar tanımıştır.<sup>188</sup> Fakat 108+ henüz Türkiye tarafından onaylanarak iç hukukumuzda dahil edilmemiştir.

### 3. Avrupa İnsan Hakları Sözleşmesi

II. Dünya Savaşı’nın ardından Avrupa’daki devletleri bir araya getirmek, hukuku, demokrasiyi, insan haklarını ve sosyal gelişimi teşvik etmek amacıyla, Avrupa Konseyi, 4 Kasım 1950 tarihinde *Avrupa İnsan Hakları Sözleşmesi*’ni (AİHS) kabul etmiştir. AİHS’in 8. maddesinde “özel ve aile hayatına saygı hakkı” düzenlenmiş olup<sup>189</sup> bu hak uyarınca “herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir”. Kişisel verilerin korunması hakkı da, bu hak ile korunan kavramlardan biridir. Nitekim, Avrupa İnsan Hakları Mahkemesi (AİHM) birçok kararında devletin gözetim faaliyetlerinin kişilerin özel hayatlarına bir müdahale olduğunu belirtmiştir.<sup>190</sup> Fakat belirtmek gerekir ki, özel hayata saygı hakkı mutlak, dokunulmaz bir hak değildir. Yukarıda bahsedilen maddenin 2. fıkrasında bu hakka müdahaleyi meşru hale getirebilecek amaçlara yer verilmiştir.<sup>191</sup>

Ayrıca, AİHM, özel hayata saygı hakkının yalnızca pasif bir hak olmadığını ve hakkın içeriğinin yerine getirebilmesi için bazı durumlarda devletlere aktif yükümlülükler de yüklediğini pek çok kararında dile getirmiştir.<sup>192</sup>

---

<sup>187</sup> Dülger, s. 55; Giakoumopoulos/Buttarelli/O’Flaherty, s. 26.

<sup>188</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 26.

<sup>189</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 22.

<sup>190</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 23; AİHM, Klass ve Diğerleri v. Almanya, No. 5029/71, 6 Eylül 1978; AİHM, Rotaru v. Romanya [GC], No. 28341/95, 4 Mayıs 2000; AİHM, Szabó and Vissy v. Hungary, No. 37138/14, 12 Ocak 2016.

<sup>191</sup> AİHS m. 8(2): “Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.”

<sup>192</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 23. Örneğin; AİHM, I v. Finlandiya, No. 20511/03, 17 Temmuz 2008; AİHM, K.U. v. Finlandiya, No. 2872/02, 2 Aralık 2008.

## **D. Avrupa Birliği**

### **1. 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi**

95/46/EC sayılı *Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi* (Direktif), 24 Ekim 1995 tarihinde yayınlanmış ve Avrupa Birliği Genel Veri Koruma Tüzüğüyle yürürlükten kaldırılana kadar AB’de veri korumasına ilişkin başlıca yasal düzenleme olmuştur.

Direktif, pek çok Üye Devletin iç hukuklarında daha önceden veri koruması ile ilgili hukuki düzenleme yaptığı bir zamanda, kişisel verilere daha güçlü bir koruma sağlanması ve Üye Devletlerin iç hukuklarını uyumlaştırma ve kişisel verilerin serbest dolaşımını sağlama gereksinimleri sebebiyle ortaya çıkmıştır.<sup>193</sup> Fakat, AB Direktifleri tüm AB ülkelerine doğrudan uygulanmaz; Direktif’te yer alan kurallar, ayrıca bu devletlerin ulusal hukuklarına aktarılmalıdır. Bu aktarım gerçekleşirken, Üye Devletlerin takdir hakkı (ve dolayısıyla marjı) söz konusudur.<sup>194</sup> Bu nedenle, Direktif, farklı ülkelerde farklı şekillerde yorumlanmış ve iç hukuklara yeknesak olarak aktarılamamıştır. Dolayısıyla, Direktif, AB’de kişisel verilerin korunmasına ilişkin yeknesaklığın sağlanmasında başarısız olmuştur.<sup>195</sup>

Genel olarak Direktif, 108 No’lu Sözleşme ve ulusal hukuklarda yer alan ilkeleri yansıtmakta ve çoğunlukla bu ilkeleri detaylandırmaktadır. Direktif’te temel olarak benimsenmiş prensipler *meşruluk ve adillik; kişisel verilerin açık, belirli ve meşru amaçlar için toplanması; şeffaflık; orantınlık; güvenlik ve veri işlemenin denetime tabi olmasıdır.*<sup>196</sup> Ayrıca, Direktif ve 108 No’lu Sözleşme arasında bir etkileşim mevcuttur. Bu etkileşim, her iki belgeyi de kişisel verilerin korunmasına ilişkin olarak olumlu yönde etkilemektedir.<sup>197</sup>

Son olarak belirtmek gerekir ki 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun hazırlanmasında Direktif önemli ölçüde yol gösterici olmuştur.

### **2. Avrupa Birliği Temel Haklar Şartı**

7 Aralık 2000 tarihinde imzalanan ve 1 Aralık 2009 tarihli Lizbon Anlaşması’nın kabul edilmesiyle bağlayıcılık kazanan *Avrupa Birliği Temel Haklar Şartı (AB Şartı)*, kişisel verilerin korunması hakkını ayrı ve bağımsız bir hak olarak düzenlemiştir. AB Şartı’nın “*kişisel verilerin*

---

<sup>193</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 29.

<sup>194</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 50.

<sup>195</sup> **Dülger**, s. 59.

<sup>196</sup> **Dülger**, s. 58.

<sup>197</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 29.



*korunması*” başlıklı 8. maddesinin 1. fıkrasına göre “*herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.*” Aynı maddenin 2. fıkrasında ise kişisel verilerin “*belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde*” kullanılması gerektiği ve “*herkesin kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına*” sahip olduğu hususları düzenlenmiştir. Bunlara ek olarak AB Şartı, söz konusu ilkelerin uygulanması için “*bağımsız bir makam tarafından denetim*” yapılmasını öngörmüştür.<sup>198</sup>

Bu düzenleme ile kişisel verilerin korunması hakkı insan hakları ile temel hak ve özgürlükler kapsamında değerlendirilmiş, ayrıca özel hayatın gizliliğinden de ayrılmıştır; böylece, kişisel verilerin korunması hakkının önemi ortaya konmuştur.<sup>199</sup>

### **3. Adli ve Kolluk Teşkilatında Kişisel Verilerin Korunmasına İlişkin 2016/680 Sayılı Direktif**

96/46/EC sayılı Direktif adli ve kolluk teşkilatının faaliyetleri için uygulama alanı bulmamaktaydı. Bu nedenle, verilerin korunması ile diğer meşru menfaatler arasında bir dengenin kurulabilmesi için başka birtakım belgelerin düzenlenmesi gerekiyordu. Emniyet teşkilatının kişisel veri işlemesi ile ilgili olarak AB kapsamında gerçekleştirilen ilk yasal düzenleme, AB Konseyinin polis ve cezai konularda adli iş birliği hakkında yayınladığı 2008/977/JHA sayılı Çerçeve Kararı’dır. Bu kararın kuralları yalnızca Üye devletler arasındaki polis ve yargı verisi değişimine uygulanmakta, emniyet teşkilatı tarafından ulusal düzeydeki kişisel veri işlemlerini ise kapsam dışı bırakmaktaydı. AB Parlamentosu ve Konseyi’nin 27 Nisan 2016 tarihli ve 2016/680 sayılı “*Yetkili Makamlar Tarafından Suçun Önlenmesi, Soruşturulması, Tespiti veya Kovuşturulması veya Cezai Süreçlerin Yürütülmesi Amacıyla İşlenen Kişisel Verilere İlişkin Gerçek Kişilerin Korunmasına ve Bu Tür Verilerin Serbest Dolaşımına Dair Direktif*” 2008/977/JHA sayılı Çerçeve Kararı yürürlükten kaldırmış ve yukarıda bahsedilen eksikliği gidermiştir. Avrupa Birliği Genel Veri Koruma Tüzüğüne paralel olarak düzenlenen 2016/680 sayılı bu Direktif, emniyet teşkilatı bağlamında kişisel verilerin korunması ile ilgili olarak ayrıntılı bir sistem kurmakla birlikte, kamu güvenliğini ilgilendiren veri işleminin özelliklerini de dikkate almıştır.<sup>200</sup>

Bu Direktif, ceza yargılamalarına dahil olan çeşitli kategorilerdeki bireylerin kişisel verilerinin korunmasını sağlamaktadır. Polis ve ceza yargılaması yetkilileri suçun önlenmesi,

---

<sup>198</sup> European Union, Charter of Fundamental Rights of the European Union, 26 Ekim 2012, 2012/C 326/02, m. 8.

<sup>199</sup> **Dülger**, s. 63.

<sup>200</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 31, 32.

soruşturulması, tespiti veya kovuşturulması ve cezai süreçlerin yürütülmesi amaçlarıyla kişisel veri işlerken, bu direktifin hükümlerine uygun davranmak yükümlülüğü altındadır.<sup>201</sup>

Genel olarak bu Direktif, Avrupa Birliği Genel Veri Koruma Tüzüğündeki ilke ve tanımlara dayanmakta olsa da, polis ve ceza yargılaması alanlarının doğasını dikkate almaktadır.<sup>202</sup>

#### **4. Avrupa Parlamentosu ve Konseyinin 2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi**

12 Temmuz 2012 tarihinde kabul edilen 2002/58/EC sayılı *Elektronik Haberleşme Sektöründe Özel Alanın Korunması ve Kişisel Bilgilerin İşlenmesi Direktifi (E-Gizlilik Direktifi)*<sup>203</sup>, kişisel verilerin telekomünikasyon ve iletişim hizmetleri alanındaki güvenliği, kişisel veri ihlallerinin bildirimi ve bu iletişimlerin gizliliği ile ilgili kuralları düzenlemektedir.<sup>204</sup>

E-Gizlilik Direktifinde sıkça 95/46/EC sayılı Direktife atıf yapılmış olup, esas itibariyle söz konusu Direktifi tamamlayıcı niteliktedir. Ek olarak, bu direktif üye devletlere söz konusu kuralları iç hukuklarına aktarmaları yönünde yükümlülük getirmiştir.<sup>205</sup>

#### **5. 2006/24/EC Sayılı İletişim Trafik Verilerinin Saklanması Direktifi**

15 Mart 2006 tarihinde, Londra Metrosunda yaşanan 7 Temmuz 2005 tarihli bombalı saldırıyı takiben ve onun etkisiyle 2006/24/EC sayılı *İletişim Trafik Verilerinin Saklanması Direktifi* kabul edilmiştir. Bu direktif, iletişim trafik bilgileri ve yer bilgileri ile ilgili hususları düzenlemektedir. Söz konusu direktif uyarınca iletişim hizmetleri kullanan kişilerin iletişim içeriği haricindeki bilgileri yalnızca ciddi suç şüphesi halinde saklanabilecektir.<sup>206</sup>

#### **6. 45/2001 ve 2018/1725 Sayılı Avrupa Birliği Kurumları Veri Koruma Tüzükleri**

95/46/EC sayılı Direktif sadece üye devletler için uygulanabilir olduğundan, AB kurum ve organlarının gerçekleştirdiği veri işleme faaliyetlerini düzenleyecek hukuki bir düzenleme ihtiyacıyla 45/2001 sayılı *Avrupa Birliği Kurumları Veri Koruma Tüzüğü* kabul edilmiştir. 45/2001 sayılı Tüzükte genel itibariyle AB veri koruma rejiminin ilkeleri benimsenmiştir. Tüzüğün uygulama alanı Birlik organ ve kurumlarınca işlenen kişisel verilerdir. Ayrıca, bu tüzük hükümlerinin uygulanmasının takip edilmesi amacıyla bağımsız bir denetim makamı olan Avrupa

---

<sup>201</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 282.

<sup>202</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, 283.

<sup>203</sup> European Parliament and Council of Europe, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 12 Temmuz 2012 (E-Privacy Regulation).

<sup>204</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 33; E-Privacy Regulation, m. 4.

<sup>205</sup> **Dülger**, s. 63.

<sup>206</sup> **Dülger**, s. 63.

Veri Koruma Denetçisi (European Data Protection Supervisor) tesis etmiştir.<sup>207</sup> Avrupa Veri Koruma Denetçisi, veri koruma hukukuna ilişkin düzenlemelerde Birliğe danışmanlık vermek, Birlik kurumlarında veri koruma hukukunun uygulanmasını sağlamak, kurumları denetlemek ve koordinasyonu sağlamakla görevlidir.

GDPR'ın yürürlüğe girmesinden sonra 23 Ekim 2018'de 45/2001 sayılı Tüzüğü ilga eden ve yerine GDPR'la uyumlu düzenlemeler getiren 2018/1725 sayılı Tüzük kabul edilmiştir. Bu yeni Tüzük GDPR ilke ve esaslarını, kamu sektörünün veri işleme konusundaki özelliklerini dikkate alarak AB kurum, kuruluş ve yetkililerinin işlediği veriler bakımından uyarlamıştır. Tüzükte GDPR hükümleri büyük ölçüde benimsenmekle birlikte Birlik bünyesinde kurum ve kuruluşların işleyeceği veriler bakımından bazı istisna halleri düzenlenmiştir. 2018/1725 sayılı Tüzükle AB veri koruma reformunun önemli bir ayağının daha tamamlandığı ve Birlik veri koruma hukukunun daha tutarlı ve modern bir yapıya kavuşturulmuş olduğu söylenebilir<sup>208</sup>.

## 7. *206/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü*

Yukarıda bahsedildiği üzere, 95/46/EC sayılı Direktif bilişim teknolojilerinin günümüzdeki kadar gelişmiş olmadığı bir dönemde kabul edilmiş olup, amaçlarından biri olan AB ülkelerinde kişisel verilerin korunması hukukunda yeknesaklığı da sağlayamamıştır. Bu durum, AB veri koruma yasalarının yeniden düzenlenmesi gereğini ortaya çıkarmıştır ve bu ihtiyaçtan hareketle Mayıs 2016'da Avrupa Birliği Genel Veri Koruma Tüzüğü kabul edilmiştir.<sup>209</sup>

## II. **Kişisel Verilerin Korunması Hakkının Sınırlandırılması**

Kişisel verilerin korunması hakkı ne bağımsız olarak ne de özel yaşamın gizliliği hakkı altında düşünüldüğünde mutlak bir haktır. Dolayısıyla bu hak belirli şartların varlığı halinde meşru olarak sınırlanabilir. Bir hakkın meşru olarak sınırlanmasından bahsedilebilmek için üç aşamalı bir test uygulanır:

(1) Söz konusu müdahale hukuki düzenlemeler tarafından öngörülmüş olmalı ve müdahaleyi düzenleyen mevzuat keyfilikten korumayı sağlayacak nitelikte olup, sonuçları açısından öngörülebilir olmalıdır.

(2) Söz konusu müdahale meşru bir amaç gütmelidir.

---

<sup>207</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 34, 35.

<sup>208</sup> 2018/1725 sayılı Tüzük kabul edilmeden önce kabul edilmiş olan GDPR'ın gerekçesinin 17. maddesinde 45/2001 sayılı Tüzüğün güncellenerek GDPR'la uyumlu hale getirilmesi gerektiği hususu açıkça belirtilmiştir.

<sup>209</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 30.

(3) Söz konusu müdahale demokratik bir toplumda gerekli olmalıdır. Bunun sağlanması için bu müdahale; (a) gerekli ve zararı önlemek açısından ölçülü olmalı ve (b) hakkın özüne zarar vermemelidir.

Bu noktada AİHS’te özel hayata saygı hakkının sınırlandırılması hususunda hangi amaçların meşru amaç kabul edildiği, 8. maddenin 2. fıkrasında belirtilmiştir. Buna göre; “*Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmuş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.*”

## **§ 2. Avrupa Genel Veri Koruma Tüzüğü’nün Ortaya Çıkışı, Uygulama Alanı ve Temel İlkeleri**

Makalenin 1. Bölümünde detaylıca anlatıldığı üzere, değişen ve gelişen teknolojinin getirdiği yenilikler ve doğurduğu riskler ile AB ülkelerinde kişisel verilerin korunması hukukunun yekneksaklaştırılması gerekliliği Avrupa Birliği Genel Veri Koruma Tüzüğü’nün (Tüzük) düzenlenmesi ihtiyacını ortaya çıkarmıştır.

Makalenin 2. Bölümünde, belirli eksiklikleri tamamlamak ve kişisel verilerin korunması hukukunu daha detaylı bir şekilde düzenlemek amacıyla düzenlenen Tüzüğü’nün kapsamı, getirdiği yenilikler, düzenlediği ilkeler, yüklediği sorumluluklar, kurduğu sistem ve bu sistemin nasıl uygulamaya konulacağı bir bütün olarak incelenecektir.

### **I. Tüzüğü’nün Ortaya Çıkma Süreci**

Tüzük, kişisel verilerin korunması hakkının öneminin zamanla daha iyi anlaşılması ve bu hakka ilişkin olarak kendisinden önce var olan düzenlemelerin değişen ve gelişen teknolojiler ile birlikte bu hakkın etkin bir şekilde korunması hususunda yetersiz kalması sebepleriyle ortaya çıkmıştır<sup>210</sup>.

Avrupa Birliği Komisyonu, bu ihtiyaçları göz önünde bulundurarak 95/46/EC sayılı Direktif’te kapsamlı değişiklikler yapılmasını içeren bir Öneri hazırlamış ve 25 Ocak 2012 tarihinde yayımlamıştır.<sup>211</sup> Söz konusu Öneri’yi Avrupa Komisyonu adına Başkan Yardımcısı

---

<sup>210</sup> Jan Philipp Albrecht, “How The GDPR Will Change The World”, Eur. Data Prot. L. Rev. 287, 2016, s. 289.

<sup>211</sup> Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Sec (2012), 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.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf)

Viviane Reding aynı gün kamuoyuna açıklamıştır. Reding, açıklamasında 17 yıl önce Avrupa'da internet kullananların oranının yalnızca % 1 olduğunu bugün ise büyük miktarda verinin saniyeler içinde kıtalar arasında aktarıldığını, Öneri'nin sektörün sağlıklı büyümesini temin ederken, bireylerin dijital ortamda kişisel verilerinin korunmasını da güçlendireceğini vurgulamıştır.<sup>212</sup>

Söz konusu yetersizliğin önemli görünüşlerinden biri de, kişisel verilerin korunmasının daha önce hiçbir düzenlemede Tüzükte olduğu kadar kapsamlı ele alınmamış olmasının yanı sıra, Tüzüğün yürürlükten kaldırdığı ve 1995'ten Mayıs 2018'e kadar Avrupa Birliği'nin kişisel verilerin korunması ile ilgili başlıca belgesi olan 95/46/EC sayılı Direktif'in bağlayıcı olmamasıdır.<sup>213</sup>

Avrupa Birliği'nde kişisel veri alanında ilk önemli düzenleme, 1995 yılında 95/46/EC sayılı Direktif ile yapılmıştır.<sup>214</sup> Bu Direktif 20 yıl yürürlükte kaldıktan sonra, 2016 yılında kabul edilen Genel Veri Koruma Tüzüğü (GDPR), 25 Mayıs 2018 tarihinden itibaren uygulanmaya başlamıştır. Avrupa Birliği müktesebatında, kurucu antlaşmalar, katılım antlaşmaları ve bu antlaşmaların ekleri olan protokoller birincil hukuk kaynaklarını oluştururken; tüzükler, direktifler, kararlar ise ikincil hukuk kaynaklarını oluşturmaktadır. Tüzükler (regulations) ile yönergeler (directives)<sup>215</sup> etkileri itibariyle birbirinden farklıdır.<sup>216</sup> AB Direktifleri, AB üyesi ülkelerin mevzuatlarını belirli bir konuda, somut ilke ve amaçlar doğrultusunda yaklaştırmak ve uyumlu hale getirmek amacıyla AB Bakanlar Konseyi ve AB Komisyonu tarafından çıkarılan yasal metinleri ifade eder. Direktif'e muhatap üye devletler, belirlenen süreler çerçevesinde kendi ulusal mevzuatları ile gerekli düzenlemeleri yapmakla yükümlüdürler. Ancak Direktif hükümleri üye ülkelerde doğrudan uygulama kabiliyetine sahip değildir. Buna karşılık AB Bakanlar Konseyi tarafından çıkarılan Tüzükler, genel kapsama sahiptir ve tüm AB üyesi ülkelerde doğrudan doğruya uygulanırlar. Tüzükler, Topluluk Resmi Gazetesi'nde yayımlandıktan sonra, yürürlük tarihinde tüm üye ülkeler için bağlayıcı metin halini alır.<sup>217</sup> Üye ülkeler bu metinleri doğrudan uygularlar. GDPR, 95/46/EC sayılı Direktif'ten farklı olarak "Tüzük (Regulation)" olarak düzenlenmiştir ve bu yönüyle tüm üye ülkeler için doğrudan bağlayıcı bir yasal metin niteliğindedir.

---

<sup>212</sup> Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, 25 January 2012, [http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm](http://europa.eu/rapid/press-release_IP-12-46_en.htm)

<sup>213</sup> **Albrecht**, s. 289.

<sup>214</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal, L 281, 23/11/1995, p. 31-50. (Data Protection Directive)

<sup>215</sup> Türkçe ifadesi 'yönerge' olarak tercüme edilebilecek olan 'directives' anlaşılabilirliği ve artık Türkçe'de de bu şekilde kullanılması nedeni ile 'Direktif' olarak ifade edilecektir.

<sup>216</sup> **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.

<sup>217</sup> **Tapan**, s. 994.

AB'nin yürürlüğe koyduğu yeni Genel Veri Koruma Tüzüğü, 95/46/EC sayılı Direktif ile kıyaslandığında bireyi daha merkeze alan anlayışı, kırtasiyecilik ve bürokrasiyi devre dışı bırakıp doğrudan uygulamaya ve sonuç almaya yönelik düzenlemeleri ve coğrafi olarak geniş uygulama alanı nedeni ile veri koruma alanında Kopernik devrimi benzeri bir etki yaratacağı ifade edilmiştir.<sup>218</sup> 16. yüzyılda Prusyalı matematikçi ve astronomi bilimcisi Nikolas Kopernik'in ortaya koyduğu yeni evren görüşünde<sup>219</sup> "dünya" değil; "güneş" merkezdedir ve gezegenler sabit bir yörünge üzerinde güneşin etrafında dönerler. Kopernik Devrimi (Copernican revolution) olarak bilinen bu anlayış, 18. yüzyılda Immanuel Kant tarafından felsefe ve düşünce dünyasında yapılmıştır.<sup>220</sup> Buna göre nasıl astronomide Güneş merkez konumuna gelmiş ise, bilme süreçlerinde de özne merkezde olmalı ve bilgi nesnelere değil, nesnelere bilgiye uymalıdır. Yeni Tüzüğün bu çerçevede birey haklarını öne çıkaran yeni bir anlayış getirdiği vurgulanmaktadır.

221

Yaşanan teknolojik gelişmeler ile birlikte bireylerin verilerinin korunmasına her zamankinden daha çok ihtiyaç duyulması karşısında daha 2011 yılının Haziran ayında 95/46/EC sayılı Direktif'in yenilenmesi ihtiyacından bahsedilmiştir.<sup>222</sup> 2012 yılı başında AB Komisyonu, bu

<sup>218</sup> **Christopher Kuner**, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report, June 2012, [http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner\\_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf](http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf) (Son Erişim Tarihi: 10.02.2019)

<sup>219</sup> Nicolaus Copernicus (1473-1543). Kopernik'in teoremini açıkladığı "De revolutionibus orbium caelestium (Göksel Kürelerin Devinimleri Üzerine)" eseri 1543 yılında basılmıştır. Bununla birlikte Kopernik'in ortaya koyduğu yeni evren görüşünün, İran'ın Merage şehrinde Nasiruddin Tusi (1201-1274) tarafından kurulan Maragha Okulu çalışmaları ile ondan 200 yıl önce ortaya konulduğu artık iddia dan öte ortaya konulmuş bir gerçek haline almıştır. Nasiruddin Tusi, Batlamyus'un evren anlayışını eleştirmiş ve samanyolunun yıldızlardan oluştuğunu belirtmiş ve yeni matematik yöntemlerle "çifte bağı teorisini" oluşturmuştur. Bu teoremin Kopernik tarafından aynen kullanıldığını 1906 yılında J.L.E. Dreyer açıklamıştır. Tusi'den sonra aynı okuldan İbnü's Şatir (Ibn al-Shatir) (1304-1375) güneş ve gezegen sistemini ortaya koymuştur. Kopernik'in İbnü's Şatir'in "Nihâyat el-Sül ve Ta'lik el-Ersâd (Nihayat alsul of c Ala' al-Din)" eserlerindeki görüş ve hesaplamaları kullandığı ise ilk kez 1950 yılında Beyrut Amerikan Üniversitesi'nden E.S. Kennedy tarafından açıklanmıştır. Kopernik İbnü's Şatir'in "merkur modeli" ve "ay modeli" hesaplamalarını birebir kullanmıştır. Kopernik'in bu bilim adamlarının eserlerine atıf yapmaması ve onlardan hiç bahsetmemesi, ayrıca hesaplamaları dahi aynen kendi eserine aktarması karşısında, Kopernik'in eserinin iktibasın ötesinde bir intihal olduğu akla gelmektedir. Bkz. **F. Jamil Ragep**, "Copernicus and His Islamic Predecessors: Some Historical Remarks", Mc. Gill University, History of Science Journal, N. XLV, 2007 s. 65-81.

<sup>220</sup> What is the Copernican Revolution in Kant, <https://www.the-philosophy.com/copernican-revolution-kant> (Son Erişim Tarihi: 10.03.2019)

<sup>221</sup> **Dave Elliman**, GDPR: It is time to rethink your approach to privacy, August 11, 2017, <https://www.thoughtworks.com/insights/blog/gdpr-it-s-time-rethink-your-approach-privacy>

<sup>222</sup> Comprehensive Approach on Personal Data Protection in the European Union, June 2011, [https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en)

konuda değişiklik teklifi hazırlamıştır. Ardından Madde 29 Çalışma Grubu,<sup>223</sup> veri koruma alanında yapılacak reforma ihtiyaç duyulduğunu belirtmiştir.<sup>224</sup> 12 Mart 2014 tarihinde GDPR Taslağı, AB Parlamentosu tarafından kabul edilmiştir.<sup>225</sup> AB Konseyi, 15 Haziran 2015 tarihinde Taslak ile ilgili görüşlerini açıklamış, sonraki süreçte müzakereler devam etmiş ve süreç sonunda 27 Nisan 2016 tarihinde GDPR kabul edilerek 4 Mayıs 2016 tarihinde AB Resmi Gazetesi'nde yayımlanmıştır.<sup>226</sup> Tüzüğün yürürlük tarihi olarak ise GDPR'ın 99/2 maddesi ile 25 Mayıs 2018 tarihi belirlenmiştir. Tüzük, bu tarihte yürürlüğe girmiştir.

AB Komisyonu tarafından 95/46/EC sayılı Direktif'in yerini almak üzere açıklanan Genel Veri Koruma Tüzüğü 11 bölüm, 99 madde ve 173 gerekçeden (recitals)<sup>227</sup> oluşmaktadır.

Direktif, kişisel verilerin korunması kapsamında belirli hedefler ortaya koymuş, fakat bu hedeflerin gerçekleştirilme yöntemlerini ülkelerin kendi iç hukuk düzenlemelerine ve Direktifin belirlediği sınırlar dahilinde üye ülkelerin takdirine bırakmıştır.<sup>228</sup> Söz konusu Direktif doğrultusunda, ülkeler ulusal hukuklarında birbirinden farklı düzenlemelere yer vermiş olup, iç hukuktaki bu farklılıklar kişisel verilerin etkin olarak korunabilmesini önünde bir engel oluşturmuştur.<sup>229</sup> Tüzük, bahsi geçen problemleri aşmak düşüncesiyle tamamen bağlayıcı

---

<sup>223</sup> Article 29 Working Group (WP 29). 1998 yılında yürürlüğe giren 95/46/EC sayılı Direktif'in 29 uncu maddesi uyarınca AB üyesi ülkelerin veri koruma otoriteleri, Avrupa Veri Koruma Denetçiliği (European Data Protection Supervisor) ve Avrupa Komisyonu (European Commission) temsilcilerinden oluşan çalışma grubunu ifade eder. Bu Çalışma Grubu karar verici olmamakla birlikte çalışmalarında bağımsızdır ve veri koruma alanında ortaya çıkan sorunların çözümü, güncel konularda görüş hazırlamak gibi yönlendirici bir etkiye sahiptir. GDPR'ın yürürlüğe girmesiyle birlikte Madde 29 Çalışma Grubu sona ermiş ve yerine Avrupa Veri Koruma Kurulu (The European Data Protection Board-EDPB) kurulmuştur. GDPR'ın 68 inci maddesiyle oluşturulan yeni Kurul, AB üyesi ülkelerin veri koruma otorite başkanları ve temsilcileri ile Avrupa Veri Koruma Denetçiliği temsilcilerinden oluşmaktadır. Bkz. European Data Protection Board, [https://edpb.europa.eu/about-edpb/about-edpb\\_en](https://edpb.europa.eu/about-edpb/about-edpb_en)

<sup>224</sup> EDPS, The History of the General Data Protection Regulation, [https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation\\_en](https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en) (Son Erişim Tarihi: 10.03.2019)

<sup>225</sup> Progress on EU Data protection reform now irreversible following European Parliament vote, Strasbourg, 12 March 2014, [http://europa.eu/rapid/press-release\\_MEMO-14-186\\_en.htm](http://europa.eu/rapid/press-release_MEMO-14-186_en.htm)

<sup>226</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4 May, 2016, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG) (Son Erişim Tarihi: 10.03.2019)

<sup>227</sup> Recitals, bir yasal metin ile ilgili beyan, açıklama ve gerekçeleri içerebilmektedir. AB müktesabatında 'recitals' politik düşünceler ile normatif dil olmaksızın, yasal metnin gerekçelerini içeren kısmı ifade etmektedir. Genellikle 'Whereas (iken, dışından anlamı verir)' ile başlarlar. Bkz. Tadas Klimas; Jurate Vaiciukaite, The Law of Recitals in European Community Legislation, ILSA Journal of International & Comparative Law, V. 15, 2008, [https://www.researchgate.net/publication/228152770\\_The\\_Law\\_of\\_Recitals\\_in\\_European\\_Community\\_Legislation](https://www.researchgate.net/publication/228152770_The_Law_of_Recitals_in_European_Community_Legislation)

<sup>228</sup> Dülger, s. 66.

<sup>229</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 29.

niteliktedir ve veri korumaya ilişkin kuralların tüm üye devletlerde yeknesak şekilde uygulanmasını amaçlamaktadır.<sup>230</sup>

## II. Temel Kavramlar

Tüzük ile ilgili detaylı açıklamalardan önce, Tüzüğün uygulama alanını, düzenlediği ilkelerin, hakların ve sorumluluklarının anlamının tam anlamıyla kavranabilmesi için, kişisel verilerin koruması hukukunun temel kavramlarının Tüzük çerçevesindeki tanımlarına değinmek gerekir.

### A. Kişisel Veri

Tüzük uyarınca, “kişisel veri”; *belirli veya belirlenebilir bir gerçek kişiye ilişkin her türlü bilgidir.*<sup>231</sup> Yani, bir kişinin kimliğini açıkça ortaya koyan veya ek bilgiler ile ortaya konulabilir kılan bilgilerdir.<sup>232</sup> Bu bağlamda “belirlenmiş bir gerçek kişi” özellikle isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir.<sup>233</sup> Bir kişinin belirlenebilir olup olmadığı değerlendirilirken; o bireyin belirlenmesi için direkt veya dolaylı olarak kullanılabilecek ve o bireye diğerlerinden farklı bir muamelede bulunulmasını mümkün kılacak makul her türlü araç dikkate alınmalıdır.

Tüzükte kişisel veri kavramı genel olarak 95/46/EC sayılı Direktifle paralel olarak düzenlenmiştir. Ancak kişiyi belirlenebilir kılan her türlü verinin kişisel veri sayılmasını garanti etmek adına Tüzüğün bazı özel vurguları olduğunu belirtmek gerekir. Özellikle Gereke m. 30’da IP adresleri, site çerezleri gibi kişiyi belirlenebilir kılabilen çevrimiçi verilerin kişisel veri olduğunun vurgulanması Tüzüğün öne çıkan yönlerindedir<sup>234</sup>.

### B. Veri Sahibi

Bir bireyin kişisel verilerinin işlenmesi söz konusu ise, kişisel verileri işlenen bu kişi “veri sahibi”dir. Bu anlamda yalnızca gerçek kişiler veri sahibi sıfatına sahip olabilir, dolayısıyla veri

---

<sup>230</sup> Dülger, s. 66.

<sup>231</sup> General Data Protection Regulation (GDPR), m. 4(1).

<sup>232</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 83.

<sup>233</sup> GDPR, m. 4(1).

<sup>234</sup> Mário Fernandes/Alberto Rodrigues da Silva/António Gonçalves, “Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation”, [https://www.researchgate.net/profile/Mario\\_Fernandes14/publication/324054218\\_Specification\\_of\\_Personal\\_Data\\_Protection\\_Requirements\\_-\\_Analysis\\_of\\_Legal\\_Requirements\\_from\\_the\\_GDPR\\_Regulation/links/5ad7b07baca272fdaf8029d1/Specification-of-Personal-Data-Protection-Requirements-Analysis-of-Legal-Requirements-from-the-GDPR-Regulation.pdf](https://www.researchgate.net/profile/Mario_Fernandes14/publication/324054218_Specification_of_Personal_Data_Protection_Requirements_-_Analysis_of_Legal_Requirements_from_the_GDPR_Regulation/links/5ad7b07baca272fdaf8029d1/Specification-of-Personal-Data-Protection-Requirements-Analysis-of-Legal-Requirements-from-the-GDPR-Regulation.pdf) (Son erişim tarihi: 19.07.2019).



koruma kurallarından faydalanabilir.<sup>235</sup> Bu durum, tüzel kişilerin hiçbir şekilde yasal koruma altında olmadıkları anlamına gelmez. Makalenin 1. Bölümünde açıklandığı üzere, AİHS’te özel ve aile hayatına saygı hakkı düzenlenmiş olup, bu hak çerçevesinde kişiler özel ve aile hayatlarına saygı gösterilmesi hakkının yanı sıra, konutlarına ve yazışmalarına saygı gösterilmesi hakkına da sahiptir. AİHM, tüzel kişilere ilişkin verilerin korunmasını, özellikle konut ve yazışmalara saygı hakkı altında ele almaktadır.<sup>236</sup> Bu anlamda veri sahibi kavramı Tüzükte, 108 No’lu Sözleşmeye kıyasla daraltılmıştır: 108 No’lu Sözleşme uyarınca, veri korumasının asıl muhatabı gerçek kişiler olmakta birlikte, bu sözleşmede Taraf Devletler’in veri korumasını ulusal hukukları ile tüzel kişileri de kapsayacak şekilde genişletebileceğini düzenlenmiştir.<sup>237</sup>

Tüzükte ise kişisel verinin tanımı yapılırken açıkça “gerçek kişi” vurgusu yapılmış (m. 4), ayrıca Gerekeç m. 14’te Tüzüğün tüzel kişilerin verileri bakımından uygulanmayacağı açık bir şekilde belirtilmiştir. Bu itibarla Tüzük çerçevesinde veri sahibi tartışmasız bir şekilde sadece gerçek kişiler olabilir.

### C. Kişisel Verilerin Anonim Hale Getirilmesi

Saklama süresinin sınırlandırılması ilkesi uyarınca, kişisel veriler, veri sahiplerinin yalnızca kişisel verilerin işleme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan şekilde tutulur.<sup>238</sup> Dolayısıyla, kişisel verilerin işleme amacı için artık gerekli olmadığı fakat bir süre daha saklanması uygun görüldüğü noktada, ilgili veriler silinmeli veya anonimleştirilmelidir.<sup>239</sup>

Kişisel verilerin anonim hale getirilmesi, bir dizi kişisel veriden, bir kişiyi belirlenebilir kılan unsurların çıkarılması, takiben veri sahibinin belirlenemez hale getirilmesidir.<sup>240</sup> Diğer bir deyişle, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.<sup>241</sup> Anonimleştirme işlemi sonrasında, kişinin belirlenebilir kılınması artık hiçbir şekilde mümkün olmamalıdır.<sup>242</sup>

### D. Takma Ad Kullanımı

Takma ad kullanımı (psödonimleştirme), kişisel verilerin belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacı ile, ek bilgilerin ayrı tutulması ve teknik

---

<sup>235</sup> GDPR, m. 4(1).

<sup>236</sup> *Giakoumopoulos/Buttarelli/O’Flaherty*, s. 84.

<sup>237</sup> *Giakoumopoulos/Buttarelli/O’Flaherty*, s. 85.

<sup>238</sup> GDPR, m. 5(1)(e).

<sup>239</sup> *Giakoumopoulos/Buttarelli/O’Flaherty*, s. 93.

<sup>240</sup> GDPR, Gerekeç 26; *Giakoumopoulos/Buttarelli/O’Flaherty*, s. 93.

<sup>241</sup> 30224 sayılı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, m. 10(1).

<sup>242</sup> GDPR, Gerekeç 26;

ve düzenlemeye ilişkin tedbirlere tabi olması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesidir.<sup>243</sup>

Anonim hale getirilmiş verilerin aksine, psödonimleştirilmiş veriler, kişisel veri olma niteliklerini korurlar, bu nedenle Tüzüğün uygulama alanı içerisinde kalmaya devam ederler.<sup>244</sup>

Kişisel veri tanımı GDPR’da, 95/46/EC sayılı Direktif’e göre daha geniş şekilde düzenlenmiştir. GDPR’da kişisel veri tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi şeklinde tanımlanmışken; 95/46/EC sayılı Direktif’te kişisel veri ilgilisi kişi ve kişilik özellikleri ile sınırlı şekilde tanımlanmıştı (95/46/EC, m. 2/1-a). GDPR kapsamında kişiye ait isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktörü de bu kapsamda belirtmiştir (GDPR, m. 4/1). Takma ad şeklinde kullanılan veriler de korunabilir kişisel veriler kapsamına dahil edilmiştir.

GDPR’in 4/5 maddesiyle takma ad kullanımı (pseudonymisation), kişisel verilerin tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacı ile ek bilgilerin ayrı şekilde tutulması ile teknik/organizasyonel tedbirlere tabi tutulması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesi olarak tanımlanmıştır. Takma ad kullanımı ile oluşturulan veriler de GDPR kapsamında kişisel veriye dahil kabul edilmiştir (GDPR, rec. 26). Çünkü bu veriler ek bilgiler ile yeniden tanımlanabilir ve kişiye atfedilebilir niteliktedir. Bu açıdan anonimleştirme, takma ad kullanımından farklıdır. Anonimleştirilmiş veriler, veri konusu tanımlanamayacak hale getirilmiş verileri ifade eder. Bu nedenle GDPR veri koruma ilkeleri istatistiksel ve araştırma amaçları dahil olmak üzere, anonimleştirilmiş veriler için geçerli bir koruma sistemi getirmez (GDPR, rec. 26).<sup>245</sup>

## **E. Veri İşleme**

Veri işleme faaliyeti, otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarılma veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya

---

<sup>243</sup> GDPR, m. 4(5).

<sup>244</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 94.

<sup>245</sup> Handbook on European Data Protection, s. 94.

işlem dizisidir. Diğer bir deyişle, kişisel veri üzerinde ve ona ilişkin gerçekleştiren her faaliyet veri işlemedir.<sup>246</sup>

## F. Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu, yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçları ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır.

Veri işleyen ise, veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır.<sup>247</sup>

İki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde ise bu veri sorumluları “ortak veri sorumluları”dır.<sup>248</sup>

Sorumlulukların belirlenmesi açısından kimin veri sorumlusu, kimin veri işleyen olduğunun belirlenmesi çok önemlidir. Veri sorumlusu ve veri işleyen arasındaki ayrım; veri sorumlusunun veri işlemenin amaçlarını ve yöntemlerini belirleyen tüzel veya gerçek kişi, veri işleyen ise veri sorumlusu adına ve onun talimatları uyarınca veri işlemeyi gerçekleştiren kişi olmasıdır.<sup>249</sup>

Belirtildiği üzere, veri sorumlusu bir gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ olabilir. Bununla ilgili olarak Madde 29 Çalışma Grubu, bireylerin haklarını kullanabilmeleri amacı ile, veri işlemenin tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organ tarafından gerçekleştirilmesi halinde, bu tüzel kişi, kuruluş, kurum veya organın içerisindeki belirli bir insanın veri sorumlusu olarak değerlendirilmesinden, ilgili tüzel kişi, kuruluş, kurum veya organın veri sorumlusu olarak düşünülmesi gerektiğini belirtmektedir.<sup>250</sup>

Veri işleyen, Birlik ya da Üye Devlet hukuku çerçevesinde bu yönde hareket etmesinin gerekmemesi durumunda, veri sorumlusundan aldığı talimatlar haricinde veri işleme faaliyeti gerçekleştiremez.<sup>251</sup> Nitekim, veri sorumlusu ve işleyen arasındaki sözleşme, bu ilişkinin kurulabilmesi için yasal bir zorunluluktur. Bu sözleşme, veri sorumlusu ile ilgili olarak işleyen açısından bağlayıcıdır ve işleme faaliyetinin konusu ve süresi, işleme faaliyetinin mahiyeti ve

---

<sup>246</sup> GDPR, m. 4(2).

<sup>247</sup> GDPR, m. 4(7), 4(8).

<sup>248</sup> GDPR, m. 26(1).

<sup>249</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 101.

<sup>250</sup> Article 29 Working Party (2010), Opinion 1/2010 on the concepts of “controller” and “processor”, WP 169, Brussels, 16 Şubat 2010.

<sup>251</sup> GDPR, m. 29.

amacı, kişisel verilerin türü ve veri sahiplerinin kategorileri ile veri sorumlusunun yükümlülükleri ve haklarını ortaya koyar.<sup>252</sup>

Veri işleyenin işleme faaliyetini veri sorumlusunun talimatlarına aykırı olarak gerçekleştirirse, veri işleyen, talimatlardan ayrıldığı ölçüde veri sorumlusu olarak değerlendirilir.<sup>253</sup> Böyle bir durumda, Madde 29 Çalışma Grubu ortak veri sorumluluğunun olduğunu varsaymaktadır.<sup>254</sup>

Değinilmesi gereken diğer bir nokta, veri işleyenin, veri sorumlusunun önceden verdiği spesifik veya genel yazılı onay olmaksızın başka bir işleyenle çalışmasının yasaklanmış olmasıdır.<sup>255</sup>

Veri sorumlusu, tek başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçları ve yöntemleri belirleyen kişi/topluluktur (GDPR, m. 4/7). İşleyici (processor) ise veri sorumlusu adına kişisel verileri işleyen kişi/topluluk olarak ifade edilmiştir (GDPR, m. 4/8).<sup>256</sup> 95/46/EC sayılı Direktif'te de yer alan bu farklılık, GDPR'da da korunmakla birlikte 95/46/EC sayılı Direktif'te sorumluluk sadece veri sorumluları açısından getirilmişken, GDPR ile her ikisine de belirli ölçüde sorumluluk getirilmiştir. Veri ilgilileri, GDPR'ın 79. maddesi uyarınca hem veri sorumlusu hem işleyenle karşı dava açma hakkına sahiptir. GDPR'ın 82. maddesi uyarınca veri sahibinin her ikisine karşı tazminat davası açma hakkı da bulunmaktadır. Ayrıca örneğin denetim makamına veri ihlalinin gecikmeksizin (without undue delay) bildirilmesi yükümlülüğü hem veri sorumluları, hem veri işleyenler için getirilmiştir (GDPR, m. 33/1-2). Bu şekilde veri işleyenler açısından da genişleyen bir sorumluluk rejimi kabul edilmiştir.

#### **f. Ortak Veri Sorumluluğu (Joint Controllers)**

Ortak veri sorumluluğu (joint controllers) terimi GDPR ile getirilen önemli yeniliklerden bir tanesidir. Bununla birlikte 95/46/EC sayılı Direktif'te yer alan veri sorumlusu tanımında da

---

<sup>252</sup> GDPR, m. 28(3).

<sup>253</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 108, 109.

<sup>254</sup> Article 29 Working Party (2010), Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Brussels, 16 Şubat 2010), s. 25.

<sup>255</sup> GDPR, m. 28(2).

<sup>256</sup> Bu tanımlar 95/46/EC sayılı Direktif'in 2. maddesindeki tanımlarla benzerdir. 95/46/EC sayılı Direktif'te yer alan veri sorumlusu tanımı da Avrupa Konseyi'nin veri koruması alanındaki ilk önemli sözleşme kabul edilen 108 sayılı Sözleşmesi'nin 2/d maddesinde yer alan "dosya kontrolörü (controller of the file)" tanımından alınmıştır. Bkz. European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No. 108, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> Sözleşme'nin 223 sayılı Sözleşme ile güncellenen versiyonunda ise veri sorumlusu, tek başına veya diğerleriyle birlikte veri işleme konusunda karar verme yetkisine sahip olan gerçek veya tüzel kişi, kamu otoritesi, hizmeti, ajansı veya diğer herhangi bir yapı şeklinde tanımlanmıştır. Bkz. Güncellenen 108 sayılı Sözleşme, <https://rm.coe.int/16808ade9d,m.2/d>.

“kişisel verilerin işleme araçlarını ve amaçlarını tek başına veya diğerleriyle ortaklaşa belirleyen” ifadesi ile birden fazla veri sorumlusu olması halinden bahsedildiği görülmektedir.

GDPR'ın 26. maddesi “ortak veri sorumluları (joint controllers)” başlığı ile düzenlenmiştir. Maddeye göre iki ya da daha fazla sayıda veri sorumlusu şayet verilerin işleme amaçlarını ve yöntemlerini birlikte belirlemişlerse, bu halde ortak veri sorumlusu olarak nitelendirileceklerdir. Eğer bir şirket, kişisel verilerin hangi araçlarla (how) ve hangi amaçlar için (why) işleneceğini belirliyor ise o takdirde, veri sorumlusu olarak kabul edilmektedir. Eğer birden fazla şirket, bu süreci birlikte yerine getiriyor ise, şirketler “ortak veri sorumluları (joint controllers)” olarak nitelendirilecektir (GDPR, m. 26). Bu anlamda örneğin bir şirket faaliyet alanı ile ilgili bir alt şirkete çalışanlarının muhasebe işlerini yaptırıyor ise, bu alt muhasebe şirketi verileri işleyen (processor), asıl şirket ise veri sorumlusu (controller) olarak çalışanların kişisel verilerinden sorumlu olacaktır. Bir başka örnek olarak online ortamda bebek bakıcılığı hizmetleri sunan bir şirket, bir başka şirket ile de bebek için gerekli olan oyun, DVD gibi araçların kiralanması için sözleşme yapmış olabilir. Her iki şirket de, hizmetlerin sunulduğu web sitesinin teknik kurulumunda yer almaktaysalar, her iki şirket “ortak veri sorumlusu (joint controller)” sıfatı ile müşterilerinin kişisel verilerinin korunmasından sorumlu olacaklardır.<sup>257</sup>

Veri sorumlularının sorumlulukları AB hukuku veya üye devlet hukukunca belirlenmediği takdirde, ortak veri sorumlularının sorumlulukları ve GDPR kapsamındaki yükümlülüklerle uygunlukları, aralarında yapacakları anlaşmayla şeffaf bir şekilde belirlenecektir. Bununla birlikte, veri sahibi GDPR kapsamındaki haklarını her veri sorumlusu açısından ve her birine karşı kullanabilir. Bu belirlemenin sorumluluğun açık bir şekilde tayinine imkân verecek şekilde yapılması gerekir (GDPR, rec. 79). Bu nedenle aralarındaki sorumluluk belirleme anlaşmasının yazılı yapılması 26. madde ile şart koşulmamakla birlikte, şeffaflık, açıklık, sorumluluğun tayini ve ispat açısından yazılı yapılmasında fayda bulunmaktadır.

Gerçek kişinin kişisel verilerinin ihlalden doğan zararlardan hem veri işleyenler hem veri sorumluları birlikte sorumlu olacaklardır. Ortak veri sorumluların bulunduğu aynı işlemlerden doğan zararlardan, her veri sorumlusu veya işleyen tüm zarardan sorumlu olacaktır (GDPR, rec. 146 ve m. 82/4). Bununla birlikte ortak veri sorumluları aynı adli sürece katılmışlar ise, iç düzenlemelerindeki sorumluluklarına göre zararın tazmin edilmesine karar verilebilecektir (GDPR,

---

<sup>257</sup> Örnekler için bkz. What is a Data Controller or a Data Processor, [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor\\_en#references](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en#references)

rec. 146 ve m. 82/5).

ABAD (Avrupa Birliği Adalet Divanı) nezdinde karara bağlanan bir uyuşmazlıkta hem Facebook hem de Facebook üzerinde fan sayfasını yöneten şirket “ortak veri sorumlusu” olarak veri işlenmesinden sorumlu tutulmuşlardır.<sup>258</sup> Karara konu olayda Alman şirketi Wirtscharft akademie Schleswig-Holstein Şirketi, Facebook’ta yer alan fan sayfaları aracılığıyla eğitim hizmetleri sunmaktadır. Facebook Insights uygulaması ile fan sayfasını ziyaret eden kullanıcıların bilgisayarlarına çerez/cookies yerleştirilmekte ve bu sayede Alman şirket ve Facebook kullanıcılara ait kişisel bilgileri toplanmaktadır. Bu ihlal nedeniyle Almanya’nın Schleswig-Holstein eyaleti Veri Koruma Otoritesi’ne (Unabhängiges Landeszentrum für Datenschutz-ULD) başvuru yapılır ve 2011 yılında ULD, Şirketin, Facebook fan sayfasının kullanımını durdurmasını çünkü kullanıcıların rızası alınmaksızın Facebook ve şirket tarafından kişisel verilerin kayıt edildiğini belirtir. Şirket, olayda kişisel verileri işleyen kendisi değil Facebook olduğunu belirterek yargı yoluna başvurur ve mahkeme olayı ABAD önüne taşır. ABAD, 5 Haziran 2018 tarihinde verdiği Karar’da hem Wirtscharftakademie Şirketi’nin hem de Facebook’un “ortak veri sorumlusu (joint controller)” niteliği taşıdığını ve sorumlusu olduğuna karar vermiştir. Wirtscharftakademie Şirketi, Facebook’ta fan sayfasının parametrelerini tanımlayarak ve bu fan sayfasını yönetmek ve kullanıcılara tanıtmak sureti ile ortak sorumlu olmuştur. Facebook Insights uygulaması ile toplanan kişisel verilere ilişkin ne Facebook tarafından ne de Wirtschaftsakademie şirketi tarafından kullanıcılar bilgilendirilmemiştir. Burada toplanan kişisel veriler, fan sayfasının ne zaman ziyaret edildiği, hangi ülkeden ziyaret edildiği, yaş grupları, kişilere ilişkin diğer kişisel verilerden oluşmaktadır. ABAD, Wirtscharftakademie Şirketinin, kişisel verileri kendisi toplaması dahi Facebook Insights uygulaması sayesinde kişisel verilerin işlenmesini talep edebileceğini ayrıca toplanan bu verilerden kendi faaliyetlerinde faydalanabileceğini belirlemiştir. Bu nedenle hem Facebook İrlanda, hem de Wirtscharftakademie Şirketinin veri ihlalden dolayı ortaklaşa sorumlu olduğuna karar verilmiştir. Eylemin oluş zamanı itibarıyla 95/46/EC sayılı Direktif’in ortak sorumluluk esası uygulanmış ve GDPR’ın 26. maddesi uygulanmamıştır. Ancak ABAD’ın GDPR 26. maddesine yaklaşımının da bu tür durumlarda birlikte sorumluluk şeklinde değerlendirilebileceği anlaşılmaktadır. Bununla birlikte ABAD, sorumluluğun eşit derecede olmayacağını da altını çizmiştir.<sup>259</sup>

---

<sup>258</sup> Judgment of the Court (Grand Chamber), C-210/16, 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, Interveners: Facebook Ireland Ltd., Vertreter des Bundesinteresses beim Bundesverwaltungsgericht.

<sup>259</sup> ABAD, C-210/16, paragraf 43.

### **III. Tüzüğün Uygulama Alanı**

#### **A. Genel Olarak**

Tüzüğün maddi kapsamı 2. maddede belirtilmiştir. Buna göre “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.”<sup>260</sup>

Fakat, Tüzükte açıkça belirtildiği üzere, Tüzük, 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 işlenmesine uygulanmaz.<sup>261</sup> Böyle bir durumda Adli ve Kolluk Teşkilatında Verilerin Korunmasına İlişkin 2016/680 Sayılı Direktif uygulama alanı bulacaktır.

#### **B. Tüzüğün Kişi Bakımından Uygulama Alanı**

Tüzük düzenlemeleri veri sorumlusu ve veri işleyenler bakımından yükümlülük ve sorumluk doğuracak, veri sahipleri de Tüzük uyarınca korunacaktır. Bu nedenle kimin veri sorumlusu, kimin veri işleyen ve kimin veri sahibi olduğunun tespit edilmesi büyük önem arz etmektedir.<sup>262</sup>

Tüzüğün kişi bakımından uygulamasında veri sorumluları ve veri işleyenler açısından bir sınırlama öngörülmüştür. Konu bakımından sınırlamayla iç içe olan bu sınırlamaya göre; Tüzüğün tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından gerçekleştirilen veri işlemlere uygulanmayacağı açıkça düzenlenmiştir.<sup>263</sup>

Veri sahipleri yönüyle kişi bakımından tek sınırlama gerçek kişi olma koşuludur. Tüzükte kişisel verinin tanımı yapılırken açıkça “gerçek kişi” vurgusu yapılmış (m. 4), ayrıca Gereke m. 14’te Tüzüğün tüzel kişilerin verileri bakımından uygulanmayacağı açık bir şekilde belirtilmiştir. Bu itibarla Tüzük sadece kişisel verisi işlenen gerçek kişiler bakımından uygulanacaktır.

#### **C. Tüzüğün Yer Bakımından Uygulama Alanı**

Tüzük, Avrupa Birliği temelli bir düzenleme olmasına rağmen, coğrafi olarak uygulama alanı Avrupa Birliği sınırlarından daha geniştir.<sup>264</sup> Öncelikle, 3. maddenin 1. fıkrası uyarınca

---

<sup>260</sup> GDPR, m. 2.

<sup>261</sup> GDPR, m. 2(2)(d).

<sup>262</sup> Paul Voigt/Axel von dem Bussche, The EU GDPR: A Practical Guide, Springer, Heidelberg, 2017, s. 17.

<sup>263</sup> GDPR, m. 2(2)(c).

<sup>264</sup> Voigt/von dem Bussche, s. 22.

“Tüzük, işleme faaliyeti Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisindeki bir veri sorumlusu veya veri işleyen işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır.” Bunun yanı sıra, aynı maddenin 2. fıkrası, Tüzüğün, Avrupa Birliği ile içerisindeki işlemler ile sınırlı olmadığını ve Tüzüğün, işleme faaliyetlerinin belirli hususlarla alakalı olması durumunda, Birlik içerisinde bulunan veri sahiplerinin kişisel verilerinin Birlik içerisinde kurulu olmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesine uygulanacağını düzenlemektedir. Buna göre Tüzük “veri sahibine bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu veri sahiplerine mal ya da hizmetlerin sunulması” veya “veri sorumlusu veya işleyen davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi” hallerinde uygulama alanı bulacaktır. Bunlar dışında Tüzük ayrıca, “Birlik içerisinde olmamasına rağmen uluslararası kamu hukukuna istinaden bir üye devletin hukukunun uygulandığı bir yerde kurulu bulunan bir veri sorumlusu tarafından kişisel verilerin işlenmesine uygulanır.”

GDPR'ın önemli yeniliklerinden bir tanesi de uygulama alanının (territorial scope) genişletilmiş olmasıdır (extraterritorial scope)<sup>265</sup>.

Avrupa Konseyi'nin 10 Ocak 1985 tarihinde yürürlüğe giren 108 sayılı Sözleşmesi'nin 1. maddesiyle uygulama alanı açısından üye ülke toprakları esas alınmıştır. Buna göre uyruğu ve ikameti ne olursa olsun, “her bir Taraf ülkedeki gerçek kişinin hakları” güvence altına alınmaktadır. Bununla birlikte 108 sayılı Sözleşme'nin değişen koşullara uyarlanması amacıyla oluşturulan 2014 tarihli Taslak'ta “ülkesel (territorial)” yaklaşım yerine, veri işleme öznelerinin yargılama yetkileri (jurisdiction) esas alınmıştır. Bu yeni ifade, Sözleşme'nin 10 Ekim 2018 tarihinde güncellenen 223 sayılı Sözleşme'de kabul edilmiştir.<sup>266</sup> Bu ifade tanımlanmamakla birlikte, Sözleşme'nin ilk haline göre uygulama alanını her üye ülkenin yargılama yetkilerinin yorumuna göre genişleteceği muhakkaktır.<sup>267</sup>

95/46/EC sayılı Direktif'te uygulama alanını düzenleyen 4/a bendi ile veri sorumlusunun yerleşik olduğu yer, 4/c bendi ile ise veri işlemede kullanılan otomatik cihazların bulunduğu yer

---

<sup>265</sup> Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 3. [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_3\\_2018\\_territorial\\_scope\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf) (Son erişim: 19.07.2019)

<sup>266</sup> Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 223, Strasbourg, 10.X. 2018, <https://www.coe.int/en/web/conventions/full-list/>

<sup>267</sup> **Paul de Hert/Michal Czerniawski**, “Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context”, *International Data Privacy Law*, V. 6, No. 3, 2016 (s. 230-243), s. 232.



esas alınmıştır. 95/46/EC sayılı Direktif'in 4/a bendinin uygulanması için ilk olarak veri sorumlusunun AB üyesi ülkelerde bulunması hali, ikinci aşamada ise veri işleme faaliyetinin bu veri sorumlusunun faaliyetlerinden kaynaklanmış olması hali dikkate alınmıştır.<sup>268</sup>

GDPR'da konunun düzenlendiği 3. Maddenin1. fıkrasında öncelikle AB topraklarındaki bir veri sorumlusu/işleyenin faaliyetleri esas alınmıştır. Bu düzenleme 95/46/EC sayılı Direktif'in 4/1 maddesi ile uyumludur. Ancak bentte yer alan "işleme faaliyetinin Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın" ifadesi de uygulama alanını genişletici etki doğurabilecektir. Çünkü AB topraklarında yer alan bir veri sorumlusunun AB toprakları dışındaki veri işleme faaliyetleri esas alındığında da uygulanacaktır.<sup>269</sup>

GDPR'ın 3/2 maddesi ise veri sorumluları ve işleyenlerin AB dışında faaliyet göstermesi durumunda da GDPR'ın uygulama alanı bulmasını sağlamaktadır. Buna göre veri veri sorumlusu/işleyen şirketin merkezi ve faaliyet alanı AB dışında olsa dahi, şayet AB topraklarında bir mal ve hizmet sunumunda bulunuyor ise bu şirketin olası kişisel veri ihlali durumunda GDPR hükümleri uygulanabilecektir. Bu ihtimalde, veri sahibine herhangi bir ödemede bulunulması şartı da aranmamaktadır (GDPR, m. 3/2-a). Bu durum, internetin söz konusu olduğu günümüzde GDPR uygulamasını aşırı genişletici bir etki doğurmaktadır.<sup>270</sup> Çünkü herhangi bir web sitesine dünyanın her yerinden girilebilmektedir. Örneğin ABD'de faaliyet gösteren bir seyahat şirketinin web sitesini kullanan bir AB vatandaşı, bu site aracılığıyla ABD'de bir otele rezervasyon yapmış olsa, bu takdirde ABD şirketi bu kişi açısından GDPR uygulaması ile karşılaşabilecektir. Aynı şekilde Türkiye'de faaliyet gösteren şirketler de, bu olasılıkları dikkate alarak GDPR uyumluluğunu sağlamakla yükümlü olabileceklerdir. Bu geniş uygulama alanı hem ülkeler ve bu ülkelerde faaliyet gösteren şirketler açısından hem de hakları ihlal edilen bireyler bakımından belirsizlik oluşturabilecek niteliktedir. Çünkü ne zaman hangi ülke hukuku ile karşılaşılacağı birey açısından da net değildir. Bu gibi durumlarda, GDPR'nın uygulama alanının belirlenmiş olması diğer ulusal kanunları devre dışı bırakmayacaktır ve kanunlar ihtilafı kurallarının uygulanması kaçınılmaz olacaktır. GDPR'da bu uygulama gerçek kişilerin GDPR'ın koruma haklarından mahrum olmamaları için konulduğu belirtilmekte ve bu tür bir veri sorumlusu/işleyenin AB içindeki veri sahiplerine mal/hizmet sunup sunmadığının belirlenmesi için bunun öngörülüp öngörülmediğinin (envisages) öncelikle belirlenmesi gerektiği ifade edilmektedir (GDPR, rec. 23). Veri

---

<sup>268</sup> Hert/Czerniawski, s. 233.

<sup>269</sup> Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 12.

<sup>270</sup> Hert/Czerniawski, s. 237.

sorumlusu/işleyeninin sadece web sitesinin AB içinden erişilebilir olması durumunda, şirketin e-posta adresi, diğer iletişim ayrıntıları, kullanılan dil, kullanılan para birimi ve AB içindeki müşterilerin yorumları gibi değerlendirmeler dikkate alınabilecektir. Şirketin nerede kurulmuş olduğu bu belirlemeleri yapmak için yeterli olmayacaktır (GDPR, rec. 23). Bununla birlikte, GDPR'nın 3/2-a maddesiyle getirilen AB vatandaşlarının korunmasına yönelik bu yetki düzenlemesinin, GDPR'nın 23. gerekçesiyle yumuşatıldığı ve internet şirketlerine GDPR dışına çıkma şansı verdiği ifade edilmektedir. Buna örnek olarak AB dışından örneğin bir Çin şirketi, global ölçekte oluşturduğu internet sitesinde ürün kataloglarını sergiler. Bu kataloglara dünyanın her yerinden erişim sağlanabilir. Bu aşamada kullanıcılar herhangi bir kişisel verisini kayıt ettirmeksizin, bu katalogları inceleyebilmektedir. Dolayısıyla bir AB vatandaşı bu kataloglardan bir ürün beğense, bu aşamada henüz GDPR uygulanması mümkün olmaz. Ne zamanki kullanıcı ürünü seçip almak için bağlantıyı tıklar. Bu halde kullanıcının önüne üçüncü kişiye ait yeni bir web sitesi açılır. Bu sitede 23. gerekçeye uygun araçlar bulunmaz. Örneğin para birimi Euro değil, ABD dolarıdır. Kullanıcı kişisel verilerini bu yeni web sitesinde kayıt ettirir. Bu üçüncü kişiye ait web sitesi, GDPR kapsamında olmadığını iddia edebilir çünkü AB üyesi ülkelere mal ve hizmet sunumu yapan bu site değil, Çin menşeli şirkete ait ilk web sitesidir. Dolayısıyla bu siteden bir mal ve hizmet sunumu gerçekleşmemiştir. Dolayısıyla GDPR yetkisini doğuran olayın sadece mal ve hizmet sunumuna indirgenmesi eleştirilmiştir. Oysa bu ifade “pazarlama (marketing) ile bağlantılı (related to marketing)” veya “mal/hizmet tedariki (supply of goods or services)” şeklinde ifade edilse yahut daha basit şekilde “AB içindeki veri sahibi ile bağlantılı” şeklinde ifade edilse, GDPR uygulama alanının daha net ve kesin olacağı ifade edilmiştir.<sup>271</sup>

GDPR'nın 3/2-b maddesiyle AB dışında merkezi olan sosyal medya şirketlerinin hedef alındığı açık olan bir düzenleme yer almaktadır. Buna göre davranışların AB içinde gerçekleştiği ölçüde, AB içindeki tüketicilerin (veri sahiplerinin) davranışlarının izlenmesi durumunda GDPR uygulama alanı bulacaktır<sup>272</sup>. Dolayısıyla AB içinde müşteri tabanı bulunan ve online davranışsal reklamcılık faaliyetinden faydalanan tüm sosyal ağ şirketleri, arama motoru şirketleri veya diğer şirketler bu madde düzenlemesi nedeniyle GDPR uygulamasına muhatap olabileceklerdir. Bu düzenlemede yer alan “davranışların AB içinde gerçekleştiği ölçüde (as far as their behaviour takes place within the Union)” ifadesi, veri sorumlusu ile veri sahibi arasında tek bağlantının veri

---

<sup>271</sup> **Robert Madge**, Five Loopholes in the GDPR, August 27, 2017, <https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b> (Son Erişim Tarihi: 20.03.2019).

<sup>272</sup> Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 12.

sahibinin AB üyesi ülkelerde ikamet etmesi olduğu, gevşek bağlantılı durumlarda GDPR'nın uygulanmasının önüne geçecektir.

Veri işleme faaliyetinin “veri sahiplerinin davranışlarının izlenmesi” olarak nitelendirilebilmesi için, başta veri sahibinin kişisel tercihleri, davranışları ve tutumlarını analiz etmek veya tahmin etmek veya o kişiyle ilgili kararlar almak için bir gerçek kişinin profilinin çıkarılması gibi, kişisel veri işleme tekniklerinin kullanımını içeren internette gerçek kişilerin izlenmesi olup olmadığı tespit edilmelidir (GDPR, rec. 24). Bu kapsamda Facebook, Google, Twitter gibi şirketlerin GDPR uygulama alanına dahil olduğu açıktır.

#### D. Tüzüğün Konu Bakımından Uygulama Alanı

Tüzük, AB hukuku kapsamına girmeyen faaliyetler ile AB üyesi devletler tarafından AB Antlaşması'nın Beşinci Başlığının İkinci Bölümü<sup>273</sup> kapsamına giren faaliyetlere ilişkin olarak kişisel verilerin işlenmesi halinde uygulanmayacaktır. Ayrıca tamamen kişisel veya ev faaliyetleri esnasında bir gerçek kişi tarafından kişisel verilerin işlenmesi ile kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dahil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkili makamlar tarafından kişisel verilerin işlenmesi halinde de Tüzük uygulanmayacaktır (GDPR, m. 2/2).

### IV. Temel İlkeler

#### A. Hukuka Uygunluk, Adillik ve Şeffaflık

##### 1. Hukuka Uygunluk

Kişisel verilerin hukuka uygun olarak işlenmesi ilkesi; veri işlemenin, veri sahibinin rızası veya Tüzükte düzenlenmiş diğer bir hukuka uygunluk sebebine dayanılarak gerçekleştirilmesi gerekliliğini ifade eder. Veri işlemenin hukuka uygunluğu, Tüzüğün 6. maddesinin 1. fıkrasında düzenlenmiştir. Buna göre veri sahibinin rızası olmamasına rağmen veri işlemenin hukuka uygun olması için işleme faaliyetinin,

(i) veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için,

(ii) veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile,

(iii) veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile,

---

<sup>273</sup> Avrupa Birliği Andlaşması, Beşinci Başlık, İkinci Bölümü, AB ortak dış ve güvenlik politikasına ilişkin özel hükümleri içerir. Bkz. Consolidated Version of The Treaty on European Union, Official Journal of the European Union, C 326/13, 26.10.2012.

(iv) kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması hususunda,

(v) özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda,

gerekli olması aranmaktadır.<sup>274</sup>

## 2. Adillik

Veri işleminin Tüzükte yer alan ilkelere uygun olması için adil olması gerekir. Bu anlamda, işleme faaliyetine dayanak yapılan hukuk normları adalete uygun olarak düzenlenmiş olmalıdır.<sup>275</sup> Ayrıca veri sorumluları; veri sahiplerini ve kamuyu, verileri hukuka uygun ve şeffaf bir şekilde işleyecekleri konusunda haberdar etmelidir. Bunun yanında, veri sorumluları veri işleme faaliyetlerinin Tüzüğe uygun olarak gerçekleştirildiğini gösterebilecek durumda olmalıdır. Ek olarak, veri sorumluları, özellikle veri sahibinin rızasının işleme faaliyeti için hukuki dayanak oluşturduğu durumlarda, mümkün olduğunca veri sahibinin taleplerine uygun hareket etmelidir.<sup>276</sup> Tüm bunlar düşünüldüğünde, adil olma ilkesi, şeffaflık yükümlülüğünün ötesinde olup kişisel verilerin etiğe uygun bir şekilde işlenmesi ile ilgilidir.<sup>277</sup>

Bu ilkeye örnek olarak AİHM'in *K.H. ve Diğerleri v. Slovakya* kararı<sup>278</sup> gösterilebilir. Bu davada başvuru, Roman etnik kökenli, hamilelikleri ve doğumları sırasında Slovakya'da bulunan iki hastanede tedavi görmüş kadınlardır. Doğumlarından sonra bu kadınlardan hiçbiri, çok kez denemelerine rağmen, hamile kalamamışlardır. Bunun üzerine yerel mahkemeler, hastanelere, hastaneye danışmaları ve tıbbi kayıtlarından el yazıları ile bilgi almaları için başvuru ve temsilcilerine izin vermelerine karar vermiş, fakat suistimalin önlenmesi gerekçesiyle bu belgelerin fotokopilerinin alınması talebini reddetmiştir. Oysa, AİHS'in 8. maddesi uyarınca, devletlerin, veri sahiplerinin dosyalarının bir kopyasını veri sahiplerine erişilir kılmak yönünde bir yükümlülükleri vardır. Bu davada ise yerel mahkeme, başvuru sahiplerinin kendi sağlıklarına ilişkin bilgilere etkili bir erişim elde etme taleplerini reddetmiş ve reddederken geçerli bir sebep ileri sürememiştir. Mahkeme ilgili bilgilerin suistimalden korunması için bu talebi reddettiğini belirtse de, kişisel

---

<sup>274</sup> GDPR, m. 6(1); Develioğlu, s. 58.

<sup>275</sup> Dülger, s. 116.

<sup>276</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 118.

<sup>277</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 119.

<sup>278</sup> AİHM, *K.H. ve Diğerleri v. Slovakya*, No. 32881/04, 28 Nisan 2009.

verilerine ilişkin dosyalarına zaten erişim elde eden bireylerin ayrıca bu dosyaların bir kopyasını alarak kendilerine ilişkin bilgileri nasıl suistimal edebileceğini düşündüğünü açıklayamamıştır. AİHM bu davada AİHS'in 8. maddesinin ihlal edildiğine karar vermiştir.<sup>279</sup>

### 3. Şeffaflık

95/46/EC sayılı Direktifteki ilkelere ek olarak düzenlenmiş şeffaflık ilkesi; veri sorumlularına, veri sahiplerini, verilerinin nasıl kullanıldığı ile ilgili bilgilendirme yükümlülüğü yüklemektedir.<sup>280</sup> Bu kapsamdaki her türlü bildirim “öz, şeffaf, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanarak” veri sahibine sağlanmalıdır. Veri sorumlusu söz konusu bilgileri yazılı olarak veya uygun olduğu hallerde, elektronik yollar da dahil olmak üzere diğer yollarla sağlayacaktır. Veri sahibi tarafından talep edilmesi durumunda, veri sahibinin kimliğinin diğer yollarla doğrulanması koşuluyla, bilgiler sözlü olarak sağlanabilir.<sup>281</sup>

Şeffaflık ilkesi; henüz işleme faaliyetleri başlamadan önce kişiye yapılan bilgilendirme için uygulama alanı bulduğu gibi, işleme sırasında veri sahiplerinin erişimine hazır bulunan bilgiler ve veri sahibine kendi verilerine erişim talep etmeleri üzerine verilen bilgiler de bu kapsamdadır.<sup>282</sup>

Bu ilke uyarınca, kişisel verilerinin işlenmesinin riskleri, kuralları, koruyucuları ve işlemeye ilişkin veri sahiplerinin hakları, ilgili kişiler için açık ve net olmalıdır.<sup>283</sup> Aynı zamanda kişisel verilerin işlenmesinin sınırlı ve belirli amacı da, verilerin toplanması sırasında, veri sahipleri tarafından biliniyor olmalıdır.<sup>284</sup>

Şeffaflık ilkesinin nasıl yorumlandığına örnek olarak AİHM'in *Haralambie v. Romanya*<sup>285</sup> kararı incelenebilir. Bu davada, başvuru, gizli servis teşkilatı bünyesinde tutulan kendisine ilişkin bilgilere erişim talep etmiştir. Başvurucuya bu bilgilere erişim ancak talebinden beş sene sonra sağlanmıştır. AİHM, bireylerin, kamu makamları tarafından tutulan şahsi dosyalarına erişebilmekte çok ciddi çıkarları olduğunu belirtmiştir. AİHM, ayrıca, yetkililerin, bu bağlamda söz konusu bilgilere ulaşımın sağlanması için efektif bir prosedür öngörülmesi gerektiğini ifade etmiştir. Bu davada AİHM, ne dosyaların sayısının çokluğunun ne de arşivleme sistemlerindeki yetersizliğin, başvuru dosyalarına erişim talebinin yerine getirilmesinde beş senelik bir gecikmeyi meşru kıldığını belirtmiştir. Yetkililerin, başvuru dosyalarına erişim sağlayabilmesi için etkili

---

<sup>279</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 118, 199.

<sup>280</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 120.

<sup>281</sup> GDPR, m. 12(1).

<sup>282</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 120.

<sup>283</sup> GDPR, Gerekeçe 39.

<sup>284</sup> GDPR, Gerekeçe 39.

<sup>285</sup> AİHM, *Haralambie v. Romanya*, No. 21737/03, 27 Ekim 2009.

ve erişilebilir bir yol sağlamaması nedeniyle, AIHM, AIHS'in 8. maddesinin ihlal edildiğine karar vermiştir.<sup>286</sup>

### **B. Belirli, Açık ve Meşru Amaçlara Yönelik İşleme (Amacın Sınırlandırılması İlkesi)**

Amacın sınırlandırılması ilkesi uyarınca, *kişisel veriler belirtilen, açık ve meşru amaçlara yönelik olarak toplanır ve yalnızca bu amaçlara uygun bir şekilde işlenebilir.*<sup>287</sup> Şeffaflık, öngörülebilirlik ve kişilerin verileri üzerindeki kontrolü nosyonları ile yakından ilgili olan bu ilke, veri sahiplerinin haklarını kullanabilmeleri açısından oldukça önemlidir.<sup>288</sup>

Yani, kişisel verilerin işlenmesini faaliyetlerinin meşruiyeti, işlemenin belirli, açık ve meşru bir amaç doğrultusunda gerçekleştirilmesine bağlıdır.<sup>289</sup> İlk amaç ile bağdaşan başka bir amaçla veri işleme faaliyetinin gerçekleştirilebilmesi için, bu işleme için veri sahibinin tekrar rızası alınmalı veya işleme faaliyeti başka bir hukuki dayanağa sahip olmalıdır.<sup>290</sup> Örneğin; bir havayolu şirketi, bir uçuşun düzgün bir şekilde idaresinin sağlanabilmesi için, rezervasyon yaptıkları sırada yolcularında bazı verileri toplar. Bu çerçevede, söz konusu havayolu, yolcuların koltuk numaralarına, özel besin gereksinimlerine, özel fiziksel ihtiyaçlarına ilişkin bilgileri alır. Fakat, bu havayolu şirketi aldığı bu bilgileri varış yerindeki göç makamlarına sağlayacak olursa, veri sahiplerinden uçuşun düzgün bir şekilde işletilmesi amacı ile toplanan ilgili verilerin toplanma sırasındaki amaçtan farklı bir amaç için kullanılması söz konusu olacaktır.<sup>291</sup> Bu nedenle, bu bilgilerin bir göç makamına aktarımının gerçekleştirilmesi için farklı ve yeni bir yasal dayanak bulunması gerekir.<sup>292</sup>

Burada vurgulanması gereken nokta, belirlenen amaçtan farklı bir amaçla işlemenin söz konusu olması için farklı bir amacın yeterli olup, mutlaka önceki ile bağdaşmayan bir amaç olmasının gerekmemesidir.<sup>293</sup> Bu çerçevede, ilave olarak gerçekleştirilmesi planlanan işlemenin orijinal amaç ile uyumlu olup olmadığı değerlendirilirken kişisel verinin toplanması amacı ve ilave işleme amaçları arasındaki ilişki, kişisel verilerin toplandığı bağlam ve veri sahiplerinin ilerideki kullanımlarına ilişkin makul beklentileri, kişisel verilerin niteliği, planlanan ilave işlemenin veri sahipleri açısından sonuçları, orijinal ve ilave işleme faaliyetleri için uygun korumaların varlığı

---

<sup>286</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 120.

<sup>287</sup> GDPR, m. 5(1)(b).

<sup>288</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 122.

<sup>289</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 122.

<sup>290</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 123.

<sup>291</sup> Guide to General Data Protection Regulation.

<sup>292</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 123.

<sup>293</sup> **Dülger**, s. 121.

gibi faktörler dikkate alınmalıdır.<sup>294</sup> Ayrıca belirtilmelidir ki, kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla işleme faaliyetlerinin baştaki amaçlara *a priori* uygunluğu Tüzükte açıkça düzenlenmiştir<sup>295</sup>. Her koşulda, ilave olarak veri işlemesi gerçekleştirilirken anonimleştirme, şifreleme veya takma ad kullanımı da dahil olmak üzere uygun güvencelerin bulunması gerekir.<sup>296</sup> Örneğin; A Şirketinin, müşterileri ile ilgili olarak müşteri ilişkileri yönetimine dair verileri topladığını ve sakladığını varsayalım. Bu verilerin, A Şirketi tarafından, müşterilerinin satın almaya yönelik davranışlarını istatistiki olarak analiz etmek için kullanılması Tüzüğün belirlediği ilkelere bir aykırılık teşkil etmeyecektir. Yine de, A Şirketinin istatistiki amaçlarla ilave işleme yapmasının hukuka uygun olması için, A Şirketi veri sahibinin hak ve özgürlüklerini korumak için gerekli güvenceleri sağlamalıdır.<sup>297</sup> Son olarak, ilave veri işlemenin, veri sahibinin rızasına dayanması veya Birlik veya Üye Devlet hukukunca kamu yararı gibi önemli hedeflerin güvence altına alınması için gerekli ve ölçülü bir tedbir niteliğinde olması durumunda, veri sorumlusu, amaçların uyumluluğuna bakılmaksızın söz konusu ilave işlemeyi gerçekleştirebilmelidir.<sup>298</sup>

### **C. Verilerin İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması (Veri Minimizasyonu)**

Veri minimizasyonu ilkesi uyarınca, *kişisel veriler; işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlı olmalıdır.*<sup>299</sup> Bu kapsamda Tüzüğün lafzı 95/46/EC sayılı Direktif ve 108 No'lu Sözleşme'den farklılık göstermektedir: Bu belgelerde verilerin toplanmasının "*gerekli olanla sınırlı olması*" yerine "*aşırı olmaması*" gerektiği düzenlenmiştir.

Veri minimizasyonu ilkesine göre veri sorumlusunun yükümlülüğü veri işlemini minimumda tutmaktan ziyade, veri toplanmasını işleme amaçlarını göz önüne alarak yeterli olan ölçüde sınırlandırmaktır.<sup>300</sup> Yani, veri sorumlusunun işleme için seçtiği veri kategorileri, işlemenin açıkça belirtilmiş amacına ulaşmak için gerekli olmalıdır ve veri sorumlusu, veri toplanmasını veri işleme ile güdülen spesifik amaç ile doğrudan ilgisi olan bilgiler ile sınırlandırmalıdır.<sup>301</sup>

---

<sup>294</sup> GDPR, m. 6(4); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 124.

<sup>295</sup> GDPR, m. 5(1)(b).

<sup>296</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 124.

<sup>297</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 125.

<sup>298</sup> GDPR, Gereğe 50.

<sup>299</sup> GDPR, m. 5(1)(c).

<sup>300</sup> **Voigt/von dem Bussche**, s. 90.

<sup>301</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 125.

Örneğin; *Digital Rights Ireland* davasında<sup>302</sup> ABAD, organize suç ve terör gibi ciddi bir suçla mücadele amacıyla ilgili verilerin yetkili makamlara olası aktarımları için kamuya açık elektronik haberleşme servisleri ve ağları tarafından oluşturulan veya işlenen kişisel verilerin saklanmasıyla ilişkin yerel hukuklarda yer alan hükümlerin yeknesaklaştırılmasını amaçlayan Veri Saklama Direktifinin geçerliliğini incelemiştir. Genel olarak ciddi bir suçla mücadele meşru bir menfaat olarak düşünülse de bu direktifin “*bir fark, sınır veya istisna gözetmeksizin tüm bireyleri ve her tür elektronik haberleşme ile trafik verisini*” kapsamı, sorunlu bulunmuştur.<sup>303</sup>

GDPR’nın 5/1-c maddesinde düzenlenen verilerin asgari ölçüde işlenmesi ilkesi nedeniyle kişisel veriler ancak gerekli olan ile sınırlı şekilde toplanabilecektir. Dolayısıyla bu ilke, kullanıcılarına ait doğum tarihi, yaşadığı yer, çalıştığı yer, meslek, arkadaşları, ilgi alanları, ailesinden uzaklığı gibi pek çok kişisel veriyi toplayan Facebook gibi sosyal medya şirketleri açısından önemli bir aşamayı içermektedir. Veri sorumlusu niteliği taşıyan sosyal medya şirketlerinin veri sahibinin haklarını kullanabilmesini teminen şeffaf bir şekilde kullanıcıyı, topladığı verilere ilişkin bilgilendirmesi, işlenen verilere ilişkin veri tabanını sunması zorunludur (GDPR, m. 12). Facebook’un kullanıcılara ilişkin tuttuğu kabul edilen bu verilerin, olayların gerçekleşme tarihlerinin, saklanan sayısız fotoğrafın ve kullanıcıların kontak listelerine ilişkin verilerin GDPR’nın 4/1 maddesi uyarınca kişisel veri olduğunda şüphe bulunmamaktadır. Dolayısıyla Facebook kullanıcıları, bu verilerin Facebook tarafından işlenmesinin ve saklanmasının GDPR’nın 5/1-c ve 5/1-e maddelerinde düzenlenen ilkeler çerçevesinde unutulma hakkının düzenlendiği 17. maddeye göre “artık gerekli olmadığını” belirterek silinmelerini talep edebileceklerdir. Bu tür taleplerde, Facebook’un bir veri sorumlusu olarak GDPR’nın 17. maddesinin gecikmeksizin uygulanmasından sorumlu olduğu, aksi takdirde 83. maddede düzenlenen müeyyidelerle karşılaşabileceği söylenebilecektir.

#### **D. Doğru ve Gerektiğinde Güncel Tutulma**

Doğruluk ve güncellik ilkesi uyarınca, *kişisel veriler doğru ve gerektiğinde güncel tutulur*; işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır.<sup>304</sup>

Bu ilke kapsamında, kişisel bir bilgiye sahip olan bir veri sorumlusu, öncelikle, verinin gerçeği yansıttığına ve güncel olduğuna dair makul bir kesinliğe ulaşmak için çaba göstermeden

---

<sup>302</sup> Kararın tam metni için bakınız: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=612496>.

<sup>303</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 126.

<sup>304</sup> GDPR, m. 5(1)(d).



bu bilgiyi kullanmamalıdır.<sup>305</sup> Ayrıca, verilerin ilk defa elde edilmesi aşamasında, veri doğrudan ilgili kişiden ve onun bilgisi dahilinde alınıyorsa, mevzubahis veri bu kişi tarafından doğru bir şekilde verilmelidir.<sup>306</sup>

Tüzüğün lafzından da anlaşıldığı üzere, kişisel verilerin güncel tutulması “*gerektiğinde*” sağlanmalıyken, kişisel verilerin doğruluğu için böyle bir parantez açılmamıştır. Bu doğrultuda, bazı verilerin mutlaka düzenli olarak kontrol edilerek güncellenmesi gerekirken, bazı kaydedilmiş verilerin güncellenmesi ise hukuken yasaklanmıştır. Örneğin; bir medikal kayıttaki bulgular daha sonra yanlış oldukları anlaşılabilir bile güncellenerek değiştirilmemelidir. Böyle durumlarda, yalnızca daha sonraki bir aşamada ekleme yapıldığının açık bir şekilde belirtilmesi suretiyle yeni bulgular kaydedilebilecektir. Diğer bir örnek ise sürekli güncelleme için gerekli olduğu durumlarla ilgilidir; bir kişi bir bankaya kredi çekmek için başvurduğunda, banka, bu iş için oluşturulmuş veri tabanlarından kişinin kredi verilebilir durumda olup olmadığını inceler. Böyle bir veri tabanının güncel olmayan veriler içermesi durumunda ilgili kişinin olumsuz sonuçlarla karşılaşması mümkündür. Bu nedenle böyle veri tabanlarını kontrol edenler verileri güncel tutmalıdır.<sup>307</sup>

Verilerin doğru ve gerektiğinde güncel tutulması ilkesi, bireylerin kişisel verilerine erişim hakkı, verilerinin düzeltilmesini veya silinmesini talep etme haklarıyla oldukça yakından ilgilidir.<sup>308</sup>

Nitekim, *Rijkeboer*<sup>309</sup> davasında ABAD, gizlilik hakkının, veri sahiplerinin kişisel verilerinin doğru ve hukuka uygun bir şekilde işlendiğinden emin olmasını da içerdiğini ifade etmiştir.<sup>310</sup>

### **E. Verilerin Amaç İçin Gereken Süre Kadar Muhafaza Edilmesi (Sınırlı Süre Saklama İlkesi)**

Sınırlı süre saklama prensibi, *veri sahiplerinin yalnızca kişisel verilerin işleme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan bir şekilde tutulması gerektiğini* ifade etmektedir.<sup>311</sup> Daha basit ve açık bir anlatımla kişisel veriler ancak ilgili amacın gerektirdiği süre boyunca işlenmeli, bu sürenin sonunda verinin işlenmesine son verilmeli, veri ya yok edilmeli ya da ilgili kişiyi teşhis edemeyecek şekilde anonimleştirilmelidir. Dolayısıyla bu ilke uyarınca, işleme

---

<sup>305</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 127.

<sup>306</sup> **Dülger**, s. 133.

<sup>307</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 128.

<sup>308</sup> **Voigt/von dem Bussche**, s. 91, 92.

<sup>309</sup> ABAD, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 Mayıs 2009.

<sup>310</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 128.

<sup>311</sup> GDPR, m. 5(1)(e).

amacı gerçekleştirildikten sonra ilgili kişisel veriler silinmeli, yok edilmeli veya anonimleştirilmelidir. Bu kapsamda belirtilmesi gereken bir nokta, sınırlı süre saklama ilkesinin, yalnızca kişilerin kimliklerinin belirlenmesine olanak verecek şekilde tutulan veriler için uygulama alanı bulacağıdır.<sup>312</sup>

Bu ilke uyarınca, kişisel verilerin gerektiğinden uzun süre tutulmaması için, veri sorumlusu tarafından verilerin silinmesi veya periyodik kontrolü için bazı zaman aralıkları belirlenmesi gerekir.<sup>313</sup> Verilerin işleme amacı için gereken süre kadar muhafaza edilmesi gerekliliği, unutulma hakkı ile doğrudan ilgilidir.<sup>314</sup>

Değnilmesi gereken bir diğer nokta ise, kişisel verilerin kamu yararı için, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla arşivlenmesi durumunda, ilgili verilerin yalnızca yukarıda belirtilen amaçlarla kullanılması ve Tüzük uyarınca gereken uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanması şartı ile, bu arşivlenmiş verilerin daha uzun süre saklanabileceğidir.<sup>315</sup>

Örneğin; *S. and Marper*<sup>316</sup> davasında, AİHM, haklarındaki ceza davaları beraat ve davanın düşmesi ile sona ermiş başvuruçuların parmak izlerinin, hücre örneklerinin ve DNA örneklerinin sınırsız bir süre boyunca saklanması ölçüsüz olduğuna ve demokratik bir toplumda gerekli olarak nitelendirilemeyeceğine karar vermiştir.<sup>317</sup> Diğer bir örnek ise, *Digital Rights Ireland*<sup>318</sup> davasıdır. Bu davada ABAD, yukarıda da açıklandığı üzere, Veri Saklama Direktifinin geçerliliğini incelemiştir. Bu direktif verilerin herhangi bir ayırım yapılmadan en az altı ay en çok yirmi dört ay boyunca saklanmasını öngörmüştür, ABAD bu çerçevede Veri Saklama Direktifinin altı ay ile yirmi dört ay arasında değişebilecek saklamanın süresinin belirlenmesi ile ilgili objektif kriterler öngörmemiş olmasını bir sorun olarak dile getirmiştir.<sup>319</sup>

Amaç için gereken sürenin sonunda kural olarak verilerin kalıcı olarak imha edilmesi gerekir. Kalıcı olarak imha etmenin hemen mümkün olmaması durumunda ilgili veri eldeki olanaklarla silinmeli, yani veri sorumlusunun olağan erişim ve kullanım alanlarından

---

<sup>312</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 129.

<sup>313</sup> GDPR, Gerekeçe 39.

<sup>314</sup> **Voigt/von dem Bussche**, s. 92.

<sup>315</sup> GDPR, m. 5(1)(e); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 129, 130.

<sup>316</sup> AİHM, *S. and Marper v. Birleşik Kırallık* [GC], Nos. 30562/04 and 30566/04, 4 Aralık 2008.

<sup>317</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 129.

<sup>318</sup> ABAD, *Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ve Diğerleri and Kärntner Landesregierung ve Diğerleri* [GC], 8 Nisan 2014.

<sup>319</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 130.

çkarılmalıdır. Bunun yanı sıra verinin anonimleştirme gibi işlemlerden geçirilerek ilgili kişileri teşhis edemeyecek bir niteliğe getirilip saklanması da mümkündür<sup>320</sup>.

## F. Veri Güvenliği İlkesi

Veri güvenliği ilkesine göre, veri sorumlusu, son teknoloji, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında, *veri koruma ilkelerinin etkili bir şekilde uygulanması ve bu Tüzüğün gerekliliklerinin yerine getirilmesine yönelik olarak, yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere, gerekli güvencelerin entegre edilmesi amacı ile tasarlanan, uygun teknik ve düzenlemeye ilişkin tedbirler uygulamalı ve veri sahiplerinin haklarını korumalıdır.*<sup>321</sup> Tüzük, takma ad kullanılmasını, açıkça veri güvenliği için uygun tedbirlerden biri olarak kabul etmiştir.

Örneğin; “*Melodi Ertekin, 9 Ocak 1992 tarihinde doğmuştur ve iki erkek kardeşi ile birlikte üç çocuklu bir ailenin tek kız çocuğudur*” cümlesi şu şekillerde psödonimleştirilebilir:

(i) “M.E. 1992 iki erkek kardeşi ile birlikte üç çocuklu bir ailenin tek kız çocuğudur”; veya  
(ii) 1701 iki erkek kardeşi ile birlikte üç çocuklu bir ailenin tek kız çocuğudur”. (i) şeklinde gerçekleştirilen psödonimleştirme, (ii) biçiminde gerçekleştirilene göre daha az güvenlidir.<sup>322</sup> Buradan anlaşılması gereken, psödonimleştirme yönteminin veri korumanın verimliliğini etkileyebileceğidir.<sup>323</sup>

## G. Hesap Verebilme Zorunluluğu

Veri sorumlusu, Tüzükte düzenlenmiş ilkelere uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmek yükümlülüğü altındadır.<sup>324</sup> Bu maksatla, veri sorumlusu, uygun teknik ve düzenlemeye ilişkin tedbirleri almalıdır. Tüzükte lafzen veri sorumlusunun hesap verebilirliğinden bahsedilmiş olsa da, belirli yükümlülükler altında olan veri işleyenin de bu ilkelere uygun davrandığına ilişkin hesap verebilir durumda olması gerekir.<sup>325</sup>

---

<sup>320</sup> GDPR uyarınca anonimleştirme ve benzer tekniklerin şartları, avantajları ve karşılaştırması için bkz. **Mike Hintze/Khaled El Emam**, “Comparing the benefits of pseudonymisation and anonymisation under the GDPR”, *Journal of Data Protection & Privacy*, Volume 2, Number 2, Autumn 2018, s. 145-158.

<sup>321</sup> GDPR, m. 5(1)(f).

<sup>322</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 131, 132.

<sup>323</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 132.

<sup>324</sup> GDPR, m. 5(2), 25.

<sup>325</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 134, 135.

Bu kapsamda izlenecek prosedürler ve kurulacaklar sistemler, veri işleminin yarattığı risk ve verinin niteliğine bağlı olarak değişiklik gösterecektir<sup>326</sup>. Bu ilkeye uygun hareket etmek için veri sorumluları ve veri işleyenler, örneğin; işleme faaliyetlerine ilişkin kayıt tutabilir ve gerektiğinde bu kayıtları denetim makamına sunabilir<sup>327</sup>, belirli durumlarda kişisel verilerin korunması ile ilgili konularda görev yapacak bir veri koruma görevlisi atanabilir<sup>328</sup>, bir işleme türünün gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, işleme faaliyetinden önce, veri koruma etki değerlendirmesi yapabilir<sup>329</sup>, özel ve olağan durumlarda veri korunmasını temin edebilir<sup>330</sup>, veri sahiplerinin haklarını kullanabilmeleri için yöntem ve prosedürler yürürlüğe koyabilir<sup>331</sup>, onaylanmış davranış kuralları veya sertifikasyon mekanizmalarına bağlı kalabilir<sup>332</sup>.

Madde 29 Çalışma Grubu hesap verme zorunluluğunu; veri sorumlusunun, işleme faaliyetleri bağlamında ve olağan şartlarda veri koruma kurallarına bağlılığı sağlayacak tedbirler alması ve veri koruma kurallarına uygun hareket edildiğini veri sahipleri ve denetim makamlarına gösterecek gerekli belgeleri hazır bulundurması yükümlülüğü olarak özetlemiştir.<sup>333</sup>

### § 3. Veri İşleminin Kuralları

#### I. Veri Sorumlusunun Genel Yükümlülükleri

##### A. Temsilci Atama Yükümlülüğü

Yukarıda açıklandığı üzere, Tüzüğün uygulama alanı AB üyesi ülkelerden daha geniş tutulmuştur. Tüzükte AB'deki kişilerin verilerinin işlenmesi halinde, veri sorumlusu veya veri işleyen AB'de bulunmasa dahi Tüzüğün uygulanacağını öngörülmesine paralel olarak, veri sorumlusu veya işleyenin yazılı olarak Birlik içerisinde bir temsilci ataması gerektiği düzenlenmiştir.<sup>334</sup> Atanacak temsilci, kişisel verileri kendilerine mal veya hizmetlerin sağlanması ile ilgili olarak işlenen veya davranışı izlenen veri sahiplerinin bulunduğu üye devletlerin birinde bulunmalıdır.<sup>335</sup>

---

<sup>326</sup> Guide to General Data Protection Regulation.

<sup>327</sup> GDPR, m. 30.

<sup>328</sup> GDPR, m. 37-39.

<sup>329</sup> GDPR, m. 35.

<sup>330</sup> GDPR, m. 25.

<sup>331</sup> GDPR, m. 12, 24.

<sup>332</sup> GDPR, m. 40, 42.

<sup>333</sup> Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173, Brussels, 13 July 2010.

<sup>334</sup> GDPR m. 27(1); Develioğlu, s. 98, 99.

<sup>335</sup> GDPR m. 27(3).

AB dışındaki veri sorumlusunun birden fazla AB ülkesinde bulunan veri sahiplerinin verilerini işliyor olması durumunda temsilcinin bu ülkelerden hangisinde bulunması ve dolayısıyla hangi ülkenin veri koruma otoritesi nezdinde tescil edilmesi gerektiği konusunda seçim hakkı veri sorumlusuna bırakılmıştır.<sup>336</sup> Veri sorumlusu ilgili ülkelerden kendisi için en uygun olanında temsilci atayabilir. Ancak temsilci hangi ülkede olursa olsun, tüm AB vatandaşlarına yönelik aydınlatma metinlerinde temsilcinin kimlik ve iletişim bilgileri yer almalıdır.<sup>337</sup>

İşlemenin nadir olarak gerçekleştiği ve özel nitelikli kişisel verilerin büyük ölçekli olarak işlenmesinin söz konusu olmadığı hallerde, işleme faaliyetinin mahiyeti, bağlamı, kapsamı ve amaçları dikkate alındığında söz konusu işlemenin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebep olmasının muhtemel olmadığı sonucuna ulaşıyorsa temsilci atanmasına gerek yoktur.<sup>338</sup> Ayrıca ilgili işleme bir kamu kuruluşu veya organı tarafından gerçekleştiriliyorsa, bu kuruluş veya organın Birlik içerisinde bir temsilci ataması aranmaz.<sup>339</sup>

95/46/EC sayılı Direktif'in 4/2. maddesine göre, veri sorumlusunun AB topraklarında yerleşik olmaması ve işleme amaçları için AB topraklarındaki otomatik cihazlar kullanılmış ise, veri sorumlusu kendisine karşı açılacak davalara zarar vermeksizin, o üye ülke topraklarında yerleşik bir temsilci atamakla yükümlü kılınmıştır.

GDPR'nin 4/17. maddesine göre temsilci AB içerisinde kurulu bulunan, 27. madde uyarınca veri sorumlusu veya işleyen tarafından yazılı olarak belirlenen, GDPR kapsamındaki yükümlülükleri ile ilgili olarak veri sorumlusu veya işleyeni temsil eden gerçek veya tüzel kişi şeklinde tanımlanmıştır. Dolayısıyla temsilci ataması yazılı olarak yapılmalıdır. Ayrıca temsilci olarak gerçek kişiler gibi tüzel kişiler de atanabilecektir (GDPR, rec. 80).

Kişisel verileri kendilerine mal veya hizmetlerin sağlanması ile ilgili olarak işlenen veya davranışı izlenen (GDPR, m. 3/2) veri sahiplerinin bulunduğu üye devletlerde faaliyet gösteren veri sorumlusu/işleyenler temsilci atamakla yükümlüdür (GDPR, rec. 80, m. 27/3).

Temsilci, işleme faaliyeti ile ilgili tüm hususlarda, GDPR'a uygunluk sağlanması amacıyla özellikle denetim makamları ve veri ilgilileri tarafından veri sorumlusu veya işleyene ek olarak veya bunlar yerine muhatap kabul edilmek üzere yetkilendirilir (GDPR, m. 27/4).

---

<sup>336</sup> Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 21.

<sup>337</sup> Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation Adopted on 16 November 2018, s. 12.

<sup>338</sup> GDPR m. 27(2)(a).

<sup>339</sup> GDPR m. 27(2)(b).

## B. Ortak Veri Sorumlularının İş Bölümü Anlaşması Yapma Yükümlülüğü

Yukarıda açıklandığı üzere, iki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde, bu veri sorumluları ortak veri sorumlularıdır. Birlik veya Üye Devlet hukuku tarafından belirlenmiş olmadıkça, ortak veri sorumlularının Tüzükte yer alan yükümlülüklerinin gerçekleştirilecek bir anlaşma ile şeffaf bir şekilde belirlenmesi gerekmektedir.<sup>340</sup>

Ortak veri sorumluları her iki veri sorumlusu nezdindeki veri işleme faaliyetlerinin hukuka uygunluğundan birlikte mesul oldukları gibi, herhangi bir ihlal durumunda da birlikte müteselsil sorumlu olmaktadır.<sup>341</sup> Diğer ortak veri sorumlusu nezdindeki ihlallerden sorumlu olmak istemeyen veri sorumlusu, hangi yükümlülüklerin hangi veri sorumlusu bakımından yerine getirileceğini açıkça düzenlemelidir.<sup>342</sup> Bu kapsamda tarafların sorumluluk ve sorumsuzluk alanları somut ve ayrıntılı olarak belirlenmelidir.<sup>343</sup> Bu noktada tarafların sorumlulukların veri sahiplerinin mağduriyetine yol açacak şekilde sorumsuzluk alanları oluşturacak şekilde düzenlenemeyeceği aşikârdır. Böyle bir düzenleme hükümsüz olacak ve her ir veri sorumlusu ayrı ayrı ve müteselsil olarak sorumlu olmaya devam edecektir. Veri sahiplerinin haklarının kullandırılmasına yönelik yükümlülükler ise ortak veri sorumlularından birine devredilemez<sup>344</sup>. Her bir veri sorumlusunun veri sahiplerinin haklarını kullanabilmeleri için gerekli başvuru ve cevap mekanizmalarını GDPR'a uygun şekilde tesis etmesi gerekir.

Sonuç olarak her bir veri sorumlusunun sorumluluk ve sorumsuzluk alanları açık ve net bir anlaşmayla belirlenmelidir. Aksi halde hangi veri sorumlusu nezdinde gerçekleştiğine bakılmaksızın her bir yükümlülük için her bir veri sorumlusu müteselsil sorumlu olacaktır<sup>345</sup>.

## C. Veri İşleyenlerin Seçimi İle İlgili Yükümlülükler

Tüzüğün 28. maddesi uyarınca, veri sorumlusunun, işleme faaliyeti esnasında Tüzüğün gerekliliklerinin yerine getirilmesini ve veri sahibinin haklarının korunmasını sağlayacak biçimde

---

<sup>340</sup> GDPR m. 26(1); **Develioğlu**, s. 102.

<sup>341</sup> Guide to General Data Protection Regulation- Information Commissioner's Office, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/> (Son erişim: 19.07.2019)

<sup>342</sup> Guide to General Data Protection Regulation.

<sup>343</sup> **Gernot Fritz/Nadja Paulus**, "CJEU rules on joint controllership – what does this mean for companies?", Freshfields Bruckhaus Deringer LLP, <https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies>, (Son erişim: 19.07.2019).

<sup>344</sup> **Fritz/Paulus**.

<sup>345</sup> Guide to General Data Protection Regulation.

uygun teknik ve düzenlemeye ilişkin tedbirler uygulama hususunda yeterli güvenceler sağlayan veri işleyenleri kullanması gerekmektedir.<sup>346</sup>

#### **D. Kayıtlar ile ilgili Yükümlülükler (Documentation Requirements)**

##### **i. Veri Koruma Politikaları Oluşturulması**

Veri sorumlusu, veri işleme faaliyetinin GDPR hükümlerine uygun olarak gerçekleştirilmesini sağlamak ve bu şekilde gerçekleştirildiğini gösterebilmek için uygun teknik ve organizasyonel tedbirleri almalı ve uygulamalıdır (GDPR, m. 24/1). Bu amaçla uygun veri koruma politikalarını uygulayacaktır (GDPR, m. 24/2). Şirketlerin uygun veri koruma politika kuralları amaçlar, anahtar terimlerin tanımları, temel ilkeler ve kişisel veri işleminin amaçları, sorumluluklar ve bu konulardaki ana denetleyici otoriteyi içermelidir.<sup>347</sup>

##### **ii. Mahremiyet Bildirimi (Privacy Notice)**

Veri sorumlusu kişisel verilerin işlenmesine ilişkin her türlü bildirim kısa, öz, şeffaf, anlaşılır ve kolay erişilebilir bir biçimde veri sahibine yazılı/elektronik/sözlü olarak sunabilmelidir (GDPR, m. 12/1). Aynı şekilde veri sahibinin kişisel verilerinin toplanması durumunda, veri sorumlusu kendi kimlik ve irtibat bilgileri, veri koruma görevlisinin irtibat bilgileri, veri işleminin yasal dayanağı, buna ilişkin varsa meşru menfaatler, kişisel verilerin alıcıları, kişisel verilerin üçüncü bir ülke/uluslararası kuruluşa aktarılıp aktarılmayacağı ile buna ilişkin güvenceleri veri sahibine sunmalıdır (GDPR, m. 13/1, 14/1). Yine verilerin kişisel verilerin saklanacağı süre, bu sürenin net olmaması halinde buna ilişkin kullanılan kriterler, verilerin taşınabilirliğine, düzeltilmesine, kısıtlanmasına ve silinmesine ilişkin açıklamalar, veri işlenmesine ilişkin rızanın geri çekilme hakkı, bir denetim makamına şikâyet hakkı gibi hususlar da veri sahibine sunulmalıdır (GDPR, m. 13/2). Bu bilgiler genel olarak veri sorumlusu şirketlerin verilerini işlediği müşterilere ilişkin açıklayıcı ve anlaşılır nitelikte olmalıdır. Şirketler bu açıklamaları web sitelerinde de sunabilecektir.

##### **iii. Veri Saklama ve İşleme Kayıtları (Data Retention/Records of processing activities)**

Veri sorumlusu işlenen kişisel verilere ilişkin yazılı (elektronik dahil) bir kayıt tutmakla yükümlü kılınmıştır (GDPR, m. 30/1). Bu kayıtlarda veri sorumlusu, veri koruma görevlisi, veri işleme amaçları, veri sahibi ve kişisel veri kategorileri, alıcılar, veri aktarımları, verilerin silinmesine ilişkin süre sınırları gibi açıklamalar yer alacaktır (GDPR, m. 30/1-2).

---

<sup>346</sup> GDPR m. 28(1).

<sup>347</sup> **Punit Bhatia**, Contents of Data Protection Policy according to GDPR, <https://advisera.com/eugdpracademy/knowledgebase/contents-of-the-data-protection-policy-according-to-gdpr/> (Son Erişim Tarihi: 18.03.2019).

#### iv. Veri Sahibi Rıza Formu

Veri işleminin rızaya dayalı olduğu hallerde, rıza talebi açık bir şekilde ayırt edilebilir, anlaşılır ve kolay erişilebilir bir biçimde açık ve sade bir dil kullanılmak suretiyle sunulmalıdır (GDPR, m. 7/2). Rıza, yazılı form dışında elektronik veya sözlü olarak da sunulabilecektir (GDPR, rec. 32). Rıza, bir internet sitesini ziyaret esnasında kutuyu işaretleme şeklinde olabilecek, buna karşılık sessizlik (silence), önceden işaretlenen kutucuklar (pre-ticked boxes) veya hareketsizlik (inactivity) rıza olarak yorumlanamayacaktır. İşlenen her bir veri için ayrı rıza gereklidir. Rızanın verildiği durumlarda, veri sorumlusu veri sahibinin rızası bulunduğunu ispatlayabilmelidir (GDPR, rec. 42).

Veri sahibinin çocuk olduğu durumlarda rızanın geçerli olabilmesi için çocuğun en az 16 yaşında olması gerekir (GDPR, m. 8/1). Veri sahibinin 16 yaşından küçük olduğu durumlarda, rızanın velayet hakkı sahibi tarafından verilmesi veya çocuk tarafından verilip velayet hakkı sahibi tarafından onaylanması şarttır (GDPR, m. 8/1).

Önceden işaretlenen kutucukların geçerli bir rıza olup olmamasına ilişkin ABAD önünde bir uyuşmazlık bulunmaktadır. Buna göre “dein-macbook.de” internet sitesi online ortamda promosyon amaçlı çekilişler yaparak alışveriş yapan kullanıcılara hediyeler dağıtmaktadır. Bunun için kullanıcıların isim, adres bilgileri gibi kişisel verileri kayıt edilmektedir. Kullanıcılar, bu bilgileri sponsorluk yapan kuruluşlara da önlerine çıkan kutucuğu işaretlemek suretiyle (pre-ticked boxes) vermeyi kabul etmektedirler. Çekilişe katılım Planet49 isimli şirketin, tüketicilerin davranışlarını takip etmesi ve hedefli reklamlarını kullanabilmesi için çerezlere izin verilmesine ilişkin kutucuk işaretleme ile mümkün olmaktadır. Olayın, GDPR’ın yürürlüğe girdiği dönem öncesi olması nedeniyle davanın Hukuk Sözcüsü (Advocate General), 95/46/EC sayılı Direktif’e göre de bir değerlendirme yapmıştır. Hukuk Sözcüsüne göre 95/46/EC sayılı Direktif’in 2/h maddesine göre rızanın “özgürce ve bilgilendirilme sonrası” verilmesinin gerekmesi, 7/a maddesine göre rızanın “açık, net ve kesin” biçimde yapılmasının gerekmesi nedeni ile bu tür önceden işaretlenmiş kutucuklar yolu ile kişisel verilerin işlenmesine rıza gösterilmesi geçersizdir. Madde 29 Çalışma Grubu’nun da rızaya ilişkin görüşü bu doğrultudadır. Ayrıca GDPR ile rıza hususu çok daha açık ve kesinlik gerektiren şekilde düzenlenmiştir. Uyuşmazlıkta, kullanıcı çekilişe katılmak için kutucuğu işaretlemek zorunda bırakılmıştır. Bu işaretleme ile de, kullanıcı çerez (cookies) kullanımına izin vermektedir. GDPR’ın 7/4. maddesiyle kullanıcıyı asıl hizmetten yararlanmak için bu tür aceleye getiren rıza alma şekilleri (bundling) yasaklanmıştır. Dolayısıyla Sözcü’ye göre kullanıcılar önceden işaretlenen bu kutucukların sonuçları hakkında yeteri kadar



bilgilendirilmemiştir ve bu tür alınmış bir rıza geçerli bir rıza olarak değerlendirilmemelidir.<sup>348</sup> ABAD'ın kararının da bu yönde olacağını düşünüyoruz. Çünkü yeterli bilgilendirme yapılmaksızın bilhassa hizmetten yararlanmayla eşzamanda yapılan işaretlenen kutucuklar hem 95/46/EC sayılı Direktif hem de GDPR'ın 7 ve 42. Gerekçesi uyarınca geçerli bir rıza olarak yorumlanamaz.

#### **v. Veri İşleme Antlaşması**

Veri sorumlusu kendi adına veri işleme faaliyetinin gerçekleştirilmesini istemesi durumunda, işleyene spesifik ve yazılı onay vermelidir. Bu onayın verildiği durumlarda veri sorumlusu, veri işleyenlerden GDPR gereksinimleri olan teknik ve organizasyonel tedbirleri uygulamak için gerekli olan uzman bilgisi, güvenilirlik ve kaynaklar gibi konularda yeterli güvenceleri sağlamasını bekleyecektir. Bu tür durumlarda veri sorumlusu ve işleyen, veri işleme konusu, süresi, amacı, işlenen kişisel verinin çeşidi, veri sahiplerinin kategorileri gibi konularda Sözleşme ve AB mevzuatı/AB üyesi ulusal mevzuatına uymakla yükümlü olacaklardır. Veri sorumlusu adına işlemenin tamamlanmasından sonra, veri işleyen, işlenen verinin AB mevzuatı veya üye ülke mevzuatı uyarınca saklanması gerekmeyeceği sürece, silmekle veya temin ettiği yere iade ile yükümlü olacaktır (GDPR, rec. 81).<sup>349</sup>

#### **vi. Veri İhlali Açıklaması ve Bildirimi**

Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusu kişisel veri ihlalini gereksiz bir gecikmeye mahal vermeden veri sahibine iletmekle yükümlüdür (GDPR, m. 34/1). Bir kişisel veri ihlali olması durumunda, veri sorumlusu ihlalden haberdar olduğu andan itibaren en geç 72 saat içinde, kişisel veri ihlalini denetim makamına bildirmekle yükümlüdür (GDPR, m. 33/1). Yapılan veri ihlali bildiriminde şu hususlara dikkat edilmelidir (GDPR, m. 33/3):

- İlgili veri sahibi ve veri kaydı kategorileri ve sayısına ilişkin açıklamaların yer aldığı veri ihlalinin niteliği açıklanmalıdır.

- Veri koruma görevlisi veya daha fazla bilginin elde edilebileceği diğer irtibat noktasına ilişkin isim ve gerekli bilgiler sağlanmalıdır.

- Kişisel veri ihlalinin olası sonuçları açıklanmalıdır.

---

<sup>348</sup> Opinion of Advocate General Szpunar, delivered on 21 March 2019 (1), Case C-673/17, Planet 49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände-Verbraucherzentrale Bundesverband e.V., <http://curia.europa.eu/juris/document/document.jsf?text=&docid=212023&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5537788> (Son Erişim Tarihi: 22.03.2019)

<sup>349</sup> Veri sorumlusunun, GDPR 28/2 maddesine göre işleyen ile yapabileceği Veri İşleme Antlaşması örneği için bkz. [http://www.fastviewer.com/demo/FV-ADV\\_Kunden\\_EN.pdf](http://www.fastviewer.com/demo/FV-ADV_Kunden_EN.pdf) (Son Erişim Tarihi: 19.03.2019)

- Veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik alınan/önerilen tedbirler açıklanmalıdır.

Bu bilgilerin aynı zamanda sağlanmasının mümkün olmadığı durumlarda, bilgiler gereksiz ek bir gecikmeye mahal vermeksizin, aşamalı olarak da sağlanabilecektir (GDPR, m. 33/4).

## **II. Veri İşlemede Hukuka Uygunluk Nedenleri**

### **A. Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri**

Yukarıda açıklandığı üzere, kişisel verilerin hukuka uygun, adil ve şeffaf bir şekilde işlenmesi Tüzükte yer alan ilkelerden birisidir. Bu ilke uyarınca kişisel verilerin işlenmesi hukuka uygun olmalıdır ve işleme faaliyeti, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve olduğu ölçüde hukuka uygundur:

(a) Veri sahibinin bir ya da daha fazla sayıda belirli bir amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi,

(b) Veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için, işleme faaliyetinin gerekli olması,

(c) Veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile işleme faaliyetinin gerekli olması,

(d) Veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile işleme faaliyetinin gerekli olması,

(e) Kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması,

(f) Özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması.

### **I. Rıza**

#### **a. Rıza Tanımları**

Tüzük uyarınca veri sahibinin rızası, “*veri sahibinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık göstergedir.*”<sup>350</sup> Diğer düzenlemelere bakılırsa rıza, 95/46/EC sayılı Direktif’te veri sahibinin “*kendisine dair kişisel verilerin işlenmesi için veri sahibinin*

---

<sup>350</sup> Geçerli bir rızadan bahsedebilmek için medeni hukuk anlamında aranan koşullar, kişisel verilerin korunması hukuku açısından da gereklidir; örneğin hak ehliyet vb.

*kabulüne işaret eden, özgürce ve bilgilendirme yapıldıktan sonra alınan rıza” şeklinde tanımlanmıştır. 6698 sayılı KVKK’da ise tek başına rıza kavramına yer verilmemiş, “açık rıza” ifadesi kullanılmıştır. KVKK’ya göre açık rıza “belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza”dır.<sup>351</sup> Bu tanımlardan yola çıkılarak Tüzük ile kişisel verilerinin işlenmesi için veri sahibinden alınması gereken rıza için öngörülen şartların kuvvetlendirildiği sonucuna ulaşılabilecektir.<sup>352</sup> Dolayısıyla her ne kadar Tüzükte sözcük olarak “açık rıza” kavramına yer verilmediyse de KVKK ile karşılaştırma yapıldığında “bilgilendirmeye dayalı bir rıza” alındığı için bunun da açık rıza olduğu görülmektedir.*

Kişisel verilerin işlenmesi için gerekli olan rıza 95/46/EC sayılı Direktif’in 7/1 maddesinde net şekilde (unambiguously) verilmesi ve açık şekilde (explicit consent) verilmesi (95/46/EC, Rec. 33) şeklinde düzenlenmişti. GDPR’da ise rıza hususu çok daha ayrıntılı ve iradeyi esas alır şekilde düzenlenmiştir.<sup>353</sup> GDPR’ın 7/2 maddesine göre veri sahibinin rızasını yazılı bir beyan ile vermesi durumunda, rıza talebinin diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolay bir şekilde erişilebilir bir biçimde (clearly distinguishable from the other matters, in an intelligible and easily accessible form), açık ve sade bir dil (clear and plain language) kullanılarak sunulması gerekir. Rızanın varlığını veri sorumlusu (controller) ispatlamalıdır (GDPR, m. 7/1). Rızanın özgür bir şekilde verilip verilmediği değerlendirilirken, her şeyden önce rızanın bir hizmetin sağlanması da dahil olmak üzere bir sözleşmenin ifası ile ilgili olarak verilip verilmediği dikkate alınmalıdır (GDPR, m. 7/4). GDPR’ın 32. gerekçesinde de rızanın serbest bir şekilde, belirli, bilgilendirilmiş şekilde ve tereddüde mahal bırakmayacak açıklıkta (clear affirmative act establishing a freely given, specific, informed and unambiguous indication) şekilde yazılı, elektronik yolla veya sözlü olarak verilebileceği düzenlenmiştir.<sup>354</sup> Veri sahibinin çocuk olması hali de Tüzüğün 8 inci maddesinde özel olarak düzenlenmiştir. Öncelikle veri sahibinin çocuk olması halinde, veri sahibinin kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basmaması gerekir ve veri işlemenin söz konusu menfaatler doğrultusunda gerekli olması gerekir (GDPR, m. 6/1-f). Veri sahibi çocuğun geçerli rızası için en az 16 yaşında olması gerekir. Çocuğun 16 yaşından küçük olması halinde, söz konusu veri işleme faaliyeti, ancak rızanın çocuk üzerinde

---

<sup>351</sup> Dülger, s. 22, 23.

<sup>352</sup> Dülger, s. 67.

<sup>353</sup> Eugenia Politou/Efthimios Alepis/Constantinos Patsakis, “Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions”, Journal of Cybersecurity, V. 4, I. 1, January 2018.

<sup>354</sup> Handbook on European Data Protection, s.112 vd.

velayet hakkı bulunan kişi tarafından verilmesi ve onaylanması halinde ve bu onay devam ettiği müddetçe hukuka uygun olacaktır (GDPR, m. 8/1).

**b. Bilinç Unsuru**

Tüzükteki tanımdan anlaşıldığı üzere, rıza “bilinçli” olmalıdır, yani veri sahibi rıza beyanında bulunmadan önce konuya ilişkin bilgi sahibi olmalıdır. Madde 29 Çalışma Grubu yapılacak bu bilgilendirmenin açık ve anlaşılabilir şekilde gerçekleştirilmesi ve işlenen veriler, işlemenin amaçları, verilerin muhtemel alıcıları ve veri sahibinin hakları gibi konularda tam ve eksiksiz bilgiler içermesi gerektiğini belirtmiştir.<sup>355</sup> Ayrıca, kişisel verilerin işlenmesine verilen rızanın konuya özel olması büyük önem arz etmektedir. Bu anlamda rıza “spesifik” olmalıdır ve rızanın hangi işleme faaliyetlerine yönelik olarak verildiği açıkça anlaşılabilir.<sup>356</sup> Dolayısıyla, verilerin işlenmesine yönelik açıklanan genel bir rıza, Tüzük anlamında koşulları sağlayan bir hukuka uygunluk hali oluşturmayacaktır.<sup>357</sup>

**c. Ayırt Edicilik, Anlaşılabilirlik ve Erişilebilirlik Unsuru**

Veri sahibinin rızasının diğer hususlarla da ilgili olan yazılı bir beyan bağlamında verilmesi durumunda, yani beyanın rızadan başka konuları da kapsamaması durumunda; rıza talebinin, diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulması gerekir. Söz konusu beyanın herhangi bir kısmının Tüzüğün ihlali niteliğinde olması durumunda bu kısmın bağlayıcı olmayacağı da açıkça düzenlenmiştir.<sup>358</sup>

Veri işleminin rızaya dayalı olduğu hallerde, rıza talebi açık bir şekilde ayırt edilebilir, anlaşılır ve kolay erişilebilir bir biçimde açık ve sade bir dil kullanılmak suretiyle sunulmalıdır (GDPR, m. 7/2). Rıza, yazılı form dışında elektronik veya sözlü olarak da sunulabilecektir (GDPR, rec. 32). Rıza, bir internet sitesini ziyaret esnasında kutuyu işaretleme şeklinde olabilecek, buna karşılık sessizlik (silence), önceden işaretlenen kutucuklar (pre-ticked boxes) veya hareketsizlik (inactivity) rıza olarak yorumlanamayacaktır. İşlenen her bir veri için ayrı rıza gereklidir. Rızanın verildiği durumlarda, veri sorumlusu veri sahibinin rızası bulunduğunu ispatlayabilmelidir (GDPR, rec. 42).

---

<sup>355</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 146; Article 29 Working Party (2007), Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, Brüksel, 15 Şubat 2007.

<sup>356</sup> **Develioğlu**, s. 52, 53.

<sup>357</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 112.

<sup>358</sup> GDPR, m. 7(2).

Bu noktada ayrıca rıza formuna ilişkin yukarıdaki açıklamalarımı hatırlatıyor, tekrara girmemek adına okuyucuyu ilgili başlığa yönlendirmekle yetiniyorum.

**d. Rızanın Geri Alınabilirliği**

Önem arz eden bir diğer husus ise veri sahibinin her zaman rızasını geri alma hakkının bulunmasıdır. Veri sahibi, rıza vermeden önce bu hususta bilgilendirilmelidir. Ayrıca rızanın geri alınması, rızanın verilmesi kadar kolay olmalıdır.<sup>359</sup> Rızanın geri alınması ileriye yönelik bir hak olup, geçmişteki işlemler için bir etki doğurmaz.<sup>360</sup>

**e. Rızanın Özgürce Verilmesi Unsuru**

Ayrıca, rızanın geçerli olması için *özgür bir şekilde verilmesi* gereklidir. Bu anlamda, rızanın özgürce verilip verilmediği değerlendirilirken, her şeyden önce, bir hizmetin sağlanması da dahil olmak üzere, bir sözleşmenin ifasının, söz konusu sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlı olup olmadığına azami özen gösterilmesi gerekir.<sup>361</sup> Böylece Tüzük, taraflar arasında güç dengesizliğinin mevcut olduğu hallerde verilen rızayı açıkça geçersiz saymıştır.<sup>362</sup> Örneğin; Madde 29 Çalışma Grubu, işçilerin, işçi/işveren ilişkisinden kaynaklanan tabi olunuş nedeniyle neredeyse hiçbir zaman özgürce rıza verebilecek, rıza vermeyi reddedebilecek veya rızasını geri alabilecek bir pozisyonda olmadığını belirtmiştir. Buna göre, güç dengesizliği sebebiyle, işçiler, yalnızca rıza vermeyi reddetmelerine herhangi bir negatif sonucun bağlanmadığı nadir durumlarda özgür iradeleriyle rıza verebileceklerdir.<sup>363</sup> Başka bir örnek ise, yolcu isim kayıtlarının bir ülkenin göç idaresine aktarılmasına ilişkin yolcular ile bir havayolu arasında yapılan bir anlaşma düşünülebilir. Yolcuların ilgili ülkeyi ziyaret edebilmeleri için başka bir şansları olmadığından böyle bir anlaşmanın veri koruma hukuku anlamında özgür bir şekilde verilen bir rızaya dayandığını söylemek mümkün değildir. Bu verilerin hukuka uygun bir şekilde göç idaresine aktarımından bahsedilebilmesi için, bu aktarımın rızadan başka bir yasal dayanağı olması gerekir.<sup>364</sup>

---

<sup>359</sup> GDPR, m. 7(3).

<sup>360</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 150.

<sup>361</sup> GDPR, m. 7(4).

<sup>362</sup> **Develioğlu**, s. 54.

<sup>363</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 144.

<sup>364</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 146.

## f. Çocukların Rızası

Rıza ile ilgili belirtilmesi gereken diğer bir konu ise, doğrudan bir çocuğa bilgi toplumu hizmetleri<sup>365</sup> sağlanması ile ilgili olarak çocuğun kişisel verilerinin işlenmesidir. Tüzük uyarınca, bir çocuğa bilgi toplumu hizmeti sunulurken kişisel verilerinin işlenmesinin geçerli bir şekilde rızasına dayanabilmesi için çocuk en az 16 yaşında olmalıdır.<sup>366</sup> Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde ve verildiği veya onaylandığı ölçüde hukuka uygundur.<sup>367</sup> Üye Devletler, belirlenen bu yaşı 13 yaşına kadar indirebilir.<sup>368</sup> Ayrıca, çocuklara ait verilerin işlenmesi ile ilgili getirilen bu düzenlemelerin, Üye Devletlerin sözleşmeler hukuku anlamında sözleşmenin geçerliliği, kurulması ve hükmüne ilişkin kurallarını etkilemeyeceği de Tüzükte belirtilmiştir.<sup>369</sup>

Veri sahibinin çocuk olduğu durumlarda rızanın geçerli olabilmesi için çocuğun en az 16 yaşında olması gerekir (GDPR, m. 8/1). Veri sahibinin 16 yaşından küçük olduğu durumlarda, rızanın velayet hakkı sahibi tarafından verilmesi veya çocuk tarafından verilir velayet hakkı sahibi tarafından onaylanması şarttır (GDPR, m. 8/1).

## 2. İşlemenin Bir Sözleşmenin Kurulması veya İfası İçin Gerekli Olması

Veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için işleme faaliyetinin gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.<sup>370</sup>

## 3. İşlemenin Veri Sorumlusunun Hukuki Yükümlüğünü Yerine Getirebilmesi İçin Zorunlu Olması

Veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile işleme faaliyetinin gerekli olması durumunda gerçekleştirilecek veri işleme hukuka uygundur.<sup>371</sup> Bu hukuka uygunluk sebebi, hem özel alandaki hem kamu alanındaki veri sorumluları için geçerlidir.<sup>372</sup> Söz konusu hukuki yükümlülük ilgili devletin yerel hukukundan veya AB

---

<sup>365</sup> 2015/1535 sayılı Avrupa Parlamentosu ve Konsey Direktifi m. 1(1)(b) uyarınca bilgi toplumu hizmetleri, uzaktan ve elektronik vasıtalarla ve hizmet alıcısının bireysel talebi sonucunda, kural olarak bedel karşılığı sağlanan hizmetlerdir.

<sup>366</sup> Develioğlu, s. 54.

<sup>367</sup> GDPR, m. 8(1).

<sup>368</sup> GDPR, m. 8(1) son cümle.

<sup>369</sup> GDPR, m. 8(3); Develioğlu, s. 55.

<sup>370</sup> GDPR, m. 6(1)(b).

<sup>371</sup> GDPR, m. 6(1)(c).

<sup>372</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 151.

hukukundan kaynaklanabilir. Kişisel verilerin işlenmesi için dayanak oluşturan ilgili mevzuatlar, AİHS'nin “özel ve aile hayatına saygı hakkı” ve AB Şartı'nın “özel ve aile yaşamına saygı” ve “kişisel bilgilerin korunması” hükümlerine uygun olmalıdır.<sup>373</sup>

#### **4. İşlemenin İlgili Kişinin veya Diğer Bir Gerçek Kişinin Hayati Menfaatlerini Korumak İçin Gerekli Olması**

Veri işleme faaliyetinin veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.<sup>374</sup> Kural olarak, bu hükme dayanarak veri işleme, yalnızca işlemenin başka bir sebebe dayandırılmadığı durumlarda yapılmalıdır. Dolayısıyla bu hüküm kapsamında veri işleme yetkisi, ikincil niteliktedir.<sup>375</sup>

Bu düzenlemenin 6698 sayılı KVKK'da birebir karşılığı yoktur.

#### **5. İşlemenin Kamu Yararı İçin Gerçekleştirilen Bir Görevin İfası İçin veya Veri Sorumlusunun Resmi Yetkisinin Kullanılması İçin Gerekli Olması**

Veri işleme faaliyetinin kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması hususunda gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.<sup>376</sup> Bu çerçevede, resmi yetkinin veri sorumlusu tarafından kullanılıyor olması şart değildir. Bu yetkiye sahip bir üçüncü kişinin yetkisi kapsamındaki taleplerine göre hareket edilmesi de bu hukuka uygunluk sebebi kapsamındadır.<sup>377</sup>

Bu başlık altında veri işlemenin gerçekleştirilebilmesi için, söz konusu işlemenin AB hukukunda veya yerel ülke hukukunda yasal bir dayanağı olmalıdır. Söz konusu hukuki dayanak açık ve net, ayrıca öngörülebilir olmalıdır.<sup>378</sup> Ayrıca, AB üyesi devletlerin, Tüzükte yer alan veri işleme yetkisine ilişkin kuralların uygulanması için daha spesifik hükümler uygulamaya devam edebileceği veya uygulamaya koyabileceği açıkça düzenlenmiştir.<sup>379</sup>

6698 sayılı KVKK'da ise, Tüzüğe kıyasla daha geniş bir ifade kullanılmıştır ve kamu yararı şartı aranmaksızın veri işleme imkânının kanunlarda açıkça öngörülmesi halinde işlemenin hukuka uygun kabul edileceği düzenlenmiştir.<sup>380</sup>

---

<sup>373</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 152.

<sup>374</sup> GDPR, m. 6(1)(d).

<sup>375</sup> **Voigt/von dem Bussche**, s. 108.

<sup>376</sup> GDPR, m. 6(1)(e).

<sup>377</sup> **Develioğlu**, s. 64.

<sup>378</sup> **Voigt/von dem Bussche**, s. 107, 108.

<sup>379</sup> GDPR, m. 6(2).

<sup>380</sup> **Develioğlu**, s. 65.

## 6. *Veri İşlemenin Meşru Menfaatlere Ulaşmak Amacıyla Gerekli Olması*

Veri sahibinin, özellikle çocuk olması halinde, kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin, bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması durumunda gerçekleştirilecek işleme hukuka uygundur.<sup>381</sup>

Meşru bir menfaatin varlığı her olay bazında dikkatle incelenmelidir.<sup>382</sup> Veri sorumlusunun veri işleme faaliyetinden meşru menfaati olduğu belirlenirse, bu meşru menfaat ile veri sahiplerinin menfaatleri veya temel hak ve özgürlükleri arasında bir denge kurulması gerekir.<sup>383</sup> Böyle bir değerlendirme sırasında veri sahibinin makul beklentileri de hesaba katılmalıdır. Veri sahibinin haklarının veri sorumlusunun meşru menfaatlerine ağır basması durumunda, veri sorumlusu, veri işlemenin veri sahibinin hakları üzerindeki etkilerini minimuma indirme amacıyla tedbirler alıp güvenceler getirebilir, böylece dengeyi tersine döndürerek bu hukuka uygunluk sebebine dayanabilir.<sup>384</sup>

ABAD, içtihatlarında “denge testi”ni detaylıca incelemiştir. Örneğin; *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*<sup>385</sup> davasında, ABAD, meşru menfaatlere dayanarak kişisel veri işleminin gerçekleştirilebilmesi için üç şartın tümünün sağlanması gerektiğini belirtmiştir<sup>386</sup>:

- (1) Kişisel verinin açıklanacağı üçüncü kişinin meşru bir menfaati olmalıdır,
- (2) Bu meşru menfaate ulaşmak için ilgili kişisel verinin işlenmesi zorunlu olmalıdır,
- (3) Veri sahibinin temel hak ve özgürlükleri veri sorumlusunun veya üçüncü kişilerin meşru menfaatlerinden önemli olmamalıdır.

ABAD ayrıca menfaatler dengesinin olay bazında değerlendirilmesi ve her olayda veri sahibinin haklarının uğrayacağı zararın ağırlığı gibi faktörlerin dikkate alınması gerektiğini ifade etmiştir.<sup>387</sup>

---

<sup>381</sup> GDPR, m. 6(1)(f).

<sup>382</sup> GDPR, Preamble, Gerekeç 47.

<sup>383</sup> Article 29 Working Party (2014), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 4 Nisan 2014.

<sup>384</sup> Article 29 Working Party (2014), Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 4 Nisan 2014.

<sup>385</sup> ABAD, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA ‘Rīgas satiksme’*, 4 Mayıs 2017.

<sup>386</sup> Rīgas satiksme, p. 28-34.

<sup>387</sup> *Giakoumopoulos/Buttarelli/O’Flaherty*, s. 156, 157.



Kişisel verilerin “meşru menfaatler”e dayanarak işlenmesi durumunda, veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı bulunur.<sup>388</sup> İşlemenin devamı için inandırıcı meşru bir sebep sunmadıkça veri sorumlusu işlemeyi durdurmalıdır.<sup>389</sup>

## **B. Özel Nitelikli Kişisel Verilerin İşlenmesinde Hukuka Uygunluk Nedenleri**

Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel verilerdir ve bu verilerin işlenmesi kural olarak yasaktır.<sup>390</sup> Tüzüğün 9. maddesinin 2. fıkrasında belirtilen istisnaların mevcudiyetinde ise özel nitelikli kişisel veriler işlenebilecektir:

(a) Veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi;

(b) Birlik veya Üye Devlet hukuku çerçevesinde ya da Üye Devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece, veri sorumlusunun veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi;

(c) Veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması;

(d) İşleme faaliyetinin bir vakıf, birlik veya kâr amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi;

(e) İşleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması;

---

<sup>388</sup> GDPR, m. 21(1).

<sup>389</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 158.

<sup>390</sup> GDPR, m. 9(1).

(f) Yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi;

(g) Gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya Üye Devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi;

(h) Koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;

(i) Özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;

(j) Kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.

Ek olarak, Tüzükte, Üye Devletler genetik veriler, biyometrik veriler veya sağlık ile ilgili veriler ile alakalı olarak sınırlamalar da dahil olmak üzere ek koşullar uygulamaya devam edebileceği ya da ek koşullar getirebileceği düzenlenmiştir.<sup>391</sup>

### **III. Veri İşlemenin Güvenliğine İlişkin Kurallar**

#### **A. Veri Güvenliğine İlişkin Başlıca Hükümler**

Veri işlemenin güvenliğine ilişkin kurallar, veri sorumlusu ve veri işleyeni, veri işleme faaliyetlerine herhangi bir izinsiz müdahaleyi önlemek için, uygun teknik ve düzenlemeye ilişkin tedbirler alma yükümlülüğü altına sokmaktadır.<sup>392</sup> Bu çerçevede, veri sorumlusu ve işleyen, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde, uygun teknik ve düzenlemeye ilişkin tedbirler uygular.<sup>393</sup>

---

<sup>391</sup> GDPR, m. 9(4).

<sup>392</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 165.

<sup>393</sup> GDPR, m. 32.

Alınabilecek önlemlerden bazıları Tüzükte belirtilmiştir. Buna göre (a) kişisel verilerde takma ad kullanımı ve şifreleme; (b) işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi; (c) fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi; (d) işleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve düzenlemeye ilişkin tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç,<sup>394</sup> gibi tedbirler veri işlemenin güvenliğinin sağlanması amacıyla uygulanabilecektir. Ayrıca, veri güvenliğinin sağlanması için alınacak en genel tedbirin, kişisel verilerin sadece gerçekten gerekli olduğu durumlarda ve gerekli olduğu ölçüde kullanılması olduğu unutulmamalıdır.<sup>395</sup>

Belirtilmelidir ki, veri güvenliğinin sağlanabilmesi için doğru teçhizata –donanım ve yazılım– sahip olunması yeterli değildir. Bu amacın gerçekleştirilmesi için dahili organizasyonel kurallara yer verilmesi gerekir. Bu kurallar, örneğin, çalışanlara veri güvenliği hakkında bilgi verilmesini ve veri koruma hukuku kapsamındaki sorumluluklarının anlatılmasını, kişisel verilerin kullanımının yalnızca yetkili kişinin talimatlarına veya genel kurallara uygun olarak gerçekleştirilmesini, kişisel verilerin işlenmesi ile ilgili yetki sınırlarını ve sorumlulukları net olarak belirlemeyi içerebilir.<sup>396</sup>

Ayrıca, Tüzük, veri işlemenin güvenliği için, bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olması halinde, veri sorumlusuna ihlali denetim makamına bildirme yükümlülüğü getirmiştir.<sup>397</sup>

Bir veri sorumlusunun veya işleyenin veri güvenliğini geliştirmesi için alabileceği önlemler arasında kişisel veri koruma görevlilerinin atanması, çalışanların veri güvenliği hakkında eğitilmesi, düzenli olarak denetleme, sızma ve kalite testlerinin yapılması sayılabilir.<sup>398</sup>

## **B. Gizlilik**

Tüzükte gizlilik genel bir prensip olarak kabul edilmiştir.<sup>399</sup> Tüzüğün 5. maddesinin 1. fıkrasının (f) bendi, kişisel verilerin “*yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere teknik veya düzenlemeye ilişkin uygun tedbirlerin*

---

<sup>394</sup> GDPR, m. 32(1).

<sup>395</sup> Dülger, s. 177.

<sup>396</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 165.

<sup>397</sup> GDPR, m. 33.

<sup>398</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 168.

<sup>399</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 169.

*kullanılması suretiyle kişisel verilerin güvenliğini sağlayan bir şekilde işlenmesi gerektiği*” ilkesini, “*bütünlük ve gizlilik*” adı altında düzenlemiştir. Ayrıca 32. maddede, yukarıda belirtildiği üzere, yüksek seviyede veri güvenliğinin sağlanması için veri sorumlusu ve işleyenin uygun teknik ve düzenlemeye ilişkin tedbirler alması gerektiği hüküm altına alınmıştır; bu kapsamda kişisel verilerde takma ad kullanımı ve şifreleme, işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi gibi önlemler örnek olarak gösterilmiştir. Bunun yanında, 28. maddede veri sorumlusu ile veri işleyen arasında veri işlemeye ilişkin detayların bir sözleşme veya diğer bir hukuki tasarruf ile düzenlenmesi gerektiği ve bu sözleşme veya diğer hukuki tasarrufta, veri işleyenin, kişisel verileri işleme yetkisi bulunan kişilerin gizlilik taahhüdünde bulunmasını veya uygun bir yasal gizlilik yükümlülüğü altında bulunmasını sağlaması gerektiği belirtilmiştir.

Gizlilik yükümlülüğü, kişisel veriye ilişkin bilginin, yalnızca bir bireyin kendi özel durumu sebebiyle o kişi tarafından bilinmesi durumlarında gündeme gelmez. Böyle hallerde, yukarıda bahsedilen 28. ve 32. maddeler dikkate alınmaz. Çünkü, bu kişiler tarafından kişisel verilerin kullanılması Tüzüğün uygulama alanı içerisinde değildir.<sup>400</sup> Tüzüğün 2. maddesinin 2. fıkrasının (c) bendinde bu Tüzüğün “*tamamen kişisel veya ev faaliyeti esnasında bir gerçek kişi tarafından kişisel verilerin işlenmesine uygulanmayacağı*” açıkça belirtilmiştir. Bu noktada dikkat edilmesi gereken husus ise, ABAD’ın *Bodil Lindqvist*<sup>401</sup> davasında, bu istisnanın dar yorumlanması gerektiğini ifade ettiği<sup>402</sup>.

Gizlilik yükümlülüğünün bir diğer görünüşü ise “*haberleşmenin gizliliği*”dir ve bu yükümlülük E-Gizlilik Direktifi’ne tabidir. Bu direktifin elektronik haberleşmelerin gizliliğini sağlamaya ilişkin kuralları, Üye Devletlerin, haberleşmenin ve ilgili üst verilerin bunları kullanan kişiler tarafından veya kullanan kişilerin onayı ile gerçekleştirilenler dışında denetlenmesi veya dinlenmesinin önüne geçilmesini sağlaması gerektiğini düzenlemektedir.<sup>403</sup> E-Gizlilik Direktifi’nde ayrıca; ülkelerin ulusal hukuklarındaki düzenlemeler ile ulusal güvenlik, savunma, suçun önlenmesi ve tespiti amaçlarıyla ve yalnızca bu amaçlar için gerekli ve ölçülü ise, bu ilkeye istisna getirebileceği ifade edilmiştir.<sup>404</sup>

---

<sup>400</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 170.

<sup>401</sup> ABAD, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 Kasım 2003.

<sup>402</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 170.

<sup>403</sup> E-Gizlilik Direktifi, m. 5(1); **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 171.

<sup>404</sup> E-Gizlilik Direktifi, m. 15(1); **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 171.

### C. Kişisel Veri İhlali Bildirimi

Kişisel verilerin güvenliğinin ihlali halinde, ihlal, ilgili kişi için teşkil ettiği risk göz önünde bulundurularak, denetim makamına ve ilgili kişiye bildirilmelidir.<sup>405</sup> Bu kapsamda, kişisel veri ihlali; iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik ihlalidir.<sup>406</sup> Veri ihlalleri bireylerin gizlilik ve veri koruma hakları üzerinde çok tehlikeli sonuçlar doğurabilir. Çünkü veri ihlali, veri sahibinin verisi üzerindeki kontrolünü kaybetmesi anlamına gelmektedir.<sup>407</sup> Bu bağlamda, Madde 29 Çalışma Grubu, ihlallerin kişisel veri üzerine üç etkisi olabileceğini ifade etmiştir: İfşa, kayıp ve/veya değişiklik.<sup>408</sup>

Tüzüğün lafzına dikkat edildiğinde, kişisel veri ihlalden bahsedebilmek için kastın veya ihmalin varlığı önemli değildir, ihlalin nasıl ve neden gerçekleştiğinin bu açıdan bir önemi yoktur.<sup>409</sup> Bildirim yükümlülüğü ise her ihlalde doğmayacaktır.<sup>410</sup>

Tüzük uyarınca, bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması haricinde, veri sorumlusu, gereksiz gecikmeye mahal vermeden ve uygun olması halinde, ihlalden haberdar olduktan itibaren *en geç 72 saat içerisinde*, kişisel veri ihlalinin yetkili denetim makamına bildirmelidir. Gecikme halinde, yapılan bildirimde gecikmenin sebeplerine de yer verilmelidir.<sup>411</sup> Tüzüğün ilgili düzenlemesinden anlaşılacağı üzere, bildirim yükümlülüğü yalnızca veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olduğu durumlarda söz konusu olacaktır.

Denetim makamlarına yapılacak kişisel veri ihlali bildiriminin, en azından, ilgili veri sahibi kategorileri ve yaklaşık sayısı ile ilgili kişisel veri kaydı kategorileri ve yaklaşık sayısı da dahil olmak üzere kişisel veri ihlalinin mahiyetini; veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgilerini; kişisel veri ihlalinin olası sonuçlarını; kişisel veri ihlalinin olası olumsuz etkilerini azaltmak için alınanlar da dahil olmak

---

<sup>405</sup> Develioğlu, s. 108.

<sup>406</sup> GDPR, m. 4(12).

<sup>407</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 172.

<sup>408</sup> Article 29 Working Party (2017), Guidelines on Personal data breach notification under Regulation 2016/679, WP250, 3 Ekim 2017, s. 6.

<sup>409</sup> Voigt/von dem Bussche, s. 68.

<sup>410</sup> Voigt/von dem Bussche, s. 68.

<sup>411</sup> GDPR, m. 33(1).

üzere, kişisel veri ihlalinin ele alınması için veri sorumlusu tarafından alınan veya alınması önerilen tedbirleri içermesi gerekir.<sup>412</sup>

Tüzüğün veri ihlali bildirimine ilişkin düzenlemesi belirli yönlerden 108 No’lu Sözleşme ve 6698 sayılı KVKK’dan farklılık gösterir. 108 No’lu Sözleşme’ye göre veri sorumlularını, veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olduğu durumlarda ihlali “*gecikmeksizin*” yetkili denetim makamına bildirmelidir.<sup>413</sup> Ayrıca, 6698 sayılı KVKK’da işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu “*en kısa sürede*” ilgilisine ve Kurula bildirmesi gerektiği düzenlenmiştir.<sup>414</sup> Burada değinilmesi gereken diğer bir nokta ise, kanunun kişisel veri ihlalinin kişisel verilerin “kanuni olmayan yollarla başkaları tarafından elde edilmesi” olarak tanımlamış olmasıdır. Dolayısıyla, Tüzüğün getirdiği düzenlemenin daha kapsamlı ve detaylı olduğunu söylemek mümkündür.

Tüzükte, veri ihlali bildiriminin denetim makamına “*en geç 72 saat içinde*” yapılması öngörülmüşken, gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesi muhtemel olan veri ihlallerini, veri sorumlusu, veri sahibine “*gereksiz bir gecikmeye mahal vermeden*” iletmelidir.<sup>415</sup> Bu bildirimde kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanmalıdır;<sup>416</sup> ayrıca bu bildirimde, denetim makamına yapılan bildirimdekilere benzer bilgilere yer verilmelidir.<sup>417</sup> Bazı durumlarda ise veri sorumlusunun veri sahibine bildirim yapma zorunluluğu yoktur. Örneğin; veri sorumlusu uygun teknik ve düzenlemeye ilişkin koruma tedbirleri almış ve bu tedbirleri kişisel veri ihlalden etkilenen kişisel verilere uygulamış ise bildirim yükümlülüğü altında değildir.<sup>418</sup> Veri sorumlusunun ihlalden sonra söz konusu yüksek riskin gerçekleşme ihtimalinin azalması için önlem almış olması durumunda da bildirim gerekmecektir.<sup>419</sup> Son olarak, eğer bildirim ölçsüz bir çaba gerektirecekse, veri sorumlusundan bu bildirim gerçekleştirilmesi beklenemez; böyle bir durumda, veri sahibi ihlal hakkında başka yollarla bilgilendirilebilir, örneğin; kamuya yönelik bir bildirim ile.<sup>420</sup>

---

<sup>412</sup> GDPR, m. 33(3).

<sup>413</sup> Convention 108, m. 7(2).

<sup>414</sup> 6698 Sayılı Kişisel Verilerin Korunması Kanunu, m. 12(5).

<sup>415</sup> GDPR, m. 34(1).

<sup>416</sup> GDPR, m. 34(2).

<sup>417</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 173.

<sup>418</sup> GDPR, m. 34(3)(a).

<sup>419</sup> GDPR, m. 34(3)(b).

<sup>420</sup> GDPR, m. 34(3)(c).

Denetim makamını ve veri sahibini kişisel veri ihlalleri hakkında bilgilendirme yükümlülüğü esasen veri sorumlularına ilişkin olarak düzenlenmiştir. Fakat bildirim konu olacak ihlaller, veri işleyen nezdinde de gerçekleşebilir.<sup>421</sup> Bu nedenle, veri işleyen, bir kişisel veri ihlalinden haberdar olduktan sonra, “herhangi bir gecikmeye mahal vermeden” veri sorumlusuna bildirimde bulunmalıdır.<sup>422</sup>

#### **IV. Hesap Verebilirlik ve Uyum Sağlanmasına İlişkin Kurallar**

Hesap verebilirlik prensibi, veri korumasına ilişkin kuralların etkili bir şekilde uygulanması için oldukça önemlidir. Bu bağlamda, veri sorumlusu, veri koruma kurallarına uyumlu hareket ettiğini göstermek zorundadır, dolayısıyla bunu gösterebilecek durumda olmalıdır. Ayrıca, hesap verebilirliğin yalnızca ihlal gerçekleşikten sonra ortaya çıktığı düşünülmemelidir. Veri sorumlularının, veri işlemenin her aşamasında, verilerin korunmasına uygun ve elverişli bir veri işleme politikası uyarınca faaliyet göstermesi gerekir. Tüzük, veri sorumlularının, veri işlemeyi kurallar ile uyumlu bir şekilde gerçekleştirdiklerini gösterebilmeleri ve gösterecek durumda olmaları için uygun teknik ve düzenlemeye ilişkin önlemler almaları gerektiğini belirtmektedir.<sup>423</sup>

##### **A. Veri Koruma Görevlileri**

Tüzükte, belirli durumlarda, veri sorumlularının veri koruma kurallarına uygun faaliyet göstermesi hususunda onlara bilgi ve tavsiye verecek “veri koruma görevlileri” atanmasını öngörmüştür. Veri koruma görevlileri, ayrıca, denetim makamları, veri sahipleri ve atandıkları kuruluş arasında bir aracı görevi görür.<sup>424</sup>

Veri koruma görevlisi atamak, 108 No’lu Sözleşme uyarınca veri koruma kurallarına uyumluluğu göstermek için tercih edilebilecek yöntemlerden biri olarak değerlendirilmekteydi. Tüzükte ise, bu durumun aksine, veri koruma görevlisinin atanması her zaman veri sorumluları ve işleyenlerinin takdirinde olmayıp, bazı durumlarda zorunludur.<sup>425</sup> Tüzükte (i) işleme faaliyetinin bir kamu kuruluşu veya organı tarafından gerçekleştirilmesi, (ii) veri sorumlusu veya işleyenin temel faaliyetlerinin yapıları, kapsamaları ve/veya amaçları gereği veri sahiplerinin düzenli ve sistematik bir şekilde büyük çaplı olarak izlenmesini gerektiren işleme faaliyetlerinden meydana gelmesi veya (iii) veri sorumlusu veya işleyenin temel faaliyetlerinin özel kategorilerdeki verilerin veya mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak

---

<sup>421</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 173.

<sup>422</sup> GDPR, m. 33(2).

<sup>423</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 174.

<sup>424</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 175.

<sup>425</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 175.

işlenmesinden meydana gelmesi durumunda bir veri koruma görevlisi belirlenmesinin zorunlu olduğu düzenlenmiştir.<sup>426</sup> Bu düzenlemede kullanılan “sistemik bir şekilde büyük çaplı olarak izlemek” ve “temel faaliyetler” gibi terimler Tüzükte tanımlanmamış olsa da, Madde 29 Çalışma Grubu bunların nasıl yorumlanması gerektiği ile alakalı kılavuzlar yayınlamıştır.<sup>427</sup> Örneğin; bir hastane ve bir sağlık sigortası şirketi, faaliyetlerinin çoğu özel kategorilerdeki kişisel verilerin büyük çaplı olarak işlenmesinden oluşan veri sorumlularıdır.<sup>428</sup>

Tüzükte, veri koruma görevlisinin belirlenmesinin zorunlu olduğu yukarıdaki açıklanan durumlar haricinde de veri sorumlusu veya işleyenin ya da birlikler ve veri sorumlusu veya işleyeni temsil eden diğer organların bir veri koruma görevlisi belirleyebileceği düzenlenmiştir. Ayrıca, Birlik veya Üye Devlet hukuklarında, sayılan durumlar dışında başka kuruluşlar içinde veri koruma görevlisi atama zorunluluğu getirilebilir ve bu hallerde, bu kişi, birlik veya organların bir veri koruma görevlisi belirlemesi gerekmektedir.<sup>429</sup>

Bir veri koruma görevlisi atandığına, veri sorumlusu ve işleyen, bu kişinin kişisel verilerin korunmasına ilişkin tüm konulara uygun bir şekilde ve zamanında müdahil olmasını sağlar.<sup>430</sup> Örneğin; veri koruma görevlisi, veri koruma etki değerlendirmesi yapılmasına ilişkin tavsiye verilmesine dahil olmalıdır.<sup>431</sup> Veri koruma görevlisinin görevlerini efektif bir şekilde yerine getirebilmesi için, veri sorumluları ve veri işleyenler, ona gereken kaynakları sağlamalıdır.<sup>432</sup> Örneğin; görevlerinin yerine getirilmesi ile ilgili olarak veri koruma görevlilerine maddi kaynak, altyapı ve teçhizatlar sağlanmalı, veri koruma görevlileri uzmanlıklarını geliştirebilmeleri ve güncel kalabilmeleri için sürekli eğitime tabii tutulmalıdır.<sup>433</sup>

İlaveten, Tüzükte, veri koruma görevlilerinin bağımsız bir şekilde hareket edebilmelerinin sağlanması için bazı teminatlar düzenlenmiştir. Bu bağlamda, veri sorumlusu ve işleyen, veri koruma görevlisinin görevlerini yerine getirmesi ile ilgili olarak hiçbir talimat almamasını sağlar. Ayrıca, veri koruma görevlisi, görevlerinin yerine getirilmesi nedeniyle veri sorumlusu ya da işleyen tarafından işten çıkarılamaz veya cezalandırılmaz.<sup>434</sup>

---

<sup>426</sup> GDPR, m. 37(1).

<sup>427</sup> Article 29 Working Party (2017), Guidelines on Data Protection Officers (DPOs), WP 243 rev.01, last revised and adopted 5 April 2017.

<sup>428</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 175, 176.

<sup>429</sup> GDPR, m. 37(4).

<sup>430</sup> GDPR, m. 38(1).

<sup>431</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 175, 176.

<sup>432</sup> GDPR, m. 38(2).

<sup>433</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 177.

<sup>434</sup> GDPR, m. 38(3).



Veri koruma görevlisinin görevleri, en azından; veri sorumluları ve işleyenler ile işleme faaliyetleri gerçekleştiren çalışanların veri koruma hükümleri uyarınca yükümlülükleri hususunda bilgilendirilmesi ve onlara tavsiyede bulunulmasını, işleme faaliyetlerine müdahil personelin bilinçlendirilmesi ve eğitimi ve ilgili denetimler de dahil olmak üzere veri sorumlusu ve işleyenin kişisel verilerin korunmasına ilişkin politikalarına uyumluluğun izlenmesini, talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunulmasını, denetim makamıyla işbirliği yapılmasını, ön istişare de dahil olmak üzere işleme faaliyetine ilişkin konularda denetim makamına yönelik bir temas noktası olarak hareket edilmesini ve, uygun olduğu hallerde, diğer her türlü konu ile ilgili olarak danışmanlık verilmesini içerir.<sup>435</sup>

AB kuruluş ve organlarının elinde bulunan kişisel verilere ilişkin 45/2001 sayılı Direktif, her Birlik kuruluş ve organının veri güvenlik görevlisi ataması gerektiğini düzenlemiştir.<sup>436</sup> Veri koruma görevlisi, bu kapsamda, bu direktifin hükümlerinin AB kuruluş ve organlarında doğru bir şekilde uygulandığını ve veri sahipleri ile veri sorumlularının hak ve yükümlülükleri hakkında bilgilendirilmiş olduğunu garantiye almak ile görevlendirilmiştir.<sup>437</sup> Tüzük ile aynı doğrultuda, 45/2001 sayılı Direktif de, veri koruma görevlilerinin görevlerini yerine getirirken bağımsız olması ve bu kişilere görevleri için gerekli eleman ve kaynakların sağlanması gerektiğini belirtmiştir.<sup>438</sup>

GDPR ile kabul edilen önemli yeniliklerden birisi de belirli ölçekteki veri sorumlusu/işleyen şirketlerin, kişisel verilerin korunması konularına müdahil olabilecek (GDPR, m. 38/1), veri koruma mevzuatı ve uygulaması konusunda uzman olan (GDPR, rec. 97) bir kişiyi veri koruma görevlisi olarak bulundurmakla yükümlü kılmasıdır. Veri koruma görevlisi, denetim makamları ile veri sahipleri ve veri sorumlusu/işleyen arasında bağlantıyı sağlar ve GDPR uyumluluğunu sağlamayı kolaylaştırdığı için de veri sorumlusu/işleyen şirketlerin sorumluluğunda köşe taşı olarak kabul edilir.<sup>439</sup> Veri sorumlusu/işleyen şirketler veri koruma görevlisine gereken kaynakları sağlamalıdır. Veri koruma görevlisi, veri işleme ile uğraşan kişi/grup/organizasyonlar için önemli bir destekçi/katkı sağlayıcı olarak görülmelidir. Veri koruma görevlisinin görevleri şu şekilde belirlenmiştir (GDPR; m. 39/1):

---

<sup>435</sup> GDPR, m. 39(1).

<sup>436</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 177.

<sup>437</sup> Veri koruma görevlilerinin tüm görevleri için bkz. Regulation (EC) No. 45/2001.

<sup>438</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 177.

<sup>439</sup> Handbook on European Data Protection Law, s. 175.

- Veri sorumlusu/işleyen ile işleme faaliyetleri gerçekleştiren çalışanların GDPR ve diğer ulusal veri koruma mevzuatı uyarınca yükümlülükler hususunda bilgilendirilmeleri ve onlara tavsiyede bulunulması,

- İşleme faaliyetlerine müdahil personelin bilinçlendirilmesi ve eğitimi ile ilgili denetimler dahil olmak üzere veri sorumlusu/işleyen kişisel verilerinin korunmasına ilişkin politikalarına uyumluluğun izlenmesi,

- Talep üzerine veri koruma etki değerlendirmesine ilişkin tavsiyede bulunmak,

- Denetim makamıyla iş birliği yapmak

- İşleme faaliyetine ilişkin konularda (ön istişare dahil) denetim makamına yönelik bir temas noktası olmak ve uygun olan durumlarda konuya ilişkin danışılması.

Veri koruma görevlisi, işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçları ile işleme faaliyetlerinin risklerini göz önünde bulundurarak görevlerini yerine getirmelidir (GDPR, m. 39/2). Veri koruma görevlisi, veri sorumlusu/işleyen bir çalışanı olabilir ve hizmet sözleşmesine dayalı olarak görevini yerine getirebilir (GDPR, m. 37/6). Veri sorumlusu, veri koruma görevlisinin irtibat bilgilerini yayımlamak ve denetim makamına iletmekle yükümlüdür (GDPR, m. 37/7).

## **B. Faaliyetlerin Kaydı**

Veri işleme kurallarına uyumlu hareket edildiğinin gösterilebilmesi ve dolayısıyla veri işleme faaliyetlerinden sorumlu tutulabilmek için, genellikle, kişilerin aktivitelerini belgelendirmesi ve kaydetmesi gereklidir.<sup>440</sup> Ayrıca, işletme faaliyetlerinin kaydedilmesi, denetim makamlarının veri işlemenin hukuka uygunluğunu denetlemesine de olanak tanır.<sup>441</sup> Tüzükte, her veri sorumlusunun ve, uygun olduğu hallerde, veri sorumlusunun temsilcisinin kendi sorumluluğu altındaki işleme faaliyetlerine ilişkin bir kayıt tutması gerektiği hüküm altına alınmıştır.<sup>442</sup> Mevzubahis bu kayıt, aşağıdaki bilgilerin tamamını içermelidir:

(a) Veri sorumlusu ve uygun olduğu hallerde, ortak veri sorumlusu, veri sorumlusunun temsilcisi ve veri koruma görevlisinin isim ve irtibat bilgileri;

(b) İşleme amaçları;

(c) İşleme ile ilgili veri sahibi kategorileri ve kişisel veri kategorileriyle ilgili bir açıklama;

(d) Üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar da dahil olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcı kategorileri;

---

<sup>440</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 178.

<sup>441</sup> GDPR, m. 30(5); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.

<sup>442</sup> GDPR, m. 30(1).

(e) Uygun olduğu hallerde, uygun güvencelere ilişkin belgelendirme de dahil olmak üzere, üçüncü ülke veya uluslararası kuruluşa yönelik kişisel veri aktarımları;

(f) Mümkün olması halinde, farklı kategorilerdeki verilerin silinmesiyle ilgili öngörülen süre sınırları;

(g) Mümkün olması halinde, teknik ve düzenlemeye ilişkin güvenlik tedbirlerine yönelik genel bir açıklama.<sup>443</sup>

Veri sorumluları haricinde, Tüzükte ayrıca veri işleyenlerin ve uygun olduğu hallerde, işleyenin temsilcilerinin de bir veri sorumlusu adına gerçekleştirilen tüm kategorilerdeki işleme faaliyetlerine ilişkin olarak kayıt tutma yükümlülüğü olduğu öngörülmüştür.<sup>444</sup> Tüzüğün kabul edilmesinden önce, veri sorumlusu ve veri işleyen arasındaki sözleşmede yalnızca veri sorumlusunun yükümlülükleri düzenlendiğinden, açık olarak veri işleyenlere faaliyetlerinin kaydını tutma yükümlülüğü getirilmesi büyük bir gelişme olarak değerlendirilmektedir.<sup>445</sup>

Ek olarak, Tüzük, işletme faaliyetlerinin kaydedilmesi yükümlülüğüne bir istisna getirmiştir. Buna göre, 250'den az kişi istihdam eden bir işletme veya kuruluş için veri sorumlusu veya veri işleyen için böyle bir yükümlülük doğmayacaktır. Fakat, işletme faaliyetlerinin kaydedilmesi yükümlülüğünden muafiyet için ayrıca veri sorumlusu veya işleyenin gerçekleştirdiği işleme faaliyetlerinin veri sahiplerinin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması, işleme faaliyetinin nadiren gerçekleştirilmesi veya işleme faaliyetinin özel nitelikli verileri ya da mahkûmiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verileri kapsamaması gerekir.<sup>446</sup>

### C. Veri Koruma Etki Değerlendirmesi ve Ön İstisna

Veri işleme faaliyetleri, işlemenin doğasına ve kapsamına bağlı olarak değişen seviyelerde bazı riskleri içlerinde barındırırlar. Bu çerçevede, veri sorumluları, veri işleme faaliyetlerine başlamadan önce, planlanan işlemenin risklerinin bireylerin hakları açısından doğurabileceği sonuçları incelemeli ve değerlendirmelidir. Bu değerlendirme, veri sorumlularının muhtemel riskleri önceden belirlemesi, ele alması ve hafifletmesine; dolayısıyla veri işleme sonucu mevzubahis risklerin bireylerin hakları üzerindeki negatif etkisinin sınırlanmasına olanak

---

<sup>443</sup> GDPR, m. 30(1).

<sup>444</sup> GDPR, m. 30(2).

<sup>445</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.

<sup>446</sup> GDPR, m. 30(5); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.

sağlayacaktır.<sup>447</sup> Bu kapsamda veri koruma etki değerlendirmesi *önleyici* bir veri koruma aracıdır.<sup>448</sup>

Tüzükte, bir veri işlemenin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, veri sorumlusuna, işleme faaliyetinden önce, bu işleme faaliyetinin kişisel verilerin korunmasına olan etkisine ilişkin bir değerlendirme yapması yükümlülüğü getirilmiştir.<sup>449</sup> Tüzük, ayrıca, yüksek risk teşkil eden ve dolayısıyla veri koruma etki değerlendirmesine en çok gerek görülen işleme faaliyetlerini de belirtmiştir. Buna göre, veri işlemenin (i) gerçek kişilerle ilgili kişisel özellikler hususunda, profil çıkarma da dahil olmak üzere, otomatik işleme dayalı olan ve gerçek kişi ile ilgili hukuki sonuçlar doğuran veya gerçek kişiyi kayda değer şekilde etkileyen kararların dayandığı sistematik ve kapsamlı bir değerlendirmeyi; (ii) özel nitelikli kişisel verilerin veya mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin büyük çaplı olarak işlenmesini veya (iii) kamunun erişebileceği bir alanın büyük çaplı olarak sistematik bir şekilde izlenmesini içermesi hallerinde, bu veri işlemenin yüksek risk taşıdığı ve veri koruma etki değerlendirmesinin gerekli olduğu kabul edilmiştir.<sup>450</sup>

Veri koruma etki değerlendirmesi yükümlülüğü ile ilgili olarak, denetim makamı, bu yükümlülüğe tabi olan ve bu yükümlülüğten muaf olan işleme faaliyeti türlerine ilişkin birer liste oluşturmalı ve bu listeleri kamuya açıklamalıdır.<sup>451</sup>

Veri koruma etki değerlendirmesinin yapılması gereken hallerde, veri sorumluları, veri işlemenin amaçlarını, gerekliliği ve ölçülülüğünü, ayrıca bireylerin haklarına ilişkin oluşturduğu muhtemel riskleri değerlendirmelidir.<sup>452</sup> Söz konusu etki değerlendirmesinde ayrıca kişisel verilerin korunmasının sağlanması ve Tüzüğe uygun hareket edildiğinin gösterilmesiyle ilgili güvenceler, güvenlik tedbirleri ve mekanizmalar da dahil olmak üzere risklerin ele alınması hususunda öngörülen tedbirler de yer almalıdır.<sup>453</sup>

Madde 29 Çalışma Grubu, veri koruma etki değerlendirmeleri ve bir işlemenin yüksek risk doğurup doğurmayacağını belirlemesi ile ilgili esaslar düzenlemiştir. Bu doğrultuda, bir işleme bazında veri koruma etki değerlendirmesinin gerekli olup olmadığının tespiti için dokuz kriter geliştirmiştir; bu çerçevede bakılması gereken, veri işleme faaliyetinin şunları içerip içermediğidir:

---

<sup>447</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 179.

<sup>448</sup> **Voigt/von dem Bussche**, s. 47.

<sup>449</sup> GDPR, m. 35(1).

<sup>450</sup> GDPR, m. 35(3).

<sup>451</sup> GDPR, m. 35(4), 35(5).

<sup>452</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 180; GDPR, m. 35(7)(a)-35(7)(c).

<sup>453</sup> GDPR, m. 35(7)(d).

- (1) Değerlendirme ve notlandırma,
- (2) Hukuki veya başka önemli sonucu olan otomatik karar verme,
- (3) Sistematiik izleme,
- (4) Özel nitelikli veriler,
- (5) Geniş kapsamlı veri işleme,
- (6) Eşlenmiş veya birleştirilmiş veri kümeleri,
- (7) Hassas veri sahiplerine ilişkin veriler,
- (8) Yenilikçi kullanım veya teknolojik veya organizasyonel çözümlerin uygulanması,
- (9) Veri işlemenin kendisinin veri sahiplerinin bir hakkını kullanmasını veya bir sözleşmeden veya hizmetten yararlanmasını engellemesi.<sup>454</sup>

Madde 29 Çalışma Grubu, sayılan dokuz halden yalnız ikisinden azının varlığı durumunda, veri işleme faaliyetinin yüksek risk teşkil etmeyeceğini, dolayısıyla veri koruma etki değerlendirmesi yapılmasına gerek olmadığını ifade etmiştir.<sup>455</sup> Ayrıca, Madde 29 Çalışma Grubu, veri koruma etki değerlendirmesi yapılmasının gereğinden emin olunamayan durumlarda, veri sorumlularının veri koruma kuralları ile uyumu hususunda katkı sağlaması sebebiyle, bu değerlendirmenin gerçekleştirilmesini tavsiye etmektedir.<sup>456</sup> Son olarak, Madde 29 Çalışma Grubu, yeni bir veri işleme teknolojisinin tanıtılması halinde, veri koruma etki değerlendirilmesi yapılmasını önemli görmektedir.<sup>457</sup>

Veri koruma etki değerlendirmesi sonucunda, veri sorumlusunun riski hafifletmek için tedbir almaması durumunda veri işlemenin bireylerin hakları için yüksek risk teşkil edeceği anlaşılırsa, veri sorumlusu işleme faaliyetinden önce denetim makamına danışmalıdır.<sup>458</sup>

Veri sorumlusu şirketler, daha GDPR yürürlüğe girmeden önce GDPR uyumluluğu için gerekli hazırlıkları yapmaya başlamışlardır. Bu kapsamda, veri sorumlusu öncelikle teknolojinin mevcut durumu, uygulama maliyeti, işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hak ve özgürlükleri bakımından içerdiği riskleri

---

<sup>454</sup> Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in high risk” for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Ekim 2017.

<sup>455</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 181.

<sup>456</sup> Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in high risk” for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Ekim 2017, s. 9.

<sup>457</sup> Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in high risk” for the purposes of Regulation 2016/679, WP 248 rev.01, Brussels, 4 Ekim 2017, s. 9.

<sup>458</sup> GDPR, m. 36

dikkate alarak hem verinin işleme yönteminin belirlenmesi hem de işleme faaliyeti sırasında, uygun teknik ve organizasyonel tedbirleri uygulamalı (takma ad kullanımı gibi), veri koruma prensiplerinin etkili bir şekilde uygulanmasını temin etmeli (asgari düzeyde veri işlenmesi ilkesi/data minimisation gibi) ve bu şekilde veri sahiplerinin haklarını koruma altına almalıdır (GDPR, m. 25/1).

Bu esaslar dahilinde kişisel verinin işlenmesinin, o kişinin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesi ihtimalinin bulunması halinde (likely to result high risk), veri sorumlusu, henüz verinin işlenmesinden önce, bu işleme faaliyetinin kişisel verilerin korunmasına etkisine ilişkin bir “veri koruma etki değerlendirmesi (data protection impact assesment-DPIA)” yapmakla yükümlüdür (GDPR, m. 35/1). Bu değerlendirme asgari olarak şu hususları içermelidir (GDPR, m. 35/7):

- Öngörülen işleme faaliyeti ve işleme amaçlarına ilişkin sistematik açıklama
- İşleme faaliyetinin amaç ile kıyasen gerekliliği ve orantılılığına ilişkin değerlendirme,
- Veri sahibinin hak ve özgürlüklerine ilişkin risklere yönelik değerlendirme,
- Veri sahibinin kişisel verilerinin korunmasına yönelik tedbirler ve mekanizmalar.

Dolayısıyla, veri sorumlusu şirket kişisel verilerin korunmasına ilişkin asgari şartları sağlamak ve gerektiğinde veri koruma etki değerlendirmesi yapmakla yükümlüdür. Veri işleyenleri de kendisinden talep edilmesi veya gerekli olan durumlarda, veri koruma etki değerlendirmesi konusunda veri sorumlusuna yardım etmekle yükümlü kılınmıştır (GDPR, rec. 95).

#### **D. Davranış Kuralları (Codes of Conduct)**

Tüzük, Üye Devletler, denetim makamları, Kurul ve Komisyon, çeşitli işleme sektörlerinin spesifik özellikleri ve mikro, küçük ve orta büyüklükteki işletmelerin spesifik ihtiyaçlarını dikkate alarak, Tüzüğün düzgün bir şekilde uygulanmasına katkıda bulunması amaçlanan davranış kurallarının hazırlanmasını teşvik etmesi için çağrıda bulunmuştur.<sup>459</sup> Bu çerçevede davranış kurallarının amacı, soyut ve teknik hukuk kurallarına, uygulamaya yönelik ve pratik bir yorum kazandırmaktır.<sup>460</sup> Bu nedenle, davranış kuralları, belirli bir sektör ile veya veri işleme faaliyetlerine ilişkin teknolojiler ile ilgili çözümler sağlamaya yöneliktir.<sup>461</sup>

---

<sup>459</sup> GDPR, m. 40.

<sup>460</sup> Voigt/von dem Bussche, s. 73.

<sup>461</sup> Voigt/von dem Bussche, s. 73.

Davranış kuralları, Tüzüğün herhangi bir boyutuna ilişkin olarak hazırlanabilir. Tüzüğün 40. maddesinin 2. fıkrasında uygulanmasını belirlemek amacıyla davranış kuralları hazırlanabilecek hususlardan bazıları örnekleme yoluyla sayılmıştır. Bunlar:

- (a) Adil ve şeffaf veri işleme,
- (b) Veri sorumluları tarafından spesifik bağlamlarda gözetilen meşru menfaatler,
- (c) Kişisel verilerin toplanması,
- (d) Kişisel verilerde takma ad kullanımı,
- (e) Kamuoyuna ve veri sahiplerine sağlanan bilgiler,
- (f) Veri sahiplerinin haklarının kullanımı,
- (g) Çocuklara sağlanan bilgiler ve çocukların korunması ve çocuklar üzerinde velayet hakkına sahip olanların rızasının alınma şekli,
- (h) İşleme faaliyetinin güvenliğinin sağlanmasına yönelik tedbirler,
- (i) Kişisel veri ihlallerinin denetim makamlarına ve veri sahiplerine bildirilmesi,
- (j) Üçüncü ülkelere veya uluslararası kuruluşlara kişisel veri aktarılması veya
- (k) veri sorumluları ve veri sahipleri arasında ihtilafların çözümüyle ilgili mahkeme dışı işlemler ve diğer uyuşmazlık çözüm usulleri.

Yine 40. maddenin 2. fıkrasında, davranış kurallarının veri koruma otoriteleri ve veri sorumlusu veya veri işleyen kategorilerini temsil eden diğer organlar tarafından hazırlanabileceği, değiştirilebileceği veya kapsamlarının genişletebileceği düzenlenmiştir. Bu kuruluşlar/organlar, davranış kurallarını hazırlarken menfaat sahiplerine danışmalı, fikir ve önerilerini dikkate almalıdır.<sup>462</sup>

Ayrıca, davranış kuralları, Tüzüğün maddi olarak yorumlanmasının dışında; bu kurallara uyumluluğun izlenmesi için, kuralların konusu ile ilgili uygun bir uzmanlık seviyesine sahip olan ve bu amaca yönelik olarak yetkin denetim makamı tarafından akredite edilen bir organın<sup>463</sup>, söz konusu görevi gerçekleştirmesine olanak sağlayacak usul kurallarına da yer vermelidir.<sup>464</sup>

Davranış kuralları hazırlandıktan sonra ilgili kuruluş/organ, kurallar, değişiklik veya kapsam genişletmeye ilişkin taslağı yetkin denetim makamına ibraz eder. Denetim makamı bu taslağın Tüzük ile uyumlu olup olmadığı konusunda bir görüş sunar. Denetim makamı, yeterli güvenceleri sağladığını tespit etmesi durumunda söz konusu taslağı onaylar.<sup>465</sup>

---

<sup>462</sup> GDPR, Gerekçe 99; **Voigt/von dem Bussche**, s. 73.

<sup>463</sup> GDPR, m. 41(1).

<sup>464</sup> **Voigt/von dem Bussche**, s. 74.

<sup>465</sup> GDPR, m. 40(5).

Davranış kurallarının birden çok Üye Devletteki işleme faaliyetlerine ilişkin olmadığı hallerde denetim makamı tarafından onaylanması durumunda, yetkili denetim makamı bu kuralları tescil eder ve yayımlar.<sup>466</sup> Veri sorumluları, Tüzüğün belirli yönleri ile uyumlarını göstermek için tescil edilmiş ve yayımlanmış bu davranış kurallarına bağlı kalabilirler. Fakat, bir davranış kuralına bağlı kalarak uyumluluğun gösterilebilmesi yalnızca ilgili Üye Devletin denetim makamının mevzubahis davranış kurallarını tescil etmiş ve yayımlamış olması ihtimalinde mümkündür.<sup>467</sup>

Davranış kurallarının çeşitli Üye Devletlerdeki işleme faaliyetlerine ilişkin olduğu durumlarda ise, yetkili ulusal denetim makamı öncelikle Kurul'un taslağa ilişkin görüşünü almalıdır.<sup>468</sup> Kurul'un taslağın Tüzük ile uyumlu olduğunu onaylaması durumunda, Kurul taslağı Komisyon'a ibraz eder.<sup>469</sup> Komisyon da taslağın Tüzük ile uyumluluğunu onaylarsa, Komisyon, uygulama tasarrufları yolu ile bu taslağın AB kapsamında genel geçerliliğe sahip olduğuna karar verir<sup>470</sup> ve genel geçerliliğe sahip olduğuna karar verilen onaylı kuralların uygun şekilde ilan edilmesini sağlar.<sup>471</sup>

Ek olarak, yukarıda belirtildiği üzere, davranış kurallarına uyumluluğun izlenmesi için, yetkili denetim makamı, kuralların konusu ile ilgili uygun bir uzmanlık seviyesine sahip olan *bağımsız* bir organ akredite edecektir.<sup>472</sup> Bu organ, veri sorumlusu ve işleyenin davranış kuralları ile uyumluluğunu izleyerek, bu kuralların ihlal edilmesi halinde, veri sorumlusu veya işleyenin kurallardan askıya alınması veya çıkarılması da dahil olmak üzere, uygun işlemleri gerçekleştirecektir.<sup>473</sup> Ayrıca bu organ böylesi işlemler ve bu işlemlerin gerçekleştirilme sebepleri hususunda yetkili denetim makamını bilgilendirmelidir.<sup>474</sup>

Akreditasyon için gerekli kriterler yetkili denetim makamları tarafından detaylıca belirlenecek olmakla birlikte,<sup>475</sup> Tüzüğün 41. maddesinin 2. fıkrası uyarınca ilgili organ, aşağıdaki özellikleri taşıması halinde, davranış kurallarına uyumluluğun izlenmesi amacı ile akredite edilebilir:

(a) Kuralların konusuna ilişkin *bağımsızlık ve uzmanlığa* sahip olması,

---

<sup>466</sup> GDPR, m. 40(6).

<sup>467</sup> GDPR, m. 40(7).

<sup>468</sup> **Voigt/von dem Bussche**, s. 74.

<sup>469</sup> GDPR, m. 40(8).

<sup>470</sup> GDPR, m. 40(9).

<sup>471</sup> GDPR, m. 40(10).

<sup>472</sup> GDPR, m. 41(1).

<sup>473</sup> GDPR, m. 41(4).

<sup>474</sup> GDPR, m. 41(4).

<sup>475</sup> GDPR, m. 41(3).



(b) İlgili veri sorumlusu ve işleyenlerin davranış kurallarını uygulamaya, bu kişilerin bu kuralların hükümlerine uyumluluğunu izlemeye ve bu kuralların işleyişini düzenli olarak gözden geçirmeye elverişliliğin değerlendirilmesini sağlayan usuller oluşturmuş olması,

(c) Kurallara veya kuralların bir veri sorumlusu veya işleyen tarafından uygulanmış olma veya uygulanma şekline ilişkin ihlallere yönelik şikâyetlerin ele alınması hususunda usuller ve yapıları oluşturmuş olması ve bu usuller ile yapıları veri sahipleri ile kamuoyuna şeffaf hale getirmiş olması ve

(d) Görev ve vazifelerinin bir çıkar çatışmasına neden olmaması.

Son olarak, akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmemesi halinde veya organ tarafından gerçekleştirilen eylemlerin Tüzüğü ihlal ettiği hallerde, yetkin denetim makamı bu organın akreditasyonunu kaldırabilecektir.<sup>476</sup>

## **E. Belgelendirme**

Veri koruma belgelendirme mekanizmaları, veri koruma mühürleri ve işaretleri (belgelendirme”, veri sorumlusu ve işleyenlerin Tüzük ile uyumluluğunu göstermelerini sağlayabilecek diğer yöntemlerdir.<sup>477</sup> Bu kapsamda Tüzük; Üye Devletlerin, denetim makamlarının, Kurul ve Komisyonun, veri sorumlusu ve işleyeni belgelendirmeye teşvik etmesini istemiştir.<sup>478</sup> Belgelendirme mekanizmalarında mikro, küçük ve orta ölçekli işletmelerin spesifik ihtiyaçlarının dikkate alınması gerekliliği açıkça düzenlenmiştir.<sup>479</sup> Ayrıca, Tüzükte belgelendirmenin gönüllülük esasına dayandığı ve şeffaf bir süreç vasıtasıyla sağlandığı ifade edilmiştir.<sup>480</sup>

Belgelendirme mekanizmaları, bir veri sorumlusu veya işleyenin Tüzük kapsamındaki veri koruma standartlarına uygun işleme faaliyeti gösterdiklerini kanıtlamaya olanak sağladığından, bu veri sorumlusu veya işleyene duyulan güveni artıracak ve bu kişilerin rekabet avantajını kuvvetlendirecektir.<sup>481</sup> Buna rağmen, sağlanan bir belgelendirmenin veri sorumlusu veya işleyenin Tüzüğe uyma sorumluluğunu azaltmayacağı ve bu yetkili denetim makamlarının görev ve yetkilerine hâle getirmeyeceği unutulmamalıdır.<sup>482</sup>

---

<sup>476</sup> GDPR, m. 41(5).

<sup>477</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 183.

<sup>478</sup> GDPR, m. 42(1).

<sup>479</sup> GDPR, m. 42(1).

<sup>480</sup> GDPR, m. 42(3).

<sup>481</sup> **Voigt/von dem Bussche**, s. 77.

<sup>482</sup> GDPR, m. 42(4).

Tüzük, belgelendirmenin nasıl gerçekleştirileceğine ilişkin olarak detaylı kurallar içermemekte, yalnızca temel bilgiler vermektedir.<sup>483</sup> Buna göre, bir belgelendirme, yetkili denetim makamı veya belgelendirme organları tarafından sağlanabilir.<sup>484</sup> Söz konusu belgelendirme organlarının yetkili denetim makamı veya ulusal akreditasyon organı tarafından akredite edilmesi gereklidir.<sup>485</sup> Bu çerçevede, belgelendirme organlarının akredite edilebilmeleri için:

- (a) Belgelendirme konusuna ilişkin *bağımsızlık ve uzmanlığa* sahip olmaları,
- (b) Yetkili denetim makamı tarafından veya Kurul tarafından onaylanan kriterlere riayet etmeyi taahhüt etmiş olmaları,
- (c) Veri koruma belgelendirmesi, mühürleri ve işaretlerinin verilmesi, düzenli aralıklarla gözden geçirilmesi ve geri çekilmesine ilişkin usuller oluşturmuş olmaları,
- (d) Belgelendirme veya belgelendirmenin bir veri sorumlusu veya işleyen tarafından uygulanmış olma veya uygulanma sekline ilişkin ihlallere yönelik şikâyetlerin ele alınması hususunda usuller ve yapıları oluşturmuş olmaları ve bu usuller ile yapıları veri sahipleri ile kamuoyuna şeffaf hale getirmiş olmaları ve
- (e) Görev ve vazifelerinin bir çıkar çatışmasına neden olmamaları gereklidir.<sup>486</sup>

Akreditasyon azami beş yıllık bir süre için verilebilir ve belgelendirme organının sayılan gereklilikleri yerine getirmesi koşuluyla, aynı koşullar altında, yenilenebilir.<sup>487</sup> Ayrıca, akreditasyon koşullarının yerine getirilmemesi veya artık yerine getirilmemesi halinde veya bir belgelendirme organı tarafından gerçekleştirilen eylemlerin Tüzüğü ihlal ettiği hallerde, yetkili denetim makamı veya ulusal akreditasyon organı ilgili belgelendirme organının akreditasyonunu kaldırabilecektir.<sup>488</sup>

Belgelendirme almak için veri sorumlusu veya işleyen, belgelendirme usulünün gerçekleştirilmesi için gerekli tüm bilgileri ve işleme faaliyetlerine erişimi, belgelendirme organına veya yetkili denetim makamına sunmalıdır.<sup>489</sup> Belgelendirme en çok üç sene için sağlanabilir ve veri sorumlusu veya işleyenin ilgili kriterlere uyumunun devam etmesi şartıyla yenilenebilir.<sup>490</sup>

---

<sup>483</sup> Voigt/von dem Bussche, s. 77.

<sup>484</sup> GDPR, m. 42(5).

<sup>485</sup> GDPR, m. 43(1).

<sup>486</sup> GDPR, m. 43(2).

<sup>487</sup> GDPR, m. 43(4).

<sup>488</sup> GDPR, m. 43(7).

<sup>489</sup> GDPR, m. 42(6).

<sup>490</sup> GDPR, m. 42(7).

## V. Özel ve Olağan Veri Koruması

### A. Özel Veri Koruması

Veri sorumlusu, veri koruma ilkelerinin etkili bir şekilde uygulanması ve Tüzüğün gerekliliklerinin yerine getirilmesine yönelik olarak gerekli güvencelerin entegre edilmesi amacı ile uygun teknik ve düzenlemeye ilişkin tedbirler alarak veri sahiplerinin haklarını korunmasını sağlamalıdır.<sup>491</sup> Bu tedbirler hem işleme yönteminin belirlenmesi esnasında hem de işleme faaliyeti esnasında uygulanmalıdır.<sup>492</sup> Ayrıca, ilgili tedbirlere karar verilmesi ve tedbirlerin uygulanması esnasında, veri sorumlusu, son teknolojiler, uygulama maliyeti ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra işleme faaliyetinin gerçek kişilerin hakları ve özgürlükleri açısından teşkil ettiği çeşitli olasılıklar ve ciddiyetlere sahip riskleri de dikkate almalıdır.<sup>493</sup>

### B. Olağan Veri Koruması

Veri sorumlusu, olağan durumlarda, yalnızca işleme amacı için gerekli olan kişisel verilerin işlenmesini sağlamaya yönelik uygun teknik ve düzenlemeye ilişkin tedbirler almalıdır.<sup>494</sup> Söz konusu yükümlülük toplanan kişisel veri miktarı, bunların işlenme derecesi, saklama süresi ve bunlara erişilebilirliğe uygulanır.<sup>495</sup> Örneğin, bu yükümlülük doğrultusunda alınan bir tedbir, bir işverenin bütün işçilerinin veri sahibinin kişisel verisine erişememesine olanak sağlamalıdır.<sup>496</sup>

#### d. Mahremiyet Artırıcı Teknolojilerin Benimsenmesi (Privacy by default / by design)

Yeni bilgi teknolojileri, karşılaştığımız mahremiyet ve veri koruma risklerini artırırken öte yandan bu riskleri bertaraf etmek için ortaya konulan yöntemleri de geliştirmektedir. Mahremiyet artırıcı teknolojiler (privacy enhancing technologies- PETs) adı verilen bu yöntemlerle, teknolojiyi kullanan bireylerin kişisel bilgilerinin gizli tutulması sağlayan araçlar çeşitlendirilir ve etkinleştirilir. Bunu yaparken de, araçların hukuka uygun olması ve teknolojik sistemlerin işlevselliğinin devam ettirilmesi amaçlanır. Bu kapsamda toplanan kişisel verileri asgari düzeye indirmek, anonimlik sağlamak için takma ad kullanımı veya anonim veri bilgileri kullanmak, kullanıcının bilinçli surette rızasının alınması gibi yöntemler tercih edilir.

---

<sup>491</sup> GDPR, m. 25(1).

<sup>492</sup> GDPR, m. 25(1).

<sup>493</sup> GDPR, m. 25(1).

<sup>494</sup> GDPR, m. 25(2).

<sup>495</sup> GDPR, m. 25(2).

<sup>496</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 184.

GDPR'nın 25. maddesi mahremiyet artırıcı teknolojilerin iki yöntemi olan "Tasarımla Veri Koruması (Privay by Design)" ve "Olağan Veri Koruması (Privacy by Default-Varsayılan Ayarlarla Veri Koruması)" hususu düzenlemiştir. Buna göre tekniğin bilinen durumu, uygulama maliyeti ve verinin işleme mahiyeti, kapsamı ve amaçları ile riskler dikkate alınmak suretiyle, veri koruma ilkelerinin etkili bir şekilde uygulanması amacıyla tasarlanan takma ad kullanımı gibi uygun teknik ve kurumsal tedbirler (Technical and Organizational Measures-TOM) veri sorumlusu tarafından uygulanacak ve bu şekilde veri sahiplerinin hakları koruma altına alınacaktır (GDPR, m. 25/1). Olağan durumda koruma özellikle, veri sahibinin müdahalesi olmaksızın, kişisel verilerin belirsiz sayıda kişinin erişimine açılmamasını sağlayacaktır (GDPR, m. 25/2). Bu maddenin gerekliliklerinin yerine getirilmesinde, veri sorumlularının standartlarının yeterliliklerinin tespiti için GDPR'nın 42. maddesine uygun şekilde onaylı bir belgelendirme mekanizması benimsenebilecektir.

Veri sorumlusu ve işleyenin tekniğin bilinen durumu (son teknoloji), uygulama maliyetleri ve işleme faaliyetinin niteliği, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hak ve özgürlükleri açısından riskleri dikkate alarak, uygun güvenlik seviyesi sağlamak üzere teknik ve organizasyona ilişkin şu tedbirleri uygulayacaktır (GDPR, m. 32/1):

- Kişisel verilerde takma ad kullanımı ve şifreleme,
- İşleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli surette sağlanabilmesi,
- Fiziksel veya teknik bir durumda, kişisel verilerin elverişliliğinin ve kişisel verilere erişimin vakit kaybetmeksizin (timely) eski haline getirilebilmesi,
- İşleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve organizasyonel tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç.

Veri güvenliğinin sağlanması açısından dikkate alınması gereken tekniğin bilinen durumu (state of the art) kavramı GDPR'da tanımlanmamıştır. Patent hukukunda tekniğin bilinen durumu, patent başvurusu tarihinden önce, yazılı veya sözlü tanıtım vasıtasıyla, kullanım veya başka herhangi bir yolla kamuya sunulan her şeyi (everything made available to the public) kapsamaktadır.<sup>497</sup> Cambridge Sözlüğü'nde tekniğin bilinen durumu "çok modern, en yeni fikir ve yöntemlerin kullanıldığı" şeklinde tanımlanmıştır.<sup>498</sup> Buna karşılık Wikipedia'da tekniğin bilinen

---

<sup>497</sup> Bu konuda bkz. **Tamer Soysal**, Tarımda Biyoteknoloji Uygulamaları ve Patent Hakları (Agricultural Biotech Patent Law), Adalet Yayınevi, 2019.

<sup>498</sup> Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/state-of-the-art> (Son Erişim Tarihi: 19.03.2019)

durumu “genel gelişmenin, cihaz, teknik veya bilimsel alanda belirli bir zamanda başarılan en yüksek seviye” şeklinde ifade edilmiştir.<sup>499</sup> Tekniğin bilinen durumunun en önemli özelliği zamana göre değişmesi ve dinamik bir kavram olmasıdır. Veri koruma alanında tekniğin bilinen durumu ise daha çok siber güvenlik ile ilişkilendirilmekte ve etkin güvenlik yöntem ve teknolojilerinin sürekli surette geliştirilmesinin öncüsü olan inovasyonu ifade eder şekilde anlaşılmaktadır.<sup>500</sup> Bu yenilikler dikkate alınırken uygulama maliyeti (the costs of implementation) de dikkate alınmak zorundadır (GDPR, m. 25/1, 32/1). Dolayısıyla veri sorumlusu ve işleyenler de bu yeni olanakları uygulayan yetkin güvenlik şirketleri ile çalışmak durumunda olacaklardır.

## VI. Sınıraşan Veri Transferleri

Tüzük, AB sınırları içerisinde verilerin serbest akışını öngörürken, kişisel verilerin yurtdışına aktarılması için belirli şartların gerçekleşmesi ve Tüzüğün 5. Bölümünde açıklanan kurallara uyulması gerektiğini düzenlemiştir.<sup>501</sup> Bu bağlamda, AB'nin politik bir birlik olması ve Birlik içinde serbest veri dolaşımının hedeflenmesi nedeniyle “yurt dışına aktarılma” özel bir anlama sahip olup, AB dışındaki üçüncü ülkelere veya uluslararası kuruluşlara veri aktarımı anlamına gelmektedir.<sup>502</sup> Tüzükte açıkça belirtildiği üzere, kişisel verilerin Birlik içerisinde serbest dolaşımı, gerçek kişilerin kişisel verilerin işlenmesiyle ilgili olarak korunması ile bağlantılı sebeplerle kısıtlanamaz veya yasaklanamaz.<sup>503</sup> Ayrıca belirtilmelidir ki serbest veri akışı alanı Avrupa Ekonomik Alan Sözleşmesi ile genişletilmiştir.<sup>504</sup>

Kurallar detaylı olarak incelenmeye başlamadan önce dikkate alınması gereken diğer bir husus ise, suçun önlenmesi, soruşturulması, tespiti veya kovuşturulması veya cezai süreçlerin yürütülmesi amacıyla işlenen kişisel verilerin Üye Devlet ve Avrupa Ekonomik Alanı içindeki serbest dolaşımının Tüzüğe değil, 2016/680 sayılı Direktif'e tabi olduğudur.<sup>505</sup>

Tüzük uyarınca bir üçüncü ülkeye veya uluslararası kuruluşa veri aktarımı yapılabilmesi için, kişisel verilerin her şeyden önce Tüzüğe uygun olarak elde edilmiş olması ve Tüzüğe uygun olarak işleniyor olması gereklidir.<sup>506</sup> Tüzüğe uygun olarak elde edilmiş ve işlenmesi

---

<sup>499</sup> Wikipedia, [https://en.wikipedia.org/wiki/State\\_of\\_the\\_art](https://en.wikipedia.org/wiki/State_of_the_art) (Son Erişim Tarihi: 19.03.2019)

<sup>500</sup> Solving the GDPR Puzzle, Data Protection with State of the Art Cybersecurity, <https://www.softcat.com/assets/uploads/pdfs/gdpr/Solving-the-GDPR-puzzle.pdf>, s. 16 (Son Erişim Tarihi: 19.03.2019)

<sup>501</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 250; GDPR, m. 44(1).

<sup>502</sup> **Develioğlu**, s. 73.

<sup>503</sup> GDPR, m. 1(3).

<sup>504</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 252.

<sup>505</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 252.

<sup>506</sup> **Develioğlu**, s. 73.

gerçekleştirilen kişisel veriler, iki şekilde üçüncü bir ülke veya uluslararası kuruluşa aktarılabilir: Avrupa Birliği Komisyonunun uygunluk kararı çerçevesinde veya Komisyon'un uygunluk kararı olmamasına rağmen belirli şartların varlığı halinde.<sup>507</sup>

#### **A. Avrupa Birliği Komisyonunun Uygunluk Kararı Çerçevesinde Aktarım**

Tüzük, Komisyonun bir üçüncü ülke veya söz konusu üçüncü ülke dahilindeki bir bölge veya bir ya da daha fazla sayıda sektörün ya da uluslararası bir kuruluşun *yeterli düzeyde bir koruma sağladığına karar verdiği hallerde*, spesifik bir onaya gerek olmaksızın bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleştirebileceğini düzenlemiştir.<sup>508</sup> Bu maddedeki “*yeterli düzeyde bir koruma sağlamak*” ABAD tarafından “*üçüncü ülkenin temel hak ve özgürlüklere ilişkin olarak sağladığı korumanın temel olarak AB hukukunca sağlanan garantiler ile eş düzeyde olması*” olarak yorumlanmıştır.<sup>509</sup>

Komisyon, yabancı ülkelerin yeterli düzeyde bir koruma sağlayıp sağlamadığına bu ülkelerin yerel hukuklarını, tabi olduğu uluslararası yükümlülüklerini ve sahip olduğu bağımsız denetim mekanizmalarını inceleyerek karar verir.<sup>510</sup> Komisyon, ilgili üçüncü ülke veya uluslararası kuruluşun yeterli düzeyde bir koruma sağladığına kanaat getirirse, bağlayıcı olan “*uygunluk kararı*” verebilir.<sup>511</sup> Komisyon, bu kararı yalnızca tüm ülke çapında her alanda geçerli olmak üzere vermek yerine, söz konusu ülke içerisindeki bir bölge veya bir ya da daha fazla sayıda sektöre ilişkin olarak da verebilir.<sup>512</sup> Bu kararın varlığı halinde dahi, bir kişinin verilerinin üçüncü bir ülkeye aktarımına ilişkin olarak ilgili ülke tarafından yeterli seviyede korumanın sağlanmadığı iddiasında bulunması durumunda, yerel denetim makamlarının bu iddiayı incelemeye yetkisi vardır.<sup>513</sup>

Uygunluk kararı ile ilgili değinilmesi gereken önemli bir nokta, 95/46/EC sayılı Direktif'te hem Üye Devletlerin hem Avrupa Birliği Komisyonunun bu kararı alma imkânı düzenlenmişken, Tüzük bu kararın yalnızca Komisyon tarafından alınabileceğini öngörmüştür.<sup>514</sup>

---

<sup>507</sup> Develioğlu, s. 74.

<sup>508</sup> GDPR, m. 45(1).

<sup>509</sup> ABAD, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015, para. 96.

<sup>510</sup> Bkz: **Hakan Üzeltürk**, Avrupa Birliği Genel Veri Koruma Düzenlemesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XV, S. 2, İstanbul, 2018, s. 168; **Develioğlu**, s. 75.

<sup>511</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 254.

<sup>512</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 255; GDPR, m. 45(3).

<sup>513</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 254, 255.

<sup>514</sup> **Develioğlu**, s. 74.

Komisyon, haklarında uygunluk kararı verilmiş üçüncü ülkeler ve uluslararası kuruluşlarda meydana gelen gelişmeleri *sürekli* olarak izler.<sup>515</sup> Verilen uygunluk kararları *en az dört yılda bir* tüm gelişmeler dikkate alınarak gözden geçirilmelidir.<sup>516</sup> Bunun yanında, elde edilen bilgiler ışığında, uygunluk kararının geri alınması, değiştirilmesi veya askıya alınması her zaman mümkündür.<sup>517</sup> Böyle bir durumun varlığı halinde Komisyon ile ilgili üçüncü ülke veya uluslararası kuruluşlar arasında söz konusu durumun giderilmesi amacıyla görüşmeler de gerçekleştirebilir.<sup>518</sup>

95/46/EC sayılı Direktif'e dayalı olarak Komisyon tarafından kabul edilen kararların, Tüzük uyarınca kabul edilen bir Komisyon Kararı ile değiştirilene, yenilenene veya yürürlükten kaldırılana kadar yürürlükte kalacağı Tüzükte açıkça belirtilmiştir.<sup>519</sup>

Son olarak, Tüzükte, Komisyon'un yeterli düzeyde bir korumanın sağlandığı veya artık sağlanmadığına karar verdiği üçüncü ülkeler, bir üçüncü ülke içerisindeki bölgeler ve sektörler ile uluslararası kuruluşların Avrupa Birliği Resmi Gazetesi ve web sitesinde yayımlanacağı düzenlenmiştir.<sup>520</sup>

## **B. Avrupa Birliği Komisyonunun Uygunluk Kararı Bulunmayan Hallerde Aktarım**

Avrupa Birliği Komisyonu tarafından alınan bir karar olmaması halinde, ancak bir veri sorumlusu veya işleyenin uygun güvenceler sağlamış olması halinde ve uygulanabilir veri sahibi hakları ve veri sahiplerine yönelik etkili kanun yollarının mevcut olması koşuluyla, söz konusu veri sorumlusu veya işleyen bir üçüncü ülke veya uluslararası bir kuruluşa kişisel veri aktarabilir.<sup>521</sup>

Bu kapsamda uygun güvenceler, bir denetim makamından spesifik bir onay alınmasına gerek olmaksızın nasıl sağlanabileceği Tüzükte sayılmıştır. Buna göre, uygun güvenceler aşağıdaki yöntemlerle sağlanabilir:

- (a) Kamu kuruluşları veya organları arasında yasal bağlayıcılığı bulunan ve uygulanabilir bir belge,
- (b) Bağlayıcı kurumsal kurallar,
- (c) Komisyon tarafından kabul edilen standart veri koruma şartları,
- (d) Bir denetim makamı tarafından kabul edilen ve Komisyon tarafından onaylanan standart veri koruma şartları,

---

<sup>515</sup> GDPR, m. 45(4).

<sup>516</sup> GDPR, m. 45(3).

<sup>517</sup> Develioğlu, s. 75.

<sup>518</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 255.

<sup>519</sup> GDPR, m. 45(9).

<sup>520</sup> GDPR, m. 45(8).

<sup>521</sup> GDPR, m. 46(1).

- (e) Onaylı davranış kuralları,
- (f) Onaylı bir belgelendirme mekanizması.<sup>522</sup>

Bu yöntemlere ek olarak, yetkili denetim makamı tarafından onaylanmaları halinde veri sahibi veya işleyen ile üçüncü ülke ya da uluslararası kuruluştaki kişisel veri sorumlusu, işleyeni ya da alıcısı arasındaki özelleştirilmiş sözleşme maddeleri de verilerin yurt dışına aktarımı hususunda uygun bir güvence teşkil edebilir.<sup>523</sup> Aynı şekilde, yetkili denetim makamı tarafından onaylanması koşuluyla, kamu kuruluşları ya da organları arasındaki idari düzenlemelere eklenecek olan uygulanabilir ve etkili veri sahibi haklarını kapsayan hükümler de uygun bir güvence olarak değerlendirilebilir.<sup>524</sup>

### C. Spesifik Durumlara Yönelik Hukuka Uygunluk Nedenleri

Tüzükte, bir uygunluk kararı veya uygun güvenceler olmaması durumunda dahi, belirli bazı hallerin varlığı halinde üçüncü bir ülkeye veya uluslararası bir kuruluşa kişisel veri aktarımı gerçekleştirilebileceği düzenlenmiştir. Bu haller Tüzükte sınırlı olarak sayılmış olup aşağıdaki gibidir:

(a) Veri sahibinin, bir yeterlilik kararı ve uygun güvencelerin bulunmaması nedeniyle söz konusu aktarımların kendisine yönelik risklerin haberdar edilmesinin ardından, önerilen aktarıma açık bir şekilde rıza göstermesi,

(b) Aktarımın veri sahibi ile veri sorumlusu arasındaki bir sözleşmenin yürütülmesi veya veri sahibinin talebiyle alınan sözleşme öncesi tedbirlerin uygulanması açısından gerekli olması,

(c) Aktarımın veri sorumlusu ile başka bir gerçek veya tüzel kişi arasında veri sahibi yararına yapılan bir sözleşmenin imzalanması veya yürütülmesi açısından gerekli olması,

(d) Aktarımın kamu yararına ilişkin önemli sebeplerden dolayı gerekli olması,

(e) Aktarımın yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından gerekli olması,

(f) Aktarımın veri sahibi veya diğer kişilerin hayati menfaatlerinin korunması açısından gerekli olması,

(g) Aktarımın istişareye açık olan bir sicilden yapılması.<sup>525</sup>

Aktarımın bir uygunluk kararına veya uygun güvencelerin sağlanmış olmasına veya yukarıda açıklanan hukuka uygunluk nedenlerine dayanmadığı hallerde, üçüncü bir ülke veya

---

<sup>522</sup> GDPR, m. 46(2).

<sup>523</sup> GDPR, m. 46(3).

<sup>524</sup> GDPR, m. 46(3).

<sup>525</sup> GDPR, m. 49(1).



uluslararası bir kuruluşa yönelik bir aktarım, yalnızca aktarımın yinelemeli olmaması, yalnızca sınırlı sayıda veri sahibini ilgilendirmesi, veri sahibi tarafından gözetilen ve veri sahibinin menfaatleri veya hakları ile özgürlüklerin ağır basmadığı zorlayıcı meşru menfaatler doğrultusunda gerekli olması ve veri sahibinin veri aktarımı ile ilgili tüm durumları değerlendirmiş olması ve bu değerlendirmeye dayalı olarak kişisel verilerin korunması ile ilgili uygun güvenceler sağlamış olması durumunda, gerçekleştirilebilir.<sup>526</sup>

Madde 29 Çalışma Grubuna göre, spesifik durumlara göre hukuka uygunluk nedenine dayanan yurt dışına veri aktarımları; istisnai nitelikte olmalı ve her bireye ilişkin durum için ayrı olarak değerlendirilmelidir, ayrıca bu yöntem yinelemeli olmamalı ve geniş kapsamlı aktarımlar için kullanılmamalıdır.<sup>527</sup>

#### **D. Uluslararası Anlaşmalara Dayalı Aktarımlar**

Avrupa Birliği ve Üye Devletler, üçüncü ülkelerle, belirli amaçlarla kişisel verilerin üçüncü ülkelere aktarımını düzenleyen uluslararası anlaşmalar imzalayabilir.<sup>528</sup> İmzalanacak anlaşmalar, ilgili bireyin kişisel verilerinin korunmasını sağlayacak uygun güvenceler içermelidir.<sup>529</sup> Tüzük, bu uluslararası anlaşmalara hanel getirmez.<sup>530</sup>

#### **§ 4. Bağımsız Denetim**

Bağımsız denetim, Avrupa veri koruma hukukunun vazgeçilmez unsurlarından biridir. Nitekim, AB Şartı'nın 8. maddesinin 3. fıkrasında kişisel bilgilerin korunmasına ilişkin kurallara uyumun bağımsız bir makam tarafından denetleneceği öngörülmüştür.<sup>531</sup> Tüzükte, her Üye Devlet'in, gerçek kişilerin işleme faaliyeti ile ilgili temel hakları ve özgürlüklerini korumak ve Birlik içerisinde kişisel verilerin serbest akışını kolaylaştırmak üzere, bir ya da daha fazla sayıda bağımsız kamu kuruluşunun (denetim makamı) bu Tüzüğün uygulamasının izlenmesinden sorumlu olmasını sağlaması gerektiği öngörülmüştür.<sup>532</sup> Bağımsız denetimin kişisel verilerin korunması için önemi mahkeme içtihatlarına da yansımıştır. Örneğin, *Schrems*<sup>533</sup> davasında ABAD, Komisyon tarafından yurt dışına transfer için verilmiş bir uygunluk kararı olması durumunda dahi, ulusal

---

<sup>526</sup> GDPR, m. 49(1).

<sup>527</sup> Article 29 Working Party (2005), Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 Kasım 2005.

<sup>528</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 265, 266.

<sup>529</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 265, 266.

<sup>530</sup> GDPR, Gerekeçe 102.

<sup>531</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 189.

<sup>532</sup> Bkz: *Üzeltürk*, s. 170-172, GDPR, m. 51(1).

<sup>533</sup> ABAD, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 Ekim 2015, para. 41.

denetim makamına bu konuda bir şikâyette bulunulması durumunda, ulusal denetim makamının bu şikâyeti özenle incelemesi gerektiğini belirtmiştir.<sup>534</sup>

## I. Bağımsızlık

Tüzükte, her denetim makamının Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken *tamamen bağımsız* olarak hareket etmesi gerektiği açıkça düzenlenmiştir.<sup>535</sup> Denetim makamının, üyelerinin ve çalışanlarının direkt veya dolaylı dış etkilere karşı bağımsız kalabilmesi, veri koruma ile ilgili hususlara ilişkin karar verilirken objektifliğin sağlanabilmesi için oldukça önemli bir gerekliliktir.<sup>536</sup> Örneğin; ABAD, *Avrupa Komisyonu v. Avusturya* davasında, Avusturya Veri Koruma Mercii'nin işgücünün Federal İdare tarafından sağlanmasının ve İdare'yi sürekli bilgilendirme yükümlülüğü bulunmasının AB Veri Koruma Hukukunda öngörülmuş denetim makamının bağımsızlığı şartını ihlal ettiğini ifade etmiştir.<sup>537</sup>

Tüzükteki düzenleme uyarınca, denetim makamlarının görevlerini yerine getirirken ve yetkilerini kullanırken tamamen bağımsız olabilmesi için:

(i) Her denetim makamının üyeleri, Tüzük uyarınca görevlerini yerine getirirken ve yetkilerini kullanırken, doğrudan veya dolaylı dış etkilere karşı bağımsız hareket etmeli ve hiç kimseden talimat talebinde bulunmalı veya talimat almamalıdır.<sup>538</sup>

(ii) Her denetim makamının üyeleri görevlerine uygun olmayan eylemlerden kaçınmalıdır ve görev süreleri boyunca, maddi getirisi olsun ya da olmasın, bu göreve uygun olmayan hiçbir işle iştirak etmemelidir.<sup>539</sup>

(iii) Her Üye Devlet görevlerini etkili bir şekilde yerine getirebilmeleri ve yetkilerini etkili bir şekilde kullanabilmeleri için gereken insan kaynağı, teknik ve mali kaynaklar, binalar ve altyapının her denetim makamına sağlanmasını temin etmelidir.<sup>540</sup>

(iv) Her Üye Devlet her denetim makamının kendi personelini kendisinin seçmesini ve bu makamın kendi personelinin olmasını sağlamalıdır.<sup>541</sup>

---

<sup>534</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 190.

<sup>535</sup> GDPR, m. 52(1).

<sup>536</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 191.

<sup>537</sup> ABAD, C-614/10, *European Commission v. Republic of Austria* [GC], 16 Ekim 2012, para. 59, 63.

<sup>538</sup> GDPR, m. 52(2).

<sup>539</sup> GDPR, m. 52(3).

<sup>540</sup> GDPR, m. 52(4).

<sup>541</sup> GDPR, m. 52(5).

(v) Her Üye Devlet her denetim makamının tabi olduğu mali kontrolün denetim makamının bağımsızlığını etkilememesini ve genel devlet bütçesi veya ulusal bütçenin parçası olabilecek ayrı yıllık kamu bütçelerinin bulunmasını sağlamalıdır.<sup>542</sup>

## II. Yetki ve Görevler

Denetim makamu, ulusal hukukta Tüzük ile uyumluluğu sağlayan esas organdır. Bu amaçtan hareketle, denetim makamlarının izlemenin ötesine geçen, proaktif ve önleyici denetleme faaliyetlerini de içeren geniş görev ve yetkileri vardır. Görevlerini ifa edebilmeleri için denetim makamlarının soruşturmaya ve tavsiye vermeye ilişkin ve düzeltici yetkileri olması gerekmektedir. Denetim makamlarının yetkileri Tüzüğün 58. maddesinde sayılmıştır:

- (a) Veri sorumluları ve veri sahiplerine verilerin korunmasına ilişkin her konuda tavsiye vermek,
- (b) Standart sözleşme maddeleri, bağlayıcı kurumsal kurallar veya idare düzenlemeleri onaylamak,
- (c) İşleme faaliyetlerini araştırmak ve buna bağlı olarak müdahale etmek,
- (d) Veri sorumlularının faaliyetlerinin denetimi için ilgili bazı bilgilerin arzını talep etmek,
- (e) Veri sorumlularını uyarmak veya kınamak ve kişisel veri ihlali bildirimlerinin veri sahiplerine gönderilmesine karar vermek,
- (f) Verinin düzeltilmesine, engellenmesine, silinmesine veya yok edilmesine karar vermek,
- (g) İşleme faaliyetlerine geçici veya kati bir sınırlama getirmek,
- (h) Bir konuyu mahkemeye havale etmek.<sup>543</sup>

Denetim makamının görevlerini yerine getirebilmesi ve yetkilerini kullanabilmesi için, bir inceleme ile ilgili gerekli tüm kişisel veri ve bilgilere, ayrıca veri sorumlusunun ilgili bilgileri tuttuğu mülklere erişimi olmalıdır.<sup>544</sup> ABAD, veri sahipleri için verilerin korunmasının etkili bir şekilde sağlanabilmesi için denetim makamının yetkilerini geniş yorumlanması gerektiğini ifade etmiştir.<sup>545</sup>

Her denetim makamu, kendi bölgesinde yetkilerini kullanmayı yetkilidir.<sup>546</sup> Bunun yanında Tüzük “*tek durak noktası*” mekanizması kurmakta ve farklı denetim makamları arasında iş birliği yapılmasını gerekli kılmaktadır. Buna göre, sınır ötesi veri işleme faaliyetleri olan hallerde etkili iş

---

<sup>542</sup> GDPR, m. 52(6).

<sup>543</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 194, 195; GDPR, m. 58.

<sup>544</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 195.

<sup>545</sup> Guide to General Data Protection Regulation.

<sup>546</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 195.

birliğinin sağlanabilmesi için, Tüzük, bir baş denetim makamının, veri sorumlusunun ana veya tek işletmesinin denetim makamını olarak kurulmasını öngörmektedir.<sup>547</sup>

Bağımsız denetim makamları ayrıca talep ve şikayetler ile ilgilenmeye, verilerin korunmasına ilişkin toplum bilinci oluşturmaya ve kişisel verilerin işlenmesine ilişkin yasal ve idari düzenlemeler için ulusal karar mekanizmalarında yer alan kişilere tavsiye sağlama yetkileri mevcuttur.<sup>548</sup>

Tüzüğün “*tek durak noktası*” mekanizması uyarınca, bir Üye Devlette birden fazla denetim makamının kurulmuş ise, söz konusu Üye Devlet bu makamları Kurul’da temsil edecek denetim makamını tayin eder ve diğer makamların 63. maddede atıfta bulunulan tutarlılık mekanizmasına ilişkin kurallara uyumluluğunu sağlayacak mekanizmayı ortaya koyar.

### III. İş Birliği

Tüzük, denetim makamları arasında iş birliğine ilişkin genel bir çerçeve çizmekle birlikte, sınır ötesi veri işleme faaliyetleri ile ilgili olarak denetim makamlarının iş birliği için daha spesifik kurallar öngörmektedir.<sup>549</sup>

Tüzük uyarınca denetim makamları, Tüzük’ün tutarlı bir şekilde yürütülmesi ve uygulanması amacıyla birbirlerine ilgili bilgileri ve karşılıklı desteği sağlamalıdır, ayrıca birbirleriyle etkili iş birliğine yönelik tedbirleri uygulamaya koymalıdır.<sup>550</sup> Bu kapsamda karşılıklı yardım, özellikle, ön onaylar ve istişarelerin, denetimlerin ve soruşturmaların yürütülmesine ilişkin talepler gibi bilgi talepleri ve denetim tedbirlerini kapsar.<sup>551</sup>

Tüzüğün “*tek durak noktası*” mekanizması uyarınca, bir veri sorumlusu veya işleyenin birden çok Üye Devlette işletmesi varsa veya tek işletmesi olmasına rağmen işleme faaliyetleri birden çok Üye Devletteki veri sahiplerini önemli ölçüde etkiliyorsa, ana (veya tek) işletmenin denetim makamı, veri sorumlusu veya işleyenin sınır ötesi faaliyetlerine ilişkin olarak baş makamdır.<sup>552</sup>

Yüksek seviyede bir veri korumasının sağlanabilmesi için, baş denetim makamı yalnız hareket etmemeli, veri sorumluları veya işleyenler tarafından gerçekleştirilen kişisel veri işlemeye yönelik kararlar alınması için ilgili diğer denetim makamları ile iş birliği yapmalıdır.<sup>553</sup> İlgili

---

<sup>547</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 197; GDPR, m. 56(1).

<sup>548</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 197.

<sup>549</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 197.

<sup>550</sup> GDPR, m. 61(1).

<sup>551</sup> GDPR, m. 61(1).

<sup>552</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 198.

<sup>553</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 198.

denetim makamları arasındaki iş birliği; karşılıklı bilgi paylaşımı, karşılıklı yardım, ortak soruşturma ve izlemeler gerçekleştirilmesini içerebilir.<sup>554</sup> Bu iş birliği, tutarlılığın sağlanması ve görüş birliğine ulaşılması için gösterilmesi gereken bir çabadır.<sup>555</sup>

Her denetim makamı başka bir denetim makamının karşılıklı yardım talebine herhangi bir *gecikmeye mahal verilmeksizin* ve talebi aldıktan sonra *en geç bir ay içerisinde* yanıt vermelidir.<sup>556</sup>

Veri sorumlusunun birden çok Üye Devlette işletmesinin bulunması halinde denetim makamları, ortak soruşturmalar ve ortak yaptırım tedbirleri de dahil olmak üzere, diğer üye devletlerin denetim makamlarının üyeleri veya personelinin müdahil olduğu ortak çalışmalar gerçekleştirebilir.<sup>557</sup>

#### IV. Avrupa Veri Koruma Kurulu (European Data Protection Board)

Veri koruma kurallarının AB içinde etkili ve istikrarlı bir biçimde uygulanmasını temin etme hususunda önem teşkil eden diğer bir kurum ise Avrupa Veri Koruma Kurulu'dur (Kurul).<sup>558</sup> Tüzük, Kurul'u tüzel kişiliğe sahip bir AB organı olarak kurmuştur.<sup>559</sup> Kurul, 95/46/EC sayılı Direktif'in, Komisyon'a bireylerin kişisel verilerin işlenmesi ve gizliliğe ilişkin haklarını etkileyen AB faaliyetleri hakkında tavsiye vermesi, direktifin yeknesak uygulanmasını teşvik etmesi ve Komisyon'a veri koruması ile ilgili konularda uzman görüşü sağlaması amacıyla kurduğu Madde 29 Çalışma Grubunun halefidir.<sup>560</sup>

Kurul her üye devletin bir denetim makamı başkanı ile Avrupa Veri Koruma Denetmeni veya bunların ilgili temsilcilerinden meydana gelir.<sup>561</sup>

Kurul'un görevleri, Tüzüğün 64, 65 ve 70. maddelerinde detaylıca anlatılmış olup, bu görevler üç ana başlık altında toplanabilir:

- **Tutarlılık:** Kurul, üç halde hukuki bağlayıcılığı olan bir karar alabilir:
  - (i) Bir denetim makamı "tek durak noktası" hallerinden birinde ilgili ve gerekçeli bir itiraz ileri sürmüştü,
  - (ii) Hangi denetim makamının "baş denetim makamı" olduğu konusunda çelişkili görüşler varsa,

---

<sup>554</sup> GDPR, m. 60(1)-60(3).

<sup>555</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 198.

<sup>556</sup> GDPR, m. 61(2).

<sup>557</sup> GDPR, m. 62(1).

<sup>558</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 199.

<sup>559</sup> GDPR, m. 68(1).

<sup>560</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 199,200.

<sup>561</sup> GDPR, m. 68(3).

(iii) Yetkili denetim makamı Kurul'un görüşünü talep etmemişse veya Kurul görüşüne uygun hareket etmiyorsa.<sup>562</sup>

Kurul'un bu bağlamdaki temel görevi, Tüzüğün tüm AB'de tutarlı bir şekilde uygulanmasını sağlamaktır.<sup>563</sup>

- **Danışma:** Kurul'un görevleri, Komisyon'a AB'de veri korumaya ilişkin herhangi bir konu ile ilgili olarak tavsiye vermeyi de içermektedir.<sup>564</sup>

- **Rehberlik:** Kurul, ayrıca, Tüzüğün tutarlı bir şekilde uygulanmasını sağlamak ve denetim makamları arasında iş birliği ve bilgi değişimini sağlamak amacıyla kılavuzlar, tavsiyeler ve örnek uygulamalar yayımlar. Ek olarak, Kurul, veri sahibi ve işleyen birliklerini davranış kuralları ve veri koruma belgelendirme mekanizmaları ve mühürleri oluşturmak hususunda teşvik etmelidir.<sup>565</sup>

Son olarak değinilmesi gereken diğer bir nokta ise, Kurul'un kararlarına karşı ABAD'a başvurulabileceğidir.<sup>566</sup>

## V. Tutarlılık Mekanizması

Tüzüğün bütün Üye Devletler'de yeknesak bir şekilde uygulanmasını sağlamak için bir tutarlılık mekanizması öngörülmüştür. Buna göre, Tüzük'ün AB içerisinde tutarlı bir şekilde uygulanmasına katkıda bulunulması amacıyla, denetim makamları, Tüzükte belirtilmiş tutarlılık mekanizması vasıtasıyla, birbirleriyle ve uygun olduğu hallerde, Komisyon ile işbirliği yapmalıdır.

Bu doğrultuda tutarlılık mekanizması iki durumda kullanılır. Bunlardan ilki, Tüzüğün 64. maddesi uyarınca yetkili bir denetim makamının belirli tedbirlerden birini kabul etmeyi amaçlaması halinde veya standart sözleşme maddelerinin tespit edilmesi için bildireceği görüşlere ilişkindir. İkincisi ise Kurul'un "tek durak noktası" durumlarında denetim makamları için verdiği bağlayıcı kararlar ve denetim makamının Kurul'un görüşünü sormadığı veya görüşüne bağlı kalmadığı hallerdir.<sup>567</sup>

## VI. İvedilik Prosedürü

İstisnai durumlarda, ilgili bir denetim makamının veri sahiplerinin hakları ve özgürlüklerinin korunmasına yönelik olarak acil bir şekilde harekete geçmesine ihtiyaç varsa, söz konusu denetim makamı, tutarlılık mekanizmasından veya iş birliği prosedüründen ayrılarak, üç,

---

<sup>562</sup> GDPR, m. 65(1).

<sup>563</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 200.

<sup>564</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 200.

<sup>565</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 201.

<sup>566</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 201.

<sup>567</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 201.

ayı geçmeyecek belirli bir süre için geçerli olacak şekilde ve ilgili Devlet sınırları içinde hukuki sonuç doğurmak üzere ivedilikle geçici tedbirler alabilir.<sup>568</sup> Geçici tedbiri alan denetim makamı, gecikmeksizin, söz konusu tedbirleri alma sebeplerini, ilgili diğer denetim makamlarına, Kurul'a ve Komisyon'a bildirir.<sup>569</sup> Aynı denetim makamı, gerekçelerini belirterek Kurul'dan acil bir görüş veya nihai bir karar vermesini talep edebilir. Bu talep, ilgili kişilerin hak ve özgürlüklerin korunmasına yönelik acil bir şekilde harekete geçilmesinin gerektiği bir durumda uygun bir tedbir almadığı hallerde, herhangi bir denetim makamı tarafından, gerekçeleri açıklanarak ileri sürülebilir.<sup>570</sup> Bu bağlamda acil bir görüş veya acil bir nihai karar Kurul üyelerinin salt çoğunluğuyla iki hafta içerisinde alınır.<sup>571</sup>

## § 5. Veri Sahiplerinin Hakları ve Kısıtlamaları

### I. Veri Sahiplerinin Hakları

#### A. Bilgilendirilme Hakkı

Veri sahiplerinin kendilerine ait kişisel verilerin işlenip işlenmediğini, hangi kişisel verilerinin işlendiğini bilmesi, kişinin verileri üzerindeki kontrolünü sağlayabilmeleri ve kişisel verilerin korunması hukukundan kaynaklanan haklarını kullanabilmeleri açısından oldukça büyük önem taşır. Bu nedenle, Tüzük, veri sorumlularına, planlanan bir veri işlemesi için kişisel veri topladıkları zaman, veri sahiplerini bilgilendirme yükümlülüğü getirmiştir. Bu yükümlülüğün doğması için veri sahibinin veri sorumlusundan bilgilendirilme talep etmesi aranmamış olup, veri sorumlusunun işlemek üzere kişisel veri toplanması yeterlidir.<sup>572</sup> Çünkü, veri sahiplerinin, hangi verilerinin nasıl toplandığını, kullanıldığını veya işlendiğini, veri işleme faaliyetlerinin barındırdığı riskleri, bu risklere karşı düzenlenen güvenceleri, işlemeye ilişkin haklarını bilme hakları mevcuttur.<sup>573</sup> Aksi takdirde bireylerin kendi verileri üzerinde kontrol sağlamaları ve işleme sebebiyle ortaya çıkabilecek olumsuz sonuçlardan korunmaları mümkün olmayacaktır. Yukarıda detaylıca açıklanan “*şeffaflık ilkesi*” ile önlenmeye çalışılan da tam olarak bu tehlikelerdir.

Tüzüğün 12. maddesi uyarınca, veri sorumlusu, işleme faaliyeti ile alakalı aşağıda detaylıca anlatılacak her türlü bilgiyi *öz, şeffaf, anlaşılır ve kolayca erişilebilir* bir biçimde, açık ve sade bir dil kullanarak veri sahibine sağlama yükümlülüğü altındadır.<sup>574</sup> Bu bilgiler, veri sahibine; *yazılı*

---

<sup>568</sup> GDPR, m. 66(1); Develioğlu, s.143.

<sup>569</sup> GDPR, m. 66(1).

<sup>570</sup> GDPR, m. 66(3).

<sup>571</sup> GDPR, m. 66(4).

<sup>572</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 207.

<sup>573</sup> GDPR, Gerekeçe 39.

<sup>574</sup> GDPR, m. 12(1).

olarak veya uygun olduğu hallerde, *elektronik yollar da dahil olmak üzere diğer yollarla*, ayrıca veri sahibi tarafından talep edilmesi durumunda, veri sahibinin kimliğinin diğer yollarla doğrulanması koşuluyla, *sözlü* olarak sağlanabilir.<sup>575</sup> Ayrıca, veri sahiplerine sağlanacak bilgilerin, planlanan işleme faaliyetine yönelik anlamlı bir genel bakışın kolayca görülebilir, anlaşılabilir ve okunaklı bir biçimde sağlanması amacı ile standart simgelerle ile bir arada sağlanabileceği de Tüzükte düzenlenmiştir.<sup>576</sup>

Bilgilendirilme hakkına ilişkin örnek kararlardan biri *Smaranda Bara ve Diğerleri v. Casa Națională de Asigurări de Sănătate ve diğerleri*<sup>577</sup> davasına ilişkindir. Bu davada ABAD, ulusal idare, öncesinde başvuruculara haber vermeksizin bilgilerini Ulusal Sağlık Sigortası Fonuna aktarmıştır. ABAD, veri sahiplerinin verilerinin işlendiği hakkında bildirilmesinin, bu kişilerin işlenen verilere erişim, bu verileri düzeltme veya bu verilerin işlenmesine itiraz haklarının kullanılmasını büyük ölçüde etkilediğinden oldukça önemli olduğunu belirtmiştir. Mahkeme, belirli şartlar altında bilgilendirilme hakkının kısıtlanabileceğinin düzenlendiğini ifade etse de olayda bu koşullar gerçekleşmediğinden, başvurucuların, verileri Ulusal Sağlık Sigortası Fonuna aktarılmadan önce bilgilendirilmeleri gerektiğine hükmetmiştir.<sup>578</sup>

Tüzükte, kişisel verilerin sahibinden toplanması ve sahibinden alınmaması durumları için farklı düzenlemeler öngörülmüştür. Buna göre, kişisel veriler sahibinden toplandığında veri sahipleri:

- (i) veri sorumlusunun ve varsa, veri sorumlusunun temsilcisinin kimlik ve irtibat bilgileri,
- (ii) varsa, veri koruma görevlisinin irtibat bilgileri,
- (iii) kişisel verilerin planlanan işleme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı,
- (iv) işleme faaliyetinin veri sorumlusunun veya 3. bir kişinin menfaatine dayanması durumunda bu kişiler tarafından gözetilen meşru menfaatler;
- (v) varsa, kişisel verilerin alıcıları veya alıcı kategorileri;
- (vi) kişisel verilerin üçüncü bir ülke veya uluslararası kuruluşu aktarılmasının amaçlanıp amaçlanmadığı, aktarım kararının Komisyon tarafından bir yeterlilik kararına dayanıp

---

<sup>575</sup> GDPR, m. 12(1).

<sup>576</sup> GDPR, m.12(1).

<sup>577</sup> ABAD, C-201/14, Smaranda Bara ve Diğerleri v. Casa Națională de Asigurări de Sănătate ve Diğerleri, 1 Ekim 2015.

<sup>578</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 209.



dayanmadığı ya da aktarım kararına ilişkin uygun veya münasip güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede erişilir kılındığı,

(vii) kişisel verilerin saklanacağı süre veya bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler,

(viii) veri işlemeye ilişkin olarak sahip olduğu haklar ve bunların nasıl kullanılacağı,

(ix) kişisel verilerin sağlanması yasal ya da sözleşmeye bağlı bir gereklilik mi yoksa bir sözleşme yapılması için gereken bir gereklilik mi olduğu ve ayrıca, veri sahibinin kişisel verileri sağlamak zorunda olup olmadığı ve söz konusu verilerin sağlanmamasının muhtemel sonuçları,

(x) profil çıkarma da dahil olmak üzere otomatik karar vermenin varlığı,

(xi) bir denetim makamına şikâyette bulunma hakkı,

(xii) rızayı geri çekme hakkının varlığı hususlarında bilgilendirilmelidir.<sup>579</sup>

Kişisel verilerin sahibinden alınmaması durumunda ise veri sorumlusu veri sahibini kişisel verinin nereden ve nasıl elde edildiği hakkında bilgilendirmelidir.<sup>580</sup> Her halükârda, veri sorumlusu, veri sahibine, verilerin sahibinden alınması halinde sayılanlara benzer bilgileri sağlamalıdır.

Ayrıca, amacın sınırlandırılması ve şeffaflık ilkeleri uyarınca, veri sorumlusunun başta veri sahibine belirttiğinden farklı bir amaçla işleme yapmayı planlaması halinde, veri sorumlusu, veri sahibini, bu yeni amaç hakkında bilgilendirmelidir. Bu bilgilendirmeyi gerçekleştirip veri sahibinin yeni amaca ilişkin rızasını almaksızın veri sahibinin ilave işleme gerçekleştirmesi mümkün değildir.<sup>581</sup>

Bilgilendirilmenin sağlanma zamanı kişisel verilerin sağlandığı kaynağa göre değişiklik gösterecektir. Buna göre, kişisel verilerin direkt sahibinden sağlandığı hallerde, veri sorumlusu bilgilendirmeyi verilerin toplanması sırasında gerçekleştirmelidir.<sup>582</sup> Kişisel verilerin sahibinden alınmadığı durumlarda ise veri sorumlusu bilgilendirmeyi makul bir süre içerisinde, ancak en geç bir ay içerisinde yapmalıdır.<sup>583</sup> Ayrıca, eğer verilerin başka bir alıcıya açıklaması öngörülmüşse en geç kişisel verilerin ilk açıklandığı zaman bu bilgilendirme gerçekleştirilmelidir.<sup>584</sup>

---

<sup>579</sup> GDPR, m. 13(1), 13(2).

<sup>580</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 211.

<sup>581</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 211.

<sup>582</sup> GDPR, m. 13(1).

<sup>583</sup> GDPR, m. 14(3).

<sup>584</sup> GDPR, m. 14(3)(c).

Bilgilendirme ücretsiz olarak sağlanmalıdır. Fakat, bir veri sahibinin taleplerinin asılsız veya ölçüsüz olduğunun, özellikle taleplerin tekrarlanması nedeniyle, açıkça anlaşıldığı hallerde, veri sorumlusu makul bir ücret talep edebilir veya taleple ilgili işlem yapmayı reddedebilir.<sup>585</sup>

Veri sahibinin halihazırda bu bilgilere sahip olduğu hallerde ve ölçüde bu yükümlülüğün doğmayacağı Tüzükte açıkça düzenlenmiştir.<sup>586</sup> Ayrıca, kişisel verilerin veri sahibinden alınmadığı hallerde; özellikle kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar için gerçekleştirilen işlemlerde, ilgili bilgilerin sağlanmasının imkânsız olması veya ölçüsüz bir çaba gerektirmesi söz konusu ise bilgilendirme yükümlülüğü doğmayacaktır.<sup>587</sup>

## **B. Erişim Hakkı**

Tüzükte bireylerin kendi kişisel verilerine erişim hakkı açıkça düzenlenmiştir. Buna göre, veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme ve eğer işleme faaliyeti varsa, ilgili kişisel verilere ve belirli bilgilere erişim hakkı vardır.<sup>588</sup>

Tüzükte yer alan düzenleme uyarınca veri sahipleri kişisel verilere ilişkin olarak:

- (i) işleme amaçları,
- (ii) ilgili kişisel veri kategorileri,
- (iii) kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri,
- (iv) varsa, kişisel verilerin saklanması açısından öngörülen süre veya süre belirlenmemişse, bu sürenin belirlenmesi amacı ile kullanılan kriterler,
- (v) kişisel verilerin düzeltilmesini ve silinmesini talep etme ve veri işleminin sınırlandırılması haklarının varlığı,
- (vi) bir denetim makamına şikâyette bulunma hakkı,
- (vii) kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler;
- (viii) otomatik karar vermenin varlığı ve en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları hakkında bilgi talep etme ve bilgi alma hakkına sahiptir.<sup>589</sup>

---

<sup>585</sup> GDPR, m. 12(5).

<sup>586</sup> GDPR, m. 13(4), 14(5)(a).

<sup>587</sup> GDPR, m. 14(5)(b).

<sup>588</sup> GDPR, m. 15(1).

<sup>589</sup> GDPR, m. 15(1).

Erişim hakkı uyarınca, veri sorumlusu, işleme faaliyetinden geçen kişisel verilerin bir nüshasını veri sahibine sağlamalıdır.<sup>590</sup> Veri sahibine sağlanan her bilgi, anlaşılabilir olmalıdır.<sup>591</sup> Örneğin; teknik kısaltmalar içeren bir bilgi, kısaltmalar açıklanmadığı müddetçe yeterli sayılmayacaktır.<sup>592</sup>

ABAD içtihatları uyarınca, kişisel verilere erişim hakkı aşırı zaman sınırlamalarına tabi olmamalıdır. Örneğin; ABAD, *Rijkeboer* davasında, veri sahiplerine geçmişteki verilerine erişim hakkının sağlanmaması durumunda, bu kişilerin, verilerinin düzeltilmesi ve silinmesi gibi haklarını kullanmasının ve yasal yollara başvurup tazminat alabilmesinin mümkün olmayacağını belirtmiştir.<sup>593</sup> Dolayısıyla, veri sahiplerinin geçmişte gerçekleşmiş veri işleme faaliyetlerine ilişkin olarak makul derecede bilgi edinme şansları olmalıdır.<sup>594</sup>

### C. Düzeltme Talep Hakkı

Verilerin doğruluğu, veri korumanın etkin olarak sağlanabilmesi için mutlaka sağlanması gereken bir özelliktir ve yukarıda açıklanan doğruluk ilkesi ile doğrudan ilgilidir.<sup>595</sup> Bu gereklilikten yola çıkılarak, Tüzükte, veri sahiplerinin kendileri ile ilgili doğru olmayan kişisel verilerin *gereksiz gecikmeye mahal verilmeksizin* düzeltilmesini veri sorumlusundan talep etme hakkı bulunduğu düzenlenmiştir.<sup>596</sup> Aynı zamanda, işlemenin amaçları dikkate alındığında, veri sahibini eksik olan kişisel verilerinin tamamlanmasını talep edebilir.

Düzelتمeyi talep etme hakkı verilerin hukuka uygun işlenmesine imkân sağladığından, veri sahipleri bu talepleri için herhangi bir neden belirtmek yükümlülüğü altında değildir.<sup>597</sup> Fakat, verilerin yanlışlığını veya eksikliğini gösterme noktasında ispat yükü veri sahibindedir.<sup>598</sup> Bu husus ile ilgili olarak AİHM'in *Ciubotaru v. Moldova*<sup>599</sup> kararı mevcuttur. Bu davada resmi kayıtlara Moldovalı etnik kimliğiyle kaydedilmiş olan başvurucu bunu Romanyalı olarak değiştirmek için talepte bulunmuş, fakat başvurucunun talebini kanıtlayamaması sebebiyle bu talep reddedilmiştir. Bu noktada, AİHM, devletlerin bir bireyin etnik kökeninin kaydını gerçekleştirirken nesnel kanıtların varlığını aramasını kabul edilebilir bulsa da söz konusu dava açısından başvurucu kendi

---

<sup>590</sup> GDPR, m. 15(3).

<sup>591</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 218.

<sup>592</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 218.

<sup>593</sup> ABAD, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7 Mayıs 2009

<sup>594</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 218.

<sup>595</sup> *Giakoumopoulos/Buttarelli/O'Flaherty*, s. 219.

<sup>596</sup> GDPR, m. 16.

<sup>597</sup> *Voigt/von dem Bussche*, s. 154, 155.

<sup>598</sup> *Voigt/von dem Bussche*, s. 154.

<sup>599</sup> AİHM, *Ciubotaru v. Moldova*, No. 27138/04, 27 April 2010, para. 51, 59.

etnik kimliğine ilişkin öznel bir düşünceden öte, Romanyalı etnik kökeninden insanlar ile arasında gerçekliği kanıtlanabilir bağlantıları zaten sunmuştur. Fakat, ulusal hukuk böyle bir durumda başvuruçunun ebeveynlerinin Romanyalı etnik grubundan olduklarına dair kanıt sunulmasını aramaktadır. Moldova'nın tarihi düşünüldüğünde, böyle bir şart, Sovyet yetkililerinin kaydettiklerinden farklı bir etnik kimliğin kaydı için büyük bir engel oluşturmaktadır. Bu davada AİHM, Moldova'nın pozitif yükümlülüklerine uygun hareket etmeyerek başvuruçunun özel hayata saygı hakkını ihlal ettiğine kanaat getirmiştir.<sup>600</sup>

Düzeltilme hakkına ilişkin diğer bir husus ise, bu hakkın yalnızca “veri sahiplerine”, “kendi kişisel verileri” ile ilgili tanınmış olduğudur. Buna göre, bir kişi, üçüncü bir kişinin kişisel verilerinin düzeltilmesi talebinde bulunamaz.<sup>601</sup>

#### **D. Silinmeyi Talep Hakkı (Unutulma Hakkı)**

Tüzükten önceki düzenlemelerde açık ve münhasır bir hak olarak yer almayan silinme hakkı, ilk olarak ABAD'ın *Google Spain*<sup>602</sup> kararı ile büyük dikkat çekmiş, daha sonra Tüzükte yer vermek suretiyle güçlenmiştir.<sup>603</sup> Söz konusu *Google Spain* kararında, ABAD, Google'ın başvuruçuya ilişkin güncel olmayan bilgileri silmek yükümlülüğü altında olup olmadığını incelemiştir. Bu davada, avukat olan başvuruçu, sosyal güvenlik borçlarının yapılandırılması için mülkünü satmak zorunda kaldığına ilişkin bilgileri içerir gazete haberlerinin Google'da adı ile yapılan bir arama sonucu listelenmesinin 95/46/EC sayılı Direktif'e aykırılık teşkil ettiğini iddia etmiştir. Bu noktada ABAD, kişinin ismiyle yayınlanmış kişisel verilerinin geçersiz veya ilgisiz hale gelmesinden sonra ve artık bu verilerin işlenmesinin amaç için gerekli olmadığı halde, ilgili kişisel verilerin silinmesi gerektiğine hükmetmiştir.<sup>604</sup>

Bu hak çerçevesinde veri sahibinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini veri sorumlusundan talep etme hakkı bulunur. Buna bağlı olarak aşağıdaki hallerden birinin geçerli olması durumunda, veri sahibinin kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğü bulunur:

(a) kişisel verilerin toplanma veya işleme amaçlarıyla ilişkili olarak artık gerekli olmaması,

---

<sup>600</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 219, 220.

<sup>601</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 155.

<sup>602</sup> ABAD, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC]* (“Google Spain”), 13 Mayıs 2014.

<sup>603</sup> *Google Spain*, s. 156.

<sup>604</sup> **Dülger**, s. 167, 168.

(b) veri sahibinin işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması,

(c) veri sahibinin işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması,

(d) kişisel verilerin yasa dışı biçimde işlenmiş olması,

(e) veri sorumlusunun tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması,

(f) kişisel verilerin Tüzüğün 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması.<sup>605</sup>

Silinme hakkı kapsamında veri işlemenin hukuka uygun olduğunu ispat yükü, işleme faaliyetlerinin hukuka uygun olmasından sorumlu veri sorumlusundadır.<sup>606</sup> Ek olarak, hesap verebilirlik ilkesi gereğince veri sorumlusu daima veri işlemenin hukuki bir temele dayandığını gösterebilir durumda olmalıdır.<sup>607</sup>

Tüzük, silinmenin talep edilebilmesi hakkına bazı sınırlamalar getirmiştir. Buna göre, veri işleme faaliyetinin:

(i) ifade ve bilgi edinme hakkının kullanılması,

(ii) veri sorumlusunun tabi olduğu Birlik veya üye devlet hukuku çerçevesinde işleme faaliyeti gerektiren bir yasal yükümlülüğe uygunluk açısından veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin uygulanması açısından,

(iii) halk sağlığı alanındaki kamu yararı sebeplerinden dolayı,

(iv) silinme hakkının ilgili işleme hedeflerinin yakalanmasını imkansız hale getirmesi veya yakalanmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde, kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veya

(v) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından gerekli olması halinde silinme talep edilemeyecektir.<sup>608</sup>

Veri sorumlusunun kişisel verileri kamuya açıklamış olduğu ve kişisel verileri silmek zorunda olduğu hallerde, veri sorumlusu, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri sahibinin silinmesini talep etmiş olduğu kişisel verileri isleyen diğer veri

---

<sup>605</sup> GDPR, m. 17.

<sup>606</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 223.

<sup>607</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 223.

<sup>608</sup> GDPR, m. 17(3).

sorumlularını silinme talebi hakkında bilgilendirmek üzere teknik tedbirler de dahil olmak üzere makul adımları atmalıdır.<sup>609</sup>

Bu hakka ilişkin olarak değinilmesi gereken son nokta ise, “unutulma hakkı” ve “silinme hakkının” aynı kavramlar olup olmadığına ilişkin bir tartışma mevcut olduğudur. Bu bağlamda, silinme hakkının yalnızca hukuka aykırı işleme, artık işleme amacı bakımından gereksiz olma gibi belirli durumların varlığı halinde, unutulma hakkının ise böyle bir sınırlama olmaksızın var olduğuna dair görüşler bulunmaktadır<sup>610</sup>.

Bu makalede konuyu GDPR ekseninde ele aldığım için Tüzüğün konuya yaklaşımıyla paralel olarak silinmeyi talep etme hakkı ve unutulma hakkını aynı hak olarak incelemeye aldım. Tüzüğün 17. maddesi bu hakkı düzenlemekte ve hakkı “*silinmeyi talep etme hakkı (unutulma hakkı)*” olarak adlandırmaktadır. Bu nedenle esasen unutulma hakkının silinme hakkından daha kapsamlı ayrı bir hak olduğu yönündeki görüşü benimsemekle birlikte, GDPR eksenli bu makalede de her iki hakkı ifade etmek için silinmeyi talep etme hakkı (unutulma hakkı) isim ve sınıflandırmasını kullandım.

#### **E. İşlemenin Sınırlandırılması Hakkı**

Tüzükte, belirli hallerin varlığı halinde, veri sahiplerinin, veri sorumlularının işletme faaliyetlerini geçici olarak kısıtlama hakları olduğu düzenlenmiştir.<sup>611</sup> Bu bağlamda sınırlamanın talep edilebileceği durumlar aşağıdaki gibidir:

(a) kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi halinde, veri sahibinin kişisel verilerin doğruluğunu teyit etmesini sağlayan bir süre boyunca,

(b) işleme faaliyetinin yasa dışı olması ve veri sahibinin kişisel verilerin silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi,

(c) veri sahibinin işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak veri sahibinin yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması amacıyla söz konusu verilere ihtiyaç duyması,

(d) veri sorumlularının meşru gerekçelerinin veri sahibinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar, veri sahibinin işleme faaliyetine itiraz etmesi.<sup>612</sup>

---

<sup>609</sup> GDPR, m. 17(2).

<sup>610</sup> Unutulma hakkı hakkında ayrıntılı bilgi için bkz. **Christina Markou**, “The Right to Be Forgotten: Ten Reasons Why It Should Be Forgotten”, Law, Governance and Technology Series 20: Reforming Data Protection Law, Springer, 2015, ss. 203-226.

<sup>611</sup> GDPR, m. 18.

<sup>612</sup> GDPR, m. 18(1).

Veri işlemenin sınırlandırılmasının talep edildiği hallerde, bu hak, örneğin; seçilmiş verilerin geçici olarak başka bir işleme sistemine aktararak kullanıcıların bu verilere ulaşmasının engellenmesi, suretiyle kullanılabilir.<sup>613</sup>

Son olarak, veri sorumlusu, bir veri işleme faaliyetine ilişkin kısıtlamanın kaldırılmasından önce veri sahibini bu konuda bilgilendirmelidir.<sup>614</sup>

## **F. Veri Taşınabilirliği Hakkı**

Veri taşınabilirliği hakkı, Tüzük ile birlikte veri sahiplerine tanınan, daha önce hiçbir belgede düzenlenmemiş bir haktır. Bu hak uyarınca, işleme faaliyetinin rızaya veya bir sözleşmeye dayanması veya işleme faaliyetinin otomatik yollarla gerçekleştirilmesi halinde, veri sahibinin kendisi ile ilgili olarak bir veri sorumlusuna sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı vardır.<sup>615</sup> Veri sahiplerinin bu kişisel verileri, verilerin sağlandığı veri sorumlusunun herhangi bir engellemesi olmaksızın başka bir veri sorumlusuna iletme hakkı bulunur.<sup>616</sup>

Veri taşınabilirliği hakkının mevcut olduğu bir durumda, veri sahibinin, teknik açıdan uygulanabilir olması şartıyla, kişisel verilerini doğrudan bir veri sorumlusundan diğerine ilettirme hakkı bulunur.<sup>617</sup> Bu iletimi kolaylaştırmak için veri sorumluları birlikte çalışabilir formatlar geliştirmeli, böylece veri taşınabilirliği hakkının kullanılmasına olanak sağlamalıdır.<sup>618</sup>

Madde 29 Çalışma Grubunun rehberine göre, veri taşınabilirliği hakkı, veri sahibinin seçimini, kontrolünü ve güçlendirilmesini destekler; veri sahibine kendi kişisel verilerini kontrol etme imkânı tanır.<sup>619</sup> Buna göre, veri taşınabilirliği hakkı başlıca şu unsurlardan oluşur:

(a) veri sahiplerinin bir veri sorumlusu tarafından işlenen kendilerine ait kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı,

(b) kişisel verileri bir veri sorumlusundan diğerine, teknik olarak mümkün olması ihtimalinde, herhangi bir engelleme olmaksızın iletme hakkı,

---

<sup>613</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 227.

<sup>614</sup> GDPR, m. 18(3).

<sup>615</sup> GDPR, m. 20(1).

<sup>616</sup> GDPR, m. 20(1).

<sup>617</sup> GDPR, m. 20(2).

<sup>618</sup> GDPR, Gerekeçe 68.

<sup>619</sup> Article 29 Working Party (2016), Guidelines on the right to data portability, WP 242, 13 Aralık 2016, 5 April 2017 (revize), s. 13.

(c) veri sahibinin veri taşıma talebi üzerine, veri sorumlusunun, veri sahibinin talimatları ile hareket etmesi rejimi,

(d) veri taşınabilirliği hakkının kullanılmasının diğer herhangi bir hakkı olumsuz yönde etkilememesi.<sup>620</sup>

## **G. İşlemeye İtiraz Hakkı**

Veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak veya kişisel verilerinin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, söz konusu kişisel verinin işlenmesine itiraz hakkı bulunmaktadır.<sup>621</sup> Bu kapsamda, veri sahibinin veri işlemeye genel bir itiraz hakkı mevcut değildir.

Yukarıdaki ilk durum ile ilgili olarak, veri sahibi, kendi özel durumu ile ilgili gerekçelere dayalı olarak, işlemenin yasal dayanağını kamu yararı için gerçekleştirilen bir görevin ifası amacının veya veri sorumlusunun meşru menfaatlerinin oluşturduğu durumlarda, kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz edebilir.<sup>622</sup> Veri sahibinin özel durumu ile ilgili gerekçelere dayalı olarak itiraz hakkının düzenlenmiş olmasının amacı, veri sahibinin veri koruma hakları ile diğer kişilerin veri işlemedeki meşru menfaatleri arasında bir denge kurulmasıdır.<sup>623</sup> Bu noktada ABAD, veri sahibinin haklarının, kural olarak, veri sorumlusunun ekonomik menfaatlerine üstün geldiğini belirtmiştir.<sup>624</sup> Ayrıca, Tüzükte, veri işlemeye devam edilmesini gerektiren hususların varlığına ilişkin ispat yükünün veri sorumlusunda olduğu açıkça düzenlenmiştir.<sup>625</sup> Veri sorumlusunun işleme faaliyetlerinin devamının gerekliliğini ispatlayamaması durumunda veri işlemeye devam etmesi mümkün değildir.<sup>626</sup>

Ayrıca, kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda ve doğrudan pazarlama ile alakalı olduğu ölçüde, veri sahibinin, kendisi ile ilgili kişisel verilerin söz konusu doğrudan pazarlama amacı ile işlenmesine herhangi bir zamanda ve ücretsiz olarak itiraz etme hakkı bulunur.<sup>627</sup>

---

<sup>620</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 229.

<sup>621</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 229.

<sup>622</sup> GDPR, m. 21(1).

<sup>623</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 230.

<sup>624</sup> Google Spain, para. 81.

<sup>625</sup> GDPR, m. 21(1).

<sup>626</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 231; GDPR, m. 21(1).

<sup>627</sup> GDPR, m. 21(2); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 231.



## H. Yalnızca Otomatik İşleme Faaliyetine Dayalı Bir Karara Tabi Olmama Hakkı

Tüzük uyarınca, veri sahibinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen, profil çıkarma da dahil olmak üzere, yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı bulunur.<sup>628</sup> Ancak, söz konusu işleme:

(i) veri sahibi ve bir veri sorumlusu arasında bir sözleşme yapılması veya uygulanması için gerekli ise veya,

(ii) veri sorumlusunun tabi olduğu ve veri sahibinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtildiği Birlik veya üye devlet hukuku çerçevesinde işlemeye izin verilmiş ise veya,

(iii) veri sahibinin açık rızası mevcut ise,  
bu şartlarda verilen bir karar yalnızca otomatik işlemeye dayalı olsa dahi hukuka aykırılık oluşturmaz.<sup>629</sup>

Madde 29 Çalışma Grubu, yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkının genel bir yasaklama hükmü olduğunu ve veri sahibinin böyle bir karara proaktif olarak itiraz etmesinin aranmadığını belirtmektedir.<sup>630</sup>

Değinilmesi gereken diğer bir nokta ise, yukarıda açıklandığı üzere, veri sahibinin bilgilendirilme hakkı kapsamında veri sorumlusunun ona sağlaması gereken bilgiler arasında profil çıkarma dahil olmak üzere otomatik karar vermenin varlığının da yer aldığıdır.<sup>631</sup> Ayrıca, erişim hakkı çerçevesinde, veri sahibinin, profil çıkarma da dahil olmak üzere otomatik karar vermenin varlığı ve bu hallerde yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları hakkında bilgi talep etme hakkı mevcuttur.<sup>632</sup>

Bu hak uyarınca veri sorumlusu, en azından veri sorumlusu açısından insan müdahalesinin sağlanması hakkı başta olmak üzere, veri sahibinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacı ile uygun tedbirler uygulamalıdır.<sup>633</sup> Daha önce bahsedildiği gibi, kişilerin verilerinin üzerinde kontrol

---

<sup>628</sup> GDPR, m. 22(1).

<sup>629</sup> GDPR, m. 22(2).

<sup>630</sup> Article 29 Working Party, Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679, WP 251, 3 Ekim 2017, s. 15.

<sup>631</sup> GDPR, m. 13(2)(f).

<sup>632</sup> GDPR, m.15(1)(h).

<sup>633</sup> GDPR, m. 22(3).

sağlayabilmeleri oldukça önemli ve Tüzük tarafından da dikkate alınmış bir husustur. Bu nedenle, karar mekanizmalarına insan müdahalesinin dahil olması, aksi durumda ortaya çıkabilecek olumsuz sonuçların önlenmesi açısından önem arz etmektedir.<sup>634</sup>

## II. Kısıtlamalar

Veri sorumlusu veya işleyen tabi olduğu Birlik veya Üye Devlet hukuku bir yasama tedbiri vasıtasıyla; temel haklar ve özgürlüklerin özüne saygı gösterilmesi ve demokratik bir toplumda aşağıdaki belirtilmiş hususların güvence altına alınması açısından gerekli ve orantılı bir tedbir teşkil etmesi durumunda öngörülen haklar ve yükümlülüklerin kapsamını kısıtlayabilir:

- (a) milli güvenlik,
- (b) savunma,
- (c) kamu güvenliği,
- (d) 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 edilmesi,
- (e) başta Birliğin veya bir Üye Devletin önemli bir ekonomik veya mali çıkarına olmak üzere parasal hususlar ile bütçe ve vergilendirmeye ilişkin hususlar, halk sağlığı ve sosyal güvenlik de dahil, Birlik ya da bir üye devletin genel kamu yararına yönelik diğer önemli hedefler,
- (f) yargı bağımsızlığının ve adli süreçlerin korunması,
- (g) düzenlenmiş mesleklere ilişkin etik kurallarının ihlalinin önlenmesi, soruşturulması, tespiti ve kovuşturulması,
- (h) nadiren olsa dahi, (a) ila (e) ve (g) bentlerinde belirtilen durumlarda resmi yetkinin kullanımı ile bağlantılı bir izleme, denetleme veya düzenleme işlevi,
- (i) veri sahibinin veya başkalarının haklarının ve özgürlüklerinin korunması,
- (j) medeni hukuktan kaynaklanan taleplere ilişkin kararların icrası.<sup>635</sup>

Kısıtlamalarla ilgili olarak getirilen yasama tedbirinde, ilgili işlemenin veya işleme kategorilerinin amaçları, kişisel veri kategorileri, getirilen kısıtlamaların kapsamı, kötüye kullanım veya yasa dışı yollarla erişim veya aktarımın engellenmesine yönelik güvenceler, veri sorumlusu veya veri sorumlusu kategorilerinin belirlenmesi, işleme veya işleme kategorilerinin mahiyeti, kapsamı ve amaçları dikkate alınarak saklama süreleri ve uygulanabilir güvenceler, veri

---

<sup>634</sup> Giakoumopoulos/Buttarelli/O'Flaherty, s. 235.

<sup>635</sup> GDPR, m. 23(1).

sahiplerinin hakları ve özgürlüklerine yönelik riskler ve kısıtlama amacına hanel getirmemesi durumunda, veri sahiplerinin kısıtlamayla ilgili bilgi sahibi olma hakkı belirtilmelidir.<sup>636</sup>

### III. Kanun Yolları, Sorumluluk, Cezalar ve Tazminat

#### A. Denetim Makamına Şikâyette Bulunma Hakkı

Her veri sahibi, kendisi ile alakalı kişisel verilerin işlenmesinin hukuka aykırı olarak gerçekleştiğini düşünmesi durumunda, başka bir idari veya adli çözüm yoluna hanel gelmeksizin, yetkili denetim makamına şikâyette bulunma hakkına sahiptir.<sup>637</sup> Bu hak kapsamında, yetkili denetim makamı bir veri sahibi veya bir organ, kuruluş ya da bir birlik tarafından yapılan şikâyetleri ele almalı ve şikâyetin konusunu, uygun olduğu ölçüde, soruşturmalı ve özellikle daha ayrıntılı soruşturma ya da başka bir denetim makamı ile koordinasyonun gerekmesi durumunda, şikâyet sahibini soruşturmanın ilerlemesi ve sonucu konusunda makul bir süre içerisinde bilgilendirmelidir.<sup>638</sup> Tüzükte ayrıca denetim makamlarının bazı tedbirler olarak şikâyetlerin sunulmasını kolaylaştırması gerektiği öngörülmüştür.<sup>639</sup>

Denetim makamı şikâyete ilişkin bir karar verdiğinde, her gerçek veya tüzel kişinin bu denetim makamının kendileriyle ilgili yasal *bağlayıcılığı* olan kararlarına karşı etkili bir kanun yoluna başvurma hakkı vardır.<sup>640</sup> Bu hak veri sahipleri için söz mevcut olduğu gibi, veri sorumluları ve işleyenler için de uygulama alanı bulur.<sup>641</sup>

#### B. Etkili Bir Kanun Yoluna Başvurma Hakkı

##### 1. Genel Olarak

Etkili bir kanun yoluna başvurma hakkı hem AİHS hem AB Şartı altında temel haklardan biri olarak kabul edilmiş ve bu hakka büyük önem atfedilmiştir. Örneğin, *Schrems* davasında, ABAD, veri sahiplerinin kişisel verilerine erişimleri, kişisel verilerini düzeltmeleri veya silmeleri için herhangi bir kanun yolu öngörmeyen bir yasal düzenlemenin, AB Şartının 47. maddesinde düzenlenen “*etkili hukuki bir yola başvurma*” temel hakkının özünü zedeleyeceğine karar vermiştir.<sup>642</sup>

Yukarıda bahsedildiği üzere, denetim makamlarının *bağlayıcı* kararlarına karşı ilgili kişilerin kanun yoluna başvurma hakkı mevcuttur. Burada dikkat edilmesi gereken nokta, bu hakkın

---

<sup>636</sup> GDPR, m. 23(2).

<sup>637</sup> GDPR, m. 77(1).

<sup>638</sup> GDPR, m. 57(1)(f).

<sup>639</sup> GDPR, m. 57(2).

<sup>640</sup> GDPR, m. 78(1).

<sup>641</sup> *Giakoumopoulos/Buttarelli/O’Flaherty*, s. 238.

<sup>642</sup> ABAD, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* [GC], 6 Ekim 2015.

denetim makamının yalnızca “bağlayıcı” kararlarına karşı doğmasıdır.<sup>643</sup> Denetim makamının görüş bildirme gibi bağlayıcı olmayan kararlarına karşı ilgililer kanun yoluna başvuramayacaklardır.<sup>644</sup>

Tüzük uyarınca, kişisel verilerinin Tüzük’e aykırı bir şekilde işlenmesi sonucu bu Tüzük kapsamındaki haklarının ihlal edildiğini değerlendirdiği hallerde, her veri sahibi etkili bir kanun yoluna başvurma hakkına sahiptir.<sup>645</sup> Mevzubahis kanun yolunun “etkili” olabilmesi için veri sahiplerinin ilgili davayı açabilecekleri yetkili mahkemeler oldukça önem taşımaktadır; çünkü, veri sorumlusu veya veri sahiplerine dava açılacak mahkemelerin sınırlanması, veri sahiplerinin çeşitli zorluklarla karşılaşmasına sebebiyet verebilecektir.<sup>646</sup> Bu doğrultuda, Tüzükte bu davaların veri sorumlusu veya işleyen bir işletmesinin ya da veri sahibinin mutlak meskeninin bulunduğu üye devletin mahkemelerinde açılacağı düzenlenmiştir.<sup>647</sup> Veri sahibi veya işleyen, bir üye devletin kamu yetkilerinin kullanımı ile ilgili olarak hareket eden bir kamu kuruluşu olması halinde ise dava açılacak mahkemelere sınır getirilmiş ve bu kişilere ilişkin davaların söz konusu kuruluşun bulunduğu üye devletin mahkemelerinde açılacağı düzenlenmiştir.<sup>648</sup>

Ayrıca, (i) bir veri sahibi, veri sorumlusu, veri işleyen veya denetim makamının direkt ve bireysel olarak kendilerini ilgilendiren Avrupa Veri Koruma Kurulunun bir kararını iptal etmek amacıyla veya (ii) bir veri sahibinin herhangi bir AB kuruluş ve organın veri koruma hukukunu ihlal ettiği iddiasına dayanarak ABAD’a başvurma hakkı vardır. İkinci halde bu başvuru, ABAD’ın ilk derece mahkemesi olan AB Genel Mahkemesine (The General Court, EGC) yapılacaktır.<sup>649</sup>

## **2. Kar Amacı Gütmeyen Bir Organ, Kuruluş veya Birlik Tarafından Temsil Edilme Hakkı**

Tüzüğün 80. maddesi uyarınca; veri sahiplerinin, bir Üye Devlet hukuku uyarınca düzgün şekilde kurulmuş, kamu yararına yasal hedefleri bulunan ve veri sahiplerinin kişisel verilerinin korunmasına ilişkin hakları ve özgürlüklerinin korunması alanında aktif olan kar amacı gütmeyen bir organ, kuruluş veya birliğe, şikâyeti onun adına yapması, 77, 78 ve 79. maddelerde atıfta bulunulan hakları onun adına kullanması ve Üye Devlet hukukunda sağlanması koşuluyla, onun adına tazminat alma hakkını kullanma yetkisi verme hakkı bulunur.<sup>650</sup> Söz konusu organ, kuruluş,

---

<sup>643</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 239.

<sup>644</sup> GDPR, Gerekeçe 143.

<sup>645</sup> GDPR, m. 79(1).

<sup>646</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 240.

<sup>647</sup> GDPR, m. 79(2).

<sup>648</sup> GDPR, m. 79(2).

<sup>649</sup> **Giakoumopoulos/Buttarelli/O’Flaherty**, s. 240.

<sup>650</sup> GDPR, m. 80(1).

veya birlik tarafından temsil edilme hakkı, bireylerin, onların uzmanlığından ve organizasyonel ve finansal kapasitelerinden faydalanmasına, dolayısıyla haklarını efektif olarak kullanılabilmesine olanak sağlar.<sup>651</sup>

### C. Sorumluluk ve Tazminat

Etkili bir kanun yoluna başvurma hakkı, kişisel verileri hukuka aykırı olarak işlenen bireylerin böyle bir işleme sonucunda uğradıkları zararlar için tazminat talep edebilme hakkını içinde barındırır.<sup>652</sup> Tüzükte, Tüzüğe ilişkin bir ihlal sonucu *maddi veya manevi* zarar gören herhangi bir kişinin, yaşanan zarara ilişkin olarak veri sorumlusu veya işleyenden tazminat alma hakkına sahip olduğu açıkça düzenlenmiştir.<sup>653</sup> Bu maddedeki “zarar” kavramı, ABAD’ın içtihatları ışığında ve Tüzüğün amaçlarına uygun olarak geniş yorumlanmalıdır.<sup>654</sup>

Tüzük uyarınca, işleme faaliyetine müdahil herhangi bir veri sahibi Tüzüğü ihlal eden işleme faaliyetinin sebep olduğu zarardan sorumludur.<sup>655</sup> Bir veri işleyen ise ancak Tüzüğün özellikle veri işleyenlerine yönelik yükümlülüklerine uyum göstermediği veya veri sorumlusunun hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hallerde, işleme faaliyetinin sebep olduğu zarardan sorumludur.<sup>656</sup>

Birden fazla veri sorumlusu veya işleyenin ya da hem bir veri sorumlusu hem de bir veri işleyenin aynı işleme faaliyetinde bulunduğu ve işleme faaliyetinin sebep olduğu herhangi bir zarardan sorumlu olduğu hallerde, veri sahibinin etkili bir şekilde tazminin sağlanması amacıyla, her veri sorumlusu veya işleyenin tüm zarardan sorumlu tutulacağı Tüzükte düzenlenmiştir.<sup>657</sup> Fakat, böyle bir durumda, tek bir veri sorumlusu veya işleyen zararın tamamını tazmin ederse, bu veri sorumlusu ve işleyen aynı işleme faaliyetine müdahil diğer veri sorumlusu veya işleyenlerden zarardan sorumlu oldukları kısma tekabül eden tazminat kısmını isteyebilecektir.<sup>658</sup> Böyle bir düzenleme getirilmesinin nedeni tazminatın, uğranılan zarara ilişkin olarak “tam ve eksiksiz” olarak sağlanması oldukça önem teşkil eden bir husus olmasıdır.<sup>659</sup>

---

<sup>651</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 245.

<sup>652</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 246.

<sup>653</sup> GDPR, m. 82(1).

<sup>654</sup> GDPR, Gereğe 146.

<sup>655</sup> GDPR, m. 82(2).

<sup>656</sup> GDPR, m. 82(2).

<sup>657</sup> GDPR, m. 82(4).

<sup>658</sup> GDPR, m. 82(5).

<sup>659</sup> Giakoumopoulos/Buttarelli/O’Flaherty, s. 246.

Tüzükte ayrıca zarara sebep olan olaydan hiçbir şekilde sorumlu olmadığını kanıtlaması halinde, bir veri sorumlusu veya işleyenin bu sorumluluktan muaf tutulabileceği düzenlenmiştir.<sup>660</sup>

#### **D. Cezalar**

Tüzük, Üye Devletlerin denetim makamlarını Tüzüğün ihlal edilmesi halinde idari cezalar uygulamaları hususunda yetkilendirmiştir. Tüzük ile getirilen idari para cezalarına konu olabilme, yeni ve oldukça önemli bir düzenlemedir. Cezaların seviyeleri, yerel makamların ceza verip vermeme noktasında dikkat etmesi gereken durumlar, uygulanabilecek en yüksek ceza gibi konular Tüzükte açıkça düzenlenmiş olup, böylece AB içerisinde cezalara ilişkin olarak yeknesak bir sistem oluşturulması amaçlanmıştır.<sup>661</sup>

Tüzüğün getirdiği düzenlemeye göre; veri işlemenin temel ilkeleri ve rızanın koşullarına aykırılık, veri sahiplerinin haklarının ihlali ve Tüzüğün yurt dışına veri aktarımına ilişkin kurallarına uyulmaması durumunda, denetim makamları 20.000.000 Euro'ya kadar veya veri sorumlusu veya işleyenin bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %4'üne kadar idari para cezası (hangi meblağ yüksek ise o geçerli olmak üzere) kesme yetkisi vardır.<sup>662</sup> Diğer ihlaller ile ilgili olarak ise denetim makamı 10.000.000 Euro'ya kadar veya veri sorumlusu veya işleyenin bir teşebbüs olması halinde, bir önceki mali yılın yıllık dünya çapındaki cirosunun %2'sine kadar idari para cezası (hangi meblağ yüksek ise o geçerlidir) kesebilecektir.<sup>663</sup>

Her münferit durumda, denetim makamı, bir idari para cezası kesilip kesilmeyeceğine ve idari para cezasının miktarına karar verirken, aşağıdaki hususları dikkate alır:

(a) ihlalin mahiyeti, ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyi,

(b) ihlalin kasıtlı olması veya ihmalkârlıktan kaynaklanması,

(c) veri sahiplerinin yaşadığı zararın azaltılması için veri sorumlusu veya işleyen tarafından gerçekleştirilen herhangi bir işlem olup olmadığı,

(d) kendileri tarafından uygulanan teknik ve düzenlemeye ilişkin tedbirler dikkate alındığında, veri sorumlusu veya işleyenin sorumluluk derecesi,

(e) veri sorumlusu veya işleyenin geçmişte konuyla ilgili ihlalleri,

---

<sup>660</sup> GDPR, m. 82(3).

<sup>661</sup> **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 247.

<sup>662</sup> GDPR, m. 83(5); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 248.

<sup>663</sup> GDPR, m. 83(4); **Giakoumopoulos/Buttarelli/O'Flaherty**, s. 248.

(f) ihlalin düzeltilmesi ve ihlalin olası olumsuz etkilerinin azaltılması amacı ile denetim makamı ile gerçekleştirilen işbirliği derecesi,

(g) ihlalden etkilenen kişisel veri kategorileri,

(h) veri sorumlusu veya işleyenin ihlali bildirip bildirmediği ve bildirdiyse ne ölçüde bildirdiği başta olmak üzere, denetim makamının ihlalden haberdar edilme şekli,

(i) aynı konu ile ilgili olarak daha önceden veri sorumlusu veya işleyene ilişkin alınmış tedbirlere uyum,

(j) onaylı davranış kurallarına veya onaylı belgelendirme mekanizmalarına uygun hareket edilip edilmemesi,

(k) ihlal nedeniyle doğrudan veya dolaylı olarak elde edilen maddi menfaatler veya kaçınılan zararlar gibi durumun özellikleri açısından geçerli diğer ağırlaştırıcı veya hafifletici faktörler.<sup>664</sup>

Ayrıca, denetim makamlarının idari para cezası kesme yetkileri dışında, çeşitli “düzeltici” yetkileri mevcuttur.<sup>665</sup> Örneğin; denetim makamları ihtarda bulunabilir, kınama cezası verebilir, bir işleme yasağı da dahil olmak üzere geçici veya kati bir sınırlama getirebilir.

Diğer bir önemli nokta ise, Tüzükte, Üye Devletler’in Tüzüğe ilişkin ihlaller açısından geçerli olan diğer cezalara ilişkin kurallar belirleyebileceği belirtilmiştir.<sup>666</sup> Buna göre, Üye Devletler, Tüzüğün ve Tüzük gereğince kabul edilen yerel düzenlemelerin ihlal edildiği durumlar için ceza verilmesine ilişkin kurallar düzenleyebilir.<sup>667</sup> Bu noktada dikkat edilmesi gereken, yerel hukuklarda getirilen düzenlemelerin aynı suçtan dolayı iki kere yargılama yapılamayacağı prensibini (*ne bis in idem*) ihlal etmemesi gerektiğidir.<sup>668</sup> Örneğin; Almanya’nın Federal Veri Koruma Yasasında (Bundesdatenschutzgesetz), bazı veri koruma kurallarının kasıtlı ihlalinin bir suç teşkil ettiğini düzenlenmiştir.<sup>669</sup> Örnek vermek gerekirse, çok sayıda veri sahibinin kamuya açık olmayan kişisel verilerinin hukuka aykırı olarak aktarılması durumunda para veya üç yıla kadar hapis cezası öngörülmüştür.

#### **e. Güçlü İhlal Uygulamaları (Stronger Enforcement of Infringements)**

---

<sup>664</sup> GDPR, m. 83(2).

<sup>665</sup> GDPR, m. 58.

<sup>666</sup> GDPR, m. 84(1).

<sup>667</sup> GDPR, Gereğe 149.

<sup>668</sup> GDPR, Gereğe 149.

<sup>669</sup> Bundesdatenschutzgesetz, m. 42.

GDPR ile getirilen en önemli yeniliklerden bir tanesi de sorumluluğun kapsamının genişletilmesi ile birlikte verilebilecek para cezalarının da dikkate değer şekilde artırılmış olmasıdır. GDPR düzenlemelerini ihlal eden şirketler yıllık 20 milyon Avro veya ihlalde bulunan şirketin bir önceki mali yılı, yıllık dünya çapındaki cirosunun % 4'üne kadar idari para cezasına tabi olma riski bulunmaktadır (GDPR, m. 83/5). Bu müeyyide hem veri sorumlusu hem veri işleyen şirketlere karşı uygulanabilecektir. Bir veri sorumlusu veya veri işleyenin aynı veya bağlantılı işleme faaliyetlerine yönelik olarak GDPR hükümlerini kasıtlı (intentionally) veya ihmalkârlıkla (negligently) ihlal etmesi durumunda, toplam idari para cezası meblağı en ağır ihlal için belirtilen 20 milyon Avro'yu aşamayacaktır (GDPR, m. 83/3 ve 83/5).

İdari para cezası kesilmesine karar verilirken ve para cezasının miktarı belirlenirken şu hususlar dikkate alınacaktır:

- i. İlgili işleme faaliyetinin niteliği, kapsamı, amacı dikkate alındığında ihlalin niteliği, ciddiyeti ve süresinin yanı sıra etkilenen veri sahibi sayısı ve veri sahiplerinin yaşadığı zarar düzeyi,
- ii. İhlalin kasıt veya ihmâl ile işlenmesi durumu,
- iii. Veri sahiplerinin zararının azaltılması için veri sorumlusu veya işleyen tarafından gerçekleştirilen işlemler,
- iv. GDPR 25 ve 32. maddeleri uyarınca uygulanan teknik ve organizasyona ilişkin tedbirler göz önünde bulundurulmak suretiyle, veri sorumlusu veya işleyenin sorumluluk derecesi,
- v. Veri sorumlusu veya işleyenin geçmişte konuyla ilgili diğer ihlal durumları,
- vi. İhlalin düzeltilmesi ve ihlalin olası olumsuz etkilerinin azaltılması amacı ile denetim makamı ile gerçekleştirilen iş birliği derecesi,
- vii. İhlalden etkilenen kişisel veri kategorileri,
- viii. Veri sorumlusu veya işleyenin ihlali bildirim bildirmedeği, denetim makamının ihlalden haberdar edilme şekli,
- ix. GDPR 58/2 maddesine uygun alınan diğer tedbirlere uyum durumu,
- x. İhlal nedeniyle doğrudan veya dolaylı olarak elde edilen maddi menfaatler veya kaçınılan zararlar gibi halin icabına göre geçerli diğer ağırlaştırıcı ve hafifletici nedenler,
- xi. Veri sorumlusu / işleyenin GDPR 40 ve 42. maddelerinde düzenlenen onaylı belgelendirme mekanizmalarına uygun hareket edip etmedikleri.

Her denetim makamı, 83. maddede sayılan idari para cezaları verilmesinin, her münferit durumda etkin (effective), orantılı (proportionate) ve caydırıcı (dissuasive) olmasını sağlamakla yükümlü tutulmuştur (GDPR, m. 83/1).



GDPR ile şirketlerin durumunu ağırlaştıran bir diğer husus da, veri sorumlusu şirket/işleyenlerin veri işlemenin rızaya dayandığı hallerde, rızanın varlığını ispat ile yükümlü tutulmalarıdır (GDPR, m. 7/1, rec. 42). Veri sorumlusu ayrıca GDPR'nın 5/1. maddesinde düzenlenen ilkelere uygun davrandığını ortaya koymakla yükümlü tutulmuştur (GDPR, m. 5/2, rec. 24). Bu hususların da GDPR ile getirilen güçlü ihlal araçlarını tamamlayıcı nitelikte olduğu söylenebilir.

GDPR ihlalden dolayı ilk para cezaları da verilmeye başlamıştır. Avusturya'da bir bahis şirketi, güvenlik nedeniyle koyduğu kameranın görüş açısının geniş olması ve GDPR kapsamında korunan kamuyu görüntülemesi nedeni ile 4800 Euro; Portekiz'de bir hastane kendi çalışanı olmadığı halde 985 fizik tedavi doktoruna ait aktif bilgileri barındırması nedeni ile bilgi güvenilirliği, bütünlüğü ve asgari düzeyde veri işleme ilkelerine aykırı davranmak nedeni ile iki kez 150.000 Euro ve bir kez 100.000 Euro para cezası ile cezalandırılmıştır. Son olarak Almanya'da Knuddels.de sosyal ağ şirketi, 1.8 milyon kayıtlı kullanıcılarına ait e-posta ile kullanıcı adı ve şifrelerinin sızdırılması nedeni ile 20.000 Euro para cezası ile cezalandırılmıştır.<sup>670</sup>

## § 6. Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Uygulanması

Yukarıda detaylıca açıklandığı üzere, Tüzüğü oldukça geniş bir uygulama alanı vardır ve Tüzük oldukça geniş ve ayrıntılı haklar tanımış ve sorumluluklar yüklemiştir. Tüzüğü kurduğu bu sistemin uygulamadaki yansımalarının etkili olarak gerçekleştirilmesi büyük önem taşımaktadır.

Bu bağlamda, Tüzüğü getirdiği düzenlemelerin uygulamaya konması için dört aşamalı bir yaklaşım izlenmesinin faydalı bir hareket biçimi olacağı düşünülmektedir. Bu dört aşama:

- (1) boşluk analizi,
- (2) risk analizi,
- (3) proje idaresi ve kaynak/bütçe planlaması ve
- (4) uygulamaya koymadır.<sup>671</sup>

Bu yaklaşım kısmen, uygulamaya koyma aşamalarını zaman ve kapsamlarına göre sınırlanmış farklı aşamalara ayıran Şelale Modelini (Waterfall Model) temel almaktadır.<sup>672</sup> Bir

---

<sup>670</sup> How much are the first fines for GDPR infringement, December 12, 2018, <https://www.pandasecurity.com/mediacenter/news/first-sanctions-gdpr-infractions/> (Son Erişim Tarihi: 15.03.2019)

<sup>671</sup> Voigt/von dem Bussche, s. 245.

<sup>672</sup> Voigt/von dem Bussche, s. 246.

işleme faaliyetinin çeşitli Üye Devletleri etkilemesi halinde ise, veri koruma sistemini yerel özelliklere uyarlamak amacıyla, beşinci bir aşama gerekli olabilecektir.<sup>673</sup>

### **I. Birinci Adım: Boşluk Analizi**

İlk adım olarak, ilgili kuruluş, kendisinin hali hazırda mevcut olan veri koruma standartlarını analiz etmeli ve bunları Tüzük kapsamında gerekli yükümlülükleri karşılamak için gerekenlerle karşılaştırmalıdır. Bunun için, bu kuruluşun farklı departmanlardaki veri işlemeden sorumlu kişiler değerlendirme aşamasına dahil edilmelidir. Mevzubahis analiz çalıştay, karşılıklı görüşme ve öz değerlendirme gibi farklı şekillerde gerçekleştirilebilir; bu noktada önemli olan ise ne tür işleme faaliyetlerinin hangi amaçlarla gerçekleştirildiği, hangi tür verilerin işlendiği, kuruluş içindeki sorumluluklarının nasıl dağıldığı ve ne gibi güvenceler alındığı konularının üzerinde durulmasıdır.<sup>674</sup>

Boşluk analizi yapılırken, ilgili kuruluşun spesifik olarak gerçekleştirdiği veri işleme faaliyetleri ve bu tür işlemler için Tüzük tarafından getirilen yükümlülükler dikkate alınmalıdır. Bu aşamanın tamamlanması için, kuruluş, kendi veri koruma standartları ile olması gerekenleri kıyaslayacak ve veri korumasına ilişkin boşlukları tespit edecektir.<sup>675</sup> Bu boşluk, diğer aşamalarda giderilmeye çalışılacaktır.

### **II. İkinci Adım: Risk Analizi**

Yukarıda pek çok defa bahsedildiği üzere, veri işleme faaliyetinin veri sahiplerinin hak ve özgürlükleri açısından taşıdığı risk miktarı, sorumlulukların belirlenmesi açısından üzerinde oldukça durulmuş bir değişkendir. Bu bağlamda, kuruluşlar farklı departmanları incelemeli ve bu departmanlardaki veri işleme faaliyetlerinin risk dereceleri ortaya konulmalıdır. Bu noktada, özellikle, veri sahiplerinin hakları ve özgürlükleri açısından en çok risk barındıran ve yüksek miktarda cezalara sebebiyet verme ihtimali en yüksek olan veri işleme faaliyetleri üzerinde durulmalıdır.<sup>676</sup>

Bu aşamanın tamamlanması için, ilgili kuruluş, kendisinin çeşitli işleme faaliyetlerinin taşıdığı riskleri de dikkate alarak, tespit edilmiş veri koruma boşluğu doğrultusunda yeni veri koruma standartlarının uygulamaya konulması amacıyla bir stratejik proje taslağı hazırlamalıdır.<sup>677</sup>

---

<sup>673</sup> Voigt/von dem Bussche, s. 246.

<sup>674</sup> Voigt/von dem Bussche, s. 246.

<sup>675</sup> Voigt/von dem Bussche, s. 246.

<sup>676</sup> Voigt/von dem Bussche, s. 247.

<sup>677</sup> Voigt/von dem Bussche, s. 247.

### III. Üçüncü Adım: Proje İdaresi ve Kaynak/Bütçe Planlaması

Söz konusu proje planı üzerinden, Tüzüğün hükümlerinin uygulanmaya konulması amacıyla kuruluş genelinde bir veri koruma organizasyonu oluşturmalıdır. Bu çerçevede, mevzubahis organizasyon, yeniden yapılanma için gerekli bütçe ve kaynakları, yasal masraflar, BT masrafları ve çalışan ihtiyacı da dahil olmak üzere dikkate almalıdır. Bu noktada hali hazırda bir veri koruma görevlisinin var olması oldukça yarar sağlayabilecektir.<sup>678</sup>

Kuruluş, en çok etkilenen alanlardaki kilit mevkideki personellere projeye ilişkin sorumluluklar tahsis etmelidir. Uygun olduğunda, AB görevlileri tarafından bir “baş” proje müdürü atanacaktır. Baş proje müdürü, veri koruma hakkında uzman bilgisine sahip bağımsız bir danışman olabilir.<sup>679</sup>

Bu aşamanın tamamlanması için, veri koruma kavramı kesinlik kazanmalıdır.<sup>680</sup>

### IV. Dördüncü Adım: Uygulamaya Koyma

Son aşamada, Tüzük ile uyum içerisindeki yeni veri koruma standartları, bir önceki aşamada kesinlik kazandırılan veri koruma kavramı uyarınca uygulamaya konulacaktır. Kuruluşun yönetimi, farklı departmanların işleme faaliyetlerinin yeni standartlara uygunluğunun sağlanması noktasında proje müdürlerine yardım edeceklerdir.<sup>681</sup> Kuruluş bünyesinde farkındalık yaratılması ve çalışanların veri işleme faaliyetlerini hukuka uygun olarak gerçekleştirmeleri hususunda eğitilmeleri için çalıştay organize edilmesi faydalı bir yöntem olarak görülmektedir.<sup>682</sup>

Bu aşamanın tamamlanması için, yeni veri işleme standartları başarılı bir şekilde uygulamaya konulmuş ve kuruluşun olağan işleyişinin bir parçası haline gelmiş olmalıdır.<sup>683</sup> Tüzük ile uyumluluğun sağlanabilmesi için bu aşamadan sonra da veri işleme faaliyetleri sürekli olarak izlenmeli ve bu standartlar devam ettirilmelidir.<sup>684</sup>

### V. Beşinci Adım: Ek Ulusal Gereklilikler

Tüzük, veri korumasına ilişkin kuralların belirlenmesi noktasında devletlere önemli ölçüde takdir marjı bırakmaktadır. Dolayısıyla, Üye Devletler, ek veri koruma gereklilikleri düzenleyebileceklerdir.<sup>685</sup> Bu noktada, birden çok AB Üyesi Devlette veri işleme faaliyeti

---

<sup>678</sup> Voigt/von dem Bussche, s. 247.

<sup>679</sup> Voigt/von dem Bussche, s. 247.

<sup>680</sup> Voigt/von dem Bussche, s. 247.

<sup>681</sup> Voigt/von dem Bussche, s. 247.

<sup>682</sup> Voigt/von dem Bussche, s. 247.

<sup>683</sup> Voigt/von dem Bussche, s. 248.

<sup>684</sup> Voigt/von dem Bussche, s. 248.

<sup>685</sup> Voigt/von dem Bussche, s. 249.

gerçekleştiren veya birden çok AB Üyesi Devleti etkileyen kuruluşlar, farklı ulusal mevzuatlardan etkilenip etkilenmeyeceklerini tespit etmelidir.<sup>686</sup>

## SONUÇ

GDPR, AB veri koruma rejiminin elden geçirilmesi ve modernleştirilmesidir. Bireyler açısından yeni koruma ve güvence mekanizmaları getiren bu yeni araç, her gün sayısız veri işleyen, depolayan ve kullanıcılara sunan şirketler açısından ise yeni yükümlülükler getirmektedir. Üstelik GDPR'ın genişleyen uygulama alanı nedeniyle sadece AB'de yerleşik şirketler değil, AB dışındaki şirketler açısından da bu yeni duruma uyum sağlamak zorunlu bir hâl almıştır.

Makalenin I. Bölüm'ünde "kişisel verilerin korunması hakkı"nın gelişimi, uluslararası düzenlemelerde nasıl yer aldığı incelenerek değerlendirilmeye çalışılmıştır. Bu çerçevede, bu hakkın yeni bir hak olmadığı fakat münhasır bir hak olarak anlaşılması ve düzenlenmesinin teknolojik gelişmeler ve dijital çağın gerekleri ile birlikte ortaya çıktığını söylemek mümkündür. Kişisel verilerin korunması ile ilgili en güncel ve en detaylı düzenleme 25 Mayıs 2018'de yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğüdür. Bu Tüzük ile kişisel verilerin korunması hukukunun AB'de yeknesaklaştırılması amaçlanmış olup, Tüzük makalenin II. Bölüm'ünde detaylıca incelenmiştir.

Bu makalenin II. Bölüm'ünde 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü kişisel verilerin korumasına ilişkin kavramların tanımı, Tüzüğün uygulama alanı, getirdiği yenilikler, yer verdiği ilkeler, getirdiği güvenceler, yüklediği sorumluluklar, kurduğu sistem ve bu sistemin nasıl uygulamaya konulabileceği detaylıca ve bir bütün olarak incelenmiştir. İlk bakışta Tüzüğün genelinde fark edilebilen ve onu önceki düzenlemelerden ayıran en önemli farklılık, Tüzüğün AB'de kişisel verilerin korunması hukukunun yeknesaklaştırılması amacıyla oldukça ayrıntılı ve etkili bir sistem kurma çabasıdır.

Tüzük, bu hedeften yola çıkarak hem tamamen yeni düzenlemelere yer vermiş, hem de daha önceden var olan düzenlemeleri daha somut ve detaylı olarak düzenlemiştir. Bu doğrultuda öncelikle Tüzüğün bölgesel kapsamı artırılmış ve belirli hallerde Tüzüğün AB dışındaki ülkelere de uygulanabilir olduğu öngörülmüştür. Kapsamın artırılmasının yanı sıra, genel olarak hukuki bir işleme faaliyetinden bahsedebilmek için gereken şartlar ağırlaştırılmış ve veri sahiplerine yeni haklar tanınmış ve veri sahiplerinin önceden mevcut hakları genişletilmiştir. Bu doğrultuda Tüzük ile birlikte "unutulma hakkı" ve "veri taşınabilirliği hakkı" ilk kez yasal bir zeminde

---

<sup>686</sup> Voigt/von dem Bussche, s. 249.

düzenlenmiştir. Ayrıca genel itibariyle veri sorumluları ve işleyenlerin yükümlülükleri arttırılmış ve somutlaştırılmıştır. Bu kapsamda, belirli durumlarda, veri sorumlularının veri koruma kurallarına uygun faaliyet göstermesi hususunda onlara bilgi ve tavsiye verecek veri koruma görevlileri atanması gerekliliği ilk kez açık olarak düzenlenmiştir. İlâveten, kişisel verileri ihlalinin ortaya çıkması durumunda veri sorumlularına ve veri işleyenlere bu ihlali denetim makamı ve ilgililere bildirme yükümlülüğünün öngörölmüş olması Tüzük ile getirilen önemli bir yeniliktir. Son olarak değinilmesi gereken başka bir yenilik ise, Üye Devletlerin denetim makamlarının Tüzüğün ihlal edilmesi halinde idari cezalar uygulamaları hususunda yetkilendirilmiş olmasıdır. Bu noktada ihlal halinde kesilebilecek cezaların oldukça yüksek düzenlenmiş olması da dikkat çeken bir noktadır.

GDPR'ın 83. maddesiyle benimsenen ağır idari para cezaları da dikkate alındığında, tüm veri işleyenlerin, özellikle şirketlerin GDPR uyumluluğunun sağlanmasının önemi daha açık şekilde ortaya çıkmaktadır.

Sonuç olarak, Tüzük, genel anlamıyla, AB'de yeknesak bir kişisel verilerin korunması hukuku oluşturmak amacıyla, var olanlara kıyasla daha kapsamlı ve detaylı bir sistem kurmuş, hükümlere aykırılıklar içinse oldukça ağır cezalar öngörmüştür. Anlatılan amaçlar düşünöldüğünde, 96/46/EC sayılı Direktif'ten temel alınarak tasarlanmış ve Tüzüğün onaylanmasından kısa bir süre önce yürürlüğe girmiş 6698 sayılı KVKK'nın, Tüzük baz alınarak geliştirilmesi oldukça faydalı olacaktır.

## KAYNAKÇA

- Albrecht**, Jan Philipp, “How The GDPR Will Change The World”, Eur. Data Prot. L. Rev. 287, 2016.
- Bhatia**, Punit, Contents of Data Protection Policy according to GDPR, <https://advisera.com/eugdpracademy/knowledgebase/contents-of-the-data-protection-policy-according-to-gdpr/> (Son Erişim Tarihi: 18.03.2019).
- de Hert**, Paul/Michal Czerniawski, “Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context”, International Data Privacy Law, V. 6, No. 3, 2016.
- Develioğlu**, Hüseyin Murat, 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul, 2017.
- Dülger**, Murat Volkan, Kişisel Verilerin Korunması Hukuku, Hukuk Akademisi, İstanbul, 2019.
- Elliman**, Dave, GDPR: It is time to rethink your approach to privacy, August 11, 2017, <https://www.thoughtworks.com/insights/blog/gdpr-it-s-time-rethink-your-approach-privacy>
- Fernandes**, Mário /Alberto Rodrigues da Silva/António Gonçalves, “Specification of Personal Data Protection Requirements: Analysis of Legal Requirements based on the GDPR Regulation”, [https://www.researchgate.net/profile/Mario\\_Fernandes14/publication/](https://www.researchgate.net/profile/Mario_Fernandes14/publication/) (Son erişim tarihi: 19.07.2019).
- Fritz**, Gernot/Nadja Paulus, “CJEU rules on joint controllership – what does this mean for companies?”, Freshfields Bruckhaus Deringer LLP, <https://digital.freshfields.com/post/102f0aw/cjeu-rules-on-joint-controllership-what-does-this-mean-for-companies>, (Son erişim: 19.07.2019).
- Giakoumopoulos**, Christos/Giovanni Buttarelli/Michael O’Flaherty, Handbook on European Data Protection Law, Publications Office of the European Union, Luxembourg, 2018.
- Guzman**, Andrew T./Timothy L. Meyer, International Soft Law, Journal of Legal Analysis, Volume 2, Issue 1, Spring 2010.
- Hintze**, Mike/Khaled El Emam, “Comparing the benefits of pseudonymisation and anonymisation under the GDPR”, Journal of Data Protection & Privacy, Volume 2, Number 2, Autumn 2018.
- Kuner**, Christopher, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy and Security Law Report, June 2012, [http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner\\_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf](http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-Copernican-Revolution-in-European-Data-Protection-Law.pdf) (Son Erişim Tarihi: 10.02.2019).

- Madge**, Robert, Five Loopholes in the GDPR, August 27, 2017, <https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b> (Son Erişim Tarihi: 20.03.2019).
- Markou**, Christina, “The Right to Be Forgotten: Ten Reasons Why It Should Be Forgotten”, Law, Governance and Technology Series 20: Reforming Data Protection Law, Springer, 2015.
- Politou**, Eugenia/Efthimios Alepis/Constantinos Patsakis, “Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions”, Journal of Cybersecurity, V. 4, I. 1, January 2018.
- Ragep**, F. Jamil, “Copernicus and His Islamic Predecessors: Some Historical Remarks”, Mc. Gill University, History of Science Journal, N. XLV, 2007.
- Soysal**, Tamer, Tarımda Biyoteknoloji Uygulamaları ve Patent Hakları (Agricultural Biotech Patent Law), Adalet Yayınevi, 2019.
- Tapan**, Mehmet Nuri, “Avrupa Birliđi (AB) Hukukunun Kaynakları ve Ulusal Hukuka Etkileri: Avrupa Adalet Divanı”, Türkiye Barolar Birliđi Dergisi, S. 3, Y. 1998.
- Üzeltürk**, Hakan, Avrupa Birliđi Genel Veri Koruma Düzenlemesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XV, S. 2, İstanbul, 2018.
- Voigt**, Paul /Axel von dem Bussche, The EU GDPR: A Practical Guide, Springer, Heidelberg, 2017.

## **CRYPTOLOCKER; BİR FİDYE VİRÜSÜNÜN CEZA HUKUKU AÇISINDAN ANALİZİ**

**Doç.Dr.Olgun DEĞİRMENÇİ\***,<sup>687</sup>

### **Özet**

Bir fidye virüsü türü olan cryptolocker, bir bilgisayar virüsünün tüm özelliklerine sahiptir. Fidye virüsü olarak tasnif edilmesinin sebebi, girmiş olduğu sistemi enfekte etmesinin yanı sıra söz konusu zararın giderilmesi için menfaat talep etmesidir. Cryptolocker virüsü, kendini hedef bilişim sistemine yükledikten sonra, güçlü bir şifreleme anahtarı kullanmak suretiyle, kullanıcıya ait olan verileri şifrelemek suretiyle erişilmez kılmaktadır. Verilerin erişilmez kılınmasının ardından, söz konusu şifreyi çözecek anahtarın verilmesi karşılığında mağdurdan kripto para ödemesi istenmektedir. Fidye virüsleri, genel olarak sistemin işleyişine zarar vermeksizin, kullanıcı açısından değerli olan verileri hedef almaktadırlar. Kullanıcı açısından değerli olan verinin erişilmez kılınması, temin edilecek menfaatin de miktarını artırmaktadır. Virüsün hedef seçici özelliğinin sonucunu, cryptolocker ile wannacry virüslerinin hedefleri arasındaki farkta görebiliriz. Nitekim birincisi daha çok bireysel kullanıcıları hedef alırken, sonuncusu verinin değerli olduğu sağlık sektörünü hedef almıştır. Fidye virüsünün oluşturulması, hedef sisteme yüklenmesi, verilerin erişilmez kılınması ve sonunda menfaatin temini, ceza kanunlarında düzenlenen ve suç teşkil eden hareketlerdir. Bu tebliğde, cryptolocker virüsünün özelinde fidye virüsüne özgü davranış şekilleri analiz edildikten sonra, oluşabilecek muhtemel suç tiplerine değinilecektir.

Anahtar Sözcükler: cryptolocker, fidye virüs, ceza hukuku, suç, bilişim suçu.

### **CryptoLocker: Analysis of a Ransom Virus in Terms of Criminal Law**

#### **Abstract**

Cryptolocker, a ransom virus type, has all the features of a computer virus. The reason why it is classified as a ransom virus is that it infects the system it enters, as well as demanding the benefit

---

\* Hukuk Fakültesi, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara, Türkiye.

<sup>687</sup> ORCID: <https://orcid.org/0000-0002-0700-2549>



of the damage. The Cryptolocker virus makes the data that belongs to the user inaccessible by encrypting, using a strong encryption key, after uploading itself to the target information system. After the data is inaccessible, the victim is required to pay crypto money in exchange for issuing the key to solve the password. In general, ransom viruses target data that are valuable to the user without damaging the functioning of the system. The invaluable data for the user increases the amount of the benefit to be provided. The result of the target selector feature of the virus, we can see the difference between the targets of cryptolocker and wannacry viruses. As a matter of fact, the first one targeted the individual users while the last one targeted the health sector where the data was valuable. Creation of the ransom virus, loading it into the target system, making the data inaccessible, and finally the provision of benefits are the criminal acts in criminal law. In this paper, after examining the behavior of the ransom virus specific behavior of the cryptolocker virus, the possible types of crime will be discussed.

Keywords: cryptolocker, ransomware, criminal law, crime, computer crime.

## I. GENEL AÇIKLAMALAR

İnceleme konumuzu teşkil eden ve hukuki açıdan analize tabi tutulacak zararlı yazılım türü olan CryptoLocker, fidye yazılım (ransomware)<sup>688</sup> ailesine mensuptur. Fidyeye virüsler, yağmacı virüs şeklinde de ifade edebileceğimiz bir mantıkta çalışırlar ve bulaştığı sistemlerde, sistem kullanıcıları için değer ifade eden verileri erişilmez kılmak suretiyle menfaat elde etmeyi hedeflerler.<sup>689</sup> ABD Federal Ticaret Komisyonu (Federal Trade Commission) tarafından 2016 yılında “iş dünyası ve bireylerin karşılaştığı en ciddi çevrimiçi tehditlerden biri” ve “kullanılan en kârlı zararlı yazılım” olarak nitelenen<sup>690</sup> fidye virüsler, bilişim sistemlerine yapılan saldırılarda kullanılan araçların evrimleşme sürecini göstermesi açısından da bizim için incelemeye değerdir. Nitekim ilk geliştirilen zararlı yazılımlar (özelinde virüsler) sadece sisteme ve verilere zarar verme amacı

---

<sup>688</sup> Çalışmanın ilerleyen bölümlerinde *ransomware* karşılığı fidye yazılım veya fidye virüs kavramları birbirinin yerine aynı anlamda kullanılacaktır.

<sup>689</sup> **Liska, Allan / Gallo, Timothy:** Ransomware Defending Against Digital Extortion, O'Reilly, 2017, s. 3; **Sherer, James A. / McLellan, Melinda L. / Fedeles, Emily R. / Sterling, Nichole L.:** Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web, Richmond Journal of Law & Technology, Vol. XXIII, Issue 3, s. 1 (ss. 1 – 48); **Pascariu, Cristiona / Barbu, Ionut – Daniell / Bacivarov, Ioan C.:** Investigative Analysis and Technical Overview of Ransomware Based Attacks. Case Study: WannaCry, International Journal of Information Security and Cybercrime, Vol. 6, Issue 1, 2017, s. 57 (ss. 57 – 62).

<sup>690</sup> **Sherer / McLellan / Fedeles / Sterling,** s. 1 – 2.

taşıırken, geçen yıllar içerisinde amaç farklılaşmış ve verilerin erişilemez kılınacağı tehdidi ile menfaat teminine yönelmiştir.

Fidyeye virüsler, bir zararlı yazılım çeşididir. Kategorik olarak yapılan sınıflandırmada ise bireylerde ortaya çıkan özel bilgilerinin ifşa edileceği, önemli verilerinin kayba uğratılacağı ya da donanımlarına zarar verileceği korkusundan yararlanılarak fayda sağlayan panik yazılım türü olan *scareware* olarak isimlendirilen yazılımların bir alt kümesinde yer almaktadır.<sup>691</sup>

Bireysel veya toplumsal hukuki menfaatlerin korunması araçlarından biri olan ceza hukukunun da, söz konusu toplumsal gelişime seyirci kalması düşünülemez. Bu kapsamda, fidye virüsler bakımından uygulanacak ceza hukuku normlarının belirlenmesi, kanunilik ilkesi bakımından uygulanabilecek bir normun tespit edilememesi durumunda ise kanunlaşma süreçlerinin başlatılması gereklidir. Shaw'ın, Uluslararası Hukuk kitabının girişinde de ifade ettiği gibi *“İnsanoğlunun mağara kovuğundan bilgisayarlar kadar uzun yürüyüşünde, düzenin gerekliliği ve düzensizliğin ise makul ve istikrarlı varoluşa düşman olduğuna dair hukuk ideası merkezi bir rol oynamıştır.”*<sup>692</sup>. Dolayısıyla düzensizliğin, düzene evrilmesi gereklidir. Nitekim bu durum teknoloji ile hukuk arasındaki ilişkinin de belgesi olarak karşımıza çıkmaktadır. Faydalı amaçlarla çevrenin insan tarafından belli bir bakış açısıyla değiştirilmesi olarak da tanımlanan teknoloji ile hukuk arasındaki ilişki bağımlı ve karşılıklı bir ilişki olarak karşımıza çıkmaktadır.<sup>693</sup> *“İnsanlık ilk önce kendi araçlarını inşa eder, sonra kendi tarafından inşa edilen araçlar da insanlığı”*<sup>694</sup> ifadesi aslında bu açıdan bakıldığında bir doğruya da işaret etmektedir. Teknolojik sistemlerin büyüüp gelişmesi toplum ile aralarındaki şekillenme – şekillendirme ilişkisine ters yönde etki etmekte ve toplumu daha fazla şekillendirirken, kendisi toplum tarafından daha az şekillendirilmektedir.<sup>695</sup>

---

<sup>691</sup> Bu kapsamda malware – scareware – ransomware alt gruplandırması yapılmaktadır. Bkz. **Kharraz, Amin / Robertson, William / Balzarotte, Davide / Bilge, Leyla / Kirda, Engin**: Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, M. Almgren et al. (Eds.): DIMVA 2015, LNCS 9148, pp. 3–24, Springer 2015, s. 3.

<sup>692</sup> **Shaw, Malcolm N.**: International Law, 6 th Edition, Oxford University Press 2008, s. 1; Bakınız aynı şekilde **Kettemann, Matthias C.**: Ensuring Cybersecurity Through International Law, 69 R.E.D.I. 281, 2017, s. 281 (ss. 281 – 289).

<sup>693</sup> **Flint, David**, Law Shaping Technology: Technology Shaping the Law, International Review of Law, Computers and Technology, Vol. 23, No. 1 – 2, March – July 2009, s. 5 – 11.

<sup>694</sup> **McLuhan, Marshall**, Understanding Media: The Extension of Man, McGraw Hill, New York 1996, s. 23.

<sup>695</sup> **Hugher, Thomas P.**, Technological Momentum, in: Does Technology Drive History? The Dilemma of Technological Determinism (Edited by Merritt Roe Smith and Leo Marx), Cambridge, MIT Press, 1994, s. 113.

Bu çalışmamızda ülkemizi de etkileyen *CryptoLocker* özelinde fidye virüslerin anatomisi incelenecek ve bu inceleme ışığında oluşabilecek suç tiplerine işaret edilecektir. Çalışmamıza konu olarak fidye virüslerin seçilmesinin nedenleri arasında, fidye virüslerin (genel olarak zararlı yazılım türü olarak), sınır aşan bilişim suçları içerisinde giderek artan sayıda görülen bir yöntem olması da gelmektedir.<sup>696</sup> Çalışma öncelikle fidye virüsler bakımından mevcut durumu ortaya koyacak ve sonrasında ceza hukukunda mevcut normların, tespit edilen durumu yaptırım altına almaya yeterli olup olmadığı incelenecektir. Bu açıdan bakıldığında çalışmanın hipotezinin konusunu buyurgan (preskriptif) değil, betimsel (deskriptif) bir iddia oluşturmaktadır.<sup>697</sup>

## II. FİDYE VİRÜSLERİN ANATOMİSİ

### A. KONUYA İLİŞKİN GENEL AÇIKLAMALAR

Fidye virüslerin, hedef bilişim sistemine sızıp, kendisini bilişim sistemine yükleyip, zararlı etkiyi gerçekleştirip, menfaat teminine kadar geçen süreçte farklı yöntemler kullandığı görülmektedir. Fidye virüsler, bir virüs ailesi olarak kendi içinde yöntem bakımından da farklılaşmaktadır. Örneğin zararlı etki bakımından bazı fidye virüsler, kullanıcının verilerine ulaşmasını basit şekilde zorlaştırırken (örneğin ekranın açılır pencere sayısını sınırlamak, dosya adını değiştirmek veya sistemin çalışmasını engellemek gibi), inceleme konumuz olan *CryptoLocker* örneğinde olduğu gibi bazı fidye virüsler de güçlü şifreleme sistemleri kullanarak hem dosya içeriğini hem de dosya adını şifreleyebilmektedirler.<sup>698</sup>

Fidye virüsler bakımından ilk kayda geçen örnek, Dünya Sağlık Organizasyonu tarafından 1989'da düzenlenen AIDS Konferansı sırasında 20.000'den fazla diski enfekte eden ve aslen bir biyolog olan Joseph Popp tarafından geliştirilen *AIDS Trojan*'dur. Simetrik şifreleme sistemi ile sadece dosya adlarını şifreleyen *AIDS Trojan* tarafından şifrelenen dosyalar kısa sürede deşifre edilebilmiştir.<sup>699</sup> 2005 yılına kadar duraksama gösteren fidye virüsler, 2005 yılında

---

<sup>696</sup> Nitekim Perloff – Giles yakın tarihli bir çalışmasında incelemiş olduğu sınır aşan bilişim suçlarında, fidye virüsleri, hizmetin engellenmesi saldırıları (DoS – Denial of Service) ile birlikte en yaygın bilişim suçları olduğunu belirtmiştir. Bu konuda bkz. **Perloff – Giles, Alexandra**: *Transnational Cyber Offences: Overcoming Jurisdictional Challenges*, 43 *Yale J. Int'l L.* (2018), s. 197 (ss. 191 – 227).

<sup>697</sup> Bu konuda bkz. **Volokh**, Eugene: *Akademik Metinler Nasıl Yazılır? Hukukçular için Rehber* (Çev.: Ertuğrul Uzun), Tekin Yayınları İstanbul 2019, s. 39

<sup>698</sup> **Liska / Gallo**, s. 6.

<sup>699</sup> **Richardson, Ronny/North, Max M.**: *Ransomware: Evolution, Mitigation and Prevention*, *International Management Review*, Vol.13, No.1, 2017, s. 12 (ss. 10 – 21); **Sherer / McLellan / Fedeles / Sterling**; s. 3.

*Trojan.Gpcoder* fidye virüsü ile birlikte dosya isimlerinin şifrlenmesinden, dosyaların şifrlenmesine evrilmiştir. 2007 yılında *Locker* isimli fidye virüsü ortaya çıkmış ve şifreleme yöntemi yerine, sistem ekranını kilitleyerek ekranda pornografik bir görüntüyü sabitlemiş ve görüntünün giderilmesi için SMS metin mesajı veya bir telefon numarasının aranması istenmiştir. 2012 yılında ilk kez fidye virüs toolkitleri yapılmıştır. *Citadel* isimli toolkit sayesinde fidye virüsü oluşturmak ve dağıtmak kolaylaştırılmıştır. 2013 yılında inceleme konumuz olan *CryptoLocker* virüsü görülmüştür. Söz konusu virüs farklı versiyonları da var olmakla birlikte 500.000'den fazla kişiye zarar vermiş ve virüs sayesinde 27 milyon dolar menfaat temin edilmiştir.<sup>700</sup> Yukarıda genel olarak fidye virüsler bakımından kilometre taşlarına yer verilmiştir. Belirtmek isteriz ki fidye virüsler birbirinden çok farklı metodolojiler kullandığı gibi aynı fidye virüsün birden fazla farklı versiyonu da bulunmaktadır. 2015 yılında yapılan bir çalışmada fidye virüslerden etkilenme oranında ABD'nin 1'nci sırada yer aldığı görülürken, Türkiye 12'nci sırada yer almaktadır.<sup>701</sup>

Fidye virüsler, önceleri bireysel kullanıcıları hedef alırken, işletmeler bakımından verilerin değeri keşfedildikten sonra daha fazla menfaat temini için işletmeleri hedef almaya başlamıştır. Bu bakımdan 2016 yılı için *Wannacry* fidye virüsünün, verinin en değerli olduğu sektörlerden biri olan sağlık sektörünü hedef alması da tahmin edilemeyecek bir durum değildir. Fidye virüslerin geleceği bakımından yapılan öngörü ise fidye virüsler tarafından öncelikle mobil cihazların hedef alınacağı ve daha sonra ise nesnelerin interneti kapsamında veri iletişimi olan her cihazın fidye virüsler bakımından hedef olabileceği şeklindedir.<sup>702</sup> Fidye virüslerin farklılaşan zararlı etki yöntemleri, zararlı etkinin gerçekleştirilmesi safhası bakımından uygulanacak ceza normunda da farklılıklara neden olmaktadır. Bu açıdan fidye virüsün saldırı süreçleri ve etkilerinin belirlenmesi gereklidir.

Fidye virüslerin genel karakteristik özellikleri şu şekilde ifade edilebilir<sup>703</sup>;

- Güçlü bir şifreleme algoritması kullanırlar (*CryptoLocker* RSA – 2048 şifreleme algoritmasını kullanmaktadır).

- Birçok dosya formatını şifreleme yetenekleri mevcuttur.

---

<sup>700</sup> Richardson / North, s. 13.

<sup>701</sup> Richardson / North, s. 14.

<sup>702</sup> Sherer / McLellan / Fedeles / Sterling, s. 44.

<sup>703</sup> Rajput, Toshima Singh: Evolving Threat Agents: Ransomware and their Variants, International Journal of Computer Applications, Vol. 164, No. 7, April 2017, s. 28 vd. (ss. 28 – 34).

- Dosya adlarını da şifrelediklerinden dolayı hangi dosyanın virüsten etkilendiğini tahmin etmek güçtür.
- Dosya adlarına *.docx.rsrc* gibi farklı uzantılar ekleyebilir.
- Ekranda bir fidye mesaj görüntüsü yer alır.
- Çoğunlukla kripto paralar menfaat olarak temin edilir.
- Mağdur bilişim sistemi ile fail bilişim sistemi arasındaki irtibatın TOR gibi güvenli iletişim ağları kullanılır.
- Antivirüs programları tarafından tespit edilmemek için karmaşık teknikler kullanır.
- Daha sonraki saldırılarda kullanılmak üzere çoğu zaman mağdur bilişim sistemini botnet haline dönüştürür.
- Bilişim sistemindeki verileri erişilmez kırkarken çoğu zaman sistemin normal işleyişini aksatmaz.

## B. FİDYE VİRÜSLERİN EVRİMİ

Fidye virüsler, ilk kez görüldüğü 1989 yılından beri bünyesine bazı özellikler katarak evrim geçirmiştir. Aynı biyolojik virüslerde olduğu gibi kendisine karşı alınan önlemleri aşarak bilişim sistem güvenliklerine karşı bağışıklık geliştirmeye çalışmışlardır. Kısaca bazı fidye virüsler ve gösterdiği etkiler liste olarak aşağıda sunulmuştur.<sup>704</sup>

Yıl	Adı	Gösterdiği Etki / Özellikleri
1989	AIDS Trojan	Bilgisayarların sınırlı bir grup tarafından kullanıldığı ve şifreleme sistemlerinin zayıf olduğu bir dönemde ortaya çıkmıştır. Şifreleme yapmamakta ve verilere zarar vermemektedir.
2005	Trojan.Gpcoder	Simetrik şifreleme sistemi kullanmaktadır. Kullanıcı tarafından sıklıkla kullanılan kullanıcı dosyalarının uzantılarını şifrelemektedir.
2011	Trojan.Ransom.C	Ekranda Windows güvenlik mesajı oluşturmakta ve bilgisayarı kilitleyerek ödemeli telefon sistemlerini aramasını istemektedir.
2013	CryptoLocker	Asimetrik şifreleme sistemi kullanarak kullanıcı dosyalarını şifrelemektedir.
2016	KeRanger	MAC işletim sistemlerini enfekte etmektedir. 300'den fazla dosya türünü şifreleyebilmektedir. Üretmiş olduğu kişisel anahtarını 3 gün

<sup>704</sup> Rajput, s. 30 – 32.

		süreyle sunumcuda saklamakta ve sürenin sonunda geriye dönüşü mümkün olmayacak şekilde imha etmektedir.
2016	Petya	Dosya yerine sisteme saldırıyı yöneltmektedir. Master boot Record üzerine yazmak suretiyle mavi ekranın çıkmasına yol açmaktadır. Sistem reboot edildiğinde ekranda kuru kafa ve kemik işareti belirlemektedir.
2017	VirLock	Bilgisayar ekranını kilitlemenin yanı sıra dosyaları da enfekte etmektedir.

## C. FİDYE VİRÜS SALDIRI SÜREÇLERİ

### 1. Yayılma (deployment)

Fidye virüs saldırıların ilk aşaması yayılma sürecidir. Bu süreçte fidye virüsün zararlı etkiyi gerçekleştireceği bilişim sisteminin tespit edilip, sisteme gönderilmesi gereklidir. Bu aşama için farklı yöntemler kullanılmaktadır; örneğin kullanıcı bilgisi olmaksızın zararlı yazılımın sisteme otomatik yüklenmesi (drive-by download), özellikle bir organizasyonun hedef alındığı durumlarda, ilgili organizasyon tarafından sık ziyaret edilen web sitelerinin tespit edilmesi suretiyle zararlı yazılımın ilgili siteye konması (watering-hole attacks), zararlı yazılımın gönderilen elektronik postalara bağlantı (link) olarak eklenmesi ve mağdurun yanıltılarak bağlantıyı tıklamasının sağlanması (phishing emails) gibi yöntemler kullanılmaktadır.<sup>705</sup>

### 2. Yükleme (installation)

İkinci aşamada, zararlı etkiyi gerçekleştirmek için fidye virüsün sisteme yüklenmesi söz konusudur. Bu aşamada önem kazanan husus, özellikle anti virüs programlarına yakalanmadan zararlı yazılımın sisteme giriş yapmasıdır. Kullanılan yöntemlerden birisi, önce anti virüs programının denetiminden kaçınmak ve failin komuta kontrol sistemi ile iletişimi sağlayacak küçük bir program parçacığının sisteme yerleştirilmesidir (download dropper methodology). Söz konusu program, zararlı yazılımın yüklenmesi için failden komut beklemekte ve gelen komut üzerine zararlı yazılımın yüklenmesi gerçekleştirilmektedir. Bunun yanı sıra güvenli olmayan elektronik marketlerden yapılan uygulama satın alınması işlemi sırasında da zararlı yazılımı sisteme sızabilmektedir (özellikle *jailbreak* yapılmış sistemlerde).

<sup>705</sup> Liska / Gallo, s. 7.

Bu aşamada fidye virüs, hangi sistemlerin enfekte olduğunu belirlemektedir. Bunun için zararlı yazılım bilişim sisteminin adı veya Mac adresi gibi tanıtıcı bilgisinin özet değerini (hash value) almak suretiyle, benzersiz bir kod yaratmaktadır.<sup>706</sup>

### 3. Komuta ve Kontrol (command-and-control)

Fidye virüsünün yayılması ve sisteme yerleşmesinden sonra, kendisine verilen komutları alması için komuta sunucularına ulaşması gereklidir. Yerleştirilen sistemde, şifrelenecek dosyaların tespiti ve sürecin başlaması için ne kadar beklenmesi gerektiği gibi hususlar zararlı yazılıma belli bir istek olarak gönderilmektedir. Zararlı yazılımın türüne göre yerleşilen sistemin bilgisi, IP adresi, alan adı, işletim sistemi, yüklü bulunan ağ gezginleri ve varsa anti virüs programının türü gibi bilgiler raporlanmaktadır. Bu aşamada fail bakımından sistemin enfekte edilip edilmediğinin yanı sıra, hedefin içerdiği verilerin mağdur bakımından değeri de tespit edilmektedir. Bu tespit, menfaat temini aşamasında istenecek menfaatin türü ve miktarını belirlemek açısından önem kazanmaktadır.<sup>707</sup>

Bu aşamada virüs yerleştirilmiş bilişim sistemi ile failin sistemi arasındaki iletişim farklı kanallardan sağlanabilmektedir. Virüsün karmaşıklığına ve yerleştirildiği bilişim sistemindeki verinin değerine göre şifrelenmemiş http protokolü üzerinden haberleşme yapılabileceği gibi, gizliliğin sağlanması ve özellikle kolluk kuvvetleri tarafından faile ulaşılmasının engellenmesi için TOR<sup>708</sup> üzerinden de iletişim sağlanabilmektedir.<sup>709</sup>

Komuta ve kontrol aşamasının temel olarak iki amacı bulunmaktadır: İlki yukarıda da ifade edildiği üzere virüsün yerleştirildiği sistemin incelenmesidir. Bu inceleme hedef bilişim sistemindeki verinin değerinin belirlenmesinden, enfekte edilen bilişim sisteminin tespitinden, kolluk tarafından gerçekleştirilen bir operasyonun parçası olup olmadığını belirlemeye kadar geniş bir alanı kapsayabilmektedir. İkinci olarak sistemin tespiti ve güvenilir olduğunun

---

<sup>706</sup> Liska / Gallo, s. 9.

<sup>707</sup> Liska / Gallo, s. 9.

<sup>708</sup> TOR (The Onion Router), Amerikan Ulusal Bilim Vakfı tarafından fonlanan ve kar amacı gütmeyen bir organizasyon olan Tor Project tarafından işletilmektedir. 2000'li yılların başında hükümetin internet üzerindeki iletişimini korumak amacıyla oluşturulmuştur. Tor Network anonim bir yazılım tarafından yönetilir ve Internet trafiğini Tor düğüm noktalarına yönlendirmek suretiyle, söz konusu noktalarda IP adreslerini maskeler ve iletişimin hedef ve kaynağını takip edilemez hale getirir. İletişimi takip edilemez kılmasından dolayı özellikle organize suç örgütleri tarafından ciddi şekilde kullanılmaktadır. (Dolliver, D.S. / Kenney, J.L.: Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison, in: Victim & Offenders, Taylor & Francis Group, 2016, s. 601, 602 (ss. 600 – 620).

<sup>709</sup> Liska / Gallo, s. 9.

belirlenmesinden sonra üretilen şifreleme anahtarının, mağdurun bilişim sistemine gönderilmesidir. Bu noktada kullanılan fidye virüsünün karmaşık yapısına göre sadece dosya adlarını değiştiren şifreleme sistemlerinden, tek bir anahtar kullanıldığı simetrik şifreleme sistemlerine veya birden fazla anahtar kullanıldığı asimetrik şifreleme sistemlerine kadar değişik sistemler kullanılmaktadır. İnceleme konumuz olan CryptoLocker virüsünde asimetrik şifreleme sistemi kullanılmaktadır. Bu sistemde, iki adet anahtar üretilmekte ve ortak anahtar (public key – şifrelemeyi gerçekleştirecek anahtar) mağdurun bilişim sistemine (client – istemci) gönderilmektedir. Özel anahtar (private key – deşifrelemeyi gerçekleştirecek anahtar) ise failin bilişim sisteminde (server – sunumcu) tutulmaktadır.<sup>710</sup>

Kullanılan simetrik veya asimetrik şifreleme sistemlerinin birbirine göre fayda ve mahzurları bulunmaktadır. Simetrik şifreleme sistemlerinde, şifrelemenin gerçekleştirilmesi için mağdur bilişim sistemi kullanılmakta ve minimum sistem kaynağı harcanmaktadır. Sistem kaynaklarının minimizasyonu, şifreleme sisteminin anti virüs yazılımları tarafından tespitini güçleştirmektedir. İkinci olarak her bir sistemin şifrenmesi için tek bir anahtarın kullanılması durumunda, virüsün yerleştirilmesi aşamasının fail tarafından takip edilmesi yeterli olacaktır. Ayrıca şifreleme için mağdurun bilişim sistemi ile failin bilişim sistemi arasında bir iletişim zorunlu olmayacak ve bu durumda, ağa bağlı olmadan da mağdurun bilişim sisteminde şifreleme işlemi başlatılabilecektir. Şifreleme bittikten sonra mağdurun bilişim sisteminde üretilen şifreleme anahtarı, menfaat temininde kullanılmak amacıyla bilişim suçu failinin bilişim sistemine gönderilecektir. Bunun için sadece mağdurun bilişim sisteminin ağ bağlantısını gerçekleştirmesi yeterli olacaktır.<sup>711</sup> Simetrik şifreleme sistemlerinin mahzuru ise mağdurun bilişim sisteminde üretilen şifreleme anahtarının, sistem ağa bağlı değilken RAM'den alınması ve deşifreleme için kullanılmasının mümkün olmasıdır. RAM'in kopyalanması farklı adli bilişim araçlarının kullanılması suretiyle mümkün olabilecektir.

Asimetrik şifreleme sistemleri ise şifreleme süreçleri için ortak ve kişisel olmak üzere iki farklı anahtar üretmektedirler. Ortak anahtar, mağdurun bilişim sisteminde, mevcut dosyaların şifrenmesi için kullanılır. Kişisel anahtar ise deşifreleme amacıyla kullanılır ve failin bilişim sisteminde bulunur. Simetrik şifreleme sisteminde olduğu gibi dosyaların şifrenmesi anında müdahale edilse dahi, kişisel anahtarın ele geçirilmesi olanaksızdır. Asimetrik şifrelemede,

---

<sup>710</sup> **Richardson / North**, s. 12.

<sup>711</sup> **Liska / Gallo**, s. 13.



şifreleme işleminin başlayabilmesi için anahtar üretimi gereklidir ve anahtarların üretilmesi için ise fail ve mağdurun bilişim sistemlerinin ağ üzerinden birbiri ile irtibat kurması gereklidir.<sup>712</sup>

#### 4. Zararlı Etkinin Gerçekleştirilmesi (destruction)

Bu safhada fidye virüsün yüküne göre (payload – zararlı etki), mağdurun bilişim sistemini kitlemekte veya sistemde yer alan verileri şifrelemektedir. Bu safhada şifrelenecek dosyalar, komuta kontrol safhasında belirlenen dosyalardır. Kullanılan fidye virüsün türüne göre dosya adları sadece küçük harf değişiklikleri ile değiştirilebilmekte, sadece dosya adları veya dosyalar tüm içerikleri ile şifrelenebilmektedir.<sup>713</sup> Örneğin *CryptoLocker* virüsünün Microsoft Office veri dosyaları da dâhil olmak üzere 67 farklı dosya türünü şifrelediği bilinmektedir.<sup>714</sup>

*CryptoLocker* virüsü genel olarak RSA 2048 şifreleme algoritmasını kullanmaktadır. Kullanılan bu güçlü algoritmanın şifrelediği bir dosyanın şifresinin çözülmesi neredeyse olanaksızdır. Örneğin sıradan bir masaüstü bilgisayar ile şifrenin çözülmesi yaklaşık olarak 6,4 katrilyon yıl sürmektedir.<sup>715</sup>

#### 5. Menfaat Temini (extortion)

Fidye virüsün son aşamasında menfaat temini yapılmaktadır. Bu aşamaya kadar kullanılan virüs yapısına göre farklı şifreleme sistemleri ile şifrelemeler yapılmış ve mağdurun bazı durumlarda verilerine bazı durumlarda sistemine ulaşması engellenmiştir. Menfaat temini aşamasında da farklı sistemler kullanılmaktadır. Bazı fidye virüsler, diğer dosyaların çözülmesi için bir anahtara ihtiyaç olduğunu göstermek için şifrelenen dosyalardan sadece bir tanesine ücretsiz ulaşmaya müsaade etmektedirler. Diğer bazı fidye virüsleri ise fail ile iletişim kanallarını gösteren bir mesajı mağdurun bilişim sistemine göndermekte ve ilgili iletişim kanalları kullanıldıktan ve menfaat temin edildikten sonra şifre çözme anahtarını ulaştırmaktadırlar. *CryptoLocker* virüsünün daha sonraki sürümlerinde, şifre anahtarına ulaşmayı zaman bakımından sınırlamak suretiyle mağdur üzerinde baskı yaratılmaya çalışılmıştır. *CryptoLocker* için bu süre 3 gün olarak belirlenmiştir.

Temin edilecek menfaatin miktarı ve türü yine fidye virüse göre değişebilmektedir. Örneğin 2006 yılında yayılan Trojan.Cryzip isimli fidye virüsü mağdura bildirmiş olduğu bazı ilaçların

---

<sup>712</sup> Liska / Gallo, s. 15.

<sup>713</sup> Liska / Gallo, s. 11.

<sup>714</sup> Richardson / North, s. 12.

<sup>715</sup> Sherer / McLellan / Fedeles / Sterling, s. 8.

online eczanelerden sipariş edilmesi ve sipariş numarasının gönderilmesi durumunda deşifre anahtarını göndermektedir. Kripto paraların yaygınlaşmasına kadar SMS, belirli bir telefon numarasının aranması, önödeme kartlar şeklinde değişik ödeme sistemleri üzerinden menfaat temini yapılmıştır. Ancak günümüzde kripto para (çoğunlukla bitcoin olmak üzere diğer alt coinlerde kabul edilmektedir) hemen hemen tüm fidye virüsler bakımından geçerli bir ödeme yöntemi olmuştur.<sup>716</sup>

CryptoLocker menfaat temini aşamasında kripto para (ve çoğunlukla bitcoin) kullanmaktadır. Kripto para transferleri, noktadan noktaya yapılmakta ve anonimlik sağlanmaktadır.<sup>717</sup> CryptoLocker, tespit edilip tedbir alınmaya kadar 27 milyon dolar değerinde Bitcoin ödeme olarak kabul etmiştir.<sup>718</sup>

### III. SAFHALARINA GÖRE UYGULANACAK NORMLAR

#### A. GENEL OLARAK

Fidye virüsler kişisel veri niteliğinde olsun veya olmasın herhangi bir veriyi ele geçirmez veya ifşa etmezler. Bundan dolayı fidye virüsler bakımından TCK m. 135 ve 136'da yer alan suçların oluşmadığı kanaatindeyiz. Nitekim Wannacry fidye virüsünün sağlık sistemine yönelik saldırısından sonra yapılan incelemelerde bu husus tartışılmıştır. Bu kapsamda, ABD hukukunda Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (The Health Insurance Portability And Accountability Act) uyarınca sağlık verilerin ifşası durumunda, ilgili kurum tarafından veri sahibine bilgi verilmesi gereklidir. Saldırıya uğrayan sağlık şirketlerinin de söz konusu yükümlülüğü yerine getirebilmesi için öncelikle sağlık verilerinin ifşa edilip edilmediği tartışılmıştır. Sonuç olarak fidye virüsün, kişisel verileri ifşa etmediği sonucuna varılmıştır.<sup>719</sup> Benzer bir tartışmanın 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12'nci maddesinin 5'nci fıkrası gereğince ülkemiz bakımından da yapılması gerektiği kanaatindeyiz. Nitekim ilgili fıkra; "*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir*" hükmünü amirdir. Bu

---

<sup>716</sup> Richardson / North, s. 10.

<sup>717</sup> Paquet – Clouston, Masarah / Haslhofer, Bernhard / Dupont, Benoît: Ransomware Payments in the Bitcoin Ecosystem, The 17th Annual Workshop on the Economics of Information Security (WEIS), June 2018, Innsbruck, Austria; TK, Anjana: Discussion on Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks, IJRTI, Vol. 2, Issue 6, 2017, s. 210 (ss. 210 – 214).

<sup>718</sup> TK, s. 211.

<sup>719</sup> Sherer / McLellan / Fedeles / Sterling, s. 24.

kapsamda veri işleyen birimler, işlenen kişisel verilerin başkaları tarafından ele geçirildiğini tespit etmesi durumunda, ilgisini durumdan haberdar etmekle yükümlüdür.

Fidye virüsler kullanılarak menfaat temini siber yağma (cyber extortion) olarak da isimlendirilmektedir. İncelemiş olduğumuz ülke kanunlarında, bir örnek dışında bu isimle anılan ve tüm süreçleri cezalandıran bir düzenlemeye rastlamadık. İstisna düzenleme Güney Afrika Bilgisayar Suçları ve Bilgisayar Güvenliği Kanunu'nun 10'ncü Bölümünde "siber yağma" olarak isimlendirilen bir suç tipidir. Söz konusu düzenlemeye göre bazı bilişim suçlarının işlenmesi veya işlenmesi tehdidi ile bir kişiden fayda sağlayan veya bir kişiyi bir şeyi yapmaya veya yapmaktan kaçınmaya zorlayan kişi cezalandırılmaktadır.<sup>720</sup> Siber yağmayı tek başına cezalandıran düzenleme dışında, ülkeler mevzuatında fidye yazılımların safhalarına göre farklı suç tipleri uygulanabilmektedir.

## **B. TCK m. 245/A YASAK CİHAZ VEYA PROGRAMLARLA İLGİLİ SUÇ TİPİ**

### **a. Zararlı Yazılımların Oluşturulması, Bulundurulması ve Ticaretinin Cezalandırılması Gerekliliği**

Fidye virüs saldırısının gerçekleştirilebilmesi için öncelikle kullanılacak zararlı yazılımın oluşturulması gereklidir. Söz konusu zararlı yazılım fail veya failer tarafından oluşturulabileceği gibi, sanal yeraltı dünyasından satın da alınabilirler. Dolayısıyla öncelikle söz konusu zararlı yazılımın oluşturulması veya satın alınması gibi hareketlerin cezalandırılabilirliği konusunu ele alacağız.

Bilişim sistemlerinin sosyal hayatta rolünün artması, söz konusu sistemlerin ve sistemler üzerinde işlenen verilerin de ekonomik olarak değerinin artmasına neden olmuştur. Bu durum ise failleri, sistemler üzerindeki verilere yönlendirmiştir. Daha önceleri sadece kredi kart bilgilerine veya bazı hizmetlerden ücretsiz istifadeye yönelen ilgi, daha az yetenekli faillere teknik destek vermeye doğru evrilmiştir. Bugün sanal yeraltı dünyasında aynen fizik dünyada yasal herhangi bir ürünün satış öncesi ve satış sonrası hizmetlerine benzer hizmetler verilmektedir. Nitekim istenen bir zararlı yazılımın oluşturulması için "kendin yap" kitlerinden, zararlı yazılımın oluşturulması, yayılması, zararlı etkinin oluşturulması ve menfaatin teminine kadar süreçlerde verilen hizmetlere kadar sanal yeraltı dünyası geniş bir yelpazede potansiyel bilişim suç faillerini desteklemektedir. Sanal yeraltı dünyasında sunulan ürünler de geniş bir alana yayılmaktadır. Örneğin bilişim

---

<sup>720</sup> **Mabunda, Sagwadi:** Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill, Statute Law Review, 2017, s. 1 vd.

sistemine yetkisiz erişimi sağlayan araçlar, yetkisiz erişim sonucunda elde edilen mali bilgiler, veri kayıtları, IP adresleri gibi sayısal varlıklar (digital assets), aynen bir bulut hizmeti gibi belli platformda sunulan bilişim suçlarına ilişkin hizmetler bu kapsamda sayılabilir. Sanal yeraltı dünyasında 16 - 325 dolar arasında değişen ücretlerle herhangi bir bilişim sistemine yetkisiz giriş hizmeti alabilir, web saldırıları için kendin yap kitlerini 15 – 20 dolar arasında oluşturabilir veya onlarca dolardan binlerce dolara varan fiyatlarla herhangi bir yazılımı hayat boyu garanti ile edebilirsiniz. Bu söz konusu sanal yeraltı pazarlarına örnek olarak Ekim 2013’de kapatılan Silk Road, Mayıs 2013’de kapatılan Liberty Reserve, Ekim 2013’de kapatılan Blackhole Exploit Kit verilebilir.<sup>721</sup>

Zararlı yazılımların kullanılması suretiyle elde edilen menfaatlerin artması, zararlı yazılım araçlarını daha kolay ulaşılabilir kılmıştır. Bir zararlı yazılımı oluşturma, elinde bulundurma veya zararlı yazılımın ticaretini yapma eylemlerinin, daha sonra işlenecek suçların önlenmesi bakımından cezalandırılması düşünülmüştür. Suç ve ceza politikası açısından bakıldığında, daha sonra işlenecek olan suçlar bakımından hazırlık hareketi niteliğinde olan zararlı yazılımların oluşturulması, bulundurulması ve ticareti eylemleri, ceza politikalarında yaşanan değişimin sonucunda cezalandırma alanının hazırlık hareketlerine doğru genişletilmesi suretiyle<sup>722</sup> cezalandırılabilir eylemler arasına alınmışlardır. Özellikle zararlı yazılım ticaretinin cezalandırılmasının amaçlarından birisi de, sanal yeraltı pazarının cezalandırılabilir alana dâhil edilmesidir.

## **b. Zararlı Yazılımların Silah Olarak Değerlendirilmesine İlişkin Tartışmalar**

Zararlı yazılımların oluşturulması veya daha bilinen adıyla virüs yazılımının suç olup olmadığının özellikle 1900’lü yılların sonundan itibaren ciddi şekilde tartışıldığı bilinmektedir. 2000’li yılların başlarında özellikle Avrupa Konseyi Siber Suç Sözleşmesi’nin oluşturulmasına yönelik gayretler esnasında, virüs yazılımının cezalandırılması tartışmaları yeniden alevlenmiştir. ABD mevzuatına göre bir virüsün sadece yazılması, bilişim sistemine zarar vermek veya yetkisiz erişmek için kullanılması veya yayılması saiki bulunmadığı sürece suç teşkil etmemesi hususları da

---

<sup>721</sup> Sanal yeraltı dünyası ile ilgili detaylı bir alan çalışması için bkz. **Ablon, Lilian / Libicki, Martin C. / Golay, Andrea A.:** Markets for Cybercrime Tools and Stolen Data, Hackers’ Bazaar, RAND 2014, s. 3 – 19.

<sup>722</sup> Bu konuda bkz. **Tekin, Derya:** Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerinin Karşılaştırmalı Analizi, Terazi Hukuk Dergisi, C. 13, S. 146, Kasım 2018, s. 50 vd. (ss. 48 – 60).

eleştirilmiştir (18 U.S.C. § 1030 (a)(5)(A)(i)).<sup>723</sup> Virüs yazımının, her ne kadar anti sosyal bir davranışa işaret etse de, cezalandırılmamasının en kuvvetli gerekçesi virüslerin faydalı amaçlar için de kullanılabileceği, faydalı amaç ile zararlı amacın yazım aşamasında ayırt edilmesinin olanaklı olmadığıdır. Ancak maksadın açık bir şekilde ortaya konulduğu durumlarda, örneğin zararlı yazılım oluşturma kitlerinin ticaretinde olduğu gibi cezalandırılmanın gerekli olduğu ifade edilmiştir.<sup>724</sup>

Zararlı yazılım oluşturma ve bulundurma eylemlerinin cezalandırılmasında fizik dünyada silah kontrolüne ilişkin düzenlemelerden hareketle birtakım görüşler de ileri sürülmüştür. Öncelikle belirtelim ki, zararlı yazılımların oluşturulması ve bulundurulması eylemlerinin suç oluşturup oluşturmadığı konusunda iki farklı eğilim oluşmuştur. Birinci eğilim, yasa dışı hareket üzerine odaklanması, zararlı yazılımın sadece oluşturulması ve bulundurulmasının suç olarak düzenlenmemesi gerektiği yönündedir.<sup>725</sup> Bu kapsamda zararlı yazılımların, ruhsatsız silah gibi düşünülerek bulundurulmasının yasaklanması gerektiği de ifade edilen diğer bir görüştür.<sup>726</sup>

Zararlı yazılımların silah olarak kabul edilmesine ilişkin özellikle uluslararası hukukta başlayan ve ulusal hukuklara da sirayet eden bir tartışma mevcuttur. 2010 yılında İran'a yönelik Stuxnet saldırısı sonrasında, başka bir ülkenin bilişim sistemlerine yapılan saldırıların Birleşmiş Milletler Sözleşmesi'nin 51'nci maddesinde yer alan "silahlı saldırı" niteliğinde olup olmadığı yönündeki farklı görüşler, kullanılan zararlı yazılımların "silah" olarak kabul edilip edilmeyeceği noktasına yoğunlaşmıştır.<sup>727</sup>

---

<sup>723</sup> **Cesare, Kelly**: Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution, *The Transnational Lawyer*, Vol. 14, 2001, s. 141 (ss. 136 – 170);

<sup>724</sup> **Kroczyński, Robert J.**: Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited?, *Fordham Intell. Prop. Media & Ent. L. J.*, Vol. 18, 2008, s. 845 (ss. 817 – 865).

<sup>725</sup> **Wang, Qianyum**: A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and Council of Europe, Ph.D. Thesis, Erasmus University, Rotterdam 2016, s. 91.

<sup>726</sup> **Downing, Richard**: Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime, *43 Colum. J. Transnat'l L.* 705, (2005), S. 733 (ss. 705 – 762).

<sup>727</sup> Bu konudaki temel tartışmalar için bkz. **Brown, Gary D. / Metcalf, Andrew O.**: Easier Said Than Done: Legal Review of Cyber Weapons, *Journal of National Security Law & Policy*, Vol. 7, 2014, ss. 115 – 138; **Denning, Dorothy**: Reflections on Cyberweapons Controls, *Computer Security Journal*, Vol. XVI, No. 4, Fall 2000, ss. 43 – 53; **Dévai Dóra**, Proliferation of Offensive Cyber Weapons. Strategic Implications and Non – Proliferation Assumptions, *AARMS* Vol. 15, No. 1, 2016, ss. 61 – 73; **Peterson, Dale**: Offensive Cyber Weapons: Construction, Development, and Employment, *The Journal of Strategic Studies*, Vol. 36, No. 1, 2013, ss. 120 – 124; **Maitra, Amit K.**: Offensive Cyber-Weapons: Technical, Legal, and Strategic Aspects, *Environ Syst Decis*, Springer 2014.

Uluslararası hukuktaki bu tartışmalar ulusal hukuklarda da karşılığını bulmuştur. Özellikle sanal ortamın silahlandırılması ifadesi ile sanal ortamda suç işlemek için kullanılan cihazların başka bir anlatımla donanımın yanı sıra yazılımın da kapsama alındığı ifade edilmiştir.<sup>728</sup> Dolayısıyla ateşli silahların üretimi, ticareti ve bulundurulmasının kontrolü için uygulanan yasal tedbirlerin, ateşli silahlarla işlenen suçları azaltmasından hareketle zararlı yazılımların bulundurulması ve ticaretinin de, bilişim suçlarında azalmaya yol açacağı ileri sürülmüştür.<sup>729</sup> Zararlı yazılımlar bünyesinde suç yaratıcı riskler taşımaktadır. Bunlar arasında elde edilmesinin ve kullanımının göreceli kolay, ancak sonuçlarının ciddi etkiler bırakacak olması sayılabilir. Bu, özellikle söz konusu zararlı yazılımlara talebi artıracaktır. Ayrıca zararlı yazılımların, sınır denetimleri olmaksızın ülkelere kolaylıkla girmesi, amaçları belli olmayan kişilerin elinde bulunması da olası suçlar için imkan sunmaktadır.<sup>730</sup> Bu tartışmaların ışığında bilişim suçları işlemek için kullanılan zararlı yazılımların oluşturulması, test edilmesi, dağıtımı ve satışının lisansa bağlanması, belirlenen zararlı yazılımların bunun dışında bulundurulması, satışı ve dağıtımının ceza kanunlarda suç olarak düzenlenmesi, DDoS saldırılarında kullanılan botnet yazılımlarında olduğu gibi bazı zararlı yazılımların yasa dışı bir amaç güdüp gütmeyeceğine bakılmaksızın yasaklanması gibi tedbirler önerilmiştir.<sup>731</sup>

Zararlı yazılımların düzenleme altına alınmasında kanaatimizce karşılaşılabilecek en büyük zorluk, söz konusu zararlı yazılımların nasıl tasnif edileceğidir. Öğretide zararlı yazılımların saldırı amaçlı kullanılanlar, savunma amaçlı kullanılanlar ve her iki amaçlı da kullanılabilir olanlar şeklinde tasniflenmesi yönünde görüşler ileri sürülmüştür.<sup>732</sup>

Türk hukuku bakımından TCK'nın 6'ncı maddesinde yer alan "silah" tanımı incelendiğinde, genel olarak cismani varlığa sahip araçların silah olarak değerlendirildiği görülmektedir. İncelemiş olduğumuz çalışmaların hiçbirisinde, zararlı yazılımların silah olarak kabul edilip edilmeyeceğine değinilmediği gibi, incelemiş olduğumuz yargı kararlarında da bu hususa temas edilmemiştir.

---

<sup>728</sup> **Prunckun, Henry:** Weaponization of Computers, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018, s. 4.

<sup>729</sup> **Prunckun, Henry:** The Rule of Law: Controlling Cyber Weapons, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018, s.88 (Prunckun, Cyber Weapons olarak anılacaktır).

<sup>730</sup> **Prunckun,** Cyber Weapons, s. 89.

<sup>731</sup> **Prunckun,** Cyber Weapons, s. 95.

<sup>732</sup> **Prunckun,** Cyber Weapons, s. 96, 97.

Ancak özellikle bilişim sistemleri vasıtasıyla kontrol edilebilen fiziksel sistemlerin artması (SCADA) ve bilişim sistemlerindeki zararlı yazılımların fizik dünyada da etki doğurabilmesinden dolayı yakın bir zamanda bu husustaki tartışmaların da Türk hukukunda yer bulacağını söylemek gerçekten uzak bir değerlendirme olmayacaktır.

### c. Zararlı Yazılım Üretme, Bulundurma ve Ticaretini Yapma Fiillerinin Değerlendirilmesi

Bilişim suçlarının işlenmesinin önlenmesi, bilişim suç faillerinin bilişim suçlarını işleyecek donanım ve yazılımı üretmesi, tedarik etmesi ve bulundurmasının engellenmesi ve son olarak sanal yeraltı pazarındaki fiillerin müeyyideye bağlanması açısından hazırlık hareketi niteliğinde olan zararlı yazılı üretme, bulundurma ve ticaretini yapma fiillerinin ülke mevzuatlarında cezalandırılmaya başlandığı görülmektedir. Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi'nin<sup>733</sup> 6'ncı maddesinde "Cihazların Kötüye Kullanılması" (Misuse of Devices) başlığı altında, Sözleşmede düzenlenen bilişim suçlarının işlenmesi için kullanılmak üzere hazırlanan donanım ve yazılımların kullanım amacıyla üretilmesi, satışı, kullanım amaçlı tedarik edilmesi, kullanım amaçlı bulundurulması, ithal edilmesi, dağıtımı ve başka şekilde erişilebilir hale getirilmesi cezalandırılmaktadır.

Siber Suçlar Sözleşmesinin ilgili maddesi, bir cihaz, bilgisayar şifresi, erişim kodu veya benzeri veriyi suçun konusu haline getirmiştir. Genel olarak bakıldığında zararlı yazılımların "benzer veri" (similar data) kapsamında değerlendirileceği söylenebilir. Ancak "cihaz" (device) ibaresinin donanım ve yazılımı da kapsayan bir ifade olduğu ve zararlı yazılımların bu kapsamda değerlendirilmesi gerektiği genel olarak ifade edilmektedir.<sup>734</sup>

Gerek 6'ncı maddenin 2'nci fıkrası gerek hazırlık çalışmaları gerekse Açıklayıcı Rapora bakıldığında bu alanda ikinci tartışmalı husus hem suç aracı olarak kullanılabilir hem de aynı zamanda bilişim sistemlerinde yasal amaçlı kullanılabilir olan yazılımların (dual use), madde kapsamına dâhil olup olmadığıdır. Açıklayıcı Rapora göre Sözleşmenin oluşturulması aşamasında bazı hususlar tartışılmıştır. Bunlardan biri yaptırım altına alınacak donanım ve yazılımların

---

<sup>733</sup> Sözleşme TBMM tarafından 22.4.2014 tarih ve 6533 sayılı Kanun ile kabul edilmiş olup, 2.5.2014 tarih ve 28988 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

<sup>734</sup> **Walden, Ian:** Computer Crimes and Digital Investigations, Oxford University Press, New York 2007, s. 193; **Clough, Johathan:** Principles of Cybercrime, Cambridge University Press, 2010, s. 120; **Viano, Emilio C.:** Cybercrime: Definition, Typology, and Criminalization, in: Cybercrime, Organized Crime and Societal Responses, International Approaches (Ed. Emilio C. Viano), Springer 2017, s. 11.

münhasıran suç işlemek amacına özgülenmesinin aranıp aranmayacağıdır. Münhasıran suç işlemek amacına özgülenmesinin aranması durumunda aşılamayacak ispat problemleri ile karşılaşılabilirdiğinden, bu öneri taraftar bulmamıştır. İkinci olarak yasal amaçlarla üretilip üretilmediğine bakılmaksızın suç işlemek tüm cihazların kapsama alınması da, belirsizliklere yol açabileceği ve kavramın çok geniş olmasından dolayı kabul görmemiştir. Bu kapsamda orta bir yol bulunmuş ve cihazın bilişim suçlarını işleme amacıyla oluşturulması, bulundurulması, ticareti aranmış ancak sadece sübjektif unsura yer verilmemiş aynı zamanda ilgili cihazın da objektif olarak ilgili suçu işleyecek şekilde oluşturulması veya uyarlanması gerektiği ifade edilmiştir.<sup>735</sup> Dolayısıyla Avrupa Konseyi Siber Suçlar Sözleşmesinin bu kapsamda karma teoriyi benimsediği söylenebilir.

Yasal veya yasadışı kullanıma uygun olarak donanım ve yazılım araçlarına web sitesi yükleme kapasite test yazılımları (website load capacity testing) verilebilir. Bunlar web sitesi sahibine kaynaklarını etkin şekilde kullanma ve bu şekilde talepleri karşılama olanağı verirken, aynı zamanda hizmetin engellenmesi (denial of service) saldırıları için de kullanılabilir. Benzer şekilde otomatik sızma test yazılımları (automated penetration testing), bilişim sisteminin sızma testlerini yapmak için kullanılabilirdiği gibi, bir bilişim sistemine hukuka aykırı olarak erişme için de kullanılabilir.<sup>736</sup> Fidyeye virüslerin bir zararlı yazılım türü olduğu yukarıda ifade edilmişti. Bu kapsamda fidye virüsler veya fidye virüs oluşturma kitlerinin birden fazla kullanıma uygun olmadığı, bunların Siber Suçlar Sözleşmesi'nin 6'ncı maddesi kapsamına giren cihazlar olduğu hususu genel olarak kabul görmektedir.<sup>737</sup>

Zararlı yazılımların üretilmesi ve bulundurulması birçok ülke mevzuatında da, Siber Suçlar Sözleşmesine paralel olarak düzenlenmiştir. Avustralya'da, Ceza Kanunu'nun 478.3 maddesinde, Nitelikli Bilgisayar Suçlarını düzenlenen 477'nci Bölümde yer alan suçların işlenmesi veya işlenmesinin kolaylaştırılması amacıyla verinin bulundurulması veya kontrol edilmesi suç olarak kabul edilmiştir. Burada yer alan veri kavramının kapsamına sadece şifre ve parolalar değil, zararlı yazılımlar da girmektedir. Benzer şekilde 478.4 maddesinde de, verinin üretimi, tedariki ve elde edilmesi yaptırımı bağlanmıştır.<sup>738</sup> Birleşik Krallık'ta Bilgisayarın Kötüye Kullanılması

---

<sup>735</sup> Bu husustaki tartışmalar için bkz. **Wang**, s. 92; **Downing**, s. 734; **Clough**, s. 122.

<sup>736</sup> Örnekler için bkz. **Sommer, Peter**: Criminalising Hacking Tools, Digital Investigation, Vol. 3, 2006, s. 70 (ss. 68 – 72).

<sup>737</sup> **Sommer**, s. 69.

<sup>738</sup> **Clough**, s. 123, 124.



Yasası'na, 2006 yılında Siber Suçlar Sözleşmesi'nin 6'ncı maddesi kapsamında uyumlaştırma amacıyla eklenen 3A maddesi ile zararlı yazılımların üretilmesi, uyarlanması, sağlanması ve sağlanmasının teklif edilmesi cezalandırılmıştır.<sup>739</sup> Benzer şekilde Hollanda Bilgisayar Suçları Kanunu'nun 139d maddesi<sup>740</sup>, Macar Ceza Kanunu'nun 424.1 maddesi<sup>741</sup>, Litvanya Ceza Kanunu'nun 198/2 maddesi<sup>742</sup>, Siber Suçlar Sözleşmesinin 6'ncı maddesine benzer şekilde zararlı yazılımların üretilmesi, bulundurulması ve ticaretini yaptırım altına almıştır.

Siber Suçlar Sözleşmesi'nin iç hukuka aktarılmasından sonra özellikle Sözleşme ile iç hukukun uyumlaştırılması kapsamında, TCK'na 245a maddesi eklenmiştir.<sup>743</sup> Söz konusu maddeye göre Bilişim Alanında Suçlar başlıklı Onuncu Bölümde ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imali, ithali, sevki, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması cezalandırılmıştır. Madde geniş bir şekilde kaleme alınmış ve bilgisayar programlarına da maddede açıkça yer verilmiştir. Bu kapsamda fidye virüsün, bilişim sistemlerindeki verilere veya sisteme zarar vermek amacıyla oluşturulması, ticarete konu edilmesi ve bulundurulması TCK m. 245a kapsamında cezalandırılacaktır.<sup>744</sup>

### C. TCK m. 244/2 SİSTEMDE YER ALAN VERİLERİ ERİŞİLMEZ KILMA SUÇ TİPİ

Fidye yazılımın yayılmasından önceki aşama olan virüsün oluşturulması, tedariki, bulundurulması eylemlerinin ayrı bir suç olarak değerlendirildiğini yukarıda belirttik. Fidye virüs ikinci aşamada hedef bilişim sistemine yerleşmektedir. Fidye yazılım önce kendisini mağdurun bilişim sistemine yerleştirmektedir. Bunu çok yaygın bir yöntem olarak sosyal mühendislik<sup>745</sup>

---

<sup>739</sup> Clough, s. 128.

<sup>740</sup> Koops, B. J.: Cybercrime Legislation in the Netherlands, Electronic Journal of Comparative Law, Vol. 14.3, December 2010, [www.ejcl.org](http://www.ejcl.org), Erişim Tarihi: 02 Nisan 2019.

<sup>741</sup> Mezei, Kitti: The Regulation of Crimes Against Information Systems in Hungary, Journal of Eastern – European Criminal Law, No. 2, 2017, s. 210 (ss. 203 – 216).

<sup>742</sup> Sauliūnasi, Darius: Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime, Jurisprudence, 2010, 4 (122), s. 213 (ss. 203 – 219).

<sup>743</sup> 24.03.2016 tarih ve 6698 sayılı Kanun'un 30'uncu maddesi ile.

<sup>744</sup> Bu konuda bkz. Korkmaz, İbrahim: Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu, Terazi Hukuk Dergisi, Vol. 13, Sayı 142, Haziran 2018, ss. 45 – 55.

<sup>745</sup> “Sosyal mühendislik, bilgi sistemlerini tehlikeye atabilecek kullanıcıları bulma sanatıdır. Sistemlere yapılan teknik saldırılar yerine, sosyal mühendisler bilgiye erişimi olan insanları hedef alır ve gizli bilgileri

saldırısı ile gerçekleştirmektedir. Mağdurun elektronik postasına ilgisini çekecek bir belge (çoğunlukla hizmet aldığı telefon şirketinden gelen yüksek bir fatura) gönderilmekte ve mağdurun söz konusu belgeye “tıklaması” suretiyle virüsün, mağdurun bilgisayarına indirilmesi gerçekleşmektedir.

Fidye yazılımda, fidye yazılımı gönderen fail, mağdur bilişim sistemine hukuka aykırı olarak erişmemektedir. Bu bakımdan fidye yazılımların kullanılmasında, bilişim sistemine hukuka aykırı erişim suçu (TCK m. 243/1) normal şartlar altında oluşmayacaktır. Bununla birlikte fidye yazılımın sisteme yerleştirilme şekline göre, bilişim sistemine hukuka aykırı erişim suçunun da oluşabileceği düşünülecektir. Örneğin bilişim sistemine fiziksel olarak erişip, taşınabilir bellek vasıtasıyla fidye yazılımın yüklenmesi veya bilişim sistemine hukuka aykırı erişerek, sisteme fidye yazılımın yerleştirilmesi durumunda ayrıca bilişim sistemine hukuka aykırı erişim suçunun oluşacağı söylenebilecektir.

Fidye yazılımın yüklenmesi aşamasında mağdurun bilişim sistemine veri yerleştirilmektedir. Dolayısıyla TCK m. 244/2’de yer alan sisteme veri yerleştirme suçunun olduğu söylenebilecektir. Fidye yazılım mağdur tarafından “tıklanmak” suretiyle indirildiğinden dolayı herhangi bir suçun oluşmadığı düşünülebilir. Çünkü TCK m. 244/2 bağlamında tipik hareket, verinin başkasının sistemine yerleştirilmesidir. Ancak burada mağdur, zararsız bir elektronik posta görüntüsü ile kandırılmakta ve suçu oluşturan (sisteme veri yerleştirme TCK m. 244/2) hareket, bizzat mağdurun kendisine yaptırılmaktadır.

Burada fidye yazılımı mağdurun bilişim sistemine yerleştirmek isteyen fail, araç durumunda bulunan mağdurun üzerindeki hâkimiyetini, mağdurda sebebiyet verdiği bir noksandan faydalanarak kurmaktadır. Başka bir anlatımla fidye yazılımı kendi bilişim sistemine yerleştiren mağdur, araç durumundaki kişidir ve hataya düşürülmek suretiyle hareketi gerçekleştirmektedir. Her ne kadar mağdurun gerçekleştirmiş olduğu hareket tipik değilse de, nitekim kendi bilişim sistemine kişinin kendi veri yerleştirmesi TCK m. 244/2’yi oluşturmamaktadır, aracının hareketinin tipik olmadığı durumlarda hataya düşüren şahıs bakımından dolayı faillik gündeme gelebilecektir.<sup>746</sup>

---

*açığa çıkarmaları için onları yanıltır veya başlamış olan kötü niyetli saldırılarını tamamlamak için onları etki altına alır ve ikna eder.” Krombholz, Katharina - Hobel, Heidelinde - Huber, Markus – Weippl, Edgar: “Advanced Social Engineering Attacks” SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria, [https://www.academia.edu/23907997/Advanced\\_social\\_engineering\\_attacks](https://www.academia.edu/23907997/Advanced_social_engineering_attacks), Erişim Tarihi: 01 Nisan 2019.*

<sup>746</sup> **Koca**, Mahmut – **Üzülmez**, İlhan, Türk Ceza Kanunu Genel Hükümler, 10. Baskı, Ankara 2017, s. 456.

Kanaatimizce sosyal mühendislik saldırısı gerçekleştirerek, mağdurda oluşturduğu bir hata sonucu, fidye yazılım olduğu gizlemek suretiyle mağdurun kendi bilişim sistemine fidye yazılımı indirmesine sebebiyet veren arkadaki kişi TCK m. 244/2 bakımından dolaylı faildir. Burada TCK m. 244/1 oluşmamaktadır çünkü söz konusu yazılım sistem dosyalarını şifrelememekte, sistem çalışmasına devam etmektedir. Bazı fidye virüs türlerinde, bilişim sisteminin işleyişinin engellenmesi de söz konusu olabilmektedir. Örneğin Locker fidye virüs ailesine mensup olan Reveton, bulaştığı bilişim sistemini kilitlemekte ve kullanıcının bilişim sistemini kullanmasını engellemektedir.<sup>747</sup>

Bazı fidye virüslerin verileri şifrelemekle kalmayıp, deşifre verileri de sildiği bilinmektedir.<sup>748</sup> Örneğin 2017 yılında yayılan SerbRansom fidye virüsü, 500 dolar ödenene kadar her 5 dakikada bir enfekte etmiş olduğu sistemden rastgele bir dosyayı silmektedir.<sup>749</sup> Dolayısıyla fidye virüsün türüne göre TCK m. 244/2’de yer alan seçimlik hareketlerden “silme” hareketi de söz konusu olabilecektir.

#### **D. TCK m. 244/4 SİSTEMDE YER ALAN VERİLERİ ERİŞİLMEZ KILMA SURETİYLE HAKSIZ ÇIKAR SAĞLAMA SUÇ TİPİ**

Bir sonraki aşamada, sistemde yer alan verilerin erişilmez kılınmasından sonra, fail, mağdura ulaşarak, verilerine tekrar erişebilmesi için belli bir menfaati kendisine temin etmeye zorlamaktadır. Burada menfaat temini, verilerin hâlihazırda geçici gelecekte ise daimi olarak erişilmez kılınacağı tehdidi ile gerçekleştirilmektedir. Fail tarafından gelecekte gerçekleştirilecek kötülüğün konusu, mağdurun bazen özel hayatı bazen de malvarlığı bakımından önemi bulunan verileridir. Fail, söz konusu verilere, mağdur tarafından bir daha erişilemeyeceği beyanını gerçekleştirmektedir. Güçlü şifreleme sistemleri göz önüne alındığında, söz konusu beyanın, verilerine bir daha erişilememe tehlikesi yaşayan mağdur bakımından da ciddi bir kaygıya neden olacağı açıktır.

Bu aşamada meseleyi, sistemde yer alan veriye erişilmesinin imkânsız kılınması suretiyle mağdurdan menfaat temini edilmesi kapsamında dar açıdan ele alırsak, TCK m. 244/4’ün oluşumu düşünülebilir. Kanun koyucu, TCK m. 244/4’de yer alan suçu tali bir norm olarak düzenlemiş ve

---

<sup>747</sup> Rajput, s. 30.

<sup>748</sup> Liska / Gallo, s. 11.

<sup>749</sup> Rajput, s. 32.

eylemin başka bir suçu oluşturmaması durumunda TCK m. 244/4'ün oluşabileceğini belirtmiştir.<sup>750</sup> TCK m. 244/4'ün tali bir norm olmasından dolayı, başka bir suçun oluşup oluşmadığı hususu da incelenmelidir.

### **E. TCK m. 148 YAĞMA SUÇ TİPİ**

Fail, mağdura ait verileri şifrelemek suretiyle erişilmez kılmakta ve verilere tekrar erişemeyeceği beyanı ile menfaat temin etmektedir. Mağdur bakımından söz konusu verilerin malvarlığına dâhil olduğu ve bazı durumlarda verilerin kaybının, malvarlığı bakımından büyük bir zararı oluşturacağı hususu daha önce de ifade edildiği üzere olasıdır. Bu durumda, TCK m. 148'de yer alan yağma suçunun tatbiki de incelenmelidir. Yağma suçunda; *“bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden ya da malvarlığı itibarıyla büyük bir zarara uğratacağından bahisle tehdit ederek veya cebir kullanarak, bir malı teslim veya malın alınmasına karşı koymamaya mecbur kılınması”* gereklidir. Bu açıdan ilerleyen bölümlerde, yağma suçunun oluşup oluşmayacağı kısaca incelenecektir.

Fidyeye virüslerinde, verilerin kalıcı olarak erişilmez kılınacağı tehdidi ile mağdurdan kripto para temini eyleminin yağma suçunu oluşturup oluşturmadığı belirlenirken kanaatimizce iki husus açıklanmalıdır. Birinci olarak verilerin kalıcı olarak erişilmez kılınmasının, yağma suçunun oluşumu için tehdidin konusu bakımından *“mağdurun malvarlığı açısından büyük bir zarar”* oluşturup oluşturmayacağı meselesi çözümlenmelidir. İkinci olarak mağdur tarafından faile yapılan ödemede kullanılan kripto paranın, TCK m. 148'de yer alan *“bir malı teslim veya malın alınmasına karşı koymama”* kapsamında mal olarak değerlendirilip değerlendirilmeyeceği açıklanmalıdır.

Öncelikle suçun oluşması bakımından failin gerçekleştirdiği tehdit, verilerin kalıcı olarak erişilmez kılınacağına ilişkindir. Tehdidin konusu bazı durumlarda *“malvarlığı”* da olabilir. Nitekim sistemde yer alan veriler, malvarlığı değeri olarak da kabul görmektedir. Özellikle bankacılık sisteminde yer alan kaydı paralarda durum böyledir. Bankacılık sisteminde yer alan ve parasal anlamda malvarlığını, bilişim sistemlerinde yer alan veri temsil etmektedir. Malvarlığını temsil eden, mağdur açısından mali değeri olan bilişim sistemindeki verinin erişilmez kılınacağı yönündeki bir beyanın, genel bir kural olarak ifade edilemese de *“malvarlığı açısından büyük bir zarar”* oluşturması ihtimali mevcuttur. Benzer şekilde, *wannacry* örneğinde olduğu gibi sağlık sisteminde sağlık hizmeti alan kişilere ait veriler de, sağlık hizmeti veren birim bakımından

---

<sup>750</sup> Koca / Üzülmez, Özel Hükümler, s. 842.

malvarlığı açısından büyük bir zarar oluşturabilecektir. Nitekim söz konusu verilere ulaşılamaması sağlık hizmetinin sunulamamasına ve dolayısıyla da sağlık hizmeti veren birimin kazanç elde edememesine neden olmaktadır. Bu açıdan verilerin kalıcı olarak erişilemez kılınması tehdidi, malvarlığı açısından büyük bir zarar oluşturma tehdidi olarak değerlendirilebilecektir. Ayrıca yine wannacry örneğinde olduğu gibi çalışan bir sağlık tesisinden hizmet alan kişilere ait verilere ulaşılamaması, teşhis ve tedavi süreçlerini aksatacağından kişiler bakımından vücut bütünlüğü ve hatta yaşam bakımından da tehdit oluşturabilecek niteliktedir.

Tehdidin gerçekleştiğini tespit ettikten sonra “*malın teslimine veya malın alınmasına karşı koymamaya mecbur kılınması*” unsurunun gerçekleşip gerçekleşmediği değerlendirilmelidir. Yağma suçunda, her ne kadar sadece “*mal*” terimi kullanılmış ve söz konusu terimin “*taşınabilir*” olma özelliği belirtilmemişse de, gerek madde gerekçesinde gerekse de öğretide, yağma suçunun kanuni tanımında yer alan malın, “*taşınabilir mal*” olduğu konusunda görüşler mevcuttur.<sup>751</sup> Bu durumda fail tarafından temin edilen menfaatin [çoğunlukla kripto/elektronik para (bitcoin) şeklindedir] madde metninde geçen “*mal*” terimi kapsamında olup olmadığı değerlendirilmelidir. Öğretide bazı yazarlar tarafından verinin, hırsızlık suçunun konusunu oluşturan taşınabilir bir mal olmadığı ileri sürülmektedir.<sup>752</sup> Karşı görüşte olan yazarlar, internet bankacılığı üzerinden yapılan para göndermelerinde bilişim sistemlerinin araç olarak kullanıldığını, burada yer alan eylemin paranın mağdurun çantasından alınmasından bir farkının olmadığını belirtmektedirler.<sup>753</sup>

Yargıtay Ceza Genel Kurulu, kişilerin internet bankacılığı hesap şifrelerinin kullanılarak, hesaplarında yer alan parayı temsil eden verilerin, başka hesaplara nakledilmesi fiillerinde oluşan suçun “Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Hırsızlık” olduğunu

---

<sup>751</sup> **Tezcan**, Durmuş – **Erdem**, Mustafa Ruhan – **Önok**, R. Murat, Teorik ve Pratik Ceza Özel Hukuku, 12. Baskı, Ankara 2015, 656; **Koca / Üzülmmez**, Özel Hükümler, s. 585; **Malkoç**, İsmail, Açıklamalı Türk Ceza Kanunu, 2. Cilt, Ankara 2013, s. 2427; **Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar / Tepe, İlker**, Türk Ceza Hukuku Özel Hükümler, 13. Baskı, Ankara 2018, s. 656.

<sup>752</sup> Bkz. **Yazıcıoğlu**, Yılmaz, “Yeni Türk Ceza Kanunu’ndaki Bilişim Suçlarının Genel Değerlendirilmesi”, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.II, S.2, 2005, s. 398; **Özbek**, Veli Özer, “Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof.Dr. Ünal Narmanlıoğlu’na Armağan, C. 9, 2007, s. 1058; **Başbüyük**, İsa, “İnternet Bankacılığı Aracılığı ile Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi”, Ceza Hukuku Dergisi, Y. 8, S. 21, Nisan 2013, s. 199.

<sup>753</sup> **Kurt**, Levent, Açıklamalı ve İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara 2005, s. 169; Başbüyük, s. 199; **Taşkın**, Şaban Cankat, Bilişim Suçları, Bursa 2008, s. 116.

kararlaştırmıştır.<sup>754</sup> Yargıtay uygulaması söz konusu Ceza Genel Kurul kararından sonra da, benzer şekilde devam etmektedir.<sup>755</sup>

Yargıtay Ceza Genel Kurulu ve sonrasında ise özel dairelerin kararlarında yer alan veri, bankacılık bilişim sisteminde yer alan ve karşılığı para olarak temsil edilen bir veridir. Söz konusu verinin gönderilmesi durumunda, TCK m. 142/2-e veya TCK m. 244/2-4 kapsamında değerlendirilmesi noktasında görüş farklılıkları bulunmakla birlikte, inceleme konumuz olan olayda verilmesi istenen şey (bitcoin) bir sanal para çeşididir.<sup>756</sup> Sanal paraların kanuni düzenlemesi bulunmamakla beraber, günümüzde mal mübadelesinde kullanılmakta ve bir ekonomik değeri temsil etmektedir.

Kanaatimizce konuyu birbirinden farklı iki ihtimale göre ayırarak incelemek gereklidir. Öğretide yağma suçuna konu olan malın; “maddi bir varlığa sahip olma”, “hâkimiyete elverişlilik” ve “kişilik dışı olma” şeklinde üç özelliğinin bulunduğu ifade edilmektedir.<sup>757</sup> Kripto paraların<sup>758</sup> kişilik dışı ve hâkimiyete elverişli olduğu noktasında büyük bir tartışma olmadığı kanaatindeyiz. Ancak maddi bir varlığa sahip olup olmadığı değerlendirilmelidir. Kripto para belli algoritmalarla matematiksel işlemler sonucunda üretilen ve benzeri bulunmayan veri parçalarıdır. Söz konusu veriler, bilişim sistem araçlarında tutulabilmektedir. Bu bilişim sistem araçları, sisteme bağlı olduğu zaman “online - sıcak cüzdan”, sisteme kullanıcı tarafından istendiği zaman bağlı olduğunda “offline – soğuk cüzdan (cold wallet)” olarak adlandırılmaktadır. Soğuk cüzdanda kripto para çoğunlukla, bir veri taşıma aracında bulunmaktadır. Bu kapsamda kripto paranın, soğuk cüzdanda bulunması durumunda, söz konusu veri taşıma aracının içindeki kripto para ile birlikte mal olarak değerlendirileceği açıktır.<sup>759</sup> Sıcak cüzdanda, başka bir anlatımla sistem üzerinde manyetik veri olarak tutulduğunda, sadece bu verinin ekonomik değer olduğundan hareketle mal

---

<sup>754</sup> Yargıtay Ceza Genel Kurulu, 17.11.2009, 11-193/268.

<sup>755</sup> Yargıtay 13.CD, 11.4.2017, 2015/15567, 2017/3907; Yargıtay 17.CD, 20.6.2016, 2015/16533, 2016/9189; Yargıtay 22.CD, 13.6.2016, 2015/17809, 2016/10066.

<sup>756</sup> **Bozkurt Yüksel**, Armağan Ebru, “Elektronik Para, Sanal Para, Bitcoin ve Linden Doları’na Hukuki Bir Bakış”, İÜHFİM, C. LXXIII, S. 2, s 173-220, 2015, s. 197.

<sup>757</sup> **Koca**, Mahmut, Yağma Cürümleri, Ankara 2003, s. 92.

<sup>758</sup> “Kripto para; güvenliğin sağlanması için kriptografi (şifreleme bilimi) kullanan dijital veya sanal bir para birimidir. Bu paralar sanal cüzdanlara şifreler kullanılarak yerleştirilmekte ve aynı şekilde şifreler aracılığıyla kullanıldığı için de bu adı almaktadır.” **Günay, Furkan / Kargı, Veli**, “Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi”, Journal of Life Economics, C. 5, S. 3, Temmuz 2018, s. 62.

<sup>759</sup> Bu konuda benzer bir değerlendirme için bkz. **Sirmen**, Lale, Eşya Hukuku, 3. Bası, Ankara 2015, s. 5.

olarak kabul edilip edilemeyeceği hususunun bu kadar açık olmadığını ifade etmeliyiz. Hırsızlık suçunun konusunun taşınabilir mal olduğu değerlendirildiğinde<sup>760</sup>, Yargıtay'ın söz konusu verinin temsil ettiği değeri esas alarak ulaştığı sonuç göz önünde bulundurulduğunda, mağdurun kripto parayı teslim zorlanması durumunda da “yağma” suçunun oluşacağı söylenebilir. Ayrıca yağma virüslerde çoğunlukla, belli bir dolar karşılığı kripto para istendiğinden dolayı, teslim zorlananın mal olduğu da rahatlıkla söylenebilecektir.

5237 sayılı TCK'da Yağma suçunun, 765 sayılı TCK'nın aksine “Mal Aleyhine Cürümler” değil, “Malvarlığına Karşı Suçlar” arasında düzenlenmiş olması da, yukarıda varmış olduğumuz sonucun desteklenmesi açısından önemlidir. Nitekim 765 sayılı TCK'nın mehası olan Zanardelli Kanunu'nda “mal” kavramı kullanılmasına rağmen, Rocco Kanunu, mal teriminin yetersizliğinden hareketle “malvarlığı” (il patrimonio) terimini kullanmıştır.<sup>761</sup> Söz konusu tercih, Türk kanun koyucusu tarafından kabul görmüş ve 5237 sayılı Kanunda “Malvarlığı” terimi kullanılmıştır.<sup>762</sup> Kripto paraların da, kişinin malvarlığına dâhil olduğu ve bu anlamda da yağma suçunun konusunu oluşturabileceği kanaatindeyiz.

#### **F. ŞANTAJ SUÇU (TCK m. 107)**

Burada kısaca şantaj suçunun uygulanma olanağının bulunup bulunmadığı hususunu da değerlendirmek istiyoruz. Fidyeye virüslerde, fail, mağdura ait ve bazen özel hayat alanına ait olan verileri de şifrelemekte ve menfaat karşılığında mağdura verilerine tekrar erişme olanağı sunmaktadır. Mağdurun menfaat temin etmemesi durumunda, verilerine bir daha ulaşamayacağı tehdidini de gerçekleştirilmektedir.

TCK'nın 107'nci maddesinde düzenlenen şantaj suçunda; a. Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle çıkar sağlama ve b. Çıkar sağlamak amacı ile kişinin şeref ve saygınlığına zarar verecek nitelikteki hususların açıklanması veya isnat edilmesi yaptırım altına alınmıştır. Bu düzenleme, fidye virüslerin yarar sağlanması amacı ile yayılması dikkate alındığında, “yarar sağlama” noktasında uygulanabilir görünmektedir.<sup>763</sup>

---

<sup>760</sup> Değerlendirme için bkz. **Evik**, Ali Hakan, “Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Hırsızlık’ Suçuna İlişkin Bir Yargıtay Kararının Değerlendirilmesi, Köksal Bayraktar’a Armağan, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2010/1, C.1, s. 703 vd.

<sup>761</sup> **Hafizoğulları**, Zeki / **Özen**, Muharrem, Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar, Ankara 2016, s. 302

<sup>762</sup> **Taşkın**, Ahmet, “Yağma Suçunda Mal Kavramı”, Terazi Hukuk Dergisi, Nisan 2008, S. 20, s. 95.

<sup>763</sup> **Taner**, Fahri Gökçen, “Türk Ceza Hukukunda Şantaj Suçu”, Türkiye Barolar Birliği Dergisi, 2011 (92), s. 127 vd.

Kanaatimizce TCK'nın 107'nci maddesinin uygulanma olanağı fidye virüsler bakımından yoktur. Nitekim, fidye virüsler çıkar sağlamayı amaçlamakta ancak söz konusu çıkarı sağlamak için mağdurun verilerine erişememesi tehdidini gerçekleştirmektedir. Söz konusu durum fidye virüs faillerinin hakkı olan veya yükümlü olduğu bir durum olmadığından dolayı TCK m. 107/1'in uygulanma olanağı yoktur. Benzer şekilde TCK m. 107/2'de de, kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği düzenlenmektedir. Mağdurun, niteliği ne olursa olsun verilerine tekrar ulaşamaması ve buna yönelik tehdit, "hususun açıklanması veya isnadı" kapsamında değerlendirilemeyecektir. Hatta söz konusu verilere ulaşamadığından dolayı kişinin şeref ve saygınlığı doğrudan veya dolaylı olarak zarar görmüş olsa bile, fidye virüsler bakımından "açıklama veya isnat" söz konusu olmayacaktır.

#### IV. SUÇLARIN İÇTİMAİ KAPSAMINDA DEĞERLENDİRME

Son olarak durumu suçların içtimaî bakımından da ele almalıyız. Bilinmektedir ki, genel kural "*ne kadar fiil, o kadar suç*", "*ne kadar suç, o kadar ceza*" şeklindedir. Dolayısıyla öncelikle fiil/hareket<sup>764</sup> sayısının belirlenmesi gereklidir. Fidye virüsün, daha sonraki eylemler bakımından oluşturulması, bulundurulması ve ticareti, TCK m. 245a kapsamında bağımsız bir suç tipidir. Fidye virüsün daha sonra kullanılıp kullanılmayacağından bağımsız olarak, TCK m. 245a'nın olduğu ifade edilebilir.

Birinci adımda gerçekleştirilen ve mağdurun, sistemine veri eklenmesini sağlayan hareket ile mağdurun sistemine bulaşan virüsün sistemdeki veriyi şifrelemesindeki hareket "*doğal anlamda fiil tekliği*"<sup>765</sup> kapsamında değerlendirilemeyecek şekilde birbirinden farklıdır. Ancak "*sisteme veri yerleştirme*" ve "*sistemde yer alan veriyi erişilmez kılma*" hareketleri aynı suçun seçimlik hareketleri olduğundan ve aynı konu üzerinde işlendiği müddetçe seçimlik hareketlerin birden fazlasının icrası "*tipik fiil tekliği*" kapsamında değerlendirileceğinden tek bir suç oluşacaktır.

Sistemde yer alan verinin kalıcı olarak erişilmez kılınmasına yönelik tehdidin sonrasında kripto paranın temini durumunda, oluşabilecek suç tipine göre farklı sonuçlara varmak gereklidir. Kripto paranın mal olarak değerlendirilemeyeceği ve dolayısıyla TCK m. 148'in oluşmadığı düşünülürse, TCK m. 244/4 oluşacaktır. TCK m. 244/1 ve 2'de yer alan fiiller, TCK m. 244/4'ün

---

<sup>764</sup> Bu konuda detaylı açıklamalar ve teoriler için bkz. **Göktürk**, Neslihan, Fikri İctima, Ankara 2013, s. 17 vd.

<sup>765</sup> **Göktürk**, s. 99.



unsuru olduğundan dolayı ayrıca cezalandırılmayacaktır. Ancak TCK m. 148'in olduğu düşünülürse, yağma suçu da bileşik bir suç olduğundan dolayı bünyesinde yer alan tehdit suçundan dolayı ayrıca cezalandırma yapılmayacaktır. Eğer TCK m. 244/4 ve TCK m. 148'in beraber olduğu düşünülecek olursa, TCK m. 244/4'ün tali norm olmasından dolayı TCK m. 148 uygulanacaktır.

#### **IV. SONUÇ VE DEĞERLENDİRME**

Zararlı yazılım yasa dışı pazarı, vaat ettiği kazanca paralel olarak büyümekte ve karmaşıklaşmaktadır. Daha önceleri basit birkaç zararlı etkiye sahip virüslerle karşılaşılırken, bugün yayılmasından, sistemi enfekte etmesine; zararlı yazılım faili ile iletişim kurmasından, menfaatin belirlenmesine kadar karmaşık ve bir o kadar da mağdurun savunmasını zayıflatan virüslerle karşı karşıyayız.

Bu çalışmada farklı bir açıdan ele almak istediğimiz cryptolocker özelinde fidye yazılımlar, yayılmasından menfaatin temini aşamasına kadar farklı suçların oluşumuna sebebiyet vermektedir. Bu kapsamda virüsün temini veya üretimi açısından TCK m. 245a maddesinin oluşumu düşünülebilecektir. Nitekim karmaşık bir yapıya ve farklı bir modus operandiye sahip olan virüs, bireysel üretimin yerine sanal yeraltı pazarlarından temin edilmektedir. Söz konusu sanal yeraltı pazarlarında virüsün yazımı, üretime hazır hale getirilmesi, yerleştirilmesi ve hatta menfaatin temini aşamasına kadar hizmetler de sunulmaktadır.

İkinci olarak virüsün, mağdurun sistemine yerleştirilmesinde mağdurun iradesinin yanıtılarak sisteme yerleştirme hareketinin mağdura yaptırıldığını görmekteyiz. Bu durumda TCK m. 244/2'de yer alan sisteme veri yerleştirme hareketi söz konusudur ancak zararlı yazılım failinin sorumluluğu dolaylı fail şeklinde olacaktır.

Üçüncü aşamada sistemin enfekte edilerek bazı verilerin ulaşılmaz kılınması söz konusudur. Bu aşamada ise TCK m. 244/2'de yer alan seçimlik hareketlerden biri olan "sistemde yer alan verinin erişilmez kılınması" gündeme gelebilecektir. Bazı fidye virüslerin, sistemin çalışmasını da etkilediği bilindiğinden TCK m. 244/1'in oluşumu da olası olacaktır.

Sistemi enfekte eden fidye virüs, söz konusu erişilmez kılınmanın daimi olacağı tehdidi ile menfaati temin etmeye çalışmaktadır. Menfaat çoğunlukla belli bir para karşılığı olan kripto paradır. Burada ise yukarıda belirttiğimiz esaslar kapsamında yağma suçunun oluşacağı kanaatindeyiz.

## KAYNAKÇA

**Ablon, Lilian / Libicki, Martin C. / Golay, Andrea A.:** Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar, RAND 2014, s. 3 – 19.

**Başbüyük, İsa,** “İnternet Bankacılığı Aracılığı ile Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi, Ceza Hukuku Dergisi, Y. 8, S. 21, Nisan 2013.

**Bozkurt Yüksel,** Armağan Ebru, “Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış”, İÜHFİM, C. LXXIII, S. 2, s 173-220, 2015.

**Brown, Gary D. / Metcalf, Andrew O.:** Easier Said Than Done: Legal Review of Cyber Weapons, Journal of National Security Law & Policy, Vol. 7, 2014, ss. 115 – 138.

**Cesare, Kelly:** Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution, The Transnational Lawyer, Vol. 14, 2001, s. 141 (ss. 136 – 170).

**Clough, Johathan:** Principles of Cybercrime, Cambridge University Press, 2010, s. 120;  
**Viano, Emilio C.:** Cybercrime: Definition, Typology, and Criminalization, in: Cybercrime, Organized Crime and Societal Responses, International Approaches (Ed. Emilio C. Viano), Springer 2017.

**Denning, Dorothy:** Reflections on Cyberweapons Controls, Computer Security Journal, Vol. XVI, No. 4, Fall 2000, ss. 43 – 53.

**Dévai Dóra,** Proliferation of Offensive Cyber Weapons. Strategic Implications and Non – Proliferation Assumptions, AARMS Vol. 15, No. 1, 2016, ss. 61 – 73.

**Dolliver, D.S. / Kenney, J.L.:** Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison, in: Victim & Offenders, Taylor & Francis Group, 2016, s. 601, 602 (ss. 600 – 620).

**Downing, Richard:** Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime, 43 Colum. J. Transnat'l L. 705, (2005), (ss. 705 – 762).

**Evik, Ali Hakan,** “Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Hırsızlık' Suçuna İlişkin Bir Yargıtay Kararının Değerlendirilmesi, Köksal Bayraktar'a Armağan, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2010/1, C.1.

**Flint, David,** Law Shaping Technology: Technology Shaping the Law, International Review of Law, Computers and Technology, Vol. 23, No. 1 – 2, March – July 2009, s. 5 – 11.

**Göktürk**, Neslihan, Fikri İçtima, Ankara 2013.

**Günay, Furkan / Kargı, Veli**, “Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi”, Journal of Life Economics, C. 5, S. 3, Temmuz 2018.

**Hafizoğulları, Zeki / Özen**, Muharrem, Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar, Ankara 2016.

**Hugher, Thomas P.**, Technological Momentum, in: Does Technology Drive History? The Dilemma of Technological Determinism (Edited by Merritt Roe Smith and Leo Marx), Cambridge, MIT Press, 1994.

**Kharraz, Amin / Robertson, William / Balzarotte, Davide / Bilge, Leyla / Kirda, Engin:** Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, M. Almgren et al. (Eds.): DIMVA 2015, LNCS 9148, pp. 3–24, Springer 2015.

**Koca, Mahmut – Üzülmöz, İlhan**, Türk Ceza Kanunu Genel Hükümler, 10. Baskı, Ankara 2017, s.

**Koca, Mahmut**, Yağma Cürümleri, Ankara 2003.

**Koops, B. J.:** Cybercrime Legislation in the Netherlands, Electronic Journal of Comparative Law, Vol. 14.3, December 2010, [www.ejcl.org](http://www.ejcl.org), Erişim Tarihi: 02 Nisan 2019.

**Korkmaz, İbrahim:** Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu, Terazi Hukuk Dergisi, Vol. 13, Sayı 142, Haziran 2018, ss. 45 – 55.

**Kroczyński, Robert J.:** Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited?, Fordham Intell. Prop. Media & Ent. L. J., Vol. 18, 2008, (ss. 817 – 865).

Krombholz, Katharina - Hobel, Heidelinde - Huber, Markus – Weippl, Edgar: “Advanced Social Engineering Attacks” SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria, [https://www.academia.edu/23907997/Advanced\\_social\\_engineering\\_attacks](https://www.academia.edu/23907997/Advanced_social_engineering_attacks), Erişim Tarihi: 01 Nisan

**Kurt, Levent**, Açıklamalı ve İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara 2005.

**Liska, Allan / Gallo, Timothy:** Ransomware Defending Against Digital Extortion, O’Reilly, 2017.

**Mabunda, Sagwadi:** Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill, Statute Law Review, 2017.

**Maitra, Amit K.:** Offensive Cyber-Weapons: Technical, Legal, and Strategic Aspects, Environs Syst Decis, Springer 2014.

**Malkoç, İsmail,** Açıklamalı Türk Ceza Kanunu, 2. Cilt, Ankara 2013.

**McLuhan, Marshall,** Understanding Media: The Extension of Man, McGraw Hill, New York 1996.

**Mezei, Kitti:** The Regulation of Crimes Against Information Systems in Hungary, Journal of Eastern – European Criminal Law, No. 2, 2017, (ss. 203 – 216).

**Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar / Tepe, İlker,** Türk Ceza Hukuku Özel Hükümler, 13. Baskı, Ankara 2018.

**Özbek, Veli Özer,** “Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu”, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof.Dr. Ünal Narmanlıoğlu’na Armağan, C. 9, 2007.

**Paquet – Clouston, Masarah / Haslhofer, Bernhard / Dupont, Benoît:** Ransomware Payments in the Bitcoin Ecosystem, The 17th Annual Workshop on the Economics of Information Security (WEIS), June 2018, Innsbruck, Austria.

**Pascariu, Cristiona / Barbu, Ionut – Daniell / Bacivarov, Ioan C.:** Investigative Analysis and Technical Overview of Ransomware Based Attacks.Case Study: WannaCry, International Journal of Information Security and Cybercrime, Vol. 6, Issue 1, 2017, s. 57 (ss. 57 – 62).

**Perloff – Giles, Alexandra:** Transnational Cyber Offences: Overcoming Jurisdictional Challenges, 43 Yale J. Int’lL. (2018), s. 197 (ss. 191 – 227).

**Peterson, Dale:** Offensive Cyber Weapons: Construction, Development, and Employment, The Journal of Strategic Studies, Vol. 36, No. 1, 2013, ss. 120 – 124.

**Prunckun, Henry:** The Rule of Law: Controlling Cyber Weapons, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018, (Prunckun, Cyber Weapons olarak anılacaktır).

**Prunckun, Henry:** Weaponization of Computers, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018.

**Rajput, Toshima Singh:** Evolving Threat Agents: Ransomware and their Variants, International Journal of Computer Applications, Vol. 164, No. 7, April 2017, s. 28 vd. (ss. 28 – 34).

**Richardson, Ronny / North, Max M.:** Ransomware: Evolution, Mitigation and Prevention, International Management Review, Vol.13, No.1, 2017, s. 12 (ss. 10 – 21).

**Sauliūnasi, Darius:** Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime, *Jurisprudence*, 2010, 4 (122), (ss. 203 – 219).

**Shaw, Malcolm N.:** *International Law*, 6 th Edition, Oxford University Press 2008, s. 1; Bakınız aynı şekilde **Kettemann, Matthias C.:** Ensuring Cybersecurity Through International Law, 69 R.E.D.I. 281, 2017, s. 281 (ss. 281 – 289).

**Sherer, James A. / McLellan, Melinda L. / Fedeles, Emily R. / Sterling, Nichole L.:** Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web, *Richmond Journal of Law & Technology*, Vol. XXIII, Issue 3, s. 1 (ss. 1 – 48).

**Sirmen, Lale,** Eşya Hukuku, 3. Bası, Ankara 2015.

**Sommer, Peter:** Criminalising Hacking Tools, *Digital Investigation*, Vol. 3, 2006, (ss. 68 – 72).

**Taner, Fahri Gökçen,** “Türk Ceza Hukukunda Şantaj Suçu”, *Türkiye Barolar Birliği Dergisi*, 2011 (92) (ss. 118 – 156).

**Taşkın, Şaban Cankat,** Bilişim Suçları, Bursa 2008.

**Taşkın, Ahmet,** “Yağma Suçunda Mal Kavramı”, *Terazi Hukuk Dergisi*, Nisan 2008, S. 20.

**Tekin, Derya:** Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerinin Karşılaştırmalı Analizi, *Terazi Hukuk Dergisi*, C. 13, S. 146, Kasım 2018, (ss. 48 – 60).

**Tezcan, Durmuş – Erdem, Mustafa Ruhan – Önok, R. Murat,** Teorik ve Pratik Ceza Özel Hukuku, 12. Baskı, Ankara 2015.

**TK, Anjana:** Discussion on Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks, *IJRTI*, Vol. 2, Issue 6, 2017, s. 210 (ss. 210 – 214).

**Volokh, Eugene:** Akademik Metinler Nasıl Yazılır? Hukukçular için Rehber (Çev.: Ertuğrul Uzun), Tekin Yayınları İstanbul 2019.

**Walden, Ian:** *Computer Crimes and Digital Investigations*, Oxford University Press, New York 2007.

**Wang, Qianyum:** A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and Council of Europe, Ph.D. Thesis, Erasmus University, Rotterdam 2016.

**Yazıcıoğlu, Yılmaz,** “Yeni Türk Ceza Kanunu’ndaki Bilişim Suçlarının Genel Değerlendirilmesi”, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, C.II, S.2, 2005.

## YILLIK ÜCRETLİ İZİN <sup>766</sup>

### ANNUAL PAID LEAVE

*Mustafa TUGAY*

#### ÖZ

Anayasa ile güvence altına alınmış olan yıllık ücretli izin hakkı, ekonomik ve sosyal bir haktır. Yıllık ücretli izin süresince yorgunluğunu gidererek dinlenen işçiye, aynı zamanda bu döneme ait ücreti ödenerek geçim kaygısı içine düşmemesi sağlanmaktadır. Dinlenmiş olarak işine dönen işçinin böylelikle hem sağlığının korunması ve hem de işgücünün yenilenmesi suretiyle verimliliğinin artması ve iş kazalarının azalması mümkün olmaktadır. Bu nedenle yıllık ücretli izin hakkının iş sözleşmesinin devamı sırasında ücreti de ödenerek, fiilen kullandırılması ülke çıkarları açısından büyük önem arz etmektedir. Ancak iş yaşamında konunun öneminin işçiler ve işverenler tarafından yeterince önemsenmediği bilinen bir vakıdır. Belirtilen nedenlerle yıllık ücretli izin hakkının yasaca öngörüldüğü şekilde, kullandırılmasını sağlayacak denetim önlemlerinin alınması veya sıkılaştırılması gerek iş ilişkisinin tarafları ve gerekse ülke menfaatleri açısından kaçınılmaz görülmektedir.

**Anahtar Kelimeler:** Yıllık Ücretli İzin, Anayasal Hak, İzin Kullandırma Zorunluluğu, İşçi Sağlığının Korunması, İzinde Çalışma Yasağı, İzin Hakkının Vazgeçilmezliği

#### ABSTRACT

The right to paid annual leave secured by the Constitution is an economic and social right. During the paid annual leave the employee who rest gets paid during this period to ensure not to fall into livelihood anxiety. By that, It is possible to see increase on work efficiency and reduction on workplace accidents for the workers who return to their jobs rested by both protecting their health and renewal of workforce. For this reason, during the continuation of the employment contract paying the wage during the annual leave of the employee is of great importance for the benefit of the country. However, it is a known fact that the importance of this subject in business life is not cared enough neither by workers nor by employers. For the reasons mentioned, it is important to

---

<sup>766</sup> ORCID: <https://orcid.org/0000-0003-3127-2423>

take necessary precautions and to conduct frequent audits to make sure paid annual leave rights are used as the way stated in the law for the benefit of the country and for the sides of the business.

**Keywords:** Annual Paid Leave, Constitutional Right, Obligation for Leave, Employee Health Protection, Prohibition to Work on Leave, Indispensable of Leave Right.

\*\*\*\*

## I- YILLIK ÜCRETLİ İZİN KAVRAMI ve YASAL TEMELLERİ

### A- TANIMI

İş Hukukunda yıllık ücretli izin kavramının birçok farklı tanımı yapılmıştır. Buna göre genel olarak yıllık ücretli izin, işçilerin dinlenmelerini sağlamak amacıyla, belli bir zaman dilimi için çalışma yükümlülüklerinden kurtarılmalardır<sup>767</sup>. Başka bir tanıma göre ise yıllık ücretli izin, işçilerin kanun, sözleşme, örf ve âdete göre belirlenmiş olan şartları yerine getirmeleri koşuluyla, çalışma sürelerinin içinde ücretlerinden herhangi bir kesinti yapılmaksızın serbest kalmalarını sağlayan, vazgeçilmesi ve devredilmesi mümkün olmayan, kişiye bağlı bir haktır<sup>768</sup>. Bir diğer tanıma göre ise yıllık ücretli izin, belirli bir bekleme süresini tamamlayarak yorulan ve halen iş görebilir durumdaki işçiye, birbirini takip eder şekilde ve kural olarak bölünmeden, ücretli olarak sağlanan yıllık dinlenme olanağıdır<sup>769</sup>.

### B- HUKUKİ NİTELİĞİ

Yıllık ücretli izin hakkının hukuki niteliği hakkında, tarihsel süreçte hak kavramına yüklenen anlam ışığında, farklı tanımlamalar yapılmıştır. Yıllık ücretli izinle ilgili savunulan ilk görüş bu hakkın işverenin lütfu olduğu şeklindedir. Yıllık ücretli iznin sözleşmeler ve toplu iş sözleşmeleri ile düzenlenmediği, kanunlarda bu hakka yer verilmediği dönemde hâkim olan bu görüşe göre, işçilerin herhangi bir talep hakkı olmadığı ve iş ilişkisindeki tüm koşulları işveren belirlediği için, yıllık ücretli izin de ancak işverenin lütfu olarak işçiye tanınmaktadır. Dolayısıyla işverenin bu izni kullandırma gibi bir borcu da bulunmamaktadır<sup>770</sup>. Başka bir görüşe göre yıllık ücretli izin, temelini örf ve adet hukukunda bulan bir haktır<sup>771</sup>. Yıllık ücretli izin hakkının işçinin çalışmalarının karşılığında elde etmiş olduğu bir hak olduğunu savunanlara göre ise, bu hakkın

---

<sup>767</sup> **Bingöl, Serkan**, Yıllık Ücretli İzin, Seçkin Yayıncılık, Ankara 2012, s. 19

<sup>768</sup> **Mollamahmutoğlu, Hamdi**, İş Hukuku, Turhan Kitabevi, Ankara 2008, s. 942

<sup>769</sup> **Akyiğit, Ercan**, Yıllık Ücretli İzin, Seçkin Yayıncılık, Ankara 2000, s. 30

<sup>770</sup> **Bingöl**, s. 21; **Akyiğit**, Yıllık Ücretli İzin, s. 56

<sup>771</sup> **Bingöl**, s. 21

yapılan hizmetin karşılığı olması nedeniyle, iş sözleşmesi işçinin sadakat borcuna aykırı davranışları nedeniyle feshedilse bile işçinin izni talep hakkı ortadan kalkmayacaktır<sup>772</sup>.

Akyiğit, Anayasanın yıllık ücretli izin hakkına ekonomik ve sosyal haklar içerisinde yer vermesi nedeniyle, bu hakkın ekonomik ve sosyal bir hak olduğu görüşündedir. Yazara göre, bu hak aynı zamanda bir yıl boyunca çalışmış olan işçinin yorgunluğunu atıp, dinlenmesini sağlamayı da amaçlandığından aynı zamanda işverenin gözetim borcu kapsamında da değerlendirilebilecektir. Ayrıca yazar, bu haktan mahrum bırakılmış işçilerin durumunun "işverenin gözetim borcu" teorisiyle izahının mümkün olmadığı gibi, bekleme süresini doldurmalarına rağmen kendilerine yıllık ücretli izin hakkı tanınmayan işçilerin hukuki durumlarını "karşılık teorisiyle" izah etmenin de mümkün olmadığı görüşündedir<sup>773</sup>.

Öğretide de, genel olarak, yıllık ücretli izin, işverenin işçiyi gözetme borcundan kaynaklanan temel, anayasal bir sosyal hak olduğu vurgulanmaktadır<sup>774</sup>.

### C- YILLIK ÜCRETLİ İZİN HAKKININ YASAL TEMELLERİ

Yıllık ücretli izin hakkı İnsan Hakları Evrensel Bildirgesi'nin 24. maddesinde çalışma hakkıyla birlikte temel bir insan hakkı olarak kabul edilmiştir. Ayrıca Avrupa Sosyal Şartı'nın 2/3 maddesinde, Roma anlaşmasının 120. maddesinde, Uluslararası Çalışma Örgütü'nün (ILO) 52, 54, 72, 91, 101, 132, 146 sayılı sözleşmelerinde ve 47, 93 ve 98 sayılı tavsiye kararlarında yıllık izin hakkına yer verilmiştir<sup>775</sup>. Bu hakkın temelinde sosyal diyaloglar kurabilme, toplumla bütünleşme, yaşam standardını yükseltme bakımından yeterince dinlenmenin her çalışan için temel bir ihtiyaç olduğunun kabulü yatmaktadır<sup>776</sup>.

Anayasamızın 50. maddesinde çalışanların dinlenme hakkı güvence altına alınmış ve bu çerçevede yıllık ücretli izin hakkının yasayla düzenleneceği hükme bağlanmıştır. Anayasanın sözü

---

<sup>772</sup> Akyiğit, Yıllık Ücretli İzin, s. 58

<sup>773</sup> Akyiğit, Yıllık Ücretli İzin, s. 59

<sup>774</sup> Çelik, Nuri/Caniklioğlu Nurşen/Canbolat, Talat, İş Hukuku Dersleri, Beta Basın Yayın A.Ş., İstanbul 2017, s. 689; Aktay, Nizamettin/Arıcı Kadir/Kaplan, Tuncay Senyen, İş Hukuku, Gazi Kitabevi, Ankara 2012, s. 250; Sümer, Haluk Hadi, İş Hukuku, Mimoza Basım, Konya 2014, s. 149; Demircioğlu, Murat/Centel Tankut, İş Hukuku, Beta Basım, İstanbul 2007, s. 139; Narmanlioğlu Ünal, İş Hukuku, Ferdi İş İlişkileri, Beta Basın Yayın A.Ş. İstanbul 2012, s. 697; Eyrenci, Ömer / Taşkent, Savaş / Ulucan Devrim, Bireysel İş Hukuku, Beta Yayınevi, İstanbul 2017, s.331; Özen, Cüneyt, Yıllık Ücretli İzin Hakkının 4857 Sayılı İş Kanunu'ndaki Görünümü, ÇSGB Çalışma Dünyası Dergisi, Cilt 3, Sayı 1, Ocak-Nisan 2015, s. 55; Öksüz, Ömer, Yıllık Ücretli İzin, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Yıl 2006, Sayı 11, s. 854

<sup>775</sup> Özveri, Murat, Yıllık Ücretli İzin Hakkı ve Yargı Kararları, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi Yıl 2007, Sayı 15, s. 923; Akyiğit, Yıllık Ücretli İzin, s. 47

<sup>776</sup> Kayhan, Necati, Ulusal Ve Uluslararası Normlara Göre Türkiye'de Yıllık İzin Hakkı, Çalışma İlişkileri Dergisi, Yıl 2010, Cilt 1, Sayı 1, s. 119



edilen maddesi uyarınca yıllık ücretli izinler, İş Kanununun 53. ve devamı maddelerinde hükme bağlanmış, ayrıca aynı kanunun 60. maddesine dayanılarak 3.3.2004 tarihinde Resmi Gazetede yayımlanan Yıllık Ücretli İzin Yönetmeliğinde çeşitli yönleriyle düzenlenmiştir.

818 sayılı. Borçlar Kanununda yıllık ücretli izinle ilgili bir hükme yer verilmediğinden, bu yasaya tabi çalışan işçilerin yasaca öngörülmüş bir yıllık ücretli izin hakkı bulunmamaktaydı. Anayasa'nın 2. maddesinde ifadesini bulan sosyal devlet ilkesi ve 10. maddesinde yer alan eşitlik ilkesi ile 50. maddesindeki dinlenme hakkına aykırı olan bu durum, ya bireysel olarak iş sözleşmeleriyle ya da Toplu İş Sözleşmelerine konulan hükümlerle giderilmeye çalışılıyordu. Nihayet 6098 sayılı Türk Borçlar Kanununun 1.7.2012 tarihinde yürürlüğe girmesiyle bu alandaki yasal düzenleme eksikliği giderilmiştir<sup>777</sup>.

4857 sayılı İş Kanununun 4. maddesi uyarınca, bu kanun kapsamı dışında kalan çalışanlara uygulanacak yıllık ücretli izin hakkı 6098 sayılı Türk Borçlar Kanununun 422 ila 425. maddelerinde düzenlenmiştir<sup>778</sup>. Diğer taraftan, Basın İş Kanununun (5953 Sayılı Basın Mesleğinde Çalışanlarla Çalıştranlar Arasındaki Münasebetlerin Tanzimi Hakkında Kanun) 21. maddesine göre, yıllık ücretli izin hakkı BİK kapsamına giren, bütün gazetecilere tanınan bir hak<sup>779</sup>. Bunun gibi 854 sayılı Deniz İş Kanununun 40. maddesinde gemiadamının yıllık ücretli izne hakkına ilişkin kurallar yer almıştır<sup>780</sup>. Yargıtay kararlarında da yıllık ücretli izin hakkının "*Anayasal temel bir hak olup bu dinlenme hakkından vazgeçilemeyeceği*" vurgulanmaktadır<sup>781</sup>.

#### D- YILLIK ÜCRETLİ İZİN HAKKINA İLİŞKİN HÜKÜMLERİN EMREDİCİLİĞİ

İş sözleşmesinde akdın bir tarafını teşkil eden işçinin, işveren karşısında ekonomik yönden daha zayıf durumda olması nedeniyle, gerek işçinin keyfi muamelelere maruz bırakılmasının önüne geçilmesi, gerekse işçinin feshe karşı korunması, iş hukukunun en temel amaçlarından biridir, Bu

<sup>777</sup> **Akyiğit, Ercan**, Yıllık Ücretli İzin Kurumunda Yeni Bir Durum: Yıllık İzin İşverence Kısıltımı (İndirimi), Çalışma ve Toplum Dergisi, Sayı 2011/3, s. 74

<sup>778</sup> **Bayram, Selahattin**, Yeni Borçlar Kanunu'nun Yıllık İzne İlişkin Hükümleri İle 4857 Sayılı İş Kanunu'nun Yıllık İzne İlişkin Hükümlerinde Farklılık Ve Değerlendirmesi, Mali Çözüm Dergisi, Sayı Ocak-Şubat 2011, s. 308

<sup>779</sup> **Karaca, Nuray Gökçek/ Günaydın, Barış**, Gazetecilerin Ücretli Tatil ve Yıllık Ücretli İzin Hakkı, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Yıl 2007, Sayı 15, s. 910

<sup>780</sup> **Karaman, Mehmet Halis**, Deniz İş Kanunu Kapsamında Çalışan İşçilerin Yıllık Ücretli İzin Hakkı, Sicil İş Hukuku Dergisi, Yıl 2018, Sayı 40, s. 116

<sup>781</sup> Örneğin, YARGITAY 22. HUKUK DAİRESİ E. 2018/14166 K. 2018/27800 T. 19.12.2018, Kazancı İçtihat Bilgi Bankası, (<http://www.kazanci.com/kho2/ibb/files/dsp.php?fn=22hd-2018-14166.htm&kw=y%C4%B1I%C4%B1k+%C3%BCcretli+izin+vazge%C3%A7ilemez#fm>, Erişim tarihi: 12.3.2019)

nedence Borçlar Hukukunun temel prensiplerinden olan sözleşme özgürlüğü ilkesi, İş Hukukunda belli sınırlar içinde uygulanmaktadır. İş Hukukundaki diğer birçok hüküm gibi yıllık ücretli izin hakkına ilişkin hükümler de nispi emredici nitelikte hükümlerdendir. Bu hükümleri, sözleşmenin tarafları işçi aleyhine olmamak koşuluyla değiştirebilirler ve işçi lehine düzenlemelere gidebilirler<sup>782</sup>.

Nitekim İş Kanunu'nun 45. maddesinin ilk fıkrasında "*toplular iş sözleşmesi veya iş sözleşmelerine hafta tatili, ulusal bayram ve genel tatillerde işçilere tanınan haklara, ücretli izinlere ve yüzde usulü ile çalışan işçilerin bu kanunla tanınan haklarına aykırı hükümler konulamaz*" denilerek ücretli izinlerle ilgili olarak işçi aleyhine düzenlemelerin yapılamayacağı vurgulanmıştır. İkinci fıkrada ise "*bu hususlarda işçilere daha elverişli hak ve menfaatler sağlayan kanun, toplular iş sözleşmesi, iş sözleşmesi veya gelenekten doğan kazanılmış haklar saklıdır*" denilerek yıllık ücretli izne ilişkin düzenlemelerin de nispi emredici nitelikte oldukları, sözleşme taraflarınca işçi lehine düzenlemelerin yapılabileceği belirtilmiştir. Yine 53. maddesinin son fıkrasında, "*yıllık izin süreleri iş sözleşmeleri ve toplular iş sözleşmeleri ile arttırılabilir*" denilmiştir. Dolayısıyla, kanunda belirtilen yıllık ücretli izin süreleri asgari olup, sözleşmelerle arttırılması mümkündür<sup>783</sup>.

İş Hukukundaki kuralların genellikle nispi emredici nitelikte olmasına karşın, bazı hükümler mutlak emredici niteliktedir. Mutlak emredici nitelikteki bu hükümlerin taraf iradeleri ile değiştirilmesi, işçi lehine olsa bile aksinin düzenlenmesi mümkün değildir. Bu bağlamda İş Kanununun yıllık ücretli izin hakkından vazgeçilemeyeceğine ilişkin m 53/2. ve işçinin izin süresi içerisinde başka işte çalışmasını yasak olmasına ilişkin, 58 madde hükümleri mutlak emredici niteliktedir<sup>784</sup>. Yıllık ücretli izin hakkından vazgeçilemeyeceğine ilişkin 53/2. madde (ve TBK m. 425/2) hükmüyle, sağlığının korunması amacıyla işçi bu konuda kendisinin yapabileceği hukuki işlemlere karşı da korunmuştur. İşçi, örneğin yüksek ücret karşılığında yıllık izin hakkından vazgeçemez, bu tür sözleşme hükümleri geçersizdir<sup>785</sup>. İşçinin kullanmadığı yıllık izin sürelerinin birleştirilerek sonraki yıllarda kullanması da Kanuna aykırıdır. Aksi halde işçi sırf para kazanmak

---

<sup>782</sup> Bingöl, s. 23

<sup>783</sup> Narmanlıoğlu, s. 705; Bingöl, s. 23; Aktay/Arıcı/Kaplan, s. 257

<sup>784</sup> Sözek, Sarper, İş Hukuku, Beta Basın Yayın A.Ş. İstanbul 2018, s. 826; Bingöl, s. 23; Akyiğit, Yıllık Ücretli İzin, s. 68 vd; Mollamahmutoğlu, s. 960; Sümer, s. 150; Özen, s. 75; Eyrenci/Taşkent/Ulucan, s. 331; Demircioğlu/Centel, s. 141; Narmanlıoğlu, s. 697; Çelik/Caniklioğlu/Canbolat, s.689; Aktay/Arıcı/Kaplan, s. 250

<sup>785</sup> Demir, Fevzi, İş Hukuku ve Uygulaması, Albi Yayıncılık, İzmir 2016, . 276; Mollamahmutoğlu, s. 942; Aktay/Arıcı/Kaplan, s. 255; Çelik/Caniklioğlu/Canbolat, s. 696; Demircioğlu/Centel, s. 141

için izin hakkından vazgeçme olanağına sahip olabilir. Bu durum ise Anayasa'da güvence altına alınmış olan dinlenme hakkına aykırılık oluşturur<sup>786</sup>. Ancak bu durumlarda işçi izin hakkını kaybetmiş sayılmayacaktır<sup>787</sup>. İşçi hiç izin kullanmadan çalışsa ve fazladan yıllık izin ücretinin ödenmesini kabul etse de Anayasal temel hak olan yıllık ücretli izin hakkından vazgeçilmesi yasal olmadığından, işveren, işçinin iş sözleşmesinin sona ermesinden itibaren beş yıl içerisinde tekrar son ücrete göre yıllık ücretli izin parasını talep halinde ödemek zorunda kalacaktır<sup>788</sup>. Öte yandan, sadece hastalığı gibi sebeplerle işçi, yıllık iznin kullanılmasını ertelettirebilir. İş sözleşmesi devam ederken işçiye gecikerek de olsa, yıllık dinlenme imkânı tanınmak ve işverenin o süre için ücretini izine çıkmadan, sağlama yükümlülüğü devam eder<sup>789</sup>. Sonuç olarak yıllık ücretli iznin niteliği, bunun işçi açısından mutlaka kullanılmasını, işveren bakımından da mutlaka kullandırılmasını gerektirir. İşverence yıllık ücretli izin hakkının kullandırılmaması halinde ise, işçi İK'nun 24/II-f maddesi uyarınca çalışma koşullarının uygulanmaması nedeniyle iş akdini derhal fesih hakkını kullanabilir<sup>790</sup>. Diğer taraftan İş Kanununun 103. maddesinde, işverenin yıllık ücretli izne ilişkin hükümlere aykırı hareket etmesi halinde idari para cezası uygulanacağı hükme bağlanmıştır<sup>791</sup>.

Keza, Basın İş Kanunu (BİK) olarak anılan, Basın Mesleğinde Çalışanlarla Çalıştıranlar Arasındaki Münasebetlerin Tanzimi Hakkında Kanunun "yıllık ücretli izin" başlığını taşıyan 21. maddesine göre, yıllık ücretli izin hakkı BİK kapsamına giren bütün gazetecilere tanınmış bir haktır. İş Kanununda olduğu gibi gazetecinin de bu haktan vazgeçebilmesi mümkün değildir (BİK m. 21/son). Kanunun bu haktan vazgeçilemeyeceğine ilişkin bu hükmü mutlak emredicidir. Bu haktan vazgeçilemeyeceğine göre, ücretli iznini kullanmakta olan gazeteci izin süresi içinde ücret karşılığı bir işte de çalışamaz; çalıştığı anlaşılırsa bu izin süresi içinde kendisine ödenen ücret işveren tarafından geri alınabilir. Bu itibarla iş sözleşmelerine ve toplu iş sözleşmelerine bu haktan vazgeçildiğine ilişkin hüküm konulamaz. Konulmuş olsa bile bu hüküm geçersizdir<sup>792</sup>.

---

<sup>786</sup> Demir, s. 277; Çelik/Caniklioğlu/Canbolat, s. 696

<sup>787</sup> Çelik/Caniklioğlu/Canbolat, s. 696; Günay, s. 32

<sup>788</sup> Günay, Cevdet İlhan, Yıllık Ücretli İzin Hakkı ve Ücretli İzin Alacağı, Sicil İş Hukuku Dergisi, Aralık 2010, Yıl 5, Sayı 20, s. 34

<sup>789</sup> Günay, s. 32

<sup>790</sup> Süzek, s. 826; Akyiğit, Yıllık Ücretli İzin, s. 70

<sup>791</sup> Gönen, Ramazan, İş Hukukunda Yıllık Ücretli İzin, İstanbul Barosu Dergisi, Cilt: 87, Sayı: 3, Mayıs 2013, s. 212

<sup>792</sup> Karaca / Günaydın, s. 911; Oğuz, Özgür/Doğan, Özge, Gazetecinin Yıllık Ücretli İzin Hakkı, 2016, Yıl: 5 / Sayı 10, s. 98

Aynı şekilde, 854 sayılı Deniz İş Kanunu'nun 40. maddesinin 3. fıkrasında, “*yıllık ücretli izin hakkından feragat edilemeyeceği*” hükme bağlanmıştır. Dolayısıyla DİK bakımından da yıllık ücretli izin hakkından vazgeçmek veya bu hakkı devretmek mümkün değildir<sup>793</sup>.

## II- YILLIK ÜCRETLİ İZNE HAK KAZANILMA ŞARTLARI

### A- EN AZ BİR YIL ÇALIŞMIŞ OLMAK

İşçinin yıllık ücretli izine hak kazanabilmesi için, İş Kanununun 53. maddesinin 1. fıkrası (TBK 422) uyarınca işyerinde fiilen<sup>794</sup> işe başladığı günden itibaren en az bir yıl<sup>795</sup> çalışmış olması gerekir<sup>796</sup>. Çalışmanın başlangıcı olarak esas alınacak tarih, iş sözleşmesinin yapıldığı ve imzalandığı tarih değil, işe fiilen başlamakla hizmet akdinin yürürlüğe girdiği tarihtir<sup>797</sup>. Hukukumuzda, işyerinde çalışması bir yılı doldurmayan işçiler için orantılı bir izin hakkı tanınmamıştır<sup>798</sup>. Bu esas uyarınca bir takvim yılındaki parçalı çalışmalar için izin hakkı ve parası söz konusu olmayacağı gibi, bir yılın dolmadığı süre için orantılı olarak izin hakkı doğmaz<sup>799</sup>.

Yıllık ücretli izine hak kazanma açısından işçinin belirli veya belirsiz süreli iş akdiyle çalışması önem taşımaz. İşyerinde bir yıl belirli süreli sözleşmeyle çalışan işçi de yıllık ücretli izine hak kazanır. Çeşitli tarihlerde belirli süreli iş sözleşmesiyle çalışan veya yenilenerek devam eden belirli süreli iş sözleşmeleriyle çalışan işçiler gibi, kötüye kullanıldığı için belirsiz süreli sayılan ya da aslında belirsiz süre için akdedilen iş sözleşmesine dayanarak çalışmasını sürdüren işçiler asgari bir yıllık süreyi doldurduklarında yıllık ücretli izin talebinde bulunabileceklerdir<sup>800</sup>.

İş akdinde bir deneme süresi kararlaştırılmış olması halinde, geçirilmesi gereken bir yılın hesabında deneme süresi de göz önünde tutulacaktır<sup>801</sup>.

---

<sup>793</sup> Karaman, s. 115

<sup>794</sup> Narmanhoğlu, s. 698

<sup>795</sup> Basın İş Kanununda da (m. 21) en az bir yıl olarak öngörülen gazetecinin çalışmış olma şartı, Deniz İş Kanununda (m. 40) gemi adamı için en az altı ay olarak belirlenmiştir.

<sup>796</sup> Süzek, s. 826; Demir, s. 271; Çelik/Caniklioğlu/Canbolat, s.689; Eyrenci/Taşkent/Ulucan, s. 332; Akyiğit, Yıllık Ücretli İzin, s. 183; Narmanhoğlu, s. 698; Bingöl, s. 28; Sümer, s. 150; Demircioğlu/Centel, s. 140; Aktay/Arıcı/Kaplan, s. 250

<sup>797</sup> Günay, s. 29

<sup>798</sup> Eyrenci/Taşkent/Ulucan, s. 332; Narmanhoğlu, s. 699

<sup>799</sup> YARGITAY 9. HDE. 1980/11339 K. 1980/11935 T. 19.11.1980 (Çelik/Caniklioğlu/Canbolat, s.689)

<sup>800</sup> Narmanhoğlu, s. 699; Süzek, s. 829; Eyrenci/Taşkent/Ulucan, s. 332

<sup>801</sup> Narmanhoğlu, s. 698; Süzek, s. 827; Aktay/Arıcı/Kaplan, s. 250

İş Kanununun 54. maddesinin 3. ve 4. fıkraları uyarınca işçinin gelecek izin hakları için geçmesi gereken bir yıllık hizmet süresi, son izne çıktığı tarihten itibaren değil, bir önceki izin hakkının doğduğu günden başlayarak, gelecek hizmet yılına doğru hesaplanacaktır<sup>802</sup>.

Basın İş Kanununun 21'inci maddesinin 1'nci fıkrasına göre "*günlük bir mevkutede çalışan gazeteciye, sürekli veya aralıklı olarak en az bir yıl çalışmış olmak şartıyla, yılda dört hafta tam ücretli izin verilir. Gazetecilik mesleğindeki hizmeti on yıldan yukarı olan bir gazeteciye, altı hafta ücretli izin verilir. ...*". Madde hükmünden de anlaşılacağı üzere, gazetecinin kıdemi aynı gazetede geçen hizmet süresine göre değil, gazetecilik mesleğinde geçen hizmet süresine göre hesaplanır. 21. maddenin 2. fıkrası uyarınca gazetecinin iş sözleşmesinin arada kesintiye uğramış veya yeniden bağlanmış olması meslek kıdemine hesaplanması bakımından rol oynamaz. Belirtilen bu şart sağlanmışsa, gazeteci kıdemine göre değişen bir süre ile yıllık ücretli izne hak kazanacaktır. Kanunda yer alan bu hükmün iş sözleşmeleri ve toplu iş sözleşmeleriyle gazeteci lehine değiştirilebilmesi mümkündür<sup>803</sup>. Yine BİK'nun 21'inci maddesinin 2'nci fıkrasına göre, günlük olmayan mevkutelere çalışan gazetecilerin ise yıllık ücretli izne hak kazanabilmeleri için, en az bir yıl çalışma şartı aranmamakta, 6 aylık çalışma devresini doldurmaları yeterli görülmektedir<sup>804</sup>.

854 Sayılı Deniz İş Kanununun 40. maddesi uyarınca, gemiadamının yıllık ücretli izne hak kazanabilmesi için, aynı işveren emrinde veya aynı gemide bir yıl içerisinde bir veya birden fazla hizmet akdine dayanarak en az altı ay çalışmış olması gerekmektedir<sup>805</sup>.

## **B- NİTELİĞİ İTİBARIYLA BİR YILDAN DAHA AZ SÜREN MEVSİM VEYA KAMPANYA İŞİ DIŞINDA ÇALIŞMAK**

İş Kanununun 53. maddesinin 3. fıkrasının "*Niteliklerinden ötürü bir yıldan az süren mevsimlik veya kampanya işlerinde çalışanlara bu Kanunun yıllık ücretli izinlere ilişkin hükümleri uygulanmaz*" hükmü gereği, kural olarak bir yıldan az süren mevsim ve kampanya işlerinde yıllık ücretli izin hakkı doğmamakla birlikte, Yıllık Ücretli izin Yönetmeliğinin 12. maddesi, "*bir yıldan az süren mevsim veya kampanya işlerinin yürütüldüğü işyerlerinde devamlı olarak çalışan işçilerin*" yıllık ücretli izin hakkından (örneğin bekçiler) yararlanacağını hükme bağlamıştır<sup>806</sup>. Aynı şekilde

---

<sup>802</sup> Demir, s. 272; Narmanlıoğlu, s. 699; Aktay/Arıcı/Kaplan, s. 252; Süzek, s. 829; Çelik/Canıklıoğlu/Canbolat, s.690; Eyrenci/Taşkent/Ülucan, s. 333

<sup>803</sup> Karaca / Günaydın, s. 911; Oğuz/Özge, s. 101

<sup>804</sup> Karaca / Günaydın, s. 911; Oğuz/Özge, s. 101

<sup>805</sup> Karaman, s. 121; Akyiğit, Ercan, Deniz İş Kanununda Yıllık Ücretli İzin, Sarper Süzek'e Armağan (I), Beta Yayınevi, İstanbul 2011, s. 316

<sup>806</sup> Demir, s. 271; Aktay/Arıcı/Kaplan, s. 251

mevsim veya kampanya işinde çalışan işçi, daha sonra sürekli işe geçirilir ya da tersi olursa, bu işçinin mevsim veya kampanya işinde çalıştığı süreler de dikkate alınarak yıllık ücretli izin hakkından yararlanması gerekir. Zira yıllık ücretli izin hakkından sadece mevsim veya kampanya işlerinde geçici olarak çalışan işçiler yoksun bulunmaktadır<sup>807</sup>.

Mevsimlik iş, işyerinde faaliyetin yılın belirli bir döneminde yoğunlaştığı, diğer zamanlarda ise azaldığı veya tamamen durduğu, fakat bu durumun düzenli olarak tekrarlandığı bir iştir. Kampanya işi ise, faaliyetin yılda ancak birkaç ay devam ettiği bir iştir. Bu nedenle, bir işin mevsimlik veya kampanya işi olup olmadığı işin özelliği ile ilgilidir<sup>808</sup>. Hangi işlerin bu nitelikte olduklarının belirlenmesi önemli bir sorun olarak ortaya çıkmaktadır. Mevsim ve kampanya işini belirginleştiren husus faaliyetin belli bir dönemde yapılması, çalışmanın önceden kestirilebilen bir iş devresinde sürdürülmesidir<sup>809</sup>.

Mevsim ve kampanya işinden ne anlaşılması gerektiği konusu üzerinde durmaksızın, işçinin bir yıldan az çalıştırılmış olmasından hareket eden Yargıtay'a göre bu kuralın iki istisnası bulunmaktadır. Buna göre, "*İlk olarak eğer işçinin bir takvim yılı içerisinde 11 ayı (330 gün) aşan çalışması var ise yalnızca o yıl yıllık izne hak kazanır. İkinci olarak ise işin mahiyetine göre her yıl çalışma dönemi olarak belirlenen dönem (mevsim) dışında çalışma söz konusu ise o yıl ile kısıtlı (olarak) çalışma süresi yıllık izin ücreti hesabında nazara alınır.. Mahkemece yapılacak iş... Davacının mevsim dışında çalışması olan yıllardaki çalışma süreleri ile 11 ayı aşan çalışması olan yıllardaki çalışma sürelerini yıllık izin hesabında dikkate alarak karar vermektir*"<sup>810</sup>.

Narmanlıoğlu, Eyrenci/Taşkent/Ulucan ve Aktay/Arıcı/Kaplan'a göre, niteliği bakımından mevsim veya kampanya işi olmayan bir işte (örneğin, inşaat işinde), uzunca bir süre çalışan bir işçinin, sırf çalışmaları her dönem bir yıldan az sürmesi nedeniyle yıllık ücretli izin hakkından yararlanmayacağı sonucuna vararak yıllık ücretli izin hakkını daraltan Yargıtay içtihadının kabul edilmesi mümkün değildir<sup>811</sup>.

Günay da, her devamlı olmayan çalışmanın mevsimlik olarak nitelendirilemeyeceğini, örneğin belediyelerde Sayıştay uygulamaları nedeniyle vize alınması zorunluluğunun, yılın tümünde çalışmayı engelleyebileceğini dile getirmektedir. Bu durumda belediyede veya bazı kamu kuruluşlarında geçici çalışan işçileri mevsimlik işlerde çalışan işçi olarak kabul etmek mümkün

---

<sup>807</sup> Eyrenci/Taşkent/Ulucan, s. 332; Narmanlıoğlu, s. 703; Aktay/Arıcı/Kaplan, s. 251

<sup>808</sup> Eyrenci/Taşkent/Ulucan, s. 337; Narmanlıoğlu, s. 703; Aktay/Arıcı/Kaplan, s. 251

<sup>809</sup> Narmanlıoğlu, s. 703

<sup>810</sup> YARGITAY 22. HUKUK DAİRESİ E. 2013/29456 K. 2015/1359 T. 28.1.2015 (Süzek, s. 830)

<sup>811</sup> Eyrenci/Taşkent/Ulucan, s. 337; Aktay/Arıcı/Kaplan, s. 251; Narmanlıoğlu, s. 703

değildir. Bu tür çalışan işçilerin her yıl çalıştıkları süreler toplanmak suretiyle her 365 gün için yıllık ücretli izin hakkı doğacaktır<sup>812</sup>.

Yukarıdaki belirtilen genel içtihadının tersine, Yargıtay bir kararında isabetli olarak, "*Yapılan iş mevsimlik değil, ancak işçi aralıklı çalıştırılmış ise, mevsimlik işten söz edilemeyeceğinden, bu sürenin de izin hesabında dikkate alınması gerekir... Çalışmada, mevsimlik iş kriterlerinin bulunup bulunmadığı araştırılmadan, sırf bir yıldan az bir çalışma olduğu için mevsimlik saymak doğru değildir*" demiştir<sup>813</sup>. Aynı şekilde Yargıtay'ın isabetli kararı uyarınca, geçici işçi olarak çalışılan dönem yıllık ücretli izin hesabında göz önünde tutulmalıdır<sup>814</sup>.

Yukarıda belirtildiği gibi, yıllık ücretli izin hakkı, kullandırılması bakımından mutlak emredici olmakla beraber, hak kazanma koşulları bakımından nispi emredicidir. Dolayısıyla yıllık ücretli izni düzenleyen hükmün aksi işçi lehine kararlaştırılabilir. Yıllık izin hakkını düzenleyen hükmün nispi emredici olması sebebiyle mevsimlik işlerde çalışan işçilerin yıllık izne hak kazanabileceği toplu iş sözleşmesiyle yahut iş sözleşmesiyle ya da iş sözleşmesi hükmündeki işyeri uygulaması ile kararlaştırılabilir<sup>815</sup>. Yargıtay da bir kararında<sup>816</sup>, "*mevsimlik işçi, 4857 sayılı İş Kanunu'nun yıllık ücretli izin hükümlerine dayanarak, yıllık ücretli izin kullanma veya buna dayanarak ücret alacağı isteminde bulunamaz. Hemen belirtmek gerekir ki, 53/3. maddede ki kural, nispi emredici kural olup, işçi lehine bireysel iş sözleşmesi ya da Toplu İş Sözleşmesi ile yıllık ücretli izne ilişkin hükümler düzenlenebilir. Bu durumda sözleşmedeki izinle ilgili hükümler uygulanacaktır.*" demiştir.

### C- KISMİ SÜRELİ İŞ SÖZLEŞMESİ VE ÇAĞRI ÜZERİNE ÇALIŞAN İŞÇİLERİN DURUMU

Bunlar dışında, "*kısmi süreli iş sözleşmesi*" ve "*çağrı üzerine çalışan işçiler*" ile "*geçici (ödünç) iş ilişkisiyle çalışan işçiler*" de yıllık ücretli izin hakkına sahiptir<sup>817</sup>. Kısmi süreli veya çağrı üzerine çalışan işçinin izin hakkı Yıllık Ücretli İzin Yönetmeliğinin 13. maddesinde düzenlenmiştir. Anılan hükme göre "*Kısmi süreli ya da çağrı üzerine iş sözleşmesi ile çalışanlar yıllık ücretli izin*

<sup>812</sup> Günay, s. 31

<sup>813</sup> YARGITAY 9. HUKUK DAİRESİ E. 2013/12664 K. 2015/7882 T. 24.2.2015 (Süzek, s. 830) ve (Çelik/Caniklioğlu/Canbolat, s.692)

<sup>814</sup> YARGITAY 22. HUKUK DAİRESİ E. 2014/28537 K. 2016/3293 T. 10.2.2016 (Süzek, s. 830)

<sup>815</sup> Bodur, Mehtap, Mevsimlik İş Sözleşmesi İle Çalışanların Yıllık Ücretli İzin Hakları, Cilt 1, Sayı 1, Ocak 2015, s. 135

<sup>816</sup> YARGITAY 9. HUKUK DAİRESİ E. 2008/14577 K. 2010/294 T. 18.1.2010, Kazancı İçtihat Bilgi Bankası, (<http://www.kazanci.com/kho2/ibb/files/dsp.php?fn=9hd-2008-14577.htm&kw=18.1.2010+14577#fm>, Erişim tarihi: 16.3.2019)

<sup>817</sup> Narmanhoğlu, s. 700; Aktay/Arıcı/Kaplan, s. 251; Çelik/Caniklioğlu/Canbolat, s.692

*hakkından tam süreli çalışanlar gibi yararlanır ve farklı işleme tabi tutulamaz. Kısmi süreli ya da çağrı üzerine iş sözleşmesi ile çalışanlar iş sözleşmeleri devam ettiği sürece her yıl için hak ettikleri izinleri, bir sonraki yıl, izin süresi içine isabet eden kısmi süreli iş günlerinde çalışmayarak kullanır. Yukarıdaki esaslara göre izine hak kazanan kısmi süreli ya da çağrı üzerine çalışan işçilerle tam süreli çalışan işçiler arasında yıllık izin süreleri ve izin ücretleri konularında bir ayırım yapılamaz".* Buna göre, bu işçiler yıllık ücretli izinlerini kısmi süreli işgünlerinde çalışmayarak kullanacaklardır. Farklı işlem yapmama ilkesi gereği yıllık ücretli izine hak kazanmak için gerekli olan bir yıllık çalışma süresinin hesaplanmasında kısmi süreli çalışan işçinin sadece fiilen çalıştığı günlerin toplamı değil, iş ilişkisinin devam süresi göz önünde tutulacaktır<sup>818</sup>.

#### **D- EN AZ BİR YILLIK SÜRENİN HESABINDA İŞÇİNİN FARKLI İŞYERLERİNDEKİ ÇALIŞMALARININ DİKKATE ALINMASI**

Yıllık ücretli izin hakkının kazanılması için gerekli olan bir yıllık çalışmanın işverenin aynı işyerinde yapılması zorunlu değildir<sup>819</sup>. İş Kanununun 54. maddesinin 1. fıkrası uyarınca "*Yıllık ücretli izine hak kazanmak için gerekli sürenin hesabında işçilerin, aynı işverenin bir veya çeşitli işyerlerinde çalıştıktan süreler birleştirilerek göz önüne alınır*".

Hükmün mutlak ifadesi karşısında işçinin, işverenin aynı veya değişik işyerlerinde kesintisiz çalışmış olması da zorunlu sayılmamalıdır. İşçinin değişik zamanlarda yani aralıklı olarak çalışması halinde de, yıllık ücretli izin hakkının doğumunda, izin süresinin ve ücretinin hesaplanmasında bu sürelerin birleştirilerek dikkate alınması gerekir<sup>820</sup>. Üstelik işçinin daha önce çalıştığı iş yerinin İş Kanunu kapsamında bir işyeri olmasının veya olmamasının da bir önemi bulunmamaktadır<sup>821</sup>. İşyerinin devri halinde işçinin devirden önceki çalışma süresi ile ilgili olarak da İK m. 6'ya dayanmak suretiyle aynı sonuca varılmalıdır<sup>822</sup>.

İşçinin aynı işveren yanında yeniden işe girmesi halinde yıllık ücretli izne esas hizmet süresinin, önceki ve sonraki çalışma süreleri birleştirilerek göz önüne alınacağını öngören düzenleme, sadece ikinci ve sonraki çalışma dönemlerinde izne hak kazanma tarihinin ve hak edilecek izin gün sayısının belirlenmesi açısından sonuç doğurur. Yoksa işçinin daha önceki

---

<sup>818</sup> **Süzek**, s. 829; **Eyrenci/Taşkent/Ulucan**, s. 332; **Aktay/Arıcı/Kaplan**, s. 251; **Günay**, s. 33

<sup>819</sup> **Süzek**, s. 827; **Demir**, s. 271; **Çelik/Caniklioğlu/Canbolat**, s.689;

<sup>820</sup> **Süzek**, s. 827; **Demir**, s. 272; **Çelik/Caniklioğlu/Canbolat**, s.690; **Narmanhoğlu**, s. 701; **Eyrenci/Taşkent/Ulucan**, s. 333

<sup>821</sup> **Demir**, s. 272; **Süzek**, s. 827; **Narmanhoğlu**, s. 701;

<sup>822</sup> **Çelik/Caniklioğlu/Canbolat**, s.690; **Narmanhoğlu**, s. 702; **Demir**, s. 273; **Aktay/Arıcı/Kaplan**, s. 252; **Mollamahmutoğlu**, s. 956; **Sümer**, s. 151; **Günay**, s. 31



çalışma dönemleri sonunda fiilen kullanmadığı için o dönemki son ücreti üzerinden karşılığı ödenen yıllık izin ücretlerinin ileride aynı işveren yanındaki sonraki çalışmalarının sona erdiği tarihteki ücreti üzerinden (fark) ödenmesini gerektirmez<sup>823</sup>.

Aynı şekilde, İK'nun 54. ve YÜİY'nin 4. maddelerinin son fıkralarında bu konuda kamu kesiminin özelliğine uygun bir hüküm öngörülmüştür<sup>824</sup>. Bu hükme göre "*Aynı bakanlığa bağlı işyerleri ile aynı bakanlığa bağlı tüzel kişilerin işyerlerinde geçen süreler ve kamu iktisadi teşebbüsleri yahut özel kanunla veya Cumhurbaşkanlığı kararnamesine dayanılarak kurulan banka ve kuruluşlar veya bunlara bağlı işyerlerinde geçen süreler, işçinin yıllık ücretli izin hakkının hesaplanmasında göz önünde bulundurulur*". Ancak, Yargıtay'a göre "*davacının sözleşmeli personel statüsünde geçirdiği çalışmalar 4857 sayılı İş Kanununun 54/1. maddesinde değerlendirilemez. Anılan yasa maddesinde kastedilen ve birleştirilebilecek çalışmalar Borçlar Kanunu, Deniz İş Kanunu, Basın İş Kanunu gibi yasalar kapsamına giren çalışmalardır. Böyle olunca davacının statü hukukuna göre sözleşmeli personel olarak görev yaptığı dönem yıllık ücretli izine hak kazanılmasında değerlendirilemez. Davacının işçilikte geçen çalışması bir yılı doldurmadığından yıllık ücretli izin alacağına hükmedilemez*"<sup>825</sup>.

Süzek tarafından, emekli olan ve aynı işyerinde çalışmasını sürdüren işçinin emekli olmadan önceki çalışma sürelerinin de yıllık ücretli iznin hesabında göz önünde tutulması gerektiği belirtilmektedir<sup>826</sup>. Buna karşın, Demir ve Çelik/Caniklioğlu/Canbolat'ın atıfta bulunduğu bir içtihadında, Yargıtay "*emekli olan işçinin çalışmasını sürdürmesi durumunda bu çalışmanın yeni bir iş sözleşmesine dayanması ve bir yılı doldurmaması nedeniyle, yıllık izin hakkını doğurmayacağı*" kabul etmiştir<sup>827</sup>.

Yargıtay kural olarak aynı işveren yanındaki aralıklı çalışmaların yıllık izin hakkı açısından birleştirilerek göz önünde bulundurulacağı görüşünde olmakla birlikte, Yüksek Mahkeme bu kuralın uygulanmasını kanunda aranmayan bir koşula bağlamıştır. Bu koşul ise, zaman içinde değişiklik göstermiştir. Yargıtay başlangıçta aynı işveren yanında geçen sürelerin ancak bu döneme

---

<sup>823</sup> **Özkaraca,ERCÜMET**, Aynı İşveren Yanındaki Aralıklı Çalışmalarda Yıllık Ücretli İzin Hakkı, Sicil İş Hukuku Dergisi, Yıl 2018, Sayı 39, s. 95

<sup>824</sup> **Narmanlıoğlu**, s. 701, **Süzek**, s. 828; **Aktay/Arıcı/Kaplan**, s. 252; **Mollamahmutoğlu**, s. 947; **Eyrenci/Taşkent/Ulucan**, s. 334; **Sümer**, s. 151

<sup>825</sup> YARGITAY 9. HUKUK DAİRESİ E. 2007/32544 K. 2009/783 T. 2.2.2009 (**Aktay/Arıcı/Kaplan**, s. 252)

<sup>826</sup> **Süzek**, s. 827

<sup>827</sup> Yargıtay 9. HD, 13.5.1991 E. 1991/451 K. 1991/8352 (**Demir**, s. 272; **Çelik/Caniklioğlu/Canbolat**, s. 690)

ilişkin kıdem tazminatı ödenmemişse birleştirilebileceğini kabul ederken<sup>828</sup>, daha sonra içtihat değiştirerek kıdem tazminatının ödenmiş olmasının birleştirmeye engel olmayacağını kabul etmiştir<sup>829</sup>. Ancak bu defa da önceki çalışma döneminde izinler kullandırılmış veya iş sözleşmesi sona erdiğinde karşılığı ödenmişse kanunda öngörülen kuralın uygulanmayarak sürelerin birleştirilmeyeceğini kabul etmiştir<sup>830</sup>.

Diğer taraftan kullanılmayan yıllık izin alacağı için zamanaşımının iş sözleşmesinin feshinden itibaren işlemeye başlayacağı ve yıllık izin özde bir dinlenme hakkı olduğundan aralıklı çalışmalarda önceki dönemin zamanaşımına uğramayacağı kabul edilmektedir<sup>831</sup>. Yargıtay'ın yine bu yöndeki bir içtihadına göre "*işçinin aralıklı olarak aynı işverene ait işyerinde çalışması halinde önceki dönemin kıdem tazminatı ödenerek feshedilmiş olması, izin yönünden sürelerin birleştirilmesine engel oluşturmaz. Yine, önceki çalışılan sürede bir yılı doldurmadığı için izne hak kazanılmayan arta kalan süreler de, işçinin aynı işverene ait işyeri ya da işyerlerindeki sonraki çalışmalarına eklenerek yıllık izin hakkı belirlenir. Yıllık izin, özde bir dinlenme hakkı olup, aralıklı çalışmalarda önceki dönem zaman aşımına uğramaz.*"<sup>832</sup>

İşveren tarafından iş akdi feshedilen işçinin İş Kanununun 20. maddesi uyarınca yaptığı başvuru üzerine mahkemece feshin geçersizliğine karar verilip işçi işe başlatılmışsa, fesih ile işe başlama tarihi arasında işçinin çalıştırılmadığı süre yıllık ücretli izin süresinin hesabında dikkate alınmalıdır. Çünkü fesih nedeninin geçerli olmadığı yargı organı tarafından saptanarak feshin geçersizliğine karar verilmesinin anlamı, feshin hiçbir hüküm ve sonuç meydana getirmemesi, taraflar arasında iş ilişkisinin aynen devam etmesidir<sup>833</sup>.

Deniz İş Kanunu Bakımından, bu konuda, gemi adamının, aynı işveren emrinde veya aynı gemide çalışmış olması yeterli görülmüştür. Dolayısıyla, gemiadamının çalıştığı geminin başka bir işverene devredilmesi durumunda, gemiadamının çalışma süresi bir bütün olarak değerlendirilecek ve yıllık ücretli izne hak kazanıp kazanmadığı veya yıllık ücretli izin süresi bu şekilde

---

<sup>828</sup> **Özel, Kayhan**, Yıllık İzinler Konusunda Bir Yargıtay Kararının İncelenmesi, İstanbul Barosu Dergisi, Cilt: 82, Sayı: 3, Mayıs 2008, s. 1379; YARGITAY 9. HUKUK DAİRESİ E. 2006/12556 K. 2007/1252 T. 30.1.2007 (Özkaraca, s. 97 ve Özel s. 1379))

<sup>829</sup> YARGITAY 9. HUKUK DAİRESİ E. 2017/7402 K. 2017/19394 T. 29.11.2017 (Özkaraca, s. 97)

<sup>830</sup> **Özkaraca**, s. 97

<sup>831</sup> **Öztürk, Mehmet Onat**, Kullandırılmayan Yıllık Ücretli İzin Hakkı Sebebiyle İş Kanunu Çerçevesinde Yapılan Ödemeler, Çalışma ve Toplum Dergisi, Sayı: 2012/4, s. 84

<sup>832</sup> YARGITAY 9. HUKUK DAİRESİ E. 2007/38515 K. 2009/10133 T. 9.4.2009, Kazancı İçtihat Bilgi Bankası, (<http://www.kazanci.com/kho2/ibb/files/dsp.php?fn=9hd-2007-38515.htm&kw=9.4.2009+38515#fm>, Erişim tarihi: 12.3.2019)

<sup>833</sup> **Süzek**, s. 828;

belirlenecektir. Bu açıdan, geminin hangi hukuki işleme dayalı olarak devredildiğinin de bir önemi yoktur<sup>834</sup>.

Basın İş Kanununun 21/2. madde hükmünden de anlaşılacağı üzere, gazetecinin kıdemi aynı gazetede geçen hizmet süresine göre değil, gazetecilik mesleğinde geçen hizmet süresine göre hesaplanır. Gazetecinin iş sözleşmesinin arada kesintiye uğramış veya yeniden bağitlanmış olması meslek kıdemini hesaplanması bakımından rol oynamayacaktır. Belirtilen bu şart sağlanmışsa, gazeteci kıdemine göre değişen bir süre ile yıllık ücretli izne hak kazanacaktır<sup>835</sup>.

### E- ÇALIŞILMIŞ GİBİ SAYILAN HALLER

Yıllık ücretli izine hak kazanılabilmesi için tamamlanması gereken bir yıllık çalışma süresinin hesaplanmasında sadece işçinin fiilen çalıştığı sürelerin değil, kanunen çalışılmış sayılan sürelerin de göz önünde tutulması gerekir<sup>836</sup>. İş Kanununun 55. maddesine göre yıllık ücretli izin hakkının doğumunun ve izin sürelerinin hesabında, işçi fiilen çalışmadığı halde çalışılmış gibi sayılan süreler şunlardır:

- İşçinin uğradığı kaza veya tutulduğu hastalıktan ötürü işine gidemediği günler. Ancak, işçinin bu nedenlerle işe gidemediği günlerin, işyerindeki çalışma süresine göre İK 17'deki bildirim sürelerine eklenecek altı haftadan sonrası (İK 25/I, b) çalışılmış gibi sayılmaz (İK 55/a).
- Kadın işçilerin İş Kanununun 74. maddesi gereğince doğumdan önce ve sonra çalıştırılmadıkları (sekizer haftalık süredeki) günler (İK 55/b).
- İşçinin muvazzaf askerlik hizmeti dışında manevra veya herhangi bir yasadan dolayı ödevlendirilmesi halinde işine gidemediği sürenin yılda en çok doksan günü (İK 55/c).
- Çalışmakta olduğu işyerinde zorlayıcı nedenler yüzünden işin bir haftadan çok tatil edilmesi halinde işçinin yeniden işe başlaması koşuluyla, çalışmadan geçen sürenin onbeş günü (İK 55/d).
- İş Kanununun 66. maddesine göre işçinin günlük çalışma süresinden sayılan zamanlar (İK 55/e).
- Hafta tatili, ulusal bayram ve genel tatil günleri (İK 55/f).

---

<sup>834</sup> **Karaman**, s. 118; **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s. 315

<sup>835</sup> **Karaca / Günaydın**, s. 911; **Oğuz/Özge**, s. 101

<sup>836</sup> **Süzek**, s. 830; **Narmanlıoğlu**, s. 700; **Eyrenci/Taşkent/Ulucan**, s. 335; **Aktay/Arıcı/Kaplan**, s. 253; **Çelik/Caniklioğlu/Canbolat**, s.693; **Mollamahmutoğlu**, s. 945; **Sümer**, s. 152; **Bingöl**, s. 37 vd; **Demir**, s. 274; **Günay**, 30

- 3153 sayılı yasaya dayanılarak çıkarılan yönetmeliğe göre röntgen muayenehanelerinde çalışanlara pazardan başka verilmesi gereken yarım günlük izinler (İK 55/g).
- İşçilerin arabuluculuk toplantılarına katılmaları, hakem kurullarında bulunmaları, bu kurullarda işçi temsilciliği görevlerini yapmaları, çalışma yaşamı ile ilgili mevzuata göre kurulan meclis, kurul, komisyon ve toplantılara yahut işçilik konuları ile ilgili uluslararası kuruluşların konferans, kongre veya kurullarına işçi veya sendika temsilcisi olarak katılmaları nedeniyle işlerine devam edemedikleri günler (İK 55/h).
- İş Kanununun Ek 2. maddesinde sayılan mazeret izni süreleri (İK 55/ı). Söz konusu Ek 2. maddeye göre, işçiye, evlenmesi veya evlat edinmesi ya da ana veya babasının, eşinin kardeşinin, çocuğunun ölümü halinde üç gün, eşinin doğum yapması halinde ise beş gün ücretli izin verilir. İşçilerin en az yüzde yetmiş oranında engelli veya süreğen hastalığı olan çocuğunun tedavisinde, hastalık raporuna dayalı olarak ve çalışan ebeveynden sadece biri tarafından kullanılması kaydıyla, bir yıl içinde toptan veya bölümler halinde on güne kadar ücretli izin verilir.
- İşveren tarafından verilen diğer izinler ile 4447 sayılı İşsizlik Sigortası Kanununun ek 2. maddesinde yer alan kısa çalışma süreleri (İK 55/j).
- Bu yasanın uygulanması sonucu olarak işçiye verilmiş bulunan yıllık ücretli izin süresi (İK 55/k).

Yıllık ücretli izine hak kazanmada yukarıda belirtilen çalışılmış gibi sayılan süreler yasada sınırlayıcı bir biçimde düzenlenmiştir. Bu nedenle örneğin kadın işçilerin doğumdan sonra altı aya kadar kullanabilecekleri ücretsiz izinler<sup>837</sup> ile grev ve lokavtta geçirilen süreler<sup>838</sup> yıllık ücretli izin hakkının hesabında çalışılmış gibi sayılmaz.

İş Kanununun 54. maddesinin 2. Fıkrası uyarınca, 55. maddede öngörülen çalışılmış gibi sayılan haller dışında veya bu hükümde belirtilen süreleri aşan bir süre işçinin işine devam etmemesi durumunda, devamsızlık süresi izne hak kazanmak için çalışılması gereken bir yıllık süreye eklenir ve bu şekilde işçinin yıllık ücretli izne hak kazanacağı tarih bulunur.

---

<sup>837</sup> Narmanhoğlu, s. 701; Demir, s. 274

<sup>838</sup> Aktay/Arıcı/Kaplan, s. 254; Eyrenci/Taşkent/Ulucan, s. 336; Süzek, s. 832; Bingöl, s. 37; Demir, s. 274

Gerek Basın İş Kanununda ve gerekse Deniz İş Kanununda, çalışılmış gibi sayılan haller ayrıca düzenlenmemiştir. Ancak, 854 sayılı DİK'nun, 42 maddesinde<sup>839</sup>, hafta tatiline hak kazanma bakımından, çalışılmadan geçirilen bazı sürelerin çalışılmış gibi değerlendirileceği hükme bağlanmıştır. Dolayısıyla, söz konusu süreler, yıllık ücretli izne hak kazanma bakımından da çalışılmış gibi kabul edilecektir<sup>840</sup>. Keza, BİK'nun 19. maddesinin ikinci fıkrasında düzenlenen olağanüstü ücretli izinlerin<sup>841</sup> yine aynı maddede senelik izinden sayılamayacağı ifade edilmiştir<sup>842</sup>.

### III- YILLIK ÜCRETLİ İZİN SÜRELERİ

İş Kanununda yıllık ücretli izin süreleri, işçilerin işyerindeki hizmet süreleri ve yaşları esas alınarak belirlenmiştir. Çalışma süresi arttıkça işçiye verilmesi gereken ücretli izin süreleri de artmaktadır<sup>843</sup>.

İş Kanununun 53. maddesinin 4. fıkrası uyarınca "*işçilere verilecek yıllık ücretli izin süresi, hizmet süresi; a) Bir yıldan beş yıla kadar (beş yıl dâhil) olanlara ondört günden, b) Beş yıldan fazla onbeş yıldan az olanlara yirmi günden, c) Onbeş yıl (dâhil) ve daha fazla olanlara yirmialtı günden, az olamaz. Yer altı işlerinde çalışan işçilerin yıllık ücretli izin süreleri dörder gün arttırılarak uygulanır.*". Aynı maddenin 5. fıkrasına göre ise "*onsekiz ve daha küçük yaştaki işçilerle elli ve daha yukarı yaştaki işçilere verilecek yıllık ücretli izin süresi yirmi günden az olamaz.*". Bu süreler asgari olup, sözleşmelerle arttırılması mümkündür<sup>844</sup>.

Yasada çalışma süresi beş yıla kadar olanlara tanınan izin süresi ile ilgili olarak "*beş yıl dâhil*" ibaresine yer verilmiş, böylece 1475 sayılı yasa döneminde beş yıl kıdemi bulunanların

---

<sup>839</sup> DİK Madde 42 – Bu kanunun uygulandığı gemilerde, haftanın tatilden önceki günlerinde sürekli olarak çalışmış bulunan gemiadamlarına çalışılmayan hafta tatili günü için işveren veya işveren vekili tarafından bir iş karşılığı olmaksızın ve ücret ödeme şekline bakılmaksızın bir gündelik tutarında ücret ödenir. Evlenmelerde üç güne, ana ve babanın, karı ve kocanın, kardeş ve çocukların ölümünde iki güne kadar verilmesi gereken izin süreleriyle bir haftalık süre içinde kalmak üzere işveren tarafından verilen diğer izinler ve hekim raporlarıyla verilen dinlenme ve hastalık izinleri, fiilen çalışılmış günler gibi hesaba katılır

<sup>840</sup> **Karaman**, s. 119; **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s. 319

<sup>841</sup> BİK m. 19/2: "gazeteci, çocuğu dünyaya geldiği zaman üç; eşi veya çocuğu, anası veya babası öldüğü zaman dört; çocuğu evlendiği, kardeşi, büyük anne veya büyük babası veya torunu öldüğü zamanlar iki gün olağanüstü ücretli izine hak kazanır. Bu izinler senelik izinden sayılmaz"

<sup>842</sup> **Karaca / Günaydın**, s. 912; **Oğuz/Özge**, s. 105

<sup>843</sup> **Narmanhoğlu**, s. 705; **Çelik/Caniklioğlu/Canbolat**, s.695; **Süzek**, s. 632; **Eyrenci/Taşkent/Ulucan**, s. 337; **Demir**, s. 275

<sup>844</sup> **Narmanhoğlu**, s. 705; **Demir**, s. 275; **Eyrenci/Taşkent/Ulucan**, s. 338; **Çelik/Caniklioğlu/Canbolat**, s.695; **Aktay/Arıcı/Kaplan**, s. 255; **Bingöl**, s. 60

hangi gruba gireceği konusunda ortaya çıkan görüş ayrılığına açıklık getirilmiştir. Bu hükme göre işyerinde beş yıl hizmet süresini doldurmuş olanlar ondört gün, altıncı yılını doldurmuş olanlar ise yirmi gün yıllık ücretli izin hakkından yararlanacaklardır<sup>845</sup>.

Genç işçiler ile belirli bir yaşın üstündeki işçilerin fiziki açıdan korunmalarını sağlamak amacıyla İK'nun 53. maddesinin 5. fıkrasında, onsekiz ve daha küçük yaştaki işçilerle elli ve daha yukarı yaştaki işçilere verilecek yıllık ücretli izin süresinin yirmi günden az olamayacağı hükme bağlanmış ve diğer taraftan aynı maddenin 4. fıkrasına 6552 sayılı yasayla bir cümle eklenerek yer altı işlerinde çalışanların yıllık ücretli izin süreleri artırılmıştır. Bu hükme göre "*Yer altında çalışan işçilerin yıllık ücretli izin süreleri dörder gün artırılarak uygulanır*". Örneğin, 1-5 yıl arasında kıdeme sahip olan yer altında çalışan işçinin en az (ondört değil) onsekiz gün yıllık ücretli izin hakkı olacaktır. Bunun gibi, yer altında elli ve daha yukarı yaşta çalışan işçi varsa, beş yılını doldurmamış da olsa, yirmi değil, yirmidört gün yıllık ücretli izin hakkından yararlanacaktır<sup>846</sup>.

Yargıtay'a göre, yıllık ücretli izin alacağı tam bir yıl dolduktan sonra doğan bir hak olup, tam yıl üzerinden hesaplanmalıdır. Yıllık ücretli iznin kıstelyevm esasına göre yani tam yıl üzerindeki artık süreler için (kıdem tazminatı gibi) oranlama yapılarak hesaplanması şeklinde bir yasal düzenleme yoktur<sup>847</sup>.

İK m. 53/son'da ise "*yıllık izin süreleri iş sözleşmeleri ve toplu iş sözleşmeleri ile artırılabilir*" hükmüne yer verilmiştir. Bunun gibi çalışma koşulu haline gelen işyeri uygulamaları sonucunda da, yasal sürelerin üzerinde yıllık ücretli izin süreleri işyerinde geçerli hale gelebilir<sup>848</sup>.

Yıllık izin süresi belirlenirken işçinin izne hak kazandığı tarihteki hizmet süresi esas alınır. Örneğin işyerinde 4 yıllık hizmet süresi olan bir işçi 14 günlük yıllık ücretli izine hak kazanır. İşçi bu iznini iki yıl sonra kullansa bile, kullanma tarihinde hizmet süresi 6 yıl olmasına rağmen, bu süreye ilişkin izin süresi 20 gün değil, 14 gündür<sup>849</sup>. Diğer taraftan izin süresinin tespitine esas olacak çalışma süresinin belirlenmesinde işyerinde ya da aynı işverene ait çeşitli işyerlerinde devamlı veya aralıklı olarak çalışmış bir işçinin tüm çalışmaları gözönüne alınacağından işyerinden herhangi bir şekilde ayrılmış işçinin daha sonra aynı işyerinde ya da aynı işverenin emri altında

---

<sup>845</sup> **Süzek**, s. 832; **Eyrenci/Taşkent/Ulucan**, s. 338; **Çelik/Caniklioğlu/Canbolat**, s.695; **Bingöl**, s. 61

<sup>846</sup> **Süzek**, s. 833; **Çelik/Caniklioğlu/Canbolat**, s.695

<sup>847</sup> **Eyrenci/Taşkent/Ulucan**, s. 332; **Narmanlioğlu**, s. 699; **Süzek**, s. 833

<sup>848</sup> **Çelik/Caniklioğlu/Canbolat**, s.695

<sup>849</sup> **Eyrenci/Taşkent/Ulucan**, s. 339; **Narmanlioğlu**, s. 706, **Süzek**, s. 833

yeniden çalışmaya başlaması halinde eski çalışma süreleri de hesaba katılarak, kıdemine göre hak ettiği iznin verilmesi gerekir<sup>850</sup>.

İK m. 56/5'e göre, izin süresine rastlayan hafta tatili, ulusal bayram ve genel tatil günleri kanunen izin süresinden sayılmadığından, bu günlerin izin süresine ilave edilmesi gerekir<sup>851</sup>. Fakat iş sözleşmesinde ya da toplu iş sözleşmesinde kanuni izin sürelerinin üstünde işçilere izin süresi tanınmış olması halinde, kanuni sürenin ötesindeki sürelerle rastlayan hafta tatili, ulusal bayram ve genel tatil günlerinin izin süresinden sayılacağı kararlaştırılabilecektir<sup>852</sup>. Diğer taraftan kanuni tatil günleri dışında sözleşmelerle tatil günü kabul edilen günler ile Cumartesi çalışılmayan ve bugüne ait sürenin diğer iş günlerine bölünerek haftalık çalışma süresinin tamamlandığı işyerlerindeki işçilerin izin sürelerine, bir günlük hafta tatili dışında, ayrıca çalışılmayan cumartesi günleri eklenmez<sup>853</sup>. Çünkü çalışılmayan cumartesi gününe ait iş saatlerinin diğer beş güne dağıtılması, işçinin haftada bir yerine iki gün tatil yapmasını sağlamaya yönelik olup, daha uzun bir yıllık izin olanağının yaratılmasıyla ilgili değildir<sup>854</sup>.

İK'nun 56. maddesinin 6. fıkrasına göre, "*Yıllık ücretli izinleri işyerinin kurulu bulunduğu yerden başka bir yerde geçirecek olanlara istemde bulunmaları ve bu hususu belgelemeleri koşulu ile gidiş ve dönüşlerinde yolda geçecek süreleri karşılamak üzere işveren toplam dört güne kadar ücretsiz izin vermek zorundadır.*"<sup>855</sup> Yol izninin süresi toplam dört günü aşmamak üzere, işçinin iznini geçireceği yerin uzaklığı ve kullanılacak araç göz önünde tutularak belirlenecektir<sup>856</sup>. İzni başka yerde geçirmeyecek olmasına karşın yol izni alan işçinin bu davranışı sadakat borcuna aykırı olduğundan işverence iş akdi haklı nedenle feshedilebilir<sup>857</sup>. Yargıtay'a göre de yol izni sadece yıllık ücretli izin kullanımına hasredilmiştir ve diğer tatil günlerine teşmil edilemez. Aksi takdirde işçi, devamsızlık nedeniyle sözleşmenin feshi yaptırımıyla karşı karşıya kalabilir<sup>858</sup>. Diğer taraftan YÜİY'nin 8. maddesine göre, işveren, dört güne kadar alınan ücretsiz yol izin süresini kullanmadan

---

<sup>850</sup> Narmanhoğlu, s. 706;

<sup>851</sup> Eyrenci/Taşkent/Ulucan, s. 339; Çelik/Caniklioğlu/Canbolat, s.695; Aktay/Arıcı/Kaplan, s. 254

<sup>852</sup> Narmanhoğlu, s. 707; Çelik/Caniklioğlu/Canbolat, s.695; Bingöl, s. 66

<sup>853</sup> Eyrenci/Taşkent/Ulucan, s. 339; Çelik/Caniklioğlu/Canbolat, s.695; Bingöl, s. 67; Süzek, s. 835

<sup>854</sup> Süzek, s. 835

<sup>855</sup> Eyrenci/Taşkent/Ulucan, s. 340; Süzek, s. 707; Demir, s. 276; Bingöl, s. 62; Çelik/Caniklioğlu/Canbolat, s. 697; Demircioğlu/Centel, s. 141; Sümer, s. 153

<sup>856</sup> Mollamahmutoğlu s. 959

<sup>857</sup> Süzek, s. 835; Bingöl, s. 62; Mollamahmutoğlu s. 960; Çelik/Caniklioğlu/Canbolat, s.697

<sup>858</sup> YARGITAY 9. HUKUK DAİRESİ E. 2015/18758 K. 2017/7248 T. 25.4.2017 (Süzek, s. 835)

işçi işe dönerse, anılan sürenin bitiminden önce işe başlatmama hakkına sahip olduğu için işçinin bu talepte bulunurken dikkatli davranması gerekecektir<sup>859</sup>.

İK'nun 56. maddesinin 4. fıkrasında, “işveren tarafından işçilere yıl içinde verilmiş olan ücretli ya da ücretsiz izinlerin veya dinlenme yahut hastalık izinlerinin yıllık izne mahsup edilemeyeceği” ayrıca belirtilmiştir. Bu şekilde yıl içinde başka nedenlerle verilen izinlerin yıllık izne karşılık tutulması suretiyle kısaltılması veya tamamen ortadan kaldırılması önlenmek istenmiştir<sup>860</sup>. Buna karşılık iznini kullanan işçinin hastalanması halinde nasıl hareket edileceğine ilişkin açık bir düzenleme bulunmamaktadır. Ancak, yıllık iznini kullanırken hastalanan işçinin raporla belgelenen istirahat günlerinin yıllık izin günlerinden sayılmayıp izin sürelerine eklenmesi gerekeceği, doktrinde isabetli olarak ifade edilmektedir<sup>861</sup>.

Basın İş Kanunu açısından, “Günlük Bir Mevkutede Çalışan Gazeteciler” ile “Günlük Olmayan Mevkutelerde Çalışan Gazeteciler” bakımından bir ayrıma gidilmiştir. BİK'nun 21. maddesine göre, günlük bir mevkutede çalışan gazeteci, kanunda öngörülen en az bir yıl çalışmış olma koşulunu sağlamışsa, yıllık ücretli izin süresini meslekteki kıdemini 10 yıldan az ya da çok oluşu belirleyecektir. Kıdemi 10 yıla kadar olan gazeteciler, yılda 4 hafta; kıdemi 10 yıldan yukarı olanlar ise 6 hafta yıllık ücretli izne hak kazanacaktır. Yukarıda değinildiği üzere, 6 aylık çalışma devresini tamamlayan günlük olmayan mevkutelerde çalışan gazeteciler, yıllık ücretli izne hak kazanmaktadırlar. Kanunda her altı aylık çalışma devresi için iki hafta ücretli izin hakkı tanındığına göre, 6 aylık çalışma devresi arttığı ölçüde yıllık ücretli izin süresi de artacaktır. Dolayısıyla iki altı aylık çalışma devresi için 4 hafta, üç altı aylık çalışma devresi için 6 hafta yıllık ücretli izin kullanılabilir<sup>862</sup>.

Deniz İş Kanununun 40. maddesinde ise, gemi adamının, altı aydan bir yıla kadar hizmetinin olması durumunda onbeş günden, bir yıl ve daha fazla hizmetinin olması durumunda ise yılda bir aydan az olmamak üzere yıllık ücretli izne hak kazanacağı düzenlenmiştir<sup>863</sup>.

Gerek Deniz İş Kanunu ve gerekse Basın İş Kanunu, 4857 sayılı İş Kanunu ve Türk Borçlar Kanunundan farklı olarak, işçinin yaşını dikkate alarak hak kazanılacak yıllık ücretli izin

---

<sup>859</sup> Günay, s. 33

<sup>860</sup> Eyrenci/Taşkent/Ulucan, s. 339; Süzek, s. 707; Bingöl, s. 65; Süzek, s. 835; Sümer, s. 153

<sup>861</sup> Narmanhoğlu, s. 707; Çelik/Caniklioğlu/Canbolat, s.697; Aktay/Arıcı/Kaplan, s. 255; Bingöl, s. 70; Süzek, s. 835

<sup>862</sup> Karaca/Günaydın, s. 912; Oğuz/Özge, s. 102

<sup>863</sup> Akyiğit, Deniz İş Kanununda Yıllık Ücretli İzin, s. 312; Karaman, s. 116



konusunda ayrı bir düzenleme getirmemiştir. Bu nedenle, gazeteci ve gemi adamının yaşı ne olursa olsun, sadece kıdem süreleri esas alınarak yıllık ücretli izin hakkı belirlenecektir<sup>864</sup>.

#### IV- YILLIK ÜCRETLİ İZİNİN KULLANILMASI

##### A- GENEL OLARAK

Yıllık ücretli iznin niteliği, onun, işçi açısından mutlaka kullanılmasını ve işveren açısından da kullandırılmasını gerektirmektedir. İşçi onay verse de, işveren izni kullandırma yükümlülüğünden kurtulamaz ve özellikle, uygulamada karşılaşıldığı şekilde, yıllık izin hakkı paraya çevrilemez<sup>865</sup>.

İK m. 54/4 uyarınca işçinin hizmet süresine göre hak ettiği yıllık ücretli iznini, hak kazandığı yılı izleyen yıl içinde kullanması asıldır. İzin kullanılmasına engel olan (hastalık, grev gibi) istisnai durumlar yoksa iznin daha sonraki yıla veya yıllara ertelenmesi, izinlerin birleştirilerek kullanılması işçinin dinlendirilmesi amacına ters düşer<sup>866</sup>. Ancak çalışmakta iken yıllık izin talebinde bulunmaması nedeniyle işçinin yıllık ücretli izin parasına ilişkin isteği reddedilemez<sup>867</sup>.

İK'nun 56. maddesinin 1 ve 2. fıkralarına göre, işçiye kıdemine göre hak ettiği yıllık izin kural olarak bölünmeden ve m.53'de gösterilen süreler içinde işveren tarafından sürekli bir şekilde verilmesi gerekir. Tarafların anlaşması ile izin sürelerinin en çok üçe bölünebileceğini<sup>868</sup> öngören İK'nun 56. maddesinin, 3. fıkrası 14.4.2016 tarihli ve 6704 sayılı yasanın 16. maddesiyle değiştirilmiş ve bir bölümü on günden az olmamak üzere bölümler halinde kullanılabilmesi hüküm altına alınmıştır.

Bu çerçevede, hak kazanıldığı yılı izleyen yıl içinde kullanılması gereken yıllık izin her yıl kullandırılması asıldır. Yıllık iznin amacı, işçinin yıl içinde belirli bir süre kesintisiz dinlenmesini sağlamaktır. Bu nedenle izinlerin birleştirilerek sonraki yıllarda kullanılması ya da

---

<sup>864</sup> **Karaman**, s. 121; **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s. 316

<sup>865</sup> **Eyrenci/Taşkent/Ulucan**, s. 339; **Narmanhoğlu**, s. 707; **Süzek**, s. 834; **Mollamahmutoğlu**, s. 953;

<sup>866</sup> **Süzek**, s. 829; **Demir**, s. 276; **Eyrenci/Taşkent/Ulucan**, s. 339; **Çelik/Caniklioğlu/Canbolat**, s.695; **Narmanhoğlu**, s. 708; **Demircioğlu/Centel** s. 140; **Sümer**, s. 153; **Sevimli**, s. 42

<sup>867</sup> **Çelik/Caniklioğlu/Canbolat**, s. 701; **Sevimli, Ahmet**, Yıllık Ücretli İzinin Kullanılmamasının Hukuki Sonuçları Hakkında Kısa Bir Not, Sicil İş Hukuku Dergisi, Yıl 2010, Yıl 5, Sayı 18, s. 41

<sup>868</sup> **Narmanhoğlu**, s. 708; **Eyrenci/Taşkent/Ulucan**, s. 340

kullanılması bu amaçla bağdaşmamaktadır. Bununla beraber, iznin kullanılmasına engel olan bir kısım (hastalık, grev gibi) sebepler söz konusuysa iznin daha sonraki yılda veya yıllarda kullanılması kararlaştırılabilir<sup>869</sup>.

## **B- İŞ AKDİ DEVAM EDERKEN YILLIK İZİN HAKKININ PARAYA TAHVİL EDİLEMEYECEĞİ**

Hak kazanıp da kullanamadığı yıllık izin süresine ait ücretini iş akdinin herhangi bir nedenle sona ermesi halinde isteyebilen işçi, iş akdi devam ederken kullanamadığı izin günlerine karşılık ücretini talep edemez. Aynı şekilde işveren de yıllık izin süresine ilişkin ücreti ayrıca ödeyerek, bu sürede işçiyi çalıştırıp, yıllık izin hakkını kullandırmaktan kaçınamaz. Çünkü yasanın amacı, bu sürelerle karşılık ücretin ödenmesi değil, işçilerin dinlenmelerinin sağlanmasıdır. Yıllık izin sürelerinin ücrete dönüşmesi ancak artık izin kullandırma olanağının kalmadığı, iş akdinin sona ermesi halinde gerçekleşir<sup>870</sup>.

Ancak, Yargıtay 7. Hukuk Dairesi ücretli izin hakkının niteliğine ilişkin olarak benimsenmiş bu temel ilkeyle bağdaşmayan bir kararında<sup>871</sup> şöyle hüküm kurmuştur: *“Davacı çalışma süresi ve kıdemine göre sadece 1 yıllık izin karşılığı 14 gün yıllık izne hak kazanmıştır. Davacının, hak ettiği bu yıllık iznini mutlaka izin olarak kullanma zorunluluğu bulunmayıp işverenle anlaşması halinde... izin hakkının karşılığı ücret almak suretiyle de o yılın izin hakkını kullanmış sayılır. Somut olayda davacı hak ettiği 1 yıllık iznin karşılığının ödendiğini belirttiğinden davacının yıllık izin ücreti alacağı bulunmamaktadır.”*

Oysa yıllık ücretli izin hakkı, işçinin sağlığının korunması ve işgücünün yenilenmesi amacıyla konulmuş anayasal bir dinlenme hakkıdır (AY 50). Bu hakkın parasal karşılığının ödenmesi suretiyle uygulanmasından kaçınılması gerekir. Nitekim Borçlar Kanununun 425. maddesinin 2. fıkrasında açıkça öngörüldüğü gibi *“İşçi, hizmet ilişkisi devam ettiği sürece, işverenden alacağı para ve başka menfaatler karşılığında yıllık ücretli izin hakkından feragat edemez.”* Ayrıca anılan yasanın 81. maddesinde *“Hukuka... aykırı bir sonucun gerçekleşmesi amacıyla verilen şey geri istenemez”* denildiğinden, işverence izin verilmemesi karşılığında işçiye ödenmiş olan ücretin, sebepsiz zenginleşme kuralları gereğince geri istenebilmesi de mümkün değildir<sup>872</sup>.

---

<sup>869</sup> Narmanhoğlu, s. 708; Eyrenci/Taşkent/Ulucan, s. 340; Mollamahmutoglu, s. 952, 953

<sup>870</sup> Süzek, s. 839; Sevimli, s. 42; Narmanhoğlu, s. 714; Yargıtay 9. HD, 1.2.2010 E. 2009/47110, K 201/1923 (Narmanhoğlu, s. 714);

<sup>871</sup> YARGITAY 7. HUKUK DAİRESİ E. 2013/20246 K. 2014/3500 T. 10.2.2014, (Süzek, s. 839)

<sup>872</sup> Süzek, s. 840

Deniz İş Kanunu açısından da, gemiadamının, yıllık ücretli izin süresince çalışarak yıllık izin ücretini talep etmesi mümkün olmaması gerekir. Bu durum, yıllık ücretli izin hakkını fiilen kullanma hakkından feragat edildiği anlamına gelecektir. Böyle bir durumun ise, Kanundaki, yıllık ücretli izin alacağından feragat edilemeyeceği şeklindeki yasal düzenleme (m. 40/3) karşısında mümkün olmadığı açıktır. Gemi adamının, iş sözleşmesinin sona ermediği bir dönemde, birikmiş izinlerini kullanmak yerine karşılığı ücretleri talep etmesi de, yıllık izin hakkının kullanılmasından feragat anlamına geleceğinden hukuken mümkün olmayacaktır<sup>873</sup>.

Yıllık ücretli izin hakkından feragat edilemeyeceği, Basın İş Kanununda da özel olarak hükme bağlandığından, yıllık ücretli iznin kullanılmak yerine işçi veya işveren tarafından paraya tahvil edilmek istenmesi mümkün değildir<sup>874</sup>. Ancak BİK'nun 29. maddesine göre, gazeteciye yıllık iznini kullandırmayan veya kullandırdığı halde izin süresine ilişkin ücreti ödemeyen işveren, izin süresine tekabül eden ücretleri gazeteciye iki katı olarak ödemek yükümlülüğündedir. İş sözleşmesi devam ederken, izin kullandırılmasına rağmen ücret ödenmemiş ise, en geç izne başlarken ödenmesi gereken bu ücret için sözleşmenin devamı sırasında dava açılabilir. Buna karşın iş sözleşmesinin devamı sırasında kullandırılmayan yıllık izin ücreti için ise dava açılabilmesi mümkün değildir<sup>875</sup>

### C- YILLIK İZİN TARİHİNİN BELİRLENMESİ

İş Kanununun 60. maddesi uyarınca, izinlerin hangi tarih ve dönemde ve hangi usul çerçevesinde uygulanacağını ayrıntıları 3.3.2004 tarihli Yıllık Ücretli İzin Yönetmeliğinde gösterilmiştir. Yönetmelikte, İş Kanununda yer alan hükümlere paralel kuralların yanında, izin kullanma dönemleri, işçinin izin isteğinin zamanı ve izin tarihinin verilmesi, toplu izinlerin uygulanması, yıllık ücretli izin kurulunun oluşumu, bu kurulun görev ve yıllık izin çizelgelerinin hazırlanması, yıllık izin kaydı tutulması ayrıntılı olarak düzenlenmiştir.

İşçi, kanunun öngördüğü şartları yerine getirdiği anda yıllık izne hak kazanırsa da, bu hak, işverenin yönetim hakkı kapsamında yer aldığından izin hakkının doğumu tarihinde kendiliğinden kullanma yoluna gitmesi mümkün değildir<sup>876</sup>. İşçinin izne çıkacağı tarihi belirleme yetkisi işverene veya işveren vekiline ait bulunmaktadır<sup>877</sup>. İşçinin izin dilekçesi bırakmış olması kendisine o tarihte

---

<sup>873</sup> Karaman, s. 123; Akyiğit, Deniz İş Kanununda Yıllık Ücretli İzin, s. 322

<sup>874</sup> Oğuz/Özge, s. 103

<sup>875</sup> Karaca / Günaydın, s. 912; Oğuz/Özge, s. 105

<sup>876</sup> Demir, s. 277

<sup>877</sup> Eyrenci/Taşkent/Ulucan, s. 340; Narmanhoğlu, s. 708; Mollamahmutoğlu, s. 954; Demircioğlu/Centel, s. 141; Sümer, s. 153; Sevimli, s. 41

izin kullanılacağı anlamına gelmeyecektir. Üstelik işyerinde eskiden böyle bir uygulama olması da işçiye bir hak sağlamayacaktır<sup>878</sup>. İşçi izni dilediği zaman kullanamayacağından, izin dilekçesini verip, işverenin bunu kabul etmesini beklemeden işten ayrılması, iş sözleşmesini o tarihte feshettiğini gösterir<sup>879</sup>. Yargıtay'ın bir kararına<sup>880</sup> göre, “İşçinin yıllık iznini kullandığını belirterek işyerine gelmemesi, işverence izinli sayılmadığı sürece devamsızlık halini oluşturur.”

Ancak, İşçinin, izne hak kazandığı hizmet yılını takip eden hizmet yılı içinde izin tarihi belirlenerek izne çıkartılmaması, hukuka aykırıdır. İşverenin bu davranışı iş koşullarının uygulanmaması (İK.m.24/II-f) ve hatta işçi aleyhine ağırlaştırılması anlamına gelir. Öte yandan bu tutum, işverenin işçiyi gözetme borcuna da aykırıdır. Bu nedenle, yıllık ücretli iznin zamanında kullanılmaması durumunun işçi için haklı nedenle derhal fesih yetkisi doğuracağına kabulü gerekir<sup>881</sup>.

Yıllık Ücretli İzin Yönetmeliği, yıllık iznin tarihinin belirlenmesi hususunda ayrıntılı düzenlemeler yapmıştır. Buna göre, yıllık izne hak kazanan işçi, izne ayrılmak istediği tarihten en az bir ay önce iznini ne zaman kullanmak istediğini işverene yazılı olarak bildirir (YÜİY m. 7/1). İşçi bu isteminde, adını soyadını, varsa sicil numarasını, iznini hangi tarihler arasında kullanmak istediğini ve ücretsiz yol izni isteyip istemediğini yazar (YÜİY m. 8/1). İzin vermeye yetkili kişi veya şartları varsa kurul<sup>882</sup>, işçilerin istedikleri tarihler ile bağlı olmamakla birlikte, işçinin talebini olabildiğince göz önünde bulundurarak ve işçilerin işyerindeki kıdemi ve önceki yıl iznini kullandığı tarihi, izni kullanmak istedikleri dönem açısından zorunluluklar ile engeller, işyerinde işin aksatılmaması ve işçi sayısını da dikkate alarak bir izin çizelgesi hazırlayarak işverenin onayına sunar<sup>883</sup>.

İzne yetkili kişi ya da kurul işçinin istediği tarihle bağlı değilse de (YÜİY m.8) bu isteği olabildiğince gözönünde bulundurmak durumundadır. Ücretli İzin Yönetmeliğine göre izin

<sup>878</sup> Özuysal, Neslihan, Yıllık Ücretli İzin, İstanbul Barosu Dergisi, Cilt: 83, Sayı: 5, Eylül 2009, s. 2585

<sup>879</sup> Mollamahmutoğlu, s. 954

<sup>880</sup> YARGITAY 9. HUKUK DAİRESİ E. 2014/30472 K. 2016/3413 T. 22.2.2016, Kazancı İçtihat Bilgi Bankası, (<http://www.kazanci.com/kho2/ibb/files/dsp.php?fn=9hd-2014-30472.htm&kw=22.2.2016+30472#fm>, Erişim Tarihi: 143.201)

<sup>881</sup> Günay, s. 32; Sevimli, s. 43

<sup>882</sup> Yıllık Ücretli İzin Yönetmeliğinin 15 maddesine göre; “İşçi sayısı yüzden fazla olan işyerlerinde işveren veya işveren vekilini temsilen bir, işçileri temsilen iki kişi olmak üzere toplam üç kişiden oluşan izin kurulu kurulur. Kurula işveren temsilcisi başkanlık eder. Kurulun başkanı dışında kalan işçi üyeleri ve yedekleri işyerinde varsa, işyeri sendika temsilcileri tarafından seçilir.”

<sup>883</sup> Eyrenci/Taşkent/Ulucan, s. 340; Narmanhoğlu, s. 709; Aktay/Arıcı/Kaplan, s. 256; Demir, s. 277; Sümer, s. 154

çizelgelerinin hazırlanmasında, işçilerin kıdemleri, izni kullanmak istedikleri dönem açısından zorunluluklar ile engeller, işyerinde işin aksatılmadan sürdürülmesi ve işçi sayısı gözönünde tutulur<sup>884</sup>. Örneğin aynı tarihe rastlayan izin isteklerinde; işyerindeki kıdem ve bir önceki yıl iznini kullandığı tarih dikkate alınarak öncelikler belirlenir (YÜİY m.8/3).

4857 Sayılı Kanunda yer verilmemesine rağmen, Yönetmelik "toplu izin" esasına yer vermiştir<sup>885</sup>. Buna göre, *"işveren veya işveren vekili nisan ayı başı ile ekim ayı sonu arasındaki süre içine, işçilerin tümünü veya bir kısmını kapsayan toplu izin uygulayabilir. Bu uygulamaya gidildiğinde, izin kurulu izin çizelgelerini, toplu izne çıkacak işçiler, aynı zamanda izne başlayacak ve izin sürelerine ve yol izni isteklerine göre her işçinin izin süresinin bitimini gösterecek biçimde düzenler ve ilan eder. Toplu izin dönemleri, bu dönemlerde henüz yıllık ücretli izin hakkını kazanmayan işçileri de kapsayacak şekilde belirlenebilir. Şu kadar ki, ertesi yıl veya yıllarda bu toplu izin yönteminin uygulanmaması halinde, bu durumda olanların gelecek yıl izne hak kazanacakları tarih genel esaslara göre belirlenir"* (YÜİY m. 10). Yönetmeliğin 11.maddesinde, toplu izin dışında bırakılacak işçiler de gösterilmiştir<sup>886</sup>.

İş Kanununun 56. maddesine 10.9.2014 tarihli ve 6552 sayılı yasa ile bir fıkra eklenmiş ve işyerinde alt işverenler yanında çalışan işçilerin yıllık ücretli izinleri güvence altına alınmıştır. Aynı hüküm, YÜİY'nin 6. maddesinin son fıkrası olarak 18.8.2017 tarih ve 30158 sayılı Resmi Gazete ile yönetmeliğe eklenmiştir<sup>887</sup>. Anılan hüküm uyarınca *"Alt işveren işçilerinden, alt işveren değiştiği halde aynı işyerinde çalışmaya devam edenlerin yıllık ücretli izin süresi, aynı işyerinde çalıştıkları süreler dikkate alınarak hesaplanır. Asıl işveren, alt işveren tarafından çalıştırılan işçilerin hak kazandıkları yıllık ücretli izin sürelerinin kullanılıp kullanılmadığını kontrol etmek ve ilgili yıl içinde kullanılmasını sağlamakla, alt işveren ise tutmak zorunda olduğu izin kayıt belgesinin bir örneğini asıl işverene vermekle yükümlüdür"*. Yargıtay'ın bu konudaki bir kararına göre, asıl işverenin işyerinde iş alan bir alt işverenin işçisi asıl işveren ile ilgili işyerinden ayrıldığı sırada hizmet akdi henüz sona ermediğine göre asıl işverenin yıllık izin alacağından sorumlu tutulması doğru değildir<sup>888</sup>.

---

<sup>884</sup> Narmanlioğlu, s. 709; Eyrenci/Taşkent/Ulucan, s. 341; Aktay/Arıcı/Kaplan, s. 256

<sup>885</sup> Eyrenci/Taşkent/Ulucan, s. 341; Aktay/Arıcı/Kaplan, s. 256; Demir, s. 277; Çelik/Caniklioğlu/Canbolat, s. 699; Sümer, s. 154

<sup>886</sup> Demir, s. 278; Aktay/Arıcı/Kaplan, s. 256; Çelik/Caniklioğlu/Canbolat, s. 700

<sup>887</sup> Süzek, s. 836; Eyrenci/Taşkent/Ulucan, s. 344; Demir, s. 278; Sümer, s. 154

<sup>888</sup> Yargıtay 9.HD. 6.5.2004, E. 2004/607 - K. 2004/10743 (Günay, s. 37)

Deniz İş Kanununun 40. maddesinin 3. fıkrasında, “*izin işverenin uygun göreceği bir zamanda kullanılır.*” denilmek suretiyle bu konuda düzenleme yapma ve nihai karar verme yetkisinin işverende olduğu açıkça belirtilmiştir. Bu nedenle, gemiadamının, yıllık ücretli izne hak kazanması ve hak kazandığı izni kullanmak için yazılı talepte bulunması iznin fiilen kullanılabilmesi için yeterli değildir. İşverenin, bu talep kapsamında işçiye yıllık ücretli izni kullanma yönünde izin vermesi ve izne çıkacağı tarihi belirlemesi de gerekecektir<sup>889</sup>. Deniz İş Kanununda, gemi adamının, yıllık ücretli iznini yabancı bir memleket limanında veya hizmet akdinin yapılmış olduğu yerden başka bir yerde kullanmaya zorlanamayacağı ayrıca hükme bağlanmıştır (m. 40/5). Bu düzenlemeden hareketle, gemi adamının, yabancı bir ülkede iken yıllık ücretli izne çıkmak istemesi ve yıllık ücretli izne çıkması halinde, yurda dönmek için de ücretsiz izin talep edebilecektir<sup>890</sup>. Diğer taraftan, Deniz İş Kanunu, “*Bir aylık izin, tarafların rızasıyla aynı yıl içerisinde kullanılmak suretiyle ikiye bölünebilir.*” hükmünü içermektedir (m.40/4). Bu düzenlemeden anlaşılacağı üzere, gemi adamının, ilk 6 aylık çalışması sonucunda hak kazanacağı ücretli izin dışında, her bir yıllık çalışması karşılığında hak kazanacağı yıllık ücretli izni, aynı yıl içerisinde olmak şartıyla, bir bütün olarak kullanılabilmesi gibi ikiye bölünmek suretiyle iki parça halinde kullanması da mümkündür<sup>891</sup>.

Basın İş Kanununda bu konuda özel bir düzenleme bulunmamakla beraber, işveren yönetim hakkı kapsamında yıllık ücretli iznin kullanım zamanını düzenleyebileceği, ancak işlerin aksamaması için yıllık izin taleplerinin zamanını belirlerken, bir yandan da işçinin menfaatini de koruyarak, yıllık iznini en verimli kullanacağı zamanı gözetmesi gerektiği sonucuna varılmalıdır<sup>892</sup>. Aynı zamanda Basın İş Kanunu’nun 21. maddesinde dört haftalık yıllık ücretli iznin tam olarak verileceği belirlenmiştir. İş Kanunu’ndan farklı olarak, Deniz İş Kanunundaki gibi yıllık iznin bölünerek verilebilmesi konusunda bir düzenleme bulunmamaktadır. Ancak gazeteci ve işveren anlaşarak, kanunda belirlenen asgari yıllık izin sürelerini azaltmadan, iznin bölünerek kullanılacağını kararlaştırabilirler<sup>893</sup>.

#### **D- YILLIK ÜCRETLİ İZİN KULLANIMININ İSPATI**

Uygulamada yıllık izin ücreti alacağına ilişkin uyuşmazlıklarda, işçinin yıllık iznini kullanıp kullanmadığı, bunun ispatı ve ispat külfetinin hangi tarafta olduğu önem kazanmaktadır.

---

<sup>889</sup> **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s. 323; **Karaman**, s. 123

<sup>890</sup> **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s. 318; **Karaman**, s. 125

<sup>891</sup> **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s. 328; **Karaman**, s. 124

<sup>892</sup> **Oğuz/Özge**, s. 104

<sup>893</sup> **Oğuz/Özge**, s. 103

Yıllık izin ile ilgili mevzuat hükümleri dikkate alındığında, işçiye yıllık ücretli izin verildiğinin ispatı işverene düşmektedir. Nitekim Yargıtay ötedenberi verdiği kararlarda izin için gerekli kayıt ve defterleri tanzim etmenin işverenin görevi olduğu ve bu bakımdan izinlerin verildiği hususunda ispat yükünün işverende olduğunu kabul etmiş ve bu öğretide de benimsenmiştir<sup>894</sup>. Yine Yargıtay kararlarına göre, işçiye yıllık ücretli izin verildiği işverenin kanunen tutmakla yükümlü olduğu belgelerle ispat etmesi gerekir. Söz konusu kayıtların ispat gücü taşıyabilmesi için ilgili işçinin imzasının da bulunması gerekir<sup>895</sup>.

## V- YILLIK İZİN ÜCRETİ

İş Kanununun 57. (ve TBK'nun m. 425) maddesinin 1. fıkrası uyarınca "*İşveren, yıllık ücretli iznini kullanan her işçiye, yıllık izin dönemine ilişkin ücretini ilgili işçinin izine başlamasından önce peşin olarak ödemek veya avans olarak vermek zorundadır*". Ayrıca aynı maddenin son fıkrasına göre işçiye "*Yıllık ücretli izin süresine rastlayan hafta tatili, ulusal bayram ve genel tatil ücretleri ayrıca ödenir*"<sup>896</sup>. YÜİY'nin 21/2. maddesine göre de "*İşveren veya işveren vekili, yıllık ücretli iznini kullanan her işçiye izin dönemine ilişkin ücreti ile ödenmesi bu döneme rastlayan diğer ücret ve ücret niteliğindeki haklarını izine başlamadan önce peşin olarak vermek veya avans olarak ödemek zorundadır*".

Ayrıca kanundaki izin sürelerinin sözleşmeyle artırılması halinde, kanuni süreyi aşan sürelerle ilişkin tatil günleri için ücret ödenmeyeceği sözleşmeyle kararlaştırılabilir<sup>897</sup>. Yıllık izin süresi içinde kalan tatil günlerine ilişkin ücretlerin de ayrıca ödenmesini öngören İş Kanununun 57. maddesinin son fıkrasına benzer bir hüküm, Borçlar Kanunu ve Deniz İş Kanununda bulunmamaktadır. Buna karşın Basın İş Kanununda ise sadece yıllık izin süresine tesadüf eden süre içindeki hafta tatili gününün izin süresine ekleneceği ve bu günlere ilişkin ücretin ayrıca ödeneceği (BİK m.19) öngörülmektedir<sup>898</sup>.

İşçinin izine çıkmadan ödenen yıllık izin ücreti temel (çıplak) ücreti üzerinden hesaplanır. İş Kanununun 57. maddesinin 2. fıkrasında, İK m. 50'ye yapılan yollama nedeniyle fazla çalışma

---

<sup>894</sup> Eyrenci/Taşkent/Ulucan, s. 344-345; Narmanhoğlu, s. 708; Süzek, s. 836; Mollamahmutoğlu, s. 958; Aktay/Arıcı/Kaplan, s. 256; Demir, s. 279; Sümer, s. 154; Sevimli, s. 41; Günay, s. 38

<sup>895</sup> Örneğin, YARGITAY 22. HUKUK DAİRESİ E. 2013/27398 K. 2015/644 T. 21.1.2015; YARGITAY 22. HUKUK DAİRESİ E. 2014/35061 K. 2015/967 T. 26.1.2015; YARGITAY 7. HUKUK DAİRESİ E. 2015/4328 K. 2015/5921 T. 31.3.2015 (Süzek, s. 836)

<sup>896</sup> Süzek, s. 836; Eyrenci/Taşkent/Ulucan, s. 341; Narmanhoğlu, s. 709; Demir, s. 280; Çelik/Caniklioğlu/Canbolat, s. 701

<sup>897</sup> Narmanhoğlu, s. 709

<sup>898</sup> Narmanhoğlu, s. 709

ücretleri, sosyal yardımlar, prim, ikramiye vb. ücretler; hazırlama, tamamlama ve temizleme işlerinden alınan ek ücretler tatil ücretlerinin belirlenmesinde göz önünde tutulmaz<sup>899</sup>.

İşçinin peşin ödenecek izin ücretinin hesaplanmasında onun bir günlük temel ücretinin bulunması ve bunun İK m. 53'e göre hak ettiği yıllık izin süresi ile çarpılması gerekir. İşçiye zamana göre (saat başına, günlük, haftalık, aylık) ücret ödenmesi halinde, hafta tatili, ulusal bayram ve genel tatil ücretlerinin hesaplanmasına ilişkin esaslar burada da uygulanır. Buna karşılık, günlük, haftalık veya aylık olarak belirli bir ücrete dayanmayıp da akort, komisyon ücreti, kâra katılma ve yüzde usulü ücret gibi belirli olmayan süre ve tutar üzerinden ücret alan işçinin yıllık izin ücreti, son bir yıllık süre içinde kazandığı ücretin fiili olarak çalıştığı günlere bölünmesi suretiyle bulunacak ortalama üzerinden hesaplanır (İK 57/3). Ancak, son bir yıl içinde işçi ücretine zam yapıldığı takdirde, izin ücreti işçinin izine çıktığı ayın başı ile zammın yapıldığı tarih arasında alınan ücretin aynı süre içinde çalışılan günlere bölünmesi suretiyle belirlenir (İK 57/4). Yüzde usulünün uygulandığı yerlerde bu ücret, yüzdelerden toplanan paralar dışında işveren tarafından ödenir (İK 57/5; YÜİY m. 21/3). Yıllık Ücretli İzin Yönetmeliğinin 21. maddesinin son fıkrası uyarınca kısmi süreli ve çağrı üzerine çalışmalarda, işçinin yıllık izin dönemine rastlayan (çalışsaydı elde edeceği) ücretleri kendisine yıllık izin ücreti olarak ödenir<sup>900</sup>.

İzin günlerine ait ücretin hesap edilebilmesi için günlük ücretin bulunması gerekir. Zaman esasına göre ücret halinde aynen tatil ücretlerinde olduğu gibi, saat ücretinde, saat başına ücretin 7,5 katı; gündelik ücrette, kararlaştırılan gündelik; haftalık ücrette, ücretin 7'ye bölünmesi suretiyle bulunan bir günlük ücret; maktu aylık ücretin de aylığın otuzda biri yıllık izin ücretinin bir güne düşen miktarını oluşturur<sup>901</sup>.

Ancak, İK m. 58 uyarınca, yıllık ücretli iznini kullanmakta olan işçinin izin süresi içinde ücret karşılığı bir işte çalıştığı anlaşılırsa, bu izin süresi için kendisine ödenen ücret işveren tarafından geri alınabilir<sup>902</sup>. Demir'e göre maddede ücret karşılığı çalışmadan bahsedildiğine göre

---

<sup>899</sup> **Süzek**, s. 837; **Narmanlioğlu**, s. 709; **Eyrenci/Taşkent/Ulucan**, s. 341; **Mollamahmutoğlu**, s. 956; **Aktay/Arıcı/Kaplan**, s. 256; **Demir**, s. 280; **Çelik/Caniklioğlu/Canbolat**, s. 700; **Sümer**, s. 155; **Günay**, s. 36; **Özdemir, Cumhuriyet Sinan**, İşçilerde Yıllık Ücretli İzin Uygulaması Ve Birikmiş İşçi İzinlerinin Kullanılması, Mali Çözüm Dergisi, Eylül-Ekim 2010, s. 274

<sup>900</sup> **Süzek**, s. 837; **Narmanlioğlu**, s. 710; **Eyrenci/Taşkent/Ulucan**, s. 342; **Aktay/Arıcı/Kaplan**, s. 256; **Demir**, s. 280; **Çelik/Caniklioğlu/Canbolat**, s. 700; **Sümer**, s. 155; **Günay**, s. 37; **Özdemir**, İşçilerde Yıllık Ücretli İzin Uygulaması, s. 274

<sup>901</sup> **Mollamahmutoğlu**, s. 956; ; **Çelik/Caniklioğlu/Canbolat**, s. 685 ve 700; **Sümer**, s. 155

<sup>902</sup> **Süzek**, s. 836; **Eyrenci/Taşkent/Ulucan**, s. 342; **Narmanlioğlu**, s. 711; **Mollamahmutoğlu**, s. 960; **Demir**, s. 280; **Çelik/Caniklioğlu/Canbolat**, s. 701



işçinin bir işverene bağlı olmaksızın pazarcılık yapması izin ücretinin geri verilmesi gerektirmez<sup>903</sup>. Mollamahmutoğlu'na göre ise, burada ücret karşılığı çalışmanın mutlaka iş sözleşmesine dayanması gerekmez; ücret karşılığı çalışma hizmet, istisna, vekâlet, nakliye, adi şirket gibi herhangi bir sözleşmeye dayanabilir. Yıllık izinde çalışma yasağı bağlamında ücret karşılığı çalışma genel bir ifadeyle izin sırasında kazanç sağlayıcı bir işte çalışmayı kapsar. Şu halde işçinin izin süresi içinde kazanç gayesi gütmeyen, bir ücret almadan çalışması mümkündür. Ancak izinde çalışma yasağı kural olduğundan çalışmanın karşılıksız olduğunu işçinin ispat etmesi gerekir<sup>904</sup>. Buna karşılık işçi kısmi süreli işte çalışıyorsa ve diğer işverenin yanında yıllık izin hakkını aynı zamana getirmediği için o işle sınırlı bir biçimde çalışıyorsa ücretin geri alınması söz konusu olmayacaktır<sup>905</sup>.

4857 sayılı İş Kanununun 58. maddesinde açıkça yasaklanmış ve işçiye verilen yıllık izin ücretinin işveren tarafından geri alınabileceğini hükme bağlamış olmakla birlikte gerek Deniz İş Kanununda, gemi adamının ve gerekse Basın İş Kanununda gazetecinin yıllık izin müddeti içerisinde başka bir işyerinde çalışması halinde benzer bir hükme yer verilmemiştir. Bir görüşe göre kanunda açık bir düzenleme yer almadığından, ücret iadesi söz konusu olmayacak, ancak, çalışanın bu eyleminin, sadakat borcuna aykırılık teşkil ettiği kabul edilerek haklı nedenle iş sözleşmesi feshedilebilecektir<sup>906</sup>. Diğer bir görüşe göre ise yıllık ücretli izin hakkından feragat edilemediğine göre işçi yıllık izin süresinde başka işte çalışmayacak, çalıştığı tespit edilirse bu süreye ilişkin kendisine ödenen ücreti geri vermek zorunda kalacaktır. Bu görüşe göre, aksi düşünce yıllık ücretli izin hakkının düzenleniş amacına aykırı düşer<sup>907</sup>.

İşçinin hesap edilen ve izne çıkmadan önce kendisine ödenmesi gereken izin ücreti, işyerinin el değiştirmesi ya da her hangi bir şekilde başkasına geçmesi durumunda İK'nun 6. maddesinin emredici hükmü gereği yeni işveren tarafından ödenmesi gerekir. Tarafların devir sözleşmesinde aksini kararlaştırmış olmaları durumu değiştirmeyecektir<sup>908</sup>.

Yukarıda değinildiği gibi Deniz İş Kanununda yıllık izin ücretinin ne zaman ödeneceği yolunda bir hüküm bulunmamaktadır. Ancak Deniz İş Kanunu karşısında genel kanun olan Borçlar

---

<sup>903</sup> Demir, s. 280

<sup>904</sup> Mollamahmutoğlu, s. 961

<sup>905</sup> Bedir, Gökhan. Kısmi Süreli Çalışan İşçilerin Yıllık Ücretli İzin Hakları, Terazi Hukuk Dergisi, Cilt: 10, Sayı: 107, Temmuz 2015, s. 49; Çelik/Caniklioğlu/Canbolat, s. 701

<sup>906</sup> Karaman, s. 123; Akyiğit, Deniz İş Kanununda Yıllık Ücretli İzin, s 340

<sup>907</sup> Karaca / Günaydın, s. 912; Oğuz/Özge, s. 103

<sup>908</sup> Narmanhoğlu, s. 711; Aktay/Arıcı/Kaplan, 255

Kanunu, bu konuda, işçinin yıllık ücretli izne çıkmasından önce izin ücretinin peşin olarak kendisine verilmesini öngörmüştür (m. 425/I). Bu nedenle, Deniz İş Kanunu kapsamındaki işçiler yönünden de, yıllık ücretli izne çıkmadan önce izin ücretinin peşin olarak ödenmesi yasal bir zorunluluktur<sup>909</sup>.

Basın İş Kanununda özel olarak düzenlenen hükme göre, yıllık iznini kullanan gazeteciye bu izin süresine ilişkin ücretin en geç yıllık izne başlarken ödenmesi gerekir. BİK'nun 29. maddesine göre, gazeteciye yıllık iznini kullandırmayan veya kullandırdığı halde izin süresine ilişkin ücreti ödemeyen işveren, izin süresine tekabül eden ücretleri gazeteciye iki katı olarak ödemek yükümlülüğündedir. İş sözleşmesi devam ederken, izin kullandırılmasına rağmen ücret ödenmemiş ise, en geç izne başlarken ödenmesi gereken bu ücret için sözleşmenin devamı sırasında dava açılabilir<sup>910</sup>.

## VI- İŞ AKDİNİN SONA ERMESİNDE YILLIK ÜCRETİ İZİN

### A- GENEL OLARAK

Yukarıda da belirtildiği gibi, iş ilişkisi devam ettiği sürece işveren işçinin hak ettiği yıllık ücretli iznini (gecikme ile de olsa) kullandırmak zorundadır ve işçi, çalışmasına devam ettiği sürece, yıllık ücretli izin hakkı kullanılmaksızın paraya tahvil edilemez<sup>911</sup>. Bu nedenle iş sözleşmesi feshedilmeden yıllık izin ücreti alacağı doğmaz<sup>912</sup>. Ancak, işçi hak ettiği iznini kullanmadan akdi sona ermişse, bu hakkın kullanılması artık olanaksız hale geldiğinden, hak edip de kullanmadığı izin süresine ait ücreti kendisine veya hak sahiplerine ödenir. Bu şekilde yasa koyucu, iş akdinin devam ettiği sürece devredilemeyen ve vazgeçilemeyen şahsa bağlı bir hak olarak gördüğü yıllık ücretli izin hakkının, sözleşmesinin sona ermesinden sonra parasal bir hak haline dönüştüğünü kabul etmiştir<sup>913</sup>. Bu durumu düzenleyen İş Kanununun 59. maddesinin 1. fıkrasına (BK 425/3) göre "*İş sözleşmesinin, herhangi bir nedenle sona ermesi halinde işçinin hak kazanıp da kullanmadığı yıllık izin sürelerine ait ücreti, sözleşmenin sona erdiği tarihteki ücreti üzerinden kendisine veya hak sahiplerine ödenir*".

---

<sup>909</sup> **Karaman**, s. 126; **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s. 336

<sup>910</sup> **Karaca / Günaydın**, s. 912; **Oğuz/Özge**, s. 105

<sup>911</sup> Yargıtay 9. HD, 1.2.2010 E. 2009/47110, K 201/1923 (Narmanlıoğlu, s. 714); **Mollamahmutoğlu**, s. 953

<sup>912</sup> **Günay**, s. 37

<sup>913</sup> **Süzek**, s. 837; **Mollamahmutoğlu**, s. 953; **Demir**, s. 281; **Sümer**, s. 155; **Terzi, Ali Kemal**, Yıllık İzin Ücreti Ve Faiz, Mali Çözüm Dergisi, Eylül-Ekim, 2014, s. 128

Ancak bir görüşe göre, İş Kanununun 59. maddesi hükmünün amacı yıllık ücretli izin hakkını ücret alacağına dönüştürmek değil, kullandırılmayan yıllık ücretli izin hakkının ayrılmaz parçası olan ücret alacağının son ücret üzerinden hesap edilip işçiye ve hak sahiplerine ödenmesini sağlamaktır. Yargıtay'ın öğretide de benimsenen yorumu, kamu düzenine ilişkin, anayasal temel bir hak olan dinlenme hakkına ilişkin bu düzenlemeyi, işverene karşı hakkın bütünü bakımından yetersiz bir yaptırım hükmüne dönüştürmektedir. Böylelikle, uygulama "işverenin izni kullandırmak yerine parasını ödemesiyle veya kimi zaman işçinin izni kullanmak yerine sözleşme sona erdiğinde topluca para almayı tercih etmesiyle" sonuçlanan bir dizi sakıncayı beraberinde getirmektedir<sup>914</sup>. Yıllık izin hakkının muhatabı olan işveren, bunu oluşturan dinlendirme ve ücret ödeme borçlarını kural olarak aynı zamanda yerine getirmek zorundadır. Bunlardan birini yerine getirmekle diğerini karşılamış olamayacağı gibi, her ikisi yerine getirilmeden bütünü oluşturan yıllık izin hakkı da karşılanmış olamaz. Bu itibarla, yıllık ücretli izin hakkının, iş akdi sona erdikten sonra bile olsa sadece ücret hakkına dönüşebileceğinin kabulü sakıncalıdır<sup>915</sup>.

59. madde hükmü uyarınca yıllık izin sürelerine ait ücret, iş akdinin sadece işveren (veya işçi) tarafından herhangi bir şekilde (haklı veya haksız) feshi halinde değil, sözleşmenin fesih dışında herhangi bir nedenle sona ermesi halinde de ödenecektir. Bu nedenle iş akdinin, belirli süresinin bitimiyle, tarafların anlaşmasıyla, işçinin ölümü nedeniyle sona ermesi sonucu değiştirmeyecek, işçi veya ölümü halinde hak sahipleri, ücretli izinden yararlanılmayan sürelerle ilişkin muaccel hale gelen ücreti talep edebileceklerdir<sup>916</sup>. Eğer sözleşmelerle yıllık ücretli izin süreleri yasanın öngördüğü sürelerin üzerinde kararlaştırılmışsa, işçiye veya hak sahiplerine bu artırılmış izin sürelerine ilişkin ücretin ödenmesi gerekir<sup>917</sup>. Diğer taraftan, İşçinin hizmet sözleşmesinin işveren tarafından haklı sebeple (İK m. 25/II) derhal ve tazminatsız olarak feshedilmesi işverene kullanılmamış izinlerin ücretini ödememe hakkını vermez<sup>918</sup>.

İK'nun 59. maddesinin 1. fıkrasında söz konusu ücretin işçinin "*sözleşmenin sona erdiği tarihteki ücreti üzerinden kendisine*" ödeneceği belirtildiğinden, izin süresinin ücreti, iznin kullandırılmadığı yıllara ait ücret üzerinden değil, iş akdinin sona erdiği tarihteki (son) ücreti göz

---

<sup>914</sup> Öztürk, s. 77

<sup>915</sup> Öztürk, s. 77

<sup>916</sup> Narmanlıoğlu, s. 713; Süzek, s. 838; Mollamahmutoglu, s. 957; Aktay/Arıcı/Kaplan, s. 257; Çelik/Caniklioğlu/Canbolat, s. 697; Sümer, s. 155

<sup>917</sup> Süzek, s. 838

<sup>918</sup> Demir, s. 281

önünde tutulmak suretiyle ödenir. Ancak hesap yapılırken hak kazanılan izin sürelerinin İK m. 53/4 dikkate alınarak ayrı ayrı değerlendirilmesi gerekir<sup>919</sup>.

DİK m. 40/son, “*gemi adamının hak ettiği yıllık ücretli izni kullanmadan hizmet akdi 14 üncü maddenin II, III ve IV üncü bentlerine göre bozulursa, işveren veya işveren vekili izin süresine ait ücreti, gemi adamına ödemek zorundadır.*” hükmünü içermektedir. Dolayısıyla, söz konusu düzenlemeden, iş sözleşmesinin Kanunun m. 14/1 kapsamında sona ermesi (işverenin haklı nedenle sözleşmeyi sona erdirmesi) durumunda, işverenin, kullanılmayan yıllık ücretli izin ücretini gemi adamına ödemek zorunda olmadığı anlaşılmaktadır<sup>920</sup>. Örneğin her hangi bir limanda geminin hareketinden önce gemiye dönerek hizmete girmemesi veya gemiye hiç dönmemesi nedeniyle feshedilmesi durumunda, gemi adamı, kullanmadığı yıllık ücretli izin süresine ait ücretlerini alamayacaktır. Ancak Kanunun m. 14/1 kapsamında fesih nedeniyle ödenmeyecek olan yıllık izin ücreti, son yıla ilişkin yıllık izin ücretidir. Daha önceki yıllarda hak kazanılan ancak fesih tarihine kadar kullandırılmayan yıllık izin haklarına ilişkin ücretler ödenecektir. Her çalışma yılına ilişkin yıllık izin hakkının biriktirilmeden kullanılması esas olduğundan, söz konusu hükmün sadece son yıla ilişkin yıllık ücretli izin alacağına yönelik olduğu da kabul edilmelidir. Bu nedenle, Kanunun bu hükmü, yıllık ücretli izne hak kazanma konusunda, önceki çalışma sürelerinin dikkate alınmamasına gerekçe yapılabilecek bir düzenleme değildir<sup>921</sup>.

Deniz İş Kanununda, iş sözleşmesinin sona erme şekilleri sadece Kanun’un 14. maddesinde sayılanlardan ibaret değildir. İş Sözleşmesinin gemi adamı veya işveren tarafından 16. madde kapsamında önelli fesih yoluyla sona erdirilmesi, belirli süre veya sefer için yapılan iş sözleşmelerinin kendiliğinden sona ermesi, ölüm nedeniyle iş sözleşmesinin kendiliğinden sona ermesi veya tarafların anlaşarak iş sözleşmesini sona erdirmeleri durumlarında kullanılmayan yıllık izin sürelerine ait ücret alacaklarının talep edilebilecektir<sup>922</sup>.

Gazetecinin iş sözleşmesinin sona ermesi durumunda ise, kullanılmayan yıllık izin ücretinin ödenmesi konusunda, sadece işverenin iş sözleşmesini sona erdirmesiyle ilgili olarak Basın İş Kanununun 6. maddesinde bir düzenlemeye rastlanmaktadır. Söz konusu madde hükmüne göre, gazetecinin iş sözleşmesinin işveren tarafından sona erdirilmesi halinde kullanılmayan yıllık izin süresine ilişkin ücreti peşin olarak verilir. Yıllık ücretli izin hakkı şahsa bağlı, feragat edilmesi

---

<sup>919</sup> **Süzek**, s. 838; **Narmanhoğlu**, s. 713; **Mollamahmutoğlu**, s. 958; **Aktay/Arıcı/Kaplan**, s. 257; **Demir**, s. 281; **Çelik/Caniklioğlu/Canbolat**, s. 702; **Terzi**, s. 128

<sup>920</sup> **Karaman**, s. 119; **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s 341

<sup>921</sup> **Karaman**, s. 127, 128; **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s 341

<sup>922</sup> **Karaman**, s. 128; **Akyiğit**, Deniz İş Kanununda Yıllık Ücretli İzin, s 345

mümkün olmayan bir hak olduğuna göre, iş sözleşmesini sona erdiren gazeteciye de kullanılmayan yıllık izin süresine ilişkin ücretin peşin olarak verilmesi gerektiği düşünülmektedir<sup>923</sup>.

## **B- YILLIK ÜCRETLİ İZİN SÜRELERİ İLE BİLDİRİM SÜRELERİNİN VE YENİ İŞ ARAMA SÜRELERİNİN İÇ İÇE GEÇEMEYECEĞİ**

İş Kanununun 59. maddesinin 2. fıkrası gereğince "*İşveren tarafından iş sözleşmesinin feshedilmesi halinde 17. maddede belirtilen bildirim süresiyle 27. madde gereğince işçiye verilmesi zorunlu yeni iş arama izinleri yıllık ücretli izin süreleri ile iç içe giremez*". O halde, işveren süreli fesih bildiriyle iş akdini sona erdirdiğinde, işçinin hak kazandığı halde kullanamadığı yıllık iznini bildirim süresi içinde kullanmasını isteyemeyeceği gibi, işçinin kullanamadığı iznini bildirim süresine ve yeni iş arama iznine yaymak suretiyle izin süresine ait ücreti ödemekten de kaçınamaz<sup>924</sup>. Başka bir söyleyişle işçi izinli bulunduğu sırada işverenin sözleşmeyi fesih bildiri yoluyla feshetmesi mümkün ise de yıllık izin süresinin bitimine kadar bildirim sürelerinin işlemesi söz konusu olmayacaktır. Dolayısıyla, bu şekildeki bir fesih sonucu geçmesi gereken bildirim süreleri izin süresinin (varsa ücretsiz yol izninin) bitiminden sonra işlemeye başlayacaktır<sup>925</sup>. Maddede getirilen düzenleme; sadece iş sözleşmesinin bildirimli fesih ile sonlandırılmasına ilişkin olup, yıllık ücretli iznini kullanmakta olan işçinin iş sözleşmesinin derhal feshine ilişkin bir sınırlandırma getirilmemiştir<sup>926</sup>.

Buna karşılık, işçinin sözleşmeyi feshi ihbar etmesi halinde, bildirim süreleri içinde yıllık iznini kullanması mümkün olmalıdır. Zira İş Kanunumuzun engellediği husus sadece, işveren tarafından iş sözleşmesinin feshedilmesi halinde, yıllık ücretli izinle yeni iş arama izninin iç içe giremeyeceğidir. İş sözleşmesinin işçi tarafından feshi halinde ise kanuni yasak söz konusu olmayacak, bildirim süresi ile yıllık izin iç içe girebilecek, işçi bu süre içinde iznini kullanabilecektir<sup>927</sup>.

Ancak işverenin İş Kanununun 17. maddesine dayanarak bildirim sürelerine ilişkin ücreti peşin ödemek suretiyle sözleşmeyi fesih yoluna gidip gidemeyeceği tartışmalıdır. Bu çerçevede işçinin bildirim süreleri içinde çalıştırılmayarak bildirim sürelerini karşılayan ücreti verilip ve işyeri ile ilgisinin derhal kesilmesi durumunda, bildirim süresini karşılayan ücretle birlikte izin

---

<sup>923</sup> Karaca / Günaydın, s. 913

<sup>924</sup> Narmanhoğlu, s. 712; Süzek, s. 839

<sup>925</sup> Narmanhoğlu, s. 711; Aktay/Arıcı/Kaplan, s. 257; Demir, s. 280

<sup>926</sup> Aktay/Arıcı/Kaplan, s. 257

<sup>927</sup> Narmanhoğlu, s. 712; Süzek, s. 839; Çelik/Caniklioğlu/Canbolat, s. 703; Sümer, s. 155; Sevimli, s.

ücretinin de verilmesi mümkün olmalı, buna karşın, işveren yıllık ücretli izin süresi içinde bildirim sürelerine ilişkin ücreti peşin ödemek suretiyle işçinin işine son vermek yoluna gidememelidir. Aksi takdirde yıllık izin süreleriyle, bildirim sürelerinin içiçe giremeyeceğini öngören kanuni kuralın bertaraf edileceği ve kanunun amacına aykırı bir yola gidilmiş olacağı düşünülmektedir<sup>928</sup>.

İş sözleşmesinin, gerek Basın İş Kanununun 6. maddesi ile Deniz İş Kanunu 16. maddesi kapsamında ihbarlı fesih yoluyla sona erdirilmesi durumunda, ihbar müddeti içerisinde yıllık ücretli iznin kullanılarak kullanılamayacağı konusunda ilgili kanunlarda özel bir düzenleme bulunmamaktadır. Buradan hareketle, ilk bakışta, gerek gazeteciye ve gerekse gemiadamına feshi ihbar süresi içerisinde yıllık ücretli izin kullanılabilir. Ancak, iş kanunlarının genel amacı dikkate alındığında, bu tür bir uygulamanın her durumda hukuka uygun olacağını kabul etmek mümkün değildir. Zira iş sözleşmesinin işveren tarafından ihbarlı olarak feshedilmesi durumunda, feshi ihbar süresi içerisinde çalışanın yıllık ücretli izne çıkarılması, işverenin, feshi ihbar süresi boyunca, çalıştırma veya bu süreye ilişkin ücreti peşin ödeme yükümlülüğünden kısmen veya tamamen kurtaracaktır.<sup>929</sup>.

### C- İŞYERİ DEVRİNDE İZİN ÜCRETİ ALACAĞI

İşçinin sözleşmenin devamı sırasında hak edip de kullanmadığı yıllık iznin ücretini isteyememesi, işyerinin devri halinde ortaya çıkan yıllık ücretli izne özgü ayrık durum açısından da önemlidir. İş Kanununun 6. maddesi gereği, devir tarihinde işyerinde veya bir bölümünde mevcut olan iş sözleşmeleri bütün hak ve borçları ile birlikte devralana geçer. Böylece devirden sonra asıl borçlu devralan olmaktadır. Ancak Kanun, borçların aslında devirden önce devreden işveren yanında çalışılırken doğduğunu da dikkate alarak, işçinin alacağına kavuşmasını kolaylaştırmak için devir halinde, devirden önce doğmuş olan ve devir tarihinde ödenmesi gereken borçlardan devreden işvereni devir tarihinden itibaren iki yıl ile sınırlı biçimde, devralan işverenle birlikte sorumlu tutmuştur. Yıllık izin ücretinin ancak sözleşme sona erdikten sonra talep edilebileceği, devirle sözleşme sona ermiş sayılmadığı, bu sebeple devirden önce ödenmesinin gerekmediği kabulü yüzünden, kullanılmayan yıllık izin ücretinden sadece devralan işveren sorumlu olmaktadır. Oysa yıllık izni zamanında kullanılmayan devreden işverendir. Ayrıca işçi yıllık izin ücretini sadece devralandan isteyebildiğinde, bu işçi alacağı devirden önce hak edilmiş diğer alacaklardan daha az korunmuş olmaktadır<sup>930</sup>.

---

<sup>928</sup> Narmanhoğlu, s. 712 ve 713

<sup>929</sup> Akyiğit, Deniz İş Kanununda Yıllık Ücretli İzin, s.321; Karaman, s. 124

<sup>930</sup> Öztürk, s. 91

## D- İZİN ÜCRETİ ALACAĞINDA ZAMANAŞIMI VE FAİZ

İş Kanununun 59. maddesinin 1. fıkrasına göre yıllık izin ücretine ilişkin zamanaşımı iş akdinin sona erdiği tarihten başlar. Bu hüküm uyarınca işçi, hak kazanıp da kullanamadığı iş ilişkisi içinde doğmuş bulunan tüm yıllık izin sürelerine ait ücretini, iş akdinin herhangi bir nedenle sona erdiği diğer bir deyişle izin hakkının ücret alacağına dönüştüğü tarihten itibaren beş yıl (İK m. 32/son) içinde işveren talep edebilecektir<sup>931</sup>.

Yargıtay'a göre "*Yıllık izin ücreti iş sözleşmesinin feshi ile muaccel olup dönemsel bir nitelik taşımadığından, 6098 sayılı Türk Borçlar Kanunu uygulaması yönünden 10 yıllık genel zamanaşımına tabidir*"<sup>932</sup>. Ancak İş Kanununa 12.10.2017 tarih ve 7036 sayılı yasanın 15. maddesi ile eklenen Ek 3. maddede, artık iş sözleşmesinden kaynaklanmak kaydıyla yıllık izin ücretinin beş yıllık zamanaşımına tabi olduğu hükme bağlanmıştır. Maddeye göre, iş sözleşmesinden kaynaklanmak kaydıyla hangi kanuna tabi olursa olsun, yıllık izin ücretinin zamanaşımı süresi beş yıldır.

Yıllık izin ücreti alacaklarında gecikme faizi İş Kanununun 34. maddesinin 1. fıkrasına göre, işverenin temerrüde düşürüldüğü tarihten itibaren hesaplanacak mevduata uygulanan en yüksek faiz olmalıdır. Ancak Yargıtay İK m. 34'ün yıllık izin ücreti alacağına uygulanmasını mümkün görmediğinden kanuni faiz yürütülmesi gerekeceği görüşündedir<sup>933</sup>. Diğer taraftan, Yargıtay'a göre iş sözleşmesinin sona erdiği tarihte izin ücreti muaccel olup, faiz başlangıcı bakımından işverenin ayrıca temerrüde düşürülmesi gerekmektedir<sup>934</sup>. Yargıtay'ın bir kararında<sup>935</sup> şöyle denilmektedir: "*Kanunda iş sözleşmesinin feshinde ödenmesi gereken izin ücreti için kesin bir ödeme günü belirlenmiş değildir. Sözleşmenin feshi anı, yıllık ücretli izin hakkının ücrete dönüşmesi, bir başka anlatımla izin ücretine hak kazanma zamanı olarak Kanunda belirtilmiştir. İş sözleşmesinin feshedildiği tarihte izin ücreti muaccel olur, ancak faiz başlangıcı bakımından işverenin ayrıca temerrüde düşürülmesi gerekir. Dairemizce, iş sözleşmesinin feshinde ödenmesi gereken izin ücreti, geniş anlamda ücret içinde değerlendirilmemiş ve 4857 sayılı İş Kanununun*

<sup>931</sup> **Süzek**, s. 840; **Aktay/Arıcı/Kaplan**, s. 257; **Demir**, s. 281; **Çelik/Caniklioğlu/Canbolat**, s. 703; **Sümer**, s. 155

<sup>932</sup> YARGITAY 9. HUKUK DAİRESİ E. 2010/38436 K. 2013/253 T. 14.1.2013 Kazancı İçtihat Bilgi Bankası (<http://www.kazanci.com/kho2/ibb/files/dsp.php?fn=9hd-2010-38436.htm&kw=14.1.2013+38436#fm>; Erişim Tarihi: 14.3.2019)

<sup>933</sup> **Mollamahmutoğlu**, s. 958; **Demir**, s. 281; **Terzi**, s. 128; **Günay**, s. 39; **Öztürk**, s. 89

<sup>934</sup> **Günay**, s. 39; **Terzi**, s. 128

<sup>935</sup> Yargıtay 9.HD. 24.10.2008 gün2007/30158 E., 2008/28418 K., (Süzek, s. 710); YARGITAY 9. HUKUK DAİRESİ E. 2008/34982 K. 2010/27914 T. 7.10.2010 (Terzi, s. 128)

34. maddesinde sözü edilen bankalarca mevduata uygulanan en yüksek faize karar verilemeyeceği kabul edilmiştir. O halde, izin ücreti için uygulanması gereken faiz, yasal faiz olmalıdır.”

## **VII- İŞ KANUNU ile TÜRK BORÇLAR KANUNUNUN YILLIK ÜCRETLİ İZİN HÜKÜMLERİNİN KARŞILAŞTIRILMASI**

### **A- GENEL OLARAK**

4857 sayılı İş Kanununun 4. maddesi hükmü nedeniyle bu kanunun kapsamına girmeyen çalışanlar ile BİK ve DİK kapsamında yer almayan çalışanların işverenleri ile ilişkileri Türk Borçlar Kanunu hükümlerine göre düzenlenmektedir. Buna göre örneğin ev hizmetlerinde çalışan kişilerin veya sporcuların yıllık ücretli izin hakları Türk Borçlar Kanunu çerçevesinde belirlenmektedir.

Türk Borçlar Kanununa tabi çalışanların, yıllık ücretli izin haklarına ilişkin düzenlemeler, 6098 Sayılı TBK'nun hizmet sözleşmelerinin 422 ila 425. maddelerinde yer almaktadır.

Sonradan az sayıda bazı değişikliklere uğramış olsa da, 4857 sayılı Kanun 22.5.2003 tarihinde, 6098 sayılı Türk Borçlar Kanunu ise 1.7.2012 tarihinde yürürlüğe girmiştir. Hizmet sözleşmeleri ile ilgili olarak Türk Borçlar Kanununda, 4857 sayılı İş Kanunu hükümlerinden ayrı düzenlemeler getirildiği gibi İş Kanunu'nda hiç düzenlenmeyen yıllık izin süresinden indirim usulü de öngörülmüştür<sup>936</sup>.

### **B- YILLIK İZİN SÜRESİ**

TBK ile İK'da yer alan yıllık ücretli izin hükümlerine ilişkin farklardan ilki, Türk Borçlar Kanunundaki düzenlemeye göre işçinin hak kazanacağı yıllık izin süresinin, işçinin kıdemine göre değişmemesidir. İş Kanununun 53/4. maddesinde, yıllık ücretli izin hakları işçinin kıdemine göre düzenlenmiştir. Buna karşın, Borçlar Kanununa tabi işçiler bakımından bu yasanın 422. maddesinde "*işveren, en az bir yıl çalışmış olan işçilere yılda en az iki hafta ve onsekiz yaşında küçük işçiler ile elli yaşından büyük işçilere de en az üç hafta ücretli izin vermekle yükümlüdür*" hükmüne yer verilmiştir<sup>937</sup>.

### **C- YILLIK İZİN SÜRESİNİN HESABINDA DİKKATE ALINMAYACAK SÜRELER VE İZİNDEN İNDİRİM**

---

<sup>936</sup> **Özdemir, Cumhuriyet Sinan**, Yıllık Ücretli İzinden “Borçlar Kanunu Kapsamında” İndirim Yapılabilir mi? Terazi Hukuk Dergisi, Cilt: 8, Sayı: 87, Kasım 2013, s. 83; **Akyiğit**, Yıllık İznin İşverence Kısaltımı, s. 84

<sup>937</sup> **Süzek**, s. 834; **Bayram**, 308



6098 sayılı TBK, 4857 sayılı İş Kanunundan farklı olarak, yıllık ücretli izne hak kazanabilmek için tamamlanması gereken çalışma süreleri konusunda, fiilen çalışılmadan geçirilen hangi sürelerin çalışma süresinden sayılacağı konusunda özel bir düzenlemeye yer vermemiştir. Dolayısıyla, TBK anlamında bekleme süresi, ilgili işçinin hizmet sözleşmesinin hukuken devam ettiği sürelerin tamamından oluşmaktadır. Buna karşın bazı durumlarda işçinin hizmet süresinden yapılabilecek indirimlere kanunda yer verilmiştir<sup>938</sup>.

Borçlar Kanunu'nun 423 üncü maddesi yıllık ücretli izinden yapılacak indirimleri düzenlemiştir. Buna göre,

- İşçinin bir hizmet yılı içinde kendi kusuruyla toplam bir aydan daha uzun bir süreyle hizmeti yerine getirmediği takdirde işverenin çalışılmayan her tam ay için, yıllık ücretli izin süresinden bir gün indirim yapabileceği,
- İşçinin bir hizmet yılı içinde kendi kusuru olmaksızın hastalık, kaza, yasal bir yükümlülüğün veya kamu görevinin yerine getirilmesi gibi kişiliğine bağlı sebeplerle en çok üç ay süreyle işgörmeye edimini yerine getiremediği takdirde, işverenin yıllık ücretli izin süresinden indirim yapamayacağı,
- İşverenin gebelik ve doğum yapma sebebiyle işgörmeye edimini en çok üç ay süreyle yerine getiremeyen kadın işçinin yıllık ücretli izin süresinden indirim yapamayacağı, hususları hükme bağlanmıştır<sup>939</sup>.

Borçlar Kanunu, bu düzenleme ile çalışılmadan geçirilen sürelerin yıllık ücretli izin hakkına etkisi bakımından İş Kanunlarından farklı bir çözüm şekli benimsemiştir. Buna göre, işçinin, yıllık ücretli izne hak kazanabilmesi için, çalışmadığı süreler kadar daha çalışması gerekmeyecektir. Tam tersine, bu süreler çalışılmış gibi kabul edilecek, ancak yıllık ücretli izin hakkında indirim yapılmasına sebebiyet verecektir. Dolayısıyla, Borçlar Kanunu'nda, çalışılmadan geçirilen ve yıllık ücretli izin hakkını etkilemeyen sürelerin, yıllık ücretli izin alacağına hak kazanma bakımından çalışılmış gibi kabul edildiği söylenebilecektir<sup>940</sup>.

Ancak yukarıda belirtilen TBK'nun 423 maddesinin 1. ve 2. fıkrasında sayılan durumlarda, yıllık izinde indirim kendiliğinden gerçekleşmeyecektir. Ayrıca işverenin de indirim gitmek zorunluluğu yoktur. Dolayısıyla bu yol işverenin isterse başvurabileceği yasal bir imkândır.

---

<sup>938</sup> Akyiğit, Yıllık İznin İşverence Kısaltımı, s. 80

<sup>939</sup> Süzek, s. 834; Bayram, s. 309

<sup>940</sup> Akyiğit, Ercan Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, Sicil İş Hukuku Dergisi, Mart 2011, Yıl 6, Sayı 21, s. 29; Karaman s. 121, Bayram, s. 311

İşveren, buna başvurmadan kısmen veya tamamen kendiliğinden vazgeçebileceği gibi, hizmet sözleşmesi ve/veya TİS ile de vazgeçebilir<sup>941</sup>.

Buna karşılık, İş Kanununda ve diğer iş yasalarında bu yönde bir düzenleme yer almamaktadır. İş Kanununda bu konuda farklı bir çözüm getirilmiş, yukarıda görüldüğü gibi işçinin uğradığı hastalık veya kaza halinde devamsızlığın (İK 55/a), bu yasanın 25. maddesinin I. bendinin b alt bendinde öngörülen süreyi aşan kısmının yıllık ücretli izin hakkının hesabında çalışılmış gibi sayılmayacağı hükme bağlanmıştır<sup>942</sup>.

#### **D- YILLIK ÜCRETLİ İZİN BÖLÜNEREK KULLANILMASI**

Diğer taraftan, TBK'nun 424. maddesinde; *“Yıllık ücretli izinler, kural olarak aralıksız biçimde verilir; ancak tarafların anlaşmasıyla ikiye bölünerek de kullanılabilir.”* hükmü öngörülmüştür. Konuyla ilgili olarak 4857 sayılı İş Kanununun 56. maddesinde ise; *“bu iznin 53 üncü maddede gösterilen süreler içinde işveren tarafından sürekli bir şekilde verilmesi zorunludur. Ancak, 53'üncü maddede öngörülen izin süreleri, tarafların anlaşması ile bir bölümü on günden aşağı olmamak üzere bölümler halinde kullanılabilir”* hükmü öngörülmüştür. Dolayısıyla TBK'nda yıllık izin süreleri tarafların anlaşması halinde en fazla ikiye bölünebileceği hükme bağlanmışken, İK'da bir bölümü on günden az olmamak kaydıyla, bölünerek kullanılması konusunda bir sınırlamaya yer verilmemiştir<sup>943</sup>.

#### **E- YILLIK İZİNİN KULLANDIRILMA ZAMANI**

İşçinin hak etmiş olduğu yıllık ücretli iznin ne zamana kadar kullanılacağına ilişkin olarak TBK'nda hüküm yer almamaktadır. Yıllık ücretli izinden beklenen dinlenme amacı ile sosyal ilişkilere zaman ayırabilme gerekliliği açılarından, yıllık izin, hak edildiği yılı izleyen yıl bitmeden kullanılması gerektiği kabul edilmelidir<sup>944</sup>.

#### **F- YOL İZİNİ**

6098 sayılı TBK'nda yıllık iznini kullanan işçiye herhangi bir yol izni verileceğine değinilmemiştir. Bu yüzden hizmet sözleşmesi veya TİS ile işçiye yıllık iznine ek olarak ücretli

---

<sup>941</sup> **Akyiğit, Ercan**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, Sicil İş Hukuku Dergisi, Aralık 2011, Yıl 6, Sayı 24, s. 61

<sup>942</sup> **Bayram**, s. 310

<sup>943</sup> **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 35, **Bayram**, s. 311

<sup>944</sup> **Akyiğit**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 67; **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 34

veya ücretsiz bir yol izni verileceği öngörülebilir. Ayrıca bunun ne miktar olacağını da sözleşmede kararlaştırabilirler<sup>945</sup>.

### **G- YILLIK İZİN ÜCRETİNİN HESABINDA TATİL GÜNLERİNİN DİKKATE ALINIP ALINMAYACAĞI**

Yıllık izin süresi içinde kalan tatil günlerine ilişkin ücretlerin de ayrıca ödenmesini öngören İş Kanununun 57. maddesinin son fıkrasına benzer bir hüküm Türk Borçlar Kanununda bulunmamaktadır. İşçiye sadece yıllık izin süresinin ücretinin ödeneceği öngörülmüşse de, yıllık iznin yalnızca ilgili işçinin normalde çalışacağı işgünlerinden oluşacağı ve ücretli hafta tatilinin (TBK. 421) varlığı gözönüne alındığında; izin dönemine denk gelen hafta tatillerinin ücretinin de işçiye ayrıca ödenmesi gerektiği düşünülmelidir. Aynı şekilde ulusal bayram ve genel tatiller hiçbir iş yasasıyla da sınırlanmadığından, TBK'na tabi işçilere de aynı günlerin ücretli tatil olarak verileceği ve bu günlerin de yıllık izinden sayılmayacağı muhakkaktır<sup>946</sup>.

### **H- YILLIK ÜCRETİ İZİN SÜRELERİ İÇERİSİNDE KALAN TATİL VE RAPORLU GÜNLERİN İZİN SÜRESİNDE SAYILIP SAYILMAYACAĞI**

Yıllık ücretli izin süreleri konusunda açıklığa kavuşturulması gereken bir diğer husus, yıllık ücretli izin süreleri içerisinde kalan hafta tatili, ulusal bayram ve genel tatiller, işveren tarafından verilen diğer izinler ile her hangi bir hastalık veya kaza nedeniyle alınan rapor sürelerinin yıllık ücretli izin süresinden sayılıp sayılmayacağıdır. Bu konuda, 4857 sayılı Kanun'dan farklı olarak, Türk Borçlar Kanununda bu konu düzenlenmemiştir. Ancak, yıllık ücretli izin müddeti içerisinde kalan söz konusu sürelerin yıllık ücretli izin süresine dâhil olmayacağını benimsemek hizmet ilişkisinin niteliği ile işçinin Anayasal hakkı olan dinlenme hakkının gerektiği gibi kullanılması açısından uygun bir çözüm olacağı düşünülmektedir<sup>947</sup>.

### **I- YILLIK İZİN MÜDDETİ İÇERİSİNDE BAŞKA BİR İŞYERİNDE ÇALIŞMA YASAĞI**

İşçinin, yıllık izin müddeti içerisinde başka bir işyerinde çalışması 4857 sayılı İş Kanununda açıkça yasaklanmış ve işçiye verilen yıllık izin ücretinin işveren tarafından geri alınabileceğini hükme bağlamıştır (m. 58). Ancak, benzer bir düzenlemeye, Deniz İş Kanunu'nda, Basın İş Kanunu'nda ve Borçlar Kanunu'nda yer verilmemiştir. Ancak, yıllık izin hakkı anayasal bir hak

---

<sup>945</sup> **Akyiğit, Ercan**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 69; **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 36

<sup>946</sup> **Akyiğit**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 70; ; **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 36

<sup>947</sup> **Akyiğit**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 70; **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 37

ve Borçlar Kanunu ve diğer iş kanunlarının bu konuya ilişkin hükümleri de kamu düzenine ilişkin olup emredici niteliktedir. Bu düzenlemelerin temel amacı yıllık izin hakkının korunmasıdır. Bu nedenle, böyle bir durumun hukuken mümkün olamayacağı kabul edilmelidir<sup>948</sup>. TBK'nun kanunlaşma sürecinde bununla ilgili bir hüküm Bilim Komisyonu Taslağında yer alıyordu. Ancak TBMM Adalet Komisyonu bu fıkra hükmünün“yıllık iznin ücret hakkının kişiye bağlı bir hak olması ve işçinin izin hakkını kullanırken çalışması durumunda izin süresi için ödenecek ücretin geri alınabilmesinin nesafet ilkesi ile bağdaşmadığı ve bu hakkı kullanılmaz hale getireceği” gerekçesiyle madde metninden çıkarmıştır<sup>949</sup>. Böylelikle, TBK açısında yıllık izinde ücretli bir işte çalıştığı anlaşılan işçiden izin parasının geri alınamayacağını kabul edilmelidir. Sebepsiz zenginleşme hükümlerine dayanılarak iade yükümü olduğu söylenemeyecektir. Ancak böyle bir çalışma, işçinin sadakat borcunu ihlal etmesi nedeniyle, sözleşmenin işverence feshi için haklı sebep veya geçerli sebep oluşturabilecektir<sup>950</sup>.

## **J- BİLDİRİMLİ FESİHTE, BİLDİRİM SÜRESİ İLE YILLIK ÜCRETİ İZİNİN İÇ İÇE GEÇMESİ**

Yıllık ücretli iznin kullanılacağı dönemle ilgili olarak üzerinde durulması gereken bir diğer konu da, iş sözleşmesinin, TBK m. 431 ve 432 kapsamında ihbarlı fesih yoluyla sona erdirilmesi durumunda, feshi ihbar süresi içerisinde yıllık ücretli iznin kullandırılıp kullandırılmayacağıdır. Bu konuya ilişkin olarak TBK'da özel bir düzenleme bulunmamaktadır. Dolayısıyla, Borçlar Kanununun bu tür bir uygulamayı yasaklamadığı söylenebilir. Ancak, hizmet sözleşmesinin niteliği ve kanunun genel amacı dikkate alındığında, bu tür bir uygulamanın hukuka uygun olmayacağı kabulü gerekir. Nitekim iş sözleşmesinin işveren tarafından süreli olarak feshedilmesi durumunda, feshi ihbar süresi içerisinde işçinin yıllık ücretli izne çıkarılması, işverenin, feshi ihbar süresi boyunca işçiyi çalıştırma veya bu süreye ilişkin ücreti peşin ödeme yükümlülüğünden kısmen veya tamamen kurtaracaktır. Borçlar Kanunu'nda, 4857 sayılı Kanun m. 59/2'de olduğu gibi açık bir düzenleme olmamasına karşın, Medeni Kanunun 2. maddesinde yer alan hakkın kötüye kullanılmasını yasaklayan ilke nedeniyle, sözleşmenin işverence süreli feshi durumunda, ihbar süresi içerisinde yıllık ücretli izin kullandırılmayacağı kabulü gerekir. İş sözleşmesinin işçi

---

<sup>948</sup> **Karaman s. 123**

<sup>949</sup> **Akyiğit**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 57; **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 38

<sup>950</sup> **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 38; **Akyiğit**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 71

tarafından süreli fesih yoluyla sona erdirilmesi durumunda ise feshi ihbar süresi içerisinde yıllık ücretli izin kullandırılacaktır<sup>951</sup>.

## **K- YILLIK ÜCRETLİ İZİN KONUSUNDAKİ FARKLI HÜKÜMLER AÇISINDAN TBK ile İK ARASINDAKİ GENEL-ÖZEL VE ÖNCEKİ-SONRAKİ KANUN İLİŞKİSİ**

Farklılık gösteren hükümler açısından genel kanun-özel kanun ve eski tarihli kanun-yeni tarihli kanun ilişkileri düşünülerek; ilk bakışta, her iki kanunun çelişen hükümleri açısından, 2011 tarihli ve 6098 sayılı genel nitelikli Türk Borçlar Kanununun, 2003 tarihli özel nitelikli 4857 sayılı İş Kanununu değiştireceği öne sürülebilir. Ancak Türk Borçlar Kanunu'nun hizmet sözleşmeleri ile ilgili hükümleri 4857 sayılı İş Kanununun kapsamı dışında kalan işçileri kapsamaktadır. Dolayısıyla Türk Borçlar Kanunu'nun bu konudaki hükümleri İş Kanunu'na tâbi işçiler bakımından geçerli değildir. Yeni tarihli genel kanunun hükümlerinin, eski tarihli özel kanunun hükümlerini yürürlükten kaldırabilmesi için, her iki kanunun aynı konuyu düzenlemeleri yetmez, bu kanunların kapsam ve içeriğinin de aynı olması gerekir. Sonuç olarak ilk bakışta Türk Borçlar Kanunu'nun da, İş Kanununun da hizmet sözleşmelerini düzenlediği bir vakıa ise de, her iki kanunun uygulanacağı kişiler bakımından kapsamı farklıdır<sup>952</sup>.

## **VIII- SONUÇ**

Temelini evrensel hukukta bulan ve Anayasamızın ekonomik ve sosyal haklar kapsamında güvence altına alınan çalışanların yıllık ücretli izin hakkı, hukukumuzda farklı çalışan grupları açısından farklı kanunlarda düzenlenmiştir.

4857 sayılı İş Kanunu, 6098 sayılı Türk Borçlar Kanunu, 5953 sayılı Basın İş Kanunu ve 854 sayılı Deniz İş Kanununun, yıllık ücretli izni düzenleyen hükümleri kimi konularda farklılıklar içerse de, bunların tümünde, işçilerin yıllık ücretli izin hakkının, feragat edilemeyen, devri mümkün olmayan, işçi tarafından kullanılması ve işveren tarafından kullandırılması zorunlu olan bir hak olduğu emredici hüküm olarak yer almaktadır.

Uygulamada işçi ve işveren arasında, özellikle iş akdinin sona ermesinde sonra sıklıkla, yıllık iznin zamanında ve gerektiği biçimde kullandırılmaması (veya kullanılmaması) sonucu ortaya çıkan yıllık ücretli izin alacağı konusundaki uyuşmazlıkların, bu hakkın kullandırılması konusunda işverenlerin isteksizlik ve ciddiyetsizlikleri yanında, işçilerin de söz konusu hakkı

---

<sup>951</sup> **Akyiğit**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 38; **Akyiğit**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, s. 72; **Karaman**, s. 124

<sup>952</sup> **Yılmaz, Ejder**, "Genel Kanun - Özel Kanun" İlişkisi (Türk Borçlar Kanunu ve İş Kanunu Bağlamında), Sicil İş Hukuku Dergisi, Haziran 2011, Yıl 6, Sayı 22, s.30

paraya tahvil etme eğiliminden kaynaklandığı düşünülmektedir.

İlgili yasalarda öngörülen koşulları yerine getiren işçinin, beden ve ruh sağlığının devamlılığı açısından dinlenebilmesi; aile ve sosyal çevresi ile olan ilişkilerini koruyabilmesi ve sürdürebilmesi, izin hakkının mutlaka gerektiği gibi kullanılmasını zorunlu kılmaktadır. Bu itibarla izin hakkının işçiler tarafından fiilen kullanılmasının, daha sıkı gözetim ve denetim mekanizmaları ile kontrol altına alınmasının gerek işçi çıkarları ve gerekse ülkenin sosyoekonomik gereklilikleri açısından zorunlu olduğu açıktır.

## KAYNAKLAR

- Aktay, Nizamettin/Arıcı, Kadir/Kaplan, Emine Tuncay**, İş Hukuku, Gazi Kitabevi, Ankara 2012
- Akyiğit, Ercan**, 6098 Sayılı Türk Borçlar Kanunu'nda Yıllık Ücretli İzin, Sicil İş Hukuku Dergisi, Aralık 2011, Yıl 6, Sayı 24, s. 55-73
- Akyiğit, Ercan**, Yeni Borçlar Kanunu'nda Yıllık Ücretli İzin, Sicil İş Hukuku Dergisi, Mart 2011, Yıl 6, Sayı 21, s. 25-40
- Akyiğit, Ercan**, Yıllık Ücretli İzin Kurumunda Yeni Bir Durum: Yıllık İznin İşverence Kısaltımı (İndirimi), Çalışma ve Toplum Dergisi, Sayı 2011/3, s. 73-92
- Akyiğit, Ercan**, Yıllık Ücretli İzin, Seçkin Yayıncılık, Ankara 2000
- Akyiğit, Ercan**, Deniz İş Kanununda Yıllık Ücretli İzin, Sarper Süzek'e Armağan (I), Beta Yayınevi, İstanbul 2011, s. 299-352
- Bayram, Selahattin**, Yeni Borçlar Kanunu'nun Yıllık İzne İlişkin Hükümleri İle 4857 Sayılı İş Kanunu'nun Yıllık İzne İlişkin Hükümlerinde Farklılık ve Değerlendirmesi, Mali Çözüm Dergisi, Sayı Ocak-Şubat 2011, s. 307-313
- Bedir, Gökhan**. Kısmi Süreli Çalışan İşçilerin Yıllık Ücretli İzin Hakları, Terazi Hukuk Dergisi, Cilt: 10, Sayı: 107, Temmuz 2015, Sayfa: 48-50
- Bingöl, Serkan**, Yıllık Ücretli İzin, Seçkin Yayıncılık, Ankara 2012
- Bodur, Mehtap**, Mevsimlik İş Sözleşmesi İle Çalışanların Yıllık Ücretli İzin Hakları, Cilt 1, Sayı 1, Ocak 2015, s.131 – 146
- Çelik, Nuri/Caniklioğlu Nursen/Canbolat**, Talat, İş Hukuku Dersleri, Beta Basım Yayın A.Ş., İstanbul 2017
- Demir, Fevzi**, İş Hukuku ve Uygulaması, Albi Yayıncılık, İzmir 2016
- Demircioğlu, Murat/Centel Tankut**, İş Hukuku, Beta Basım, İstanbul 2007
- Eyrenci, Ömer/Taşkent, Savaş/Ulucan Devrim**, Bireysel İş Hukuku, Beta Yayınevi, İstanbul 2017
- Gönen, Ramazan**, İş Hukukunda Yıllık Ücretli İzin, İstanbul Barosu Dergisi, Cilt: 87, Sayı: 3, Mayıs 2013, s. 206-213
- Günay, Cevdet, İlhan**, Yıllık Ücretli İzin Hakkı ve Ücretli İzin Alacağı, Sicil İş Hukuku Dergisi, Aralık 2010, Yıl 5, Sayı 20, s. 28-50
- Karaca, Nuray Gökçek/Günaydın, Barış**, Gazetecilerin Ücretli Tatil ve Yıllık Ücretli İzin Hakkı, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Yıl 2007, Sayı 15, s. 907-919

- Karaman, Mehmet Halis**, Deniz İş Kanunu Kapsamında Çalışan İşçilerin Yıllık Ücretli İzin Hakkı, Sicil İş Hukuku Dergisi, Yıl 2018, Sayı 40, s. 114-131
- Kayhan, Necati**, Ulusal ve Uluslararası Normlara Göre Türkiye’de Yıllık İzin Hakkı, Çalışma İlişkileri Dergisi, Yıl 2010, Cilt 1, Sayı 1, s. 119 – 149
- Mollamahmutoğlu, Hamdi**, İş Hukuku, Turhan Kitabevi, Ankara 2008
- Narmanlıoğlu Ünal**, İş Hukuku Ferdi İş İlişkileri, Beta Basın Yayın A.Ş. İstanbul 2012
- Oğuz, Özgür/Doğan, Özge**, Gazetecinin Yıllık Ücretli İzin Hakkı, 2016, Yıl: 5 / Sayı 10, s. 95-110
- Öksüz, Ömer**, Yıllık Ücretli İzin, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi, Yıl 2006, Sayı 11, s. 853-865
- Özdemir, Cumhuri Sinan**, İşçilerde Yıllık Ücretli İzin Uygulaması ve Birikmiş İşçi İzinlerinin Kullandırılması, Mali Çözüm Dergisi, Eylül-Ekim 2010, s. 269-280
- Özdemir, Cumhuri Sinan**, Yıllık Ücretli İzinden “Borçlar Kanunu Kapsamında” İndirim Yapılabilir mi? Terazi Hukuk Dergisi, Cilt: 8, Sayı: 87, Kasım 2013, Sayfa: 82-84
- Özel, Kayhan**, Yıllık İzinler Konusunda Bir Yargıtay Kararının İncelenmesi, İstanbul Barosu Dergisi, Cilt: 82, Sayı: 3, Mayıs 2008, Sayfa: 1377-1382
- Özen, Cüneyt**, Yıllık Ücretli İzin Hakkının 4857 Sayılı İş Kanunu’ndaki Görünümü, ÇSGB Çalışma Dünyası Dergisi, Cilt 3, Sayı 1, Ocak-Nisan 2015, Sayfa: 55-77
- Özkaraca,ERCÜMET**, Aynı İşveren Yanındaki Aralıklı Çalışmalarda Yıllık Ücretli İzin Hakkı, Sicil İş Hukuku Dergisi, Yıl 2018, Sayı 39, s. 90-104
- Öztürk, Mehmet Onat**, Kullandırılmayan Yıllık Ücretli İzin Hakkı Sebebiyle İş Kanunu Çerçevesinde Yapılan Ödemeler, Çalışma ve Toplum Dergisi, Sayı: 2012/4, s. 73-98
- Özuysal, Neslihan**, Yıllık Ücretli İzin, İstanbul Barosu Dergisi, Cilt: 83, Sayı: 5, Eylül 2009, s. 2575-2596
- Özveri, Murat**, Yıllık Ücretli İzin Hakkı ve Yargı Kararları, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi Yıl 2007, Sayı 15, s. 921-942
- Sevimli, Ahmet**, Yıllık Ücretli İznin Kullandırılmamasının Hukuki Sonuçları Hakkında Kısa Bir Not, Sicil İş Hukuku Dergisi, Yıl 2010, Yıl 5, Sayı 18, s. 40-47
- Sümer, Haluk Hadi**, İş Hukuku, Mimoza Basım, Konya 2014
- Süzek, Sarper**, İş Hukuku, Beta Basın Yayın A.Ş. İstanbul 2018
- Yılmaz, Ejder**, “Genel Kanun - Özel Kanun” İlişkisi (Türk Borçlar Kanunu ve İş Kanunu Bağlamında), Sicil İş Hukuku Dergisi, Haziran 2011, Yıl 6, Sayı 22, s. 22-32



## VELAYET DAVALARINDA ÇOCUKLARIN DURUŞMA SALONUNDA DİNLENMESİNE İLİŞKİN HÂKİM, AVUKAT VE UZMAN GÖRÜŞLERİ

Umut Haydar COŞKUN<sup>953</sup> , Ayşe Dolunay SARICA<sup>954</sup> , Yeliz COŞKUN<sup>955</sup>

### ÖZET

“Çocuğun üstün yararı” varsayımı gerekçesine dayanılarak, Yargıtay içtihatları aile mahkemelerinde idrak çağını yedi olarak kabul etmiş ve 2017 yılından bu yana aile mahkemelerinde sekiz yaşından gün almış çocukların hâkimler tarafından dinlenmesi uygulaması başlatılmıştır. Gelişim alanyazını ise, çekişmeli davalarda bireyin doğru kararlar almasını sağlayan soyut düşünme yetisinin 12-14 yaşlarda belirli bir aşamaya geldiğine ve her bireyde farklı bir gelişim seyri izlediğine dair bulgulara işaret etmektedir. Bu çerçevede yeni uygulamanın, gerçekten de çocuğun üstün yararı ilkesine hizmet edip etmediğine dair bilimsel sonuçlara gereksinim olduğu düşünülmüş ve aile mahkemelerinde görev yapan alan çalışanlarının gözlem ve görüşlerine başvurmanın verimli sonuçlar ortaya koyacağına inanılmıştır. Dolayısıyla bu araştırmanın amacı, sekiz yaşından gün alan çocukların aile mahkemelerinde dinlenmeleri uygulamasına yönelik hâkim, avukat ve aile mahkemesi uzmanlarının görüşlerinin belirlenmesidir. Araştırma, nitel araştırma modellerinden betimsel yöntem şeklinde desenlenmiştir. Her gruptan 15 olmak üzere İzmir Adliyesi Aile Mahkemelerinde görev yapan toplam 45 hâkim, avukat ve aile mahkemesi uzmanıyla yarı yapılandırılmış görüşmeler gerçekleştirilmiş, elde edilen dökümler tümevarımsal analiz tekniğiyle analiz edilmiştir. Analizlerden üç ana tema ortaya çıkmıştır: (1) yeni uygulamanın sürece getirileri, (2) yeni uygulamanın bireyler üzerindeki etkileri, (3) yeni uygulamaya ilişkin genel değerlendirme ve öneriler. Katılımcıların büyük çoğunluğu yeni uygulamanın iş yükünü artırdığı ve zaman kaybına yol açtığını, süreçte en yoğun yıprananların çocuklar olduğunu, aynı zamanda ailelerin de birtakım güçlüklerle karşılaştığını ifade etmişlerdir. Katılımcılar ayrıca çocuk dinleme yaşının sekize çekilmesinin de doğru bir uygulama olmadığını vurgulamışlardır.

---

953 İzmir Adliyesi, 9. Aile Mahkemesi, Pedagog, (uhcoskun@hotmail.com) <https://orcid.org/0000-0002-0892-8175>.

954 Dokuz Eylül Üniversitesi, Eğitim Fakültesi, Özel Eğitim Bölümü, Doç. Dr. (dolunaysarica@gmail.com) <http://orcid.org/0000-0003-3626-9469>

955 İzmir Adliyesi 12. Aile Mahkemesi, Pedagog, (uysalyeliz5@hotmail.com) <https://orcid.org/0000-0002-1807-6113>

Katılımcıların önerileri ise, eski sistemin yeniye kıyasla daha işlevsel olduğu yönündedir. Bu bulgular doğrultusunda, yeni uygulamanın revize edilmesi gerektiği sonucuna varılmıştır.

**Anahtar Sözcükler:** *Aile mahkemesi, Yargıtay İçtihatları, Velayet, İdrak Çağı*

## **JUDGE, LAWYER AND SPECIALİST OPINIONS ON CHILD HEARING IN CUSTODY LAWSUITS**

### **SUMMARY**

Beginning in 2017, based on the assumption of “the child’s best interest”, The Court of Appeals case law stated the age of perception in family courts be considered seven. Since then Turkish family courts have begun to hear children aged seven and over. Child development research however, has confirmed that abstract thinking in complex situations develops around the ages of 12-14. Therefore, the age of perception criterion in the 2017 trend calls for evidence on whether it is truly to the child’s best interest and the opinions of related professionals may be one of the best ways to investigate the situation in hand. Thus the aim of this study was to investigate the views of judges, lawyers and family court specialists regarding the hearing of children aged seven in family courts. The qualitative study included semi-structured interviews with a total of 45 participants (15 judges, 15 lawyers and 15 family court specialists) working in Izmir family courts. Three themes emerged as a result of deductive analysis conducted by the first and second authors: (1) the effects of the 2017 trend on family court cases, (2) the effects of the 2017 trend on related persons, and (3) recommendations for the 2017 trend. The results generally yielded opposing beliefs against the 2017 trend, including: an increase in the workload, loss of time, children being the first ones to go through the negative consequences and families having to face many difficulties. The participants also claimed that the age criterion for child hearing was an ineffective practice. Their recommendations were parallel to these beliefs, stating that the practice prior to 2017 was much more effective for all parties. Based on these findings, the authors concluded that the 2017 trend in family courts be revised.

**Key Words:** *Family court, Court of Appeals Case Law, Custody, Age of Perception.*

## I. GİRİŞ

Aile, tarihin ilk aşamalarından bu zamana kadar uzanan köklü bir kurum olmasına karşın, toplumsal değişimler, hukuki düzenlemeler ve sosyal yaşamı etkileyen tüm etmenlerden etkilenebilmekte, süre giden bir değişim döngüsü içerisinde yer almaktadır. Aile kurumu ile ilgili yaşanan bu değişim döngüsü sürecinden aile hukuku da doğrudan etkilenmekte, günümüzde aile içi uyuşmazlık konuları hızla artmakta ve hızla farklılaşmaktadır.<sup>956</sup> Aile kurumunda ortaya çıkan söz konusu değişimlere yanıt vermeyi amaçlayan ve anayasal olarak aile birliğinin korunması hususunda önlem alma sorumluluğu bulunan Türkiye Cumhuriyeti; Türk Medeni Kanunu, Aile Mahkemelerinin Kuruluş, Görev ve Yargılama Usullerine İlişkin Kanun, 6284 sayılı Ailenin Korunması ve Kadına Karşı Şiddeti Önlenmesine Dair Kanun ve Çocuk Koruma Kanunu gibi kanunlar düzenlemiştir. Diğer bir deyişle Türkiye Cumhuriyeti, mahkemeler aracılığıyla ailelerin gereksinimlerine yanıt vermeyi ve anayasal sorumluluğunu yerine getirmeyi hedeflemektedir.<sup>957</sup>

Aile kurumundaki değişimler ve aile uzlaşmazlıklarındaki niteliksel ve niceliksel artışın etkisiyle Aile Mahkemeleri'nin kurulması yargı süreci açısından önemli bir dönüm noktasıdır. Son olarak 2003 yılında yayınlanan 4787 sayılı Aile Mahkemelerinin Kuruluş, Görev ve Yargılama Usullerine İlişkin Kanun'la aile ile ilgili davalar, tercihen aile hukuku alanında lisansüstü eğitim almış, evli ve çocuklu aile mahkemesi hâkimleri tarafından yürütülmeye başlanmıştır. 4787 sayılı Aile Mahkemelerinin Kuruluş, Görev ve Yargılama Usullerine İlişkin Kanun ile ilgili bir diğer dönüm noktası aile mahkemelerinde tercihen evli, çocuklu ve aileler ile ilgili lisansüstü eğitim almış pedagoğ, psikoloğ ve sosyal hizmet uzmanlarının yer almasıdır. İlgili kanun ile atanan mahkeme uzmanlarından tüm dava sürecinde, davaya dâhil olan çocuklara eşlik etmeleri, çocuğun örselenmeden ya da mümkün olduğu kadar az zarar görerek yargı sisteminin dışına çıkmalarını

---

956 **Erbay, Ercüment / Gök, Fulya Akgül / Kardeş, Tuba Yüceer:** Aile Mahkemelerine Başvuran ve Boşanma Sürecinde Olan Ailelerin Problem Çözme Becerilerinin İncelenmesi. Türkiye Sosyal Araştırmalar Dergisi, 2015, 19.1: 139-154. Ayrıca bkz. **Erdem, Mehmet:** Aile Hukuku, Seçkin, İstanbul 2018, **Meşe, İlknur:** Sosyal Değişim Sürecinde Aile ve Kadın, in Elmas, Nazım (Ed.), Kadın ve Aile Hayatı, Pegem Yayınları, Ankara 2017, **Özcan, Cem:** Fransız Hukukunda Aile Arabuluculuğu. Journal of Judgments by the Court of Jurisdictional Disputes/Uyumsuzluk Mahkemesi Dergisi, 2017, 9, 383-396, **Ünal, Fatma:** Aile Eğitiminde Ebeveyn Hakları ile ilgili Yasalar ve Etik Kurallar, in Temel, Zeynep Fulya (Ed.), Aile Eğitimi ve Erken Çocukluk Eğitiminde Aile Katılım Çalışmaları, Anı Yayıncılık, Ankara 2015.

957 **Filiz, Orhan:** Türkiye'de Aile Mahkemeleri Uygulaması ve Uygulamanın Değerlendirilmesi Üzerine Bir Araştırma. Sosyal Politika Çalışmaları Dergisi, 2011, 25.25: 73-96. Ayrıca bkz. **Günay-İnan, Esra:** "Aile Hukukunda Geçici Hukuki Himaye Tedbirleri" Adalet Yayınevi, Ankara 2018, **Özel, Çağlar/ Tatar, Erol:** Aile Mahkemelerinin Yapısı ve Kararları Üzerine Genel Bir Değerlendirme. Sosyoekonomi, 2008, 1: 49- 88, **Ünal,** s. 116.

sağlamaları beklenmektedir. Bu yanıyla uzmanların aile mahkemelerinde çalışmalarının ve aile mahkemesi hâkimleri ile koordine bir çalışma yürütmelerinin çocuk merkezli bir uygulama olduğu söylenebilir.<sup>958</sup>

Aile mahkemeleri uzmanları genellikle boşanma, velayetin değiştirilmesi, kişisel ilişkinin düzenlenmesi, evlat edinme ve evliliğe izin dosyalarında görev almaktadır. Uzmanlardan, boşanma davalarında tarafların evlilik birlikteliği durumunu ve sulh imkânını değerlendirmeleri, tarafların 18 yaşının altında çocukları varsa, çocuğun velayetinin kime verileceği ve diğer ebeveyn ile kişisel ilişkinin nasıl düzenleneceği hususunda görüş bildirmeleri beklenmekteyken, velayetin değiştirilmesi davalarında çocuğun velayetinin bulunduğu ebeveyninden alınıp diğer ebeveynine verilmesinin uygun olup olmadığını değerlendirmeleri beklenmektedir. Kişisel ilişki davalarında çocuğun velayetinin bulunmadığı ebeveyni ile hangi süre zarflarında görüşeceklerini değerlendirmeleri, evlat edinme davalarında ise evlat edinme talebinde bulunan tarafların ve evlat edinilmesi talep edilen çocuğun uygunluğunu değerlendirmeleri istenmektedir. Uzmanlardan bu amaçlar doğrultusunda çocuklarla, çocukların ebeveynleriyle ya da ilgili diğerleriyle görüşme yapmaları, okul ve sosyal çevre incelemeleri gerçekleştirmeleri, son olarak da yazılı bir rapor şeklinde görüşlerini beyan etmeleri talep edilmektedir.<sup>959</sup>

Aile mahkemelerinin kurulması ve uzmanların aile mahkemelerinde görev almasıyla birlikte çocukların aile mahkemesi duruşmasında hâkim tarafından dinlenme uygulaması büyük ölçüde son bulmuş, bu uygulamanın yerine aile mahkemesi uzmanı tarafından çocuğun ev, okul ve sosyal çevre incelemelerinin yapıldığı, duruşma ortamından bağımsız bir ortamda kapsamlı ve düzeyine uygun olarak dinlendiği, ebeveynleri ve çevresindeki diğerleriyle de görüşülerek daha kapsamlı bir değerlendirmenin yapıldığı yeni bir uygulamaya geçilmiştir. Bu yeni uygulamayla, uzmanlar bir yandan bilimsel bir yaklaşım çerçevesinde çocuğun velayeti gibi konularda mahkeme sürecine katkı sunarken, diğer yandan ailenin ve çocuğun korunmasına yönelik koruyucu ve destekleyici önlemler önerebilmektedir.<sup>960</sup>

---

958 **Özel / Tatar**, s. 84. Ayrıca bkz. **Altındağ, Özgür. / Sağlam, Mehmet**: Boşanma Sürecinde Çocukların Haklarının Belirlenmesi ve Korunmasında Aile Mahkemesi Uzmanlarının Rol ve İşlevleri, Uluslararası Katılımlı Çocuk İhtiyaçları Sempozyumu Bildiri Kitabı, Mutlu Çocuklar Derneği Yayınları, Ankara 2012.

959 **Ardıç, Oğuzhan**: Medeni Hukuk. Seçkin Yayınevi, Ankara 2008. Ayrıca bkz. **Altındağ / Sağlam**, s. 427.

960 **Altındağ / Sağlam**, s. 431. Ayrıca bkz. **Buz, Sema / Düzyurt, Kübra. / Sağlam, Mehmet**: Aile Mahkemesinde Çalışan Sosyal Çalışma Görevlilerinin Sosyal İnceleme Raporlarına İlişkin Değerlendirmeleri: Ankara Adliyesi Örneği. Toplum ve Sosyal Hizmet, 2015, 26.2: 7-30, **Filiz**, s. 74, **Kılıç, Çiğdem**: Aile Mahkemelerinde Görev Yapan Uzmanların Hizmet İçi Eğitim İhtiyacı. Ahi Evran Üniversitesi Kırşehir Eğitim Fakültesi Dergisi, 14(2), 2013, 14.2: 273-290, **Özel / Tatar**, s. 59.

Aile mahkemesi hâkimlerinin büyük çoğunluğu tarafından tercih edilen çocuğun uzman tarafından dinlenmesi ve ailesi, evi, okulu, sosyal çevresi göz önüne alınarak kapsamlı bir şekilde değerlendirilmesi uygulaması Yargıtay 2. Hukuk Dairesinin içtihatları doğrultusunda yeni bir sürece girmiştir. Yargıtay 2. Hukuk Dairesi 2017/3117 Esas ve 2018/1278 Karar, 2017/226 Esas ve 2017/1180 Karar, 2017/399 Esas ve 2017/1406 Karar, 2017/371 Esas ve 2017/2508 Karar numaralı içtihatlarında sekiz yaşından itibaren çocukların idrak çağında olduğu, bu çocukların Birleşmiş Milletler Çocuk Hakları Sözleşmesi'nin 12. maddesine ve Çocuk Haklarının Kullanılmasına Dair Avrupa Sözleşmesinin 3. ve 6. maddelerine göre kendilerini ilgilendiren davalarda söz hakkına sahip olduğu, bu nedenle duruşmada mahkeme hâkimi tarafından dinlenmesi gerektiği vurgulanmıştır. Bu içtihatlar doğrultusunda aile mahkemeleri hâkimleri sekiz yaşından gün alan çocukları duruşma salonunda dinlemeye başlamıştır.

Türkiye alanyazını, aile mahkemelerinde çocukların duruşma salonunda dinlenmesinin çocuklar ve aileleri üzerinde doğurabileceği sonuçlara ilişkin herhangi bir araştırmaya işaret etmemektedir. Dolayısıyla çocuğun üstün yararına olduğu iddia edilen söz konusu uygulamanın, gerçekten de bu görüşe hizmet edip etmediğine dair bilimsel sonuçlara gereksinim olduğu düşünülmüştür. Yürürlükte olan uygulamanın, bizzat merkezinde olanlar tarafından değerlendirilmesinin, çocukların iyilik halinin gözetilmesi kapsamında adalet sistemimize yol gösterici olacağına inanılmıştır ve bu noktadan hareketle hâkim, avukat ve uzmanların görüşlerine başvurulması planlanmıştır. Dolayısıyla bu araştırmanın amacını, sekiz yaşından gün alan çocukların velayet davalarında mahkeme tarafından doğrudan dinlenmeleri uygulamasına yönelik hâkim, avukat ve uzmanların görüşlerinin belirlenmesi oluşturmaktadır. Bu amaç doğrultusunda şu sorulara yanıt aranmıştır:

1. Hâkimler, avukatlar ve aile mahkemesi uzmanlarının, velayet davalarındaki yeni uygulamanın mahkeme sürecine etkilerine ilişkin görüşleri nelerdir?
2. Hâkimler, avukatlar ve aile mahkemesi uzmanlarının, velayet davalarındaki yeni uygulamanın ilgili bireyler üzerinde yarattığı etkilere ilişkin görüşleri nelerdir?
3. Hâkimler, avukatlar ve aile mahkemesi uzmanlarının, velayet davalarındaki yeni uygulamanın iyileştirilmesine ilişkin önerileri nelerdir?

## II. YÖNTEM

Bu araştırmada, bir konuda katılımcı görüşlerine kapsamlı olarak ulaşmada en etkili modeller arasında yer alan nitel araştırma modellerinden betimsel yöntem tercih edilmiştir.<sup>961</sup>

## A. ÇALIŞMA GRUPLARI

Araştırmanın çalışma grubu, İzmir Adliyesi'nde görev yapan 15 hâkim, İzmir Barosu'na kayıtlı olan 15 avukat ve 15 Aile Mahkemesi uzmanı olmak üzere toplam 45 kişiden oluşmaktadır. Katılımcıların demografik özellikleri Tablo 1'de özetlenmiştir.

**Tablo 1.** Katılımcıların Demografik Özellikleri

		Hâkim		Avukat		Uzman	
		f	%	f	%	f	%
Yaş	26-35	1	6.7	5	33.3	5	33.3
	36-45	-	-	9	60	9	60
	46 - ...	14	93.3	1	6.7	1	6.7
Cinsiyet	Erkek	3	20	6	40	5	33.3
	Kadın	12	80	9	60	10	66.6
Aile mahkemesinde görev süresi (yıl)	0-5	7	46.7	6	40	4	26.7
	6-10	5	33.3	6	40	6	40
	11-15	3	20	3	20	5	33.3

961 Glesne, Corrine / Peshkin, Alan: Becoming Qualitative Researchers. White Plains, New York 1992. Ayrıca bkz. Miles, Matthew / Huberman, Micheal: Qualitative Data Analysis: An Expanded Sourcebook. SAGE, Londra 1994, Şimşek, Hasan / Yıldırım, Ali: Sosyal Bilimlerde Nitel Araştırma Yöntemleri. Ankara: Seçkin Yayıncılık, 2011.

## **B. VERİ TOPLAMA ARAÇLARI**

Araştırmacılar tarafından gerçekleştirilen kapsamlı alanyazın taramasında, araştırma sorularının yanıtlanmasında kullanılacak herhangi bir ölçme aracına rastlanamamıştır. Bu gerekçe doğrultusunda araştırmanın verileri, araştırmacılar tarafından geliştirilen Hâkim, Avukat ve Uzman Görüşme Formları ile toplanmıştır. Katılımcıların yaş, cinsiyet ve görevdeki sürelerine ilişkin bilgiler, görüşmelerin başında katılımcılara sorularak her görüşme formunun üst bölümüne eklenen ilgili kutucuklara yazılarak elde edilmiştir. Gizlilik prensibi dikkate alınarak, katılımcılardan isim ve adres gibi kişisel bilgiler talep edilmemiştir.

### **1. Hâkim Görüşme Formu**

Yarı yapılandırılmış sorulardan oluşan form ilk olarak aile mahkemesinde çalışan bir hâkim ile psikolojik danışmanlık alanında doktora eğitimini tamamlamış bir aile mahkemesi uzmanı tarafından yüz ve kapsam geçerliği bakımından değerlendirilmiş ve geribildirimler doğrultusunda formun altı soruluk son hali elde edilmiştir. Form bu haliyle, aile mahkemesi geçmişi olan bir hâkimle denenmiş, formda herhangi bir sorun gözlenmemiştir.

### **2. Avukat Görüşme Formu**

Beş sorudan oluşan bu form, ilk aşamada İzmir barosuna kayıtlı olarak avukatlık yapan ve sıklıkla aile mahkemesinde çalışan bir avukata ve psikolojik danışmanlık alanında doktorasını tamamlayan bir aile mahkemesi uzmanına gönderilmiş ve bu uzmanlar tarafından yüz ve kapsam geçerliği boyutlarında değerlendirilmiştir. Geribildirimler ışığında revize edilen form, aile mahkemesinde sıklıkla dosyası bulunan bir avukat ile pilot uygulamaya tabi tutulmuş ve ikinci bir revizyonla son haline kavuşmuştur.

### **3. Uzman Görüşme Formu**

Yine araştırmacılar tarafından oluşturulan bu görüşme formunun ilk hali, psikolojik danışmanlık alanında doktor öğretim üyesi olan bir akademisyene ve psikolojik danışmanlık alanında doktora eğitimini tamamlayan bir aile mahkemesi uzmanına gönderilerek yüz ve kapsam

geçerliği bakımından sınınmıştır. Geribildirimler doğrultusunda ikinci kez düzenlenen formun bir aile mahkemesi uzmanıyla gerçekleştirilen pilot uygulaması sonrasında forma son hali verilmiştir. Uzman görüş formu toplam altı maddeden oluşmaktadır.

### C. SÜREÇ VE VERİLERİN ANALİZİ

T.C. Adalet Bakanlığı Hâkimler ve Savcılar Kurulu ile Personel Genel Müdürlüğü'nden gerekli izinlerin alınmasıyla birlikte, katılımcılara telefon yoluyla ulaşılarak görüşme talep edilmiş ve araştırmaya katılmaya gönüllü olan toplam 45 hâkim, avukat ve aile mahkemesi uzmanıyla 2019 Şubat ayı içerisinde birinci araştırmacı tarafından yüz yüze bireysel görüşmeler gerçekleştirilmiştir. Görüşme esnasında Hâkimler ve Savcılar Kurulu talepleri doğrultusunda ses ve görüntü kaydı alınamamış, görüşmelerde yardımcı görüşmeci olarak üçüncü araştırmacı bulunmuştur. Her iki araştırmacı, katılımcıların yanıtlarını görüşme esnasında not almış ve görüşmeler sonrasında iki grup not karşılaştırılarak, verilerin geçerliği ve güvenilirliği sağlanmaya çalışılmıştır. Tüm görüşmeler İzmir Adliyesi'nde gerçekleştirilmiştir.

Görüşmelerin tamamlanmasıyla birlikte veriler Betimsel Veri İndeksi formatına uygun olarak Word 2003 dosyasına aktarılmış ve birinci ve ikinci araştırmacı tarafından bağımsız olarak analiz edilmiştir. Katılımcıların kimlik bilgilerinin gizli tutulması amacıyla Betimsel Veri İndeksi'ne aktarılan verilerde tüm katılımcılar için kodlar kullanılmıştır (Örneğin H4, görüşülen dördüncü hâkimi ifade etmiştir).

Veriler tümevarımsal içerik analizi tekniğiyle analiz edilmiştir. Araştırmacılar bu aşamada, verileri detaylı okuyup Betimsel Veri İndeksi'nde yer alan ilgili sütunlara görüşlerini yazmışlar ve bu görüşler çerçevesinde kategoriler ve temalar oluşturmuşlardır. Bağımsız analizlerden elde edilen iki grup bulgu, birinci ve ikinci araştırmacı tarafından karşılaştırılmış ve 0.84 düzeyinde gözlemciler arası güvenilirlik katsayısı elde edilmiştir. Güvenirlik katsayısı görüş birliği / görüş birliği + görüş ayrılığı X 100 formülüyle hesaplanmış ve elde edilen oranın, bulguların güvenilir olduğunu göstermiştir. <sup>962</sup>

Üç katılımcı gruptan (hâkimler, avukatlar ve uzmanlar) elde edilen kategorilerin gruplar arasında binişiklikler gösterdiği gözlenmiş, bu nedenle üç veri grubu ortak analiz edilerek üç ana temaya ulaşılmıştır.

---

962 Miles / Huberman, s. 48.



### III. BULGULAR

Verilerin analizi, 45 katılımcıdan elde edilen verilerin üç temada toplandığını göstermiştir. Bu temalar "Yargıtay içtihatları sonrası uygulamanın sürece getirileri", "Yargıtay içtihatları sonrası uygulamanın bireyler üzerindeki etkileri" ve "Yargıtay içtihatları sonrası uygulamaya yönelik genel değerlendirme ve öneriler" olmak üzere farklı başlıklar altında sunulmuştur.

#### A. TEMA 1. YARGITAY İÇTİHATLARI SONRASI UYGULAMANIN SÜRECE GETİRİLERİ

Katılımcılar, Yargıtay içtihatları öncesindeki tercihlerini dile getirirken 12 hâkim, uzman tarafından hazırlanan ev ve sosyal inceleme raporunu yeterli gördüklerini, üçü ise bu raporla birlikte çocuğu da mahkeme salonunda dinlediklerini belirtmişlerdir. Avukatların 12'si de rapor dışında çocuğun duruşma salonunda dinlenmesi gibi bir talepte bulunmadıklarını, üçü ise çocuğun dinlenmesini talep ettiklerini ifade etmişlerdir. Son olarak 10 uzman, bağlı buldukları hâkimlerinin raporla yetindiklerini, ikisi çocuğu uzman ile birlikte nadiren de olsa duruşma salonunda dinlediğini ve diğer ikisi ise hâkimlerinin yine mağdurun yanında uzman olmak koşuluyla çocuğu dinlemeyi tercih ettiklerini açıklamışlardır. Önceki uygulamadaki genel eğilimlerin bu özetleri doğrultusunda, katılımcılar, yeni uygulamanın başlatılmasıyla birlikte yargı aşamasında meydana gelen birtakım değişikliklerden söz etmişlerdir. Tablo 3'te bu temadan elde edilen görüşlerin frekans ve yüzde dağılımları yer almaktadır.

**Tablo 2.** *Yargıtay İçtihatları Sonrası Uygulamanın Sürece Getirilerine İlişkin Görüşler*

Görüş	f
Hâkimlerin yeni tedbirlere başvurmak durumunda kalmaları (çocuğun beyanı esnasında salonu boşaltma, soruları uygun dil kullanarak sormaya çalışma, cübbe çıkartma, duruşmayı adliyenin nispeten boş olduğu saatlerde yürütme, Adli Görüşme Odası uygulaması talep etme)	36
Yeni uygulamanın süreci herhangi bir şekilde etkilememesi	16
Çocuğun uzman görüş raporundaki beyanlarını tekrar etmesi	12

Uzmanın, acil duruşma çağrılarında süregiden görüşmelerine ara vermek durumunda kalması	9
Yargı sürecinin gereksiz uzaması	7
Yeni uygulamanın, hâkimin daha sağlıklı kararlar almasını desteklemesi	6
İş yükünün artması	4
<b>Toplam görüş sayısı</b>	<b>90</b>

Tablo 2’de de görüldüğü gibi, katılımcıların %35.56’sı (n=16), yeni uygulamanın süreçte herhangi bir değişikliğe neden olmadığı yönünde görüş bildirmiştir. Bununla birlikte diğerlerinin çeşitli olumlu ya da olumsuz değişimleri ifade ettikleri dikkat çekmektedir. Bunlar arasında en sık belirtilen değişiklik, hâkimlerin çocukları dinlerken başvurmak durumunda oldukları bazı stratejilerdir. Bu kategori altında 14 hâkimin salonu boşalttırarak çocuğu dinlemeyi uygun bulması, 12 hâkimin çocuğu rencide etmeyecek uygun bir dil kullanmaya özen göstermesi, dört hâkimin çocuğun tedirgin olmaması adına cübbesini çıkartarak duruşmayı yürütmesi, dört hâkimin adli görüşme uygulaması talep etmesi ve ikisinin duruşma saatlerini adliyenin nispeten boş olduğu saatlere yerleştirmesi türünde uygulamalar sayılabilir. Bu gibi uygulamalar, hâkimlerin çocukların iyilikleri adına bireysel çabalar sarf ettiklerini düşündürmektedir. Bununla birlikte, dört hâkimin, yeni uygulamanın iş yükünü artırdığını, yedi avukatın ise sürecin gereksiz yere uzadığını belirtmeleri dikkat çekmiştir. Uzmanların %80’i de (n=12), hâkim ve avukatlara paralel olarak, çocukların duruşma salonunda dinlenmelerinin, hazırladıkları raporun yersiz tekrarından öte bir uygulama olmadığını belirtmişlerdir. Buna ek olarak dokuz uzman, kendilerine yapılan acil duruşma çağrılarının artmasıyla, yürütmekte oldukları çocuk görüşmelerini bölmek durumunda kaldıklarından ve bunun da görüşülen çocuğu olumsuz etkilediğinden yakınmışlardır. Özetle, üç katılımcı grupta yer alanların önemli bir yüzdesinin yeni uygulamanın olumsuz getirilerine işaret ettikleri gözlenmiştir.

## **B. TEMA 2. YARGITAY İÇTİHATLARI SONRASI UYGULAMANIN BİREYLER ÜZERİNDEKİ ETKİLERİ**

Verilerden elde edilen ikinci tema, katılımcıların, yeni uygulamanın süreçte yer alan bireyler üzerindeki duygusal etkilerine ilişkin görüşleri içermektedir. Hâkimler, aileler ve çocuklara ilişkin etkilerin belirlendiği bu temada yer alan kategoriler Tablo 3’te sunulmuştur.

**Tablo 3. Yargıtay İçtihatları Sonrası Uygulamanın Bireyler Üzerindeki Etkilerine İlişkin Görüşler**

<b>Görüş</b>	<b>f</b>
Çocukların adliye ortamına gelmekteki isteksizlikleri	21
Ailelerin, hâkim talepleri doğrultusunda ancak kendi istekleri dışında çocuklarını duruşma salonuna getirmek zorunda kalmaları	13
Çocuk dinlemenin hâkimlerde olumsuz duygular yaratması	7
Çocuğun aile bireylerinin etkisi altında ifade vermesi	5
Çocuğun hâkim karşısında tercih yapmada zorlanması	5
<b>Toplam görüş sayısı</b>	<b>51</b>

Tablo 3'te görüldüğü üzere, katılımcıların yeni uygulamanın hâkimler, aileler ve çocuklar üzerinde birtakım olumsuz etkiler yarattığını düşündükleri görülmektedir. Katılımcıların yaklaşık yarısı (7 hâkim, 5 avukat ve 9 uzman olmak üzere toplam 21 katılımcı), çocukların duruşmalara katılma konusunda isteksizlik yaşadıklarını gözlemlemişlerdir. Uzmanlar, söz konusu isteksizliği çocukların aileleriyle yaptıkları görüşmelerde fark ettiklerini belirtmişlerdir. Bu gözlemlerle bağlantılı olarak, yedi avukat ve altı uzman (katılımcıların %28.89'u), ailelerin bunun farkında olmalarına karşın, hâkimin, bir diğer deyişle otoritenin taleplerine uyum gösterme zorunluluğu hissederek çocuklarını duruşma salonuna getirmek zorunda kaldıklarını vurgulamışlardır. Beş hâkimin, çocukların ifadelerinden, onların aile bireylerinin etkisi altında ifade verdikleri ve yine hâkim grubundan beş katılımcının çocukların ifade sürecinde karar vermede zorlandıklarına dair gözlemleri, bir anlamda süreç içerisinde çocukların duygusal bağlamda ne derece yıprandıklarını gözler önüne sermektedir. Diğer yandan yedi hâkimin, duruşma salonunda çocuk dinlemenin kendilerinde olumsuz duygular yarattığını belirtmeleri de, ilginç kabul edilebilecek bulgular arasında yer almaktadır.

### **C. TEMA 3. YARGITAY İÇTİHATLARI SONRASI UYGULAMAYA YÖNELİK GENEL DEĞERLENDİRME VE ÖNERİLER**

Katılımcılar, Yargıtay içtihatları sonrası yürürlükte olan uygulamanın genel değerlendirmesini de yapmışlar ve çocukların hâkim tarafından dinlenmesi sürecine ilişkin

birtakım önerilerde de bulunmuşlardır. Tablo 4’te, söz konusu değerlendirme ve öneriler yer almaktadır.

**Tablo 4.** Yargıtay İçtihatları Sonrası Uygulamaya Yönelik Genel Değerlendirme ve Öneriler

<b>Görüş</b>	<b>f</b>
Uzman raporunun karar vermede başvurulacak ölçüt olması	20
Her durumda çocukla ilgili sosyal çevrenin değerlendirildiği raporun olması	9
Çocukların mahkemede dinlenmelerinin etkili bir uygulama olması	7
Çocuğun, uygun fiziksel koşulların sağlanması ve uygun yaşta olması koşuluyla mahkemede dinlenmesi	4
Çocuğun dinlenmesinde yaş ve gelişimsel özelliklerin dikkate alınması	3
Çocuk dinleme yaşı alt sınırının 12 olması	3
<b>Toplam görüş sayısı</b>	<b>46</b>

Tablo 4 genel olarak incelendiğinde, görüşlerin iki ana kategoride toplandığını söylemek mümkündür. İlk kategori, çocukların mahkemede dinlenmesinin uygun olmadığı, bunun yerine uzman tarafından yapılacak çalışmalar sonrasında mahkemeye sunulacak raporun yeterli olduğu görüşünü içermektedir. Sekiz hâkim ve 12 uzmanın dâhil olduğu bu görüşün, avukatlar tarafından destek görmemiş olması dikkate değerdir. Ne var ki avukatların önemli bir yüzdesi (%60), her durumda uzman tarafından ev, okul ve sosyal çevre değerlendirmesinin yapılması görüşünü öne sürmüştür. İkinci kategoriyi oluşturan görüş ise, çocukların duruşmalarda hâkim tarafından dinlenmesi yönündedir ancak bu görüşü savunan bazı katılımcılar, bunun birtakım koşulların sağlanması durumunda yapılması gerektiğini vurgulamışlardır. Buna göre üç hâkim, üç avukat ve bir uzman kararın doğruluğunu koşulsuz savunurken, dört hâkim uygun fiziksel koşulların sağlanması (neler olduğunu belirtmemişlerdir) ve dinlenme yaşının artırılması koşullarıyla çocuk dinlemenin uygun olabileceğini belirtmişlerdir. Ayrıca üç avukat çocukların yaş ve gelişimsel özelliklerinin dikkate alınarak dinlenmelerinin, üç uzman ise çocukların duruşma salonunda dinlenme yaşlarının minimum 12 olmasının doğru yaklaşımlar olduğunu ifade etmişlerdir.

#### IV. TARTIŞMA VE SONUÇ

2017’de yürürlüğe giren ve sekiz yaşından gün alan çocukların aile mahkemelerinde dinlenmelerini öngören Yargıtay 2. Hukuk Dairesi 2017/3117 Esas ve 2018/1278 Karar, 2017/226 Esas ve 2017/1180 Karar, 2017/399 Esas ve 2017/1406 Karar, 2017/371 Esas ve 2017/2508 Karar numaralı içtihatlarının pratikte ne gibi sonuçlar doğurduğuna yönelik gerçekleştirilen bu araştırmada, söz konusu uygulamanın hâkim, avukat ve aile mahkemesi uzmanı görüşlerine göre birtakım sakıncaları olduğu sonucunu çıkartmak mümkün görünmektedir. Uygulamanın doğrudan içinde olan bu meslek mensupları, kendilerine dair belirttikleri güçlükleri açıklamanın yanında, süreçte yer alan çocuklar ve ailelerin de örselendiklerini ifade etmişlerdir.

Katılımcı görüşlerinin toplandığı ilk tema, yeni uygulamayla birlikte süreçte nelerin değiştiğini içermiştir. Bu konuya ilişkin elde edilen toplam 90 yanıtın %75.56’sı (n=68), yeni uygulamanın yargı sürecini olumsuz etkilediği yönündedir. Her üç grupta yer alan katılımcılar, bu uygulamayla iş yükünün artması ve sürecin yersiz uzaması gerekçelerini öne sürmüşlerdir. Örneğin hâkimler, daha küçük yaştaki çocukları mahkeme salonunda dinlemeye başladıklarından bu yana gerçekleştirdikleri kişisel düzenlemelerden söz etmişlerdir. 36 yanıtın belirlendiği bu kategoride hâkimler, cübbe çıkartma, çocuğa daha uygun bir dille yaklaşma, çocuğu yalnız dinleyebilmek için salonu boşalttırma ve duruşmayı adliyenin nispeten boş olduğu saatlerde yürütme gibi uygulamalar yapmak durumunda kaldıklarını belirtmişlerdir. Bir hâkim, yaşadığı söz konusu güçlüğü şu sözlerle ifade etmiştir:

*“İş yükünde artış oldu. Mesela dosyalarda tanık varsa, o gün çocuk çağırmıyorum. Tek tek o günkü dosyalara bakmam gerekiyor. Bazen de öğleden sonra, daha geç bir saatte çocuğu çağırıyorum. Çocuğun zarar görmemesi adına çok zaman ayırıyorum. Çalışma koşulları ve adliye şartları çok zorlayıcı. Çocuklara uygun bir şey yok burada.” (H5).*

Ayrıca dört hâkim, Adli Görüşme Odası (AGO) talep ettiğini ancak adliyede yalnızca bir AGO olmasından dolayı bu hizmetten yararlanamadıklarını ifade etmiştir. Çocuğun iyilik halini gözetmek adına bu tür uygulamalara başvuran hâkimlerin olduğunu bilmek, elbette yüz güldürücüdür. Ne var ki, bu noktada şunları sorgulamak doğru olacaktır: (1) bu tür inisiyatifler hâkimlerin görev ve sorumlulukları arasında sayılmalı mıdır? (2) sayılmalı ise, hâkimler bu tür düzenlemelere başvurmak üzere hizmet içi eğitim almışlar mıdır? (3) bu tür tedbirlere başvurmeyen bir hâkimle karşılaşan çocuğun ve ailesinin iyilik halinden söz edilebilir mi? Bu üç tartışma noktasından çıkarılması gereken sonuç, çocukların dinlendiği tüm aile mahkemesi davalarında bu tür tedbirlerin her hâkim tarafından alınması gereğidir. Bir diğer deyişle, hiçbir çocuğun ve ailesinin farklı hâkimler tarafından farklı süreçlere tabi tutulmaması garanti altına alınmalıdır. Ne var ki,

hâkimler bu tür çocuk dostu uygulamalara ilişkin herhangi bir eğitimden yararlandırılmamaktadırlar. Ayrıca böyle bir eğitim aldıkları takdirde, bunun gerçekten de çocuk adına işe yarayıp yaramadığının belirlenmesi gerekmektedir. Dolayısıyla bu tür bir hizmet içi eğitim sağlama ve eğitimin sonuçlarını değerlendirme sürecinin ileriki araştırmalarda ele alınmasını önermek doğru gibi görünmektedir.

Aile mahkemesi uzmanları da, hâkimler gibi, süreçte yaşadıkları güçlüklerden söz etmişlerdir. Uzmanların %60'ı (n=9), yeni uygulamayla birlikte sıklaşan acil duruşma çağrılarının, hâlihazırda yürütmekte oldukları çocuk ve aile görüşmelerini sekteye uğrattığından ve bunun da çocuğu olumsuz etkilediğinden yakınmışlardır. Bir uzman: *“Bazen (bir çocukla) görüşmedeyken duruşma salonuna çağrılıyorum. Görüşmecim ağlıyor olsa bile onu görüşme odasından çıkartıp duruşma salonuna gidiyorum. ... Görüşme daha sonra verimli olmuyor.”* (U15) sözleriyle yeni uygulamanın kendisi ve çocuk üzerindeki olumsuz etkilerini açık şekilde ortaya koymuştur.

Araştırmanın ikinci teması, yeni uygulamanın çocuklar, aileler ve hâkimler üzerinde yarattığı olumsuz duygusal sonuçları içermektedir. Buna ilişkin hâkim, avukat ve uzman görüşleri, yeni uygulamadan duygusal bağlamda en yoğun etkilenenlerin çocuklar olduğu yönünde birleşmektedir. Katılımcılar, çocukların duruşma ortamına gelmekten rahatsızlık duyduklarını, hâkim huzurunda beyan verirken de ebeveynlerinin etkisinde kalabildiklerini ve velayet konusunda karar vermekte zorlandıklarını gözlemlenmişlerdir. Bir hâkim, durumu şu sözlerle ifade etmiştir:

*“Genel olarak çocuklar geliyor ama bazen gelmek istemiyorlar. Duruşma salonunda beyan vermek istemiyorlar. Onlarla ilgili sadece rapor alma yoluna gittim. Israrla getirmek istemedim. Çocuk gelmek istemiyorsa, gelmemeli. Bazı aileler duruşma salonunda ve adliyede kavga ediyor. Çocukları anlayabiliyorum”* (H9).

Bu durum, çocukların duruşma ortamında olduğu kadar, duruşma öncesi süreçlerde de duygusal yıpranmayla karşı karşıya kaldıklarını düşündürmektedir. Katılımcıların ayrıca, ailelerin çocuklarını duruşma ortamına getirmek istememelerine karşın otorite figürü olarak kabul ettikleri hâkimlerin talepleri doğrultusunda bunu “mecburen” yapmaktan rahatsız olduklarına ilişkin gözlemleri de, uygulamanın çocukların olduğu kadar ailelerin de üzerinde duygusal baskılar oluşturduğunu gözler önüne sermektedir. Bu aynı zamanda, farklı bir zorluğu da beraberinde getirecek bir uygulama olabilir. Şöyle ki, bazı ebeveynler, çocuklarının velayetini alabilmek için çocuklarına baskı yapabilir ve çocuğun baskı yapan ebeveyn lehine tercih yaptığının hâkim tarafından da bilinmesini isteyebilirler. Nitekim 11 katılımcı avukat, bu yönde tercih yapan aileler olduğunu bildirmiştir. Bunun da (en azından bazı) hâkimler tarafından dikkate alınması

kaçınılmazdır. Dolayısıyla nihai karar, çocuğun yararına hizmet etmekten ziyade onun zararına olma riski taşıyacaktır. Bu aynı zamanda, çocuğu geniş bir zaman diliminde duygusal yıpranmayla karşı karşıya bırakacaktır. Günümüzde, söz konusu geniş bir zaman dilimindeki yıpranma sürecinin farkına varılmış ve hâkimler “çocuğun yüksek yararı adına karar” yerine “çocuğun yüksek yararı adına süreç yürütme” bakış açısını dikkate almaya başlamışlardır.<sup>963</sup> Ne var ki, Türkiye’de yürütülen bu yeni süreç, bu anlayış doğrultusunda hareket etmede yetersiz kalıyor gibi görünmektedir.

Avukatlar ve uzmanların bir kısmı (n=13), ailelerin süreçte çocuklarının dinlenmesini tercih etmeyebildiklerini ancak hâkim talebi doğrultusunda çocuklarının dinlenmesi işlemi kabul etmek durumunda kaldıklarını öne sürmüşlerdir. Türkiye Cumhuriyeti bireysel hak ve tercihleri dikkate alan bir siyasi ve toplumsal yapılanmayı benimsemiştir ancak bu sistem vatandaşların da hak ve özgürlüklerinin bilincinde olmaları ve gerekli durumlarda bu hak ve özgürlükleri talep etmeleriyle ayakta durabilecektir. Ülkemizde aile mahkemelerine intikal etmiş davalarda yer alan aile bireylerinin, söz konusu haklarının ne derece farkında oldukları tartışmalı bir konudur. Nitekim yasal mevzuat ve ilgili uluslararası sözleşmeler incelendiğinde, bu araştırmanın katılımcılarının mahkeme salonlarında gerçekleşen uygulamalara ilişkin gözlemleri bu metinlerle ters düşebilmektedir. Örneğin, Birleşmiş Milletler Çocuk Hakları Sözleşmesi’nin 3. ve 6. maddeleri ile Çocuk Haklarının Kullanılmasına İlişkin Avrupa Sözleşmesi’nin 12. maddesine atıfta bulunan Yargıtay 2. Hukuk Dairesi’nin ilgili içtihatları incelendiğinde, idrak çağındaki çocuğun hâkim tarafından bizzat dinlenmesi gerektiği yönünde bozma kararının olduğu görülmektedir. İdrak çağı olarak da soyutlama yeteneğinin tıbben gelişmeye başladığı yedinci yaşın doldurulması temel alınmaktadır.<sup>964</sup> Çocuk Haklarının Kullanılmasına İlişkin Avrupa Sözleşmesinin Onaylanmasının Uygun Olduğuna Dair Kanun’un 3. maddesinde ise aşağıdaki hüküm yer almaktadır.

*“Yeterli idrake sahip olduğu iç hukuk tarafından kabul edilen bir çocuğa, bir adli merci önündeki, kendisini ilgilendiren davalarda, yararlanmayı bizzat da talep edebileceği aşağıda sayılan haklar verilir: a) ilgili tüm bilgileri almak; b) kendisine danışılmak ve kendi görüşünü ifade etmek; c) görüşlerinin uygulanmasının olası sonuçlarından ve her tür kararın olası sonuçlarından bilgilendirilmek”*

Aynı kanunun 6. maddesinde aşağıdaki hüküm yer almaktadır.

---

963 **Vorderstrasse, Donna Jo:** A Judicial Perspective On Child Custody Evaluations. In Goldstein, Mark (Ed.), Handbook of Child Custody, Springer, London 2016.

964 **Yenisey, Feridun:** Mağdur Çocuk Haklarına İlişkin Öneriler, Uğur Eğitim Pazarlama ve Yayıncılık, İstanbul 2017.

*“Bir çocuğu ilgilendiren davalarda adli merci, bir karar almadan önce: a) Çocuğun yüksek çıkarına uygun karar almak için yeterli bilgiye sahip olup olmadığını kontrol etmeli ve gerektiğinde özellikle velayet sorumluluğunu elinde bulunduranlardan ek bilgi sağlamalıdır. b) Çocuğun iç hukuk tarafından yeterli idrak gücüne sahip olduğunun kabul edildiği durumlarda, çocuğun bütün gerekli bilgiyi edindiğinden emin olmalıdır. Çocuğun yüksek çıkarına açıkça ters düşmediği takdirde, gerekirse kendine veya diğer şahıs ve kurumlar vasıtasıyla, çocuk için elverişli durumlarda ve onun kavrayışına uygun bir tarzda çocuğa danışmalıdır. Çocuğun görüşünü ifade etmesine müsaade etmelidir. c) Çocuğun ifade ettiği görüşe gereken önemi vermelidir.”*

Birleşmiş Milletler Çocuk Hakları Sözleşmesi 12. maddesinde ise aşağıdaki hüküm dikkat çekmektedir.

*“Taraf Devletler, görüşlerini oluşturma yeteneğine sahip çocuğun kendini ilgilendiren her konuda görüşlerini serbestçe ifade etme hakkını bu görüşlere çocuğun yaşı ve olgunluk derecesine uygun olarak, gereken özen gösterilmek suretiyle tanırlar. Bu amaçla, çocuğu etkileyen herhangi bir adli veya idari kovuşturmada çocuğun ya doğrudan doğruya veya bir temsilci ya da uygun bir makam yoluyla dinlenilmesi fırsatı, ulusal yasanın usule ilişkin kurallarına uygun olarak çocuğa, özellikle sağlanacaktır.”*

Yukarıda yer alan sözleşme maddeleri incelendiğinde, yeni uygulamanın yürütülmesine yönelik birtakım olumsuzluklar göze çarpmaktadır. İlk olarak, çocuğun bizzat hâkim tarafından duruşma salonunda dinlenmesi gerektiğini bildiren bir hüküm bulunmamaktadır. Hatta Birleşmiş Milletler Çocuk Hakları Sözleşmesi'nin 12. maddesinde çocuğun bir temsilci ya da uygun bir makam yoluyla dinlenebileceği, yüksek çıkarına ters düşmediği sürece, diğer şahıs ve kurumlar aracılığıyla doğrudan kendisine danışılabileceği yer almaktadır. Bu nedenlerle çocuğun dava süreci, velayet, boşanma, kişisel ilişki gibi kavramlar hakkında bilgilendirilmesi, çocuğa kendi görüşünü ifade etme olanağı verilmesi, çocuk hakkında ebeveynlerinden ek bilgi alınması, çocuğun dava süreci hakkında görüşlerinin alınması haklarının, çocuk gelişimi ile ailenin yapısı ve dinamiklerine ilişkin bilgi ve deneyim sahibi olan bir uzman tarafından sunulması daha uygun bir yaklaşım gibi görünmektedir. Bu uzmanların ise, hâlihazırda adli sistem bünyesinde görev yapmakta olan aile mahkemesi uzmanlarının olması gerektiği açıktır. Bu noktada, çocuğun çekişmeli boşanma gibi zorlayıcı davalarda yaşadıkları duyguları açıklamak, bu görevin uzmanlara verilmesinin gerekçelerini daha net ortaya koymaktadır.

Evlilik birlikteliği içerisinde sık çatışma yaşayan çiftler, çatışmalarını büyük ölçüde boşanma sürecinde de sürdürmektedir. Çiftin çocuğu olması durumunda çocuk, hem evlilik birlikteliği hem



de çekişmeli boşanma sürecinde kendisini bu ebeveyn çatışmasının ortasında bulabilmektedir. Böyle bir ortamda çocuk ebeveynlerinin boşanmasından kendini sorumlu hissedebilmekte, ebeveynleri tarafından ebeveyn seçimine zorlanabilmektedirler. Şüphesiz ebeveyn seçimine zorlanmak, çocuğun birlikte yaşamadığı ebeveynine yabancılaşmasına ve boşanma sonrası uyum zorluğu yaşamasına yol açabilecek bir süreçtir. <sup>965</sup> Boşanma sürecindeki çatışmalara maruz kalan çocuklara, ayrıca aile mahkemelerinde velayet konusundaki görüşünün sorulması, duygusal karmaşa içerisindeki çocuğu bambaşka bir olumsuzluğa sürüklemekte, diğer ebeveynine karşı yaşadığı suçluluk duygusunu derinleştirmektedir. Bu konuda bir katılımcı uzmanın gözlemleri dikkate değerdir: *“Çocuklar ön görüşmede adliyede olmaktan dolayı gergin olduklarını söylüyorlar. ... Çünkü ebeveyni yanında soru sormak onları rahatsız ediyor. Günün sonunda tercih etmedikleri ebeveynlerine yabancılaştırıyor.”* (U13). Gerçekten de, ebeveyn tercihinin zorlanmak, somut ve olumsuz bir ebeveyn öyküsü olmamasına ve ebeveyniyle keyifli zaman geçirmesine karşın, çocuğun kısa ya da uzun vadede ebeveyn yabancılaşması duygusu geliştirmesine neden olabilmektedir. Hatta bu yabancılaşma, babaanne, hala ve dede gibi yakınlarla da sıçrayabilmektedir. <sup>966</sup> Bu gibi nedenlerle çocuklar velayet kararı sorumluluğunu tek başlarına yüklenmektense, bu sorumluluğu aile üyeleri ya da kamu görevlileri gibi farklı kişilerle paylaşma eğilimindedirler. <sup>967</sup> Söz konusu duygusal süreci çocuk için kolaylaştırmak, bir diğer deyişle çocuğun ebeveyn ve/veya hâkim gibi figürlerce zor durumda bırakılmadan tercihinin beyan etmesini sağlamak, çocukla önyargısız ve onun gelişim evresine duyarlı bir iletişim stili oluşturabilecek kişilerin görevi olmalıdır <sup>968</sup> ve adalet sisteminde çalışanlar arasında olan aile mahkemesi uzmanları bu görev için bir anlamda biçilmiş kaftanlardır.

---

<sup>965</sup> **Elam, Kit / Sandler, Irwin / Wolchik, Sharlena / Tein, Jein Yun:** Non-Residential Father–Child Involvement, Interparental Conflict and Mental Health of Children Following Divorce: A Person-Focused Approach.” *Journal of Youth and Adolescence*, 2016, 45.3: 581-593. Ayrıca bkz. **Gardner, Richard:** Recent Trends in Divorce And Custody Litigation. *Academy Forum*. 1985, 29,2: 3-7, **Neale, Bren:** Dialogues with Children: Children, Divorce and Citizenship. *Childhood* 2002, 9.4: 455-475, **Neale, Bren / Smart, Carol:** Good to Talk?: Conversations with Children After Divorce.. *Young Voice*, East Molesey 2001, **Öngider Gregory, Nilgün:** Boşanma mı Yoksa Çocuk için Evliliği Sürdürmek mi? Çocuğun Psikolojik Uyumu Açısından Önemli Bir Soru. *Psikiyatride Güncel Yaklaşımlar*, 2016, 8.3: 275-289, **Viry, Gil:** Coparenting and Children’s Adjustment to Divorce: The Role of Geographical Distance from Fathers. *Journal of Divorce & Remarriage* 2014, 55.7, 503-526.

<sup>966</sup> **Baker, Amy / Eichler, Amy:** The Linkage Between Parental Alienation Behaviors And Child Alienation. *Journal of Divorce & Remarriage*, 2016, 57.7: 475-484. Ayrıca bkz. **Gardner,** s.4, **Polat, Oğuz / GÜldoğan, Evin:** Uzman Görüşünün Boşanma Davalarında Velayetin Saptanmasındaki Önemi. *Türkiye Barolar Birliği Dergisi*, 2015, 118: 243-254.

<sup>967</sup> **Eekelaar, John:** “The Interest Of The Child And The Child’s Wishes: The Role Of Dynamic Self-Determinism.” In Alston, Philip (Ed.), *The Best Interests of the Child: Reconciling Culture and Human Rights*, Clarendon Pres, Oxford 1994. Ayrıca bkz. **Gardner,** s. 455.

<sup>968</sup> **Yenisey,** s. 56.

Çocukların aile mahkemelerine yansıyan davalarda dinlenmeleri uygulamasına ilişkin katılımcı önerilerinin yer aldığı üçüncü tema, yukarıda yer alan tartışma konularını destekler niteliktedir. 46 görüşün belirlendiği bu tema altında yeni uygulamanın devam etmesini savunan az oranda görüş (%15.22) dikkat çekmiş, çoğu görüş ise aile mahkemesi uzmanının hazırladığı raporun kararlarda tek başına yeterli olduğu (%43.48) ya da çocukların belirli koşullar sağlandığı takdirde dinlenmelerinin uygun olduğu (%41.30) etrafında toplanmıştır. Belirli koşullar altında uygun fiziksel koşulların sağlanması ile çocukların yaş ve gelişimsel özelliklerinin dikkate alınması gelmektedir. Neale'ın <sup>969</sup> da, bu görüşlere paralel olarak, gelişimsel özellikler doğrultusunda çocukların dinlenip dinlenmemelerine karar verilmesi gerektiğini belirtmesi, bir anlamda katılımcıların da akılcı yönlerini ortaya koymaktadır. Bunlara ek olarak dokuz avukatın, çocukların dinlenmelerinden bağımsız olarak her davada sosyal çevre incelemesini içeren uzman görüş raporunun da olması gerektiğini vurgulamaları, üç uzmanın da çocuk dinleme yaşının 12'ye çekilmesine ilişkin görüş bildirmeleri kayda değer bulgular arasındadır.

Katılımcıların söz konusu olumsuz görüşleri ve bunlara ilişkin çözüm önerileri, Yargıtay içtihatları öncesi uygulamanın tüm taraflar için daha verimli bir süreç olduğunu düşündürmektedir. Katılımcıların bu yaklaşımları aynı zamanda farklı ülkelerdeki uygulamalarla paralellik göstermektedir. Örneğin İtalya'da çocuk velayetini içeren boşanma davalarında anne baba ilk aşamada bu konuya ilişkin zorunlu bir eğitimden geçirilmekte, bu eğitim sonrasında uzlaşma sağlanamadığı takdirde velayet mahkemeye intikal etmektedir. Bu uygulamayla birlikte, boşanma davalarının yalnızca %10'unda çekişmeli velayet olduğu bildirilmektedir. Duruşma sürecinde ise, çocuğun dinlenmesi yerine uzman raporu temel alınmakta ve nihai karar hâkim tarafından bu rapor doğrultusunda alınmaktadır. Dolayısıyla çocukların duruşma ya da mahkeme ortamlarından uzak tutularak örselenmelerinin önüne geçilmekte, aynı zamanda hâkimlerin üzerindeki iş yükü de azaltılmaktadır. <sup>970</sup>

Katılımcıların yeni uygulamaya ilişkin önerilerinden çıkan bir diğer tartışma konusu, "idrak çağı", bir diğer deyişle çocukların sağlıklı bir tercih yapacakları ve bunu uygun bir şekilde ifade edebileceklerine inanılan minimum dinlenme yaşıdır. Her ne kadar 7 takvim yaşını tamamlamış çocukların idrak çağında olduğu kabul edilse de, bu yaşta soyut düşünme becerileri, bireysel, ailesel ve kültürel özelliklerden etkilenebilmektedir. Gelişimsel normlara bakıldığında, soyut düşünmenin

---

969 Neale, s. 456

970 **Ranieri, Sonia / Molgora, Sara / Tamanza, Giancarlo / Emery, Robert:** Promoting Coparenting After Divorce: A Relational Perspective On Child Custody Evaluations in Italy. *Journal of Divorce & Remarriage*, 2016, 57.5: 361-373.

temelleri ilkökul çağında atılmakla birlikte, bu bilişsel sürecin 12-14 yaş döneminde anlamlı bir yetkinliğe ulaştığı görülmektedir. Çoklu değişkenleri içeren durumlarda akıl yürütme, planlama, neden-sonuç ilişkisi kurma ve problem çözme gibi pek çok üst bilişsel becerinin o yaşlarda kazanıldığı düşünülürse, henüz somut düşüncenin baskın olduğu ergenlik öncesi dönemdeki çocukların yeni girdikleri ortamlarda (mahkeme salonunda) tanımadıkları bir kişi (hâkim) karşısında zorlanmaları kaçınılmaz gibi görünmektedir.<sup>971</sup> Bu araştırmada da, katılımcıların, çocukları dinleme yaşının 7 takvim yaşına çekilmesine karşı çıktıkları görülmektedir. Katılımcı avukatlardan biri: *“7 yaş gerçekten uygun değil. Biz ailelere velayeti tam anlatamıyoruz. Geçenlerde bir anne ve babaya 1.5 saat ortak velayeti anlatmaya çalıştım. Bunu 7 yaşında çocuk nasıl anlatsın?”* (A13) sözleriyle, karara karşı olduğunu açıklamıştır. Üç uzman ise, dinlenme yaşının minimum 12 olması gerektiğini bildirerek, gelişim araştırmalarıyla paralel bir görüş ortaya koymuşlardır.

Gerçekten de soyut düşüncenin henüz tam gelişmediği dönemlerde çocukların söylenenleri yanlış ya da farklı algılayabildikleri bilinmektedir. Duruşma ortamı düşünülecek olursa, hâkimin *“Annemi mi seçiyorsun, yoksa babanı mı?”* şeklinde doğrudan sorduğu bir soru, henüz somut işlemler aşamasında olan bir çocuk tarafından *“Annemi mi yoksa babanı mı daha çok seviyorsun?”* olarak algılanabilmektedir. Farklı algılanan bu sorunun yanıtı da çocuğun görüşlerinde anlık değişimlere göre değişkenlik gösterebilmekte, bu da hâkimin kararda tereddüt etmesine neden olabilmektedir. Bu tür çelişkili beyanlarda hâkimler genellikle çocuğu hastaneye sevk etmekte, dolayısıyla da çocuğun dava sürecinde ek duygusal güçlükler yaşaması söz konusu olabilmektedir. Oysa mahkeme uzmanları ya da dosya içeriğine göre görevlendirilen çocuk psikiyatrları gibi alan uzmanları, çocukları velayet hususunda doğrudan dinlemek yerine ilk aşamada çocukla olumlu iletişim geliştirmekte, daha sonra çocuğa uygun görüşme tekniğiyle yaklaşarak çocuğun zarar görmeden dava sürecine katılımını sağlamaya çalışmaktadır.<sup>972</sup> Dolayısıyla aile mahkemesi uzmanlarının hazırlayacakları raporlar eşliğinde hâkimlerle işbirliği yapmalarını içeren bir uygulamanın gerekliliği bir kez daha karşımıza çıkmaktadır.<sup>973</sup>

---

971 **Dumontheil, Iroise**: “Development Of Abstract Thinking During Childhood And Adolescence: The Role Of Rostrolateral Prefrontal Cortex.” *Developmental Cognitive Neuroscience*, 2016, 10: 57-76. Ayrıca bkz. **Uysal-Koğ, Oya / Başer, Neş’e**: Gørselleştirme Yaklaşımının Matematikte Öğrenilmiş Çaresizliğe ve Soyut Düşünmeye Etkisi. *Batı Anadolu Eğitim Bilimleri Dergisi*. 2011, 2.3: 89-108, **Van Oers, Bert**: Meaningful Cultural Learning by Imitative Participation: The Case of Abstract Thinking in Primary School. *Human Development*, 2012, 55.3: 136-158, **Yenisey**, s. 25.

972 **Altındağ, / Sağlam**, s. 430. Ayrıca bkz. **Polat / GÜldoğan**, s. 253.

973 **Altındağ / Sağlam**, s. 432. Ayrıca bkz. **Özel / Tatar**, s. 61.

Bu araştırmanın bulguları genel olarak, Yargıtay içtihatları sonrası getirilen yeni uygulamanın olumsuz getirilerine işaret etmiş ve uygulayıcıların 2017 ve öncesi uygulamayı anımsatan öneriler getirdiklerini ortaya koymuştur. Bu doğrultuda şu sorular akla gelmektedir: Çoğu hâkim, avukat ve aile mahkemesi uzmanının, kendileri ve ilgili diğerleri adına işlevsel olduğunu düşündükleri eski uygulama neden değiştirilmiştir? Aile mahkemelerinde çocuk dinleme yaşı hangi gerekçeyle 7'ye çekilmiştir? Bu araştırma kapsamında, yalnızca İzmir Adliyesi'nde görev yapmakta olan 45 katılımcıdan görüş alınmasına bağlı olarak bu sorular kısmen yanıtlanabilmiştir. Buna karşın, bulguların belirli bir eğilimi yansıtmaya olasılığının yüksek olduğu düşünülmüş ve sonuçların ilgili merciler tarafından dikkate alınması gerektiği sonucuna varılmıştır. Farklı illerde yürütülecek benzer araştırmaların ise, Türkiye'deki çocuk velayeti içerikli aile mahkemesi davalarında neler olduğuna ilişkin daha gerçekçi bir tabloya ulaşılmasını sağlayacaktır.

Çocukların ve ailelerin örselenmelerine ilişkin bu araştırmada elde edilen sonuçlar, ileriki araştırmalara bir konuda daha yol göstermektedir: süreci çocuklar ve ailelerin gözünden görmek. Bu bireyler bir anlamda sistemin müşterileridir ve eğer sistemin amacı onlara hizmet etmekse, sistem onların yüksek çıkarları doğrultusunda işlemelidir. Çocuklar ve ailelerle yürütülecek araştırmaların da, bu konuda yararlı bilgiler sağlamaları söz konusu olacaktır.

Bulgular anımsanacak olursa, dört hâkim AGO uygulamasına gereksinim duyduklarını belirtmişlerdi. AGO uygulaması, çocuğa nispeten daha kolay iletişime geçerek herhangi olumsuz bir etki altında kalmadan görüşlerini bildirebileceği bir ortam sunmakta olup, Türk Adli Sistemi'nde yeni gündeme gelmiş sayılabilecek bir uygulamadır. Hakimlerin AGO'ya yönelik belirttikleri bu gereksinim, AGO'nun etkililiğinin bilimsel bir çerçevede bir an önce incelenerek yaygınlaştırılması gereğini ortaya koymaktadır. Nitekim bu araştırmanın yazarları, şu günlerde söz konusu uygulamanın etkililiğine ilişkin bir çalışma yürütmekte ve bu tür çalışmaların ülke genelinde de yapılmasını önermektedirler.

Yeni uygulama doğrultusunda çekişmeli boşanmalarda, dinlenme yaşının düşürülmesiyle birlikte dava sürecinde dinlenecek çocuk sayısında artış olması kaçınılmaz gibi görünmektedir. Bu artışla birlikte, süreçte daha fazla oranda çocuğun duygusal olarak yıpranması, aynı zamanda katılımcıların da belirttikleri gibi iş yükünde artış söz konusu olacaktır. Dolayısıyla adli sistem içerisinde görev yapanların da mağduriyetinden söz etmek mümkündür. Tüm tarafların olumsuz etkilendiği böyle bir uygulamaya ilişkin katılımcı önerilerinden yola çıkılacak olunursa, uzman görüş raporunun temel alınması, çocuklar hâkim tarafından adliye ortamında dinleneceklerse de, çocuk dinleme yaşının, katılımcıların da önerdiği gibi 12 yaşa çekilmesi, AGO uygulamasının aktif

hale getirilmesi ve çocukların uygun koşullar altında dinlenmesi etkili uygulamaların temel taşıdır. Bunun yanında dava sürecinde başrolü oynayan hâkimlere hizmet içi eğitim olanaklarının sağlanması da, adli sistemin önemli sorumlulukları arasında gibi görünmektedir. Ne var ki, belki de en önemlisi, Türkiye'nin imza attığı uluslararası antlaşmalar doğrultusunda Aile Mahkemeleri bünyesindeki uygulamalarını revize ederek çocuk yaştakiler başta olmak üzere süreçte yer alan tüm vatandaşlarının üstün yararını gözetmesidir.

## KAYNAKÇA

**Altındağ, Özgür / Sağlam, Mehmet:** Boşanma Sürecinde Çocukların Haklarının Belirlenmesi ve Korunmasında Aile Mahkemesi Uzmanlarının Rol ve İşlevleri, Uluslararası Katılımlı Çocuk İhtiyaçları Sempozyumu Bildiri Kitabı, Mutlu Çocuklar Derneği Yayınları, Ankara 2012.

**Ardıç, Oğuzhan:** Medeni Hukuk. Seçkin Yayınevi, Ankara 2008.

**Baker, Amy / Eichler, Amy:** The Linkage Between Parental Alienation Behaviors And Child Alienation. Journal of Divorce & Remarriage, 2016, 57.7. 475-484.

**Buz, Sema / Düzyurt, Kübra/ Sağlam, Mehmet:** Aile Mahkemesinde Çalışan Sosyal Çalışma Görevlilerinin Sosyal İnceleme Raporlarına İlişkin Değerlendirmeleri: Ankara Adliyesi Örneği. Toplum ve Sosyal Hizmet, 2015, 26.2, 7-30.

**Dumontheil, Iroise:** Development of Abstract Thinking During Childhood and Adolescence: The Role of Rostrolateral Prefrontal Cortex. Developmental Cognitive Neuroscience, 2014, 10, 57-76.

**Eekelaar, John:** The Interest of The Child and The Child's Wishes: The Role of Dynamic Self-Determinism. In Alston, Philip (Ed.), The Best Interests Of The Child: Reconciling Culture And Human Rights, Clarendon Pres, Oxford 1994, 129-148.

**Elam, Kit / Sandler, Irwin / Wolchik, Sharlena / Tein, Jein Yun:** Non-Residential Father-Child Involvement, Interparental Conflict and Mental Health of Children Following Divorce: A Person-Focused Approach. Journal of Youth and Adolescence, 2016, 45, 581-593.

**Erbay, Ercüment / Akgül Gök, Fulya / Yüceer Kardeş, Tuba:** Aile Mahkemelerine Başvuran ve Boşanma Sürecinde Olan Ailelerin Problem Çözme Becerilerinin İncelenmesi. Türkiye Sosyal Araştırmalar Dergisi, 2015, 1.1, 139-154.

**Erdem, Mehmet:** Aile Hukuku, Seçkin Yayıncılık, İstanbul 2018.

**Filiz, Orhan:** Türkiye'de Aile Mahkemeleri Uygulaması Ve Uygulamanın Değerlendirilmesi Üzerine Bir Araştırma. *Aile ve Toplum Dergisi*, 2011, 7.25, 73-96.

**Gardner Richard:** Recent Trends in Divorce and Custody Litigation". Academy Forum. 1985, 29, 3-7.

**Günay-İnan, Esra:** Aile Hukukunda Geçici Hukuki Himaye Tedbirleri. Adalet Yayınevi, Ankara 2018.

**Kılıç, Çiğdem:** Aile Mahkemelerinde Görev Yapan Uzmanların Hizmet İçi Eğitim İhtiyacı. Ahi Evran Üniversitesi Kırşehir Eğitim Fakültesi Dergisi, 2013, 14.2, 273-290.

**Meşe, İlknur:** Sosyal Değişim Sürecinde Aile ve Kadın, İn Elmas, Nazım (Ed.), Kadın ve Aile Hayatı, Pegem Yayınları, Ankara 2017, S. 137-161.

**Miles, Matthew / Huberman, Alan Michael:** Qualitative Data Analysis. Sage Pub, Londra 1994.

**Neale, Bren:** Dialogues with Children: Children, Divorce and Citizenship. *Childhood*. 2002, 9.4, 455-475

**Neale, Bren:** “SMART, Carol. *Good to Talk?: Conversations with Children After Divorce*”. Young Voice, East Molesey 2001.

**Öngider Gregory, Nilgün:** Boşanma mı Yoksa Çocuk için Evliliği Sürdürmek mi? Çocuğun Psikolojik Uyumu Açısından Önemli bir Soru”. *Psikiyatride Güncel Yaklaşımlar*, 2016, 8.3, 275-289.

**Özcan, Cem:** Fransız Hukukunda Aile Arabuluculuğu. *Uyuşmazlık Mahkemesi Dergisi*, 2017, 9, 383-396.

**Özel, Çağlar / Tatar, Erol:** Aile Mahkemelerinin Yapısı ve Kararları Üzerine Genel bir Değerlendirme. *Sosyoekonomi*, 2008, 7.7, 49-88.

**Polat, Oğuz / Gündoğan, Evin.** Uzman Görüşünün Boşanma Davalarında Velayetin Saptanmasındaki Önemi. *Türkiye Barolar Birliği Dergisi*, 2015, 118, 243-254.

**Ranieri, Sonia / Molgora, Sara / Tamanza, Giancarlo / Emery, Robert:** Promoting Coparenting After Divorce: A Relational Perspective on Child Custody Evaluations in Italy. *Journal of Divorce & Remarriage*, 2016, 57.5, 361-373.

**Uysal-Koğ, Oya / Başer, Neş'e.** Görselleştirme Yaklaşımının Matematikte Öğrenilmiş Çaresizliğe ve Soyut Düşünmeye Etkisi. *Batı Anadolu Eğitim Bilimleri Dergisi*, 2011, 2.3, 89-108.

**Ünal, Fatma:** Aile Eğitiminde Ebeveyn Hakları ile İlgili Yasalar ve Etik Kurallar, İn Temel, Zeynep Fulya (Ed.), *Aile Eğitimi ve Erken Çocukluk Eğitiminde Aile Katılım Çalışmaları*, Anı Yayıncılık, Ankara 2015, S. 109-155.

**Van Oers, Bert.** Meaningful Cultural Learning by Imitative Participation: The Case of Abstract Thinking in Primary School. *Human Development*, 2012, 55.3, 136-158.

**Viry, Gil:** Coparenting and Children’s Adjustment to Divorce: The Role of Geographical Distance From Fathers. *Journal of Divorce & Remarriage*, 2014, 55.7, 503-526.

**Vorderstrasse, Donna Jo:** A Judicial Perspective on Child Custody Evaluations. In Goldstein, Mark (Ed.), *Handbook of Child Custody*, Springer, London 2016, S. 17-20.

**Yenisey, Feridun:** Mağdur Çocuk Haklarına İlişkin Öneriler. *Uğur Eğitim Pazarlama ve Yayıncılık*, İstanbul 2017.

## CEZA MUHALEMESİNDE BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA (CMK m. 134)<sup>974, 975, 976</sup>

*Prof. Dr. Cumhuri ŞAHİN*

### I. Genel Açıklamalar

Ceza muhakemesinin başlaması, sağlıklı bir biçimde ilerlemesi ve uyuşmazlığın çözümlenebilmesi için delillere ihtiyaç vardır. Delil elde etmenin ceza muhakemesi sürecinde çeşitli yol ve yöntemleri bulunmaktadır. Koruma tedbirlerinin önemli bir kısmı da aynı zamanda birer delil elde etme aracıdır. Teknolojinin toplum hayatında artan biçimde kullanılmasıyla ilişkili olarak, ceza muhakemesinde ispat bakımından sayısal-dijital-elektronik deliller gittikçe önemli hale gelmektedir.

Ceza muhakemesinde kullanılacak olan (elektronik) delillerin bilişim sistemlerinde araştırılması faaliyeti, bir yönü itibariyle, CMK m. 134’de “bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma” olarak ifade edilmektedir (ayrıca bkz. Adli ve Önleme Aramaları Yönetmeliği m. 17). Bu yönüyle hüküm, özel bir arama ve elkoyma düzenlemesidir.

Delil elde etme aracı olmayanlar da dahil olmak üzere, koruma tedbirlerinin uygulanmasıyla, aynı zamanda kişilerin temel hak ve özgürlüklerine müdahale de edilmektedir. CMK madde 134 uygulamasıyla da özel hayatın gizliliği<sup>977</sup>, haberleşmenin gizliliği, kişisel

---

974 Prof. Dr. Cumhuri Şahin, Ankara HBV Üniversitesi Hukuk Fakültesi.

975 ORCID: <https://orcid.org/0000-0002-0612-6486>

976 Bu çalışma Yaşar Üniversitesi Hukuk Fakültesi tarafından 30 Nisan 2019 tarihinde gerçekleştirilmiş bulunan “Ceza Hukuku ve Veri Koruma Boyutuyla Bilişim Hukuku Sempozyumu”nda tebliğ olarak sunulmuştur.

977 AİHM bilgisayarlarda yapılan arama, kopyalama ve elkoyma tedbirleri yoluyla bireyin özel hayatına, kişisel verilerine ve haberleşmesine yönelik müdahaleleri AİHS m. 8’de ifadesini bulan özel hayatın ve aile hayatının korunması bağlamında ele almaktadır. Bu konuda kararlar için bkz. YAŞAR, Yusuf/DURSUN, İsmail, “Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve Elkoyma Koruma Tedbiri”, MÜHFD-HAD, C.19/3, s. 30-32.



verilerin korunması, ticari sırlar, bilimsel sırlar, basın özgürlüğü, ifade özgürlüğü, mülkiyet hakkı<sup>978</sup> gibi çeşitli değerlere ilişilebilmektedir<sup>979</sup>.

Dijital delilin elde edilmesi işi, teknik bir disiplin olarak adli bilişimin konusudur. Sayısal verilerin aranması ve bu verilerden ceza muhakemesinde kullanılmak üzere delil elde edilmesine ilişkin standartlar ve süreçlerden söz edilmekle birlikte, bunlar ülkemizde henüz tamamlanmadığı için sayısal verilere yaklaşım konusunda kurumsal yaklaşım yerine kişiye bağlı yaklaşımların söz konusu olduğu, buna bağlı olarak da verilerin elde edilemediği veya usulüne uygun elde edilmediği söylenmektedir<sup>980</sup>.

Maddede geçen “bilgisayar, bilgisayar programları ve bilgisayar kütükleri” terimleri yerine yaygın olarak “bilişim sistemi” terimi kullanılmaktadır. Bilgisayar kavramı teknolojik gelişmelere bağlı olarak yorumlanmalıdır<sup>981</sup>. Veri depolayan ve işleyen tüm cihazlar bu

---

978 Konunun mülkiyet hakkı bağlamında tartışıldığı da vardır. “Somut olayda başvuru şirketinin bazı evrakı ve bilgisayar kütükleri hakkında, delil olduğu şüphesiyle ceza soruşturması sırasında Sulh Ceza Hakiminin kararma istinaden el koyma tedbiri uygulanmıştır. // Anayasa Mahkemesi daha önce bir suç isnadına bağlı olarak uygulanan el koyma tedbirinin, mülkten geçici süreyle de olsa yoksun bırakma sonucuna yol açtığından dolayı mülkiyet hakkına müdahale teşkil ettiğini kabul etmiştir. Diğer taraftan somut olayda başvuru şirketinin eşyasına bir ceza soruşturması sürecinde maddi gerçeğin ortaya çıkarılabilmesi amacıyla ve delil olduğu şüphesiyle el konulmuştur. Bu durumda müdahalenin belirtilen amacı da gözetildiğinde mülkiyetin kamu yararına kullanımının düzenlenmesine ilişkin üçüncü kural çerçevesinde incelenmesi gerekmektedir. // Anayasanın 13. ve 35. maddelerine göre mülkiyet hakkına yapılan bir müdahalenin Anayasa'ya uygun olabilmesi için, müdahalenin kanuna dayanması, kamu yararı amacı taşıması ve ayrıca ölçülülük ilkesi gözetilerek yapılması gerekmektedir. // Başvuru konusu olayda el koyma tedbirinin 5271 sayılı Kanununun 127. ve 134. maddelerine dayanılarak uygulandığı görülmektedir. Bu hükümlerin öngörülebilir, açık ve ulaşılabilir mahiyette olduğunda tereddüt bulunmamaktadır. Dolayısıyla müdahalenin kanunilik koşulunu taşıdığı anlaşılmaktadır. // Ayrıca bir suç şüphesiyle başlatılan ceza soruşturması sırasında maddi gerçeğin ortaya çıkarılması amacıyla uygulandığı anlaşılan el koyma tedbiri yönünden mülkiyet hakkına yapılan müdahalenin kamu yararına dayalı meşru bir amacının olduğu sonucuna ulaşılmaktadır. // Orantılılık yönünden ise ilk olarak el koyma tedbirinin Sulh Ceza Hakimisi tarafından verildiğine ve başvuru şirketinin ise bu karara karşı etkin bir biçimde itiraz imkanı bulamadığına dair açık bir şikayetin bulunmadığına değinmek gerekir. Bunun yanında el koyma tedbirine yönelik olarak yargısal makamların kararlarının makul bir değerlendirme içermediği veya keyfi olduğu da başvuru şirketinin tarafından ortaya konulamamıştır. // Sonuç olarak bir ceza soruşturması kapsamında maddi gerçeğin ortaya çıkarılabilmesi amacıyla başvuru şirketinin eşyası hakkında el koyma tedbirinin uygulandığı olayda, mülkiyet hakkına yapılan müdahalenin - mevcut aşama itibarıyla - Anayasanın 35. maddesinde öngörülen güvenceler sağlandığından dolayı kamu yararı ile karşılaştırıldığında başvurucuya şahsi olarak aşırı bir külfet yüklenmediği değerlendirilmiştir. Buna göre başvuru şirketinin mülkiyet hakkının korunması ile müdahalenin kamu yararı arasında olması gereken adil denge bozulmamış olup mülkiyet hakkına yapılan müdahale ölçülüdür. Bu durumda başvuru şirketinin mülkiyet hakkının ihlal edilmediği açıktır.” (AYM, Gaye Özel Eğitim İnşaat Bilişim Yemek Dağıtım Tic. A.Ş., B. No: 2015/19961, 26.12.2018, p. 32, 34, 35-37, 40, 42).

979 Bu nedenledir ki, temel hak ve özgürlüklere ağır müdahale sonucu doğuran benzer koruma tedbirlerinde olduğu gibi burada da ölçülülük ilkesine uygun bir suç sınırlaması getirilmesi gerektiği ifade edilmektedir (bkz. YAŞAR/DURSUN, s. 10).

980 DEĞİRMENCİ, s. 454.

981 Dar yorum, maddede sayılmadığı için bu tür cihazlarda veri aramaya genel soruşturma yetkisi veren düzenlemeler (CMK m. 160-161) çerçevesinde başvurulması sonucunu doğuracaktır. Başta özel hayat olmak üzere temel hakların daha etkin korunabilmesi, sorunun m. 134 kapsamında ele alınmasını gerektirmektedir. (Sınırlayıcı hüküm dar yorumlamak burada çözüm değildir. Bu tür hükümlerde dar yorumun amacı temel hak ve özgürlüklere orantısız müdahaleyi engellemektir. Oysa burada dar yorumlarsak asıl o zaman temel haklara ölçüsü müdahaleden söz edilecektir). (Değirmenci)

kapsamdadır. Akıllı telefon (bylock kararları gibi), yazıcı, faks cihazları gibi. Bilgisayar kütüğü teriminden ise, sabit ya da taşınabilir her türlü veri taşıyan ve depolamaya yarayan araçlar anlaşılmalıdır<sup>982</sup>. Yargıtay kararlarında da CMK m. 134 kapsamında; “CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerleri”nden söz edilmektedir<sup>983</sup>.

### III. Tedbirin Uygulanma Şartları

Maddenin uygulanabilmesi bazı şartlara tabi kılınmıştır. Başka surette (suretle) delil elde etme imkanının bulunmaması şartı, 5271 sayılı Kanunun ilk halinde tek şart olarak yer almakta idi. Ayrıca tedbire karar verme yetkisi de sadece hakime aitti.

İlk olarak 21.2.2014 tarihli ve 6526 s. K (m. 11)<sup>984</sup> ile yapılan değişiklikle, “somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı” ayrı bir şart olarak eklenmiştir.

25.7.2018 tarihli ve 7145 s. Kanun ile (m. 16)<sup>985</sup> tedbire karar verme bakımından Cumhuriyet savcısı da yetkili kılınmıştır.

Bahse konu değişikliklerle<sup>986</sup> birlikte, tedbire başvurabilmek için yeni bir şart öngörülmüş, tedbire karar vermeye de iki makam-merci yetkili kılınmıştır.

1) 134. maddenin uygulanabilmesi için, her şeyden önce, kuvvetli suç şüphesinin bulunması gerekmektedir. Kuvvetli şüphe, mahkumiyetin çok yüksek bir ihtimalle gerçekleşeceği durumlarda söz konusu olur. Koruma tedbirlerinin önemli bir kısmında aranan bu şüphenin somut delillere dayanması gerekir<sup>987</sup>.

---

982 **DÜLGER**, s. 549.

983 Yargıtay 16. CD, 21.9.2017, 2015/2056-2017/5023.

984 21.2.2014 tarihli ve 6526 sayılı Kanunun 11 inci maddesiyle, bu maddenin birinci fıkrasında yer alan “soruşturmada,” ibaresinden sonra gelmek üzere “somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve” ibaresi eklenmiş ve dördüncü fıkrasında yer alan “İstemesi halinde, bu” ibaresi “Üçüncü fıkraya göre alınan” şeklinde değiştirilmiştir.

985 **MADDE 16-** 5271 sayılı Kanunun 134 üncü maddesinin birinci fıkrasında yer alan “Cumhuriyet savcısının istemi üzerine” ibaresi “hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından” şeklinde değiştirilmiş, fıkrada yer alan “hâkim tarafından” ibaresi madde metninden çıkarılmış, fıkraya aşağıdaki cümleler eklenmiş ve ikinci fıkrasına “bilgilere ulaşılamaması” ibaresinden sonra gelmek üzere “ya da işlemin uzun sürecek olması” ibaresi eklenmiştir.

“Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.”

986 Maddede yapılan değişiklikler konusunda ayrıntılı bilgi için bkz. **DEĞİRMENCİ, Olgun**: “Bilgisayarlar, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve Elkoyma Koruma Tedbirinde (CMK m. 134) 7145 Sayılı Kanunla Yapılan Değişikliklerin Değerlendirilmesi”, Terazi, Aylık Hukuk Dergisi, Cilt: 13, Sayı: 147, Kasım 2018, s. 146 vd.

987 Burada şüphe sebebi ile kastedilenin delile dayalı bir şüphe sebebi, kısaca delil olduğu tartışmasızdır. Nitekim Anayasa Mahkemesine göre de, “suçlamanın kuvvetli sayılabilecek inandırıcı delillerle desteklenmesi gerekir.

Basit ve herhangi bir olguya dayanmayan şüphe halinde bu tedbire karar verilemez. Başka bir ifadeyle, sadece soyut şüphe yeterli olmamakta, karar verebilmek için, olaylara, somut delillere dayanan, belli bir yoğunluğa ulaşmış şüphe aranmaktadır.

Kuvvetli şüphe, kişinin suçu işlediği hususunda yüksek bir ihtimali gerektirmektedir. Yargılama sonunda sanığın mahkum olması kuvvetle muhtemel ise, kuvvetli suç şüphesinin varlığından söz edilebilir. Bu şüphe, makul şüphenin ötesine geçen, bir suçun işlendiği yönünde çok güçlü işaretler taşıyan bulgulara yönelir.

Kuvvetli şüpheyi, hem şüphelinin soruşturma konusu suçu işlediği yönünde, hem de üzerinde arama yapılacak bilgisayarda suç delillerinin bulunacağı yönünde kuvvetli şüphe olarak anlamak gerekir<sup>988</sup>.

Madde metnine yapılan ekleme ile inceleme konusu koruma tedbirinin uygulanması zorlaştırılmak istenmiştir. Ancak, genel arama ve elkoymada aranan şartın yeterli olması da uygun olabilirdi. Nitekim 2014 yılı değişikliğine kadar, şüphe derecesi bakımından maddede herhangi bir ifade yer almamakta idi.

2) Başka surette delil elde imkanının bulunmaması şartı, bir bakıma bu tedbirin son çare olarak uygulanmasını gerektirmektedir. Başka surette delil elde etme imkanının bulunmaması, mutlaka her zaman önce temel hak ve özgürlüklere daha hafif müdahaleyi gerektiren delil elde etme yöntemlerine başvurulmasını zorunlu kılmaz. Diğer delil elde etme yöntemlerine yönelindiğinde artık hiç delil elde edememe tehlikesinin söz konusu olduğu durumlarda da başka surette delil elde imkanı bulunmayabilir.

Nitekim mevzuatta da, benzer bir şekilde; “*soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu yönetmelikte düzenlenen tedbirlerle ulaşılabilecek olması*” başka surette delil elde edememe olarak tanımlanmıştır<sup>989</sup>.

Bu şartın arandığı tedbirlere konu suçlarda esasen en başından itibaren başka surette delil elde imkanının bulunmamasından söz edilebilir.

---

*İnanırcı delil sayılabilecek olgu ve bilgilerin niteliği büyük ölçüde somut olayın kendine özgü şartlarına bağlıdır*” (AYM, Hikmet Kopar ve diğerleri (GK), B. No: 2014/14061, 8.4.2015, p. 78).

988 **ÖZEN, Muharrem/ÖZOCAK, Gürkan**: “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi”, Ankara Barosu Dergisi, 2015/1, s. 62.

989 Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik, m.4/c.

3) Karar şartı: Tedbire hakim veya gecikmede sakınca halinde Cumhuriyet savcısı karar verir. Cumhuriyet savcının kararı hakim onayına tabidir. Hakim kararına (veya onayına) itiraz edilebilir (CMK m. 267).

Arama ve elkoyma kararı doğrudan CMK 134. madde için olabileceği gibi, 119 ve 127. maddeler uyarınca verilen genel arama-elkoyma kararı üzerine yapılan aramalarda bilgisayarlar da elkonabilir. Elkonulan bilgisayarlar da ayrıca aramaya ihtiyaç duyulmakta ise, inceleme yapabilmek için ayrıca karar gerekir.

Genel arama-elkoyma kararına istinaden yapılan konut-işyeri aramasında oradaki bilgisayar, telefon gibi CMK m. 134'e tabi sistemlerde arama yapılamaz; ya karar baştan bunları da kapsamalı ya da bunlara tesadüf edildiğinde, incelemeye ihtiyaç duyuluyorsa, bunun için ayrıca karar alınmalıdır. Buna karşılık CMK m. 134 uyarınca verilen bir kararla, cihaza ulaşabilmek için ve bulmayı sağlamaya yetecek ölçüde, onun bulunduğu yerlerde de arama yapılabilir<sup>990</sup>.

Uygulamada da bu şekilde hareket edilmektedir:

“Somut olayda ... Cumhuriyet Başsavcılığının yazılı talimatı uyarınca başvuru konutu ve işyerinde yapılan arama sırasında ele geçirilen ve suç delili olabileceği değerlendirilen bilgisayar, tablet, CD ve cep telefonu gibi bazı dijital materyallere el konulmuştur. ... Sulh Ceza Hakimliği 16/7/2016 tarihinde, bu dijital materyaller üzerinde arama yapılmasına -5271 sayılı Kanun'un 134. maddesine göre- izin verilmesine karar vermiştir”<sup>991</sup>.

“Sanık tarafından işletilen iki ayrı işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan hükümlere göre verilmiş bir arama kararı bulunmadığı anlaşılmakla, işyerinde bulunan bilgisayarlar üzerinde yapılan arama sonucunda elkonulan ve içerisinde müşteki firmaya ait lisanssız yazılımların olduğu belirtilen harddiskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağından” (Yargıtay 19. CD, 6.5.2015, 2015/2092-1175).

Aynı değerlendirmeler, hem telefon hem bilgisayar işlevi gören yeni teknoloji (akıllı) cep telefonları bakımından da geçerlidir; salt telefon işlevine yönelik arama-elkoyma işlemi için CMK m. 119, 127 uygulanabilecekken, bilgisayar işlevine yönelik arama-elkoyma CMK m. 134 hükmüne tabidir<sup>992</sup>.

---

990 Kararda bu hususların açıkça belirtilmesi ve konut-işyeri için de geçerli olacak şekilde karar oluşturulması uygun olur.

991 (AYM, *Alpaslan Altan* (GK), B. No: 2016/15586, 11.1.208, p. 89).

992 Ancak günümüzde, gelişen teknoloji ile birlikte, elektronik donanımı düşünüldüğünde birçok cep telefonu bilgisayardan farksız olup, bir bilgisayarla yapılabilecek her şey (İnternet bağlantısı, e-posta haberleşmesi, kelime

“şüpheli üzerine durdurulan sanığın cep telefonunun Cumhuriyet savcısının emri ya da mahkeme kararı olmadan kolluk görevlileri tarafından incelendiği ve telefonda, müştekiye ait çalıntı motosikletin fotoğrafının telefonda K ismiyle kayıtlı bir kişiye gönderildiğinin tespiti üzerine sanık hakkında mahkumiyet kararı verilmiş ise de; işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK'nın 134. maddesi uyarınca hakim kararı alınması gerektiği bu kararın alınmaması sebebiyle arama ve incelemenin yasaya aykırı olduğu ve bu delilin mahkumiyete esas alınmayacağı” (Yargıtay 17. CD, 15.2.2017, 2015/27517-2017/1716).

#### IV. Düzenlemenin Kapsamı ve Uygulama Alanı

134. maddede arama, kopyalama ve elkoyma işlemlerinden söz edilmektedir.

Birinci fıkra genel şartları ve aramayı düzenleyen genel kural olup, elkoymadan söz etmemektedir. Burada ve 5. fıkrada ayrıca kopyalama işlemi düzenlenmektedir. 2. fıkra (ve 3, 4. fıkralar) esasen alıkoymasız elkoymayı, istisnaen de klasik elkoymayı düzenliyor. 5. fıkra 2. fıkrada açıkça zikredilmeyen alıkoymasız elkoymayı tekraren düzenliyor. Doğrusu, 5. fıkrayı 2. fıkranın ilk cümlesi diye okumak lazım. Kural bu olacak, mevcut 2. fıkra da, “Ancak” diye başlayacak ve istisnayı düzenlemiş olacaktır<sup>993</sup>. Fakat 2. fıkra mutlaka bilgisayardaki bütün verilen kopyalanması ve bir imaj alma zorunluluğu getirdiği halde, 1. ve 5. fıkralarda sadece soruşturulan suçla bağlantılı verilerin kopyalanması yeterli olacak, soruşturmaya ilgisi bulunmayan bilgisayardaki tüm verilerin kopyalanması gerekmeyecektir<sup>994</sup>.

işlemci programlarının kullanımı, veri saklanması vb.) yeni teknoloji cep telefonlarıyla da yapılabilmektedir. Ne var ki, bir suç şüphesinin var olduğu durumlarda, bilgisayarlardan farklı olmak üzere, cep telefonlarına kolluk amirinin yazılı emriyle el konulabilmekte ve bu el koyma işlemi esnasında hiçbir şekilde yedekleme vb. önlemlere başvurulmamaktadır. Hiç şüpheli yok ki, uygulamadaki bu sorun, yukarıda bahsettiğimiz temel hak ve özgürlüklere doğrudan zarar verici nitelikte olup, kişilerin kişisel verilerinin ve özel hayatlarının gizliliğine de evrensel hukuka aykırı bir biçimde müdahale anlamına gelmektedir. Cep telefonlarına el konulması ile ilgili olarak, şöyle bir ayırım yapılması doğru olacaktır: i. Eğer cep telefonunda yapılan arama – elkoyma işlemi, cihazın telefon özelliği ile ilgiliyse; örneğin, konuşma veya mesaj kayıtları incelenecekse, bu durumda genel arama hükmü olan CMK m. 119; ii. Yapılan arama – el koyma işlemi, cihazın bilgisayar özelliği ile ilgiliyse; örneğin, arama motoru, trafik kaydı, e-posta kayıtları vb. incelenecekse, bu durumda özel arama hükmü olan CMK m. 134 uygulanmalıdır (**ÖZEN/ÖZAOCAK**, s. 69-70). 993 “134. maddenin 1. fıkrasının metninde açıkça anlaşıldığı üzere bu tedbir kural olarak; şüphelinin kullandığı bilişim sistemlerinde arama yapılması, sistemdeki verilerin kopyasının çıkarılması ve kayıtların çözümünün yapılması haline getirilmesini içermektedir. Yani *kural olan arama tedbiridir*; şüphelinin kullandığı bilişim sistemi olduğu yerde bırakılacak ve kopyalama işlemi sistemin bulunduğu yerde yapılacaktır. Ayrıca kolluk güçleri sistemin ya da veri taşıma aracının aslını almayacaktır. Kural olan budur ve öncelikle bu tedbirlerin uygulanması gerekir. // 134. maddenin 2. fıkrasında ise 1. fıkranın istisnası olarak el koyma tedbiri düzenlenmiştir. 5. Fıkra da ise yukarıdaki düzenlemelerle çelişki yaratan bir fıkraya yer verilmiştir. Çünkü yukarıda belirttiğimiz üzere bilişim sistemlerinden delil elde edilmesinde kural, bilişim sisteminin olduğu yerde arama yapılması ve sistem verilerinin kopyalanmasıdır; el koyma ise istisnadır. Oysa bu fıkradaki düzenlemede sanki el koyma kuralı, bu tedbir uygulanmadan sistemin olduğu yerde kopyasının alınması istisna imiş gibi bir anlam çıkmaktadır. Dolayısıyla bu fıkra gereksiz yere maddede yer alan ve anlam karışıklığına yol açan bir düzenlemedir. (**DÜLGER**, s. 552).

994 YASAR/DURSUN, s. 14.

Arama şüphelinin (ve sanığın) kullandığı bilgisayar, bilgisayar programı ve kütüklerinde yapılabilir. Kullanılan bilgisayar suç şüphesi altında olmayan kişilere ait olsa da (CMK m. 117) arama yapılması mümkündür. Keza, maddede açıkça ifade edilmemekle birlikte, mağdura karşı işlenen suçlarla sınırlı olmak üzere, onun bilgisayarında bulunan delillere ulaşabilmek için mağdurun bilgisayarında da arama yapılabilirdir. Ancak bu son durum CMK m. 134 kapsamında değerlendirilecek bir husus değildir.

İkinci fıkrada yer alan istisna hükmünün kural gibi yaygın bir biçimde kullanıldığı ifade edilmektedir. Kanun, bilgisayarları ve bilgisayar kütüklerini bulunduğu yerden alıp götürmeksizin delile ulaşmanın mümkün olması halinde, sistemdeki verilerin kopyasının alınmasını öngörmektedir (CMK m. 134/2, 5). Bu durumda, tamamen veya kısmen kopyası alınan veriler kağıda yazdırılarak<sup>995</sup>, bu husus tutanağa kaydedilecek ve ilgililer tarafından imza altına alınacaktır.

Buna karşılık; bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşamaması ya da işlemin uzun süreceği olması<sup>996</sup> halinde ise, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir (CMK m. 134/2).

Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklenmesi yapılır. Şüphelinin veya vekilinin herhangi bir talebi olmasa dahi alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır (CMK m. 134/3, 4). Yedeğin bir kopyasının savunma makamına verilmesinin zorunlu kılınması suretiyle, alınan yedek üzerinde sonradan müdahalede bulunulduğu iddiası önlenmek istenmektedir.

Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir (CMK m. 134/2).

Kanundan farklı olarak Yönetmelikte, yedekleme işleminin; “bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanacağı (17/3) belirtilmiştir. Kanunda ismi geçmeyen bazı cihazların Yönetmelikte zikredilmesinin, hükmün açıklığa

---

995 “Hükmün 5. Fıkrasındaki “kopyalanan verilerin kağıda dökülmesi” gibi uygulanması hem gereksiz, hem de bazen maddi olarak imkansız (tele baytlarca verinin kağıda dökülmesi gibi) kuralların yapılacak yeni düzenlemede yer almaması gerekmektedir” (ÖZEN/ÖZOCAK, s. 70).

996 25.7.2018 tarihli ve 7145 sayılı Kanunla (m. 16) işlemin uzun süreceği olması da bilgisayara elkoyma sebepleri arasında sayılmıştır. Bu husus ilk olarak olağanüstü hal döneminde kabul edilen 668 sayılı KHK’da (m. 3) yer almaktaydı.

kavuşturulması mı yoksa kapsamının genişletilmesi mi olduğu hususu tartışılabilir. Bize göre burada bir genişletme yoktur. 134. madde kapsamına hangi cihazların girdiği ve teknolojik gelişmelere bağlı olarak ilerde gireceği, normun amacına bakılarak belirlenecektir. Ayrıca bunların her birinin tek tek Yönetmelikte zikredilmesi de gerekmez. Nitekim yeni teknoloji (akıllı) telefonlar da mevzuatta bir yerde zikredilmemektedir.

Maddede sadece “soruşturma”, “hakim”, “Cumhuriyet savcısı” ve “şüpheli” den söz edilmekte, buna karşılık; “kovuşturma”, “mahkeme” ve “sanık” kavramlarına yer verilmemektedir. Bu durum, bu koruma tedbirine sadece soruşturma evresinde başvurulabileceği izlenimini doğurmaktadır. Bu bakımdan aslında ceza muhakemesi sistemi ile çelişmemektedir. Çünkü CMK delillerin asıl olarak soruşturma evresinde toplanmasını öngörmektedir. Bununla birlikte, yargılama sırasında delil toplanmasını engelleyen bir hüküm bulunmadığından, hatta mahkeme re’sen araştırma yetkisine sahip olduğundan, kovuşturma evresinde de bu tedbire başvurulabilmesi mümkün olmalıdır.

Aramada hazır bulunabileceklerle ilgili olarak CMK. m.134’te açık bir hüküm bulunmamaktadır. 134/4’de zikredilen şüphelinin “vekili” bir hukukçu değil onu temsil eden esasen aileden birisidir. Müdafinin durumu da dahil olmak üzere, hazır bulunma konusunda genel aramaya ilişkin CMK m. 120 uygulanabilir.

Bilgisayarlarda arama avukat bürosunda yapılmakta ise, arama ve elkoyma 130. maddede düzenlenmektedir.

Arama sonunda verilecek belgeye ilişkin olarak da, genel aramaya ilişkin 121. madde hükümleri uygulanmalıdır. Kopyalamada da, kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve tutanağın bir sureti de ilgiliye verilir<sup>997</sup>.

Arama sırasında başka bir suça ilişkin delile tesadüf edilmesi halinde CMK m. 138/1 hükmü uygulama alanı bulacaktır.

Elkonulan “eşyanın” iadesine ilişkin CMK m. 131 madde de uygulama alanı bulur.

Müsadere konusuna madde dolaylı olarak temas etmektedir. Asıl olan, cihaza elkoymaksızın delil elde edilmesi gerekmekte (CMK m. 134/1, 2, 5), elkonulduktan sonra da gerekli kopyaların alınması üzerine bilgisayarın gecikmeksizin iade edilmesidir (CMK m. 134/2; KHK 668/3-1-j). Zira burada elkoyma bakımından önemli olan eşyalara elkonulması değil verilere elkonulmasıdır. Ayrıca, her koruma tedbiri gibi bu da geçicidir.

---

997 Adli ve Önleme Aramaları Yönetmeliği m.17/5.

Ancak müsaderecinin gerekli olduğu durumlar da olabilir<sup>998</sup>. Bu durumda da, TCK m. 54/5’de yer alan “Bir şeyin sadece bazı kısımlarının müsadereci gerektiğinde, tümüne zarar verilmeksizin bu kısmı ayırmak olanaklı ise, sadece bu kısmın müsadereci karar verilir” hükmü uyarınca sadece harddiskinin müsadereci söz konusu olur. Harddiskinin müsadereci yapılırken de, harddisk içindeki örneğin kitap, makale ... gibi suç oluşturmeyen bilgilerin kopyasının kendisine geri verilmesi gerekir.

Koruma tedbirleri nedeniyle tazminat bakımından CMK m. 141/1-i ve j bentleri uygulama alanı bulabilir<sup>999</sup>.

## V. Tedbirin Uygulanması

Elkoyma tedbirinin uygulanması için, arama ve kopyalama kararına ihtiyaç vardır. Zira araçlar aranmadan, içindeki verilerin tespit edilebilmesi mümkün değildir. Bu itibarla tedbirin konusunu oluşturan araçlarda veri araması yapılmadan elkoyma işlemi yapılması hukuka aykırı olur<sup>1000</sup>.

Arama ve kopyalama işleminin yapılabilmesi için cihazların bulunduğu yerden başka bir yere götürülmesine gerek yoktur<sup>1001</sup>. Kişinin konutunda ya da işyerinde fiziki olarak bulunan bu araçlar içerisinde, cihazın bulunduğu yerde arama yapılabilir (CMK m. 134/1, 5).

---

998 “Örneğin; TCK m. 226’da düzenlenen Müstehcenlik suçunda çocuk pornografisi içeren görüntülerin yahut TCK m. 245 uyarınca yapılan bir aramada ele geçirilen mağdurun kredi kart bilgilerinin el konulan hard diskin içinde bulunduğu durumlarda, bu cihazların kopyalama sonrası şüpheliye iade edilmesi, suçun işlenmesine devam edilmesine kanun tarafından cevaz verilmesi anlamına gelecektir. Bu gibi durumlarda TCK m. 54 uyarınca eşya müsadereci gündeme gelebilecekse de, CMK m. 134’ün bu ayrıksı durumlara ilişkin bir düzenleme öngörmemiş olması kanımızca önemli bir eksikliktir” (ÖZEN/ÖZOCAK, s. 70). **Doktrinde**, bilgisayar programlarında ve kütüklerinde yer alan kayıtların bir kopyasının şüpheliye veya vekiline verilmesi halinde konusu suç oluşturan veya suç işlemede araç olarak kullanılabilecek veriler üzerinde şüpheliye yeniden tasarruf etme hakkı ortaya çıkacağı belirtilerek, bu sorunu çözmek amacıyla; ilerde müsadereciye tabi olabilecek eşya olması gerekçesiyle, bu araç ve gereçler üzerinde CMK m. 123 ve devam hükümlerine göre elkoyma kararı verilmesi önerilmektedir (bkz. ÜNVER, Yener/HAKERİ, Hakan: Ceza Muhakemesi Hukuku, 14. Baskı, Ankara 2018, s. 411). **Uygulamanın** da bu yönde olduğu, ancak bu konuda bir ayırım yapılarak; imajın yedeğinin şüpheliye verilmemesi, buna karşılık müdafiyeye verilebileceği yönünde bkz. DÜLGER, s. 550.

999 CMK m. 141/1-i ve j bentlerinde göre: Hakkındaki arama kararı ölçüsüz bir şekilde gerçekleştirilen; eşyasına veya diğer malvarlığı değerlerine, koşulları oluşmadığı halde elkonulan veya korunması için gerekli tedbirler alınmayan ya da eşyası veya diğer malvarlığı değerleri amaç dışı kullanılan veya zamanında geri verilmeyen kişiler, maddi ve manevi manevi her türlü zararlarını talep edebilirler.

1000 Bununla birlikte, m. 116 ve 123’deki genel arama ve elkoymanın aksine, m. 134’de, önce verilere elkoyma sonra elkonulan veriler üzerinde arama (delil elde etme) işlemi gerçekleştirildiği yönünde bkz. DEĞİRMENCİ, **Olgun**: Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara 2014, s. 455.

1001 Bazı yazarlar, genel kanaatin aksine; bilgisayarlara ... elkonulmasını, şifrenin çözülememesi, gizlenmiş bilgilere ulaşılamaması, incelemenin uzun süreceği olması gibi şartlarla sınırlayan hükmün teknik olarak hatalı olduğunu, zira bilgisayarda yerinde inceleme yapılması çoğu kez mümkün olmadığını, tedbirin doğru uygulanışının, delilleri koruyucu ve şüphelinin mağduriyetini önleyici tüm önlemler alınarak, bilgisayara el konulması ve teknik uzmanlar tarafından laboratuvar ortamında incelenmesi olduğunu belirtmektedirler (ÖZEN/ÖZOCAK, s. 63).



Aramanın konusu “elektronik veri” olup, elektronik verinin araştırılması ya da sorgulanması, bilişim sisteminin içerisinde yer alan verilen taranması suretiyle, elektronik ortamda gerçekleştirilir<sup>1002</sup>.

Arama işleminde amaç, suçla bağlantılı her türlü elektronik veriye ulaşmaktır. Bu kapsamda, bilgisayarda mevcut klasörlerdeki dokümanların tamamı aranabilir.

CMK Tasarısının m. 134 gerekçesinde de ifade edildiği gibi, bu madde uyarınca arama geçmişe dönük olarak, statik haldeki veriler üzerinde gerçekleştirilir. Bu nedenle, bilgisayarda, şüpheli veya sanığın -internet ortamında çeşitli programlar ya da sosyal iletişim siteleri (Msn Messenger, Facebook, Twitter, vb.) vasıtasıyla-gerçekleştirdiği iletişime ilişkin kayıtların aranması, CMK. m. 134’ göre yapılabilir. Zira internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından, bu iletişim kayıtları hakkında arama, kopyalama ve elkoyma tedbirleri uygulanabilir. Buna karşılık internet ortamında gerçekleştirilen konuşmaların teknik araçlarla dinlenilmesi, kayda alınması, CMK. m.134’e göre değil, CMK. m.135’e göre gerçekleştirilecektir. Zira CMK. m.135’e göre yapılan iletişimin dinlenmesi ve kaydı geçmişe dönük olarak değil, geleceğe dönük olarak yapılabilir.

Elkoymada yedekleme işlemi yapılmalıdır (CMK m. 134/2). Savunmanın da hazır bulundurulacağı bir ortamda gerçekleştirilmesi gereken yedekleme işlemi, elkoyma öncesinde veya sırasında yapılmalıdır<sup>1003</sup>.

Yedekleme işlemi için, kolluk veya diğer uzman tarafından hedef sistemin kullanıcısının bulunduğu yerdeki tüm bilişim sistemlerinin üçüncü kişilerin kullanımına kapatılması gerekmektedir.

Bilişim sistemlerinden bilgisayarların hard disk (depolama birimleri) bağımsız olarak veya ek modüllerle çalışan bir imaj alma cihazı ile imajlarının alınması ve alınan hash değeri<sup>1004</sup> ile digital mühür yapılmak suretiyle imaj almadan sonra söz konusu sisteme veri yerleştirmenin veya müdahalenin yapılmaması garanti altına alınır.

Mobil cihazlar için yukarıda bahsedilen yöntemle imajlarının alınması gerekmektedir. Ancak mobil cihazlardaki güvenlik önlemleri nedeniyle özellikle telefon açılış şifrelerinin elde

---

1002 Bkz. YAŞAR/DURSUN, s. 23.

1003 Yedekleme işleminin savunma nezdinde yapılacak olması başta işi uzatıyor gibi gözükse de, aslında muhakemenin makul sürede bitmesini sağlayan önemli hususlardan birisidir birçok durumda. Zira bilahare delillerin güvenilirliğine yönelik itirazlar ve bunun üzerine yapılan incelemeler işi daha fazla uzatmaktadır.

1004 Hash (özet) değeri: Dosyaların parmak izi de denilen ve dosya üzerinde en küçük bir değişiklik yapıldığında baştan sona değişen, dolayısıyla yedeklenen verilerin bütünlüğünü teminat almaya yarayan sayısal değerler. Ayrıntı için bkz. DEĞİRMENCİ, s.248 vd.

edilmemesi nedeniyle de bu cihazların imajlarının alınmasında zorlukların yaşanmasına neden olmaktadır.

Sistem kapalı iken imaj alınması önemlidir; çünkü çalışan sistem üzerinde yapılan işlemlerin delil güvenliğini tehlikeye sokma ihtimali vardır. Eğer kapalı bir şekilde imaj alınırsa hem şüphelinin hakları korunmuş olur hem de veri güvenliği sağlanmış, veri manipülasyonunun önüne geçilmiş olur.

İmajlar çeşitli foresing yazılımları kullanılmak suretiyle incelenir. Bu yazılımlardan bazıları ile imajı alınan sistem üzerinde silinen verilere ilişkin bilgilere de erişilmesi mümkündür. “Mevzuatta *imaj almadan* ya da *hash değerinden* bahsedilmemekte, bunun yerine *yedek alma* ve *kopyalama* terimleri kullanılmaktadır. Oysa bir veri taşıma aracının yedeğinin ya da kopyasının alınması ile imajının alınması ve bunun sonucunda hash değerinin elde edilmesi çok farklı işlemlerdir. Yedekleme ve kopyalamada, boş sektörler kopyalanmadığı gibi, veri bütünlüğü ve güvenliği de sağlanamaz. Bu ise dijital verilerin *güvenilir delil* olma özelliğini ortadan kaldırır. Uygulamada ise soruşturma görevlileri *tamamen kendi iyi niyetleri ve görevi düzgün yapma istekleriyle*, bu alandaki uluslararası standartları takip ederek her soruşturmada imaj ve hash değerini almaktadırlar”<sup>1005</sup>.

## VI. Tedbirin Uygulanması Sürecinde Ceza Hukuku Sorumluluğu Gerektiren Haller

Cumhuriyet savcısı tarafından verilen kararın süresinde hakim onayına sunulmaması ya da hakim tarafından onaylanmaması halinde, CMK m. 134’e göre yapılan incelemelerin tamamının imha edilmesi gerekmekte olup, aksi durumda Türk Ceza Kanununun 138. maddesindeki verileri yok etmeme suçu meydana gelecektir.

Bu tarama işlemi sırasında, arama konusu suçla bağlantısı olmayıp, şüpheli veya sanığın özel hayatına ilişkin verilerin bilerek ve istenerek açılması durumunda, kanun hükmünün yerine getirilmesi hukuka uygunluk sebebinde sınır kasten aşılmış olacağından, TCK. m. 134’te düzenlenen özel hayatın gizliliğini ihlal suçu gündeme gelebilecektir. Diğer taraftan, tarama işlemi sırasında, gerekli araştırma yapılmadan, suçla bağlantılı olduğu düşünülen ve fakat şüpheli veya sanığın özel hayatına ilişkin dokümanların açılması durumunda, sınır taksirle aşılmış olacağından ve TCK. m.134’teki suç yalnızca kasten işlenebileceğinden, özel hayatın gizliliğini ihlal suçu oluşmaz (TCK. m. 27)<sup>1006</sup>.

---

1005 DÜLGER, s. 552.

1006 YAŞAR/DURSUN, s. 23.

Suçla bağlantılı olarak kopyalanan verilerle birlikte, suçla bağlantısı olmayan ve şüpheli veya sanığın kişisel verilerinin kopyalanması durumunda TCK. m. 135’de düzenlenen kişisel verilerin kaydedilmesi suçu gündeme gelebilir.

Bilgisayarda arama, fiziki olarak bilgisayardaki verilerin aranması suretiyle gerçekleştirilebilir. Uzaktan erişim yoluyla bilgisayardaki verilere ulaşılması, hukuka aykırıdır (TCK m. 134, 136).

İmaj alınıp sureti savunmaya verilmeden gerçekleştirilen elkoyma sonrasında ise her türlü sahte delil üretme ihtimali gündeme gelebilir.

## VII. Dijital Delillerin Hukukiliği Sorunu

CMK m. 134’de öngörülen tedbire başvurulmak suretiyle elde edilen delillerin ispat hukuku bakımından ayrıca üzerinde durulması gerekir.

Her şeyden önce, hukuki nitelikleri itibariyle belirti (belge!) delili olarak kabul edilebilecek olan sayısal deliller, çoğunlukla dolaylı delil niteliğindedirler. Dolaylı delil oluşu nedeniyle, fiil ile fail arasında bağa doğrudan işaret etmezler; 134. maddede öngörülen şartlara ve usule uygun elde edildiklerinde dahi başka delillerle desteklenmeye muhtaçtırlar.

Bununla birlikte, 134. maddede öngörülen şartlara ve usule uyulmaksızın elde edilen sayısal delillerin değerlendirilebilir olup olmadığı ve değerlendirilebilecekse ispat gücü konularında değişik tespitler yapılabilir.

Sayısal deliller tahrife açıktırlar. Yüksek mahkemelerin kararlarında da bu konular tartışılmıştır<sup>1007</sup>. Ancak, bu şekilde elde edilen delillerin muhakemede hiçbir durumda

---

1007 “Kural olarak, bilirkişilerin sunduğu rapor ve mütalaalar derece mahkemeleri açısından bağlayıcı olmamakla birlikte, İlk Derece Mahkemesi tarafından esasa ilişkin değerlendirmeler yapılırken Cumhuriyet Savcısı tarafından sunulan bilirkişi raporlarının belirleyici bir etkisi olmuştur. Başka bir deyişle somut davada İlk Derece Mahkemesi, yalnızca Cumhuriyet Savcısı tarafından sunulan bilirkişi raporlarına itibar etmiş, bu raporlara karşın başvuruca savunmalarının bir parçası olarak sundukları bilirkişi rapor ve uzman görüşleri ise dikkate alınmamıştır. Mahkeme ayrıca başvuruca mahkumiyet kararının dayanağı olan dijital verilerin gerçeği yansıtmadığı iddialarını değerlendirmek üzere mahkemenin bilirkişi heyeti tayin etmesi ve rapor aldırması yönündeki taleplerini de yeterli olmayan gerekçe ile reddetmiştir. // Sanıklara isnat edilen suç fiillerinin esaslı biçimde bilgisayar programlarıyla oluşturulmuş belgelere dayandığı, bu belgelerin içeriklerinin maddi olay ve olguları yansıttığı ve gerçek olduklarının kabul edildiği, **bilirkişi raporlarında/uzman görüşlerinde belirtildiği üzere bu verilerin müdahale edilebilir nitelikte olduğu ve bu verilerin teknik bilgileri ile içeriklerinin uyumsuzluğu** dikkate alındığında, tanık olarak dinlenmesi talep edilen bu kişilerin beyanları maddi gerçeğe ulaşma bakımından önemsiz kabul edilemez” (AYM, *Sencer Başat vd.*, 2013/7800, 2013/7800, 18/6/2014, p. 70, 85); “**CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden** elde edilen ve tamamı "dijital delil" olarak adlandırılan, suistimale müsait olan verilerin; ... . **Dijital delillere harici müdahalenin teknik olarak mümkün olması, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi** karşısında ... (Yargıtay 16. CD, 21.9.2017, 2015/2056-2017/5023).

kullanılmayacağı görüşünü<sup>1008</sup> isabetli bulmamaktayız. Bu şekilde elde edilen delillerin güvenilirliği ayrı bir sorun olup, bu her zaman bir değerlendirme yasağı sonucu doğurmaz.

Anayasa mahkemesi, dijital delillere elkonulurken verilerin yedeklenmemesi ve imajlarının alınmaması nedenleriyle hukuka aykırılık ve özel hayata saygı hakkının ihlali iddiaları karşısında; esasen bir delilin geçerli-hukuka uygun olup olmadığı konusunda bir değerlendirmede bulunmamaktadır, zira delilleri değerlendirme yetkisi kural olarak yargılamayı yapan mahkemeye aittir. Bununla birlikte, kanuna-hukuka aykırı şekilde elde edilen delilin tek ve(ya) belirleyici delil olarak yargılamada kullanılması ve bu delile göre karar verilmesi halinde, bir bütün olarak yargılamanın hakkaniyetinin zedeleneceğini belirtmektedir<sup>1009</sup>.

Karar olmaksızın 134 uygulaması durumunda kesin bir değerlendirme yasağı vardır. Nitekim yukarıda yer verilen Yargıtay kararlarında da bu husus vurgulanmaktadır<sup>1010</sup>.

Fıkradaki zorunluluk oluşmadan, zorunluluğun gerekçeleri ortaya konmadan, mahalde veya kolluk biriminde savunma huzurunda imaj alınmadan elde edilen deliller; uygulamaya ve/veya delillerin sıhhatine yönelik itiraz halinde değerlendirme yasağıyla karşılaşılır.

Buna karşılık, mahalde yedekleme ve yedekten kopya verme olanağının bulunmadığının objektif olarak kabulünde zorunluluk bulunan hallerde, aramayı yapan kolluk birimince dijital

---

1008 “Bu fıkra çok açık biçimde bir istisnayı düzenlemesine rağmen, ülkemiz mevzuatında yer alan pek çok istisna hükmünün uygulamada kural haline getirilmesinde olduğu gibi, bilişim sistemlerinde yapılan aramalarda da bu istisna, kural haline getirilmiştir. Kolluk güçleri CMK'nın 134. maddesine göre yaptıkları aramaların tamamında 2. fıkradaki istisna hükmünü işletmekte, bunun için arama yapacakları bilişim sisteminde şifre olduğuna ilişkin işleme katılan diğer kolluk güçleriyle birlikte bir tutanak tutmakta ve böylelikle yasaı dolanmak suretiyle görünüşte de olsa yasa ya uygun davrandıkları düşüncesiyle görevlerini yerine getirmektedirler. Bunun gerekçesi olarak ise “*yeterli personellerinin olmadığını, eğer sistemin olduğu yerde arama ve kopyalama yapmaya kalkarlarsa hiçbir işi yetiştirmeyeceklerini*” beyan etmektedirler. Aslında içinde büyük oranda gerçeklik payı olan bu bahane yasa maddesini değiştirme hakkını vermediği gibi bu şekilde elde edilen delili de hukuka uygun hale getirmemektedir. **Zira tutulan tutanaklarda ne tür bir şifrenin ya da gizli verinin bulunduğu, bunun işin uzmanı olan bilişim polisi tarafından neden etkisiz kılınmadığına ilişkin herhangi bir kayıt bu tutanaklarda yer almamaktadır. Dolayısıyla bu tutanağın gerçekte bir ilgisi ve denetlenebilir bir tarafı olmadığı gibi, hukuken hiçbir değeri de bulunmamaktadır.** Bu işlem açıkça yasanın arkasına dolanmaktadır ve hukuka aykırıdır. Söz konusu işlemin yapıldığı şekli hukuka aykırı bir delil elde etme yöntemi olduğu gibi bu yolla elde edilen deliller de yasak delil niteliğindedir ve yargılamanın hiçbir aşamasında kullanılmamaları gerekir” (DÜLGER, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, tamamen güncellenmiş 7. Baskı, Ankara 2018, s. 550).

1009 AYM, *Bilgin Özkaynak*, B. No: 2014/3129, 27.10.2016, p. 35-37. Kararın karşıoy gerekçesinde ise; “... Başvurucunun çiftlik evinde yapılan aramada ele geçirildiği ve el konduğu belirtilen “Pandora” adlı veri tabanyla ilgili olarak emniyet birimlerinde yedeklemesi yapılmamış, sanığa (başvurucuya) ve müdafisine bunun bir kopyası verilmemiş ve bilahare emniyetçe şifresinin kırılarak içeriğine ulaşıldığı belirtilerek, yine emniyetçe tek taraflı olarak Savcılığa ibraz edilen içerik bilgileri esas alınarak sanık hakkında dava açılmış ve tutuklanmıştır. ... CMK'nun bu emredici açık hükmüne (CMK m. 134) rağmen başvurucunun çitliğinde ele geçirildiği söylenen Pandora isimli bilgisayar veri tabanının yedeklenmesi yapılmadan ve bir kopyası kendisine ve müdafisine verilmeden elde edilen verilerin, Anayasanın 38 nci maddesindeki “Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez” hükmü karşısında “kanunsuz delil” mahiyetinde olduğu açık olup; bu “delil” e dayalı bir tutuklama da, verildiği andan itibaren hukuka aykırıdır.”

1010 Yargıtay 17. CD, 15.2.2017, 2015/27517-2017/1716; Yargıtay 19. CD, 6.5.2015, 2015/2092-1175.

delillere müdahaleyi önleyecek şekilde, seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak zapt edilip mühürlenerek, şüpheli veya müdafinin istemesi halinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmak ve bu yerde şüpheli veya müdafinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, dijital medyanın derhal imajının alınarak ilgisine de imajlardan bir kopya ve orijinal medya teslim edilerek, yine sanık veya müdafinin mühür açma işlemi sırasında hazır bulunmasının mümkün olmadığı hallerde, mühür açma işleminin arama ve el koyma kararını veren (veya onaylayan) hakimin huzurunda açılarak imaj alma işleminin bu sırada yapılması yoluna gidilerek inceleme yapılması halinde 134/2 ye ve hukuka uygun bir süreç izlenmiştir.

“Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma 5271 Sayılı CMK'nın 134. maddesinde düzenlenmiş olup, CMK'nın 116 ve 123. maddeleri arasında yer alan arama koruma tedbirinin özel bir görünümünü oluşturmaktadır. CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen ve tamamı "dijital delil" olarak adlandırılan, suistimale müsait olan verilerin; sıhhatini ve güvenliğini sağlamak amacıyla ve bireyin özel hayatına, kişisel verilerine yönelik olumsuz tesirleri göz önünde tutularak “son çare” olarak başvurulabilecek “özel koşullara bağlı” bir koruma tedbiri olması nedeniyle, genel adli aramadan ayrık ve istisnai olarak, ayrıntılı düzenlenmiş olup, bu hallerde arama kararının yalnızca hakim tarafından verilebileceği öngörülmüştür. Ceza muhakemesinde deliller kanuna uygun olmalı ve kanuna uygun yöntemlerle elde edilmelidir. Adil yargılanmanın sağlanabilmesi, soruşturma ve kovuşturma aşamalarında toplanan bulguların delil değeri taşıyabilmesi için, şüpheli veya sanıktan elde edilen dijital verilerin, kanun ile sınırları belirlenmiş teknik gerekliliklere uygun olarak toplanması ve sonucunda yargılama makamlarına eksiksiz, bozulmamış halde sunulması gerekmektedir. Kanun koyucunun, CMK'nın 134. maddesini ayrıntılı olarak düzenlemesinin amacı da budur. Dijital delillere harici müdahalenin teknik olarak mümkün olması, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında, güvenli bir şekilde el konulup incelenebilmesi için mahallinde imaj alındıktan sonra orijinal medyanın şüpheliye bırakılması gerekmekte ise de bu şart soruşturma yapan kolluk personelinin teknik yetersizliği, ekipman yokluğu, ortamın incelemeye elverişli olmaması gibi sebeplerle yerine getirilememektedir.

Bu itibarla arama ve elkoymanın özel bir hali olarak CMK'nın 134. maddesinde düzenlenen ve özel hayatın gizliliğine daha fazla müdahale içermesi sebebiyle kanun koyucu tarafından genel arama ve elkoymadan daha sıkı koşullara tabi tutulan bilgisayarlarda, bilgisayar programlarında ve

kütüklerinde arama ve elkoymanın bu özelliği gözardı edilmek suretiyle, aramayı gerçekleştiren kişilerce elkoyma işlemine geçildiği sırada sistemdeki verilerin yedeklemesi (imaj-adli kopya) yapılmadan ve yedekten bir kopya alınıp şüpheli veya vekiline verilmeden, ya da yukarıda yazılı nedenlerden dolayı mahalde yedekleme ve yedekten kopya verme olanağının bulunmadığının objektif olarak kabulünde zorunluluk bulunan hallerde, aramayı yapan kolluk birimince dijital delillere müdahaleyi önleyecek şekilde, seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak zapt edilip mühürlenmeden, şüpheli veya müdafinin istemesi halinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmadan ve bu yerde şüpheli veya müdafinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, dijital medyanın derhal imajının alınarak ilgisine de imajlardan bir kopya ve orijinal medya teslim edilmeden, yine sanık veya müdafinin mühür açma işlemi sırasında hazır bulunmasının mümkün olmadığı hallerde, mühür açma işleminin arama ve el koyma kararını veren hakim huzurunda açılarak imaj alma işleminin bu sırada yapılması yoluna gidilmeden inceleme yapılması halinde arama ve elkoyma işleminin kanuna ve hukuka uygunluğundan bahsetmek mümkün olmadığı gibi bu yolla elde edilen delillerin de hukuka uygunluğu tartışılır hale gelecek ve yargılama makamınca hükme esas alınması mümkün olmayacaktır. Bu bakımdan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma yapılabilmesine dair CMK'nın 134. maddesi uyarınca açık bir ibare bulunmadığı halde, sanıkların ev veya iş yerlerinde yapılan aramalarda hard disk, bilgisayar kasası, CD ve DVD gibi dijital medyalara, arama mahallinde imaj alınmadan, ilgisine bir kopyası verilmeden ve kanuna uygun gerekçesi de tutanağa yazılmadan el konulması ve bu şekilde elde edilen delillerin sanık bakımından hükme esas alınmasının CMK'nın 134. maddesine aykırı olduğu ...<sup>1011</sup>.

---

1011 Yargıtay 16. CD, 21.9.2017, 2015/2056-2017/5023. Doktrinde de benzer değerlendirmeler yapılmaktadır: “Yedek alma işleminin kolluk görevlilerinin kendi çalıştıkları merkezlerde ve ayrıca şüpheli ve/veya müdafinin olmadığı ortamda yapılması, soruşturmanın güvenilirliği, tarafsızlığı ve adil yargılanma hakkına uygunluğu açısından sorun oluşturabilir. Şöyle ki: // Üzerinde tedbir uygulanan bilişim sisteminin sabit diskini ya da veri taşıma aracı örneğin 320 GB veri taşıma kapasitesine sahiptir. Ancak bunun tamamı hiçbir zaman kullanılmamaktadır. Örneğin; bu diskte 100 GB veri olduğunu kabul ettiğimizde geri kalan 220 GB boştur. **Yalnızca veri bulunan kısımlar yedeklendiğinde boş kalan kısımlara daha sonra başka verilerin yazılması mümkündür.** Dolayısıyla dolu ve boş kısımlarıyla **tüm diskin olduğu gibi yedeklenmesi** teknik tabiriyle “*imajının alınması*” ve bunun sonucunda “*hash değeri*”nin alınması yani işlem yapıldıktan sonra **diskin bir nevi mühürlenmesi** gerekir. **İşlemlerin şüpheli ve müdafinin önünde yapılmaması halinde, imaj alınmadan önce veri yerleştirildiği ve daha sonra imaj alındığı şüphesi ve iddiaları daima söz konusu olacaktır.** Bu durum doğru ve adilane yürütülen soruşturmaların da güvenilirliğini etkileyecektir. ... Ayrıca **bilişim sistemleri üzerinde yapılan adli bilişim incelemeleri daima bu yedekler üzerinde yapılmaktadır; delilin aslının saklanması ve ileride söz konusu olabilecek itirazlarda incelenmek üzere bozulmamış halde muhafazası için aslı üzerinde hiçbir işlem yapılmaması gerekir.** // Bununla birlikte, yine kolluğun başvurduğu şu tür uygulamalar makul sayılabilir: Kolluk görevlileri, CMK'nın 134. maddesine göre arama ve el koyma tedbirinin uygulanmasına ilişkin kararı aldıktan sonra, tedbirin uygulanacağı yere gitmekte ve şüphelinin kullandığı tüm veri

taşıyabilen araçları usulünce fişten çektikten sonra bunları özel yapılmış torbalara koymakta ve ağzını mühürlemektedirler. Bu esnada yapılan tüm işlemleri tutanağa bağlamaktadırlar. Merkeze götürülen bu araçlar üzerinde inceleme yapılacağı zaman duruma göre şüpheli ve/veya müdafii incelemenin yapılacağı merkeze çağrılmakta ve bu işlem için hazırlanmış özel yere alınmaktadırlar. Adli bilişim uzmanı tozdan arındırılmış özel yerlerinde araçlar üzerinde inceleme yaparlarken, buraya yerleştirilmiş kameralar sayesinde, şüpheli ve/veya müdafii kendilerine ayrılan yerde kameralardan aktarılan bu görüntüleri canlı olarak monitörlerden izlemektedirler. Böylelikle bir yandan araçların olduğu yerde inceleme zorunluluğundan kurtulup kendi laboratuvarlarında inceleme yaparlarken, bir yandan da verilere müdahale edildiği ve hukuka aykırı delil elde edildiği itirazından kurtulmaya çalışmaktadırlar” (Dülger, s. 553).

Yaşar Üniversitesi "Ceza Hukuku ve Veri Koruma Boyutuyla Bilişim Hukuku" Sempozyumu

30/04/2019

## **BİLİŞİM SUÇLARINDA ULUSLARARASIALDİYARDIMLAŞMA**

**Prof. Dr. Durmuş TEZCAN<sup>1012</sup>**

(d.tezcan@iku.edu.tr)

1. Bilgisayarın ve onun aracılığıyla yapılan faaliyetlere verilen isimlerden biri olan “bilişim”in yaşamımızda çok büyük bir önem kazandığı çok açık bir gerçektir. Bu durum karşısında, bu alanda hukuka aykırı davranışlara karşı ciddi önemler alınması kaçınılmaz olmuştur. Zira günlük hayatta gerek bireylerin ve gerekse kamu kurum ve kuruluşları kadar, bankalar gibi işletmelerin tamamına yakınının yaptığı yazışmaların kağıt yerine internet ortamında yapılıp, elektronik imza ile imza edilmeye başlanması; alışverişlerin nakit para yerine banka kartlarıyla veya doğrudan internet üzerinden yapılması ve bunlarla ilgili bilişim programları oluşturulması söz konusudur. Böylece bu işler için yer sağlayıcıların kazandığı önem de yadsınmaz. Bu durum karşısında, klasik suçların internet yoluyla ya da yardımıyla işlenmesi yanında, adına bilişim suçları veya siber suçlar (veya sanal ortamda işlenen suçlar) denilen yeni tür suçlar ortaya çıkmıştır<sup>1013</sup>. Bu gelişmelerin tarihi ise, çok yeni olup, son 30 - 40 yılı aşmamaktadır. Her gün bilişim alanında yeni gelişmeler olurken, artık yapay zekânın günlük yaşamımızda çok geniş bir şekilde yer alacağı dikkate alınarak doğuracağı yeni sorunlar da tartışılır hale gelmiştir.

2. Genelde tutucu bir yapıya sahip olan hukukun elektronik çağdaki bu gelişmelere hızlı ayak uydurması kolay olmamakta ve özellikle konu suçlulukla mücadelede sıkı bir işbirliği kurmak zaman almaktadır. Bütün dünyada olduğu gibi, Türkiye’de bu alandaki gelişmeleri mümkün olduğunca yakından izlemeye çalışmaktadır. Zira internet ortamının tüm ülkelerin sınırlarını aşan bir yapıya sahip olması karşısında, hiç bir ülkenin bu yeni tür suçlulukla mücadelede tek başına

---

1012 ORCID: <https://orcid.org/0000-0003-1925-5380>

1013 Siber suç terimini tercih eden Murat Önok’un bu suçlara Türk Hukukunda çeşitli yazarların verdiği isimlerle ilgili olarak bkz. Önok Murat, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, [dergipark.gov.tr/download/issue-file/517](http://dergipark.gov.tr/download/issue-file/517) (20.04.2019). Ancak yazarın ele aldığı sözleşmenin resmi tercümesinde ise, bu suçlar için “Sanal Ortamda İşlenen Suçlar” deyiminin kullanıldığını da ifade etmek isteriz. Ayrıca bkz. <https://www.fmprc.gov.cn/fra/wjdt/wjzc/ty/t1442395.shtml>



başarıya ulaşması mümkün gözükmemektedir. Adli işbirliği konusunda ulusal mevzuatta yer alan kurallara zarar vermeksizin uluslararası işbirliğinin geliştirilmesi de bir zorunluluk haline gelmiştir. Bu yüzden gerek bölgesel olarak ve gerekse Birleşmiş Milletler düzeyinde konu ile ilgilenilmektedir. Terörle mücadele başta olmak üzere, pek çok suçluluğa karşı bilgisayar ortamında hazırlanan mücadele programları da çok büyük bir öneme sahip bulunmaktadır.

3. Bilişim suçlarında uluslararası adli yardımlaşma konusunu ele aldığımız bu tebliğde, özellikle şu hususların altını çizmek gerekmektedir:

1. Bilişim suçları kavramı, kanaatimizce tüm bilişim ortamında işlenen suçları içermektedir. Bunun yanında, internet suçları, sanal ortamda işlenen suçlar gibi terimlerde kullanılmaktadır. Fakat bu kavramlar, sonuçta bilişim alanında işlenen suçları ifade etmektedir.

2. Bilişim suçlarında uluslararası adli işbirliği, tüm ülkeler bakımından, çok hızlı çalışan donanımlı bir alt yapıyı gerektirmektedir. Ülkeler, bürokratik engeller nedeniyle, genellikle bu tür işbirliği konusunda hızlı hareket edememektedir. . Bu duruma örnek Avrupa Birliğinden gösterilebilir: Avrupa Birliğinde (kısaca AB'de) şüpheli, sanık ve hükümlü iadesi konusunda yapılan sözleşmeyi tüm üye devletlerin onaylamaması nedeniyle Avrupa Birliği Konseyi'nin yapıp yürürlüğe koyduğu bir Çerçeve Kararla gerçekleştirilebilmiştir. Aynı durum, AB'nin mali bütünlüğüne karşı işlenen sınır aşan suçlarla mücadeleye ilişkin olarak yıllardır kurulması düşünülen Avrupa Savcılığı konusunda da yaşanmıştır. Lizbon Sözleşmesine de giren Avrupa Savcılığı kurulması konusu, AB üyeleri arasında oy birliği sağlanamadığından, AB Konseyi'nin bir Çerçeve Kararıyla, sayıları 2018'de önce yirmi ve daha sonra yirmi ikiye çıkan AB ülkesi arasında gerçekleşme aşamasına gelmiş ve 2021'de Lüksemburg'da faaliyete geçeceği ümit edilmektedir. Bu örnek de Avrupa Birliği için çok önem taşıyan bir işbirliğinin sağlanmasının ne kadar çok zaman aldığını göstermektedir.

Bu duruma örnek Avrupa Birliğinden gösterilebilir: Avrupa Birliğinde (kısaca AB'de) şüpheli, sanık ve hükümlü iadesi konusunda yapılan sözleşmeyi tüm üye devletlerin onaylamaması nedeniyle Avrupa Birliği Konseyi'nin yapıp yürürlüğe koyduğu bir Çerçeve Kararla gerçekleştirilebilmiştir. Aynı durum, AB'nin mali bütünlüğüne karşı işlenen sınır aşan suçlarla mücadeleye ilişkin olarak yıllardır kurulması düşünülen Avrupa Savcılığı konusunda da yaşanmıştır. Lizbon Sözleşmesine de giren Avrupa Savcılığı kurulması konusu, Avrupa Birliği üyeleri arasında oy birliği sağlanamadığından, Avrupa Birliği Konseyi'nin bir Çerçeve Kararıyla, sayıları 2018'de önce yirmi ve daha sonra yirmi ikiye çıkan Avrupa Birliği ülkesi arasında gerçekleşme aşamasına gelmiş ve 2021'de Lüksemburg'da faaliyete geçeceği ümit edilmektedir.

Bu örnek de Avrupa Birliği için çok önem taşıyan bir işbirliğinin sağlanmasının ne kadar çok zaman aldığını göstermektedir. Bununla birlikte, bu sorun, Avrupa Birliği üyesi ülkeler gibi Türkiye'nin de kurucu üyesi olduğu Avrupa Konseyi bünyesinde hazırlansa da, diğer üçüncü ülkelerin katılmasını kabul eden 23.01.2001 tarihli Sanal Ortamda İşlenen Suçlar Sözleşmesi ile aşılmıştır<sup>1014</sup>.

3. Tüm cezai konularda uluslararası adli işbirliğinde olduğu gibi, bilişim suçlarına ilişkin uluslararası adli işbirliği alanın kapsamına öncelikle klasik adli yardımlaşmalardan oluşan istinabe ve iade konuları girer. Bunlar yanında yeni tür adli yardımlaşmalar dediğimiz, kovuşturmaların devri, yabancı ceza ilamlarının tanınip yerine getirilmesi ve hükümlülerin nakli gibi konularda yer alır<sup>1015</sup>. Nitekim bu Sözleşme'nin yasa dışı erişimle ilgili 2.maddesi, bu Sözleşmeye taraf her ülkenin bir bilgisayar sistemine kısmen veya tamamen hukuka aykırı şekilde kasten erişimi suç haline getirmesini ve dolayısıyla da, bu tür eylemleri hem cezalandırmasını, hem de adli işbirliği kapsamına almasını öngörmektedir. Böylece bu Sözleşme ile taraf devletler, bu tür suçlulukla mücadele için, karşılıklı olarak egemenlik kavramına yeni bir anlam kazandırmış olmaktadır. Taraf devletlerin bu Sözleşme ile üstlendikleri bilişim suçlarını kovuşturma yükümlülüğü, ise, kimi ülkelerde bağlantılı dava kavramıyla izah edilmektedir<sup>1016</sup>. Konuya Türkiye açısından bakarsak, 2005 de yeni yürürlüğe giren yeni ceza mevzuatımız bu tür yükümlülüklerin yerine getirilmesi açısından daha uyumlu bir yapıya sahiptir. Ayrıca bu durum, 23.04.2016 tarih ve 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu ile daha da güçlendirilmiştir. Zira TCK m.8 ile suçun işlendiği yer konusunda karma teori benimsendiğinden, başka ülkelerde işlenen bu suçların sonuçlarının Türkiye'de meydana gelmesi halinde, bunların Türkiye'de işlenmiş suç kavramı içinde değerlendirilmesi mevzuatımızda bir sorun yaratmayacaktır. Bunun dışında kalan hallerde ise, failin ülkemizde bulunması ve suç yeri ülkesine ya da uyruğunda bulunduğu ülkeye iade edilememesi durumunda TCK m. 12-13 kapsamında kovuşturulması söz konusu olacaktır.

4. Öte yandan, uluslararası adli yardımlaşma açısından önem taşıyan temel bilişim suçları ise, Türk Ceza Kanununun 243-246.maddeleri arasında düzenlenmiştir<sup>1017</sup>. Bu tür suçlarda ülkeler

---

1014 28/04/2019 tarihi itibarıyla 62 devlet bu Sözleşmeye taraf olup, ayrıca 10 devlet de, gözlemci statüsünde yer almaktadır. (Bkz. <https://www.coe.int/fr/web/cybercrime/parties-observers>, 28/04/2019 tarihi itibarıyla)

1015 Bkz. Tezcan D/Erdem MR/Önok M, Uluslararası Ceza Hukuku, Seçkin yay, 5.b. Ankara, 2019; 23/04/2016 tarih ve 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu'nda da benzer bir sistem benimsenmiştir, bkz.05/05/2016 tarih ve 29703 sayılı RG.

1016 FRANCILLON Jacques, Cybercriminalité. Aspects de droit pénal international, Revue Internationale de Droit Pénal (RIDP) 2013, [www.penal.org/sites/default/files/files/RH-7.pdf](http://www.penal.org/sites/default/files/files/RH-7.pdf)

1017 Doğrudan bu suçlara ilişkin Türk Hukukunda pek çok yayın bulunmakla birlikte, kısa bir bilgi için bkz. Tezcan Durmuş/ Erdem Mustafa Ruhan/ Önok Murat, Ceza Özel Hukuku, 16.b, Seçkin Kitabevi, Ankara, 2018, s. 1033-1043.

arasında sıkı bir adli yardımlaşmanın önemi ise, bir örnek verirsek daha kolay anlaşılacaktır. Bilgisayar güvenlik sistemlerini aşarak basit bir bilgisayardaki çok güçlü koruma altındaki bankaların bilişim sistemine girerek banka için miktarı çok büyük sayılmayacak, ancak fail için birey olarak önemli bir miktar sayılacak yasa dışı menfaatler elde etmeleri durumunda adli işbirliği konusu büyük önem taşır. Bazen de, örneğin Türkiye’den internet üzerinden yurt dışında aldığı yasal izinle paralı şans oyunları oynatan bir yabancı siteye giren bir kimsenin, kendisinden istenen özel bilgileri vermeyerek oyun oynamaktan vazgeçmesi üzerine ortaya çıkabilmektedir. Böyle bir olayda yatırdığı parayı iade etmeyen bu kişinin internet sitesine ulaşımı birkaç saatliğine öç almak için kapatması gibi durumlar nedeniyle zarara uğrayan yabancı firmanın, Türkiye’de bu işi gerçekleştiren kişinin belirlenip kovuşturulması için şikâyetine konu olabilir. Uluslararası adli yardımlaşmaya konu olan ve yargılanması uzun yıllar alan bir olayı burada örnek olarak verebiliriz: Türkiye’de Üniversiteyi yeni bitirmiş (A.K. isimli) bir bilgisayar teknisyeninin, bundan on beş yıl kadar önce, evindeki bilgisayarla ABD’nin büyük bankalarından birinin bilgisayar sistemine girerek, o bankanın en yetkili kişinin komutuymuş gibi kredi kartı yolsuzluğu gerçekleştirebilmiştir. Bunu, o bankada, bir yıl önce en yüksek internet ortamında alışveriş yapma hakkına sahip bazı kişilerin süresi biten kredi kartlarının geçerlik süresini uzattırarak sağlamıştır. Ardından bu kartlarla en pahalı bilişim programları satın alıp, sonrada bunları Türkiye’ye ithal edemediği şekilde bir yalanla yarı fiyatına sattırmak için yine internetten ABD’den bir kişiyi bulmuş ve onun aracılığıyla o program paketlerini sattırmıştır. Her paket için kararlaştırdıkları hizmet bedelini, son satıştan sonra bu satış hizmetini veren kişiye ödememesi üzerine, hizmet veren kişinin ısrarlı şikâyeti nedeniyle FBI tarafından, Türk makamlarıyla kurulan adli işbirliği çerçevesinde yapılan uzun araştırmalar sonucu olay ortaya çıkarılmıştır. Böylece ABD’den gelen belgeler çerçevesinde bu kişi, İstanbul 2.Ağır Ceza Mahkemesinde yargılanarak çeşitli bozma kararlarını müteakip İstanbul 2.Ağır Ceza Mahkemesinin 02.4.2019 tarih ve 2011/158 Es.-2019/134 karar sayılı ilamıyla ABD’de oturan on beş ABD vatandaşına karşı kredi kartı yolsuzluğundan TCK245/1.maddesi çerçevesinde on beş defa ayrı ayrı 2 yıl 6 ay hapis ve 80 TL adli para cezasına (toplam 22 yıl 6 ay hapis ve 120 bin TL adli para cezasına) mahkûm edilmiştir<sup>1018</sup>.

Bu tür olaylarda gösteriyor ki, kişiler örneğin Türkiye’den internet üzerinden bir başka ülkede ya da tersine bir başka ülkede Türkiye ile ilgili olarak kolayca bilişim suçu

---

1018 Bu karar metnine ulaşmamızı sağlayan eski öğrencimiz Yargıtay Üyesi Sn. Fehmi Tosun’a içten teşekkürlerimi sunarım.

işleyebilmektedirler. Bu örnekleri çoğaltmak mümkündür. Bu nedenle bu tür suçlarda uluslararası adli yardımlaşma çok büyük bir öneme sahip bulunmaktadır.

4. Bu ön bilgilerin ışığında konuyu analiz edersek, yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı, bilgisayarlarla ilişkili sahtecilik fiilleri, çocuk pornografisiyle ilişkili suçlar ve telif haklarının ve benzer hakların ihlaline ilişkin suçlar gibi pek çok suça “Sanal Ortamda İşlenen Suçlar Sözleşmesi”nde yer verildiği görülmektedir (m.2 vd). Sözleşmede yer verilen bu suçlarla ilgili uluslararası adli işbirliği açısından geniş kapsamlı bir işbirliği ise, bu sözleşme ile birlikte anlam kazanan 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu’nu kabul ettiği kurallara göre gerçekleştirilir<sup>1019</sup>.

5. Türkiye’de bilişim suçlarıyla ilgili olarak adli yardımlaşma konusu iki şekilde gündeme gelir. Bunlardan ilkinde, bu tür suçlulukla mücadelede Türkiye adli yardım talep eden bir ülke iken, ikincisinde ise, yabancı ülkeler tarafından Türkiye’den istenen adli yardım talepleri gündeme gelir. Gerek Türkiye’de yapılan yargılamalarda ve gerekse yabancı ülkelere gelen adli yardım taleplerinde, tüm adli yardımlaşmalarda olduğu gibi, 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu’nda merkezi makam olarak Adalet Bakanlığı gösterilmiştir (6706 sayılı Kanun, m.2/1b, 3 ve 4). Bakanlık adına da Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü bu faaliyeti sürdürmektedir. Nitekim bu Genel Müdürlük, internet ortamında işlenen suçlarda istinabe işlemleri bakımından da, kendi sitesinde yararlı bilgiler vermektedir<sup>1020</sup>. Bu durumda C.savcılıkları ve mahkemelerin, bu suçlarla ilgili, istinabe taleplerini, Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü’ne, evrakın, ilgili devletin diline yapılan çevirisiyle birlikte göndermeleri gerekir.

6. Öte yandan, Sanal Ortamda İşlenen Suçlar Sözleşmesi ise, bilişim suçlarının hızlı bir iş birliğini gerektirdiğini dikkate alarak, üye devletlerin, bilişim suçlarıyla ilgili soruşturma ve kovuşturmaların yürütülmesi ya da bu suçlarla ilgili olarak “elektronik ortamda delil toplanması konusunda birbirlerine mümkün olan en geniş ölçüde” yardımcı olmaları yükümlülüğünü

---

1019 Sanal Ortamda İşlenen Suçlar Sözleşmesi’nin 23 vd maddelerinde yer alan ve Türk Hukukundaki mevcut kuralları zenginleştiren düzenlemeler ışığında 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu’na göre yapılacak adli yardımlaşmalar konusunda bkz. Bkz. Tezcan D/Erdem MR/Önok M, Uluslararası Ceza Hukuku, Seçkin yay, 5.b. Ankara, 2019 s. ; Ayrıca bkz. Önok Murat, Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, <https://docplayer.biz.tr/18748312-Avrupa-konsevi-siber-suc-sozlesmesi-isi-ginda-siber-suclarla-mucadelede-uluslararasi-isbirligi.html> (Erişim tarihi 02/04/2019); Mavzer Şener, Siber Suçlarla Mücadelede Uluslar Arası İşbirliği, bkz. cybercrimesmavzer.blogspot.com /2014/.../[siber-suclarla-mucadelede-uluslar-arasi.htm...](http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adli_isbirligi_ceza/cz_istinabe_9_internet_ortaminda_islenen_suclar.html) (Erişim tarihi 02/04/2019).

1020 Bkz. IX- İnternet Ortamında İşlenen Suçlarda Uluslararası Ceza İstinabe İşlemleri, [http://www.uhdigm.adalet.gov.tr/adli\\_yardimlasma/adli\\_isbirligi\\_ceza/cz\\_istinabe\\_9\\_internet\\_ortaminda\\_islenen\\_suclar.html](http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adli_isbirligi_ceza/cz_istinabe_9_internet_ortaminda_islenen_suclar.html)

getirmiştir (m.25/1). Hatta üye devletlerden her birine, acil durumlarda faks ve elektronik posta gibi hızlı iletişim araçlarıyla yardım verilmesi ya da irtibat kurulması talebinde bulunabilme olanağını da kabul etmiştir (m.25/3).

7. Uluslararası adli yardımlaşma bakımından burada belirtmemiz gereken bir başka husus ise, Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde, bilişim suçlarına ilişkin yapılan adli yardımlaşma taleplerinin değerlendirilmesinde, bu suçlarla ilgili olarak kendisinden talepte bulunulan ülkede eylemin suç tasnifindeki yerinin farklı olmasının, yardım talebini geri çevirme nedeni olmamasıdır (m. 25/5). Bunun dışında, başlangıçta devletler, mali suçlarda, hiçbir devlet, diğer devletin vergi tahsildarı olmadığı gibi bir düşünceyle hareket etmişken bugün bu anlayış değişmiş ve bu Sözleşmede de istemin sadece mali suç olduğu gerekçesine dayandırılarak da ret edilemeyeceği kuralına yer verilmiştir (m.25/4).

8. Anılan Sözleşmede, adli işbirliği kapsamında, taraf devletlerden birinin diğerine, gizlilik koşulu gibi çekinceler koyarak, kendiliğinden, suç ihbarında bulunma yetkisi de vermektedir (m.26/1-2).

9. Burada vurgulanması gereken bir başka konu ise, kimi Birleşmiş Milletler sözleşmelerinde olduğu gibi, Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde tamamlayıcı adli yardım kurallarının ön görülmesidir. Buna göre, bu Sözleşmeye taraf olan ülkeler arasında ikili veya çok taraflı bir adli yardım sözleşmesinin bulunmaması halinde geçerli olacak temel adli yardımlaşma kurallarına da yer vermiştir (m.27). Bu kurallar arasında talepleri iletmekle görevli bir merci ya da merciler oluşturulması (m.27/2 a) ve bu mercilerin birbirleri arasında doğrudan yazışma yapması (m.27/2 b); kendisinden talepte bulunulan Taraf, yardım vermeyi red ya da tehir etmeden önce ve gerekli durumlarda yardım talep eden Taraf ile görüş alışverişinde bulunarak, yardımın kısmen verilip verilemeyeceği ya da bazı şartlara tabi olarak verilebileceği hususunu karara bağlaması şartı da getirilmiştir (m.27/6).

10. Sözleşmeye taraf devletler arasında korunan trafik verilerinin açıklanması işleminin kolaylaştırılması da öngörülmüştür (m.30). Adalet Bakanlığının verdiği bilgiye göre, Türkiye'de yer alan erişim sağlayıcıların trafik bilgisini saklama süreleri 5651 sayılı İnternet Ortamında İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 6/1.maddesi çerçevesinde hazırlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin 8/b maddesi gereğince, erişim sağlayıcıların, trafik bilgisini bir yıl saklamak yükümlülüğü bulunmaktadır. Bununla birlikte, Telekomünikasyon İletişim Başkanlığı (TİB), trafik kayıtlarını 5 yıl süre ile muhafaza etmekte ve adli makamlarca bu süre içinde yapılan talepleri yerine

getirmektedir. Türkiye’den adli yardım talebinde bulunan ülkelerin bu sürelere dikkat etmesi gerekmektedir. Buna karşılık internet üzerinden yer sağlayıcıların büyük çoğunluğu ise, ABD’de bulunduğundan, bu ülkedeki yer sağlayıcılarla ilgili adli yardım taleplerinin de, ABD ile Türkiye arasında yürürlükte bulunan Adli Yardım Sözleşmesine göre Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü aracılığıyla gerçekleştirilmesi gerekmektedir<sup>1021</sup>.

11. Adli yardımlaşma kapsamında bir diğer konu ise, Taraflardan her birinin, bilgisayar sistemleri ve verileriyle ilgili olarak, adli suçlarla ilgili soruşturma ve kovuşturmanın yürütülmesi ya da elektronik ortamda delil toplanabilmesini temin için, haftanın 7 günü 24 saat boyunca elverişli olan bir irtibat noktası belirlemesi yükümlülüğüne yer verilmiştir (m.35). Bu hizmet Cumhuriyet Savcılarının gözetiminde kolluk tarafından sağlanmaktadır<sup>1022</sup>.

12. Sanal Ortamda İşlenen Suçlar Sözleşmesi’nde bilişim suçları nedeniyle yurt dışında bulunan bir sanık veya hükümlünün iadesi konusu da 24.maddede düzenlenmiştir. Bu konuda kural olarak iade ilgili ülkenin taraf olduğu ikili ve veya çok taraflı iade sözleşmeleri çerçevesinde gerçekleştirilir. Türkiye’nin çok taraflı bir sözleşme olan Avrupa Konseyinin 1959 tarihli iade sözleşmesi ve ek 1 nolu protokolü başta olmak üzere pek çok devlet ile cezai konularda ikili iade ve adli yardım sözleşmeleri bulunmaktadır<sup>1023</sup>. Gerek Avrupa Konseyinin 1959 tarihli iade sözleşmesi, gerekse 6706 sayılı Kanun (m.10) ile Sanal Ortamda İşlenen Suçlar Sözleşmesi (m.24/1 a) asgari bir yıl hapis cezasını gerektiren bir suçtan, bir başka deyişle bilişim suçundan söz etmektedir<sup>1024</sup>.

13. Bilişim suçlarında uluslararası işbirliğinde dikkat edilmesi gereken bir konu da, şüpheli, sanık ve hükümlülerin temel insan haklarına saygılı olunmasıdır. Nitekim uluslararası adli yardım talebine konu olan suçun kendisinden yardım talep edilen Tarafça siyasi suç ya da siyasi bir suçla bağlantılı olan bir suç olarak değerlendirilmesi (m.27/4a) bu konuya bir örnektir.

14. Öte yandan anılan Sözleşmede, söz konusu talebin gereğinin yerine getirilmesinin kendisinden yardım talep edilen Tarafın egemenliğine, emniyetine, kamu düzenine ya da diğer önemli menfaatlerine zarar verici olarak değerlendirilmesi (m.27/4b) halinde de talebin geri çevrilmesi mümkündür.

---

1021 Gerekli yazışmalar için bkz. [http://www.uhdigm.adalet.gov.tr/adli\\_yardimlasma/adli\\_isbirligi\\_ceza/cz\\_istinabe\\_9\\_internet\\_ortaminda\\_islenen\\_suclar.html](http://www.uhdigm.adalet.gov.tr/adli_yardimlasma/adli_isbirligi_ceza/cz_istinabe_9_internet_ortaminda_islenen_suclar.html)

1022 Bu konuda bkz. Taşçı Ufuk/Can Ali, Türkiye’de Polisin Siber Suçlarla Mücadele Politikası:1997-2014, [dergiipark.gov.tr/download/article-file/157433](http://dergiipark.gov.tr/download/article-file/157433), (Erişim tarihi 5/4/2019)

1023 Bu liste için bkz. Tezcan D/Erdem MR/Önok M, Uluslararası Ceza Hukuku, Seçkin yay, 5.b. Ankara, 2019, Ekteki liste.

1024 Bkz Tezcan D/Erdem MR/Önok M, Uluslararası Ceza Hukuku, Geri vermenin koşulları: 1/ac, s. 200 vd

15. Aynı şekilde, kendisinden talepte bulunulan Taraf, herhangi bir talebe ilişkin olarak işlem yapmasının yetkili mercilerince sürdürülmekte olan cezaî soruşturma ya da işlemlere zarar vermesinin söz konusu olabileceği durumlarda da, bu talebe ilişkin işlemleri tehir edebileceği hüküm altına alınmıştır (m.27/5).

16. Sözleşmede, Sözleşmeye Taraf ülkeler arasında yetki çatışmalarını önlemek için 22.madde de **yargı yetkisi de düzenlenmiştir. Buna göre, eylemin diğer ülkenin sınırları içinde işlenmesine veya bayrağını taşıyan gemilerde açık denizlerde işlenmesi haline zarar vermeyecek şekilde yer bakımından yetkilerini belirlemesi yükümlüğü de getirilmiştir. Bununla birlikte, Anayasa m.38'e göre, vatandaşın diğer ülkede işlediği bir suçtan dolayı iade edilememesi halinde bu kişinin bir başka ülkede kovuşturulması bu Sözleşmeye aykırı olmayacağı gibi, kovuşturmanın aktarılması yoluyla sorunun çözülmesi de mümkün olacaktır.**

17. **Varılan sonuç**, bilişim suçlarında uluslararası işbirliği konusu, Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde öngörülen kurallarla güçlendirilmiş bir görünüm kazanmıştır. Böylece Türk Hukukunda 6706 sayılı Cezai Konularda Uluslararası Adli İş Birliği Kanunu ile getirilen kurallarla bu sözleşmedeki adli yardımlaşma anlayışı pekiştirilmiştir. Bilişimin artan önemi ve sınır tanımaması karşısında, Türk Hukuku, uluslararası adli yardımlaşma bakımından sağlam bir alt yapıya sahip bulunmaktadır.

**YARGITAY KARARLARI IŞIĞINDA  
DOĞRUDAN BİLİŞİM SUÇLARI<sup>1025, 1026</sup>  
(TCK. 243 ve 244 )**

*Nevzat ÖZSOY*

**BİRİNCİ BÖLÜM**

**I- GİRİŞ**

Bilişim suçları, Yargıtay Kararlarında kabul edildiği üzere;

- Doğrudan bilişim suçları (gerçek bilişim suçları); TCK. m. 243, 244, 245, 245/A ve 246. maddelerinde yer alan suçlar,
- Dolayısıyla bilişim suçları (bilişim bağlantılı suçlar); TCK. m. 112, 113, 125, 132, 133, 134, 135, 136, 138, 142/2-e, 158/1-f, 213, 218, 226 ve 228. maddelerinde yer alan suçlar şeklinde bir tasnife tabi tutulmaktadır.<sup>1027</sup>

Bilişim suçları Türk Ceza Kanun'un 10. Bölümde 243, 244 ve 245. Maddelerinde düzenlenmiştir, bu bölümde yer alan 243.maddenin 1.fikrasında bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme veya orada kalmaya devam etme, 2. fıkrasında 1. fıkrada yer alan fiilin bedeli karşılığında yararlanılabilen sistemler hakkında işlenmesi, 3. fıkrasında bu fiiller nedeniyle sistemin içeriklerinin yok olması veya değişmesi fiilleri, 244. maddenin 1. fıkrasında bilişim sisteminin işleyişini engelleme veya bozma eylemi, 2. fıkrasında bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme fiilleri, 3. fıkrasında Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali cezalandırılmıştır. Maddenin 4.fıkrasında ise “Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamanın başka bir suç oluşturulmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.” Denilmek suretiyle önceki fıkralarda tanımlanan eylemler nedeniyle şüphelinin,

---

1025 Nevzat ÖZSOY Yargıtay 8. Ceza Dairesi Üyesi

1026 ORCID: [orcid.org/0000-0001-8749-6333](https://orcid.org/0000-0001-8749-6333)

1027 Yargıtay Ceza Daireleri uygulamasında sıklıkla rastlanan bozma sebepleri, Yargıtay Cumhuriyet Başsavcılığı, Ankara 2018 s. 829



kendisi veya bir başkası yararına sağladığı haksız çıkarım, bir başka suçu oluşturmaması halinde bu fıkra uyarınca cezalandırılması öngörülmüş, 245. Maddesinde ise banka ve kredi kartlarının kötüye kullanılması suç olarak düzenlenmiştir.

Ancak TCK.nun 245. Maddesinin bilişim suçları kategorisi içerisinde düzenlenmesi yerinde değildir. Bu suçun Yasa'nın 2.Kitabının 2.Kısımının 10.Bölümünde yer alan "Malvarlığına Karşı Suçlar" arasında düzenlenmesinin daha doğru olacağı düşünülmektedir. Bu çalışmada sadece TCKnın 243 ve 244. maddelerinde düzenlenen doğrudan bilişim suçları inceleme konusu yapılmıştır.

07.04.2006 tarihinde yürürlüğe giren 24.03.2016 tarihli 6698 sayılı Kanununun 30. maddesi ile birinci fıkradaki "ve" ibaresi "veya" olarak değiştirilmiş, gerekçe ile metin arasındaki çelişki giderilerek eylem seçimlik hale getirilmiştir. Ayrıca aynı Kanun ile 243. maddeye 4. fıkra eklenmiş, yeni bir suç düzenlemesi yapılmıştır. Ancak bu düzenlemede "bilişim sistemine girme" sözkonusu olmadığından ilk üç fıkradan farklı bir düzenleme yapılmıştır. <sup>1028</sup>

## II- KAVRAM ve TANIM

**1.Bilişim;** bilginin saklanması ve iletilmesini konu alan akademik ve mesleki disiplin olarak tanımlanabilir. Bilişim, insanların teknik, ekonomik, sosyal, kültürel, hukuksal ve benzeri alanlarda sahip oldukları verinin saklanması, saklanan bu verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılmasıdır. Böylece bilişim, hem verilerin işlenmesini hem de bu işlem sonuçlarının aktarılmasını yani veri iletişimini de içeren bir kavramdır. O halde, veri – işlem ve veri – iletişim unsurlarını taşıyan araçların bütününe bilişim sistemi denilmektedir.

**2.Bilişim suçu;** bilişim suçunu "verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanında işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı haksız eylem olarak tarif etmek mümkündür."

"Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenen suçlardır." "Bilişim Teknolojileri kullanılarak işlenen tüm suçlar "Bilişim Suçlarını" oluşturur."

"Bilgisayar suçu (computer crime): Bir bilgisayar ya da bilgisayar ağına yönelik ya da onları kullanarak (bilgisayar teknolojisi bilgilerinden yararlanılarak) gerçekleştirilen yasa dışı eylem."

“Siber suçlar (cyber crimes): Herhangi bir suçun elektronik ortam içerisinde işlenebilme imkanı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçları siber suçlar olarak tanımlayabiliriz. Siber suç bilgisayar ve ağ sistemleri yoluyla bilgisayar veya ağ sistemleri içerisinde ya da bilgisayar tarafından suç olarak yaratılmış fiillerin siber ortamda işlenmesi ve daha önce suç olarak yaratılmamış bu ortamın karakteristiğe has bir takım ihmallerin bir bütünüdür.”

Tanımlarda da görüldüğü gibi bilişim suçlarının net olarak çizgileri çizilmemiştir çünkü gelişen teknolojiyle birlikte bilişim suçları da değişmektedir. Bu nedenle “bilişim suçları”, “bilgisayar suçları”, “internet suçları”, “siber suç”, “ileri teknoloji suçu”, “dijital suçlar”, “sanal suç” gibi kavramların tek bir tanımının yapılmaması bir eksiklik olarak değerlendirilmemelidir. Ancak biz bu kavramların hepsini genel olarak “bilişim suçu” olarak adlandırabiliriz. Günümüzde bilişim suçlarına “**internet suçları**” ismi verilmektedir.

**3.Bilişim sistemi;** verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağını veren manyetik sistemlerdir.Bu tanımın, sadece “veri – işleme” esas alması, “veri – iletişimine” yer vermemesi bakımından eksik olduğu belirtilmektedir.<sup>1029</sup> Bilişim sisteminin, bilgileri otomatik olarak işleme tabi tutması ve manyetik olması dışında ki en önemli özelliği genel amaçlı kullanım özelliğidir. Yani belli bir işin yapılmasına özgülüne başka bir fonksiyon eda edemeyen bir sistem bilişim sistemi değildir. Mesela; otomatik çamaşır makineleri, elektronik uzaktan kumandalı TV, programlanabilen buzdolabı, genel amaçlı işlem yapamadıklarından yani yüklenen değişik programlara göre başka nitelikli işlemleri yapamadıklarından, bilişim sistemi olarak kabul edilmeyecektir.<sup>1030</sup>Bilgisayar, çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, 297ery, klavye, kulaklık, yazıcı vb), iletişim altyapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifade eder.

**4.Bilişim alanı;** bilgileri depo ettikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden oluşan alan olarak tanımlanabilir.<sup>1031</sup>

---

1029 Prof. Dr. Mehmet Emin Artuk, Prof. Dr. Ahmet Gökçen, Doç. Dr. Caner Yenidünya, Türk Ceza Kanunu Şerhi, Özel Hükümler, C. 5, s.4643, Ankara 2009

1030 Levent Kurt, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınevi, s.141, Ankara 2005

1031 Yrd. Doç. Dr. R. Yılmaz YAZICIOĞLU, Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı, s.2, 21-22 Mayıs 2001, İzmir Uluslararası İnternet Hukuku Sempozyumunda sunulan tebliğ.

**5.Bilgisayar;** belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, yürüteceği 298ery298f298 ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen masaüstü, dizüstü bilgisayarlar, cep telefonu ve benzeri tüm elektronik araçları ifade eder.

Bilgisayarın elektronik kısmına donanım (Hardware), program kısmına ise yazılım (Software) denir. Bilgisayarda 4 unsur bulunmaktadır: Bunlar;

- a-Bilginin girişi (giriş birimleri: klavye, fare, kamera, scanner yani tarayıcı, fax-modem),
- b-Bilginin saklanması (hafıza: hard disk, disket, CD, DVD, USB, harici hard disk, bulut bilişim vb.),
- c-Bilginin işlenmesi (beyin: merkezi işlem birimi yani CPU),
- ç-Bilginin çıkışı (çıkış birimleri: monitör yani ekran, yazıcı, çizici, modem gibi).

**6.Veri;** bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri ifade eder (bkz. 5651 Sk'nun 2/a mad.).

**7.Elektronik Veri;** elektronik, 298ery298 veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları ifade eder (bkz. 5070 Sk'nun 3/a mad.)

**8.IP (Internet Protocol) Adresi;** belirli bir ağa bağlı cihazların birbirini tanımak, birbirleri ile iletişim kurmak ve birbirlerine 298ery yollamak için kullandıkları, internet protokolü standartlarına 298ery verilen adresi ifade eder.

İnternete bağlanan her bilgisayara internet servis sağlayıcı tarafından bir IP adresi atanır ve internetteki diğer bilgisayarlar bu bilgisayara verilen IP adresi ile ulaşırlar. IP adresleri, dinamik ve statik olarak iki bölüme ayrılır. Genel olarak dinamik IP adresi kullanılır. Dinamik IP adresleri, zamana ve oturuma göre değişir. Çünkü servis sağlayıcı o an için boş olan IP adresini kullanıcıya atar. Statik IP adresi ise, zamana ve oturuma göre değişmeyen adresi ifade eder. Ancak sistem yöneticisi tarafından tanımlanıp değiştirilebilir.

Ayrıca alan adları için de bir IP adresi vardır. Bir internet sayfasını yazdığımız kısma (ağ tarayıcı) bu IP adresi de yazılarak bağlanılabilir. Ancak bu rakamları yazmak pratik ve akılda kalıcı olmadığından alan adı IP adresine karşılık gelen bir alan adı sistemi kullanılmaktadır.

**9.Ethernet Kartı;** Network (ağ) sistemlerinde kullanılan, bilgisayarla ağ arasında iletişimi sağlayan ağ ara birim kartıdır. Her Ethernet kartının MAC adresi vardır. Bu adres, 00-23-c3-45-00-b3 şeklindedir. Ethernet kartı iletilecek olan verileri, paketlere böler ve kart çıkışına bağlı ağ kablosuna gönderir.

**10.Mac (Media Access Control) Adresi;** Ethernet ağında sistemler birbirlerinden sahip oldukları MAC adresi ile ayırt edilirler. Ethernet, wi-fi, ery299f299 gibi ortamlarda ağ donanımını tanımlamaya yarayan, bir bilgisayarın ery299f299 kartına üretici tarafından kodlanmış fiziksel adres bilgileri ifade eder. Her Ethernet kartının dünyada eşi olmayan bir adrese sahiptir. Örneğin; bir notebook bilgisayarda modem kablolu Ethernet ve wireless (wi-fi) Ethernet varsa üç ayrı MAC adresi vardır.

MAC, 48 bit'lik bir adres olduğundan dolayı  $2^{48} = 281,474,976,710,656$  değişik ağ kartını tanımlamak için kullanılabilir. Örnek bir MAC adresi: 01:23:45:67:89:AB.([www.wikipedia.com](http://www.wikipedia.com))

**11.Bilgisayar Kütüğü;** bilgisayarın ve bilgisayarda yer alan dosyaların, geçirdiği safahatlara dair kayıtların tutulduğu verileri ifade eder.

**12.Sunucu Kütüğü;** bir sunucudaki bütün değişikliklerin kayıt altına alındığı kütük dosyasını ifade eder. Kütüklerde bilgisayar ağına erişim, dosyalarda yapılan değişiklikler, 299ery f indirme ve yükleme gibi kayıtlar tutulur.

**13.Bilgisayar Programı;** bilgisayara bir işi yaptırmak için verilen komutlar bütününe bilgisayar ery299f299 denir. Bilgisayar 299ery299f299 bir programlama dili kullanılarak yazılır. Program çalıştırıldığında bilgisayar ilgili komutları okuyarak programda kendisine ery299f edilen işi yapar

**14.RAM (Random Access Memory);** rastgele erişimli bellek demektir. Birbirinden bağımsız hafıza hücrelerinden oluşur. Veri depolanabilir, silinebilir, okunabilir, değiştirilebilir. Bilgisayar çalıştığı sürece RAM faaliyetine devam eder. Bilgisayar kapandığında ise RAM' de depolanmış veriler silinir.

#### **15.İmaj Alma ve Hash Değeri :**

**İmaj Alma;** veri depolama cihazlarının sektör bazında başka bir veri depolama cihazına kopyalanması işlemini ifade eder.

**Hash Değeri;** dosyaların parmak izi olarak nitelendirilebilir. Dosyalar çeşitli karmaşık algoritmalar ile taranır ve dosyanın benzersiz bir parmak izi çıkarılır. Adli bilişimde geçen bir zaman sürecinde bir depolama alanındaki bilgiler üzerinde değişiklik olup olmadığının anlaşılması için kullanılır. Dataya ilişkin olarak yapılan işlemler öncesinde ve sonrasında datanın hash değeri alınır. Eğer hash değeri işlem öncesinde ve sonrasında aynı ise datada herhangi bir değişiklik olmadığı, eğer hash değeri farklı ise datada değişiklik olduğu sonucuna varılabilir. Ancak bunun istisnaları da söz konusudur. Örneğin, bozuk sektörler sonucu alınan imajlarda ilk hash işleminden sonra "bad sektör" oluşması halinde doğal olarak belirli bir zaman sonra ikinci hash işleminde hash değeri farklı çıkar. Bir diğer istisna da RAM arızasıdır. Ayrıca kullanılan donanımların bozulması

veya arızalı olmaları veya elektriksel sorunlar sebebiyle de hash değeri farklı çıkabilir. Kolluk kuvvetleri bu nedenle uygulamada hash değerinin farklı çıkmasını ve olası tartışmaları önlemek için bilgisayarların imajlarını kendi birimlerinde almayı tercih etmektedir.

### **16.Bilişim Ağı (Network), İnternet, İnternet Ortamı, Intranet, Bulut Bilişim (Cloud Computing):**

**Bilişim Ağı (Network);** bilgisayarların birbirlerine bağlanması ile oluşan yapıyı,

**İnternet;** dünya genelindeki bilgisayar ağlarını ve kurumsal bilgisayar sistemlerini birbirlerine bağlayan elektronik iletişim ağını,

**İnternet ortamı;** haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

**Intranet;** sadece belirli bir kuruluş içerisindeki bilgisayarları yerel ağları ve geniş alan ağlarını birbirlerine bağlayan ağı,

**Bulut Bilişim (Cloud Computing);** bilişim aygıtları arasında ortak bilgi paylaşımı sağlayan hizmetlere verilen genel ismi ifade eder.

### **17.Geniş Alan Ağı (Wan), Yerel Alan Ağı (Lan);**

**Geniş Alan Ağı;** birden fazla cihazın birbirleri ile iletişim kurmasını sağlayan fiziksel veya mantıksal büyük ağı ifade eder. Yerel alan ağlarının birbirlerine bağlanmasını sağlayan çok geniş ağlardır. En meşhur geniş alan ağı internettir.

**Yerel Alan Ağı;** ev, okul, işyerleri gibi sınırlı coğrafi alanda bilgisayarları ve araçları birbirlerine bağlayan bilgisayar ağını ifade eder.

**18.Etki Alanı (Domain Name);** bir web sitesinin internetteki adı ve adresidir. Bunlar bilgisayar ortamında nümeriktir, ancak akılda kalması ve kolay kullanım açısından anlamlı kelimelere dönüştürülmüştür.

### **19.Yer Sağlayıcı, İçerik Sağlayıcı, Servis/Erişim Sağlayıcı, Toplu Kullanım Sağlayıcı, Elektronik Sertifika Hizmet Sağlayıcısı;**

**İçerik sağlayıcı;** internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

**Yer sağlayıcı;** hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,

**Servis / Erişim sağlayıcı;** Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

**Toplu kullanım sağlayıcı;** kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan kişileri,

**Elektronik sertifika hizmet sağlayıcısı;** elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri ifade eder.

**20.Trafik Bilgisi ( Log Kayıtları);** internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, 301ery, yararlanılan hizmetin türü, aktarılan 301ery miktarı ve bağlantı noktaları gibi değerleri ifade eder.

**Yer sağlayıcı trafik bilgisi;** internet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgileri,

**Erişim sağlayıcı trafik bilgisi;** internet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri ifade eder.

### III. BİLİŞİM SUÇLARINDA SORUŞTURMA, GÖREVLİ VE YETKİLİ MAHKEME

#### A- SORUŞTURMA

5237 sayılı Türk Ceza Kanunu'nun 243 ve 244. maddelerinde düzenlenen bilişim suçları şikâyete bağlı suçlardan değildir. Bu suçlar nedeniyle Cumhuriyet savcılarını resen soruşturma başlatabilir.

5271 sayılı Ceza Muhakemesi Kanunu'nun 160. maddesi uyarınca Cumhuriyet savcısı TCK. nun 243 ve 244. maddelerinde belirtilen bilişim suçlarından her hangi birisinin işlendiğini öğrendiğinde, bir şikâyet beklemeksizin gerekli araştırma ve soruşturmayı yaparak yeterli delil elde ettiği takdirde CMK. nun 170. maddesi gereğince kamu davasını açacaktır.

#### B- GÖREVLİ MAHKEME

5237 sayılı TCK. nun da 243 ve 244. maddelerinde düzenlenen bilişim suçlarında hangi mahkemenin görevli olduğuna dair Kanun metninde bir düzenlemeye yer verilmemiştir. Bu nedenle görevli mahkeme 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10. 11. ve 12. Maddelerine

göre belirlenecektir. Bu bağlamda TCK. Nun 243 ve 244 . maddelerinde düzenlenen suçlar bakımından görevli mahkeme asliye ceza mahkemeleridir.

### **C- YETKİLİ MAHKEME**

Bilişim suçları konusunda yer bakımından yetki konusunda suçun niteliği ve işleniş şekilleri nedeniyle çok fazla sorun yaşanmaktadır.

Bilişim suçlarında yer yönünden yetki konusunda özel bir düzenleme bulunmadığından yer yönünden yetkili mahkeme Ceza Muhakemesi Kanunu'nun 12. maddesinin 1 ve 2. fıkralarına göre belirlenecektir.

Ceza Muhakemesi Kanunu'nun 12. Maddesindeki düzenlemeye göre davaya bakmak yetkisi suçun işlendiği yer mahkemesine aittir. Eğer eylem teşebbüs aşamasında kalmış ise son icra hareketinin yapıldığı, kesintisiz suçlarda da kesintinin yapıldığı yer mahkemesi yetkili olacaktır. Seçimlik hareketli fiiller ile işlenebilen bilişim suçları teşebbüse de müsait suçlardır. Dolayısıyla yer yönünden yetkili mahkemenin tayininde CMK.nun 12. maddenin 1-2. fıkralarının işlerliği farklı olabilecektir.

**TCK. nun 243. Maddesinde düzenlenen bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve orada kalma suçlarında yetkili genel kural gereği suçun işlendiği yer mahkemesi, sistemin tamamına ya da bir kısmına hukuka aykırı olarak girilen yer yani** gerçekleşen fiilin icra edildiği yer mahkemesi olan asliye ceza mahkemesi olacaktır.

Türk Ceza Kanunu'nun 243/1. madde ve fıkrasında belirtilen girme veya kalma eylemleri seçimlik hareketlidir. Sisteme hukuka aykırı olarak girmek veya kalmak suçu oluşumu için yeterlidir. Bu nedenle **CMK. nun 12/2 maddesi gereği eylemin sona erdiği yer mahkemesi yetkili olacaktır.**

**TCK. nun 244. Maddesinde düzenlenen suçlar** birden fazla seçimlik hareketi içerdiğinden, engelleme, bozma, veri yerleştirme, veri yok etme veya verileri değiştirme fiillerinin işlendiği yer mahkemesi yer yönünden yetkili mahkemedir.

TCK. nun 243 ve 244. maddelerinde düzenlenen eylemlerin teşebbüs aşamasında kalması halinde ise yine genel kural gereği son icra hareketinin yapıldığı yer mahkemesi yer yönünden yetkili mahkeme olacaktır.

**Bu suçların uluslar arası** alanda işlenmesi halinde ise yer yönünden yetki sorunu Türk Ceza Kanunu'nun 8. Maddesi çerçevesinde çözümlenecektir. Burada da yetki konusunda hem “**suçun işlendiği yer**” hem de “**sonucun gerçekleştiği yer**” esas alınarak genel bir düzenleme yapılmıştır.

Artuk – Gökçen – Yenidünya’ya göre; bilişim sistemine fiziksel temas ile girilmesi halinde eylem nerede yapılmışsa suç orada işlenmiştir. Buna karşılık bilişim sistemine ağ üzerinden erişilmiş ise bu takdirde suçun araç bilişim sisteminin bulunduğu yerde mi, yoksa hedef bilişim sisteminin bulunduğu yerde mi işlendiği tartışılabilir. Hareketin parçaları veya hareket ile netice arasında siyasi ve coğrafi sınır bulunan bu tür suçlara mesafe suçu denilmektedir. Kanımızca burada bilişim suçlarının özellikleri dikkate alınarak suç, hareket, hareketin kısımları ve neticenin gerçekleştirildiği her yerde işlenmiş sayılmalıdır. Böylece bilişim suçlarının cezasız kalması önlenmiş olacaktır. Nitekim TCK.nun 8. maddesinde; “fiilin kısmen veya tamamen Türkiye’de gerçekleşmesi halinde suç, Türkiye’de işlenmiş sayılır” denilerek sınır aşan mesafe suçları basımından ortaya çıkabilecek tartışmalara son vermiştir. Şu halde, gerek içeriden dışarıya (failin ağa bağlandığı bilişim sisteminin Türkiye’de, hedef bilişim sisteminin yurt dışında olması), gerekse dışarıdan içeriye (failin ağa bağlandığı bilişim sisteminin yurt dışında, hedef bilişim sisteminin Türkiye’de olması) mesafe suçları Türkiye’de işlenmiş sayılır<sup>1032</sup>

## İKİNCİ BÖLÜM

### **I.5237 SAYILI TÜRK CEZA KANUNU’NUN 243. MADDESİ**

#### **A.Hukuka Aykırı Olarak Bilişim Sistemine Girme Ve Orada Kalma**

**Madde 243 -(1)** *Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (24.03.2016 tarihli ve 6698 sayılı Kanununun 30. maddesi ile yapılan değişiklikle birinci fıkrada yer alan “ve” ibaresi “veya” olarak değiştirilmiştir)*

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

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

*“(4) 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” (24.03.2016 tarihli ve 6698 sayılı Kanununun 30. maddesi ile maddeye 4. fıkra eklenmiştir)*

#### **Madde Gereği**



*Bilişim sistemlerine karşı suçların düzenlendiği bölümde yer alan bu maddede bilişim sistemine girme fiili suç olarak tanımlanmıştır.*

*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.*

*Maddenin birinci fıkrasında bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili suç hâline getirilmiştir. Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir.*

*İkinci fıkraya göre, birinci fıkroda tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirmektedir.*

*Üçüncü fıkroda, bu suçun neticesi sebebiyle ağırlaşmış hâli düzenlenmiştir. Birinci fıkroda tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.*

*Sistem içindeki bütün soyut unsurlar, fıkroda geçen “veri” teriminin kapsamındadır.*

Bilişim sistemine girmekten kasıt sistemin donanımsal bölümüne girmek değildir. Burada girmekle ifade edilen sisteme erişimdir. “izinsiz erişim” Avrupa komisyonu tarafından bilgisayar sistemleri bir bölümüne ya da tümüne yapılan izinsiz erişimleri tanımlamak için kullanılmıştır.<sup>1033</sup>

5651 sayılı Kanuna dayanarak çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usûl ve Esaslar Hakkında Yönetmelik’in tanımları açıklayan 3/1-e maddesinde ve 01.11.2007 tarihinde yayınlanan İnternet Toplu Kullanım Sağlayıcılar Hakkındaki Yönetmelik’in tanımları belirleyen 3/1-c maddesinde “erişim” kavramı kullanılmış ve erişim her iki düzenlemede de “herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılmasını ifade eder.” şeklinde tanımlanmıştır.<sup>1034</sup>

Yargıtay 8. Ceza dairesinin yerleşik kararlarında belirtildiği gibi "Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden

---

1033 Erdoğan, Dr. Yavuz, Türk Ceza Kanununda bilişim sistemini engelleme bozma verileri yok etme değiştirme suçu, Doktora tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011, s.110

1034 Erdoğan, s.111

virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, “bilgisayara tecavüz”, “kod kırma” ya da “bilgisayar korsanlığı” olarak da tanımlanmaktadır. Bu suç, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.

E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikâyeti üzerine öncelikle erişimi engellenen adresin şikâyetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adresin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolü) numarası sorulmalıdır. Microsoft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde e-mail adresine giriş yapıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli ve loglar üzerinde inceleme yapılmalıdır<sup>1035</sup>

### **1.Korunan Hukuki Yarar**

Bu suçla korunan hukuki yarar karma bir nitelik taşımakla birlikte asıl olan bilişim sisteminin güvenliğidir. Ancak bu suç bilişim sisteminin güvenliği yanında, verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi kişilerin farklı türden çıkarlarını da koruma altına almaktadır. Ancak tüm bunların üstünde ve bunları kapsayacak şekilde yer alan hukuksal değer bilişim sisteminin güvenliğidir.<sup>1036</sup>

Madde ile sistemdeki veriler ele geçirilmeden verilere hukuka aykırı olarak erişim suç haline getirilmiştir. Sisteme erişimin sağlanmasından sonra kişisel verilerin hukuka aykırı olarak

---

1035 Bakınız. Y.8.CD. 11.10.2017 gün, 2016/12839, 2017/11114, 26.03.2009 gün 18190/3058, 07.05.2014 gün 2013/10402, 2014/11836

1036 Doç. Dr. Murat Volkan Dülger, bilişim suçları ve internet iletişim hukuku, Ankara 2015, sh. 348 gül, G, ag, s. 57

ele geçirilmesi durumunda ayrıca TCK. nun 136. maddesinde düzenlenen “verileri hukuka aykırı olarak verme veya ele geçirme” suçu, verilerin sistemden tamamen kaldırılarak ele geçirilmesi durumunda ise TCK. nun 244/2. maddesinde düzenlenen suç gündeme gelecektir.<sup>1037</sup>

## **2.Suçun Unsurları**

### **a.Fail**

Bu suçun faili herkes olabilir. Özgü bir suç değildir. Çünkü madde metninde suçu işleyecek kişi açısından herhangi bir özellik belirtilmemiştir.

Fail kendisi için ya da başkaları için (bilgi sistemine girebilir) suçu işleyebilir.

TCK.nun 246. maddesindeki “bu bölümde yer alan suçların (243, 244, 245) işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükümlenir.” düzenlemesi karşısında fail bir tüzel kişinin temsilcisi ya da onun yararına suç işlese TCK.nun 20. maddesi gereğince tüzel kişiye ceza verilmez, ancak aynı kanunun 60. maddesindeki güvenlik tedbirleri uygulanabilir.

Failin belirlenmesi suçun sübutuna ilişkin bir husus olup failin doğru belirlenmesi, iyi bir soruşturma gerektirir. 8. Ceza Dairesinin bir çok kararında eksik araştırmadan bozma kararı verilirken ilamlarda soruşturmanın ne şekilde yapılması gerektiği de anlatılmaktadır. (Y. 8. C.D. 11.10.2017 gün, 2016/12839, 2017/11114)

### **b.Mağdur**

Mağdur, belirli bir suçla zarara veya tehlikeye uğratılan hak veya çıkarın, suçla korunan hukuksal değerlerin sahibi olan kişidir. Bu suçun mağduru açısından da Yasa metninde bir özellik gösterilmemektedir, herkes bu suçun mağduru olabilir. Bilgi sisteminin güvenliğinin ihlal edilmesiyle çıkarı zarara uğratılan kişi suçun mağduru olmaktadır. Suçun mağdurunun ancak gerçek kişiler olabileceğini kabul eden yazarlar yönünden tüzel kişiler bu suçun mağduru değil suçtan zarar görenidir.<sup>1038</sup> Bununla birlikte bir kişiye ait bilgi sistemine izinsiz olarak girildikten sonra, bir başka kişinin gizli kalması gereken kişisel bilgilerinin elde edilmesi (veri nakli

---

1037 CD.11.02.2014gün, 2012/32093-2014/2779 “...suça konu .....@hotmail.com ve .....@yahoo.com elektronik posta adresleri hesaplarının oluşturulduğu sırada elektronik posta hizmeti veren şirketlere beyan edilen kimlik bilgilerinin ilgili yerlerden tespit edilerek, sanığın eyleminin TCK.nun 136/1. madde ve fıkrasında düzenlenen “kişisel verileri hukuka aykırı olarak verme veya ele geçirme” suçunu oluşturup oluşturmayacağı tartışılmadan yazılı şekilde hüküm kurulması, Yasaya aykırı”

1038 Dülger, age, sh. 359, Yaşar, Osman/Gökçen, Hasan Tahsin/Artuç, Mustafa yorumlu uygulamalı Türk Ceza Kanunu, cilt IV, Adalet Yayınları, Ankara 2010, sh. 6739

olmaksızın) halinde bu kişisel bilgilerin sahibi de TCK.nın 135, 136. maddelerinde tanımlanan suçlar yönünden suçun mağduru olacaklardır.<sup>1039</sup>

8. Ceza Dairesi uygulamasında gerek gerçek kişi gerekse tüzel kişiler suçun mağduru olarak tanımlanmaktadır.<sup>1040</sup>

### **c. Suçun Konusu**

Birinci fıkrada düzenlenen suçun hukuki konusu içine girilen ve kalınan bilişim sisteminin kendisidir. Üçüncü fıkrada düzenlenen suç açısından bilişim sisteminde yer alan verilerdir. İkinci fıkrada düzenlenen cezayı hafifletici hal için ise suçun konusu bedeli karşılığı yararlanılabilen verilerdir.

Burada dikkat edilmesi gereken husus; TCK.nun 243/3. madde ve fıkrasındaki hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.

### **d. Eylem**

Suçun oluşabilmesi için “*hukuka aykırı olarak girme ve orada kalmaya devam etme*” eyleminin birlikte gerçekleştirilmesi gerekmekte iken TCK’nun 243. maddesinin 1. fıkrasında 24.03.2016 tarihli ve 6698 sayılı Kanunun 30. maddesiyle yapılan değişiklikle birinci fıkrada yer alan “*ve*” ibaresinin madde gerekçesine uygun olarak “*veya*” şeklinde değiştirilmesi üzerine suç seçimlik hareketli hale gelmiştir.

Daha önce Yargıtay uygulamalarında girme aynı zamanda kalmayı da içerir, suçun oluşması için bir zarar meydana gelmesine ya da bir menfaat sağlanmasına gerek yoktur. Zaten bu soyut tehlike suçudur. Bu nedenle bir milisaniye bile kalırsa suç oluşur şeklinde bir yaklaşım vardı. Başka bir anlatımla failin sisteme girdiğini fark etmesiyle derhal çıkmaması durumunda suçun işlendiği kabul edilmekteydi.

Yeni düzenleme ile eylem seçimlik hareketli hale geldiğine göre “*orada kalmaya devam etme*” eyleminin oluşabilmesi için belirli bir süre aranacak mı?

Bilişim sistemine hukuka aykırı olarak girme veya orada kalma eylemlerinin gerçekleşmesi için sistemde ne kadar süreyle kalınacağı konusunda kanunda bir açıklık yoktur. Ancak suçun soyut tehlike suçu olması ve sisteme hukuka aykırı olarak girme veya kalma sonucunda bir zararın doğması ya da bir yarar sağlanması gerekli olmadığından, sisteme hukuka aykırı olarak girilmesi veya sisteme girildikten sonra bir milisaniye dahi kalınması halinde dahi suç oluşacaktır. Sistemde

---

1039 Erdoğan, age, s.116

1040 8. CD. 19.03.2018, 2494-2967 18.01.2018, 22781-560

kalma süresinin herhangi bir işlem yapmaya elverişli olması gibi bir zorunluluk ta yoktur. Çünkü bu sırf hareket suçudur.

Eylem olarak gösterilen “girme” ve “sistemde kalma” kavramlarından anlaşılması gerekenin “erişim” olarak tarif edilen eylem olduğundan Yargıtay kararlarında da bu kavram kullanılmaktadır. (bknz. Ekli kararlar 3,4,5,7) Ayrıca fail bilişim sistemine hukuka uygun olarak girip izni bittikten sonra hukuka aykırı olarak kalmaya devam etmesi durumunda da TCK.nun 243/1. maddesindeki suç oluşacaktır.

#### **e. Suçun (Cezayı Hafifletici) Nitelikli Hali**

TCK 243. maddesinin 2. fıkrasında, hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma eylemlerinin, “bedeli karşılığı yararlanılabilen sistemler” hakkında işlenmesi cezayı hafifletici bir neden olarak öngörülmüştür.<sup>1041</sup> Buna göre, maddenin 1. fıkrasında tanımlanan fiillerin, bedeli karşılığı yararlanılan sistemler hakkında işlenmesi indirim nedenini oluşturmaktadır.

Gerek madde metninde gerekse de gerekçede bedeli karşılığında yararlanılan sistemin ne olduğu konusunda bir açıklamaya yer verilmemiştir. Ancak bedeli karşılığında yararlanılan sistemlere internet üzerinden ücret karşılığı hizmet veren web siteleri, oyun siteleri vb. örnek olarak gösterilebilir<sup>1042</sup>. Bunların hepsinde kişiler belli bir bedel karşılığı bir bilişim sistemine girip sistemin kendisinden ya da sağladığı hizmetlerden yararlanmaktadır. Kanunda geçen bu kavramdan anlaşılması gereken TCK.nun 163. maddesinde yazılı ve karşılıksız yararlanma suçunun konusunu oluşturan otomatlar değildir.<sup>1043</sup>

#### **f.Suçun Neticesi Sebebiyle Ağırlaşmış Hali**

TCK.nun 243. maddesinin 1. fıkrasındaki suçun kasten işlenmesi sonucunda; istenmediği halde (yani sonuç yönünden kastı bulunmaksızın) bilişim sisteminin içerdiği verilerin yok olması ya da değişmesi hali 3. fıkrada suçun neticesi sebebiyle ağırlaşmış hali olarak düzenlenmiştir. TCK.nun 23. maddesi de gözetildiğinde burada sonuç yönünden sanığın en azından taksirinin bulunması aranmaktadır. Fıkradaki sonuçlar sadece “verinin yok olması” ve “verinin değişmesi” ile sınırlı tutulmuştur. Elbette bu netice sebebiyle ağırlaşma hali, diğer iki fıkra için de

---

1041 1-Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması,

2-Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması gerektiğinin gözetilmemesi, Y.8. CD.08.01.2014. 2012/33044- 2014/236.

1042 Bozma sebepleri, s.833

1043 Gül, age, s.64

geçerlidir.<sup>1044</sup> 8. Ceza Dairesinin uygulamasında TCK.nun 61/4 maddesi uyarınca önce TCK.nun 243/3. maddesindeki nitelikli halden temel ceza belirlenip daha sonra aynı maddenin 2. fıkrasına göre indirim yapılacaktır.

### **3.Suçun Manevi Unsuru**

TCK.nun 243/1. maddesinde düzenlenen bilişim sistemine girme veya sistemde kalmaya devam etme suçu kasten işlenebilen bir suçtur. Failin bilişim sistemine izinsiz/yetkisiz girdiğini bilmesi yeterlidir. Taksirle işlenebileceğine dair bir düzenleme bulunmadığı için suçun taksirle işlenmesi mümkün değildir. Ancak, bilişim sistemine girme ve sistemde kalmaya devam etme eylemi sırasında sistemin içerdiği veriler yok olur veya değişirse bu durumda aynı Yasanın 243/3. maddesindeki düzenleme akla gelecektir. Yasa maddesinin bu fıkrasındaki eylemin gerçekleşmesi için kast aranmaz. Failin hukuka aykırı olarak sisteme girmesi ve kalması sırasında istemeyerek sisteme ve verilere zarar verilmesi durumunda bu hüküm uygulanacaktır. Örneğin sanığın bir bilişim sistemine hukuka aykırı olarak girmesi veya orada kalmaya devam etmesi sırasında istemeyerek sistemdeki verilere zarar vermesi gibi.

Bu nedenle maddenin 3. fıkrasında düzenlenen eylemde kast yoktur, kastın aşılması söz konusu olacaktır. Yani failin sisteme zarar verme amacı yoktur. Eğer fail sisteme hukuka aykırı ya da uygun olarak girdikten sonra isteyerek bir zarar verirse bu durumda TCK. nun 244/2. maddesi gündeme gelecektir.

Bu fıkranın uygulanabilmesi için failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir. Yoksa fail, verileri bilerek ve isteyerek yok ederse TCK'nın 244/2. maddesindeki suç oluşacaktır.

### **4.Hukuka Aykırılık Unsuru**

TCK'nun 243. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalmaya devam etme suçu açısından söz konusu olabilecek hukuka uygunluk nedenleri, TCK. nun 24/1. maddesinde düzenlenen “kanunun hükmünü yerine getirme” ve TCK. nun 26/3. maddesinde düzenlenen “ilgilinin rızası”dır.<sup>1045</sup> Rıza ancak hak sahibi olan kimse tarafından verilebilir<sup>1046</sup>. Örneğin bir soruşturma gereği bilişim sistemine girilmesi durumunda eylem suç teşkil etmeyecektir.

---

1044 Aksi görüş için bkz. Dülger, age, s. 360

1045 Dülger, age. s.390.391, Yaşar/Gökçen/Artuç, age s.6746

1046 Dülger, age, s.391

Rıza, hukuka aykırılığı ortadan kaldırır. Ancak, rızanın suçun işlendiği sırada var olması gerekir. Fiil sonrasındaki şikâyetçi olmama, suçu ortadan kaldırmaz.

## **5.Suçun Özel Görünüş Şekilleri**

### **a.Teşebbüs**

Birinci fıkrada belirtilen bilişim sistemine girme ve sistemde kalma hareketlerinin yapılmasıyla suç tamamlanmış olacaktır. Bu fıkrada düzenlenen suç için ayrıca bir netice (zarar) aranmamıştır. Birinci fıkrada düzenlenen suça teşebbüs mümkündür. Şöyleki; sisteme girmek için gerekli icrai hareketlerin başlamasına rağmen girme veya kalma eyleminin gerçekleştirilememesi halihde teşebbüs hükümleri uygulanabilecektir. Zira sisteme girilmek istenirken internet bağlantısının kesilmesi, elektriğin kesilmesi veya şifreli bir sitem için şifrenin çözülememesi gibi durumlarda eylemin teşebbüs aşamasında kaldığından bahsetmek mümkün olacaktır.

6698 sayılı Yasa ile yapılan değişiklik öncesi ancak bilişim sistemine girildikten sonra sistemde kalma fiili temadi niteliğinden dolayı bu fiil yönünden suçun teşebbüse elverişli olmadığı ile sürülebilir<sup>1047</sup> ise de söz konusu yasa ile “ve” ibaresi “veya” olarak değiştirildikten sonra bu suça teşebbüs imkansız hale gelmiştir. Bunun yanında TCK. nun 243/3. maddesinde düzenlenen suçun neticesi sebebiyle ağırlaşmış hali yönünden ise teşebbüs olanaklı değildir.

### **b. İştirak**

Madde metninde özel bir iştirak hükmüne yer verilmemiştir. Bu nedenle suçlara iştirak açısından bir özellik söz konusu olmayıp TCK.nun 37., 38., 39. ve 40. maddelerindeki suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir. Bu suçlara iştirak her zaman mümkündür.

### **c. İçtima**

Bu suçların zincirleme şekilde işlenmesi mümkündür. Bilişim sistemine hukuka aykırı olarak girme ve orada kalma eylemi içerisinde bir süreklilik mevcuttur. Kalma eyleminin devam etmesiyle eylem gerçekleşmiş olacaktır. Suç zorunlu olarak bir mütemadi suçtur. Ancak fail sisteme girdikten sonra çok uzun süre kalır ve kalmaya devam ederse ne olacaktır? Zincirleme suç hükümleri uygulanacak mı? Sorunu gündeme gelmektedir. İşte failin bilişim sisteminde kalmasıyla temadi gerçekleşmiş olacağından fail hakkında zincirleme suç hükümlerinin uygulanma olanağı yoktur. Bu durumda TCK. Nun 3. ve 61. maddeleri uyarınca Hâkim madde metninde öngörülen cezanın alt ve üst sınırlarına göre bir ceza tayin edebilecektir.

---

1047 Dülger, age.

TCK.nun 43. Maddesinde düzenlenen zincirleme suç hükümlerinin uygulanması failin aynı suç işleme kararıyla bir bilişim sistemine farklı zaman dilimlerinde girmesi ve sistemde kalmaya devam etmesi halinde mümkün olacaktır. Örneğin sanık bir bilişim sistemine kısa aralıklarla birden çok girip orada kalır ve çıkarsa bu durumda faile verilecek cezanın TCK.nın 43. maddesi uyarınca arttırılarak verilmesi gerekir. Ancak fail aynı suç işleme kararından bahsedilemeyecek kadar uzun aralıklarla sisteme giriyor ve orada kalmaya devam ediyorsa bu durumda failin aynı suç işleme kararıyla hareket ettiği söylenemeyecek ve her eylem için ayrı ceza verilip cezaların içtimalı kuralı uygulanacaktır. <sup>1048</sup>

Failin eyleminin hem suçun nitelikli halini, hem de neticesi sebebiyle ağırlaşmış halini ihlal etmesi durumunda, yani bedeli karşılığı hizmet veren bir bilişim sistemine yetkisiz girip veya orada kalmaya devam ederken taksirli bir hareketiyle sistemde yer alan bazı verilerin yok olmasına ya da değişmesine neden olursa Yargıtay 8. Ceza Dairesi (suçun TCK.nun 243/2. maddesindeki nitelikli halinin işlenmesi sonucunda 3. fıkradaki neticenin oluşması halinde) her iki fıkranın da uygulanmasına karar vermektedir. Yani 3. fıkra göre belirlenecek cezadan 2. fıkra göre indirim yapılacaktır.

Bilişim sistemine hukuka aykırı olarak girme ve orada kalma eylemi açısından öne çıkan en önemli sorunlardan birisi, bir bilişim sistemine girilerek TCK. nun 244. maddesindeki “sistemi engelleme, bozma, verileri yok etme veya değiştirme” suçunun işlenmesi durumunda ayrıca TCK. nun 243/1. maddesi uyarınca da ceza tayin edilip edilmeyeceğidir. Ancak TCK. nun 244. maddesindeki eylem, TCK. nun 243/1. maddesinde tanımlanan eylemi de içerdiğinden TCK.nun 44. maddesi uyarınca yalnızca TCK.nun 244. maddesi uygulanacaktır. <sup>1049</sup> Ancak 244. maddedeki eylemlerin gerçekleşmesi için bilişim sistemine girmeye veya kalmaya mutlaka gerek yoktur. <sup>1050</sup>

Fail TCK.nın 244/2. maddesindeki seçimlik eylemlerden birini gerçekleştirmek kastıyla değil de sadece sisteme girip kalmak maksadıyla girmiş, ancak sonradan 244/2. maddede belirtilen hareketlerden birini (kasten) gerçekleştirmiş (örneğin: e-postalarına bakmak için girmiş ancak şifreyi değiştirmiş) ise bu durumda eklenen kast nedeniyle TCK.nın 244/2. maddesiyle cezalandırılacaktır. <sup>1051</sup>

---

1048 ”sanığın tespit edilen IP ile suç tarihinde bir kez girdiği ve kaldığı anlaşılmasına rağmen hakkında zincirleme suç hükümleri uygulanarak fazla ceza tayini” 8. C.D. 17.05.2017, 2016/9971, 2017/5660 bkz, benzer; 8. C.D. 04.06.2014, 2014/3984-13848,

1049 (Aksi görüş için bkz, Dülger, age, s...)

1050 (Gül, age, s. 87)

1051 (Gül, age, s. 87, aksi görüş için Dülger, age, s. 406,407)



8. Ceza Dairesi katılana ait ...hotmail.com internet adresinin ve Facebook hesabının fail tarafından şifrelerinin kırılmak suretiyle girip sonra da şifreyi değiştirerek sahibine karşı bilişim sisteminin erişilmez kılındığı takdirde TCK.nun 244/2. aksi takdirde aynı Yasanın 243/1. maddesi kapsamındaki suçun oluşacağına karar vermiştir. <sup>1052</sup>

Ayrıca TCK.nun 244/1 ve 2. fıkralarındaki suçların fail tarafından ayrı ayrı ihlal edilmesi, iki suçun da ayrı ayrı işlenmesi de mümkündür.<sup>1053</sup>

## 6.Yaptırım

TCK. nun 243/1. maddesinde düzenlenen bilişim sistemine girme ve sistemde kalma suçunu işleyen failer için “*bir yıla kadar hapis veya adli para cezası*” öngörülmüştür. Bu cezalar seçimlik olarak düzenlendiği için iki cezanın birlikte verilmesi mümkün değildir; fail hakkında gerekçesi gösterilerek ya hürriyeti bağlayıcı ceza ya da adli para cezasına karar verilecektir.

Adli para cezasının tercih edilmesi halinde ceza miktarı TCK.nun 52. maddesinde gösterilen miktara göre beş günden az ve yediyüzotuz günden fazla olmamak üzere belirlenecektir. Ancak 5237 sayılı TCK.nun 61/9. maddesinin yürürlüğe girdiği 19.12.2006 tarihinden önce işlenen suçlarda 5 gün, bu tarihten sonra işlenen suçlarda ise 30 gündür. Adli para cezasının üst sınırı da 19.12.2006 tarihinden önce işlenen suçlarda 730 iken, bu tarihten sonra işlenen suçlarda 365 gündür<sup>1054</sup>.

Bu suç açısından 2. fıkrada belirtilen cezayı hafifletici nitelikli halin gerçekleşmesi halinde yukarıda belirtilen cezalar yarı oranına kadar indirilecektir.

243. maddenin 3. fıkrasında belirtilen suçun netice sebebiyle ağırlaşan halinin gerçekleşmesi halinde ise faile verilecek ceza altı aydan iki yıla kadar hapis cezası olacak ve bu durumda faile hürriyeti bağlayıcı ceza yerine adli para cezası verilemeyecektir.

## B- VERİ NAKİLLERİNİ İZLEME (TCK. m. 243/4)

07.04.2016 tarihinde Resmi Gazetede yayımlanarak yürürlüğe giren 24.03.2016 tarihli ve 6698 sayılı Kanunun 30. maddesi ile maddeye eklenen 4. fıkraya göre “*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*”

6698 sayılı Kişisel Verilerin Korunması Kanununun Adalet Alt Komisyonu’nda yapılan görüşmesi sonucu düzenlenen raporda “Sanal Ortamda İşler Suçlar Sözleşmesi’nin 3. maddesiyle

---

1052 (Y. 8. C.D. 18.11.2015, 2015/7531-24704)

1053 (Gül, age, s. 88)

1054 Yaşar/Gökçen/Artuç, age. s.6752

üye ülkeler yasa dışı araya girme eylemini cezalandırmaya davet edildiğinden 5237 sayılı Kanunun 243. maddesinde değişiklik öngörülmüştür. Böylece bilişim sistemlerinin bütününe veya bir kısmına hukuka aykırı olarak girmekle birlikte belirli bir süre kalmak da suçun unsuru olarak düzenlenmiş olmasına rağmen sözleşmeye uyum amacıyla sadece sisteme/sistemlere girmek fiili suç olarak düzenlenmektedir. Verilerin izelenmesi eylemi, bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesini ifade etmektedir. Bütün elektronik veri transferleri, bu çerçevede korunması amaçlanan veri transferinin gizliliği kapsamında kalmaktadır. Yasa dışı araya girme eylemleri, temelde bilişim sistemlerine girmeksizin işlenen fiillerdir. Bu doğrultuda sözleşmeye uyum amacıyla yine aynı maddenin 1. fıkrasının hüküm eklemek suretiyle, bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla izleyen kişinin 6 aydan 3 yıla kadar hapis cezası ile cezalandırılması öngörülmüştür.

Bu fıkra hükmüne göre fail sisteme girmeksizin bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini teknik araçlarla hukuka aykırı olarak izlenmelidir.

Bu fiil yönünden de mağdur ve fail yönünden bir ayırım yapılmamış olup, mağdur veya fail herkes olabilir. Suçun, hukuka aykırılık, kusurluluk, özel görünüş şekilleri yönünden birinci fıkradaki fiil ile ilgili yapılan anlatımlar geçerlidir. Eylem ile bir yarar sağlanması öngörülmemiş, tehlike suçu olarak düzenlenmiştir. Suç, kasten işlenebilen bir suçtur. Suçun konusu bilişim sistemleri arasında ya da aynı bilişim sisteminde nakledilen verilerdir.

Bu fıkraya göre öncelikle;

1- Öncelikle bilişim sisteminin kendi içinde veya bilişim sistemleri arasındaki veri nakilleri suçun konusu olabilecektir.

2- Sisteme girmeksizin eylem gerçekleştirilmelidir.

3- Eylem teknik araçlarla izleme şeklinde gerçekleştirilmelidir.

4- İzleme hukuka aykırı olarak yapılmalıdır. Mahkeme kararı gibi hukuka uygunluk nedenleri söz konusu ise maddedeki suçtan söz edilemeyecektir.

Bu izleme ile başkalarına ait kişisel verilerin ele geçirilmesi ya da özel hayatın gizliliğinin ihlal edilmesi durumunda TCK'nın 134, 135 ve 136. maddelerinin uygulanması gündeme gelecektir<sup>1055</sup>.

---

1055 Gül, age, s. 65, 66

## **C- SORUŞTURMA VE KOVUŞTURMADA DİKKAT EDİLMESİ GEREKEN HUSUSLAR**

Öncelikle belirtmek gerekir ki bilişim teknolojisi ve üretilen zararlı yazılım ve teknikler paralelinde değişen hukuki normlar ve mevzuat ile uygulamaya konulan stratejilerin birbirleriyle uyum ve ahenk içerisinde olmaması tehditlerle mücadelede kaynakların israf edilmesine ve gerekli önlemlerin etkin ve verimli olarak alınmamasına neden olmaktadır<sup>1056</sup>.

8. Ceza Dairesinin 11.10.2017 gün, 2016/12839, 2017/11114 sayılı ve bir çok kararında belirtildiği üzere; bilişim suçlarından deliller büyük oranda soruşturma aşamasında toplanabildiğinden ve bu deliller ışığında bir sonuca varıldığından kovuşturma aşamasında yeni bir delil-bilgi temin edilebilmesi genellikle çok zor ya da imkansızdır. Bu nedenle soruşturma aşamasında toplanamayan deliller nedeniyle yargılama aşaması genellikle “delil yetersizliğinden beraat kararları” ile sonuçlanmaktadır. Sanal ortamda işlenen bu suçların delillendirilmesi oldukça güç olduğundan en önemli ve güvenilir delil dijital materyaller üzerinde yapılacak inceleme ve failin eylemi kabul etmesidir. Sanığın ikrarı az rastlanan bir durum olduğundan suça konu sistem üzerinde yapılacak inceleme son derece önemlidir<sup>1057</sup>.

### **1. Müştekinin Kontrolünde Olan Sisteme Girme İddiası**

Müştekinin kurulu bulunan sisteme yönelik eylem gerçekleştirildiğini iddia etmesi durumunda; öncelikle bu sistemin server (ana sunucu bilgisayar) üzerinde adli bilişim uzmanlarınca inceleme yapılması ve yetkisiz erişim olup olmadığı, oluşturma sisteme düşen IP adresi, URL adresi tespit edilmeye çalışılmalıdır. Keza server üzerinde tüm bilgilerin saklandığı ve diğer bilgisayarlara oranla daha hızlı ve kapasitesi yüksek bilgisayarlardır. İnceleme sonucu sisteme yetkisiz erişim, IP ve URL adresi tespit edildiğinde ilgili servis sağlayıcısından bu adres kullanıcısı internet abonesinin tespitine çalışılacaktır.

CMK 234. maddesinde yazılı mağdurun hakları ve CMK 161. maddesinde yazılı cumhuriyet savcılarının yetkileri çerçevesinde bu incelemenin yapılabilmesi için herhangi bir şekilde el koyma ya da inceleme kararına gerek yoktur. Ancak incelemenin delil değeri için müşteki tarafından değil, görevlendirilmiş adli bilişim uzmanları ya da bilirkişiler tarafından yapılması gereklidir.

---

1056 Efe, Dr. Ahmet, Bilişim Hukuku ile Uluslararası Hukuk Kesişiminde Yeni Bir Paradigma: Siber Yönetişim, Türkiye Noterler Birliği Hukuk Dergisi, Ankara, 2017, yıl:4 sayı:2 s.157  
1057 Gül, age, s. 70

Uygulamada bu inceleme işlemleri uzun süre (aylar, bazen yıllar) aldığından, bu süreçte ilgili kurum, şirket ya da kişiler sistemi kullanamamaları nedeniyle mağdur olacağından sisteme yeni program yükleyip (formatlayıp) kullanmaya devam etmekte, sistem üzerindeki deliller elde edilememektedir. Neticede iddia edilen bir eylem ve dilleri olup olmadığı, iddianın inandırıcılığı tespit edilemeyeceğinden kovuşturmayaya yer olmadığına dair karar verilecektir. Bunu engellemek maksadıyla topyalama, imaj alma yöntemleri izlenebilir. Yaşanan gecikmeler, yeterli sayı ve bilgi düzeyinde adli bilişim uzmanlığının önemini göstermektedir.

İnceleme yapılması için gerekli dijital materyaller (bilgisayar, cep telefonu, tablet, el bilgisayarı, dijital kamera ve fotoğraf makinesi, hard disk, flash gibi) şüphelenilen failde ise şartlar oluşması durumunda CMK 134. maddesinde yazılı arama, kopyalama ve el koyma yollarına başvurulacak, bu konuda sul hceza hakimliğinden karar alınacaktır. İnceleme sonucunda, veri saklamaya yarayan hard disk ve kullanıcının seyir defterini gösteren log kayıtları üzerinde yapılan inceleme son derece önemlidir. Bilgisayarlar arasında veri akışı olup olmadığı ayrıntılı bir şekilde belirlenmelidir.

Yetkisiz erişim sağlandığı iddia edilen sistem bir bankaya ait ise, ilgili bankadan bir yazı ile inceleme sonucu elde edilen tüm bilgiler istenebilir.

Sisteme erişim sırasında tespite düşen IP adres bilgileri, sisteme ne şekilde girildiği, bu sistemden başkasına yarar sağlanıp sağlanmadığı, bilgi temin edilip başka yerde kullanılıp kullanılmadığı, sisteme zarar verilip verilmediği, TCK.nun243. maddesinde yazılı suçlar harcinide başka suçların ayrıca oluşup oluşmadığını tespit bakımından önemlidir. Tespit edilecek IP adresi kullanıcıları bilgileri hızlı bir şekilde internet servis sağlayıcılarından (Türk Telekom, Aevea, Turkcell, Vodafone vs.) temin edilmelidir<sup>1058</sup>.

## **2. Müştekinin Kontrolü Dışındaki Sisteme Yetkisiz Erişim**

Bu iddialar genellikle e-posta hesabına izinsiz (şifre kırılarak girilmesi) sosyal paylaşım sitesi (facebook, twitter, instagram gibi) şifresinin kırılıp girilmesi, bu hesaplar üzerinden üçüncü kişilerin dolandırılması, yazışmalar yapılması, resimlerin paylaşılması ve hesaptan temin edilecek resim ya da kişisel bilgilerle hesap açılması şeklinde olabilmektedir.

Bu durum genellikle TCK.nun 243. maddesi dışındaki (TCK. 244, 158/1-f, 134, 135, 136 maddelerindeki suçlar gibi) suçları gündeme getirmekte ise de; eylemin niteliği ve ne şekilde gerçekleştiğinin tespiti için aynı yöntemin izlenmesi gerekecektir.

---

1058 Gül, age, s. 70,71,72

E-posta hesabına izinsiz girilerek bu hesap ile bağlantılı sosyal paylaşım sitesine girme eylemini araştırırken e-posta adresine müşteki harici erişim sağlanıp sağlanmadığı, ilgili şirket (Microsoft Corporation gibi) temsilciliğinden sorularak erişim sağlayan IP adres bilgileri temin edilebilecektir. Ancak ülke içinde temsilciliği olmayan şurt dışı kaynaklı servis sağlayıcısı ([www.gmail.com](http://www.gmail.com), [www.yandex.com](http://www.yandex.com), googlenin e-posta hizmet servisi, yahoo.com gibi) söz konusu olduğunda IP adresi bilgilerinin tespiti için istinade yoluna başvurulacaktır. Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün web sitesinde duyurduğu üzere, özellikle şirket merkezi ABD olan gmail.com'dan bilgi temini oldukça zor şartlara bağlı olmakla beraber, yabancı bir ülkenin kontrolündeki şirket verileri olarak iletilebilecek bilgilerin güvenilirliği/delil değerinde ayrı bir tartışma konusudur.

Aynı şekilde facebook, twitter, instagram gibi Amerikan menşeli sosyal paylaşım sitelerinden sisteme erişim sağlayan IP adreslerinin temini birinci kısımda değinildiği gibi oldukça sıkı şartlara bağlanmıştır.

Sadece hesabım çalındı, kişisel bilgilerin, fotoğraflarım paylaşıldı, hakaret edildi, arkadaşlarım hesabım üzerinden dolandırıldı gibi iddialarla IP adresinin tespiti mümkün olmadığından, dolayısıyla iddiaların doğruluğu araştırılıp sonuçlandırılmayacağından, soruşturma yapma imkanı olmadığından müracaatlar sonuçsuz kalacaktır. Ancak insan ticareti, çocuk pornosu, uyuşturucu ticareti gibi tüm dünyada hassasiyet gösterilen suçlarda Türkiye temsilcilikleri aracılığıyla bilgi paylaşımı yapılmakta, hassas davranılmaktadır.

### **D-TCK. NUN 243. MADDESİ İLE İLGİLİ YARGITAY KARARLARI**

1.Sanığın soruşturma aşamasında müdafii huzurunda alınan beyanında katılan şirketten ayrıldıktan sonra katılan şirkete ait bilgisayar programına girdiğini kabul etmesi ve değişik zamanlarda bu programa girdiğinin dosya içerisindeki belgelerden anlaşılmış olması karşısında, sanığın oluşan eylemi nedeniyle bilişim sistemine izinsiz girme suçundan TCK.nun 243, 43. maddeleri gereğince cezalandırılması yerine dosya içeriğiyle uyuşmayan gerekçelerle beraat kararı verilmesi, (Y.8.CD. 04.06.2014 gün, 2014/3984-2014/13848)

2."Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir. Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Bilgisayar veri ve sistemlerine

yapılan izinsiz giriş, aynı zamanda, “bilgisayara tecavüz”, “kod kırma” ya da “bilgisayar korsanlığı” olarak da tanımlanmaktadır. Bu suç, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine (windows, linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır.

E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikayeti üzerine öncelikle erişimi engellenen adresin şikayetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adresin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolü) numarası sorulmalıdır. Microsoft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde e-mail adresine giriş yapıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli ve loglar üzerinde inceleme yapılmalıdır.

Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şikayetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.

Şikayetçiye ait e-mail adresine veya ele geçirilen adresten başkalarına, görüntü, yazı veya ses kaydı gönderildiğinin iddia olunması halinde ise, bu husus/hususlar üzerinde durularak gerekli tespitler yapıp örnekleri de alınarak dosya içine konulmalıdır.

Şikayetçi ve şüphelilerin bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak görüntü ve yazı gönderilerek ulaşılan adres sahipleri tanık olarak dinlenmelidir.

Somut olayda; katılana ait .....@hotmail.com internet adresine sanık tarafından şifresinin kırılması yoluyla MSN adresine girilerek kullanılamaz hale getirildiği iddiasıyla açılan davada, sanık E.A'ya ve başka kişilere ait IP numaraları ile katılanın E-Mail hesabına giriş yapıldığının tespit edildiği, bu haliyle eylemin TCK.nun 243/1. Maddesi kapsamındaki suçu

oluşturacağı, ancak katılanın girişinin 04.05.2010 tarihi itibarıyla engellendiğini iddia etmişse de buna ilişkin bir tespite rastlanmadığının anlaşılması karşısında; anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit olunmamıştır. Sanık tarafından giriş yapıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığının ilgili internet sağlayıcısından sorulmadığı anlaşılmıştır.

Bu itibarla yukarıda açıklanan yöntem izlenerek eksiklikler yerine getirilip sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, (Y.8.CD. 07.05.2014 gün, 2013/10402- 2014/11836)

**3-Sanığın katılan şirkette çalıştığı sırada kendisine görevi nedeniyle verilen internet şifresini, iş yerinden ayrıldıktan sonra hakkı bulunmadığı halde kullanmak suretiyle katılan şirkete ait bilişim sistemine girdiği ve orada kalmaya devam ettiğini iddia ve sanığmda bu iddiayı doğrulayan katılan şirkete ait bilişim sistemine hükümsüz kalan şifresi ile girip, buradaki şirket çalışanlarına ait maillerin kendi kurduğu siteye yönlendirmesini yapabilecek kadar süre ile kaldığını savunması karşısında; yüklenen TCK'nun 243/1. maddesindeki suçun bir bilişim sistemine hukuka aykırı olarak girmek ve orada kalmaya devam etmek unsurlarının gerçekleştiğinin kabulü ile mahkumiyetine karar verilmesi yerine yazılı şekilde beraatine hüküm kurulması, Y. 11. CD. 19.03.2012. 2009/22385-2012/3683.**

**4-Sanığın, katılanın yetkilisi olduğu ..... Tekstil Şirketinin Türkiye Ekonomi Bankası Denizli şubesinde bulunan hesabına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı TCK.nun 243/1. maddesinde düzenlenen suç oluşturduğu gözetilmeden yazılı şekilde (5237 sayılı TCK.nun 244/4, 35/2. maddeleri gereğince) hüküm tesisi, (Y.11.CD., 26.03.2009, 18190/3058)**

**5- "... şifre değiştirildiğine ilişkin deliller tespit edilip değiştirilmediğinin tespiti halinde sanığın sadece bilişim sistemine giriş yaptığı ve kalmaya devam ettiğinin belirlenmesi halinde eyleminin TCK.nın 244/2. maddesinde düzenlenen suç değil aynı Kanunun 243/1. maddesi kapsamındaki suç oluşturacağı..." (Y. 8. C.D. 13.04.2017 gün, 2016/8243, 2017/4158)**

**6- ...şikayetçinin adresine girişinin engellendiğine dair bir tespitin bulunmaması karşısında; şikayet tarihinden önce Facebook adresinin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı araştırılarak ve şifrenin değiştirilip değiştirilmediği, değiştirilmişse**

hangi tarihte ve hangi IP numarasından sağlanan erişim sonucu değiştirildiği ilgili internet sağlayıcısından ve Facebook şirketinden sorulup erişilmez kılındığı takdirde TCK.nın 244/2 aksi takdirde aynı Yasanın 243/1. maddesi kapsamındaki suçu oluşturacağı... (Y. 8. C.D. 2015/11993, 2016/3544)

**7-** ...gelen yazı cevaplarında şikayetçinin girişinin ne şekilde engellendiğine ilişkin bir tespite rastlanmadığının anlaşılması ve tüm dosya kapsamında, sanığın eyleminin TCK.nın 243. maddesi kapsamında değerlendirilmesi gerekirken... (Y. 8. C.D. 17.01.2018 gün, 2017/23248, 2018/501)

**8-** ...şikayetçinin hesabına sanığın giriş yaptığının tespit edildiği ancak dosya içerisinde e-mail şifresinin değiştirilmesine dair bir tespitin bulunmaması karşısında, sanığın sadece giriş yaptığı ve kalmaya devam ettiği anlaşılmakla eyleminin TCK.nın 243/1. maddesi kapsamındaki suçu oluşturacağı gözetilmeden... (Y. 8. C.D. 07.02.2018 gün, 2017/25385, 2018/1217)

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

E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikayeti üzerine öncelikle erişimi engellenen adresin ve sanığa ait olduğu iddia olunan e-mail adresinin sanığa ve şikayetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adreslerin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (İnternet Protokolü) numarası sorulmalıdır. Microsoft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde şikayetçinin e-mail adresine giriş yapıp yapmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler



itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli, aynı şekilde sanığa ait olduğu iddia olunan e-mail adresini kullanan IP numaraları saptanıp adres ve telefon bilgileri de istenmelidir.

Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şika- yetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.

Şikayetçi ve sanığın bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp ele geçirilen adresten bir başka adrese yazı veya görüntü gönderilmiş ise, bu olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak ulaşılan adres sahipleri varsa tanık olarak dinlenmelidir.

Somut olayda; sanığın, şikayetçinin kullandığı ".....@hotmail. com" e-posta adresi ile irtibatlı olan facebook adresine bilgisi ve rızası olmaksızın şifreyi değiştirerek erişilmez kıldığından bahisle açılan davada, yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan hüküm kurulmuştur. Sanığın suçlamayı kabul etmediği gibi hattına başkalarının girmiş olabileceği savunmasına ilişkin olmak üzere internet hattını sanık dışında başkalarının da kullanıp kullanmadığı ve kendisine ait olduğu belirtilen e-mail adresinin sanığa aidiyeti hususunda dosyada bir bilgiye rastlanmamıştır. Şikayetçinin 05.12.2012 tarihinden itibaren e-mail adresine giremediğini belirttiğinin anlaşılması karşısında, anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit edilmemiştir. Sanık tarafından suç tarihinden sonra giriş yapıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulmadan hüküm kurulmuştur.

Bu itibarla; yukarıda açıklanan yöntem izlenmeden yapılan soruşturma ve kovuşturma sonucu aradan geçen sürede dikkate alındığında bu eksikliklerin yerine getirilmesi imkansız hale gelmiş olmakla tebliğnamedeki bozma düşüncesine iştirak edilmemiştir.(Y. 8. C.D. 11.10.2017 gün, 2016/12839 - 2017/11114)

**10-** ...arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı elektronik posta adersine rızası dışında birçok kez girdiği olayda, sanığın, bu şekildeki eyleminin TCK.nın 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu ve mahkemenin hükmün gerekçesinde de eylem bu şekilde kabul edildiği halde, sanık hakkında bilişim sistemine girme suçu

yerine, TCK.nın 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan hüküm kurulmak suretiyle sanık hakkında fazla ceza tayini, (Y. 12. C.D. 13.01.2016 gün, 2015/15933, 2016/277)

**11-** Katılan Şirketin sahibi olduğu web sitesi, müşterilerine ilan yapmaya kullanıcılarına da bu ilanları görmelerine imkan sağlayan dolayısı ile bu ilanlar üzerinden de karşılıklı iletişim sağlanarak alışveriş imkanı yaratan hizmet kolunda faaliyet gösterdiği ve kendisine verilen ilanlardan oluşan internet sitesi bazında bir veri tabanına sahip olduğu, sanığın da bu şirkete ait web sitesindeki veri tabanındaki ilanlara erişip izinsiz olarak kendisine ait internet sitesine gönderip kullanarak üzerine atılı bilişim sistemindeki verileri başka yere göndermek ve kullanmak suçunu işlediğinden bahisle açılan davada;

Sanık kurduğu sitenin arama motoru görevi gördüğünü, yaptığı işlerin link vermek şeklinde olduğunu savunmuştur. Katılan ise link verilmesi dahi izne tabi olup olayda sanık şirketin sayfasını kopyalayıp kendi sayfasına almış, ancak silemediği için logonun o sayfada görülmekte olduğunu belirterek şikayetçi olmuştur.

Bilirkişi, örümcek olarak tabir edilen bu sistemin çeşitli internet sitelerinde belirli kelime aramaları yaparak verileri çekmekte ve bu konuda arama motoru görevi yapmakta olduğunu, sitede ilanların hangi sayfadan alındığı görünmekte ve o siteye link verilmekte olup ilgilene kişi gerçek bilgiye kendi sitesinde ulaşabildiğini bunların içerisinde katılan şirketin web sayfasında bulunan ilanların da bulunduğunun tespit edildiğini belirtmiştir.

İnternette ilanla mal satışlarında, ilanlar belirlenen süre ücretsiz olup daha sonraki ilanlar ücretli yayınlanabildiği dikkate alındığında ve dosya içinde bilirkişi raporuna ekli sayfa görüntülerinde; ilanda katılan şirketin logosu da dahil olmak üzere örneğin satılık arabanın resmi, teknik özellikleri, bedeli ve satıcı bilgileri tümüyle yayınlanıp alıcının tekrar katılan şirkete ait siteye gitmesine gerek kalmadığı açıkça görülmekte olup bilirkişi raporunda bahsolunan" çeşitli internet sitelerinde belirli kelime aramaları yaparak verileri çekmekte bu konuda arama motoru görevi yapmak"tan farklı olduğu anlaşılınca, dosyaya uygun düşmeyen bilirkişi raporuna dayanarak ve eylemin TCK.nın 244/2. maddesindeki suçu oluşturup mahkumiyetine karar verilmesi gerektiği gözetilmeden, yazılı şekilde beraatine karar verilmesi, (Y. 8. CD 2013/4675, 2014/12406)

**12-** Sanık ile şikayetçinin bir dönem duygusal beraberlik yaşadıkları, ayrıldıktan sonra şikayetçinin kullanmış olduğu posta adresine habersiz olarak şifresini kırarak girdiği, bazı fotoğraflarını söz konusu hesaptan aldığından bahisle açılan davada, sanığın "..... kullanıcılar en az

270 günde bir oturum açmak zorundadırlar ve bu oturum belirtilen bu zamanda açılmaz ise mail hesapları kalıcı olarak şirket tarafından iptal edilir. Şikayetçi de bu Amerikan şirketinin kurallarına uymamış ve hesabını kalıcı olarak kaybetmiştir. Ben 01.04.2013 tarihinde bu hesabı yasal yoldan/sıfırdan/şifre kırmadan ve bilakis yeni şifre belirleyerek oluşturduğum ve daha sonra şikayetçinin ricası üzerine benim olan bu hesabı kendisine kendi rızam ile teslim ettim"şeklindeki savunması karşısında, suç tarihinden önceki dönemde, bu adresin faal olup olmadığı, ve suç tarihinde önce ve sonraki tarihlerde şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı ilgili yer sağlayıcısından sorulup, sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, (Y. 8. CD 2016/9188, 2017/5663)

**13-** Sanığın tespit edilen IP ile suç tarihinde bir kez girdiği ve kaldığı anlaşılmasına rağmen hakkında zincirleme suç hükümleri uygulanarak fazla ceza tayini, (Y. 8. CD 2016/9971, 2017/5660)

**14-** ...sanığın soruşturma aşamasında müdafii huzurunda alınan beyanında katılan şirketten ayrıldıktan sonra katılan şirkete ait bilgisayar programına girdiğini kabul etmesi ve değişik zamanlarda bu programa girdiğinin dosya içerisindeki belgelerden anlaşılması karşısında, sanığın oluşan eylemi nedeniyle bilişim sistemine izinsiz girme suçundan TCK.nun 243, 43. maddeleri gereğince cezalandırılması yerine dosya içeriğiyle uyuşmayan gerekçelerle beraat kararı verilmesi...( 8. C.D. 04.06.2014, 2014/3984-13848)

**15-** Sanık hakkında katılan Mehmet KESİCİ'nin rızası olmaması nedeniyle TCK.nun 168. maddesinde düzenlenen etkin pişmanlık hükümleri uygulanmamış ise de; banka tarafından üretilmiş kredi kartının henüz sahibine teslim edilmeden kullanılması halinde suçun mağdurunun banka olacağı cihetle ve katılan Mehmet KESİCİ'nin 9.2.2011 tarihli talimatla alınan beyanında sanığın babasının zararın 500 TL'lik kısmını kendisine ödediğini beyan etmesi karşısında mağdur bankadan sanık hakkında etkin pişmanlık hükümlerinin uygulanmasına rızası bulunup bulunmadığı sorularak sonucuna göre TCK.nun 168. maddesinin uygulanıp uygulanmayacağına karar verilmesi gerektiği gözetilmeden yazılı şekilde hüküm kurulması, (8. CD. 18.01.2018, 22781-560)

## **ÜÇÜNCÜ BÖLÜM**

### **I. 5237 SAYILI TÜRK CEZA KANUNU'N 244. MADDESİ**

#### **A. BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİN ENGELLENMESİ VEYA BOZULMASI, VERİLERİN YOK EDİLMESİ VEYA DEĞİŞTİRİLMESİ SUÇUN (TCK. 244)**

**Madde 244** -(1) *Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

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

### **Madde Gerekeçesi**

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 ızzar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkroda seçimlik hareketli bir suç meydana getirilmiştir.

İkinci fıkroda, 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 fıkroda ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımına altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğinin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.

Madde metninden de açıkça anlaşıldığı gibi 1. fıkrasında bir bilişim sisteminin işleyişini engelleme veya bozma, ikinci fıkrasında ise bir bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme fiilleri suç olarak tanımlanmıştır.

Maddenin 3. fıkrasında ki da 1. ve 2. fıkrasındaki fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza yarı oranında artırılacağı belirtilerek ağırlaştırılmış hal düzenlenmiştir.

Maddenin 4. fıkrasında ise maddenin 1. ve 2. fıkrasında tanımlanan fiillerin işlenmesi sonucunda kişinin kendisine veya başkasına haksız bir yarar sağlaması hali düzenlenmiştir. Failin maddenin 1. ve 2. fıkrasında tanımlanan fiilleri işlenmesi sonucunda kendisine veya başkasına haksız bir yarar sağlaması durumunda ise fiil başka bir suç oluşturuyorsa fail hakkında maddenin 4. fıkrası uyarınca ceza tayin edilecektir.

Burada dikkat edilmesi gereken husus, her ne kadar gerekçede fiilin daha ağır bir cezayı gerektiren başka bir suç oluşturulmaması halinde bu hükmün uygulanacağı belirtilmekte ise de, madde metninde başka bir suç oluşturulmaması halinde bu hükmün uygulanacağı belirtildiğinden kanunilik ilkesi gereğince eylemin başka bir suç oluşturulmaması halinde bu fıkra uyarınca ceza tayin edilecektir.

TCK'nun 244. maddesinin 4. fıkrasında düzenlenen suç tali norm niteliğindedir. Bu hükmün uygulanabilmesi için fiilin başka bir suç oluşturulmaması gerekmektedir. 244. maddenin 1. ve 2. fıkralarında belirtilen fiillerin gerçekleşmesi durumunda haksız bir yarar da elde edilmiş ise bu durumda eylemin dolandırıcılık, hırsızlık, güveni kötüye kullanma gibi başka bir suç oluşturup oluşturmadığı araştırılmalıdır. Eğer eylem bu suçlardan birini oluşturuyorsa artık 244. maddenin 4. fıkrası uygulanmayacaktır. Eylem bu suçlardan birisinin tanımına uymuyorsa, o zaman 244. maddenin 4. fıkrası hükmü uygulanabilecektir. 244. maddenin 4. fıkrası ancak eylemin başka bir suç oluşturulmaması halinde uygulanabilecektir. Örneğin eylem hırsızlık suçunu oluşturuyorsa artık TCK'nın 244/4. maddesi ile hüküm kurulmayacak, sadece oluşan hırsızlık suçundan hüküm kurulacaktır.<sup>1059</sup>

TCK'nun 244/1 maddesiyle bilişim sisteminin işleyişinin engellenmesi ve bozulması yaptırım altına alınırken özel bir zarar verme fiili düzenlenmiş olmaktadır. Nitekim inceleme konusu fıkranın gerekçesinde “böylece sistemlere yöneltilen ızzar fiilleri özel bir suç haline getirilmiştir.” denilmek suretiyle bu görüşün haklılığı vurgulanmıştır<sup>1060</sup>.

### **1.Korunan Hukuki Yarar**

244. maddenin 1. ve 2. fıkrasında düzenlenen suçlarda korunan hukuki yarar bilişim sisteminde yer alan veriler ve yazılımlardır. Bir başka deyişle hem bilişim sisteminin hem de bu sistem içerisinde yer alan verilerin veya diğer unsurların sağlam ve güvenli bir şekilde çalışabilirliği

---

1059 2.CD. 19.06.2014 gün, 2014/22676-2014/17536.”Sanıkların, katılanın banka hesabına bilgisi dışında internet yoluyla erişim sağlayarak, hesabındaki parasını sanık Şahin Tüncer'in hesabına havale etmeleri şeklinde gerçekleştiği kabul edilen eyleminin 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunu oluşturduğu gözetilmeden, yazılı şekilde aynı Kanunun 244/4 maddesi uyarınca hüküm kurulması.”

1060 Erdoğan, age s.138

korunmaktadır.(Karagülmez Ali, bilişim suçları ve soruşturma-kovuşturma evreleri, Ankara 2011, sh. 211) Yani sistemin donanımı bu suçun kapsamı içerisinde değildir. TCK.nun244. maddesindeki bu düzenleme Avrupa Konseyi Siber Suç Sözleşmesi'nin 4. ve 5. maddelerine ilişkin açıklayıcı rapora paralel bir düzenlemedir. Avrupa Konseyi Siber Suç Sözleşmesi'nin 4. ve 5. maddelerine ilişkin açıklayıcı raporda, 4. maddede korunan hukuksal değer, bilişim sisteminde yer alan verilere veya yazılımlara zarar verilmesini, veri ve yazılımların bozulmasını, zarar görmesini engellemek, böylelikle bunların doğru ve işlevsel olarak çalışmalarını sağlamak olduğu ifade edilmektedir.<sup>1061</sup>

Ancak 244. maddenin 4. fıkrasındaki suçun oluşması için failin hukuka aykırı bir yarar elde etmesi gerekmektedir; ancak bunun nasıl bir yarar olduğu konusu açıklanmamıştır. Yararın türü bakımından bir ayırım yapılmadığına göre fail tarafından elde edilen maddi ya da manevi yarar suçla korunan hukuksal değeri oluşturmaktadır.

Ayrıca verilerin başka yere gönderilmesi, haberleşmenin engellenmesi durumunda üçüncü kişilerin özel hayatına ve haberleşme hürriyetine de müdahale söz konusudur<sup>1062</sup>.

Bilişim sisteminin işleyişini sağlayan herhangi bir soyut unsura, sistemin bir bütün olarak kendisinden beklenen fonksiyonu yerine getirmesine engel olabilecek şekilde müdahalede bulunmakla suç oluşur. Bu tür müdahaleler çeşitli şekillerde gerçekleştirilebilir. Örneğin; bilgisayara virüs bulaştırılması, yazılım sisteminin çökertilmesi, bilgisayarın şifresinin değiştirilmesi, çok sayıda elektronik posta gönderilmek suretiyle sistemin işlemez hale getirilmesi gibi hareketler bu suçu oluştururlar. Keza, yoğun elektromanyetik dalgalarla sistem merkezi üzerinde etkide bulunmak suretiyle de sistemin işleyişi engellenebilir. Kısaca, bilişim sisteminin soyut unsuruna, sistemin kendisinden beklenen işlevi yerine getirmemesini sağlamaya yönelik her türlü müdahale bu suçu oluşturacaktır<sup>1063</sup>.

Bu düzenlemeye göre, bir bilişim sisteminin donanım olarak ifade edilen (merkezi işlem ünitesi, klavye vs.) maddi unsurlarına yönelik zarar verici davranışlar bu madde hükmüne göre değil, mala zarar verme suçuna ilişkin hükümler (TCK m.151) çerçevesinde cezalandırılacaktır. Buna karşılık yazılım olarak ifade edilen (programlar bütünü) sistemin işleyişini engelleyici veya

---

1061 Dülger, age, s.413

1062 Erdoğan, s. 146

1063 Taşdemir, Kubilay, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara 2009, s. 37.

bozucu davranışlar maddenin birinci fıkrası hükmüne istinaden ceza yaptırımını altına alınmış olmaktadır<sup>1064</sup>.

## **2.Suçun Unsurları**

### **a.Fail**

Bu suçun faili herkes olabilir. Özgü bir suç değildir. Çünkü 244. maddenin 1., 2. ve 4. fıkralarında düzenlenen suçları işleyecek kişi açısından herhangi bir özellik belirtilmemiştir. Kişinin, başkasının haklarına zarar vermeksizin herhangi bir bilişim sisteminde bulunan kendisine ait verilere zarar vermesi suç oluşturmayaacağından failin tespit edilmesi önem taşımaktadır. Ancak failin kendisine ait olmayan bir bilişim sisteminde bulunan kendisine ait olan verileri yok etmek ya da erişilmez kılmak için sistemin işleyişini bozması ya da engel olması halinde ise her ne kadar 244. maddenin 2. fıkrasındaki suç gerçekleşmeyecek olsa da 1. fıkradaki suç gerçekleşmiş olacaktır.

### **b.Mağdur**

Mağdur, belirli bir suçla zarara veya tehlikeye uğratılan hak veya çıkarın, suçla korunan hukuksal değer sahibi olan kişidir. Gerçek kişiler suçun mağduru olabilir, bazı yazarlara göre<sup>1065</sup> tüzel kişiler ancak suçtan zarar gören olabilirler, dolayısıyla bu suçun mağduru da gerçek kişilerdir, ancak bir şirketin ya da kamu tüzel kişisinin sistemine karşı bu suç işlendiğinde söz konusu tüzel kişiler suçtan zarar gören olacaktırlar. Bu suçun mağduru açısından da Yasa metninde bir özellik gösterilmemektedir, herkes bu suçun mağduru olabilir. 244. maddenin 1., 2. 3 ve 4. fıkralarında belirtilen hareketlerden birinin gerçekleşmesi durumunda çıkarı zarara uğratılan, bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi olan herkes olabilecektir.

### **c.Suçların Hukuki Konusu**

244. maddenin 1. fıkrasında düzenlenen suçun hukuki konusu “*bilişim sistemi*”dir. 2. fıkrada yer alan suçun hukuki konusu ise “*bilişim sisteminde yer alan veriler*”dir. Bu nedenle 244. maddenin 1. fıkrasında düzenlenen suç, 2. fıkrada düzenlenen suçtan ayıran en önemli husus suçun konusudur.

Bunun yanında 244. maddenin 4. fıkrasında düzenlenen suçun konusu ise failin sağladığı “*hukuka aykırı yarar*” oluşturmaktadır. 8. Ceza Dairesinin kararlarına göre bu yarar ekonomik değeri olan mali bir yarar yanında sosyal ve yönetsel bir statü değişikliği sonucunu doğuran bir manevi yararın da suçun hukuki konusunu oluşturduğu kabul edilmektedir.

---

1064 Prof.Dr. İzzet Özgenç, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), s.1003, Seçkin Yayınevi 2005

1065 Dülger, age. s.359 Yaşar/Gökçan/Artuç age. s.6739

## **d.Eylem**

### **aa)244. Maddenin 1. Fıkrasında Eylem**

244. maddenin 1 fıkrasında “bilgişim sisteminin işleyişini engellemek” ve “bilgişim sisteminin işleyişini bozmak” fiilleri tanımlanmıştır. Bu fıkrada düzenlenen suçun oluşabilmesi için, ortada işleyişi engellenen veya bozulan bir “bilgişim sistemi” bulunmalıdır.

Maddenin 1. fıkrasında “engelleme” ve “bozma” gibi iki seçimlik hareket düzenlenmiştir. Suçun oluşması için bu iki seçimlik hareketten birisinin gerçekleşmesi yeterlidir. İkisinin birlikte gerçekleşmesi halinde de “tek suç” vardır. Seçimlik hareketlerin birlikte gerçekleşmesi halinde hakim TCK.nun 3 ve 61. maddeleri çerçevesinde temel cezayı tayin edecektir.

### **aaa) Bilgişim Sisteminin İşleyişini Engellemek**

Bu fıkrada tanımlanan hareket, sistemin düzgün işlemeden elde edilecek her türlü faydanın engellenmesi ve sistemin işlevlerini yerine getirmesine engel olan hareketlerdir. Yasa koyucu burada kavramı çok geniş tutmuş ve nasıl olduğunu aramaksızın sistemin işleyişini bozmak dışında, sistemin işlemeden engelleyen her türlü eylemi buraya dahil etmek istemiştir. Bu hareketlerle sistemin düzenli çalışması engellenmekte ya da sistem çalışamaz hale getirilmektedir. Böylece sistemin veri işleme hızı, düzenli çalışma yetenekleri olumsuz şekilde etkilenmektedir. Yoksa sistem bozulmamakta, ancak sağlıklı da çalışmamaktadır<sup>1066</sup>. Örneğin; sistem devamlı e-mail (e-posta) ya da zararlı virüs gönderilmek suretiyle çalışamaz hale getirilmektedir. Engellenme sürekli veya geçici olabilir.<sup>1067</sup>

### **bbb) Bilgişim Sisteminin İşleyişini Bozmak**

244. maddenin 1. fıkrasında yer alan bozmak ifadesiyle bilgişim sisteminin kendisinden beklenen işi yapamayacak duruma getirilmesi, bilgişim sisteminin düzeninin karıştırılması, bilgişim sistemine zarar verilmesi veya kötü duruma getirilmesi kastedilmektedir. Bir başka deyişle bilgişim sisteminin işleyişinin bozulması, sistemin kısmen ya da tamamen işleyemez hale getirilmesidir.<sup>1068</sup>

Bozmak eyleminin gerçekleştirilme yöntemi, suçun oluşması bakımından önemli değildir. Böylece sistem çöktürülmekte, verileri ve işleyiş düzeni bozulmaktadır. “Sözlükte “engellemek”, bir şeyin gerçekleşmesini veya yapılmasını önlemek; “bozmak” ise bir şeyi kendisinden beklenen

---

1066 8.CD. 24.06.2013 gün, 2012/32866- 2013/18872. “Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suçta sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suç oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması”

1067 Taşdemir, age.

1068 Dülger age sh, 419



*işi yapamayacak duruma getirmek; bir yerin, bir şeyin düzenini karıştırmak, dokunmak ve zarar vermek anlamlarına gelmektedir. Bu tanımlardan da anlaşılacağı üzere bokmak, engelleme sonucunu da doğuran bir anlama sahiptir. Bir bilişim sisteminin işleyişini bozan bir müdahale, aynı zamanda onun işleyişini engellemiş de olur. Ancak bu durum her iki kavramın aynı anlama geldiğini göstermez. Çünkü engellemek, bozmak demek değildir ve bir bilişim sisteminin işleyişi bozulmadan da engellenebilir” şeklinde açıklamıştır<sup>1069</sup>.*

Bilişim sistemine yapılan müdahalelerle sistemin veri işleme fonksiyonunu yerine getirememesi halinde bilişim sisteminin engellenmesi; sistemin işlem yapabilmesini sağlayan unsurlarına yapılan müdahalelerle fonksiyonunu tamamen veya kısmen yerine getiremeyecek duruma sokulması halinde ise bozulması söz konusudur<sup>1070</sup>.

Bilişim sistemine zarar vermek kastıyla icra hareketlerine başlayan failin fiziki saldırıları sonunda bilgisayarın kırılması durumunda (örneğin; balta ile vurulup parçalanması gibi), aynı zamanda bilişim sisteminin de bozulacağı mutlaklıdır. Failin tek fiil ile Yasanın çeşitli maddelerini ihlâl etmesi halinde, TCK.nun 44. maddesi uyarınca en ağır cezayı gerektiren aynı Yasanın 244/1. maddesi uyarınca cezalandırılması gerekir.<sup>1071</sup>

## **bb) 244. Maddenin 2. Fıkrasındaki Eylem**

### **aaa) Verileri Bozmak**

Bilişim sisteminin işleyişinin engellenmesi için verilerin bozulması halinde failin amacı sistemde bulunan verilere zarar vermek değil bir şekilde bilişim sisteminin işleyişini bozmaktır; oysaki maddenin 2. fıkrasında yer alan verileri bozmak hareketinde fail bilişim sisteminin işleyişine zarar vermek istememekte, sadece bir kısım verileri kullanılamaz hale getirmeyi amaçlamaktadır. Yani bir uygulama yazılımını ya da depolanmış bazı bilgileri kullanılamaz hale getirmek istemektedir.

### **bbb) Verileri Yok Etmek**

Bilişim sistemindeki verileri tamamen ortadan kaldırmak ve varlığına son vermektir. Bu anlamda yok etme, verilerin silinmesini de kapsamaktadır. Ancak bilişim sistemindeki verileri her zaman tamamen ortadan kaldırmak-yok etmek mümkün değildir. Verilerin yok edilmesindeki kasıt verinin, mağdurun tasarruf alanından çıkartılmış olması ve normal yollardan ulaşılmasının güçleştirilmesidir. Yok edilen veriye, mağdurun kendisinin veya bir uzmanın tekrar ulaşabilme

---

1069 Koca, Prof. Mahmut, Hukukumuzda TCK.nun 244. maddesi kapsamında bilişim sistemini engelleme, bozma verileri yok etme ve değiştirme suçu, bilişim hukuk konferansı, 9-10 Ekim 2008, Yargıtay Yayınları s.93

1070 Koca, age. s93

1071 Taşdemir, age.

imkânının varlığı suçun oluşmasını engellemeyecektir. Bu nedenle yok edilmek eyleminden kasıt somut anlamda yok etmek eylemini değil, bilişim alanında geçerli olan soyut anlamda mantıksal yok etmek eylemini kastetmektedir. Örneğin; bir dosyanın geri dönüşüm kutusuna atılması gibi, verinin sistemde tutulmakla birlikte, sırf yerinin değiştirilmesi niteliğindeki hareketler bu suç oluşturmayacaktır<sup>1072</sup>.

### **ccc) Verileri Değiştirmek**

Verilerin değiştirilmesi eylemiyle, bir veri ya da veri grubu yerine başka verilerin konulması kastedilmektedir. Bu birkaç veriden oluşan bir bilgi notu ya da resmin değiştirilmesi şeklinde olabileceği gibi verilerden oluşan örneğin bir uygulama yazılımının ya da bir sistem içerisindeki bilgilerin değiştirilmesi şeklinde de olabilecektir<sup>1073</sup>. Örneğin kullanıcının sisteme koyduğu şifrenin yerine bir başka şifrenin konulması, bir bilginin değiştirilmesi halinde bu durum söz konusu olacaktır.

### **ddd) Verileri Erişilmez Kılmak**

Burada veriler tamamen yok edilmemekte ancak sahibinin ya da ilgisinin istediği zaman verilere ulaşması engellenmektedir. Bu hareket neticesinde veri bütünlüğü korunmaktadır, veri yok edilmemiş ya da bozulmamıştır, ancak verilere ulaşım bir şekilde engellenmiştir ve veri üzerindeki hak sahibi kendi verilerine erişememektedir. Bu sonuç bir kişinin bilgisayarına ya da bilgisayardaki dosyasına virüs bulaştırmak, şifre koymak gibi çok çeşitli şekillerde sağlanabilir.

Yargıtay 15. C.D. sinin 15.11.2016 tarih 2016/3781-8608 sayılı kararında “...sanığın, müşterinin elektronik posta adresinin şifresini kırarak, hesaba giriş şifresini değiştirerek, erişimini engellemesi şeklinde gerçekleşen eyleminin TCK.nun 244/2. maddesi kapsamında kaldığını...” kabul etmiştir.

### **eee) Bilişim Sistemine Veri Yerleştirmek**

Bilişim sistemine veri yerleştirmek hareketiyle, maliki ya da ilgisinden izin alınmaksızın çeşitli verilerin sisteme kaydedilmesi, yüklenilmesi ya da eklenilmesi kast edilmektedir. Bu yerleştirme hareketi “harici bellek” ya da “USB” gibi veri taşıma aracını sürücü donanıma yerleştirip içindeki verileri bilgisayara yüklemek şeklinde yapılabileceği gibi; internet üzerinden veri yüklemek şeklinde de gerçekleştirilebilecektir. Sisteme yerleştirilen veriler, daha sonra

---

1072 Taşdemir, a.g.

1073 8.CD. 24.06.2013 gün, 2012/32866-2013/18872. “Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması”

oluşturulan bir belgenin içeriğini etkilemişse, faili ayrıca belgede sahtecilikten de sorumlu tutan yargı kararları bulunmaktadır<sup>1074</sup>.

#### **fff) Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Göndermek**

Burada, madde metninde açıkça ifade edildiği gibi bir bilişim sisteminde bulunan verilerin başka bir bilişim sistemine ya da veri taşıma aracına herhangi bir şekilde aktarılması, gönderilmesi hareketlerinden bahsedilmektedir. Bu hareketle veri ortadan kaldırılmamakta veya bütünlüğü bozulmaktadır. Bu hareketle sadece verinin, hak sahibi tarafından kullanılmasının engellenmektedir. Bilişim sisteminde var olan verilerin başka yere gönderilmesi eylemi internet ya da “wifi” gibi veri iletim ağları üzerinden bir başka bilişim sistemine verilerin aktarılması yoluyla gerçekleştirilebileceği gibi, verilerin bulunduğu bilgisayara bir veri taşıma aracının bağlanması ve verilerin bu aracın üzerine kaydedilmesi yoluyla da yapılabilmektedir.

244. maddenin 1 ve 2. fıkralarında düzenlenen suç seçimlik hareketli suçlardır. Maddede belirtilen seçimlik hareketlerden herhangi birisinin gerçekleştirilmesi durumunda suç oluşacaktır. Seçimlik hareketlerin birden fazlasının gerçekleşmesi halinde faile bir kez ceza verilecektir. Örneğin; verileri erişilmez kılma ve verileri değiştirme hareketlerinin aynı anda gerçekleşmesi gibi durumlarda tek suçtan ceza tayin edilecektir. Ancak burada da hakim TCK. nun 3 ve 61. maddeleri uyarınca alt sınırdan uzaklaşarak ceza tayin edebilecektir.

TCK'nın 243. maddesindeki bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren ve orada kalmaya devam eden kimse, kasten sistemdeki verileri bozar veya diğer seçimlik hareketlerden herhangi birisini gerçekleştirirse, bilişim sistemine hukuka aykırı olarak girmek 244. maddenin 2. fıkrasında düzenlenen suçun unsuru olduğundan fail daha ağır ceza içeren 244/2. maddedeki suç nedeniyle cezalandırılacaktır.

#### **cc) 244. Maddenin 4. Fıkrasındaki Eylem**

Bu suçun oluşabilmesi için failin 244. maddenin 1. ve 2. fıkralarında belirtilen bilişim sisteminin işleyişini engellemek, bilişim sistemin işleyişini bozmak, verileri bozmak, bilişim sistemine veri yerleştirmek, bilişim sisteminde var olan verileri başka bir yere göndermek, verileri erişilmez kılmak, verileri değiştirmek ve verileri yok etmek hareketlerinden birini ya da bir kaçını gerçekleştirilmesi ve gerçekleştirdiği eylemler neticesinde hukuka aykırı yarar, yasanın ifadesiyle

---

1074 “5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 10. maddesinde yer alan “Elektronik ortamda hazırlanacak bilgi ve belgeler adli ve idari makamlar nezdinde resmi belge olarak geçerlidir.” şeklindeki düzenleme karşısında sanığın bir başkasına ait şifreyi kullanarak çalışmayan kişilerin çalışmaya başladıkları yönünde e-bildirge hazırlanması şeklindeki eyleminin resmi evrakta sahtecilik suçunu oluşturup oluşturmayacağı tartışılmadan yazılı şekilde karar verilmesi,” (8. CD. 12.12.2013, 31922-29069)

“haksız bir çıkar sağlaması” gerekmektedir. Haksız çıkar ifadesiyle kastedilen “hukuka aykırı yararadır”. Yani 244. maddenin 1. ve 2. fıkrasındaki seçimlik hareketlerden bir veya daha fazlasını gerçekleştiren fail, fiilinin neticesinde haksız bir çıkar sağlamış ise bu durumda sanık hakkında 244. maddenin 4. fıkrası gereğince ceza tayin edilecektir. 244. maddenin 1. ve 2. fıkralarında düzenlenen eylemler 244. maddenin 4. fıkrasında düzenlenen suçun da eylem unsurunu oluşturmaktadır.

Failin gerçekleştirdiği eylemin sonucunda hukuka aykırı yarar elde edememesi durumunda 244. maddenin 4. fıkrasında düzenlenen suç oluşmayacaktır. Bu durumda 244. maddenin 1. ve 2. fıkralarında yer alan suçların gerçekleşmesi söz konusu olabilecektir.

244. maddenin 4. fıkrasında hukuka aykırı olarak çıkar maddi bir yarar olabileceği gibi bazı yazarlara göre tamamen duygulara hitap eden manevi bir yarar da olabilir. Haksız çıkarın mutlaka maddi olması şart değildir. Yasa metninde de çıkarın mutlaka maddi olması gerektiğine işaret edilmemiştir. Yargıtay 8. Ceza Dairesi öğrenci notunun yükseltilmesini ya da devamsız gün sayısının azaltılmasını TCK.nun 244/4 kapsamında “haksız çıkar” olarak değerlendirmemiştir. (Y. 8. CD. 08.01.2014, 2014/33044, 2014/236, 15.02.2017 2016/3794, 2017/1405) Suçun oluşabilmesi için failin sağladığı çıkarın haksız olduğunun farkında olması da zorunludur<sup>1075</sup>. Fail hukuka aykırı yararı kendisine ya da üçüncü şahsa sağlayabilir. Hukuka aykırı çıkarın elde edilmesiyle suç tamamlanacaktır.

Ancak 244. maddenin birinci ve ikinci fıkralarında belirtilen fiilleri işleyen failin, kendisine veya başkasına haksız bir yarar sağlamasının başka bir suç oluşturmaması gerekir. Eğer eylem başka bir suçu oluşturuyorsa artık fail hakkında gerçekleşen bu eylemden dolayı ceza tayin edilecektir. Örneğin gerçekleşen eylemin, dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne dayanılarak ceza tayin edilemeyecektir. Bu hükmün uygulanmasında suçun hukuki konusu çok önem arz etmektedir. Bu suçun hukuki konusu veridir. Veri taşınabilir mal değildir. Taşınabilir mal ancak hırsızlık gibi mala karşı suçların hukuki konusunu oluşturabilir.<sup>1076</sup> Bu genel kuralın istisnası olan TCK.nun 142/2-e maddesindeki

---

1075 Taşdemir, a.g.e.

1076 Y.11.CD. 18.09.2013 gün, 2012/2764- 2013/13257. “Katılanların ortağı ve yöneticisi oldukları Ef Turizm Organizasyon Hizmetleri ve Seles Kongre Organizasyon Ticaret Limited Şirketinin sigortalı çalışanları olan sanıkların, mülkiyeti anılan şirketlere ait olup sanıkların kullanımına bırakılan bilgisayarlardan, şirketlerin faaliyet alanları nedeniyle gelen e-mail tekliflerini ve müşteri portföylerini kopyalayarak şahsi e-mail adreslerine aktardıkları gibi mevcut bilgisayarlardan bu teklife-mail’lerini silerek daha sonra kendilerinin ortak olarak kurdukları şirketleri olan 3 Gen Turizm Organizasyon Ltd. Şirketine aktardıkları somut olayda, suçta konu verilerin güveni kötüye kullanma suçunun konusunu oluşturan eşya kavramı içerisinde değerlendirilemeyeceği de dikkate alındığında, 5237 sayılı TCK’nun 244/2-4. maddesinde yazılı “bilgi işlem suçunu” oluşturduğu gözetilmeden, sanıkların eylemlerinin aynı

düzenleme karşısında failin bir başkasının interaktif banka hesabına internet yoluyla girerek kendi hesabına para (veri) transfer etmesi halinde TCK.nun 142/2-e maddesinde düzenlenen “bilgişim suretiyle hırsızlık” suçu oluşacaktır<sup>1077</sup>. Yine failin içerisinde mal bulunan bir deponun şifreli kilidinin bilgişim sistemi kullanılarak açılması suretiyle içeriden mal çalınması durumlarında TCK. nun 142/2-e maddesinde düzenlenen bilgişim sistemleri aracı kılınarak hırsızlık suçu gündeme gelecektir. Bu halde artık 244. maddenin 4. fıkrası uyarınca hüküm kurulamayacaktır.

Ceza Genel Kurulunun 2009/11-193, 2009/268 sayılı kararında “...sanığın, katılan şirketin banka hesabının internet şifresini kırarak bu hesaptan kendi hesabına havale yaparak haksız menfaat sağlamak şeklindeki eyleminin 5237 sayılı Yasanın 142/2-e maddesine uyduğu” kabul edilmiştir.

Dolandırıcılık suçunda da suçun hukuki konuları insan iradesinin özgürlüğü ve malvarlığına ilişkin varlık ve menfaatlerdir. Dolandırıcılık suçunda, bir şeyin teslimi, hile ile sakatlanmış ve özgür olmayan bir iradeye dayanmaktadır.

Dolandırıcılık suçunun oluşabilmesi için; failin bir kimseyi kandırabilecek nitelikte hileli davranışlarla hataya düşürüp onun veya başkasının zararına, kendisine veya başkasına yarar sağlaması gerekmektedir. Dolandırıcılık suçunun oluşabilmesi için; failin bir kimseyi kandırabilecek nitelikte hileli davranışlarla hataya düşürüp onun veya başkasının zararına, kendisine veya başkasına yarar sağlaması gerekmektedir. Dolandırıcılık suçunda hileli hareketin gerçek kişiye yöneltilmesi gerekmektedir. Eğer hileli hareketle bir bilgişim sistemi yanıltılarak haksız yarar elde edilmesi halinde dolandırıcılık suçu oluşmayacaktır. Bu durumda 244. maddenin 4. fıkrası gündeme gelecektir<sup>1078</sup>.

Yukarıda da bahsedildiği gibi 244. maddenin 4. fıkrasında düzenlenen suç tali norm niteliğindedir. Bu hükmün uygulanabilmesi için failin başka bir suçu oluşturmaması gerekmektedir. 244. maddenin 1. ve 2. fıkralarında belirtilen fiillerin gerçekleşmesi durumunda haksız bir yarar da elde edilmiş ise bu durumda eylemin dolandırıcılık, hırsızlık, güveni kötüye kullanma gibi başka bir suçu oluşturup oluşturmadığı araştırılmalıdır. Eğer eylem bu suçlardan birini oluşturuyorsa artık

---

Kanununun 155/2. maddesinde düzenlenen "hizmet nedeniyle güveni kötüye kullanma" suçunu oluşturduğundan bahisle yazılı şekilde hüküm tesisi;"

1077 CGK. 17.11.2009 gün ve 193/268 sayılı karar.

1078 **Y.8.CD. 24.12.2012 gün, 2012/21826-2012/39370.**”Oluşa ve dosya kapsamına göre, mağdure F.Ç.'nin işvereni olan A.Y.'ün facebook şifresini bir şekilde ele geçiren sanığın, bu adresten mağdure ile A. A. gibi yazışarak 700 TL'lik kontör kartı aldırıp şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK.nun 158/1-f maddesinde yazılı bilgişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturabileceği ve bu suça bakma ve delilleri takdir etmenin ağır ceza mahkemesine ait olmasına karşın, görevsizlik kararı verilmeyerek yargılamaya devamlı yazılı şekilde hüküm kurulması,

244. maddenin 4. fıkrası uygulanmayacaktır. Eylem bu suçlardan birisinin tanımına uymuyorsa, o zaman 244. maddenin 4. fıkrası hükmü uygulanabilecektir. 244. maddenin 4. fıkrası ancak eylemin başka bir suçu oluşturmaması halinde uygulanabilecektir. Örneğin eylem hırsızlık suçunu oluşturuyorsa artık TCK. nun 244/4. maddesi ile hüküm kurulmayacak, sadece oluşan hırsızlık suçundan hüküm kurulacaktır.<sup>1079</sup>.

Ceza Genel Kurulunun 2013/13-448, 2014/524, 2015/15-867, 2013/13, 2012/15-1293, 2013/11 ve 2015/23-1100, 2015/10 sayılı kararlarında “[www.arabam.com](http://www.arabam.com), [www.srexi.com](http://www.srexi.com)” gibi aynı anda birçok kişiye ulaşmada çabukluk ve kolaylık sağlayan bilişim sistemlerine yanıltıcı ilanlar verilerek gerçekleştirilen dolandırıcılık fiillerinin TCK.nın 158/1-f maddesi kapsamında kaldığı kabul edilmiştir.

Ancak, Ceza Genel Kurulu sanığın müştekiyi telefonda söylediği nitelikli yalanla ikna ettikten sonra istediği peşinatı internet bankacılığı yoluyla kendisine gönderilmesini istemesi ve müştekinin de bu şekilde parayı göndermesinde dolandırıcılıkta araç olarak kullanılan telefon olup, bankanın bilişim sisteminin araç olarak değil, ödeme aracı olarak kullanıldığı gerekçesiyle eylemin TCK.nın 157/1. maddesinde tanımlanan suçu oluşturduğuna karar vermiştir. (CGK. 10.05.2016 gün, 2014/15-288, 2016/255)

Yargıtay 8. Ceza Dairesi kararlarında bilişim sisteminde bulunan ve mağdura ait oyun karakterlerini rızası haricinde alarak kendi ya da başkasının hesabına aktaran failin eylemini daha önceleri hırsızlık olarak değerlendirmiş ise de (2015/14257, 2016/1702) son olarak hırsızlık suçunu değil TCK.nın 244/2. maddesinde tanımlanan suçu oluşturduğuna karar vermiştir.(8. C.D. 2017/897 2017/6019, 2017/1283-14186)

Mali müşavir olan sanığın hiçbir işyerinde çalışmayan kişileri çalışıyor göstermek için şifre ve imza kullanarak Sosyal Güvenlik Kurumuna ait sisteme girerek e-bildirge oluşturması durumunda eylemi hangi suçu oluşturacaktır?

Yargıtay 8. Ceza Dairesine<sup>1080</sup> göre 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 100. Maddesi ile birlikte değerlendirildiğinde eylemin TCK'nın 204. maddesindeki sahtecilik suçunu oluşturduğunun kabulü gerekecektir.

---

1079 Y.2.CD. 19.06.2014 gün, 2014/22676-2014/17536.”Sanıkların, katılanın banka hesabına bilgisi dışında internet yoluyla erişim sağlayarak, hesabındaki parasını sanık Ş. T.'in hesabına havale etmeleri şeklinde gerçekleştiği kabul edilen eyleminin 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunu oluşturduğu gözetilmeden, yazılı şekilde aynı Kanunun 244/4 maddesi uyarınca hüküm kurulması.”

1080 Y. 8. CD. 12.12.2013, 31911-29069

Ancak Yargıtay 11. Ceza Dairesi<sup>1081</sup> ise; TCK'nun 244/2. maddesindeki sisteme veri yerleştirme suçunu oluşturduğunu kabul etmektedir.

Ceza hükmü içeren başkaca özel kanunlarda “*ayrıca düzenlenmiş olmadığı sürece*”, elektronik ortamdaki verilerin ceza hukuku anlamında “*belge*” olarak kabul edilmeleri ve ceza hukuku korumasından yararlanmaları mümkün değildir. Dolayısıyla, bilgisayar sistemine hukuka aykırı olarak girilerek gerçeğe aykırı olarak verilerin sisteme yüklenmesi veya değiştirilmesi halinde, ortada fiziki anlamda bir belge mevcut olmadığı için, fiil TCK md. 204 vey 207’de tanımlanan suçları oluşturmayacaktır. Belirtilen eksiklik nedeniyle, bilgisayarlarla ilişkili sahtecilik fiillerinin resmi veya özel evrakta sahtecilik suçunu değil, TCK.nun 244/2. maddesinde düzenlenen verileri değiştirme veya yok etme suçunu oluşturmakta, bu da –*yaptırım açısından*- doktrinde bir tür ödüllendirme olarak nitelendirilmektedir. Kısacası TCK, elektronik ortamda gerçekleşecek sahtecilik filleri yönüyle Sözleşme’de öngörülen yükümlülükleri karşılamaktan uzaktır<sup>1082</sup>.

### 3. Suçun Nitelikli Hali:

Maddenin 1. ve 2. fıkralarındaki eylemlerin bir banka veya kredi kurumuna<sup>1083</sup> ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi ağırlatıcı neden olarak düzenlenmiştir. Ancak bu fıkranın uygulanabilmesi için bilişim sisteminin bir banka veya kredi kurumuna ya da bir kamu kurum ve kuruluşuna ait olması gerekir. Belirtilen ağırlatıcı nedenin gerçekleşmesi durumunda, faile verilecek ceza yarı oranında artırılabacaktır. Örneğin failin ÖSYM'nin bilişim sistemine ya da öğrenim gördüğü okulun bilişim sistemine girerek kendi sınav sonuçlarını değiştirmesi gibi<sup>1084</sup>.

---

1081 Y. 11. CD. 03.12.2015 gün, 10595-31550, 27.11.2017, 2015/8801, 2017/8230

1082 Arslan, Prof. Dr. Çetin, Baştürk, İhsan, Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Veriler, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, cilt VIII, sayı:2, yıl:2013, s.209,210

1083 5411 sayılı Bankacılık Kanunu'nun 3. maddesinde “Kredi kuruluşu: Mevduat bankalarını ve katılım bankalarını”, “Banka: Mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını” ifade eder şekilde tanımlama yapılırken “Mevduat bankası: Bu Kanuna göre kendi nam ve hesabına mevduat kabul etmek ve kredi kullanılmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye’deki şubelerini”, “Katılım bankası: Bu Kanuna göre özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullanılmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye’deki şubelerini”, “Kalkınma ve yatırım bankası: Bu Kanuna göre mevduat veya katılım fonu kabul etme dışında; kredi kullanılmak esas olmak üzere faaliyet gösteren ve/veya özel kanunlarla kendilerine verilen görevleri yerine getiren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye’deki şubelerini” ifade eder şekilde tanımlamalara devam edilmiştir.

1084 **Y.8.CD. 29.04.2014 gün, 2013/9376-2014/10958.** “Sağığın, katılana ait eczane şifresiyle S.G.K.'nun bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçete bilgilerini silme şeklindeki eylemi nedeniyle hükmolunan cezanın S.G.K.'nun kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiğinin gözetilmemesi karşı temyiz bulunmadığından bozma nedeni yapılmamıştır.”

Bu nitelikli halin uygulanabilmesi için suçun konusunu oluşturan bilişim sisteminin bankaya, kredi kurumuna, kamu kurumu veya kuruluşuna ait olması gerekir. Bu kurumlara ait bir bilişim sisteminin işleyişinin engellenmesi, bozulması bu sistemdeki verilere yönelik müdahalelerde bulunulması halinde ceza artırılabilecektir. İfade edelim ki buradaki banka veya kredi kurumunun kamuya ait olması gerekmemektedir. Özel bir bankanın bilişim sistemine yönelik zarar verici fiiller bakımından da bu nitelikli hal gerçekleşir. Ancak diğer kurum veya kuruluşların “kamu kurum veya kuruluşu” olması şarttır. Böylece suçtan zarar görenin sıfatına göre bir nitelikli hal kabul edilmiş olmaktadır<sup>1085</sup>.

#### **4.Suçun Manevi Unsuru**

TCK.nun 244. maddesinde düzenlenen suçlar genel kasıtlı işlenebilen suçlardır. Özel kast aranmaz. Kast, doğrudan kast olabileceği gibi, olası kast da olabilir. Failin maddede belirtilen hareketleri kasten yapması yeterlidir. Yasada açıkça suçun taksirle işlenebileceği belirtilmediği için suçun taksirle işlenmesi mümkün değildir. Ancak 244. maddenin 2. fıkrasında tanımlanan hareketlerin gerçekleştirilmesiyle sistemin işleyişinin engellenmesi veya bozulması da mümkün olabilmektedir. Bu durumda da failin eyleminin hangi fıkraya göre cezalandırılacağına belirlenmesinde suçun unsuru olarak belirtilmemişse de faildeki amacın belirlenmesi gerekecektir<sup>1086</sup>.

#### **5.Hukuka Aykırılık Unsuru**

244. maddedeki eylemlerin, hukuka aykırı olarak gerçekleştirilmesi yeterlidir. Bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile sistemin çalışması korunurken, verilerin yok edilmesi veya değiştirilmesi suçu ile veriler üzerinde tasarruf yetkisi bulunan kişinin, verilere her hangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanmasındaki çıkarı korunduğundan, söz konusu bu hakların sahibinin ya da yetkilisinin rızası, hukuka uygunluk sebebini oluşturacaktır. Yani sahibinin veya kullanıcısının rızası, hukuka aykırılığı ortadan kaldıracaktır. Ancak bu rızanın fiilin işlenmesinden önce olması gerekir. Fiilin gerçekleşmesinden sonraki rıza fiili hukuka uygun hale getirmeyecektir.

#### **6.Suçun Özel Görünüş Şekilleri**

##### **a.Teşebbüs**

244. maddenin 1., 2. ve 4. fıkralarında düzenlenen suçlara teşebbüs mümkündür. Teşebbüs icra hareketlerine başladıktan sonra bu hareketlerin yarıda kalması şeklinde olabileceği gibi suçun

---

1085 Koca, age, s.95,96

1086 Dülger, age, s.435



icrasına ilişkin bütün eylemler tamamlandıktan sonra suçun oluşumu için aranan netice meydana gelmeden failin elinde olmayan nedenlerle suçun gerçekleşmemesi şeklinde de olabilecektir.

Ancak 244. maddenin 4. fıkrasında düzenlenen suçta failin amacı haksız çıkar elde etmek olduğundan, failin verilere müdahale etmesine rağmen eylemi neticesinde haksız çıkar elde edememesi durumunda teşebbüs hükmünün uygulanabilmesi için failin haksız çıkar sağlama kastının ortaya konması gerekecektir. Failin kastının hukuka aykırı çıkar elde etmek olduğunun ortaya konamaması durumunda failin maksadına bakılacaktır. Failin maksadı yalnızca verilere veya sisteme zarar vermekse, bu durumda maddenin 4. fıkradaki suça teşebbüsten değil, 1. veya 2. fıkradaki suçun tamamlanmış halinden hüküm kurulacaktır.<sup>1087</sup>

### **b.İştirak**

Madde metninde özel bir iştirak hükmüne yer verilmemiştir. Bu nedenle suçlara iştirak açısından bir özellik söz konusu olmayıp TCK.nun 37., 38., 39. ve 40. maddelerindeki suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir. Bu suçlara iştirak her zaman mümkündür.

### **c.İçtima**

244. maddenin 1., 2. ve 4. fıkralarında düzenlenen bu suçların zincirleme şekilde işlenmesi mümkündür. Örneğin failin okuduğu üniversitenin sistemine farklı zamanlarda girerek ders notlarını değiştirmesi halinde zincirleme suç hükümlerinin uygulanması gündeme gelecektir<sup>1088</sup>.

Burada en önemli bir sorun, 244. maddedeki suç oluştuğu zaman aynı zamanda TCK.nun 243/1. maddesindeki suçun da oluştuğu kabul edilecek ve ayrı ayrı cezalar mı tayin edilecek yoksa yalnızca TCK'nın 244. maddesindeki suçtan mı ceza verilecektir.

Yukarıda 243. maddenin uygulamasında da değinildiği gibi bu durumda geçitli suç hükümleri uygulanarak iki ayrı suçtan değil, yalnızca sonuç suçtan, yani TCK. nun.244. maddesi uyarınca ceza tayin edilecektir<sup>1089</sup>. Yani bir bilişim sistemindeki verileri değiştirmek isteyen fail, bu suçun icra hareketlerini gerçekleştirirken, sisteme de girmekte ve dolayısıyla 243. maddeyi de

---

1087 Dülger, age, s.451

1088 Y.8CD. 08.01.2014 gün, 2012/33044-2014/236.

1-Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince artırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması, 2-Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince artırılması gerektiğinin gözetilmemesi.

1089 Artuk – Gökçen – Yenidünya, age., s.4664, Ankara 2009

ihlal etmektedir. Bu itibarla, failin bu suçlardan yalnızca en ağır cezayı gerektiren 244. maddedeki suçtan dolayı cezalandırılması gerekecektir<sup>1090</sup>.

Bununla birlikte 15. Ceza Dairesi 15.11.2016 gün, 2016/3871-8608 sayılı ilamında “..sanık M.Ç’in olay tarihinde annesi F.Ç’in abonesi gözüktüğü 0 532... numaralı cep telefonu hattıyla müşteki Ç.D’in e-posta adresine şifresini kırmak suretiyle müştekinin izni ve bilgisi olmaksızın erişim sağladığı ve müştekinin erişimini şifresini değiştirerek engellediği, ardından da kendisine müşteki Ç.D’in arkadaşı P.N olarak tanıtarak para talep ettiği, müştekinin arkadaşı P. ile telefonla görüşerek söz konusu mailin P. tarafından gönderilmediği, P.’e ait mail adresinin başkalarınınca ele geçirildiğini öğrenmesi üzerine para göndermediği, sanığın bu şekilde üzerine atılı suçu işlediğinin iddia edildiği olayda” hem dolandırıcılık (158/1-f) hem de bilişim suçu (244/2) işlediğine karar vermiştir.

Bu suçun diğer bir özelliği ise tali norm niteliğinde olmasıdır. Nitekim madde metninde suçun bu özelliğini ifade etmek üzere fiilin başka bir suçu oluşturmaması gerektiğinden bahsedilmiştir. Bu durumda bilişim sistemleri aracılığıyla haksız çıkar sağlama şeklinde bir olayla karşılaşıldığında, ilk önce fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet gibi başka bir suçu oluşturup oluşturmadığı araştırılmalıdır. Şayet olayın gerçekleştiriliş şekli bu suçlardan birisinin tanımına uygun ise, bu suçlar işlenmiş olacaktır. Gerçekleştirilen fiil bu suçlardan birisinin tanımına uymuyorsa, o zaman 244. maddenin 4. fıkrası hükmü uygulanabilecektir. “Asli normun önceliği ilkesi” gereğince, bir fiil hakkında asli ve tali norm şeklinde iki hüküm bulunuyorsa, asli norm öncelikle uygulanacaktır<sup>1091</sup>.

TCK.nun 244. maddesinin 4. fıkrasının metnine göre bu fıkra düzenlenmiş suçu oluşturan fiil aynı zamanda başka bir suç oluşturuyorsa, diğer suçun daha ağır ya da hafif olması dikkate alınmaksızın olayda diğer suçun hükümleri uygulanacaktır. Gereğindeki aksine anlatıma rağmen maddenin 4. fıkrasında sözü edilen başka suçun cezasının daha ağır olması zorunlu değildir<sup>1092</sup>.

Yargıtay Ceza Dairelerince; failin bilişim sistemine şifre kırarak kirip, buradan aldığı fotoğrafı yayınlacağı tehditiyle para isteme şeklindeki eylemlerinin, şantaj, özel hayatın gizliliğini ihlal ve bilişim sistemine izinsiz girme suçlarını oluşturduğu ve gerçek içtima kurallarına göre her suçtan ayrı ayrı cezalandırılması gerektiğine (4. CD 18.03.2015 gün, 2014/2222, 2015/24755, mağdurun e-posta adresinden izinsiz olarak fotoğraflar ve video görüntüleri temin

---

1090 Taşdemir, age. aksi görüş Dülger age, sh 438

1091 Koca, age, s.97

1092 Dülger age, sh. 453

ederek katılanın arkadaşlarına göndererek ve arkadaşlarına gönderdiği fotoğraflar yanında katılana sövme içeren sözler sarfetmek eylemlerinde; 114/2, 125/2-1, 243/1. maddelerinde tanımlanan suçların oluştuğuna karar verilmiştir. (12. CD 03.01.2016, 2015/5933, 2016/277)

Yargıtay 8. Ceza Dairesinin kararlarında da belirtildiği gibi “Bilişim sistemleri aracılığıyla bir çıkar sağlandığında öncelikle bilişim sistemlerinin kullanılması suretiyle hırsızlık, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık, zimmet gibi bir başka suçun oluşup oluşmadığı tartışılmalı, eylem başka bir suçu oluşturmamışsa TCK.nun 244/4 maddesi irdelenmelidir. Örneğin şikayetçinin hesabına ilişim sistemi kullanılarak girmek suretiyle başka birinin hesabına şikayetçinin hesabından para havale etmek başka bir suçu (TCK m. 142/2-e) oluşturacağından TCK.nun 244/4. maddesi uyarınca mahkumiyet hükmü kurulamayacaktır<sup>1093</sup>.

### **7.Yaptırım**

TCK.nun 244/1. maddesinde öngörülen hürriyeti bağlayıcı ceza 1 yıldan 5 yıla kadar, 244/2. maddesinde ise 6 aydan 3 yıla kadar hapis olarak öngörülmüştür. Aynı maddenin 3. fıkrasında düzenlenen suçun nitelikli halinin gerçekleşmesi durumunda cezalar yarı oranında arttırılacaktır.

Bazen bilişim sistemindeki bir verinin değeri bilişim sisteminin kendisinden ya da işleyişinden daha değerli olabilir. Bu durumda hakim, TCK.nun 3 ve 61. maddesindeki argümanları kullanmalıdır.

TCK.nun 244/4 maddesinde düzenlenen bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçundan 2 yıldan 6 yıla kadar hapis ve birlikte 5000 güne kadar adli para cezası öngörülmüştür.

### **B- SORUŞTURMA VE KOVUŞTURMADA DİKKAT EDİLMESİ GEREKEN HUSUSLAR**

Bu madde kapsamında genellikle;

- (Facebook, twitter, instagram gibi) sosyal paylaşım sitesi hesabının şifresinin ele geçirilmesi, değiştirilmesi, hesabın kullanılamaması,

- Hesaptan bilgilerin ve resimlerin ele geçirilip sahte hesap açılması, hesap sahibinin yakınlarına arkadaşlık isteğinin gönderilmesi ya da hakaret içerikli iletiler gönderilmesi,

- Sahte hesap açılıp başkasına ait resmin kullanılması, hesapta başkalarının telefon numaralarının yazılması, bu şahsın fuhuş yaptığına dair ibarelerin eklenmesi,

- Hesabın ele geçirilerek hesap sahibinin arkadaşlarından zor durumda olduğu gerekçesiyle borç istenmesi ya da bir alışveriş merkezinden çekilişe katılacakları söylenip hile ile cep telefonu

ya da kredi kartı bilgileri alınıp harcama yapılması, cep telefonlarına ücretlendirme doğruacak işlem yapılması,

- Şirkete ait web sitesinin ele geçirilmesi, hesabın iadesi için para talep edilmesi,

- Şirkete ait hesap bilgilerinin eski çalışanın yetkisiz erişimi ile ele geçirilmesi, yeni çalıştığı rakip firmada aleyhe kullanılması,

- Okulun web sitesine girilerek ders notlarına müdahale edilmesi, sisteme erişimin engellenmesi, sitede bulunan öğrenci bilgilerinin başka yerlere gönderilmesi gibi iddialarla gündeme gelmektedir.

Örneklerden görüldüğü üzere TCK 244. maddesi yanında başka suçlar (TCK 134, 136, 158/1-f maddeleri) da gündeme gelebilmektedir.

Sisteme girme ve kalmaya devam etme suçunda uygulandığı üzere, bu suçlarda da özellikle soruşturma aşamasında kaybolacak deliller gecikmeksizin ve hukuka uygun olarak toplanmalıdır.

Sistemin işleyişine ya da içeriğine müdahale ile işlenen bu suçlarda suçun konusu olan sistem ve içeriği son derece önemlidir.

Müdahale edildiği söylenen sistem üzerinde herhangi bir değişiklik yapılmadan gerekli incelemenin yapılması, sisteme ya da içeriğine zarar verip verilmediği, verilmiş ise ne şekilde gerçekleştiği (virüs, solucan, trojen vs.), bilgi aktarılmış ise nereye aktarıldığı, başkasına yarar sağlanıp sağlanmadığı, (banka hesabından para transferi, cep telefonuna ya da internet faturasına ücret yansıtılması gibi) bu işlemler sırasında sisteme düşen IP adresi server ve log kayıtları üzerinde yapılacak inceleme ile tespit edilmeye çalışılmalıdır.

*“... İnternette kişisel amaçlı bilgi ve paylaşım için açtığı siteyi çalıştırmak için internet üzerinden sponsor hosting hizmeti veren şikayetçiye ait olan “Türkmno” adli siteden “CnnTurk” niki ile 23.09.2013 günü sponsor host istediği, onun da internet üzerinden gönderdiği, hostu alan ve olay günü “voLk4n” niki ile subdomain açıp shell adlı zararlı kodları şikayetçiye ait siteye yükleyerek hosting hizmeti verdiği siteleri hackleyip zarar verildiği iddiasıyla açılan davada, şikayetçinin dilekçesi ekinde biraz ettiği deliller dışında delil toplanmamıştır. Şikayetçinin ve suça sürüklenen çocuğun bilgisayarları üzerinde suç tarihine ilişkin LOG kayıtlarının karşılıklı olarak incelenmesi, suç tarihinde şikayetçinin sitesine izinsiz giriş yapan IP numaralarının ilgili servis sağlayıcısından tespiti, bilişim sistemindeki verilerin bozulup bozulmadığı, yok edilip edilmediği, değiştirilip değiştirilmediği veya erişilmez kılınıp kılınmadığı, sisteme veri yerleştirilip yerleştirilmediği, var olan verilerin başka bir yere gönderilip gönderilmediği saptanıp sonucuna göre, TCK.nun 244/2. maddesinde düzenlenen suçun oluşup oluşmadığı da değerlendirilerek suça*

*sürüklenen çocuğun hukuki durumun takdir ve tayini gerekirken, eksik incelemeye ve herhangi bir somut veriye dayanmadığı anlaşılan bilirkişi raporuna dayanarak yazılı şekilde hüküm kurulması, Yasaya aykırı, (BOZULMASINA)” (8. CD. 18.03.2015 gün, 2014/26822 E-2015/13964K)*

Sisteme düşen IP adresi kullanıcısı ilgili servis sağlayıcı şirketten (Türk Telekom, Turkcell, Avea, Vodafone, Superonline vs.) sorularak tespit edilebilir ise de, uygulamada yurt dışı kaynaklı IP adresi ya da NAT uygulamasında kullanılan (ağ adresi dönüşüm uygulamasında kullanılan) IP adresi olması, kaynak IP ve port bilgisine ihtiyaç duyulması gibi nedenlerle kullanıcıya ulaşılamamakta ya da daha önce vurgulandığı üzere toplu kullanım alanlarında sisteme girilmesi nedeniyle failin tespiti imkansızlaşmaktadır.

Bu durumda şüphelenilen şahıs varsa onun kullandığı dijital materyaller üzerinde inceleme yapılması, ayrıca lehine yarar sağlanan kişi ya da kişiler yönünden de araştırma yapılması gerekmektedir. Ancak bu da kesin çözüm değildir. Keza lehine yarar sağlanan kişilerin de çoğu zaman eylemden haberdar olmadıkları, örneğin bir banka hesabından kendi hesabına para transferi yapılan şahsın bu eylemden haberdar olmadığı, zira menfaatin daha sonra bir başka hesaba ya da (sahte isimle başkası adına çıkartılmış) cep telefonuna aktarıldığı görülmektedir.

Şüpheliye ait dijital materyallerde inceleme yapılırken olay tarihi ve zamanı tüm ayrıntısıyla tespit edilmeli, hangi kullanıcı ile internete bağlandığı, olaya ilişkin veri olup olmadığı belirlenmeli, yine müşterki ya da başkalarına ait benzer kişisel ya da hesap bilgileri olup olmadığı, şifre kırıcı programın kullanılıp kullanılmadığı ya da başka kullanıcılar ile benzer konularda bağlantı kurulup kurulmadığı araştırılmalıdır.

Bir hesap bilgisine girilmesi ve ödeme yapılması (oyun satın alınması, telefon ya da internet faturası ödenmesi) gibi durumda sanal ortamda ödeme işlemleri yapan şirketler aracılığıyla işlem hakkında bilgi temini sağlanabilecektir.

Eğer lehine yarar sağlanan bir cep telefonu abonesi tespit edilebilirse, bu transferin hangi IP adresi üzerinden yapıldığı ve cep telefonu abone bilgileri ilgili GSM şirketinden temin edilebilecektir.

Eğer bir banka, şirket ya da kurumun bilişim sistemine girildiği iddiası varsa, öncelikle söz konusu banka/kurum/şirketten yapılan işlemin niteliği, sisteme ne şekilde girildiği, sisteme girildiği sırada düşen IP adresi tespit edilip edilemediği, bu işlem ile bilgi ya da para transferi olup olmadığı, yapılmış ise hangi cep telefonu, hesap ya da sisteme aktarıldığı hususları ayrıntılı olarak sorulmalıdır.

Bir başka hesaba ya da cep telefonuna para aktarılması söz konusu ise, bu paranın ne suretle harcandığı, nereden çekildiği ilgili banka ya da GSM şirketinden sorulmalı, varsa kamera görüntülürü gecikmeden temin edilmelidir. Eğer bir bankadaki hesaptan başka hesaba para aktarma söz konusu ise, her iki hesabın bağlı olduğu bankalardan ayrıntılı bir şekilde hesap hareketleri istenmeli, şüpheli konumunda bulunan şahısların hesabına başka yerlerden de benzer para transferi olup olmadığı incelenmelidir.

### **C.TCK. NUN 244. MADDESİ İLE İLGİLİ YARGITAY KARARLARI**

1.Sanığın, katılana ait eczane şifresiyle S.G.K.'nun bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçete bilgilerini silme şeklindeki eylemi nedeniyle hükmolunan cezanın S.G.K.'nun kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiğinin gözetilmemesi karşı temyiz bulunmadığından bozma nedeni yapılmamıştır. (Y.8.CD. 29.04.2014 gün, 2013/9376-2014/10958)

2.Sanığın; SGK.nun bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçeteleri sistemden silmek şeklindeki eylemi nedeniyle hükmolunan cezanın SGK.nun kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden, yazılı şekilde hüküm kurulması aleyhe temyiz bulunmadığından bozma nedeni yapılmamıştır. (Y.8.CD. 15.04.2014 gün, 2013/9180- 2014/9692)

3.Sanık hakkında düzenlenen ve davanın temelini oluşturan 23.09.2011 tarihli iddianamede; "şüphelinin, şikayetçinin arkadaşı olan Fatma'ya ait mail adresini ele geçirerek, şikayetçi ..... ile yazışıp ona cinsel taciz ve tehditte bulunduğu belirtilerek" dava açılmış olup, CMK.nun 225. maddesi uyarınca hükmün konusunun iddianamede açıklanan fiil olduğu, iddianamede yer almayan olaylara ilişkin yargılama yapılamayacağı gözetilmeden sulh ceza mahkemesinin iddianame kapsamı dışına çıkarak "sanık tarafından şikayetçinin msn ve facebook şifrelerini ele geçirip değiştirilerek erişimin engellendiği, şikayetçinin başka bir mail adresi edinerek, sanıkla iletişime geçtiğinde, sanığın tehdit, hakaret ve cinsel tacizde bulunduğundan" bahisle verdiği görevsizlik kararına dayanılarak ve bilişim sisteminin ne şekilde engellendiği ve değiştirildiğine ilişkin kanıtların neler olduğu da kararda gösterilip tartışılmadan TCK.nun 244/2. madde ve fıkrası ile mahkumiyet hükmü kurulması, (24.09.2013. 2012/30296- 2013/23181 SB. 8. CD)

4.5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 100. maddesinde yer alan "Elektronik ortamda hazırlanacak bilgi ve belgeler adli ve idari makamlar nezdinde resmi belge olarak geçerlidir." şeklindeki düzenleme karşısında sanığın bir başkasına ait şifreyi

kullanarak çalışmayan kişilerin çalışmaya başladıkları yönünde e-bildirge hazırlaması şeklindeki eyleminin resmi evrakta sahtecilik suçunu oluşturup oluşturmayacağı tartışılmadan yazılı şekilde karar verilmesi, (Y.8. CD. 12.12.2013. 2012/31922-2013/29069.)

**5.**Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturularak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması, (Y.8. CD. 24.06.2013 gün, 2012/32866-2013/18872)

**6.**Oluşa ve dosya kapsamına göre, mağdure F.Ç'nin işvereni olan Av.A.A'nın facebook şifresini bir şekilde ele geçiren sanığın, bu adresten mağdure ile A.A gibi yazışarak 700 TL'lik kontör kartı alırdır şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK.nun 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturabileceği ve bu suça bakma ve delilleri takdir etmenin ağır ceza mahkemesine ait olmasına karşın, görevsizlik kararı verilmeyerek yargılamaya devamla yazılı şekilde hüküm kurulması, (24.12.2012. 2012/21826-2012/39370. SB. Y. 8. CD)

**7.**Oluşa ve dosya kapsamına göre; şikayetçiler K.T, Z.V, Ö.Ş isimli kişilere ait msn adreslerini kırarak ilgili adreslerdeki kişilerin arkadaşlarından onlarmış gibi yazışarak kendine yarar sağlamak amacı ile kontör talep edip şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK.nun 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturup oluşturmayacağına ilişkin delilleri takdir ve tartışmanın 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanununun 12. maddesi uyarınca ağır ceza mahkemesinin görevinde bulunduğu gözetilerek görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı biçimde hüküm kurulması, (Y. 8. CD. 18.12.2013. 2013/735- 2013/29491 SB.)

**8.** 1-Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması,

2- Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması gerektiğinin gözetilmemesi, (Y. 8. CD. 08.01.2014. 2012/33044- 2014/236. SB.)

**9.**Sanık E.A'nın, internet platformu hazırlamak ve işletmek amacıyla faaliyet gösteren katılan şirket bizimalem.com adlı bir site ile arkadaş bulmak, forumlarda bilgi alışverişi yapmak, sohbet etmek, oyun oynamak üzere üye kaydı esasına göre çalışan bir sistemine girip onun işleyişini engellediği, kayıtlarını ve bazı bilgilerini başka bir siteye aktardığından bahisle açılan davada, sanığın suçlamayı kabul etmediği, sitenin kendisine iş teklif ettiği, bu nedenle hesap numarası istendiğinde kendisinin bir bankada hesabı olmadığından tanıdığı olan internet cafe sahibinin hesabını bildirdiğini, daha sonra kendisine gönderilen sözleşmenin sözlü anlaşmaya uygun olmadığını görünce vazgeçtiğini, bu nedenle kendisine iftira atıldığını savunması, mahkemece alınan bilirkişi raporunda yukarıdaki fiillerin başkasına ait internet cafeden gerçekleştirildiğini, anılan web sitesinin işletim sistemine girmek, çökertme işlemlerinin gerçekleştirilmesinin zor olup uzmanlık veya şans gerektirdiği, internet cafeye ait bilgisayarların hard diskleri üzerinde yapılan incelemede yabancı MSN, Hotmail kullanıcılarının olduğunun saptandığı, bunun amacının, katılana ait site üyelerini sanığın sitesine yönlendirme ve tüm bilgilerini buraya aktarmak olduğu, katılan şirket yöneticisi ile sanığın görüntülü görüşmelerinin bulunduğu belirtilmiş ise de dosya içindeki belgeler arasında sanığın görüntüsünü içeren bir belgeye rastlanmadığı gibi yapılan işlemleri açıklamaktan uzak olduğu dikkate alındığında, bu konuda uzman bilirkişi heyeti vasıtasıyla yeniden inceleme yapılarak sanığın atılı suçu işlediğine ilişkin delillerin kesin olarak neler olduğunun saptanması gerekirken yetersiz bilirkişi raporuna dayanarak yazılı şekilde hüküm kurulması, (Y.11. CD. 27.03.2013. 2011/5893-2013/5065)

**10.**Katılanların ortağı ve yöneticisi oldukları ..... Turizm Organizasyon Hizmetleri ve ..... Kongre Organizasyon Ticaret Limited Şirketinin sigortalı çalışanları olan sanıkların, mülkiyeti anılan şirketlere ait olup sanıkların kullanımına bırakılan bilgisayarlardan, şirketlerin faaliyet alanları nedeniyle gelen e-mail tekliflerini ve müşteri portföylerini kopyalayarak şahsi e-mail adreslerine aktardıkları gibi mevcut bilgisayarlardan bu teklif e-mail'lerini silerek daha sonra kendilerinin ortak olarak kurdukları şirketleri olan ..... Turizm Organizasyon Ltd. Şirketine aktardıkları somut olayda, suça konu verilerin güveni kötüye kullanma suçunun konusunu oluşturan eşya kavramı içerisinde değerlendirilemeyeceği de dikkate alındığında, 5237 sayılı TCK'nun 244/2-4. maddesinde yazılı "bilişim suçunu" oluşturduğu gözetilmeden, sanıkların eylemlerinin aynı Kanunun 155/2. maddesinde düzenlenen "hizmet nedeniyle güveni kötüye



kullanma" suçunu oluşturduğundan bahisle yazılı şekilde hüküm tesisi; (Y. 11. CD.18.09.2013 gün, 2012/2764- 2013/13257. )

**11.**Katılana ait hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması, (Y. 8.CD. 24.06.2013 gün,2012/32866-2013/18872)

**12.**TCK.nun 245/1. maddesinde yazılı suçun oluşabilmesi için, her ne suretle olursa olsun ele geçirilen bir kredi veya banka kartının ATM cihazında kullanılması yahut alışveriş yapılması, bu suça teşebbüs için de kartın kullanılmasına yönelik icra hareketlerine başlamış olması gerektiği cihetle,

Somut olayda; ATM'de tertibat aldıktan sonra kart yuvasına kurduğu düzeneğe sayesinde, şikâyetçinin kartının sıkışmasını sağladıktan sonra yardım bahanesiyle yaklaşp, kartın şifresini öğrenmeye çalıştığı, şikâyetçinin durumdan şüphelenip şifresini vermemesi üzerine sanığın makinedeki düzeneği ve kartı çıkartıp şikâyetçiye vermek şeklindeki eylemde; kartın sıkışmasını sağlamak için yerleştirilen aparatın takılı olduğu süre boyunca bilişim sisteminin bir parçası olan ATM'nin kullanılmaması karşısında; gerçeğin ve suç niteliğinin kuşkuya yer vermeyecek şekilde belirlenebilmesi için ATM üzerinde gerçekleştirdiği hareketlerinin ayrıntılı olarak tespiti ile bu hareketin bir bilişim sisteminin parçası olan ATM'nin kısa süreliğine de olsa çalışmasına engel teşkil edip etmediği, bağlı bulunduğu bilişim sistemi veya cihaza bir zarar verip vermediği hususları ilgili banka şubesinden sorulup, bu hususta gerektiğinde bilirkişi raporu da alınarak, cihazın ait olduğu banka davadan haberdar edildikten sonra, sanığın hukuki durumunun takdir ve tayini gerektiği ve suça konu kartın sanık tarafından ele geçirilmediği ve kullanılmadığı gözetilmeden, eksik soruşturma sonucu yazılı şekilde hükümler kurulması, (Y. 8. CD.12.03.2014 gün, 2013/13519- 2014/6128) (Banka veya kredi kartlarının kötüye kullanılması ve hırsızlık suçlarından hüküm kuruldu)

**13.** 2797 sayılı Yargıtay Yasasının 6110 sayılı Yasa ile değişik 14. mad- desinde “Ceza Dairesinde, Daireler arasındaki işbölümünün belirlenmesinde, dava açılan belgedeki nitelendirme esas alınır. Açıklama ile sevk maddelerinin uyumsuz olduğu durumlarda, açıklamaya itibar edilir” hükmü yer almaktadır. Yasa, sevk maddelerine değil, iddianamedeki tavsife ağırlık tanımıştır. Bu nedenle Ceza Dairelerinin görevinde Ceza Daireleri Başkanlar Kurulunun yerleşik kararlarında da belirtildiği üzere tavsif esas alınmalıdır.

Adana Cumhuriyet Başsavcılığı'nın iddianamesine göre sanığın şikâyetçinin interaktif banka hesabına internet aracılığıyla girerek kendi hesabına para transfer edip çekmeye çalıştığı iddia olunması karşısında; Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün ve 193/268 sayılı kararında açıklandığı üzere 5237 sayılı TCK'nun 142/2-e maddesinde öngörülen “bilişim suretiyle hırsızlık” suçu tavsif edilerek dava açılmıştır.

Bu itibarla, iddianamedeki anlatıma, temyizın kapsamına ve Yargıtay Kanununun 14. maddesine göre temyiz inceleme görevinin Yüksek (2.) Ceza Dairesine ait olduğu anlaşıldığından; Dairemizin görevsizliğine, dosyanın görevli daireye gönderilmesine. (Y.8.CD.02.06.2014 gün, 2013/4709-2014/13494)

**14.**Oluşa ve dosya kapsamına göre, sanığın 20.09.2006 tarihinde İzmir/Bornova'da bulunup tank V.A'nın tarafından işletilen internet kafeye giderek burada bulunan bilgisayarlardan biriyle gündüz sayılan saat 15:58-16:06 saatleri arasında yaptığı 7 ayrı internet bankacılığı işlemi ile, Akbank İstanbul/İstinye/Carrefoursa şubesindeki katılana ait banka hesabına bağlı internet şubesi hesabına katılanın bilgi ve rızası dışında girip hesaptaki döviz ve hazine bonolarını bozdurarak ve hesapta bulunan nakit parayı da kullanıp toplam 57.500 TL'yi aynı bankanın İzmir/Konak şubesinde bulunan kendi adına açtığı hesaba havale yoluyla aktardıktan sonra 21.09.2006 günü yine aynı bankanın Konak, Hatay ve Buca olmak üzere 3 ayrı şubesinden 20.000, 15.000 ve 22.500 TL şeklinde parça parça çektiği olayda; sanığın eyleminin 5237 sayılı TCK'nın 142/2-e düzenlenen bilişim sisteminin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden, eylemin vasıflandırılmasında yanılıya düşülerek yazılı şekilde aynı Yasanın 244/4. maddesi ile hüküm kurulması. (Y.6. CD. 27.05.2014 gün, 2012/7246- 2014/10715)

**15.**Sanıkların haksız bir şekilde ele geçirdiği yakına ait internet bankacılık şifresini kullanmak suretiyle, yakınının Yapı Kredi Bankası Harput Şubesinde bulunan hesabından, sanık M.E.K'nin hesabına 2070 TL havale yapıp, bankamatik kartı ile sanık U.A tarafından paranın çekildiğinin anlaşılması karşısında; yakınının banka hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanan sanıkların tamamlanan eylemlerinin Yargıtay Ceza Genel Kurulunun 17.11.2009 tarih ve 11-193/268 sayılı kararında da ayrıntıları açıklanan 5237 sayılı TCK'nın 142/2-e maddesine uyan suçu oluşturduğu dikkate alınmadan suçun vasfında yanılıya düşülerek yazılı şekilde uygulama yapılması. (Y.6. CD. 30.06.2014 gün, 2012/3216- 2014/13608)

**16.**Sanıkların, katılanın banka hesabına bilgisi dışında internet yoluyla erişim sağlayarak, hesabındaki parasını sanık Ş.T'nin hesabına havale etmeleri şeklinde gerçekleştiği kabul edilen eyleminin 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen hırsızlık suçunu oluşturduğu

gözetilmeden, yazılı şekilde aynı Kanunun 244/4 maddesi uyarınca hüküm kurulması. (Y.2.CD. 19.06.2014 gün, 2014/22676-2014/17536)

**17.** Katılanın rızası olmaksızın ele geçirdiği kredi kartı bilgilerini internet üzerinden mail order yöntemiyle kullanan sanığın eyleminin bir bütün olarak TCK.nun 245/1. maddesinde düzenlenen banka veya kredi kartının kötüye kullanılması suçunu oluşturduğu ve suça konu eylemin işlendiği internet sitelerine yönelik hukuka aykırı bir fiil bulunmadığı gözetilmeden, TCK.nun 244. maddesinde düzenlenen ve olayda unsurları bulunmayan bilişim sistemine girme suçundan mahkumiyet kararı verilmesi, (Y.8.CD. 08.05.2014 gün, 2013/4704-2014/11881)

**18-** Katılana ait hotmail adresine hukuka aykırı olarak giren ve yeni şifre oluşturup katılanın erişimini engelleyerek e-mail adresini kullanan sanığın eylemine uyan TCK.nın 244/2. madde ve fıkrası uyarınca cezalandırılması gerektiği gözetilmeden yazılı şekilde beraat kararı verilmesi (Y. 8. C.D. 23.06.2014 gün, 2013/771- 2014/15833)

**19-** Şikayetçinin 01.11.2011 tarihinde internette KNİGHT ONLINE WORLD isimli oyunu oynarken ...@hotmail.com.tr adresinden arkadaşlık teklifi geldiğini, bu teklifi kabul ederek karşıdaki şahısla bu adresten konuştuğunu, tekrar oyuna döndüğünde oyun şifresinin çalınıp oyun karakterlerinin aldığından bahisle açılan davada, sanığın suçlamayı kabul etmemesi, anılan mail adresini kullanmadığını savunması, adli bilişim büro amirliğinin 17.07.2013 tarihli imaj alma tutanağında, sanığın evinde mikro-2 GB SD kart üzerinde yapılan incelemede suç unsuruna rastlanılmadığının bildirilmesi, bilirkişi tarafından düzenlenen 01.04.2014 tarihli raporda, oyun şifresini çalacak kadar bilgi ve beceriye sahip bir kişinin işlemi yapmış olduğu, bilgisayarın kullandığı IP adresinin de sisteme düşeceğini bileceği değerlendirildiğinden suçu işlediği hususunda kanaat oluşmadığının belirtilmesi, microsoft şirketinden gelen cevapta ...@hotmail.com.tr adresine girenler arasında sanığa ait IP numarasına rastlandığı ancak başka IP numaralarının da olduğu halde araştırılmaması karşısında, anılan mail adresinin bilgilerinin bağlı olduğu şirketten sorulup, suç tarihinde kimin kullanımında olduğunun belirlenmesi, oyun sitesinden suç tarihinde, şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemin TCK.nun 244/4. maddesindeki suçu oluşturacağı da dikkate alınarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, (Y. 8. C.D. 25.05.2017 gün, 2017/897 – 6019)

**20-** Aşamalarda sanığın şifreyi değiştirdiğini beyan etmesi karşısında; şikayetçi A. B.'a ait Facebook ve e-mail adreslerine girerek şifreleri değiştirmek suretiyle erişilmez kılan sanığı neyleminin TCK.nun 244/2. maddesinde düzenlenen suç oluşturacağı gözetilmeden aynı maddenin 1. fıkrası ile hüküm kurulması (8. C.D. 17.05.2017 gün, 2016/10061 - 2017/5649)

**21-** Sanığın G... Eczanesi sahibi, sanık H. B. ile M. C. G.'ün ise kalfa olarak çalıştıkları, Medula sistemini kullanmaya yetkili sanıklar H. B. ile M. C. G.'ün olay tarihlerinde kendi çalıştıkları G... Eczanesi'nin şifresi ve katılan A. T.'ya ait T.. Eczanesi'nin haksız şekilde elde ettikleri Medula sistemine giriş şifresi ile önce hayali bir reçetenin eczanelerden birinin şifresiyle ..... Eczane sistemine giriş yapıldığı, hayali reçete ..... Eczane Sistemine kayıtlı iken bu kez diğer eczanenin sisteminden giriş yapılarak gerçek reçetenin sisteme kaydedildiği, hayali reçetenin sisteme kaydedilmesi ile hasta muayene ücretinin çıktığı, ancak hayali reçete sistemde kayıtlı bulunduğu halde diğer eczaneden gerçek reçetenin girişi yapıldığında muayene ücretinin çıkmadığı ve reçetenin karşılandığı, bu kez gerçek reçete karşılandıktan sonra hayali reçetenin sistemden silindiği ve hastaya ait muayene ücretinin bu işlemle bir sonraki ilaç alışına kadar ötelenerek bilişim sistemindeki verileri bozma, yok etme, sisteme veri yerleştirme suçunu işlediklerinden bahisle açılan davada; sanıkların sübut bulan eylemlerinde, dosya kapsamından yapılan işlemlerin katılan kurumun alacağını geciktirmekten ibaret olduğu, ortadan kaldırmadığı, bu surette bir haksız menfaat elde edilmediğinin anlaşılması karşısında, katılan A.T.'ya ait eczanenin şifresini haksız ele geçirip bunun vasıtasıyla Sosyal Güvenlik Kurumu'na ait bilişim sistemine giriş yapıp sahte veri yerleştirip amacına ulaştıktan sonra silmek şeklindeki eylemin TCK.nun 244/2 ve 3. maddelerindeki suç kapsamında değerlendirilmesi gerektiği gözetilmeden anılan maddenin 4. fıkrasıyla hüküm kurulması, (Y. 8. C.D. 31.05.2017 gün, 2016/12437 – 2017/6369 benzer 2016/6938 – 9936)

**22-** Katılanlar Akbank ile Finansbank adlarına vekillerinin temyiz istemlerinin bankalarına ait bilişim sistemlerine girip sahte internet siteleri oluşturmak ve bu suretle müşteri bilgilerini elde ederek kayıt etmek suçlarına yönelik olduğu anlaşılacakla,inceleme bu suçlarla sınırlı olarak yapılmıştır.

Sanıkların Akbank TAŞ ile Finansbank AŞ. adlarına sahte internet siteleri oluşturup sahte site sayfası açarak katılan bankaların müşterilerine sahte e-mailler gönderilerek sahte oluşturulan internet sayfaları ile ilgili yanıltıcı bilgiler verilerek güncelleme VS adı altında kişisel bilgilerini ve şifrelerini girmelerini istedikleri, bilgisayar çıktısında liste halinde belirlenen birçok bankaların müşterisinin bu sahte e-maillere inanarak verilen kişisel bilgileri ve banka şifrelerini dosyası tefrik

olunan suça sürüklenen çocuk B.B.'ın e- mail hesaplarında depolamaktan ibaret eylemlerinin TCK.nun 244/2 ve 136. maddeleri kapsamındaki suçları oluşturduğu, sanıklara yüklenen suçların yasa maddelerinde öngörülen cezalarının türü ve üst sınırları itibariyle tabi oldukları 5237 sayılı TCK.nun 66/1-e maddesinde belirlenen 8 yıllık dava zamanaşımının, zamanaşımını kesen son işlem olan sanıkların savunmalarının alındığı tarihler olan 17.09.2008 ve 27.05.2009 tarihlerinden temyiz inceleme tarihine kadar gerçekleştiği anlaşılmış ve katılanlar vekillerinin temyiz itirazları bu nedenle yerinde görülmele sair yönleri incelenmeyen hükümlerin 5320 sayılı Yasanın 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK.nun 321. maddesi uyarınca BOZULMASINA, ancak yeniden yargılama yapılmasını gerektirmeyen bu hususta anılan Yasanın 322. maddesinin verdiği yetkiye dayanılarak karar verilmesi mümkün olduğundan sanıklar hakkında açılan kamu davalarının gerçekleşen dava zamanaşımı nedeniyle 5237 sayılı TCK.nun 66/1-e ve CMK.nun 223/8. maddeleri gözetilerek DÜŞÜRÜLMESİNE, (Y. 8. C.D. 07.06.2017 gün, 2016/12067 – 2017/6651)

**23-** Şikayetçinin e-mail ve facebook hesaplarına ait şifrelerinin elde edilerek değiştirilmesi nedeniyle erişemediğini, bu şifrelerle oyun oynadığı sitedeki oyun karakterlerinin de çalındığını, daha sonra e-mail şifresini geri aldığını ancak facebook şifresini alamadığını belirterek şikayetçi olması, sanığın suçlamayı kabul etmeyerek, bilgisayardan anlamadığını, sadece oyun oynadığını, oğlunun da bilgisayarı kullandığını savunması, şikayetçinin mail adresine girenler arasında sanığa ait IP numarasına rastlandığı ancak başka IP numaralarının da olduğu halde evrakların tefrik olması nedeniyle Manisa Cumhuriyet Başsavcılığında bulunan soruşturmanın akıbetinin araştırılmaması karşısında, anılan mail ve facebook adreslerinin bilgilerinin bağlı olduğu şirketten sorulup, suç tarihinde kimin kullanımında olduğunun belirlenmesi, Manisa Cumhuriyet Başsavcılığı'nın 2014/731 soruşturma nolu evrakın akıbetinin sorulması, yetkisizlik kararı verilmişse ilgili Cumhuriyet Başsavcılığında bilgi istenmesi, sanığın oğlu T. D.'in CMK.nun 48. maddesi uyarınca dinlenmesi, şikayetçiden hangi oyun sitesinde oyun oynadığı ve çalındığı iddia olunan karakterleri sorulup ilgili oyun sitesinden suç tarihinde, şikayetçinin kullanıcı adı ve şifresiyle hangi IP numaraları ile oyuna giriş yapıldığı tespit edilip, çalındığı iddia edilen oyun karakterine ait sanal eşyaların suç tarihinden itibaren kimin kullanımında olduğu araştırılarak tüm deliller birlikte değerlendirilip sübutu halinde eylemin TCK.nun 244/2 veya 244/4. maddelerindeki suçları oluşturup oluşturmayacağı değerlendirilerek sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, (Y. 8. C.D. 13.12.2017 gün, 2017/1283-14186)

**24-** Oluşu ve tüm dosya kapsamına göre; hakkındaki dosya tefrik edilen M.G'nin işletmekte olduğu, katılan kurum ile anlaşması olmayan fatura ödeme merkezinde kurulu bulunan bilgisayar üzerinden katılan kurumdan emekli vezne şefi A.A'ya ait kullanıcı kodu ve şifresi kullanılarak ASKİ'nin fatura ödemelerinin yapıldığı sistemine girildiğinin ve sanığa ait toplam 1027.40 TL tutarındaki faturaların ödenmediğinin, sanığın ise borcundan dolayı kapalı olan su aboneliğine ait faturalarının kim tarafından ödendiğini bilmediğine yönelik suçtan kurtulmaya yönelik savunmada bulunduğu anlaşılmaması karşısında sanığın atılı suçtan mahkumiyeti yerine yazılı şekilde beraatine hükümlenmesi, (Y. 8. CD 2013/12582, 2014/10065)

**25-** 08/01/2014 günü saat 14:30 sıralarında kurumsal ve resmi olarak kullandıkları "www.igdirkhb.gov.tr" web sitesine yönetim menüsü altında idari ve mali işler başkanı linkine tıkladığında normalde çalışması gereken sayfa olan "www.igdirkhb.gov.tr/idari.php"nin açılmayarak bu sayfanın yerine "yilsan.net/index.html" isimli web sitesinin açıldığını, sitenin bu şekilde yönlendirildiğini, yönlendirilen sitede kuruma yakışmayan yazı, resim ve müziklerin olduğundan bahisle açılan davada, sanığın suçlamayı kabul etmemesi,şikayetçi idarenin internet sitesine girenler arasında sanığa ait IP numarasına rastlandığı ancak başka IP numaralarının da olduğu halde evrakın tefrik olması nedeniyle diğerlerinin Iğdır Cumhuriyet Başsavcılığı'nda bulunan soruşturmanın akıbetinin araştırılmaması karşısında, Iğdır Cumhuriyet Başsavcılığı'nın 2014/2212 soruşturma nolu evrakın akıbetinin sorulması, yetkisizlik kararı verilmişse ilgili Cumhuriyet Başsavcılıklarından bilgi istenmesi,dava açılmışsa dava dosyalarının getirilmesi, incelenip birleştirilmesi, mümkün değilse bu davayı ilgilendiren delillerin onaylı örneklerinin dosyaya konulması, sonucuna göre sanığın atılı suçu işlediğine ilişkin şikayetçi kurum tarafından verilen LOG kayıtlarından saptanan IP numarası tespiti dışındaki delillerin varlığı da karar yerinde gösterilerek hüküm verilmesi gerekirken eksik incelemeye dayanarak yazılı şekilde karar verilmesi, (Y. 8. CD 2018/1759, 2018/2386)

**26-** Katılanın alt bayi olarak internet sitesi üzerinden kontör alım satımı ve fatura ödemeleri gerçekleştirmek üzere kendisine verilen şifre bilgilerini bilgisini ve rızasını olmaksızın ele geçirerek kontör satışı gerçekleştirmekten ibaret eylemlerin TCK.nun 142/2-e maddesi kapsamındaki suçu oluşturacağı gözetilmeden ve bilişim sistemi üzerinde çalışmasını engelleyecek girişimde bulunup veri değiştirerek haksız menfaat elde ettiklerine dair delil bulunmadığı halde suç vasfından yanılığa düşülerek yazılı şekilde hükümler kurulması,

Suç tarihi itibarıyla 18 yaşını ikmal etmeyen suça sürüklenen çocuk hakkında 5237 sayılı TCK.nun 53/4. madde ve fıkrasına aykırı olarak aynı Yasanın 53/1. madde ve fıkrasında yer alan hak yoksunluklarına hükmolunması, (Y. 8. CD 2016/12723, 2017/5659)

**27-** ... oyun sitesine girerek katılanın gerek ücreti karşılığında gerekse level atlama şeklinde kazandığı oyun karakterini ele geçirmek şeklindeki eyleminin, sübutu halinde bilişim suretiyle hırsızlık suçunu oluşturacağı (8. CD 17.02.2016, 2015/14257, 2016/1702)

**28-** Hakkı hükmün açıklanmasının geri bırakılması kararı verilen sanıklardan M.A'nın, e-bildirge ile bilgisayar ortamında sahte işe giriş bildirgesi düzenleyerek, işyerinde çalışmayan sanığı sigortalı olarak gösterdiği ve bu suretle iştirak halinde resmi belgede sahtecilik suçunu işlediklerinin iddia ve kabul olunduğu olayda; imza ve şifre ile bilgisayar ortamında işe giriş bildirelerinin verilmesi eyleminde, sahte oluşturulmuş maddi ve somut bir belge olmadığı, eylemin bu hali ile TCK.nun 244/2. maddesinde yazılı "sisteme veri yerleştirme" suçunu oluşturduğu gözetilmeden, suç niteliğinde yanılı ile yazılı şekilde resmi belgede sahtecilik suçundan hüküm kurulması, (11. CD 27.11.2017, 2015/8801, 2017/8230)

**29-** Sanığın katılanın telefon hafıza kartını bir şekilde ele geçirip facebook şifrelerini de kırarak bu hesabı kullanmaya başlayıp elde ettiği fotoğrafları facebooktan yaymaya başlayacağını söyleyerek kendisiyle görüşmeyed evam etmesi için kendine ait telefonda katılana ait telefona gönderdiği "elimde görüntülerin var, bunları yayınlayacağım", "faceteki resimleri beğendiysen değiştireyim mesela oteldeki faturayı ya da seni s.... görüntüleri koyayım", "Nazillideyim gel görüşelim yoksa orayı başınıza yıkarım haber bekliyorum", "benim sana yaptığım masrafı yollamazsan 29 Nisan gecesi ..... Otelde kaldığımızı belgeleyen faturayı bütün Nazilli'ye, eşine, ailesine yollarım, kesinlikle haber bekliyorum en geç yarına" gibi mesajların içerikleri ve tüm dosya kapsamına göre, sanığın şantaj, bilişim sistemine girme ve özel hayatın gizliliğini ihlal suçlarını işlediği anlaşılınca, TCK:nun 107/2, 243/1 ve 134/2. maddeleri uyarınca cezalandırılması gerekirken, yerinde olmayan gerekçelerle beraat hükümleri kurulması, (4. CD 18.03.2015, 2014/2222, 2015/24755)

**30-** Sanığın, katılan ile internette tanıştığı ve bir süre telefonda ve msn üzerinden görüntülü görüşerek arkadaşlık yürüttüğü, sanığın teklifi üzerine katılanın, kendisi, kızı ve sanık ile birlikte bir otelde yaklaşık 1 hafta süreyle tatil yaptıkları, arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı elektronik posta adresine rızası dışında birçok kez girdiği olayda, sanığın, bu şekilde eyleminin TCK.nun 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu ve mahkemenin hükmün gerekçesinde de eylem bu şekilde kabul edildiği halde, sanık hakkında

bilişim sistemine girme suçu yerine, TCK.nun 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan hüküm kurulmak suretiyle sanık hakkında fazla ceza tayini, (12. CD 13.01.2016, 2015/15933, 2016/277)

**31-** ... Bilişim sisteminde yapılan işlemler sonucu devamsızlık ve not düzeltmelerin dışında sağlandığı belirtilen haksız menfaatlerin ne olup kim tarafından sağlandığı karar yerinde açıklanıp tartışılmadan yetersiz gerekçe ile yazılı şekilde TCK.nun 244/4. maddesinin uygulanması (8. CD 15.02.2017, 2016/3794, 2017/1405)

**32-** ...TCK.nun 244/4. maddesindeki "yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde" şeklindeki düzenleme karşısında; şikayetçinin hesabına bilişim sistemi kullanılarak girmek sureti ile başka birinin hesabına şikayetçinin hesabından 4.985 TL havale etmek şeklindeki eylemin, TCK.nun 142/2-e madde ve fıkrasında yer alan nitelikli hırsızlık suçunu oluşturduğu gözetilmeden, TCK.nun 244/4. maddesi uyarınca mahkumiyet hükmü kurulması, ( 8. CD. 21.05.2018, 1115-5608)



### KAYNAKLAR

**Arslan, Prof. Dr. Çetin, Baştürk, İhsan**, Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Veriler, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, cilt VIII, sayı:2, yıl:2013

**Artuk, Prof. Dr. Mehmet Emin/Gökçen, Prof. Dr. Ahmet /Yenidünya, Doç. Dr. Caner Türk** Ceza Kanunu Şerhi, Özel Hükümler, C. 5, Ankara 2009

**Dülger, Doç. Dr. Murat Volkan**, bilişim suçları ve internet iletişim hukuku, Ankara 2015, gül, G, ag

**Efe, Dr. Ahmet**, Bilişim Hukuku ile Uluslararası Hukuk Kesişiminde Yeni Bir Paradigma: Siber Yönetişim, Türkiye Noterler Birliği Hukuk Dergisi, Ankara, 2017, yıl:4 sayı:2

**Erdoğan, Yavuz**, Türk Ceza Kanununda bilişim sistemini engelleme bozma verileri yok etme değiştirme suçu, Doktora tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2011

**Gül, Ahmet**, Doğrudan Dolaylı Bilişim Suçları, Seçkin, Ankara, 2019

**Koca, Prof. Mahmut**, Hukukumuzda TCK.nun 244. maddesi kapsamında bilişim sistemini engelleme, bozma verileri yok etme ve değiştirme suçu, bilişim hukuk konferansı, 9-10 Ekim 2008, Yargıtay Yayınları

**Kurt, Levent**, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınevi, Ankara 2005

**Özgenç, Prof.Dr. İzzet**, Türk Ceza Kanunu Gazi Şerhi (Genel Hükümler), Seçkin Yayınevi 2005

**Taşdemir, Kubilay**, Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara 2009

Yargıtay Ceza Daireleri uygulamasında sıklıkla rastlanan bozma sebepleri, Yargıtay Cumhuriyet Başsavcılığı, Ankara 2018

**Yaşar, Osman/Gökçen, Hasan Tahsin/Artuç, Mustafa**, yorumlu uygulamalı Türk Ceza Kanunu, cilt V, Adalet Yayınları, Ankara 2010

**YAZICIOĞLU, Yrd. Doç. Dr. R. Yılmaz**, Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı, 21-22 Mayıs 2001, İzmir Uluslararası İnternet Hukuku Sempozyumunda sunulan tebliğ.