

T.C.  
İSTANBUL BEYKENT ÜNİVERSİTESİ  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

HUKUK ANABİLİM DALI  
KAMU HUKUKU BİLİM DALI

**ÇEVİRİMİÇİ OYUN HESABININ VE OYUN  
KARAKTERİNİN ELE GEÇİRİLMESİNİN BİLİŞİM  
SUÇLARI KAPSAMINDA DEĞERLENDİRİLMESİ**

Yüksek Lisans Tezi

Tezi Hazırlayan  
**Oğuz Alp YÜCE**

İstanbul, 2024

T.C.  
İSTANBUL BEYKENT ÜNİVERSİTESİ  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

HUKUK ANABİLİM DALI  
KAMU HUKUKU BİLİM DALI

**ÇEVİRİMİÇİ OYUN HESABININ VE OYUN  
KARAKTERİNİN ELE GEÇİRİLMESİNİN BİLİŞİM  
SUÇLARI KAPSAMINDA DEĞERLENDİRİLMESİ**

Yüksek Lisans Tezi

Tezi Hazırlayan  
**Oğuz Alp YÜCE**

Öğrenci No  
**2120036025**

ORCID ID  
**0000-0003-0361-0456**

Danışman  
**Dr. Öğr. Üyesi Aslıhan ÖZTEZEL**

İstanbul, 2024

## YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Çevrimiçi Oyun Hesabının ve Oyun Karakterinin Ele Geçirilmesinin Bilişim Suçları Kapsamında Değerlendirilmesi” başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını, patent ve telif haklarını ihlal edici bir davranışımın olmadığını belirtir ve bunu onurumla doğrularım. 07.06.2024

Oğuz Alp YÜCE

T.C.  
İSTANBUL BEYKENT ÜNİVERSİTESİ  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ  
TEZLİ YÜKSEK LİSANS SINAV TUTANAĞI

7.6.2024

Enstitümüz *Hukuk* Anabilim Dalı *Kamu Hukuku* Programı yüksek lisans öğrencilerinden **2120036025** numaralı **Oğuz Alp YÜCE**'nin "*İstanbul Beykent Üniversitesi Lisansüstü Eğitim – Öğretim Yönetmeliği*"nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği "*Çevrimiçi Oyun Hesabının ve Oyun Karakterinin Ele Geçirilmesinin Bilişim Suçları Kapsamında Değerlendirilmesi*" konulu tezini, Yönetim Kurulumuzun 21/05/2024 tarih ve 2024/23 sayılı toplantısında seçilen ve Taksim yerleşkesinde toplanan biz jüri üyeleri huzurunda, Beykent Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 29. maddesinin 3. fıkrası gereğince 45 dakika süre ile aday tarafından savunulmuş ve sonuçta adayın tezi hakkında "**OYBİRLİĞİ**" ile "**KABUL**" kararı verilmiştir.

İşbu tutanak, 2 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

**DANIŞMAN**

Dr. Öğr. Üyesi As\*\*\* ÖZ\*\*\*  
(İstanbul Beykent Üniversitesi)

**ÜYE**

Dr. Öğr. Üyesi Fa\*\*\* YU\*\*\*  
(İstanbul Beykent Üniversitesi)

**ÜYE**

Dr. Öğr. Üyesi Ha\*\*\* UL\*\*\*  
(Bahçeşehir Üniversitesi)

Adı ve Soyadı : Oğuz Alp YÜCE  
Danışmanı : Dr. Öğr. Üyesi Aslıhan ÖZTEZEL  
Derecesi ve Tarihi : Yüksek Lisans (Tezli), 2024  
Alanı : Kamu Hukuku  
Anahtar Kelimeler : Bilişim Suçları, Çevrimiçi Oyunlar, Oyun Karakteri  
Güvenliği, Dijital Varlık, Hesap Hırsızlığı

## ÖZ

### ÇEVİRİMİÇİ OYUN HESABININ VE OYUN KARAKTERİNİN ELE GEÇİRİLMESİNİN BİLİŞİM SUÇLARI KAPSAMINDA DEĞERLENDİRİLMESİ

Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, özellikle genç kullanıcıları hedef alarak onların mülkiyet ve özel hayat haklarını ihlal eden ciddi bir bilişim suçudur. Bu çalışma, bu tür suçların hukuki boyutlarını Türk Ceza Kanunu ve uluslararası hukuk normları çerçevesinde incelerken, mevcut yasal düzenlemelerin yetersiz kaldığı noktaları ortaya koymakta ve etkin mücadele için gerekli kanuni değişiklikleri önermektedir. Araştırma, dijital mülkiyet haklarının korunması, kişisel verilerin güvenliği ve bilişim suçlarına karşı cezai sorumluluğun artırılması gibi konuları ele alarak, bu suçların önlenmesi için hukuki düzenlemelerin nasıl güncellenmesi gerektiğini tartışmaktadır. Özellikle Türk Ceza Kanunu'nda yapılması önerilen değişiklikler, bu tür suç faaliyetlerinin önlenmesinde önemli bir adım olacaktır.

Çalışma aynı zamanda, bu önerilerin sadece teoride kalmayıp, gerçek hayatta etkin bir şekilde uygulanması gerektiğini vurgulamakta; böylece hem yasal boşlukların kapatılması hem de uluslararası iş birliği ile bu tür suçların önüne geçilmesinin mümkün olabileceğini belirtmektedir.

Name and Surname : Oğuz Alp YÜCE  
Supervisor : Asst. Prof. Dr. Aslıhan ÖZTEZEL  
Degree and Date : Master's (Thesis), 2024  
Major : Public Law  
Keywords : Cyber Crimes, Online Games, Game Character Security,  
Digital Asset, Account Theft

## **ABSTRACT**

### **EVALUATION OF THE SEIZURE OF ONLINE GAME ACCOUNTS AND GAME CHARACTERS WITHIN THE SCOPE OF CYBERCRIMES**

The seizure of online game accounts and characters is a grave cybercrime, particularly targeting young users, infringing on their property and privacy rights. This study examines the legal dimensions of such crimes within the framework of the Turkish Penal Code and international legal norms, highlighting the inadequacies of existing legal regulations and proposing necessary amendments for effective combat. The research addresses issues such as the protection of digital property rights, the security of personal data and the enhancement of criminal liability for cybercrimes, discussing how legal frameworks should be updated to prevent these crimes. Specifically, the amendments suggested in the Turkish Penal Code would be a significant step toward curbing such criminal activities.

The study also emphasizes that these proposals should not remain merely theoretical but be implemented effectively in real life, thereby closing legal gaps and potentially curtailing such crimes through international cooperation.

## İÇİNDEKİLER

Sayfa No.

**ÖZ**

**ABSTRACT**

**KISALTMALAR ..... iv**

**SÖZLÜK.....v**

**GİRİŞ .....1**

### **1. ADLİ BİLİŞİM VE BİLİŞİM SUÇLARI**

#### **1.1. Adli Bilişim Kavramının Tanımı ve Mukayeseli Hukukta Bilişim Suçları**

**Düzenlemeleri..... 3**

1.1.1. Bilişim Suçlarının Türleri ve Örnekleri ..... 7

1.1.1.1. Kimlik Hırsızlığı ve Dolandırıcılık ..... 8

1.1.1.2. Siber Saldırıları ve Bilgisayar Virüsleri ..... 10

1.1.1.3. Çevrimiçi Taciz ve Çevrimiçi Zorbalık.....11

1.1.1.4. Çevrimiçi Oyun Hesaplarının ve Karakterlerinin Ele Geçirilmesi ... 13

1.1.2. Uluslararası Hukukta Bilişim Suçları..... 14

1.1.3. Mukayeseli Hukukta Bilişim Suçları Yasal Düzenlemeleri ..... 15

1.1.4. Türkiye’de Bilişim Suçlarının Gelişimi ..... 17

#### **1.2. Adli Bilişim Uygulamaları ve Delil Toplama ..... 18**

1.2.1. Adli Bilişim Süreçleri ..... 19

1.2.1.1. İncelenmesi Gereken Dijital Sistemlerin ve Verinin Belirlenmesi ... 20

1.2.1.2. Dijital Veri ve Delillerin Toplanması ..... 21

1.2.2. Adli Bilişim Teknikleri..... 22

1.2.2.1. Dijital Delillerin Analiz Edilmesi ..... 23

1.2.2.2. Raporlama ..... 24

### **2. SİBER GÜVENLİK VE ÇEVİRİMİÇİ OYUNLAR**

#### **2.1. Tanımlar ve Kavramlar..... 27**

2.1.1. Siber Güvenlik Kavramı ..... 28

2.1.2. Çevrimiçi Oyun Endüstrisi..... 29

#### **2.2. Çevrimiçi Oyun Hesaplarının Değeri ve Mülkiyet Kavramı..... 31**

|                                                                               |           |
|-------------------------------------------------------------------------------|-----------|
| 2.2.1. Klasik Mülkiyet Hakkı Kavramından Farklılıkları .....                  | 39        |
| <b>2.3. Hesap Güvenliği Önlemleri ve Kullanıcı Sorumlulukları.....</b>        | <b>46</b> |
| 2.3.1. Güçlü ve Benzersiz Parolalar Kullanma .....                            | 47        |
| 2.3.2. İki Faktörlü Kimlik Doğrulama .....                                    | 48        |
| 2.3.3. Phishing Saldırılarına Karşı Dikkatli Olma .....                       | 48        |
| 2.3.4. Güvenlik Yazılımları Kullanma .....                                    | 49        |
| 2.3.5. Açık Ağlarda Oyuna Giriş Yapmaktan Kaçınma .....                       | 50        |
| 2.3.6. Oyun İçi İletişime Dikkat Edinme .....                                 | 51        |
| <b>3. ÇEVİRİMİÇİ OYUN HESAPLARININ VE KARAKTERLERİNİN ELE</b>                 |           |
| <b>GEÇİRİLMESİ: YÖNTEMLER VE MOTİVASYONLAR</b>                                |           |
| <b>3.1. Hesap Ele Geçirme Yöntemleri ve Teknikleri.....</b>                   | <b>54</b> |
| 3.1.1. Phishing (Oltalama) Yöntemi.....                                       | 55        |
| 3.1.2. Keylogging ( Keylogger ) Yöntemi .....                                 | 55        |
| 3.1.3. Çevrimiçi Oyunlarda Hesap Paylaşımı Yöntemi .....                      | 56        |
| 3.1.4. Güvenlik Açıkları Yöntemi .....                                        | 57        |
| 3.1.5. Çevrimiçi Oyunlarda Sosyal Mühendislik Yöntemi .....                   | 57        |
| 3.1.6. Brute Force (Kaba Kuvvet) Saldırıları Yöntemi .....                    | 58        |
| 3.1.7. Denial of Service (Hizmet Dışı Bırakma) Saldırıları Yöntemi .....      | 59        |
| 3.1.8. Çoklu Hesap Kullanımı (Multi-Accounting) Yöntemi .....                 | 60        |
| <b>3.2. Saldırganların Motivasyonları ve Hedefleri.....</b>                   | <b>61</b> |
| 3.2.1. Ekonomik Kazanç: Oyun İçi Varlıklar ve Para Aklama.....                | 63        |
| 3.2.2. Kişisel Verilerin İhlali ve Kimlik Hırsızlığı .....                    | 64        |
| 3.2.3. Rekabet Avantajı ve Oyun İçi Manipülasyon.....                         | 67        |
| <b>4. HUKUKİ BOYUT: SORUMLULUKLAR VE YAPTIRIMLAR</b>                          |           |
| <b>4.1. TCK Nezdinde “Çevrimiçi Oyun Hesabının ve Oyun Karakterinin Ele</b>   |           |
| <b>Geçirilmesinin Bilişim Suçları Kapsamında Değerlendirilmesi”</b>           |           |
| <b>Eylemlerinin Değerlendirilmesi.....</b>                                    | <b>69</b> |
| <b>4.2. “Çevrimiçi Oyun Karakteri Ele Geçirme” Eyleminin Türk Ceza</b>        |           |
| <b>Kanunu’ndaki Uygun Suç Tipleri Açısından Değerlendirilmesi.....</b>        | <b>70</b> |
| 4.2.1. Bilişim Sistemine Girme (TCK md.243) .....                             | 75        |
| 4.2.2. Madde 244: Bilişim Sistemini Engelleme, Bozma, Veri Gönderme, Verileri |           |
| Yok Etme veya Değiştirme .....                                                | 77        |

|                                                                                                                                                                       |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 4.2.3. Madde 245: Banka veya Kredi Kartlarının Kötüye Kullanılması.....                                                                                               | 78         |
| 4.2.4. Madde 245/A: Yasak Cihaz veya Programlar .....                                                                                                                 | 79         |
| 4.2.5. Madde 246: Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması .....                                                                                           | 81         |
| 4.2.6. Madde 142/2/e: Nitelikli Hırsızlık/Bilişim Sistemlerinin Kullanılması<br>Suretiyle.....                                                                        | 82         |
| 4.2.7. TCK Madde 158 Nitelikli Dolandırıcılık 1.Fıkrasının f Bendi Bilişim<br>Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması<br>Suretiyle..... | 85         |
| 4.2.8. TCK Madde 228/3: Kumar Oynanması İçin Yer ve İmkân Sağlama / Suçun<br>Bilişim Sistemleri Kullanılması Suretiyle İşlenmesi.....                                 | 88         |
| 4.3. Hukuki Yaptırımlar ve Cezai Müeyyideler .....                                                                                                                    | 89         |
| 4.4. Soruşturma ve Kovuşturma Aşamasında İspat Sorunu.....                                                                                                            | 92         |
| 4.4.1. Çevrimiçi ve Fiziki Suçlar Arasındaki İspat Mekanizmalarının<br>Karşılaştırılması.....                                                                         | 94         |
| 4.4.2. Çevrimiçi Oyun Platformlarından Toplanan Verilerin Rolü .....                                                                                                  | 95         |
| 4.4.3. Çevrimiçi Oyunlarda Veri Manipülasyonu ve Yok Edilmesi .....                                                                                                   | 96         |
| 4.4.4. Çözüm Önerileri.....                                                                                                                                           | 97         |
| 4.5. Delile Ulaşma Yöntemleri .....                                                                                                                                   | 100        |
| 4.6. Zarar Gören Taraflar ve Tazminat Hakkı.....                                                                                                                      | 102        |
| 4.7. Uluslararası İş Birliği ve Sınır Ötesi Suçlar .....                                                                                                              | 103        |
| <b>SONUÇ .....</b>                                                                                                                                                    | <b>106</b> |
| <b>KAYNAKÇA .....</b>                                                                                                                                                 | <b>113</b> |

## KISALTMALAR

|                 |                                                                                  |
|-----------------|----------------------------------------------------------------------------------|
| <b>AB</b>       | : Avrupa Birliđi                                                                 |
| <b>BM</b>       | : Birleşmiş Milletler                                                            |
| <b>BTK</b>      | : Bilgi Teknolojileri ve İletişim Kurumu                                         |
| <b>CART</b>     | : Computer Analysis and Response Team ( Bilgisayar Analizi ve Reaksiyon Takımı ) |
| <b>CERT</b>     | : Computer Emergency Response Team ( Bilgisayar Acil Durumu Müdahale Ekibi)      |
| <b>CMK</b>      | : Ceza Muhakemesi Kanunu                                                         |
| <b>DDoS</b>     | : Distributed Denial of Service ( Dağıtık Hizmet Reddi )                         |
| <b>Dos</b>      | : Denial of Service (Hizmet Reddi )                                              |
| <b>EGM</b>      | : Emniyet Genel Müdürlüğü                                                        |
| <b>EULA</b>     | : End User License Agreement ( Son Kullanıcı Lisans Sözleşmesi )                 |
| <b>EUROPOL</b>  | : Avrupa Birliđi Teşkilatı                                                       |
| <b>FBI</b>      | : Federal Bureau of Investigation ( Federal Soruşturma Bürosu )                  |
| <b>GDPR</b>     | : General Data Protection Regulation ( Genel Veri Koruma Tüzüğü )                |
| <b>INTERPOL</b> | : Uluslararası Kriminal Polis Teşkilatı                                          |
| <b>IP</b>       | : Internet Protocol ( İnternet Protokolü )                                       |
| <b>JNGK</b>     | : Jandarma Genel Komutanlığı                                                     |
| <b>KVKK</b>     | : Kişisel Verilerin Korunması Kanunu                                             |
| <b>TBK</b>      | : Türk Borçlar Kanunu                                                            |
| <b>TCK</b>      | : Türk Ceza Kanunu                                                               |
| <b>TÜBİTAK</b>  | : Türkiye Bilimsel ve Teknik Araştırma Kurumu                                    |
| <b>USA</b>      | : United States of America ( Amerika Birleşik Devletleri )                       |
| <b>VPN</b>      | : Virtual Private Network ( Sanal Özel Ağ )                                      |
| <b>Wi-Fi</b>    | : Wireless Fidelity ( Kablosuz İnternet )                                        |

## SÖZLÜK

**Banlanmak (Banned):** Yasaklanmak, yasaklanmış, kısıtlanmış.

**Bilişim:** İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi; enformatik.

**Çevrimiçi:** Bir bilgisayarın sunucuya ve bilgisayar ağına bağlı olarak çalışır olma durumu.

**Dijital Veri:** Sayısallaştırılmış veri.

**Mukayese:** Karşılaştırma.

**Siber Saldırı:** Bir veya birden fazla bilgisayardan başka bilgisayarlara veya ağlara veri çalmak, değiştirmek ya da yok etmek için çeşitli yöntemler kullanılarak yapılan saldırı eylemlerinin bütünü.

**Yapay Zeka:** Bir bilgisayarın, bilgisayar kontrolündeki bir robotun veya programlanabilir bir aygıtın insana benzer biçimde algılama, öğrenme, fikir yürütme, karar verme, sorun çözme, iletişim kurma vb. işlevleri sergileyebilme yeteneği.

## GİRİŞ

Bilişim teknolojilerinin hızla ilerlemesi modern toplumun yapısını ve işleyişini köklü bir şekilde dönüştürmüştür. İnternetin evrensel bir hale gelmesiyle dijital dünya günlük yaşamımızın ayrılmaz bir parçası olmuştur. Bu dönüşüm pek çok yenilik ve kolaylık getirse de yeni tür suçları da beraberinde getirmiştir. Özellikle çevrimiçi oyunlar ve sosyal medya platformları bilişim suçlarının odak noktası haline gelmiştir. Bu çalışma, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi gibi bilişim suçlarının hukuk çerçevesinde nasıl ele alınması gerektiğini detaylı bir şekilde incelemeyi amaçlamaktadır. Bilişim suçları, geleneksel suç kavramlarının ötesine geçerek siber güvenliğin önemini ve zorluklarını ortaya koymaktadır. Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi sadece maddi zararlara yol açmakla kalmayıp, aynı zamanda bireylerin özel yaşamına ve kişisel verilerine ciddi müdahalelerde bulunabilmektedir. Bu suçların benzersiz doğası hukukun sınırlarını zorlamakta ve mevcut yasal düzenlemelerin yetersiz kaldığı durumları ortaya çıkarmaktadır.

Türkiye'de bilişim suçlarına karşı mücadele Türk Ceza Kanunu'nda belirli başlıklar altında düzenlenmiştir. Ancak dijital mülkiyetin korunması ve çevrimiçi hesapların güvenliği gibi konularda mevcut yasal çerçeve yeterli değildir. Dijital dünyanın sürekli evrim geçirmesi yasal düzenlemelerin de bu değişimlere ayak uydurabilmesi için dinamik ve esnek olmasını gerektirir. Bu bağlamda, çevrimiçi oyun hesaplarının ele geçirilmesi gibi suçlar sadece bireysel mağdurları değil aynı zamanda geniş çapta toplumsal etkilere sahiptir. Bu nedenle bu suçların önlenmesi ve cezalandırılması sadece hukuki bir mesele olmanın ötesinde bir toplumsal sorumluluk haline gelmiştir.

Hukukun bu yeni siber tehditlere yanıt verebilmesi için adli bilişim uzmanları, hukukçular ve teknoloji uzmanlarının multidisipliner bir yaklaşımla iş birliği yapması gerekmektedir. Bu iş birliği suçların daha etkili bir şekilde tespit edilmesini, soruşturulmasını ve cezalandırılmasını sağlayacak teknik ve hukuki altyapının geliştirilmesine katkıda bulunacaktır. Ayrıca bu suçlara karşı farkındalığın artırılması ve çevrimiçi ortamlarda güvenliği sağlayacak eğitim programlarının hayata geçirilmesi önleyici tedbirlerin alınmasında kritik bir rol oynayacaktır.

Sonuç olarak dijitalleşen dünyada bilişim teknolojilerinin getirdiği faydaların yanı sıra karşılaştığımız riskler ve tehditler de artmaktadır. Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi gibi suçlar bireylerin ve toplumun güvenliğini tehdit etmekte, bu nedenle hukuki düzenlemelerin bu yeni suç türlerine uygun şekilde geliştirilmesi zorunluluğunu ortaya koymaktadır. Bu çalışma bilişim suçlarına karşı etkili bir mücadele stratejisi geliştirmek için gerekli olan hukuki, teknik ve toplumsal boyutları ele almayı hedeflemekte olup, bu alanda atılacak adımların temelini oluşturmayı amaçlamaktadır.



## 1. ADLİ BİLİŞİM VE BİLİŞİM SUÇLARI

Adli bilişim, dijital verilerin yasal süreçlerde kullanımını ifade eden bir disiplindir ve günümüzde bilişim suçlarıyla mücadelede kritik bir role sahiptir. Bu alanda uzmanlar suç delillerinin dijital ortamlardan adil ve güvenilir bir şekilde toplanmasını, korunmasını ve analiz edilmesini sağlarlar. Bilişim suçları internet üzerinden gerçekleştirilen dolandırıcılık, kimlik hırsızlığı, veri ihlali gibi faaliyetleri kapsar ve sürekli evrilmekte olan teknolojik gelişmelere bağlı olarak da sürekli yeni suç tipleri ortaya çıkmaktadır. Adli bilişim uzmanları bu suçları aydınlatmak ve failleri adalet önüne çıkarmak için dijital izleri takip ederken aynı zamanda siber güvenlik önlemlerinin geliştirilmesine de katkıda bulunurlar. Bu çerçevede detaylı tanımlamalar ve kapsamlı bir inceleme gerektiren adli bilişim ve bilişim suçları hukuku ilerleyen bölümlerde daha ayrıntılı bir şekilde ele alınacaktır.

### 1.1. Adli Bilişim Kavramının Tanımı ve Mukayeseli Hukukta Bilişim Suçları Düzenlemeleri

Teknolojinin hızla ilerlemesi ve internet kullanımının yaygınlaşmasıyla birlikte günlük yaşamımızda elektronik cihazların ve bilişim teknolojilerinin vazgeçilmez birer parçası haline gelmesi yeni bir suç kategorisi olan bilişim suçlarının ortaya çıkmasına zemin hazırlamıştır. 1990'lı yıllardan itibaren cep telefonlarının evrim geçirerek sadece iletişim aracı olmaktan çıkıp alışveriş yapma, video ve fotoğraf çekme gibi işlevler kazanması; WhatsApp, e-posta ve sosyal medya gibi platformların yaygın iletişim kanalları haline gelmesi bilişim suçlarının işlenme biçimlerini ve tanımlarını değiştirmiştir. Kredi kartı dolandırıcılığı, hakaret, taciz gibi suçların bilişim araçları üzerinden işlenmeye başlaması adli bilişim alanının doğuşuna ve gelişimine önyak olmuştur. Bu durum dijital özgürlük alanlarının bazen yıkıcı etkilere sahip olabileceği gerçeğini de önümüze sermektedir.<sup>1</sup>

Adli bilişim suçlarına karşı alınan önlemleri, bu suçların tespit edilmesini, delillerin toplanmasını ve bu delillerin adli mercilere sunulmasını kapsayan bir bilim dalıdır. Bilgisayar teknolojilerinin hukuki süreçlere dahil edilmesiyle ilgilenen bir

---

<sup>1</sup>Ö. M. Gökalp, *Bilgisayar Ağları ve Adli Bilişim*, Gazi Üniversitesi, Ankara, 2021, s. 10.

alandır. Bu terim genellikle "computer forensics" olarak adlandırılan bir disiplinin Türkçeye adaptasyonu sonucunda ortaya çıkmıştır. Ancak bu adaptasyon sırasında bilişim kavramının genişliği göz önünde bulundurularak sadece "bilgisayar" kelimesiyle sınırlı olmayan daha kapsayıcı bir anlamla "adli bilişim" şeklinde dilimize kazandırılmıştır. Bu alandaki çalışmalar dijital verinin adli analizini, delil toplama yöntemlerini ve bu verilerin hukuki süreçlerde nasıl kullanılacağını inceler. Adli bilişim uzmanları hukukçularla birlikte çalışarak, dijital delillerin doğru ve adil bir şekilde kullanılmasını sağlar.<sup>2</sup> Bu çağımızın dijitalleşen dünyasında giderek daha fazla önem taşımaktadır.

Adli bilişim uzmanları, siber suçlarla mücadelede kritik bir role sahiptir. Bu uzmanlar suçun işlendiği dijital ortamlardan delil toplama, bu delilleri koruma ve analiz etme konularında uzmandırlar. Siber güvenlik alanında çalışan adli bilişim uzmanları, dijital dünyada gerçekleşen suçları aydınlatma konusunda önemli bir göreve sahiptirler. Bu profesyoneller dijital ayak izlerini takip ederek siber suçluların izini sürerler ve adli süreçlerde kullanılmak üzere elektronik delilleri tespit ederler. Teknolojinin süratli ilerlemesiyle adli bilişim bilimi sadece yargısal mekanizmalar için değil aynı zamanda özel sektörde de vazgeçilmez bir öneme bürünmüştür. Özellikle büyük ölçekli işletmeler, veri güvenliği ve sızıntılarını önleme amacıyla adli bilişim uzmanlarına yatırım yapmaktadırlar. Adli bilişim faaliyetlerinin başarısında uzmanlığın yanı sıra, gelişmiş laboratuvar koşulları ve doğru araçların kullanılması da büyük bir rol oynamaktadır. Genelde bu tür incelemeler sahadaki güvenlik ekipleri tarafından başlatılır, ardından detaylı analizler için uzman laboratuvarlara yönlendirilir. Bu, dijital delillerin doğruluğunun ve bütünlüğünün korunmasını garantiler.<sup>3</sup>

Dijital ortamda gerçekleşen suçlar modern hukuk sistemlerinin karşısına yeni zorluklar getirmektedir. Siber suçlar olarak adlandırılan bu tür eylemler genellikle internet üzerinden işlenen veya internetin bir araç olarak kullanıldığı suçları kapsar.

---

<sup>2</sup>Y. Başlar, 'Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri', *TBB Dergisi*, cilt: 148, 2020, s. 49.

<sup>3</sup>Başlar, a.g.e., s. 54.

Örneğin, dijital verilere izinsiz erişim kişisel bilgilere sızma veya bunları başkalarıyla paylaşma bu kategoriye girmektedir.<sup>4</sup>

Türkiye'de siber suçlarla mücadele, 5237 sayılı Türk Ceza Kanunu'nun Onuncu Bölümünde sınıflandırılan bilişim alanındaki suçlar başlığı altında ve diğer ilgili mevzuatlarda yer alan özel hükümlerle düzenlenmiştir. Bu çerçevede Türk Ceza Kanunu'ndaki ilgili maddelerle birlikte bilişim suçlarına özgü düzenlemeleri kapsayıcı bir şekilde ele alarak, siber suçlarla etkin bir şekilde mücadele edilmesini amaçlamaktadır. Bu hukuki düzenlemeler, bilişim teknolojilerinin suistimali sonucu ortaya çıkan suç faaliyetlerine karşı koyacak şekilde tasarlanmıştır ve ülkemizde siber güvenliğin sağlanması için kritik bir öneme sahiptir. Yasal çerçeveler arasındaki çeşitlilik, siber suçların tanım ve sınıflandırılmasında karışıklıklara yol açarken, bu durum hukuki müdahalelerin etkinliğini de olumsuz etkilemektedir. Net terminoloji ve uluslararası standartlara uyum, caydırıcılığı artırıp daha geniş kapsamlı bir yaklaşım sunarak, siber suçlarla mücadelede kritik bir önem taşımaktadır. Özellikle diğer bazı eylemlerin sınıflandırılması konusundaki farklı yaklaşımlar, ulusal hukuk literatüründe bazen yanıltıcı olabilmektedir. Örneğin, bir eylemin sadece bilişim teknolojileri kullanılarak işlenmesi, onu otomatik olarak bir siber suç haline getirmez.<sup>5</sup> TCK madde 158'de belirtilen dolandırıcılık suçunun nitelikli hali olarak TCK madde 158/1/f'de tanımlanmıştır. Cep telefonu aracılığı ile kendisini polis, asker, hâkim veya savcı olarak tanıtarak karşı tarafı dolandıran bir kişi bilişim sistemlerini kullanarak dolandırıcılık suçunu işlemiş olarak sayılmamalıdır. Bu olay tamamen insanlık tarihinden itibaren süre gelen geleneksel bir suç tipi olan dolandırıcılık suçudur. Bazı suçlar geleneksel bir suç olup sadece dijital bir ortamda işleniyor olabilir. Bu nedenle bir eylemin siber bir suç olup olmadığını belirlerken, sadece kullanılan araçlara değil aynı zamanda suçun doğasına ve sonuçlarına da bakılması gerekmektedir. Örnek olarak çevrimiçi oyunlar içerisinde meydana gelebilecek bir dolandırıcılık olayı TCK madde 158/1/f kapsamında dolaylı bir şekilde bilişim suçu olarak değerlendirilebilmelidir.

---

<sup>4</sup>H. Akarslan, 'Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Kavramı', Yüksek Lisans Tezi, *Polis Akademisi*, Ankara, 2011.

<sup>5</sup>Akarslan, a.g.e., s. 127.

Adli biliřim, dijital çağın getirdiđi suç tipleriyle başa çıkmak, delil toplamak ve bu delillerin hukuki bir değeri taşımasını sağlamak amacıyla oluşturulmuş multidisipliner bir alandır. Kriminal incelemelerde kullanılan yöntemler ve adli bilimlerin nasıl bir evrim geçirdiđi, uzun yıllardır merak konusu olmuştur. Bu evrim sürecinde, antropoloji<sup>6</sup>, ontoloji<sup>7</sup> ve psikoloji<sup>8</sup> gibi birçok bilim dalından yararlanılmış; bu bilim dalları ile adli soruşturmalarının daha etkin ve doğru bir şekilde yapılabilmesi için birlikte çalışılmıştır. Ancak, dijitalleşen dünyada, suçların da dijital bir boyut kazanmasıyla birlikte, adli biliřim bu anlamda tüm bu bilim dallarının farklı bir hizmet vermek amacıyla sınırlarını genişletmiş ve değıştirmiştir.

Adli biliřim, hukukun dijital çağdaki yansımasıdır ve bilgisayar mühendisliđi ile hukukun birleşiminden doğmuştur. Computer Emergency Response Team - Bilgisayar Acil Durumu Müdahale Ekibi (CERT/CC) göre adli biliřim; bilgisayar sistemlerinden, ağlardan ve depolama ünitelerinden adli makamlarca kabul edilebilecek şekilde delil toplama ve veri analiz etme işlemidir.<sup>9</sup> Günümüzde suçların ve delillerin dijital bir yapıya bürünmesi, bu alanda uzmanlaşmış hukuk profesyonellerine olan ihtiyacı artırmıştır. Ancak bu süreç, sadece teknik bir analizle sınırlı değildir. Dijital delillerin hukuki bir değeri taşıyabilmesi için, hukuki normlara ve usullere uygun bir şekilde toplanması, saklanması ve sunulması gerekmektedir.

Adli biliřimin tarihçesine göz attığımızda, ilk çalışmaların 1970'lerin sonlarına doğru başladığını ve bilgisayarların hayatımıza girmesiyle birlikte biliřim suçlarının arttığını görmekteyiz; bu artış, hem ceza kanunlarında var olduđu haliyle suçların işleme sıklığının yükselmesine, hem de yeni suç işleme tekniklerinin, modus operandilerinin<sup>10</sup> ortaya çıkmasına yol açmıştır, böylece adli biliřim alanının gelişimini ve önemini sürekli artmasını zorunlu kılmaktadır. Dünya genelinde bu alandaki çalışmalar, 1984 yılında Amerika Birleşik Devletleri (United States of

---

<sup>6</sup><https://ansiklopedi.tubitak.gov.tr/ansiklopedi/antropoloji>, 'Antropoloji', E.T: 25 Mart 2024.

<sup>7</sup><https://ansiklopedi.tubitak.gov.tr/ansiklopedi/ontolojivarlikbilim>, 'Varlığı ve var olanları nelik ve nasıllıkları bakımından inceleyen felsefe dalıdır. Felsefenin ana disiplinlerinden biri olan metafiziğin alt dalıdır.', E.T: 25.03.2024

<sup>8</sup><https://ansiklopedi.tubitak.gov.tr/ansiklopedi/psikoloji>, 'Psikoloji, düşünme, hatırlama, öğrenme, problem çözme, muhakeme gibi zihinsel süreçler ile davranışları bilimsel olarak inceleyen bir bilim dalıdır.', E.T: 25.03.2024

<sup>9</sup>C. C. Wood, 'Computer Security Alert', *CSI Members-Only Web / Audio Conference on Incident Response*, Temmuz 2009.

<sup>10</sup>Delogu, Suç Genel Teorisinde 'Alet', (Çev. D. Soyaslan), *Rivista Italiana di Diritto e Procedura Penale*, Nuova Serie, Ankara, 1989, s. 251-282.

America - USA) ve Federal Soruşturma Bürosu (Federal Bureau of Investigation – FBI) öncülüğünde dijital delilleri inceleme amaçlı bilgisayar programlarının geliştirilmesiyle başlamıştır ve bu ihtiyaç FBI tarafından Bilgisayar Analizi ve Reaksiyon Takımı (Computer Analysis and Response Team - CART) adı altında bir birimin kurulmasını sağlamıştır.<sup>11</sup>

Ülkemizde ise bilişim suçlarıyla mücadelede ve adli bilişim incelemelerinde Emniyet Genel Müdürlüğü<sup>12</sup>, Jandarma Genel Komutanlığı<sup>13</sup>, Telekomünikasyon Kurumu<sup>14</sup>, TÜBİTAK<sup>15</sup> gibi kurumlar öne çıkmaktadır. Ancak bu kurumlar arasındaki dağıtık yapı, koordinasyon ihtiyacını da beraberinde getirmiştir. Özellikle ulusal düzeyde meydana gelebilecek siber saldırılara karşı koordinasyonun ve standart bir adli bilişim soruşturma modelinin oluşturulması, ülkemizin siber güvenlik açısından daha korunaklı hale gelmesini sağlayacaktır. Teknolojinin hızla ilerlemesi ve dijitalleşen dünyada suçların da evrim geçirmesi, adli bilişim uzmanlığının önemini artırmaktadır. Bu alandaki uzmanların hem teknik hem de hukuki bilgiye sahip olması ve sürekli olarak kendilerini güncellemesi gerekmektedir. Adli bilişim hukuku, dijital çağın hukuki sorunlarına çözüm üretmek için var olan bir alandır ve bu alandaki çalışmaların önemi, gün geçtikçe artmaktadır. Bu multidisipliner yaklaşım, suçların daha etkin bir şekilde çözülmesine ve hukuki süreçlerin daha sağlam temellere oturtulmasına olanak sağlamaktadır.

### 1.1.1. Bilişim Suçlarının Türleri ve Örnekleri

Bilişim teknolojilerinin hızla gelişimi ve internetin hayatımızın her alanına nüfuz etmesiyle birlikte, bilişim suçları da bu evrimin bir parçası olarak farklılaşmış ve derinleşmiştir. Bu suçlar, günümüzde adli bilişim uzmanlarına ve hukukçulara daha önce karşılaşmadıkları yeni ve karmaşık zorluklara maruz bırakmıştır. Modern bilişim

---

<sup>11</sup>H. Yeşilyurt, 'Adli Bilişim Soruşturma Metotlarının Standartlaştırılması ve Etkinlik-Verimlilik Perspektifinde Değerlendirilmesi', *Adli Bilimler Dergisi*, cilt: 13, sayı: 3, Eylül 2024, s. 3.

<sup>12</sup><https://www.egm.gov.tr/siber>, 'Siber Suçlarla Mücadele', Emniyet Genel Müdürlüğü, E.T: 13.09.2023.

<sup>13</sup><https://www.jandarma.gov.tr/asayis/siber-sucmucdbskligi>, 'Siber Suçlarla Mücadele', Jandarma Genel Komutanlığı, E.T: 13.09.2023.

<sup>14</sup><https://www.btk.gov.tr/siber-guvenlik-kurulu>, 'Siber Güvenlik Kurulu', Bilgi Teknolojileri ve İletişim Kurumu, E.T: 13.09.2023.

<sup>15</sup><https://bilgem.tubitak.gov.tr/sge/>, 'Siber Güvenlik Eğitimleri', TÜBİTAK BİLGEM, E.T: 13.09.2023.

suçlarının spektrumu geniş olup, kimlik hırsızlığından dolandırıcılığa, siber saldırılardan bilgisayar virüslerinin yayılmasına ve çevrimiçi taciz vakalarına kadar uzanmaktadır. Her bir suç tipi hem bireylerin hem de kurumların güvenliğini tehdit ederken, adli süreçlerin de giderek daha fazla uzmanlık ve teknolojik beceri gerektirmesine neden olmaktadır.<sup>16</sup>

Özellikle dikkat çeken bir sorun, çevrimiçi oyun hesaplarının ve karakterlerinin yetkisiz kişiler tarafından ele geçirilmesidir. Bu, dijital dünyada ciddi bir sorun haline gelmiş olup, kullanıcıların yalnızca sosyal etkileşimlerde bulunmalarını sağlamakla kalmayıp, aynı zamanda değerli sanal öğeleri de bilişim suçlarının hedefi haline getirmektedir. Bu sanal öğeler, oyun içi para birimlerinden nadir bulunan eşyalara kadar değişebilir ve gerçek dünya para birimi karşılığı ile önemli değerlere sahip olabilir. Bu tür suçlar sadece oyun topluluklarını değil aynı zamanda geniş anlamda toplumu, sosyal hayatı, dolayısıyla kamu güvenliğini etkilemektedir. Bilişim suçlarıyla mücadele, sadece teknik güvenlik önlemlerinin ötesine geçerek hukuki düzenlemelerin ve uluslararası iş birliğinin güçlendirilmesini gerektirmektedir. Adli bilişim uzmanları, sürekli olarak yeni suç yöntemleri ve teknolojik gelişmelere uyum sağlayabilmek için eğitimlerini ve araçlarını güncel tutmak zorundadır. Hukukçular ise, bu suçları tanımlayan ve cezalandıran yasaların, teknolojinin hızlı değişimine ayak uydurabilmesi için sürekli olarak revize edilmesi gerektiğinin farkındadırlar. Bu, bilişim suçlarıyla mücadelede çok disiplinli bir yaklaşımın benimsenmesini zorunlu kılar; bu yaklaşım, hukuk, teknoloji ve sosyal bilimlerin kesişiminde yer alır ve suçların önlenmesi, tespiti ve soruşturulması süreçlerinde kritik bir role sahiptir. Çalışmamızda şu ana kadar yaygın olarak işlenen bilişim suçlarının türleri inceleme altına alınacak ve Çevrimiçi Oyun Hesaplarının ve Karakterlerinin Ele Geçirilmesi konusuna özel önem verilecektir.

#### **1.1.1.1. Kimlik Hırsızlığı ve Dolandırıcılık**

21.yüzyılın başlangıcından itibaren, teknolojinin hızla ilerlemesi ve Internet'in hayatımızın merkezine oturması, pek çok faydayı beraberinde getirmiştir. Ancak bu

---

<sup>16</sup>Bilgi Teknolojileri ve İletişim Kurumu, 'Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri', *Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı*, Ankara, 2022, s. 18.

gelişmeler, kimlik hırsızlığı gibi ciddi sorunları da gün yüzüne çıkarmıştır. Online alışveriş, bankacılık işlemleri, sosyal medya platformları ve çevrimiçi oyunlar gibi dijital ortamların yaygınlaşması, kimlik hırsızlarının işini kolaylaştırmıştır. İnternetin yaygınlaşması, bireylerin kişisel ve finansal bilgilerinin korunmasını daha da zorlaştırmıştır. Kimlik hırsızlığı, bireylerin kişisel bilgilerinin izinsiz ve yasa dışı yollarla ele geçirilerek yasadışı amaçlarla kullanılması suçudur. Bu eylem, hem özel yaşamlara ciddi müdahaleler yapmakta hem de finansal zararlara neden olabilmektedir. Bu geniş tanım, suçun doğasını ve bireyler üzerindeki olası etkilerini kapsamlı bir şekilde açıklar.<sup>17</sup> Bu tanımlama, suçun uluslararası boyutunu ve çeşitliliğini gözler önüne sermektedir. Özellikle teknolojik gelişmeler, kimlik hırsızlığı ve dolandırıcılığının iç içe geçmesine ve bu suçların daha kolay işlenmesine olanak tanımıştır.

Çevrimiçi oyunlar özelinde, oyuncuların kişisel ve finansal bilgilerini içeren hesapları, kötü niyetli kişiler için cazip hedefler haline gelmiştir. Oyuncular, oyun içi satın alımlar yaparken kredi kartı bilgilerini paylaşmak zorunda kaldıklarında, bu bilgilerin kimlik hırsızları tarafından ele geçirilme riski artmaktadır.<sup>18</sup> Bu durum, özellikle genç ve tecrübesiz kullanıcılar için büyük bir risk teşkil etmektedir. Avrupa Birliği (AB) hukuku, kişisel verilerin korunması konusunda öncü bir rol üstlenmiştir. Avrupa Birliği Genel Veri Koruma Tüzüğü<sup>19</sup>, kişisel verilerin gizliliğinin ihlalinin kimlik hırsızlığına yol açabileceği konusunda açık uyarılarda bulunmaktadır. Bu tüzük, kişisel verilerin korunması konusunda AB üyesi ülkeler için bir rehber niteliğinde olup, bireylerin veri güvenliğini sağlamaya yönelik önemli bir adımdır.

Sonuç olarak, 21. yüzyılın getirdiği teknolojik olanaklar, kimlik hırsızlığının daha karmaşık bir hal almasına neden olmuştur. Çevrimiçi platformlar, bu suçun işlenmesi için yeni fırsatlar sunarken, ulusal ve uluslararası düzeyde alınacak önlemler, teknolojik gelişmelerin getirdiği riskleri minimize edebilir. Bireylerin de kendi kişisel ve finansal bilgilerini korumak için daha bilinçli olmaları gerekmektedir. Avrupa

---

<sup>17</sup>T. Bayzıt, ‘Kimlik Hırsızlığının Türk Ceza Hukuku ve Karşılaştırmalı Hukuk Bakımından Değerlendirilmesi’, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, cilt: XIX, sayı: 2, 2022, s. 637.

<sup>18</sup>[https://www.ab.gov.tr/ab-hukuku-ve-ceviri-daire-baskanligi\\_51631.html](https://www.ab.gov.tr/ab-hukuku-ve-ceviri-daire-baskanligi_51631.html), ‘AB Hukuku ve Çeviri Daire Başkanlığı’, Türkiye Cumhuriyeti Avrupa Birliği Başkanlığı, E.T: 15.10.2023.

<sup>19</sup>Avrupa Birliği, ‘Avrupa Birliği Genel Veri Koruma Tüzüğü’, *Resmî Gazete*, Ankara, 25 Mayıs 2018.

Birliđi'nin Veri Koruma Tüzüğü gibi mevzuatlar, bu süreçte önemli bir destek sağlamakta ve bireylerin haklarını güçlendirmektedir.

#### **1.1.1.2. Siber Saldırılar ve Bilgisayar Virüsleri**

Siber güvenlik ekosisteminde, saldırganların geniş ve karmaşık bir yelpazeyi kapsayan yöntemleri arasında bilgi ve veri aldatmacası, süper darbe, truva atı, zararlı yazılımlar, mantık bombaları, oltalama, bukalemun taktikleri, spam saldırıları, çöpe dalma, kimlik avı, sistem güvenliğinin ihlali, hukuka aykırı içerik dağıtımı, web sayfası hırsızlığı ve yönlendirme, sosyal mühendislik gibi teknikler bulunur. Bu tekniklerle, saldırganlar kurumların ve bireylerin bilgi güvenliğini ciddi şekilde tehdit eder. Çalışmanın odaklandığı çevrimiçi oyun hesabının ve oyun karakterinin ele geçirilmesi konusu, bu tekniklerin oyun hesapları ve karakterler üzerindeki etkisini örnekleyen bir durum olarak ele alınabilir. Oyun hesapları ve karakterler, kullanıcıların kişisel bilgilerini, oyun içi değerli eşyaları ve sanal para birimlerini barındırdığı için, özellikle oltalama, truva atı, zararlı yazılımlar ve sosyal mühendislik gibi yöntemlerle saldırganların hedefi haline gelmektedir. Bu saldırılar, kullanıcıların sadece oyun içi varlıklarını değil, kişisel ve finansal bilgilerini de tehlikeye atarak, siber güvenlik stratejilerinin önemli bir parçasını oluşturur ve bilişim suçları kapsamında ciddi bir tehdit olarak değerlendirilmelidir.<sup>20</sup>

Yukarıda belirtilen yöntemlerin yanında Ransomware saldırıları, son yıllarda özellikle kurumlar için büyük bir tehdit haline gelmiştir. Bu tür saldırılarda saldırganlar, hedeflenen kurumun bilgisayar sistemlerine veya ağlarına sızarak verileri şifreler ve bu verilere erişimin yeniden sağlanabilmesi için fidye talep eder. Bu durum hem mali kayıplara hem de kurumların itibarının zarar görmesine neden olabilir. Distributed Denial of Service (Dağıtık Hizmet Reddi – DDoS) saldırıları ise, hedeflenen web sitelerini veya çevrimiçi hizmetleri aşırı miktarda sahte trafik ile bombardımana tutarak erişilemez hale getirir. Bu tür saldırılar, özellikle e-ticaret

---

<sup>20</sup>F. Aslay, 'Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi', *International Journal of Multidisciplinary Studies and Innovative Technologies*, cilt: 1, sayı: 1, 2017, s. 25.

siteleri ve çevrimiçi hizmetler için ciddi bir tehdit oluşturmakta, kullanıcı deneyimini olumsuz etkileyerek iş kaybına yol açabilmektedir.<sup>21</sup>

Truva atları, zararlı kodları masum görünen yazılımların içerisine gizleyerek kullanıcıların bu yazılımları indirmesini ve çalıştırmasını sağlayan bir yöntemdir. Bu sayede, saldırganlar kullanıcıların bilgisayarlarına veya ağlarına sızabilir ve çeşitli zararlı faaliyetlerde bulunabilir. Zararlı yazılımlar ve mantık bombaları da benzer şekilde, belirli koşullar altında aktive olmak üzere tasarlanmış kod parçacıklarıdır. Bu kodlar, sistemde ciddi hasara veya veri kaybına neden olabilir.<sup>22</sup>

Oltaama (phishing) saldırıları, sahte e-postalar, mesajlar veya web siteleri aracılığıyla kullanıcıların kişisel bilgilerini, özellikle de kimlik bilgileri ve finansal bilgileri ele geçirmeyi amaçlar.<sup>23</sup> Sosyal mühendislik, insan psikolojisinden faydalanarak güvenilir bir kaynakmış gibi davranıp kullanıcıları kandırma ve onlardan hassas bilgileri elde etme yöntemidir.<sup>24</sup>

Bu çeşitlilik ve karmaşıklık, siber güvenlik stratejilerinin sürekli olarak güncellenmesini ve saldırılara karşı proaktif önlemlerin alınmasını zorunlu kılmaktadır. Kurumlar, siber tehdit istihbaratı, güvenlik farkındalık eğitimleri, düzenli güvenlik denetimleri ve etkili olay müdahale planları gibi çok yönlü savunma stratejileri geliştirerek bu tehditlere karşı koymalıdır. Bu bağlamda, siber güvenlik, yalnızca teknolojik önlemlerle sınırlı kalmayıp, aynı zamanda eğitim ve organizasyonel politikaların bir bütünü olarak ele alınmalıdır. Bu kapsamlı yaklaşım, siber saldırıların neden olabileceği zararları en aza indirmek için kritik öneme sahiptir.

### 1.1.1.3. Çevrimiçi Taciz ve Çevrimiçi Zorbalık

Bireylerin internet ve sosyal medya aracılığıyla birbirleriyle iletişim kurması sıradanlaşmıştır. Ancak bu durum, bazı bireylerin kötü niyetli eylemlerde bulunmasına

---

<sup>21</sup>Aslay, a.g.e., s. 26.

<sup>22</sup>G. Canbek ve Ş. Sağiroğlu, 'Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma', *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi*, cilt 22, sayı 1, 2007, s. 125.

<sup>23</sup>Y. Arslan, 'Oltaama Saldırıları Farkındalık Tatbikatı Örneği', *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, cilt: 9, sayı: 3, 2021, s. s. 348-358.

<sup>24</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

da zemin hazırlamaktadır. Çevrimiçi taciz, bireyin hakaret, tehdit ya da aşağılama içerikli mesajları sürekli ve ısrarla mağdura göndermesi eylemidir. Bu tür saldırılar, genellikle mağdurun kişisel, psikolojik ya da sosyal zarar görmesi amacıyla gerçekleştirilir.<sup>25</sup> Bu tür saldırıların en belirgin özelliği, mesajların hakaret ve saldırı amaçlı olmasıdır. Mağdura yöneltilen bu mesajlar, kişisel iletişim araçları, sosyal medya platformları ve elektronik posta gibi dijital ortamlar aracılığıyla ulaştırılır. Çevrimiçi tacizin, karşılıklı bir tartışma veya iletişimden ziyade tek taraflı bir saldırı şeklinde gerçekleştiği de önemli bir husustur. Yani saldırgan, mağdura sürekli ve ısrarla hakaret içeren mesajlar gönderirken, mağdur bu mesajları engellemeye veya bu tür saldırılardan korunmaya çalışır.

Çevrim içi zorbalık, dijital ortamlarda gerçekleşen kötü niyetli eylemler bütünü olarak tanımlanabilir. Teknolojik ilerlemelerle birlikte bu tür zorbalıklar, sadece sosyal medya veya mesajlaşma platformlarında değil, çevrimiçi oyunlarda da sıkça rastlanan bir sorun haline gelmiştir. Özellikle çok oyunculu online oyunlar, rekabetçi bir atmosferin doğmasına sebep olabilmekte ve bu durum, oyuncuların rakiplerini psikolojik olarak etkilemek, kızdırmak ya da oyundan soğutmak amacıyla aşağılayıcı yorumlar yapmalarına ya da kişisel bilgilerini ifşa etmelerine yol açabilmektedir.<sup>26</sup>

Çevrim içi zorbalığın en belirgin özellikleri, hedef alınan kişiye karşı tekrar eden ve kasıtlı zarar verme eylemlerinin gerçekleştirilmesi, sosyal medya platformlarında kişisel bilgilerin ya da utandırıcı görsellerin paylaşılması, mesajlaşma platformları ya da oyun içi sohbetler aracılığıyla tehditkâr ve hakaret içeren mesajların gönderilmesi ve sahte hesaplar oluşturarak bir kişinin kimliğini taklit edip, o kişi adına başkalarına zarar verme eylemlerinde bulunulmasıdır. Geleneksel yüz yüze zorbalığın aksine, çevrim içi zorbalık fiziksel bir etkileşimi gerektirmez. Ancak, bu iki zorbalık türü sıklıkla bir arada yaşanabilir. Özellikle okul çağındaki gençlerde, yüz yüze yaşanan zorbalıkların çevrim içi platformlara taşınması yaygın bir durumdur. Ancak çevrim içi zorbalığın bir avantajı, geride dijital izler bırakmasıdır; bu da zorbalığın kaynağını belirlemek ve durdurmak için yararlı olabilmektedir.

---

<sup>25</sup>S. Karakuş ve S.G. Turan, ‘Yetişkinlerin Siber Zorbalık Davranımları ile Dijital Vatandaşlık Becerileri Arasındaki İlişkinin İncelenmesi’, *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, sayı: 49, 2021, s. 410.

<sup>26</sup>S. Livingstone ve A. Third, ‘Çevrim İçi Zorbalık: Nedir ve Nasıl Önlenir ?’ *UNICEF*, Ankara, 2020, s. 5.

#### 1.1.1.4. Çevrimiçi Oyun Hesaplarının ve Karakterlerinin Ele Geçirilmesi

Çevrimiçi oyunlar modern dünyanın vazgeçilmez eğlencelerinden biri haline gelmiştir. Teknolojinin sunduğu olanaklar sayesinde, oyun severler dünyanın dört bir yanındaki diğer oyuncularla etkileşimde bulunarak, bu sanal ortamda eğlenceli vakitler geçirmektedirler. Ancak bu eğlenceli ortam, aynı zamanda çeşitli riskleri de beraberinde getirir. Özellikle yüksek grafik kapasiteli oyunlar için yatırım yapan oyuncular hem zamanlarını hem de finansal kaynaklarını bu sanal dünyalara adarlar.<sup>27</sup> Bu durum, siber güvenlik açısından bazı tehlikeleri de ortaya çıkarır. Oyun platformları, özellikle oyun içi alışverişler ve oyuncuların kişisel bilgilerini barındıran hesapları nedeniyle, siber suçlular için çekici bir hedef haline gelmiştir. Bunun yanı sıra, oyunlarda yer alan bazı güvenlik açıklıkları, saldırganların bu platformları kendi amaçları<sup>28</sup> doğrultusunda kullanmalarına olanak sağlar.<sup>29</sup>

Çevrimiçi oyun dünyası, oyuncuların sanal karakterler ve hesaplar üzerinde önemli zaman ve mali kaynaklar yatırımı yapmasına olanak tanıyan bir ortam sunarken, bu ortam aynı zamanda siber suçlular için cazip bir hedef haline gelmiştir. Tehlikeler arasında, oyuncu hesaplarının ve karakterlerinin yetkisiz kişiler tarafından ele geçirilmesi başta gelmektedir. Bu durum, oyuncuların sadece sanal varlıklarını kaybetmelerine neden olmakla kalmaz, aynı zamanda kişisel ve finansal bilgilerinin ifşa olmasına, dolandırıcılık ve kimlik hırsızlığı gibi daha geniş çaplı güvenlik ihlallerine kapı açabilir. Oyun içi alışveriş sistemleri ve kişisel bilgilerin saklandığı veri tabanları, zayıf güvenlik önlemleri nedeniyle sıkça saldırıya uğramakta, bu da oyuncuların maruz kaldığı riskleri artırmaktadır. Ek olarak, oyuncuların farkında olmadan kötü amaçlı yazılımlar indirmesi veya phishing<sup>30</sup> (oltalama) saldırılarına kurban gitmesi, hesaplarının kolaylıkla ele geçirilmesine yol açabilir. Bu riskler, oyuncuların ve oyun platformlarının sürekli teyakkuz halinde olmasını gerektirir, zira siber suçluların yöntemleri sürekli evrim geçirmekte ve daha sofistike hale gelmektedir. Dolayısıyla, çevrimiçi oyun ortamlarının keyfini güvenli bir şekilde

<sup>27</sup>Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı, 'Çevrimiçi Oyunlara İlişkin Güvenlik Riskleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Kasım 2014, s. 3.

<sup>28</sup>Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı, 'Çevrimiçi Oyunlara İlişkin Güvenlik Riskleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Kasım 2014, s. 7.

<sup>29</sup>Sayfa 63'te alt başlıkta daha detaylı anlatılacaktır.

<sup>30</sup>Arslan, a.g.e., s. 348-358.

çıkarabilmek için, oyuncuların güçlü parolalar kullanması, iki faktörlü kimlik doğrulama gibi ek güvenlik önlemlerini aktif etmesi ve düzenli olarak hesap güvenlik ayarlarını gözden geçirmesi büyük önem taşımaktadır.

Bu nedenle, çevrimiçi oyunlarla ilgilenen bireylerin, oyunun getirdiği eğlenceye dalarken aynı zamanda teknolojik ve sosyal risklere karşı da bilinçlenmeleri gerekmektedir. Oyun hesaplarının güvenliğinden, kişisel bilgilerin korunmasına kadar birçok alanda dikkatli ve bilinçli adımlar atılması, bu sanal dünyaların güven içinde keşfedilmesini sağlar. Hukuk dünyası da bu tür siber tehditlere karşı bireyleri korumak ve suçluları adalet önüne çıkarmak için sürekli evrilmekte ve yeni düzenlemeler yapmalıdır.

### 1.1.2. Uluslararası Hukukta Bilişim Suçları

Uluslararası düzeyde ise Birleşmiş Milletler<sup>31</sup>, Avrupa Konseyi<sup>32</sup> gibi önemli kuruluşlar, bilişim suçlarına karşı iş birliğini teşvik etmek ve bu suçların etkilerini azaltmak için çeşitli sözleşmeler ve anlaşmalar imzalamıştır ve bu sözleşmelerin başında gelen Avrupa Konseyi'nin "Bilişim Suçları Sözleşmesi" (Convention on Cybercrime) uluslararası düzeyde bilişim suçlarına yönelik yasal düzenlemelerin standartlaştırılmasına yardımcı olmuştur.<sup>33</sup> Bu sözleşme, bilişim suçlarına karşı uluslararası iş birliğini teşvik etmeyi amaçlar ve üye ülkelerin bu suçlara karşı nasıl hareket edeceğini belirtir.<sup>34</sup> Bunun yanı sıra, Birleşmiş Milletler Bilişim Suçlarına Karşı Eylem Planı<sup>35</sup>, G8 Ülkeleri Bilişim Suçlarına Karşı Eylem Planı<sup>36</sup> ve Avrupa Birliği Bilişim Suçları Direktifi<sup>37</sup> gibi uluslararası düzenlemeler de bilişim suçlarına karşı uluslararası iş birliğini ve bilgi paylaşımını teşvik eder.

<sup>31</sup><https://turkiye.un.org/tr>, 'Birleşmiş Milletler Türkiye', E.T.: 26.10.2023.

<sup>32</sup><https://diabgm.adalet.gov.tr/Home/SayfaDetay/avrupa-konseyine-genel-bir-bakis27022020030011>, 'Avrupa Konseyine Genel Bir Bakış', Adalet Bakanlığı, E.T.: 26.10.2023.

<sup>33</sup>M. Önok, 'Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği', *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, cilt 19, sayı 2, 2013, s.1239.

<sup>34</sup>Önok, a.g.e., s. 1234-1235.

<sup>35</sup>A. Aldoeri, 'Uluslararası Hukukta Siber Suçla Mücadele', Yüksek Lisans Tezi, *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2020.

<sup>36</sup>F. B. Nacar, 'Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları', Yüksek Lisans Tezi, *Atılım Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2010.

<sup>37</sup>B. Ergün, 'Türkiye ile Avrupa Birliği Arasında Hizmet Ticaretinin Karşılıklı Olarak Serbestleştirilmesi', Doktora Tezi, *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2009.

Ancak, dijital teknolojilerin hızla deęiřtięi ve evrildięi bu çağda, hukukçulara ve politika yapıcılara sürekli zorluklar sunmaktadır. Biliřim suçlarının önüne geçmek için yasaların ve düzenlemelerin sürekli güncellenmesi ve adapte edilmesi gerekmektedir. Özellikle çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi gibi spesifik suç türleri için uluslararası düzeyde net bir düzenleme bulunmamaktadır. Bu, uluslararası düzeyde de bu tür suçların tanımlanması ve cezalandırılması konusunda bir boşluk olduğunu göstermektedir. Bu alanda sürekli bir bilgi ve farkındalık yaratılması, biliřim suçlarına karşı daha etkili bir mücadele stratejisi geliştirilmesine yardımcı olacaktır.

### **1.1.3. Mukayeseli Hukukta Biliřim Suçları Yasal Düzenlemeleri**

Biliřim suçlarına karşı etkin ve kapsayıcı bir yasal çerçevenin oluşturulması büyük bir önem arz etmektedir. Hem ulusal hem de uluslararası düzeyde, bu suçların önüne geçmek, bireylerin ve kurumların dijital varlıklarını, gizliliklerini ve güvenliklerini korumak amacıyla hukukçular ve politika yapıcılar tarafından çeřitli yasalar ve düzenlemeler geliştirilmiřtir.<sup>38</sup>

Çevrimiçi oyun hesapları ve karakterlerinin yetkisiz ele geçirilmesi, dünya genelinde biliřim suçları arasında giderek artan bir yer tutmaktadır. Bu tür suçların yasal düzenlemeler açısından deęerlendirilmesi, ülkeden ülkeye farklılık göstermekle birlikte, ortak bir hukuki zemin arayışı da söz konusudur. Türkiye, Almanya, Güney Kore, ABD ve İngiltere gibi ülkeler, biliřim suçlarına karşı kendi hukuk sistemleri çerçevesinde önlemler almıřtır. Ancak, çevrimiçi oyun hesaplarının ele geçirilmesi gibi spesifik suçlar söz konusu olduğunda, bu ülkelerin yasal yaklaşımları ve suç tipolojilerinin tanımı arasında belirgin farklılıklar bulunmaktadır.

Türkiye'de, çevrimiçi oyun hesaplarının yetkisiz ele geçirilmesi, mevcut yasal çerçevede TCK madde 158/1/f'de "nitelikli dolandırıcılık" suç tasnifi ile deęerlendirilmeye meyilli olmakla birlikte, doğrudan TCK madde 142/2/e'de "nitelikli hırsızlık" suçu olarak tanımlanması için net bir yasal düzenleme bulunmamaktadır. Bu,

---

<sup>38</sup>Türk Ceza Kanunu (5237 Kanun Numaralı), Kiřisel Verilerin Korunması Kanunu (6698 Kanun Numaralı), Budapeřte Sözleşmesi (Biliřim Suçları Sözleşmesi) ve AB Genel Veri Koruma Tüzüğü (GDPR).

5237 sayılı Türk Ceza Kanunu'nda açıkça belirtilmemiş olup, bilişim suçlarına ilişkin mevcut düzenlemelerin bu tür suçları tam anlamıyla kapsayıp kapsamadığı konusunda tartışmalar bulunmaktadır. Dolayısıyla, bu alandaki yasal boşlukların giderilmesi ve suç tiplerinin net bir şekilde tanımlanması, suçla mücadelede daha etkin yöntemlerin geliştirilmesine katkı sağlayacaktır.

İsviçre, çevrimiçi oyunlardaki karakter hırsızlığı konusunda öne çıkan ülkelerden biridir. İsviçre Ceza Kanunu'nun 143. maddesi, izinsiz girişe karşı elektronik aygıtlar tarafından korunan bir bilişim sistemine yetkisiz olarak erişmeyi suç olarak kabul etmektedir. Bu düzenleme, çevrimiçi oyun hesaplarının yetkisiz ele geçirilmesi ve karakter hırsızlığı gibi eylemleri de kapsayabilir. İsviçre, bu tür suçlara karşı ciddi önlemler alarak bilişim suçlarıyla mücadelede önemli bir örnek teşkil etmektedir. İsviçre'nin bu yaklaşımı, çevrimiçi oyunlardaki karakter hırsızlığı gibi bilişim suçlarına karşı alınan önlemlerin uluslararası alanda nasıl farklılık gösterebileceğini göstermesi açısından dikkat çekicidir.<sup>39</sup>

Almanya'da ise, bilişim suçlarına karşı oldukça kapsamlı yasal düzenlemeler mevcuttur. Alman Ceza Kanunu (Strafgesetzbuch - StGB), bilişim teknolojileri yoluyla gerçekleştirilen dolandırıcılık ve hırsızlık eylemlerini kapsayacak şekilde genişletilmiştir. Özellikle, çevrimiçi oyun hesaplarının ele geçirilmesi, "Betrug"<sup>40</sup> (§263 StGB) yani dolandırıcılık suçu kapsamında değerlendirilebilecek bir eylemdir. Aynı zamanda, veri hırsızlığı ve kimlik hırsızlığı gibi suçlar da bu kapsamda ele alınmaktadır. Ancak, çevrimiçi oyun hesaplarının yetkisiz ele geçirilmesi ve oyun içi varlıkların çalınması spesifik olarak Alman yasalarında tanımlanmış bir suç tipi olarak belirtilmemiştir.<sup>41</sup>

ABD ve İngiltere gibi ülkelerde bilişim suçlarına ilişkin mevcut yasal düzenlemeler, genellikle "Computer Fraud and Abuse Act" (ABD) ve "Computer Misuse Act" (İngiltere) gibi kanunlar aracılığıyla sağlanmaktadır. Bu kanunlar, yetkisiz erişim, veri hırsızlığı ve dolandırıcılık gibi geniş bir suç yelpazesini kapsar.

<sup>39</sup>M.B. Kızıltan, '5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları', Yüksek Lisans Tezi, *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2007.

<sup>40</sup>S. Demirtaş, 'Alman Ceza Kanunu'nda Kurala İlişkin Örnekler Müessesesi: Kanunilik İlkesi Açısından Bir Değerlendirme', *Türkiye Adalet Akademisi Dergisi*, cilt: 13, sayı: 49, Ocak 2022, s. 434-440.

<sup>41</sup>A. İ. Erdağ, 'Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)', *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, cilt XIV, 2010, s. 276-300.

Ancak, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesine dair spesifik hükümler, bu genel düzenlemelerin kapsamı içinde değerlendirilmektedir. Her iki ülkede de dijital varlıkların çalınması ve çevrimiçi dolandırıcılık suçları ciddiye alınmakta, ancak bu suç tiplerine yönelik net ve açık yasal tanımların geliştirilmesi gerektiği konusunda bir ihtiyaç bulunmaktadır.<sup>42</sup>

Çevrimiçi oyun hesaplarının ve karakterlerinin yetkisiz ele geçirilmesi, uluslararası hukuk normları ve ulusal yasal düzenlemeler çerçevesinde spesifik bir suç tipi olarak tanımlanma ihtiyacı duymaktadır. Bu tür suçların hem dolandırıcılık hem de hırsızlık kategorilerinde değerlendirilmesi mümkün olsa da dijital varlıkların özgün niteliği, yasal düzenlemelerde daha açık ve spesifik tanımlamalar yapılmasını gerektirmektedir. Bu alandaki yasal boşlukların giderilmesi, bilişim suçlarıyla mücadelede önemli bir adım olacaktır.

#### **1.1.4. Türkiye’de Bilişim Suçlarının Gelişimi**

Türkiye özellikle bilişim suçlarına yönelik özelleşmiş yasalar ve düzenlemeler oluşturarak bu alanda önemli adımlar atmıştır. 2007 yılında kabul edilen 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, çevrimiçi aktiviteler ve bilişim suçları üzerinde bir denetim mekanizması oluşturarak, bireylerin ve kurumların dijital haklarını koruma altına almıştır. Bunun yanı sıra, 5237 sayılı Türk Ceza Kanunu, bilişim suçlarına yönelik detaylı tanımlamaları ve bu suçlara karşı uygulanacak cezai yaptırımları belirleyerek, ulusal düzeyde bu suçlarla mücadelede kritik bir rol oynamaktadır.

Teknolojinin ilerlemesiyle birlikte internet, hayatımızın ayrılmaz bir parçası haline gelmiştir. Ancak bu ilerlemenin getirdiği kolaylıkların yanı sıra, bilişim suçları da artış göstererek ciddi tehditler oluşturmaya başlamıştır.<sup>43</sup> Bu nedenle, ulusal ve uluslararası düzeyde yasal düzenlemelerin sürekli olarak güncellenmesi ve yeni ortaya çıkan suç türlerini de kapsayacak şekilde genişletilmesi gerekmektedir. Bu bağlamda,

---

<sup>42</sup>Kızıltan, a.g.e. s.32-34

<sup>43</sup>M.B. Kaya, ‘Bilişim Suç İstatistikleri - Türkiye Siber Güvenlik’, <https://mbkaya.com/bilisim-suc-istatistik-turkiye-siber-guvenlik/>, E.T: 25 Ekim 2023.

bilişim suçlarına karşı alınacak tedbirlerin ve yasal düzenlemelerin, sadece suçları cezalandırmakla kalmayıp, aynı zamanda bu suçların önlenmesinde de etkili olması beklenmektedir. Bu, bireylerin ve kurumların dijital dünyada daha güvenli bir şekilde faaliyet göstermelerini sağlayacak, aynı zamanda dijital teknolojilerin getirdiği fırsatlardan daha etkili bir şekilde yararlanmalarına olanak tanıyacaktır.

Türkiye'de bilişim suçlarına yönelik en önemli yasal düzenleme, 5237 sayılı Türk Ceza Kanunu'dur. Bu kanun, bilişim suçlarını detaylı bir şekilde tanımlar ve bu suçlara yönelik cezai yaptırımları belirlemektedir. Ancak, TCK'da bilişim suçlarına dair maddeler, genel bilişim suçlarını tanımlamakla birlikte, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi gibi daha spesifik suç türleri için net bir düzenleme bulunmamaktadır. Bu, ulusal düzeyde bu tür suçların tanımlanması ve cezalandırılması konusunda bir boşluk olduğunu göstermektedir. Hukuki düzenlemelerdeki bu boşluk, bilişim teknolojilerinin hızla geliştiği ve çevrimiçi oyunların popülerliğinin arttığı günümüzde, kullanıcıların haklarının yeterince korunamadığını göstermektedir. Dolayısıyla, çevrimiçi oyun hesaplarının ve oyun karakterlerinin ele geçirilmesi gibi yeni nesil bilişim suçlarına karşı daha spesifik yasal düzenlemelerin yapılması gerekmektedir. Bu düzenlemeler, mağduriyetlerin önlenmesi ve adaletin sağlanması adına büyük önem taşımaktadır.

## **1.2. Adli Bilişim Uygulamaları ve Delil Toplama**

Adli bilişim, hukuki süreçlerde dijital verilerin toplanması, incelenmesi ve raporlanması ile ilgili bir disiplindir. Bu alan, özellikle dijital çağda, suçların aydınlatılmasında ve kanıtların sunulmasında hayati bir rol oynamaktadır. Dijital çağ, her türlü bilginin elektronik ortamda saklandığı ve işlendiği bir dönemi ifade eder. Bu durum, suçların işlenme biçimlerinde değişikliklere yol açmış, dolayısıyla hukuki süreçlerin bu yeni gerçekliğe adapte olmasını zorunlu kılmıştır. Adli bilişim, bu bağlamda, dijital verilerin hukuki süreçlerde nasıl kullanılacağını ve değerlendirileceğini belirleyen kritik bir disiplindir.<sup>44</sup>

---

<sup>44</sup>Y. Bucak, 'Adli Bilişim ve Türk Ceza Muhakemesi Hukukunda Bilgisayarda Arama', Yüksek Lisans Tezi, *Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü*, İstanbul, 2019.

Adli biliřim alanında, delil toplama süreci, Anayasa madde 36 ve CMK madde 116, 119, 134 ve 135'in öngördüğü çerçevede titizlikle yürütülmelidir. Bu süreçte, bireylerin temel hak ve özgürlüklerine, özellikle özel hayatın gizliliğı ve veri koruma ilkelerine büyük önem verilmelidir.

Deliller, yetkili makamlarca ve CMK madde 160 kapsamında yasal sınırlar dahilinde toplanmalıdır. Adli biliřim uzmanlarının, delil toplama aşamasından itibaren mahkemeye sunulana kadar olan süreçteki asli görevleri, veri kaybını önlemek ve delillerin bütünlüğünü korumaktır. Özellikle acil müdahale gerektiren durumlar ve müdahale edilmemesi gereken durumlar dikkatle değerlendirilmelidir. Örneğın, bir biliřim sistemi saldırıya uğramış ve veri kaybı tehlikesi varsa, uzmanın hızlıca müdahale etmesi; ancak sistemin bir indirme işlemi yapıyor olması gibi potansiyel delil içerebilecek durumlarda ise müdahale etmemesi gerekmektedir.<sup>45</sup>

CMK madde 217/2 kapsamında delil toplama sürecinde hukuki ve etik kurallara sıkı sıkıya bağılı kalınması esastır. Delillerin manipüle edilmesi, yanlış yorumlanması veya hukuka aykırı yollarla elde edilmesi, delilin geçersiz sayılmasına ve hukuki sürecin zarar görmesine yol açabilir. Bu nedenle, adli biliřim uzmanlarının eğitimi, etik ilkelerin bilinmesi ve hukuki süreçlere hâkim olmaları büyük önem taşımaktadır. Bu yaklaşım, adli biliřim alanında hukukun üstünlüğünün korunmasına ve adil yargılamaların sağlanmasına katkıda bulunur.

### **1.2.1. Adli Biliřim Süreçleri**

Adli biliřim, çağımızın dijitalleşen dünyasında ortaya çıkan suçları aydınlatma ve adalete ulaşmada hayati bir rol oynar. Bu disiplin, biliřim teknolojilerinin tüm karmaşıklığı içinde işlenen suçların izini sürmek, delilleri toplamak ve bunları hukuki süreçlerde geçerli kanıtlar olarak sunmakla yükümlüdür. Adli biliřim uzmanları, dijital ortamlarda saklı bilgileri çözümleyerek, suçların arkasındaki gerçekleri gün ışığına çıkarmak için derinlemesine teknik bilgi ve keskin analitik düşünce becerilerini kullanır. Fiziksel boyutları göz önünde bulundurulduğunda mütevazı olan çalışma alanları, aslında sanal dünyanın sınırsız veri okyanusunda gezinen, suçların

---

<sup>45</sup>E. Gönenç, 'Adli Biliřim ve Elektronik Delillerin Hukuk Yargılamasındaki Yeri', Yüksek Lisans Tezi, *İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2015.

çözülmesine yardımcı olan bilgi avcılarıdır. Bu kapsamlı ve detaylı araştırma süreci, adli bilişim metodolojisinin titizlikle tasarlanmış adımlarını takip eder; bu adımlar, uzmanların dijital veriler arasında sistematik bir şekilde ilerlemelerini, her aşamada elde ettikleri bulguları değerlendirmelerini ve nihayetinde bu bulguları mahkemelerde delil olarak sunabilecek şekilde hazırlamalarını sağlar. Bu süreç, teknolojik uzmanlıkla hukuki bilginin entegrasyonunu gerektirir ve adli bilişim uzmanlarını, modern hukuk sisteminin vazgeçilmez unsurlarından biri haline getirir. Öyle ki, adli bilişim alanında yapılan çalışmalar, sadece suçların çözümünde değil, aynı zamanda suçların önlenmesinde de kritik öneme sahiptir. Böylelikle, adli bilişim, hukuki süreçlerle bütünleşik, dinamik ve sürekli gelişen bir disiplin olarak, dijital çağın getirdiği zorluklarla başa çıkmada merkezi bir role sahiptir.<sup>46</sup> Bu, adli bilişim uzmanlarının, her bir veri parçasının arkasında yatan hikâyeyi anlamlandırma ve adaletin tecellisine katkıda bulunma yolundaki çabalarının, yalnızca teknik bir beceriden çok daha fazlasını temsil ettiğini gösterir.

#### **1.2.1.1. İncelenmesi Gereken Dijital Sistemlerin ve Verinin Belirlenmesi**

Dijital çağın suç tipleri üzerindeki dönüştürücü etkisi, yasal ve adli süreçlerde yeni ve karmaşık zorluklar ortaya çıkarmaktadır. Özellikle internet ve bilişim teknolojilerinin gelişimi, geleneksel suç tiplerinin TCK madde 125/2 hakaret, TCK madde 105/2/d cinsel taciz, TCK madde 142/2/e hırsızlık ve TCK madde 158/1/f dolandırıcılık gibi dijital ortamlarda yeni biçimler almasına neden olmuş, bu da adli bilişim süreçlerinde dijital delillerin rolünü ön plana çıkarmıştır. Bu bağlamda, dijital delillerin adli süreçlerdeki kullanımı, sadece teknik bir mesele olmanın ötesinde, yasal uygunluk, etik standartlar ve hukuki geçerlilik açısından derinlemesine bir uzmanlık gerektirmektedir.

Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, dijital çağın yükselen bilişim suçlarından biri olarak dikkat çekmekte olup, sadece eğlence amaçlı platformlar olmaktan çıkıp, ekonomik değer taşıyan varlıkların birer sahnesi haline gelmiştir. Oyun içi karakterler, eşyalar ve hesaplar, gerçek dünya para birimi ile satın alınabilir ve takas edilebilir hale gelmiş, bu durum da bu varlıkları hedef alan suç

---

<sup>46</sup>Gönenç, a.g.e., s. 8.

faaliyetlerini artırmıştır. Dolayısıyla, bu tür varlıkların hukuki koruma altına alınması ve bilişim suçları kapsamında ciddiye alınması gerekmektedir. Adli bilişim süreçlerinde, bu yeni suç tiplerinin doğru bir şekilde anlaşılması ve soruşturulması adli bilişim uzmanlarının teknik yetkinliklerinin yanı sıra, hukuki ve etik düzlemlerde derin bir anlayışa sahip olmalarını zorunlu kılmaktadır. Bu kapsamda, dijital delillerin adli süreçlerdeki kullanımı, yasal standartlara ve etik ilkelere uygun bir şekilde gerçekleştirilmesi gereken karmaşık bir süreçtir. Dijital delillerin toplanması, analizi ve sunumu, suçların aydınlatılmasında ve gerçeklerin ortaya çıkarılmasında kritik bir role sahiptir. Bu sürecin etkin bir şekilde yönetilmesi, suçların adil ve etkin bir şekilde çözülmesine olanak tanır. Çevrimiçi oyun içi varlıkların ele geçirilmesi, modern bilişim suçları arasında öne çıkan bir fenomen olarak, adli bilişim alanının yetkinliklerini ve hukuki çerçevenin adaptasyonunu test eden bir vakadır. Bu suç türü, yalnızca bilişim teknolojilerinin suçlar üzerindeki etkisini değil, aynı zamanda adli süreçlerin bu yeni zorluklara nasıl yanıt verdiğini de göstermektedir. Adli bilişim sürecinde elde edilen bulguların hukuki geçerliliğinin ve güvenilirliğinin sağlanması, bu alanda çalışan profesyonellerin multidisipliner bir yaklaşım benimsemesini gerektirmekte, bu da adli bilişim alanını hem teknolojik hem de yasal bir perspektiften sürekli gelişen bir disiplin haline getirmektedir.<sup>47</sup>

#### **1.2.1.2. Dijital Veri ve Delillerin Toplanması**

Adli süreçlerde delilin önemi tartışılmaz bir gerçektir ve dijital çağda bu süreçler, dijital veri ve delillerin elde edilmesi, saklanması ve analiz edilmesi ile daha da karmaşık hale gelmiştir. Dijital deliller, e-postalar, metin mesajları, sosyal medya verileri, bulut depolama içerikleri ve daha pek çok dijital ortamda bulunan bilgileri kapsar. Bu tür deliller, suçların aydınlatılmasında, hukuk davalarında kanıt olarak kullanılmada ve hatta uluslararası anlaşmazlıkların çözümünde kritik rol oynar. Ancak dijital verilerin doğası gereği, veri bozulması, silinme ya da izinsiz değişiklik gibi risklerle karşı karşıya olması, adli bilişim uzmanları ve hukuk profesyonelleri için özel bir dikkat ve hassasiyet gerektirir.<sup>48</sup>

---

<sup>47</sup>M. A. Eren, 'Dijital Deliller ve Delil Yasakları', Doktora Tezi, *Hacettepe Üniversitesi Adli Bilimler Enstitüsü*, İstanbul, 2023.

<sup>48</sup>Ç. Arslan, 'Dijital Delil ve İletişimin Denetlenmesi', *Ceza Hukuku ve Kriminoloji Dergisi*, cilt: 3, sayı: 2, 2015, s. 256.

Uluslararası standartlar ve prosedürlere uyum, dijital delillerin bütünlüğünü korumak için elzemdir. Örneğin, bir bilgisayar korsanlığı vakasında elde edilen dijital kanıtlar, delillerin toplanma şekline itibaren titizlikle ele alınmalıdır. Bu özellikle delillerin adil bir yargılama için mahkemede sunulabilmesi açısından önemlidir. Delilin toplanması sırasında kullanılan yazılım ve donanım araçlarının uluslararası kabul görmüş standartlara uygun olması veri bütünlüğünün korunması açısından kritik öneme sahiptir. Ayrıca, dijital delillerin saklanması süreci de büyük bir önem taşır. Örneğin, bir şirketin iç yazışmaları veya finansal kayıtlarını içeren bir sunucudan elde edilen bilgiler, davanın seyrini değiştirebilecek potansiyele sahiptir. Bu nedenle, bu tür verilerin kopyalanması, şifrelenmesi ve güvenli bir şekilde saklanması, herhangi bir izinsiz erişim veya değişiklik riskini minimize eder. Delillerin analizi aşamasında ise, adli bilişim uzmanları tarafından kullanılan metodolojilerin ve araçların, deliller üzerinde herhangi bir değişiklik yapmadan, orijinalliğini koruyacak şekilde tasarlanması gerekmektedir. Bu özellikle karmaşık siber suçlar ve finansal dolandırıcılık vakalarında elde edilen dijital delillerin değerlendirilmesinde önemli bir faktördür. Bu süreçler, uluslararası standartlara ve prosedürlere sıkı sıkıya bağlı olarak yürütüldüğünde, adli süreçlerin adil ve etkin bir şekilde işlemesine katkıda bulunur.<sup>49</sup>

### **1.2.2. Adli Bilişim Teknikleri**

Ceza muhakemelerinde dijital delillerin kullanılabilmesi, bu verilerin teknik ve hukuki gerekliliklere uygun bir şekilde toplanıp işlenmesine bağlıdır. Bilgisayar ve diğer bilişim sistemlerinden elde edilen verilerin delil değeri taşıyabilmesi için, adli bilişim süreçlerinin titizlikle uygulanması gerekmektedir. Adli bilişim teknikleri, suç soruşturmaları ve hukuki süreçlerin etkin bir şekilde yönetilmesinde hayati öneme sahiptir. Bu teknikler, verilerin toplanması ve analiz edilmesinin yanı sıra, elde edilen bilgilerin hukuki çerçevede nasıl değerlendirileceğini ve kullanılacağını da kapsar. Adli bilişim alanında görev yapan uzmanlar, teknik yeteneklerinin yanı sıra hukuki ve etik bilgilerle donatılmış olarak, dijital verilerin yargı önünde güvenilir ve kabul

---

<sup>49</sup>Ö. Akcan, 'Adli Bilişim Veri İncelemelerinin Araştırılması', Yüksek Lisans Tezi, *Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü*, İstanbul, 2021.

edilebilir kanıtlar olarak kullanılmasını sağlama görevini üstlenirler. Bu nedenle adli bilişim, suçla mücadelede kritik bir rol oynayarak, teknoloji ve hukukun kesiştiği alanda yenilikçi çözümler sunmaktadır. Bu disiplin, hukuki süreçlerin adil ve etkin bir şekilde işlemesine katkıda bulunmakla kalmayıp, aynı zamanda suçların aydınlatılmasında ve adaletin tecellisinde temel bir araç olarak ön plana çıkmaktadır.<sup>50</sup>

### 1.2.2.1. Dijital Delillerin Analiz Edilmesi

Dijital delillerin analizi, çağımızın yargılamalarında merkezi bir öneme sahip, son derece detaylı ve kapsamlı bir süreçtir. Bu sürecin başlangıcı, suçun özgül doğasına göre olası delil konumlarının dikkatle tespit edilmesiyle işlemeye başlar. Bu adımda, delillerin yerleri, dosyaların adları, oluşturulma zamanları ve sahiplik bilgileri gibi kritik meta verilerin saptanması ve bunların hiçbir şekilde değişikliğe uğramadan korunması gereklidir. Bu, adli süreçlerde delillerin bütünlüğünün ve güvenirliliğinin korunmasının temelini oluşturur ve her bir işlemin titizlikle kayıt altına alınmasını zorunlu kılar.<sup>51</sup>

Dijital delil analizinin bir sonraki aşaması, delillerin hukuki ağırlığını ve mahkemede ispat değerini titiz bir şekilde değerlendirirken, dava ile ilgili olmayan bilgilerin ayıklanmasını içerir. Bu süreçte, çeşitli yazılım araçları kullanılarak gerçekleştirilen analiz, sadece ilgili ve davadaki iddialarla doğrudan bağlantılı olan veriler üzerine yoğunlaşır. Farklı suç türlerine yönelik olarak geliştirilen özelleşmiş analiz yöntemleri, bu sürecin hem etkin hem de hızlı bir şekilde ilerlemesini sağlar. Örneğin, internet tabanlı saldırılar söz konusu olduğunda, suçla ilişkilendirilen bilgisayarların depolama birimlerindeki yazılımlar, kullanıcı etkinlikleri ve internet geçmişi gibi veriler incelenirken, yasa dışı içerik bulundurma iddialarında ise öncelikli olarak resim ve video dosyaları detaylı bir şekilde analiz edilir.<sup>52</sup>

Bu kapsamlı analiz süreci, teknik bilgi ve becerilerin yanı sıra, hukuki normlar ve prosedürlere de derinlemesine hakimiyet gerektirir. Dijital delillerin analizinin

---

<sup>50</sup>M. Özen ve G. Özocak, 'Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)', *Ankara Barosu Dergisi*, 2015/1, s. 51.

<sup>51</sup>M. Orta, 'Bilişim Suçlarında Adli Analiz', Doktora Tezi, *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü*, Konya, 2015.

<sup>52</sup>U. Kaynakçıoğlu, 'Ceza Muhakemesinde Dijital Deliller', Yüksek Lisans Tezi, *Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2015.

yargılamalardaki etkinliđi, analiz edilen delillerin dođruluđu, güvenilirliđi ve hukuki geçerliliđi ile dođrudan ilişkilidir. Adli sürecin her aşamasında, delillerin toplanması, saklanması ve analiz edilmesi sırasında gösterilen titizlik ve hukuka uygunluk, adli işlemlerin sağlam temeller üzerinde yükselmesini sağlar. Nihayetinde, adli bilişim teknolojilerinin bilinçli ve etkin kullanımı sayesinde yürütölen dijital delil analizi, adaletin tecellisi için hayati bir öneme sahiptir. Bu süreç, sadece yargılamaların adil ve hızlı bir şekilde sonuçlanmasını sağlamakla kalmaz, aynı zamanda suçla mücadelede önemli bir araç olarak da işlev görür.

#### **1.2.2.2. Raporlama**

Adli bilişim süreci, Cumhuriyet Savcısı ve hâkim adına hareket eden adli bilişim uzmanı ve bilirkişileri kapsamaktadır. Bu uzmanlar, delillerin toplanması, inceleme/analiz ve raporlandırma işlemlerini gerçekleştirirler. Deliller, delil bütönlüğünü koruyarak toplanır ve analiz edilir. Sonuçlar, rapor halinde adli makamlara sunulur. Rapor hazırlanırken Ceza Muhakemesi Kanunu'nun 67. ve 68. maddelerinde belirtilen hususlara uyulur. Raporun anlaşılır, açık, kısa ve öz olması gerekmektedir ve içerisinde olay hakkında bilgiler, incelemenin özeti, deliller, kullanılan kaynaklar, elde edilen delillerin teslim bilgileri, bulgular ve hash hesaplamaları bulunmalıdır. Ek olarak, incelenen verilere dair detaylar ve olay günlükleri eklenmelidir. Raporların, tarafsız, objektif ve standartlara uygun şekilde hazırlanması, hâkim kararlarını etkileyebilecek öneme sahiptir. Mahkemeler, özellikle taşrada, yetersiz sayıda adli bilişim uzmanı nedeniyle sıkça standartlardan sapmış raporlarla karşılaşmaktadırlar. Bu durum, raporların yetersiz bulunarak yeniden değerlendirilmesine veya sürecin uzamasına yol açabilmektedir.<sup>53</sup>

"Çevrimiçi Oyun Hesabının ve Oyun Karakterinin Ele Geçirilmesinin Bilişim Suçları Kapsamında Deđerlendirilmesi" konulu raporda dikkate alınması gereken hususlar řu şekilde sıralayabiliriz;

1. Bilişim Suçlarındaki Tanım ve Kapsamın Açıklanması; Çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi, bilişim suçları çerçevesinde

---

<sup>53</sup>Bucak, a.g.e., s. 32.

nasıl tanımlandığının ve bu suçun hangi yasal kapsamlara girdiğinin detaylı bir şekilde incelenmesi gerekmektedir.

2. Korunan Hukuki Değerlerin Belirlenmesi; Bu tür suçların temelinde yatan hukuki değerlerin (örneğin, kişisel gizlilik, mülkiyet hakları) ve bu değerlerin nasıl ihlal edildiğinin açık bir şekilde ifade edilmesi önemlidir.
3. Delil Toplama Süreçlerinin İncelenmesi; Çevrimiçi oyun sunucuları ve diğer dijital platformlardan delil toplama metodolojilerinin ve bu süreçlerin hukuki çerçevelerinin detaylandırılması, raporun temel taşlarından biri olmalıdır.
4. Dijital Delillerin Korunması; Toplanan dijital delillerin bütünlüğünün nasıl korunduğu ve bu delillerin saklanma yöntemlerinin, adli bilişim prensipleri doğrultusunda açıklanması gerekmektedir.
5. Adli Bilişim Analiz Yöntemleri; Hesap ve karakter incelemelerinde kullanılan adli bilişim araçları ve yöntemlerinin, bu suçların aydınlatılmasında nasıl bir rol oynadığının anlatılması önemlidir.
6. İhlal Edilen Güvenlik Protokollerinin Analizi; Olayda ihlal edilen güvenlik protokolleri ve bu ihlallerin nasıl gerçekleştiğinin teknik analizinin yapılması, raporda yer alması gereken kritik bir bölümdür.
7. Zararın Boyutunun Değerlendirilmesi; Mağdurun uğradığı maddi ve manevi zararların boyutunun değerlendirilmesi ve bu zararların kapsamlı bir şekilde raporlanması.
8. Suçlunun Kimliğinin Belirlenme Yöntemleri; Suçlunun kimliğinin nasıl tespit edildiği ve bu süreçte kullanılan yöntemlerin, teknolojik ve hukuki açıdan incelenmesi.
9. Yasal Dayanakların İncelenmesi; İlgili yasal mevzuatın ve hukuki yorumların, bu tür suçların cezai sorumluluğunu nasıl şekillendirdiğinin detaylı bir şekilde ele alınması.
10. Güvenlik Önlemleri ve Kullanıcı Tedbirlerinin Önerilmesi; Benzer suçların önlenmesine yönelik önerilen güvenlik önlemleri ve kullanıcıların alabileceği tedbirlerin sıralanması.
11. Mağdur Profilinin Tanımlanması; Mağdurun demografik özellikleri ve suçun mağdur üzerindeki etkilerinin, sosyal ve psikolojik açıdan değerlendirilmesi.

12. Faillerin Motivasyon Analizi: Suçun faillerinin arkasındaki motivasyonların ve hedeflerin, suç psikolojisi ve sosyal etkiler açısından analiz edilmesi.
13. Kullanılan Teknolojik Araçların İncelemesi: Suçta kullanılan teknolojik araçlar ve yazılımların detaylı bir şekilde incelenmesi ve bu araçların nasıl kullanıldığının açıklanması.
14. Siber Güvenlik Uygulamalarının Değerlendirilmesi: Olayda kullanılan siber güvenlik uygulamalarının ve bu uygulamaların etkinliğinin değerlendirilmesi.
15. Olayın Zaman Çizelgesinin Oluşturulması: Suçun işleniş sürecinin ayrıntılı bir zaman çizelgesi ile belgelenmesi ve bu sürecin adım adım açıklanması.
16. Ulusal ve Uluslararası Mevzuatın Değerlendirilmesi: Olayın ulusal ve uluslararası hukuk çerçevesindeki yerinin ve öneminin değerlendirilmesi.
17. Benzer Olayların Analizi: Önceki benzer olaylarla karşılaştırmalar yaparak, bu suçların özellikleri ve ortak noktalarının belirlenmesi.
18. Sonuç ve Öneriler: Araştırmanın bulgularının özetlenmesi ve bu tür suçlarla mücadelede ileriye yönelik önerilerin sunulması.

Bu hususlar, raporun hem içeriğinin zenginliğini hem de analizin derinliğini sağlayacak şekilde detaylandırılmıştır, bilişim suçları bağlamında çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi konusunda kapsamlı bir çerçeve sunar.

## 2. SİBER GÜVENLİK VE ÇEVİRİMİÇİ OYUNLAR

Siber güvenlik, dijital ortamlarda güvenliği sağlama pratiği olarak öne çıkmakta olup, çevrimiçi oyunlar bu bağlamda önemli bir odak noktasıdır. Çevrimiçi oyunlar, dünya genelinde milyonlarca kullanıcıyı bir araya getiren interaktif platformlar olup, bu platformlar üzerinde kullanıcı verilerinin korunması ve oyun içi işlemlerin güvenliği büyük önem taşımaktadır. Siber güvenlik uzmanları, bu alanda kullanıcı hesaplarının izinsiz erişime ve saldırılara karşı korunması için çeşitli güvenlik önlemleri geliştirirken, aynı zamanda oyun içi alışverişler ve kişisel veri akışının şifrelenmesi gibi konularda da yenilikçi çözümler sunmaktadırlar. Çevrimiçi oyun sektörünün sürekli büyümesi ve evrimleşmesi, bu alanda siber güvenlik stratejilerinin de dinamik bir şekilde güncellenmesini zorunlu kılmaktadır. Bu bağlamda, ilerleyen bölümlerde çevrimiçi oyunlar ve siber güvenlik arasındaki ilişki daha kapsamlı bir şekilde ele alınacaktır.

### 2.1. Tanımlar ve Kavramlar

Dijitalleşme sürecinin hız kazanmasıyla birlikte, çevrimiçi oyunlar çağımızın en popüler eğlence ve sosyal etkileşim araçlarından biri haline gelmiştir. Bu alandaki büyüme, sadece gençler arasında değil, tüm yaş grupları arasında oyunların yaygınlaşmasına yol açmış ve oyun endüstrisinin ekonomik değeri, son on yılda muazzam bir artış göstererek 2012 yılında yaklaşık 70 milyar dolardan, 2022'de ise 200 milyar dolara yükselmiştir.<sup>54</sup> Ancak bu büyümenin bir yansıması olarak, siber güvenlik tehditleri de artış göstermiştir. Oyun hesapları, sadece bir karaktere erişim sağlamak amacıyla değil, aynı zamanda oyun içi satın alımlar ve gerçek para değeri taşıyan özel eşyalar için de kullanılmaktadır. Bu durum, siber suçlular için büyük bir çekicilik oluşturarak, hesap güvenliği meselesini önemli bir problem haline getirmiştir.

Çevrimiçi oyun sektörü, bu dijital çağın tehditlerine ve fırsatlarına hızla uyum sağlama çabası içerisinde. Oyun şirketleri, kullanıcıların bilgilerini korumak, hilecilik faaliyetlerini engellemek ve siber saldırılara karşı dayanıklı hale gelmek için sürekli olarak yatırım yapmaktadır. Buna karşılık, kullanıcıların da kendi

<sup>54</sup><https://kalkinmaguncesi.izka.org.tr/index.php/2021/02/02/kuresel-pazarlara-giden-yol-dijital-oyun-sektoru/>, 'Küresel Pazarlara Giden Yol: Dijital Oyun Sektörü', İZKA, E.T: 27 Ekim 2023.

güvenliklerini sağlama konusunda proaktif davranmaları gerekmekte; şifrelerini düzenli olarak değiştirmeleri, iki faktörlü kimlik doğrulama gibi yöntemler kullanmaları önerilmektedir. Bu yöntemler, sadece maddi kayıpları önlemekle kalmaz, aynı zamanda güvenli bir oyun deneyimi sunar.<sup>55</sup>

Ancak, bazı oyunların yönetici yetkilerini talep etmesi, özellikle ücretsiz oyunlar söz konusu olduğunda, zararlı yazılım riskini arttırabilir. Bu nedenle, yönetici haklarıyla çalıştırılacak oyunların güvenilirliği konusunda dikkatli olunmalı ve tarayıcı üzerinden oynanan oyunlarda güvenlik ayarlarının doğru yapılandırılması büyük önem taşımaktadır.<sup>56</sup> Ayrıca, ev kullanıcılarının güvenlik duvarlarında, çok oyunculu oyunlar için açık bıraktıkları istisnalar, bilgisayarın güvenliğini riske atabilir. Bu durum, tanınmış oyuncular için IP temelli ayrıcalıkların tanınmasını, siber güvenlikte bir adım önde olmanın bir yolu olarak öne çıkarır.<sup>57</sup> Dijital oyunların popülerliği ve ekonomik değeri arttıkça, siber güvenlik tehditleri de aynı oranda yükselmekte ve bu durum hem oyun şirketlerinin hem de kullanıcıların sürekli dikkatli ve koruyucu önlemler almasını zorunlu kılmaktadır. Bu çerçevede, güvenlik önlemlerinin artırılması, bilinçli kullanım ve sürekli güncellenen güvenlik stratejileri, güvenli bir çevrimiçi oyun deneyimi için olmazsa olmazlar arasında yer almaktadır.

### 2.1.1. Siber Güvenlik Kavramı

Siber güvenlik, internetin modern çağda hayatımızın her alanına nüfuz etmesiyle önem kazanmıştır. İnternet, bireylerin özel yaşantılarından iş dünyasına, kamu kuruluşlarından uluslararası ilişkilere kadar geniş bir yelpazede etkin bir şekilde kullanılmaktadır. İnternetin bilgi erişimi ve aktarımında sunduğu kolaylıklar, kamu ve özel sektördeki işleyişin verimliliğini artırmıştır. Ancak, bu olumlu yönlerinin yanında, 2000'li yılların başından itibaren teknolojik gelişmelerle birlikte siber tehditlerin de ortaya çıkmasına neden olmuştur.<sup>58</sup> Bu bağlamda, siber güvenlik, bu tehditlere karşı alınacak önlemlerin hukuki boyutunu ifade etmektedir.

<sup>55</sup>Türkiye Cumhuriyeti, Dijital Dönüşüm Ofisi, 'Video Oyun Endüstrisi', Ankara, 2022, s. 15.

<sup>56</sup>Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı, 'Çevrimiçi Oyunlara İlişkin Güvenlik Riskleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Kasım 2014, s. 6.

<sup>57</sup>Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı, 'Çevrimiçi Oyunlara İlişkin Güvenlik Riskleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Kasım 2014, s. 7.

<sup>58</sup>S. Tunca, 'Modern Çağda Siber Güvenlik Kavramı', *Dumlupınar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, sayı: 3, 2015, s. 3.

Siber alandaki tehditlerin artışı, siber güvenlik ihtiyacını beraberinde getirmiştir. Bireylerin ve kurumların teknolojik cihazlarda sakladığı geniş bilgi yelpazesi, kimlikten banka hesap bilgilerine kadar çeşitlilik göstermekte ve bu durum, siber tehditlerin potansiyelini artırmaktadır.<sup>59</sup> Çevrimiçi oyunlar, sosyal etkileşim ve eğlence sunmanın yanı sıra, kullanıcıların kişisel bilgilerini ve oyun içi kazanımlarını sakladığı platformlar haline gelmiştir. Bu nedenle siber güvenlik hem kişisel verileri hem de çevrimiçi oyun hesap bilgilerini koruma amacını taşımaktadır. Kullanıcıların internet üzerindeki reklamlara, sahte e-postalara veya tehlikeli programlara tıklaması, siber tehditlere maruz kalma riskini artırabilir. Ancak, bilinçli bir çevrimiçi oyun deneyimi ve doğru güvenlik önlemleri ile bu riskler minimize edilebilir. Bu bağlamda, siber güvenlik, bireylerin ve kurumların bilgilerini, çevrimiçi oyun hesaplarını ve oyun içi kazanımlarını koruma altına almayı amaçlayan hukuki bir zorunluluktur.

Siber ortamda, bireylerin ve kurumların bilgilerini tehdit eden çeşitli saldırı araç ve yöntemleri bulunmaktadır. Bu araçlar arasında virüsler, solucanlar, Truva atları, robotlar (botlar) ve casus yazılımlar öne çıkmaktadır.<sup>60</sup> Virüsler, teknolojik cihazlara bulaşarak zarar verebilen ve başka programlara ihtiyaç duyarak çoğalan zararlı yazılımlar; solucanlar, ağlar üzerinden bulaşan ve başka bir dosya veya programa ihtiyaç duymadan çoğalan zararlı yazılımlar; truva atları, normal bir dosya gibi görünse de zararlı faaliyetlerde bulunan yazılımlar; robotlar (botlar), bir dizi bot oluşumundan kaynaklanarak teknolojik cihazlara bulaşan zararlı yazılımlar ve casus yazılımlar ise, kullanıcıların kişisel ve gizli bilgilerini üçüncü kişilere aktarmak amacıyla oluşturulan zararlı yazılımlardır.<sup>61</sup> Bu tehditler, bireylerin ve kurumların siber güvenliğini riske atmaktadır ve bu nedenle hukuki önlemlerin alınması zorunludur.

### 2.1.2. Çevrimiçi Oyun Endüstrisi

Çevrimiçi oyun endüstrisi, son on yılda teknolojik devrimin yanında sosyal, ekonomik ve kültürel bir fenomen haline gelmiştir. Bu evrim, gençlerden yaşlılara

---

<sup>59</sup>Tunca, a.g.e., s. 4.

<sup>60</sup>M. N. Ögün ve A. Kaya, 'Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler', *Güvenlik Stratejileri Dergisi*, cilt: 9, sayı: 18, 2013, s. 153.

<sup>61</sup>Ögün ve Kaya, a.g.e., s. 154.

kadar geniş bir demografik yelpazeyi kapsayan milyarlarca kullanıcının hayatında önemli bir yer edinmiştir. Gelişen internet altyapısı ve mobil cihazların yaygınlaşmasıyla, oyunlar sadece bir eğlence aracı olmanın ötesine geçmiş, sosyal etkileşim, stratejik düşünce ve kültürel keşif için bir platform olmuştur.

Küresel geliri 2022 yılında yaklaşık 200 milyar dolar<sup>62</sup> olan bu sektör, sadece eğlence endüstrisinde değil, aynı zamanda ekonomide de önemli bir oyuncu haline gelmiştir. Bu gelirin yarısını mobil oyunlar oluştururken, yaklaşık 2.7 milyar insanın<sup>63</sup> aktif olarak çevrimiçi oyun oynadığı belirtiliyor. Bu rakamlar, oyun endüstrisinin sadece bir eğlence aracı olmadığını, aynı zamanda sosyal ve ekonomik bir güç olarak da kabul edilmesi gerektiğini gösteriyor. Oyunların teknolojik olarak ne kadar ileriye gittiği konusunda bulut tabanlı oyun hizmetleri, sanal ve artırılmış gerçeklik uygulamaları en belirgin örneklerdendir. Bu teknolojiler sayesinde kullanıcılar, daha önce hayal bile edemedikleri deneyimleri yaşama fırsatı bulmuşlardır. Yüksek hızlı internet bağlantıları ve yapay zekâ ile desteklenen oyun mekanikleri, gerçekçilik ve oynanabilirlik seviyelerini yeni zirvelere taşımıştır.

Bu hızlı büyüme ve teknolojik ilerleme, doğal olarak bir dizi hukuki ve etik sorunu da beraberinde getirmiştir. Oyuncuların kişisel verilerinin nasıl kullanılacağı, saklanacağı ve paylaşılacağı konuları, veri koruma ve gizlilik yasalarını gündeme getirmiştir. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR)<sup>64</sup> gibi düzenlemeler, bireylerin verilerini koruma altına almayı amaçlamaktadır. Oyun içi satın almaların ve rastgele ödüllendirme mekanizmalarının kumarla benzerlikleri, oyun endüstrisini kumar düzenlemeleriyle karşı karşıya bırakmıştır. Bazı ülkeler, bu tür özellikleri sınırlayan veya yasaklayan yasaları uygulamaya koymuştur.

Oyunların tasarım, hikâye ve karakterlerinin korunması, 5846 numaralı kanun ile fikri mülkiyet haklarının önemini ortaya koymaktadır. Oyun şirketleri, bu hakları koruma altına alabilmek ve olası ihlalleri önlemek için hukuki yollara başvurma ihtiyacı duymaktadır. Çevrimiçi oyun endüstrisi hem teknolojik hem de sosyal

<sup>62</sup><https://kalkinmaguncesi.izka.org.tr/index.php/2021/02/02/kuresel-pazarlara-giden-yol-dijital-oyun-sektoru/>, 'Küresel Pazarlara Giden Yol: Dijital Oyun Sektörü', İZKA, E.T: 27 Ekim 2023.

<sup>63</sup><https://kalkinmaguncesi.izka.org.tr/index.php/2021/02/02/kuresel-pazarlara-giden-yol-dijital-oyun-sektoru/>, 'Küresel Pazarlara Giden Yol: Dijital Oyun Sektörü', İZKA, E.T: 27 Ekim 2023.

<sup>64</sup>A. N. Akıncı, 'Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi', *Çalışma Raporu 6, Türkiye Cumhuriyeti Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü*, Ankara, 2017, s. 7.

yönleriyle günümüz dünyasında öne çıkmaktadır ve bu büyümenin getirdiği fırsatlar kadar, karşılaşılan hukuki ve etik zorluklar da bulunmaktadır. Bu büyümeyle birlikte, oyuncuların kişisel verilerinin korunması, fikri mülkiyet hakları, oyun içi satın almaların düzenlenmesi ve oyun bağımlılığı gibi konularda hukuki ve etik zorluklar da ortaya çıkmıştır.<sup>65</sup> Özellikle, oyuncuların kişisel verilerinin korunması konusunda, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) gibi uluslararası düzenlemelerin yanı sıra ulusal mevzuatlarda da önemli değişiklikler yapılmıştır. Fikri mülkiyet hakları, oyun tasarımcıları, geliştiricileri ve yayıncıları için kritik bir öneme sahip olup, bu hakların ihlali durumunda ciddi hukuki yaptırımların uygulanabileceği unutulmamalıdır. Oyun şirketleri, oyuncular ve yasa yapıcılar, bu zorlukların üstesinden gelmek ve sürdürülebilir bir gelecek inşa etmek için bir araya gelmelidirler.

## **2.2. Çevrimiçi Oyun Hesaplarının Değeri ve Mülkiyet Kavramı**

Çevrimiçi oyunların büyüyen dünyası, gelişen teknoloji ve küresel bağlantıların bir sonucu olarak, bireysel hesapların değerini artırmıştır. Oyuncular, seviye atlamak, eşya toplamak veya oyun içi para birimi kazanmak için saatlerce, hatta günlerce zaman harcarlar. Bu çabanın bir sonucu olarak, bir oyuncunun hesabı sadece duygusal değil, aynı zamanda maddi bir değere de sahip olabilir. Özellikle popüler Çok Oyunculu Çevrimiçi Rol Yapma Oyunu (Massively Multiplayer Online Role-Playing Game)<sup>66</sup> ve Çok Oyunculu Çevrimiçi Savaş Arenası (Multiplayer Online Battle Arena)<sup>67</sup> oyunları gibi, geniş oyuncu tabanına sahip oyunlarda bu durum daha belirgindir. Sanal ortamlarda, özellikle çevrimiçi oyunlarda, kullanıcıların gerçek para yatırımı yaparak elde ettikleri hesaplar, karakterler ve oyun içi eşyalar gibi dijital varlıkların giderek artan maddi değeri, geleneksel mülkiyet hukuku ilkelerini zorlayarak, bu varlıkların hukuki statüsünün, sahiplik haklarının ve devredilebilirliğinin netleştirilmesi gerektiğini vurgulamakta ve hukukçuları, sanal

---

<sup>65</sup>A. N. Akıncı, 'Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi', *Çalışma Raporu 6, Türkiye Cumhuriyeti Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü*, Ankara, 2017, s. 14.

<sup>66</sup>'Dijital Oyun Sektörü Raporu', *Ankara Kalkınma Ajansı*, Ankara, 2017, s. 19.

<sup>67</sup>'Dijital Oyun Sektörü Raporu', *Ankara Kalkınma Ajansı*, Ankara, 2017, s. 6.

dünyanın özgün dinamiklerine uygun yeni yasal çerçeveler geliştirmeye teşvik etmektedir.<sup>68</sup>

Mülkiyet hakkı Anayasa madde 35’de, bireylerin mal edinme ve devretme özgürlüğünü ifade eder; ancak bu hak, kamu menfaati gözetilerek yasal çerçevede sınırlanabilir ve toplumsal fayda ile çatışmamalıdır. Anayasa'nın mülkiyet hakkının sınırlarını kanun koyucunun belirlemesine imkan tanıdığı halde, bu takdir yetkisinin, Anayasa'nın 35. maddesinde özel mülkiyetin varlığını kabul eden temel ilkelere bağlı kalarak kullanılması gerektiği, dolayısıyla kanun koyucunun özel mülkiyeti tamamen ortadan kaldıracak nitelikte düzenlemeler yapmasının mümkün olmadığı, mülkiyet hakkının kapsamının belirlenmesinde ise mülkiyet konusu nesnenin özellikleri, dijital mülkiyetin kaynağı, dijital mal sahibine tanınan haklar ve yüklenen yükümlülükler gibi faktörlerin bireysel olarak değerlendirilmesi gerektiği anlaşılmaktadır.<sup>69</sup> Mülkiyet hakkının klasik tanımı, somut varlıkların mülkiyetine yönelikken, dijital çağın yükselişiyle birlikte bu hak, sanal varlıkların sahipliği konusunda yeni ve karmaşık boyutlar kazanmıştır. Oyun içi öğeler ve karakterler genellikle oyunun geliştiricileri veya yayıncıları tarafından kontrol edilir ve kullanıcılar bu öğeleri kullanma hakkına sahip olurlar,<sup>70</sup> ancak bu öğelerin gerçek sahipleri olarak kabul edilmezler.<sup>71</sup> Bu durum, oyun içi öğelerin ve hesapların hukuki statüsünün belirsizliğine yol açar.

Daha da karmaşıklaşan durum, oyun şirketlerinin genellikle kullanıcılarına hesaplarını veya oyun içi öğeleri satmamaları veya takas etmemeleri konusunda kısıtlamalar getiriyor olmasıdır. Ancak, bu kısıtlamalar, çevrimiçi oyun hesaplarının ve oyun içi eşyaların 'gri pazar' olarak bilinen bir alanda büyük miktarda alınıp satıldığı gerçeğini engellemez. Gri pazar ürünleri, resmi dağıtım ağlarının dışında ticareti yapılan otantik mallar olup, özellikle dijital alanda, oyun şirketlerinin kullanıcıların

---

<sup>68</sup>B. Fidan, ‘Çevrimiçi Oyun Oynayan Kişiler ile Oyun Karakterleri Arasındaki Bağlar ve Tüketici Davranışları İlişkisi: Metin2 ve League Of Legends Örnekleri’, Yüksek Lisans Tezi, *Ankara Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2020.

<sup>69</sup>S. Şimşek, ‘Mülkiyet Hakkının Kapsamı, Sınırlandırma Nedenleri ve Şartları Açısından 1982 Anayasası ve Avrupa İnsan Hakları Sözleşmesi: Karşılaştırmalı Bir Analiz -I’, *TBB Dergisi*, sayı: 91, 2010, s. 188.

<sup>70</sup>‘Şirket işbu Sözleşme ile Kullanıcıya münhasır olmayan, geri çağırılabilir, devredilemez, alt lisanslamaya konu olmayan bir sınırlı lisans ve *My.Games* Ekosistemini ticari olmayan, kişisel amaçlar için kullanma hakkı tanımaktadır.’, *My.Games, EULA Sözleşmesi*, s. 4.

<sup>71</sup>‘Kullanma Hakkı. İşbu EULA'nın hüküm ve koşullarına tam olarak uymanız koşuluyla ve bunlara tam olarak uyduğunuzda Lisans Veren Size, geçerli Siparişte belirtilen süre (süre belirtilmemişse Yazılımı daima kullanabilirsiniz) boyunca Yazılımı kullanmanız için kişisel, münhasır olmayan bir lisans verir.’, *Dell, EULA Sözleşmesi*, s. 1.

hesaplarını veya oyun içi varlıklarını satışa veya takasa sunmalarına yönelik getirdikleri kısıtlamalara rağmen, bu tür dijital varlıkların ve hesapların, 'gri pazar' olarak adlandırılan ve yasal olmayan bir ticaret alanında yoğun bir şekilde alınıp satıldığı bir gerçekliği yansıtmaktadır.<sup>72</sup> Hesap hırsızlığı, dolandırıcılık ve diğer bilişim suçları, bu 'gri pazar'ın bir sonucudur. Kullanıcı hesaplarının değeri, onları siber suçlular için cazip hedefler haline getirir. Oyun hesaplarının, eşyalarının veya oyun içi para biriminin çalınması, sadece oyun içi etkileşimleri değil, aynı zamanda oyun dışı sosyal ve ekonomik etkileşimleri de etkileyebilir.

Bu durum, oyun şirketlerinin, hukuk düzenleyicilerinin ve kullanıcıların bu konuları daha iyi anlamaları ve etkin bir çözüm bulmaları gerektiğini göstermektedir. Çevrimiçi oyunların etkisi ve çapı arttıkça, bu tür sorunları çözmek için gelişmiş yasal ve teknolojik çözümler ihtiyacı da artmaktadır. Geliştiriciler ve yayıncılar tarafından daha güvenli hesap doğrulama ve izleme sistemlerinin yanı sıra kullanıcılar arasında daha iyi bir bilinç yayılması gerekmektedir. Bununla birlikte, hukukun da bu yeni dijital mülkiyet formlarını tanıyan ve düzenleyen yasaları geliştirmesi ve uygulaması gerekmektedir. Yasal düzenlemeler, geliştiricilerin kullanıcılarına sunduğu hizmetler ve kullanıcılar arasında gerçekleşen etkileşimler arasında bir denge sağlamalıdır. Bu, dijital mülkiyet haklarının yanı sıra dijital mülkiyetin hırsızlığını ve kötüye kullanılmasını önlemek için önemlidir.

Çevrimiçi oyun hesaplarının değeri ve mülkiyet kavramı, dijital dünyada hızla büyüyen ve evrim geçiren bir alan olup hem yasal hem de teknolojik düzlemde özel bir dikkat gerektirir. Bu alandaki zorlukları ve fırsatları anlamak, çevrimiçi oyun topluluklarının sadece daha adil ve güvenli olmasını sağlamakla kalmaz, aynı zamanda çevrimiçi oyun endüstrisinin genel sürdürülebilirliğini ve büyümesini de destekler. Gelişen bu durum, oyun şirketlerinin, hukuk düzenleyicilerinin ve kullanıcıların bu konuları daha iyi anlamaları ve etkin bir çözüm bulmaları gerektiğini göstermektedir. Özellikle bazı ülkelerin bu konudaki yaklaşımlarını ele alarak daha geniş bir perspektif kazanabiliriz:

---

<sup>72</sup>H. H. Ceylan ve B. Köse, 'Tüketicilerin Gri Pazar Ürün Tercihleri Üzerine Bir Araştırma', *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, Karaman, cilt: 20, sayı: 34, 2018, s. 2.

Güney Kore, çevrimiçi oyun sektöründeki öncü konumu nedeniyle dijital mülkiyet ve oyun içi eşya ticareti konularında bazı hukuki meydan okumalarla karşılaşmıştır. 2010 yılında, gençler arasında artan kumar alışkanlıklarına ve aşırı harcamalara yanıt olarak, hükümet, oyun içi eşyaların gerçek para karşılığında ticaretini yasaklayan mevzuatları kabul etti.<sup>73</sup> Bu, oyun içi eşya ticaretinin potansiyel zararlarını sınırlamayı amaçlayan stratejik bir harekettir.

Bu yasal düzenlemelere ek olarak, oyun içi eşya ve karakter hırsızlığına yönelik ciddi cezai yaptırımların getirilmesi, dijital varlıkların gerçek dünyada somut bir değeri olduğunun resmi bir kabulü olarak görülebilir.<sup>74</sup> Bu düzenlemelerin ardından oyun şirketleri, kullanıcılarına daha şeffaf olmayı taahhüt ederek ve koruyarak kendi iç düzenlemelerini hayata geçirmiştir. Şirketler, oyun içi satın alımların ve eşya ticaretinin nasıl gerçekleştirildiğine dair politikalarını revize etmiştir. Ancak, dijital mülkiyetin<sup>75</sup> tanımı ve sınırları konusundaki tartışmalar, özellikle blockchain teknolojisi ve kripto paraların<sup>76</sup> ortaya çıkışıyla birlikte, hukuki alanda devam eden bir konu olmaya devam etmektedir. Bu, hukukun, teknolojinin ve endüstrinin hızla değişen doğasını takip edebilmesi için sürekli bir adaptasyon ve yeniden değerlendirme gerektiren bir meseledir.

Çin, nüfusu gereği dünya genelindeki online oyun pazarında önemli bir oyuncudur. Bu öncülük, ülkede dijital mülkiyet ve oyun içi eşya ticareti konularında bazı hukuki zorluklara neden olmuştur. Çin, dijital mülkiyetin tanımı ve korunması konusunda bazı proaktif adımlar atmıştır. Özellikle, sanal eşya ve oyun içi hesap ticaretinin artmasıyla birlikte, bu tür varlıkların hukuki olarak tanınması ve korunması ihtiyacı ortaya çıkmıştır. Bu bağlamda, Çin Yüksek Mahkemesi, sanal eşya ve hesap hırsızlığı gibi dijital varlıkları gerçek dünyadaki mülkiyet hırsızlığına eşdeğer olarak kabul eden<sup>77</sup> yasal kararlar almıştır. Bu kararlar, oyun içi eşyaların ve dijital varlıkların

---

<sup>73</sup>Ö. Simav, 'Geç Saatlere Kadar Oyun Yasak', <https://www.hurriyet.com.tr/aile/yazarlar/oznur-simav/gec-saatlere-kadar-oyun-yasak-401410>, E.T: 29 Ekim 2023.

<sup>74</sup>P. Özkaya, 'Dijital Dünyada Çevrimiçi Riskler, Bilişim Suçları ve Mağdur Çocuk', *Türkiye Adalet Akademisi Dergisi*, cilt: 14, sayı: 53, Ocak 2023, s. 13-42.

<sup>75</sup>T. Yayla, 'Sanal Hırsızlık', <https://talhayayla.av.tr/sanal-mulkiyet/>, E.T: 29 Ekim 2023.

<sup>76</sup><https://www.trthaber.com/haber/dunya/guney-kore-nft-oyunlarini-yasaklayacak-640720.html>, 'Güney Kore NFT Oyunlarını Yasaklayacak', E.T: 29 Ekim 2023.

<sup>77</sup><https://www.bloomberght.com/cin-de-yuksek-mahkeme-dijital-varlik-haklarinin-korunmasi-cagrisinda-bulundu-2260616>, 'Çin'de Yüksek Mahkeme Dijital Varlık Haklarının Korunması Çağrısında Bulundu', E.T: 30 Ekim 2023.

gerçek dünyada bir değeri olduğunu resmi olarak kabul etmektedir. Bu yasal kararlar, dijital mülkiyet haklarının korunması için bir temel oluşturmaktadır. Ancak, bu yasal düzenlemelere rağmen, oyun içi eşya ticareti ve dijital mülkiyet hakkında devam eden tartışmalar vardır. Özellikle, dijital varlıkların, fiziksel mülkiyete göre nasıl bir hukuki statüye sahip olması gerektiği konusunda belirsizlikler bulunmaktadır.<sup>78</sup> Buna ek olarak, Çin'deki oyun şirketleri, kullanıcıların dijital haklarını korumak ve şeffaflığı artırmak için kendi politika ve uygulamalarını gözden geçirmişlerdir. Bu, oyun içi satın alımların ve eşya ticaretinin nasıl gerçekleştirildiğine dair daha açık ve anlaşılır politikaların benimsenmesini içermektedir.

Amerika Birleşik Devletleri, online oyun endüstrisinin küresel olarak büyümesinde hem teknolojik imkanlar olarak hem de nüfus açısından önemli bir rol oynamaktadır. Bu konum, ülkede dijital mülkiyet ve oyun içi eşya ticareti hakkındaki hukuki tartışmaların ve zorlukların artmasına neden olmuştur. ABD'de, dijital mülkiyetin tanımı ve korunması konusundaki yasal çerçeve, diğer ülkelere göre daha dağınık ve belirsizdir. Özellikle, oyun içi eşyalar ve online oyun hesapları genellikle "dijital mülkiyet" olarak tanımlanmaz.<sup>79</sup> Bunun yerine, bu varlıkların kullanımı, oyun şirketlerinin Kullanıcı Sözleşmesi (EULA) tarafından düzenlenir. EULA genellikle oyun şirketlerine geniş haklar tanıırken, kullanıcılara sınırlı lisans hakları verir.<sup>80</sup>

EULA (End User License Agreement), Türkçede "Son Kullanıcı Lisans Sözleşmesi" olarak bilinir. EULA, bir yazılımın veya ürünün son kullanıcıya sunulan ve kullanıcının yazılımı veya ürünü kullanabilmesi için kabul etmesi gereken bir lisans sözleşmesidir.<sup>81</sup> EULA'nın temel özellikleri şunlardır:

Kullanım Hakları, EULA, kullanıcının yazılımı veya ürünü nasıl kullanabileceğini detaylı olarak açıklar. Örneğin, bir yazılımın kaç bilgisayarda çalıştırılabileceği veya yazılımın ticari amaçlarla kullanılıp kullanılamayacağı bu bölümde belirtilir.<sup>82</sup>

---

<sup>78</sup> <https://zhuanlan.zhihu.com/p/260383465>, 'Zhihu', E.T: 30 Ekim 2023.

<sup>79</sup> <https://www.forbes.com/sites/oliverherzfeld/2012/12/04/what-is-the-legal-status-of-virtual-goods/?sh=51076f8b108a>, O. Herzfeld, 'What Is The Legal Status Of Virtual Goods?', E.T: 30 Ekim 2023.

<sup>80</sup> <https://law.stackexchange.com/questions/8992/is-legal-to-sell-virtual-goods>, 'Is Legal To Sell Virtual Goods?', E.T: 30 Ekim 2023.

<sup>81</sup> <https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, 'The Importance Of The End-User License Agreement', E.T: 30 Ekim 2023.

<sup>82</sup> <https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, 'The Importance Of The End-User License Agreement', E.T: 30 Ekim 2023.

Kısıtlamalar, Sözleşme, yazılımın veya ürünün kullanımıyla ilgili belirli kısıtlamaları da içerebilir. Bu, yazılımın tersine mühendislik uygulamalarına karşı korunması, kopyalanmaması veya dağıtılmaması gibi kısıtlamaları içerebilir.<sup>83</sup>

Fikri Mülkiyet Hakları, EULA genellikle yazılımın veya ürünün fikri mülkiyet haklarını korur. Bu, yazılımın veya ürünün telif hakları, ticari markaları ve diğer fikri mülkiyet haklarının yazılımın veya ürünün üreticisine ait olduğunu belirtir.<sup>84</sup>

Sorumluluk Reddi, EULA sözleşmelerinde genellikle bir sorumluluk reddi bölümü bulunur. Bu bölüm, yazılımın veya ürünün kullanımından kaynaklanabilecek olası zararlar için üreticinin sorumluluk taşımadığını belirtir.<sup>85</sup>

Sonlandırma, EULA, kullanıcının sözleşme şartlarına uymadığı durumlarda lisansın nasıl sonlandırılacağını açıklar.<sup>86</sup> Diğer Şartlar, EULA ayrıca gizlilik politikaları, veri toplama ve kullanımı, güncellemeler ve diğer önemli konuları da kapsayabilir.

EULA sözleşmeleri, genellikle bir yazılımı veya dijital ürünü ilk kez yüklerken veya kullanırken karşınıza çıkar.<sup>87</sup> Kullanıcılar, bu sözleşmeyi kabul etmeden yazılımı veya ürünü kullanamazlar. Ancak, birçok kullanıcı bu tür sözleşmeleri dikkatlice okumadan hızla kabul eder, bu da bazı hukuki risklere yol açabilir. Bu nedenle, bir EULA'nın şartlarını kabul etmeden önce dikkatlice okunması gerekmektedir. Ancak, bu tür sözleşmelerin ötesinde, oyun içi eşya ve hesap hırsızlığı gibi suçlar genellikle dolandırıcılık veya bilgisayar suçları olarak değerlendirilir. Bu suçlarda, çalınan dijital varlıkların yasal sahipleri hem mülkiyet haklarını kaybetmiş hem de mağdur konumuna düşmüş kişilerdir, bu nedenle suçluların yargılanması ve hakların iadesi büyük önem taşır. Bu tür suçlar federal veya eyalet yasaları kapsamında cezai yaptırımlarla karşılaşılabılır.<sup>88</sup>

<sup>83</sup><https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, 'The Importance Of The End-User License Agreement', E.T: 30 Ekim 2023.

<sup>84</sup><https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, 'The Importance Of The End-User License Agreement', E.T: 30 Ekim 2023.

<sup>85</sup><https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, 'The Importance Of The End-User License Agreement', E.T: 30 Ekim 2023.

<sup>86</sup><https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, 'The Importance Of The End-User License Agreement', E.T: 30 Ekim 2023.

<sup>87</sup><https://www.epicgames.com/help/tr/fall-guys-c9505712380315/teknik-destek-c9505744757531/son-kullanici-lisans-sozlesmesi-eula-a9505740271131>, 'Son Kullanıcı Lisans Sözleşmesi (EULA)', E.T: 30 Ekim 2023.

<sup>88</sup><https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22congress%22%3A118%7D>, 'Legislation Search', E.T: 30 Ekim 2023.

Oyun ii eřya ticareti konusunda, birok oyun řirketi kullanıcılarını bu tr ticaretten kaınmaları konusunda uyarır. Ancak, bu uyarılara raėmen, oyun ii eřya ticareti, "gri pazar"<sup>89</sup> olarak adlandırılan alanlarda yaygın bir řekilde devam etmektedir. Bu lkelerdeki geliřmelere ek olarak, Trkiye'nin de dijital mlkiyet hakları konusunda yasal dzenlemeler yapması gerektiėi aıktır. Anayasa, mlkiyet hakkının sınırlarını izme yetkisini yasama organına tevdi etmiř olmakla birlikte, bu yetkinin kullanımı sırasında, mlkiyet hakkının temel erevesini ve sınırlarını belirleyen Anayasal hkmlere sadık kalınması zorunluluėu, kanun koyucunun bu alandaki dzenlemelerinde Anayasa'nın ngrdėu temel ilkelerle uyumlu bir yol izlemesini kaınılmaz kılmaktadır.<sup>90</sup> evrimii oyun hesaplarının deėeri ve mlkiyet kavramı, hukuk, teknoloji ve etik arasında karmařık bir dengeyi temsil etmektedir. Oyun řirketleri, oyuncuların hakları ve kendi iř modelleri arasında denge kurarken, dijital mlkiyet zerindeki tartıřmaların devam edeceėi kesindir. Bu nedenle hem yasal hem de teknolojik zmlerin bu alandaki zorlukları ve fırsatları dikkate alarak geliřtirilmesi gerekmektedir.

Dijital mlkiyetin tanımlanması ve korunmasına dair nerdiėimiz kanun teklifleri, aėdař hukuk normlarına uygun bir yaklařım sergilemektedir. Ancak, bu tekliflerin daha kapsamlı bir hukuki ereveye oturtulabilmesi iin bazı hususların detaylandırılması ve geniřletilmesi elzemdir. İlk olarak, "dijital mlkiyet" teriminin hukuki tanımının dahada somutlařtırılması gerekmektedir. Dijital eserler, sanal paralar, oyun ii varlıklar gibi ok geniř bir yelpazeyi kapsayan bu mlkiyet kavramının, hukuki bir erevede neyi ifade ettiėinin net bir řekilde sınırlarının izilmesi gerekmektedir. Bu baėlamda, dijital mlkiyetin somutlařtırılması iin dijital eserler, sanal paralar ve oyun ii varlıkların ayrı ayrı tanımlanması nem arz etmektedir. Dijital eserler, dijital ortamda oluřturulan ve depolanan her trl sanatsal, edebi veya bilimsel alıřmayı kapsamaktadır. Sanal paralar, evrimii platformlarda kullanılan, gerek para birimiyle satın alınabilen veya deėiřtirilebilen dijital para birimlerini ifade eder. Oyun ii varlıklar ise video oyunlarında kazanılan veya satın alınan, karakterlerin glenmesini veya oyun deneyiminin zenginleřmesini saėlayan eřyalar, karakterler veya diėer dijital gelerdir. Bu unsurların her biri iin ayrı ayrı

---

<sup>89</sup>Ceylan ve Kse, a.g.e., s. 2.

<sup>90</sup>řimřek, a.g.e., s. 188.

hukuki tanımlar ve koruma mekanizmaları geliştirilmelidir. Böylece, dijital mülkiyetin kapsamı ve sınırları net bir şekilde belirlenerek, yasal düzenlemeler daha etkin ve uygulanabilir hale getirilebilir.

Dijital ürünlerin ve servislerin çoğu, kullanıcılara lisans aracılığıyla sunulmaktadır. Bu lisansların hukuki mahiyeti, dijital mülkiyet haklarının tanımı ve sınırları üzerinde belirleyici bir rol oynamaktadır. Bu sebeple, dijital mülkiyet haklarının düzenlenmesi sırasında, bu lisansların hukuki statüsüne dair açık ve net bir çerçevenin de sunulması gerekmektedir. Dijital mülkiyetin korunmasının yanı sıra, bireylerin dijital alanda sahip olduğu kişisel veri güvenliği de oldukça kritik bir konudur. Bu, bireylerin temel hak ve özgürlüklerine dair gizlilik haklarının korunması anlamına gelmektedir. Bu nedenle, dijital mülkiyet haklarına dair düzenlemelerde, gizlilik haklarıyla dijital mülkiyet hakları arasında bir denge kurulması zorunludur.

Ayrıca Alman Federal Mahkemesi'nin özellikle Facebook üzerine verdiği kararlar, dijital mirasın intikali konusunda çığır açıcı niteliktedir. Bu kararlar, miras bırakanın sosyal medya hesapları ve bu hesapların içerdiği kişisel verilerin mirasçılara geçişini düzenlemekte; bu geçişin, miras hukukunun genel prensipleri ışığında, miras bırakanın özel hayatının gizliliği ile diğer kişilerin haklarını koruyacak şekilde nasıl gerçekleşmesi gerektiği konusunda yol gösterici olmaktadır. Öte yandan, Türk hukukuna dair yorumlar ve karşılaştırmalar, mevcut yasal çerçevenin dijital miras gibi yeni ve karmaşık konuları yeterince adreslemediğini ortaya koymaktadır. Çalışmam Türk Medeni Kanunu'nda dijital mirasın açıkça tanımlanmamasının yarattığı hukuki boşlukları ve bu boşlukların pratikteki yansımalarını değerlendirmekte, dijital mirasın hukuksal tanımı ve düzenlemesi konusunda reform ihtiyacını vurgulamaktadır.<sup>91</sup>

Dijitalleşen dünya düzeninde, hukuki çerçevelerin de bu yeni gerçeklikler karşısında evrilmesi ve güncellenmesi gerekmektedir; bu çalışma da dijital mirasın hukuki düzenlemeler

deki yerini belirleme ve gelecekteki yasal reformlar için bir temel oluşturma amacı gütmektedir. Özellikle Türk Medeni Kanunu kapsamında dijital mirasın nasıl ele alınması gerektiği ve yasal düzenlemelerin dijitalleşme sürecine nasıl uyum

---

<sup>91</sup>Ç. İleri, 'Dijital Miras' - Alman Federal Mahkemesi'nin 'Facebook' Kararı Üzerine Bir İnceleme', *TBB Dergisi*, sayı: 146, 2020, s. 137-150.

sağlayabileceği üzerinde durulmuş, Türk hukuk düzeninin bu yeni ve önemli meseleye cevap vermesi gerektiği sonucuna varılmıştır.

Sonuç olarak uluslararası alanda, dijital mülkiyetin korunmasına dair bir standartlaşma ve iş birliği ihtiyacı da bulunmaktadır. Dijital alandaki sınırsız etkileşimler göz önüne alındığında, dijital mülkiyet haklarına dair uyumsuzlukların çözümü için uluslararası hukuki mekanizmaların oluşturulması gerekmektedir. Dijital mülkiyetin hukuka aykırı bir biçimde ihlal edilmesi ya da zarara uğratılması durumunda, bu zararın tespiti ve tazmini konularında da standart bir hukuki yaklaşımın benimsenmesi şarttır. Bu hem maddi hem de manevi zararların adil bir şekilde tazmin edilmesini sağlayacaktır.

### **2.2.1. Klasik Mülkiyet Hakkı Kavramından Farklılıkları**

Tarih boyunca mülkiyet hakkı, somut fiziksel varlıkların sahipliği ile özdeşleşmiştir. Topraklar, binalar, araçlar gibi elle tutulur, gözle görülür varlıklar, mülkiyet hakkının temelini oluştururken, bu haklar bireylerin bu varlıkları kontrol etme, satma, kiraya verme veya miras bırakma gibi yetkilerini içermekteydi. Ancak, dijital çağın yükselişi ile birlikte, mülkiyet hakkı kavramı önemli bir evrim geçirmiştir. Bu evrim, özellikle çevrimiçi oyunlar, dijital varlıklar ve sanal ürünler gibi yeni mülkiyet biçimlerinin ortaya çıkışıyla belirginleşmiştir. Dijital mülkiyet, geleneksel mülkiyet anlayışından önemli ölçüde farklılık göstermektedir. Çevrimiçi oyun hesapları, sanal dünyalar ve dijital içerikler, fiziksel varlıkların aksine, somut olmayan ve sıklıkla kopyalanabilir niteliklere sahiptir. Bu yeni mülkiyet türü, kullanıcıların genellikle sınırlı ve şartlı haklarla bu varlıkları kullanmasını içerir. Örneğin, bir oyuncu çevrimiçi bir oyun içinde karakter satın alabilir, ancak bu karakter üzerindeki kontrolü ve sahipliği, oyun şirketinin belirlediği kurallar ve kullanıcı sözleşmeleri tarafından belirlenir. Bu durum, dijital mülkiyet haklarının anlamını ve kapsamını yeniden düşünmeyi gerektirir. Anayasa Mahkemesi ve benzeri yüksek yargı organları, mülkiyet hakkının bu yeni biçimini nasıl ele alacakları konusunda önemli bir dönemeçte bulunmaktadır. Geleneksel olarak, mülkiyet hakkı fiziksel varlıklarla sınırlı olarak görülse de dijital çağda bu sınırların genişletilmesi zorunlu hale gelmiştir. Mahkemeler, dijital varlıkların ekonomik değerinin ve toplumsal etkisinin farkında

olarak, bu yeni mülkiyet türünün yasal tanımını ve korunmasını nasıl şekillendirecekleri konusunda kararlar vermeye başlamıştır.<sup>92</sup> Bu yeni mülkiyet biçiminin hukuki çerçevesi, bir dizi zorluğu beraberinde getirmektedir. Dijital mülkiyetin temelinde yatan 'sahip olunan şey' kavramı, fiziksel olmayan ve sıklıkla kopyalanabilir nitelikleri nedeniyle, geleneksel mülkiyet hukuku ilkeleriyle tam bir uyum içinde değildir. Dijital varlıkların sahipliği ve kontrolü, genellikle lisans anlaşmaları ve kullanıcı sözleşmeleri<sup>93</sup> ile düzenlenmektedir. Bu durum, kullanıcıların dijital varlıklar üzerinde tam bir kontrol ve serbestlik sahibi olmadıklarını göstermektedir. Örneğin, bir kullanıcının çevrimiçi oyun içinde kazandığı veya satın aldığı bir eşya, oyun şirketinin politikalarına tabi olabilir ve bu eşyanın kullanımı, devri veya satışı belirli kısıtlamalar içerebilir.<sup>94</sup>

Dijital mülkiyetin bu özellikleri, hukukçuları ve yasa koyucuları, mevcut mülkiyet hukuku çerçevesini yeniden değerlendirmeye ve dijital çağın gerekliliklerine uyum sağlamaya zorlamaktadır. Dijital varlıkların mülkiyet haklarının tanımı, korunması ve ihlallerinin cezalandırılması, ulusal ve uluslararası hukuk alanında yeni düzenlemelerin yapılmasını gerektirmektedir. Bu sadece bireysel kullanıcıların haklarını korumakla kalmayıp, aynı zamanda dijital ekonominin sağlıklı ve adil bir şekilde büyümesini de destekleyecektir. Bu bağlamda, dijital mülkiyetin hukuki statüsünün netleştirilmesi, bu alanda faaliyet gösteren şirketler, kullanıcılar ve hukuk profesyonelleri için büyük önem taşımaktadır. Dijital mülkiyet haklarının açıkça tanımlanması, bu varlıkların nasıl kullanılabilceği, devredilebileceği veya satılabileceği konusunda rehberlik sağlayacaktır. Ayrıca, dijital mülkiyetin ihlali durumunda uygulanacak yasal süreçler ve cezai yaptırımların belirlenmesi, dijital dünyada hukuki güvenliği ve istikrarı artıracaktır. Bu hem bireylerin dijital varlıklarını korumak hem de dijital mülkiyetin kötüye kullanılmasını önlemek açısından kritik bir adımdır. Teknolojik gelişmeler, bilginin kopyalanmasını ve dağıtımını önceki dönemlere kıyasla çok daha hızlı ve kolay hale getirirken, bu sürecin sonucunda ortaya

---

<sup>92</sup>H. Egeli, 'Türk Anayasa Hukukunda Mülkiyet Hakkının Kullanımının Durdurulması', *Liberal Düşünce Dergisi*, cilt: 27, sayı: 105, 2022, s. 223-236.

<sup>93</sup><https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, 'The Importance Of The End-User License Agreement', E.T: 02 Ocak 2024.

<sup>94</sup>M. C. Kirova, 'Fikir ve Sanat Eserleri Kanunu'nda Manevi, Mali veya Bağlantılı Haklara Tecavüz Suçu', Yüksek Lisans Tezi, *Antalya Bilim Üniversitesi Lisansüstü Eğitim Enstitüsü*, Antalya, 2023.

çıkan eserlerin orijinal mi yoksa kopya mı olduğu konusunda belirsizlikler yaratmaktadır. Bu durum hem eser sahiplerinin hem de kullanıcıların haklarını koruma konusunda yeni sorunlara yol açmaktadır. Geleneksel telif hukuku, dijital eserlerin özelliklerini ve dağıtım kanallarını yeterince yansıtamamakta ve bu nedenle güncellenmesi gerekmektedir. Eser sahipleri, yaratımlarını yanlış kullanımlardan korumak ve emeklerinin karşılığını almak istemekte, ancak mevcut yasalar teknolojinin getirdiği zorluklara tam olarak cevap verememektedir. Ayrıca, dijital bilginin mülkiyeti konusunda sadece yazarlar ve yayıncılar değil, kütüphaneler gibi bilgi hizmeti sağlayan kurumlar da önemli rol oynamakta ve bu alanda cevaplanması gereken birçok soru bulunmaktadır. Dijital mülkiyetin hukuki tanımı, geleneksel mülkiyet anlayışının ötesine geçen ve dijital varlıkların somut olmayan doğasını, kopyalanabilir özelliklerini ve bu varlıklar üzerindeki hakların nasıl edinildiğini, kullanıldığını ve devredildiğini dikkate alan yeni bir yaklaşımı gerektirmektedir. Bu, dijital mülkiyet haklarının sınırlarını daha net bir şekilde belirlememize ve kullanıcıların bu varlıklar üzerindeki haklarını daha iyi anlamamıza yardımcı olacaktır. Böylece, teknolojik gelişmelerin sunduğu fırsatlar en iyi şekilde değerlendirilirken, eser sahiplerinin hakları da korunabilecektir. Bu bağlamda, uluslararası iş birliği ve düzenlemelerin önemi artmaktadır. Telif hakkı ihlalleri artık ulusal değil, uluslararası bir problem olarak ele alınmalıdır. Ülkeler arası güven inşası ve iş birliği, dijital çağda mülkiyet haklarının korunması için kritik öneme sahiptir. Amerikan Kongre Kütüphanesi gibi kurumların dijital eserleri koleksiyonlarına eklemeleri ve bunları geniş bir kullanıcı kitlesine sunmaları, "adil kullanım" ve "eğitimsel amaçlı kullanım" hakları çerçevesinde değerlendirilmeli ve bu süreçte eser sahiplerinin hakları dikkate alınmalıdır. Sonuç olarak, dijital mülkiyetin hukuki çerçevesinin geliştirilmesi hem eser sahiplerinin haklarını koruyacak hem de teknolojinin sunduğu imkanlardan en geniş kullanıcı kitlesinin faydalanmasını sağlayacak şekilde olmalıdır. Bu, sadece yasaların güncellenmesiyle değil, aynı zamanda bilgi ve teknoloji politikalarının, eğitim sistemlerinin ve toplumsal farkındalığın artırılmasıyla mümkün olacaktır.<sup>95</sup>

Dijital mülkiyet hakkının temelinde yatan '*sahip olunan şey*' kavramı, dijital çağda yeniden yorumlanmalıdır. Fiziksel mülkiyetin aksine, dijital mülkiyet genellikle

---

<sup>95</sup>Y. Ünal ve N. Selçuk, 'Elektronik Bilgi Kaynakları İçin Entelektüel Mülkiyet ve Dijital İçerik Hakları, Düzenleme ve Dijital Ödeme Sistemleri', *Bilgi Dünyası*, cilt: 1, sayı: 1, 2000, s. 180-191.

lisans anlaşmaları ve kullanıcı sözleşmeleri<sup>96</sup> ile sınırlandırılmıştır. Bu kullanıcının dijital varlıkları '*sahip olma*' yerine '*kullanma*' hakkına sahip olduğu anlamına gelir. Örneğin, bir müzik dosyasını indirmek veya bir çevrimiçi oyun içinde karakter satın almak, kullanıcıya bu varlıkların sınırsız kontrolünü veya sahipliğini vermez. Kullanıcılar, genellikle bu varlıkları yalnızca belirli şartlar altında kullanabilir ve bu haklar, dijital varlığın yaratıcısı veya sahibi tarafından belirlenen kurallara tabidir.<sup>97</sup> Bu sınırlamalar dijital mülkiyetin ticaretini ve devrini karmaşıklaştırmaktadır. Dijital varlıkların satışı ve transferi, genellikle yaratıcılarının veya hizmet sağlayıcılarının politikalarına bağlıdır. Bu politikalar genellikle kullanıcıların bu varlıkları satmalarını, değiştirmelerini veya başkalarına devretmelerini kısıtlar veya yasaklar. Bu durum, dijital mülkiyetin klasik mülkiyetten önemli bir farkı olarak ortaya çıkmaktadır. Klasik mülkiyet hukuku, mülkiyetin devredilebilirliğini ve ticaretini temel bir hak olarak kabul ederken, dijital mülkiyet bu konuda daha sınırlı bir yaklaşım sergilemektedir.<sup>98</sup> Bu nedenle, dijital mülkiyetin hukuki çerçevesinin oluşturulması, kullanıcı haklarını ve dijital ekonominin gerekliliklerini dengeli bir şekilde ele almalıdır. Dijital mülkiyet haklarının korunması, kullanıcıların bu varlıkları adil ve makul şartlar altında kullanmalarını sağlamalıdır. Aynı zamanda, dijital mülkiyetin yaratıcılarının ve sahiplerinin hakları da korunmalıdır. Bu, dijital içerik üreticilerinin yaratıcı çabalarını ve yatırımlarını teşvik ederken, aynı zamanda kullanıcıların bu içeriklere erişimini ve kullanımını adil bir şekilde düzenlemeyi gerektirir.

Dijital mülkiyetin hukuki çerçevesinin oluşturulmasında uluslararası iş birliği ve standartların belirlenmesi de büyük önem taşımaktadır. Dijital varlıkların sınırsız doğası ve küresel erişimi, ulusal sınırların ötesinde etkileşimlere yol açmaktadır. Bu, dijital mülkiyet haklarının korunması ve ihlallerinin cezalandırılması konusunda

---

<sup>96</sup>Ü. Özgüven Ceylan ve Ş. Eroğlu, 'Elektronik Kaynaklarda Telif Hakkı ve Lisans Sözleşmeleri Üzerine Bir Değerlendirme: Bartın Üniversitesi Örneği', *Bilgi Yönetimi Dergisi*, cilt: 6, sayı: 2, 2023, s. 197-216.

<sup>97</sup>'Kullanma Hakkı. İşbu EULA'nın hüküm ve koşullarına tam olarak uymanız koşuluyla ve bunlara tam olarak uyduğunuzda lisans veren size, geçerli siparişte belirtilen süre (süre belirtilmemişse yazılıma daima kullanabilirsiniz) boyunca yazılımı kullanmanız için kişisel, münhasır olmayan bir lisans verir.', Dell EULA Sözleşmesi, s. 1.

<sup>98</sup>'Şirket işbu Sözleşme ile Kullanıcıya münhasır olmayan, geri çağırılabilir, devredilemez, alt lisanslamaya konu olmayan bir sınırlı lisans ve My.Games Ekosistemini ticari olmayan, kişisel amaçlar için kullanma hakkı tanımaktadır.', My.Games EULA Sözleşmesi, s. 4.

uluslararası düzeyde uyumlu yasal düzenlemelerin<sup>99</sup> geliştirilmesini zorunlu kılmaktadır. Uluslararası standartlar, dijital mülkiyetin ticareti ve transferi konusunda rehberlik sağlayacak ve bu alandaki yasal belirsizlikleri azaltacaktır.

Dijital mülkiyetin hukuki korunması, modern hukukun karşılaştığı en büyük meydan okumalardan biridir. Dijital varlıkların doğası, geleneksel hukuki çerçeveleri zorlar ve bu alanda yenilikçi yaklaşımların geliştirilmesini gerektirir. Dijital mülkiyet haklarının korunması, yalnızca kullanıcıların ve yaratıcıların haklarını güvence altına almakla kalmaz, aynı zamanda dijital ekonominin bütünlüğünü ve güvenilirliğini de destekler. Yenilikçi hukuki yaklaşımlar, dijital mülkiyetin özgün niteliklerini dikkate almalıdır. Örneğin, dijital içeriklerin kopyalana bilirliliği ve çoğaltıla bilirliliği, telif hakları ve 5846 sayılı kanun ile fikri mülkiyet yasalarının yeniden düşünülmesini zorunlu kılar. Bu, dijital içerik üreticilerinin haklarının korunmasını sağlarken, aynı zamanda bu içeriklerin geniş kitleler tarafından erişilebilir ve kullanılabilir olmasını dengelemeyi amaçlamalıdır. Dijital mülkiyet haklarının korunması, yaratıcıların ve yatırımcıların çabalarını teşvik ederken, aynı zamanda kullanıcıların bu varlıkları etkili ve adil bir şekilde kullanmalarını sağlamalıdır. Dijital mülkiyetin hukuki korunmasında, lisans anlaşmaları ve kullanıcı sözleşmeleri<sup>100</sup> önemli bir rol oynamaktadır. Bu anlaşmalar, dijital varlıkların kullanımını düzenler ve kullanıcıların haklarını ve sorumluluklarını belirler. Ancak, bu anlaşmaların adil ve makul olması, tüketicilerin haklarını korumak için hayati önem taşır. Hukuk sistemleri, kullanıcıları aşırı kısıtlayıcı veya adil olmayan sözleşme şartlarından korumak için düzenlemeler yapmalıdır. Bu, 6502 sayılı kanun ile tüketici haklarının korunmasını sağlarken, aynı zamanda dijital içerik sağlayıcılarına karşı adil bir rekabet ortamı oluşturur.

İnternetin yükselişi ve dijitalleşmenin hızlanması, bilgi toplumunda fikri mülkiyet hakları ve yaratıcılık üzerinde önemli etkiler yaratmıştır. Bir yandan, fikri mülkiyet haklarının bireylerin yaratıcılığını ve bilginin serbest dolaşımını sınırladığı eleştirileriyle, diğer yandan yeni medya araçlarının klasik fikri mülkiyet kavramının sınırlarını aştığı kabulüyle, bu dönem karakterize edilmiştir. İnternet, eserlerin çoğaltılması, dağıtılması ve işlenmesini kolaylaştırırken, sayısal ortamda kopyalama

<sup>99</sup>[chromeextension://efaidnbmninnibpcapjpcglclefindmkaj/https://afyonluoglu.org/PublicWebFiles/cyber/legislation/2001Avrupa%20Birli%C4%9Fi%20Siber%20Su%C3%A7lar%20S%C3%B6zle%C5%9Fmesi-TR.pdf](https://chromeextension://efaidnbmninnibpcapjpcglclefindmkaj/https://afyonluoglu.org/PublicWebFiles/cyber/legislation/2001Avrupa%20Birli%C4%9Fi%20Siber%20Su%C3%A7lar%20S%C3%B6zle%C5%9Fmesi-TR.pdf), 'Avrupa Birliği Siber Suçlar Sözleşmesi - Budapeşte Sözleşmesi', E.T: 30 Ekim 2023.

<sup>100</sup><https://www.dell.com/eula>, 'Son Kullanıcı Lisans Sözleşmesi (EULA)', E.T: 30 Ekim 2023.

ve paylaşım, asıl ile kopya arasındaki farkı neredeyse ortadan kaldırmıştır. Ancak, İnternetin geniş ve kontrolsüz bir mecra oluşu, hak ihlallerinin tespiti ve önlenmesini zorlaştıran anonimlik gibi özelliklerle doludur. Bu bağlamda, siber güvenliğin dijital mülkiyetin korunmasındaki kritik rolü, yaratıcılar ve kullanıcılar arasında güven inşa ederek, siber saldırılara ve hırsızlığa karşı koruma sağlamayı amaçlamaktadır. Hukuk sistemlerinin, dijital mülkiyeti kötüye kullanımlara karşı koruyacak etkili yasalar ve düzenlemeler geliştirmesi zorunlu hale gelmiştir, bu da dijital ekonomi ve toplumun genel çıkarlarını koruyacak şekilde tasarlanmış yenilikçi yaklaşımlar ve düzenlemelerin büyük bir önem taşıdığını göstermektedir.<sup>101</sup>

Dijital mülkiyet hukukunun evrimi, teknoloji ile toplum arasındaki sürekli değişen etkileşimi yansıtan dinamik bir süreç olarak kendini göstermektedir. Gelecekte, dijital mülkiyet haklarının daha da karmaşıklaşması ve genişlemesi beklenirken, hukuk sistemlerinin adaptasyon ve yenilikçilik kapasitesi sınanacak, toplumsal normlar ve değerler üzerinde önemli etkiler yaratılacaktır. Blockchain teknolojisi ve kripto paralar gibi yeni teknolojik gelişmeler, dijital varlıkların sahipliği, ticareti ve güvenliği konusunda devrim yaratmaktadır. Bu gelişmeler, dijital varlıkların izlenebilirliğini artırırken, kullanıcılara daha fazla kontrol ve sahiplik hissi kazandırma potansiyeline sahiptir, ancak hukukun bu yeni teknolojileri nasıl düzenleyeceği ve koruyacağı konusunda yeni zorlukları da beraberinde getirir. Bu nedenle, hukuk sistemlerinin dijital mülkiyeti koruma stratejilerini sürekli olarak yeniden değerlendirmesi ve güncellemesi, teknolojinin hızlı evrimine uyum sağlama kapasitesinin bir göstergesidir. Esnek ve dinamik yasaların oluşturulması, dijital dünyanın bütünlüğünü ve kullanıcıların haklarını koruyacak şekilde tasarlanmalıdır. Bu sadece bir yasal zorunluluk değil, aynı zamanda toplumsal bir sorumluluktur. Dijital mülkiyetin korunması, yaratıcılığı teşvik etmenin yanı sıra, dijital ekonomi ve toplumun sağlıklı bir şekilde gelişimini destekleyen temel bir unsurdur, hukukun bu alandaki yeniliklerle uyum içinde evrimleşmesi toplumun bütünlüklü bir dijital geleceğe doğru ilerlemesinin temel taşlarından biridir.

---

<sup>101</sup>D. Doğan ve G. Özocak, 'Dijital Oyunlar, Multimedya Yaratımlar ve Güncel Hukuki Problemler', *Özocak Blog*, Haziran 2013, [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://ozocak.com/Dosyalar/88cd5f.pdf](http://ozocak.com/Dosyalar/88cd5f.pdf), E.T: 22 Şubat 2024.

Dijital içeriklerin geniş erişilebilirliği, bilgiye erişim ve ifade özgürlüğü gibi temel haklar üzerinde önemli etkiler yaratırken, bu hakların adil ve dengeli bir şekilde korunması hem toplumun kültürel zenginliğini artırmakta hem de yaratıcılık ile yeniliği teşvik etmektedir. Bu denge, yaratıcıların ve içerik üreticilerinin haklarının korunmasını sağlayacak yasal düzenlemelerin güncellenmesi ve geliştirilmesi, aynı zamanda hukuk eğitimi ve uygulamasının bu yeni gerçekliklere uyum sağlaması gerektiğini vurgulamaktadır.<sup>102</sup>

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun eser sahipliği ile ilgili maddeleri günümüzde dijital ortamlarda giderek daha fazla önem kazanan çevrimiçi oyun hesapları ve karakterlerinin korunması konusunda önemli bir temel teşkil etmektedir. Özellikle bilgisayar oyunları gibi multimedya ürünleri söz konusu olduğunda eserlerin birleşimi ve dijitalleştirilmesi süreci eser sahipliği kavramını daha karmaşık hale getirmektedir. Bu eserler sadece metin, görsel ya da ses unsurlarının bir araya getirilmesinden ibaret olmayıp, bu bileşenlerin etkileşimli ve dinamik bir şekilde entegre edilmesiyle kendine özgü bir bütünlük kazanmaktadır. Eser sahipliği üzerine tartışmalar özellikle multimedya kategorisinde değerlendirilen çevrimiçi oyunların her bir bileşenin tek başına birer eser olarak kabul edilemeyeceği ancak birlikte yarattıkları sinerji ile yeni ve özgün bir eser ortaya çıkardıkları fikri üzerine yoğunlaşmaktadır. Bu durum multimedya oluşumların kendi içlerinde barındırdıkları her bir unsurdan bağımsız olarak yeni bir eser olarak değerlendirilmesi gerektiğini vurgulamaktadır. Sinema eserleri için de geçerli olan bu durum, eser unsurlarının birleşiminden doğan yeni bir değer yaratma sürecine işaret etmektedir.<sup>103</sup> Bu bağlamda, çevrimiçi oyunlar gibi dijital platformlarda yaratılan multimedya eserlerin korunması, sadece içerik üreticileri ve hak sahipleri için değil, aynı zamanda tüketiciler için de büyük önem taşımaktadır. Bu eserlerin hukuki koruma altına alınması, yaratıcıların haklarının korunması ve eserlerin izinsiz kullanımına karşı etkin bir mücadele sağlaması açısından kritiktir. Ayrıca, dijitalleşme ve teknolojik gelişmelerin hızına uyum sağlayabilen bir hukuk sistemi, bu yeni eser türlerinin doğurduğu ihtiyaçları karşılayabilecek esneklikte olmalıdır. Bu yeni eser türlerinin yasal olarak tanınması ve

---

<sup>102</sup>M. E. Durmuş, 'Bilgisayar Oyunlarının Türk Hukukunda Korunması', Yüksek Lisans Tezi, *İstanbul Şehir Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2020.

<sup>103</sup>E. H. Uysal, 'Fikrî Mülkiyet Hukukunda Bilgisayar Oyunlarının Korunması', Yüksek Lisans Tezi, *Ankara Sosyal Bilimler Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2021.

korunması, yalnızca ulusal düzeyde değil, uluslararası hukuk çerçevesinde de ele alınmalıdır. Çünkü çevrimiçi oyunlar gibi multimedya ürünleri, genellikle küresel bir kullanıcı kitlesine hitap etmektedir. Bu nedenle, bu eserlerin korunması, uluslararası işbirliği ve uyumlu hukuk düzenlemelerini gerektirmektedir.

Sonuç olarak, multimedya eserlerin, özellikle de çevrimiçi oyunların hukuki korunması, modern hukukun önemli bir sorunu haline gelmiştir. Eser sahipliği ve telif hakları kavramlarının bu yeni eser türlerine uygun şekilde geliştirilmesi, hukuki uyumsuzlukların önlenmesi ve yaratıcı içeriklerin korunması için elzemdir. Bu, sadece mevcut yasaların güncellenmesiyle değil, aynı zamanda hukukçuların, yargı organlarının ve ilgili tüm tarafların bu yeni eser türlerini ve ortaya çıkardıkları özgün sorunları anlamaları ve bu yeni gerçekliklere uyum sağlamaları ile mümkün olacaktır.

### **2.3. Hesap Güvenliği Önlemleri ve Kullanıcı Sorumlulukları**

Çevrimiçi oyunlar son yıllarda özellikle gençler arasında popüler hale gelmiştir. Ancak bu popülerlik, oyun hesaplarının ve karakterlerinin ele geçirilmesi gibi riskleri de beraberinde getirmiştir. Bu bağlamda, hukukun bu yeni dijital mülkiyet formunu düzenlemesi ve koruması gerekmektedir. Özellikle Türk Hukuk Sistemi'nin, Anayasa madde 35'de mülkiyet kavramını, bir kişinin bir şeye karşı en geniş yetki ve tasarruf hakkını kullanma durumu olarak tanımladığı düşünüldüğünde, çevrimiçi oyun hesaplarının artık sadece eğlence değil, aynı zamanda önemli bir ekonomik değere sahip olan bir mülkiyet unsuru olarak kabul edilmektedir. Böyle bir ortamda, oyun içi eşya ve karakterlerinin değerini bilen kullanıcıların, bu değerlere uygun güvenlik önlemleri almaları kritik bir öneme sahiptir. Oyun içi eşya satışı ve takası yapılan platformlarda, kullanıcıların dikkatli olmaları ve bilinmeyen ya da şüpheli kişilerle ticaret yapmamaları önerilir. Aynı zamanda, oyun içi etkileşimlerde kişisel bilgilerin paylaşılmaması, hesap güvenliği için kritik bir önem taşır. Kullanıcıların, kendi güvenlik önlemlerini almakla ve bu önlemlere uymakla yükümlü oldukları unutulmamalıdır. Bu, güçlü parolalar oluşturmayı, iki faktörlü kimlik doğrulama kullanmayı, hesap bilgilerini güvende tutmayı ve güvence altına almayı içerir.<sup>104</sup> Öte

---

<sup>104</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

yandan, oyun şirketlerinin de bu konuda bir rolü vardır. Kullanıcı hesaplarını korumak için etkili güvenlik protokolleri ve politikalar geliştirmeli ve bunları uygulamalıdır. Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, modern bilişim suçlarının bir parçası olarak ortaya çıkmaktadır. Bu tür saldırılara karşı korunma için, kullanıcıların bilmeleri ve uygulamaları gereken bazı temel koruma yöntemleri bulunmaktadır:

### **2.3.1. Güçlü ve Benzersiz Parolalar Kullanma**

Çevrimiçi oyunlarda kullanıcı hesaplarının güvenliği, siber saldırganlara karşı korunmanın ilk adımı olarak, güçlü ve benzersiz parolaların kullanımını zorunlu kılar. Rakamlar, büyük ve küçük harfler ile özel karakterlerin dengeli bir kombinasyonundan oluşan karmaşık parolalar, basit ve tahmin edilebilir parolalara kıyasla çok daha güvenlidir. 'F1@zK3p\$' gibi bir parola, 'futbol123' gibi basit bir alternatifte göre siber tehditlere karşı önemli bir güvenlik katmanı ekler. Bu güvenlik önlemleri, kullanıcıların oyun içi varlıklarını ve kişisel bilgilerini korumada kritik bir rol oynar. Her oyun ve platform için farklı parolalar kullanmak ve bu parolaları düzenli olarak değiştirmek, güvenlik seviyesini artırırken, bir hesabın güvenliğinin ihlal edilmesi durumunda diğer hesapları koruma altına alır.<sup>105</sup>

Çevrimiçi oyun platformları ve geliştiricileri, kullanıcıları parola güvenliği konusunda bilinçlendirmek ve eğitmek için önemli bir sorumluluğa sahiptir. Bu, sadece güçlü parolalar oluşturma konusunda değil, aynı zamanda bu parolaları koruma ve yönetme konusunda da kullanıcıları donanımlı hale getirir. Güvenlik risklerini azaltma ve kullanıcıların oyun deneyimlerini daha güvenli bir hale getirme çabası, bireysel ve kolektif bir gayreti temsil eder. Bu çabaların birleşimi, siber güvenlik tehditlerine karşı daha dirençli bir kullanıcı topluluğu oluşturarak, çevrimiçi oyunların keyfini güven içinde çıkarmayı mümkün kılar.

---

<sup>105</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

### 2.3.2. İki Faktörlü Kimlik Doğrulama

Çevrimiçi oyun platformlarında, iki faktörlü kimlik doğrulama (2FA) yöntemi, kullanıcı hesaplarını korumak için hayati bir güvenlik katmanı olarak öne çıkmaktadır; bu yöntem, kullanıcıların kimliklerini, genellikle bir parola ve bir doğrulama kodu olmak üzere iki farklı faktörün kombinasyonunu kullanarak onaylamalarını gerektirir, bu da tek faktörlü kimlik doğrulama sistemlerine kıyasla önemli ölçüde daha yüksek bir güvenlik düzeyi sağlar.<sup>106</sup> Türkiye'de internet kullanıcılarının büyük bir kısmının parolalarını nadiren değiştirdiği göz önüne alındığında, 2FA'nın desteklendiği uygulamalar ve platformlar üzerindeki kullanımının teşvik edilmesi, hesap güvenliğini önemli ölçüde artırarak kullanıcıların dijital varlıklarını korumalarına yardımcı olacaktır.

### 2.3.3. Phishing Saldırılarına Karşı Dikkatli Olma

İnternetin derinlemesine entegrasyonu ve çevrimiçi oyun platformlarının popülerliği, kullanıcı hesaplarının güvenliğini daha da önemli hale getirmiştir. Bu bağlamda, iki faktörlü kimlik doğrulama (2FA) yöntemi, kullanıcı kimliklerini doğrulamak için bir parola ve bir doğrulama kodu olmak üzere iki ayrı faktör gerektiren güçlü bir güvenlik katmanı sunar. Bu yöntem, tek faktörlü kimlik doğrulama sistemlerine kıyasla önemli ölçüde daha yüksek bir güvenlik düzeyi sağlar. Özellikle Türkiye'de kullanıcıların parolalarını nadiren değiştirmesi ve basit parolalar kullanma eğilimi göz önüne alındığında, 2FA'nın benimsenmesi, kullanıcıların dijital varlıklarını siber saldırılara karşı korumada kritik bir önem taşımaktadır.<sup>107</sup>

2FA'nın önemi, sadece kullanıcıların güvenlik alışkanlıklarını güçlendirmekle kalmayıp, aynı zamanda siber saldırganların hesaplara erişimini zorlaştırarak bir ek koruma katmanı sunmasıyla da vurgulanmaktadır. Doğrulama kodları, genellikle kullanıcının mobil cihazına gönderilir, bu da saldırganın hem parolayı hem de geçici doğrulama kodunu ele geçirmesini gerektirir, saldırı başarısını önemli ölçüde azaltır. Bu nedenle, 2FA'nın teşvik edilmesi ve yaygınlaştırılması, siber güvenliği artırmanın

<sup>106</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

<sup>107</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

yanı sıra, kullanıcıların çevrimiçi ortamda kendilerini daha güvende hissetmelerini sağlayan bir adımdır.

#### 2.3.4. Güvenlik Yazılımları Kullanma

Çevrimiçi oyun ekosistemi, günümüz dijital çağının en popüler ve etkileşimli platformlarından biri olarak ön plana çıkmaktadır. Bu sanal dünyalar, oyunculara sadece eğlence sunmakla kalmayıp, aynı zamanda sosyal etkileşim, rekabet ve hatta ekonomik kazanç fırsatları da sağlar. Ancak, bu sanal ortamların sunduğu fırsatlar, kötü niyetli bireyler için de cazip hedefler haline gelmiştir. Siber suçlular, oyuncuların kişisel bilgilerini, oyun içi varlıklarını ve hatta finansal bilgilerini hedef alarak, zararlı yazılımlar ve phishing (oltalama) saldırıları aracılığıyla dolandırıcılık yapmaktadır. Bu nedenle, çevrimiçi oyun dünyasında güvenilir antivirüs ve anti-malware<sup>108</sup> programlarının kullanımı, kullanıcıların dijital güvenliğini sağlamada hayati bir öneme sahiptir. Güvenilir güvenlik yazılımlarının etkin kullanımı, sadece zararlı yazılımlara karşı bir savunma hattı oluşturmakla kalmaz, aynı zamanda kullanıcıların dijital varlıklarını koruyarak güvenli bir oyun deneyimi sunar. Her gün binlerce yeni kötü amaçlı yazılımın ortaya çıkması, bu yazılımların sürekli güncellenmesini ve düzenli taramalar yapılmasını zorunlu kılar. Güncellemeler, yeni tehditlere karşı korumayı sağlarken, düzenli taramalar, herhangi bir zararlı yazılımın sistemde bulunup bulunmadığını kontrol eder. Bu süreçler, kullanıcıların kişisel bilgilerinin yanı sıra oyun içi varlıklarının korunmasına katkıda bulunur.<sup>109</sup>

Güvenlik yazılımlarının proaktif kullanımı, çevrimiçi oyunlarda güvenli bir deneyim için temel bir gerekliliktir. Bu, sadece bireysel kullanıcılar için değil, oyun geliştiricileri ve platform sağlayıcıları için de geçerlidir. Geliştiriciler, oyunlarını tasarlarken ve güncellerken güvenlik önlemlerini entegre etmeli, platform sağlayıcıları ise kullanıcıların güvenliğini sağlamak için sürekli olarak güvenlik yazılımlarını güncellemeli ve desteklemelidir. Çevrimiçi oyun dünyasında güvenliğin sağlanması, yalnızca güçlü şifreler ve iki faktörlü kimlik doğrulama gibi temel güvenlik

---

<sup>108</sup>S. Çakır ve M. Kesler, 'Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımları', *Akademik Bilişim 12 - XIV. Akademik Bilişim Konferansı Bildirileri*, Uşak, 1-3 Şubat 2012, s. 472.

<sup>109</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

önlemleriyle sınırlı değildir. Güvenilir antivirüs ve anti-malware programlarının kullanımı, bu güvenlik önlemlerinin önemli bir tamamlayıcısı olarak, kullanıcıların ve oyun platformlarının, siber tehditlere karşı etkili bir şekilde korunmasını sağlar. Bu nedenle, her oyuncunun ve platform sağlayıcının, dijital güvenliği ciddiye alması ve gerekli tüm önlemleri proaktif bir şekilde uygulaması gerekmektedir. Bu kapsamlı yaklaşım, çevrimiçi oyun dünyasını, kötü niyetli faaliyetlere karşı daha güvenli bir hale getirecek ve tüm kullanıcıların güven içinde oyun oynamasını sağlayacaktır.

### **2.3.5. Açık Ağlarda Oyuna Giriş Yapmaktan Kaçınma**

Çevrimiçi oyun dünyasında güvenliğin korunması, siber tehditlerin her geçen gün arttığı bu dijital çağda, kullanıcıların öncelikli sorumlulukları arasında yer almaktadır. Özellikle halka açık Wi-Fi gibi güvensiz ağlarda oyun oynarken, kişisel verilerin korunması ve izinsiz erişimlerin önlenmesi, sadece bir tercih değil, zorunluluk haline gelmiştir. Bu bağlamda, VPN (Sanal Özel Ağ)<sup>110</sup> kullanımı, bağlantının şifrelenmesi yoluyla güvenlik seviyesini artırır, böylece kullanıcıların çevrimiçi faaliyetleri sırasında karşılaşılabilecekleri riskler minimize edilir. VPN teknolojisi, kullanıcıların internet trafiğini güvenli bir tünel içinden geçirerek, meraklı gözlerden korunmasını sağlar ve böylece, özellikle hassas bilgilerin halka açık ağlar üzerinde transferi sırasında, siber saldırılara karşı bir kalkan görevi görür.

Diğer yandan, evde veya halka açık alanlarda kullanılan Wi-Fi ağlarının güvenliğinin sağlanması da büyük önem taşır. Güçlü şifreleme protokolleri ve güvenli ağ ayarlarının kullanımı, izinsiz erişimleri büyük ölçüde engeller ve veri hırsızlığı riskini azaltır. Kullanıcılar, ağ ayarlarında gerekli güvenlik önlemlerini alarak, cihazlarının ve verilerinin korunmasını sağlayabilirler. Bu kapsamda, özellikle halka açık ağlarda, güvenilirlikten emin olunamayan bağlantı noktalarından kaçınmak, dijital kimlik ve kişisel verilerin korunması açısından kritik bir öneme sahiptir. Sonuç olarak, VPN kullanımının yanı sıra, evde ve halka açık alanlarda güvenli Wi-Fi ağlarına bağlanmak, kullanıcıların dijital dünyada güven içinde gezinmelerini sağlar

---

<sup>110</sup>N. Aydoğdu, ‘Sanal Özel Ağ (VPN) Bağlantı Mantığı (VPN Teknolojisi) ve TOKEN Güvenliğinin PİN Kodu ile Arttırılması’, Yüksek Lisans Tezi, *Beykent Üniversitesi Fen Bilimleri Enstitüsü*, İstanbul, 2014.

ve siber tehditlere karşı etkili bir savunma mekanizması oluşturur.<sup>111</sup> Bu stratejiler, siber güvenliğin sağlanmasında hayati rol oynar ve kullanıcıların çevrimiçi varlıklarını korumalarına yardımcı olur, böylece onlara güvenli ve keyifli bir oyun deneyimi sunar.

### 2.3.6. Oyun İçi İletişime Dikkat Edinme

Çevrimiçi oyunlarda, oyun içi sohbetlerde veya forumlarda kişisel bilgilerin paylaşılması, sosyal mühendislik saldırıları için potansiyel bir zemin oluşturabilir; bu tür saldırılar, sahte kimlikler ve manipülasyon teknikleri kullanarak kişileri aldatmayı ve hassas bilgilere erişmeyi amaçlar, bu nedenle kullanıcı adları, parolalar ve diğer kişisel bilgilerin korunması, hesap güvenliğinin temel bir unsuru olarak ön plana çıkar.<sup>112</sup> Bu koruma yöntemleri, çevrimiçi oyun hesaplarınızı ve karakterlerinizi potansiyel tehditlere karşı korumanın temel yollarıdır. Ancak, çevrimiçi oyunlarda siber güvenlikte bir süreçtir ve yeni tehditlere karşı tetikte olmak, koruma stratejilerinizi güncel tutmak için kritik bir öneme sahiptir.

Çevrimiçi oyun hesapları ve karakterlerin güvenliği, günümüzde sadece teknolojik bir zorluk değil, aynı zamanda hukuki bir mesele haline gelmiştir. Çevrimiçi oyun ortamlarında, kullanıcıların kişisel verilerinin yetkisiz kişilerce ele geçirilmesi, oyun içi varlıkların yitirilmesinin ötesinde, kişisel verilerin ifşa edilmesi riskini de beraberinde getirir; bu durum, kullanıcıların yeterli güvenlik önlemlerine uymamaları halinde, dijital kayıpların yanı sıra hukuki yaptırımlara da maruz kalabilecekleri bir ortamı ortaya çıkarır.<sup>113</sup> Hukuki perspektiften bakıldığında, hesap güvenliğine dikkat edilmemesi durumunda, kullanıcının kişisel veri ihlali nedeniyle tazminat talep etme hakkı olabilir. Ancak, birçok oyun hizmet sağlayıcısı, kullanıcı sözleşmelerinde, hesap güvenliğiyle ilgili sorumluluğun büyük ölçüde kullanıcıya ait olduğunu belirtir. Bu nedenle, kullanıcılar, güvenlik önlemlerini ihmal ederek hesaplarına erişim sağlanmasına izin verirlerse, oyun şirketleri bu tür kayıplar için sorumlu tutulmayabilir.

---

<sup>111</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

<sup>112</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

<sup>113</sup>H. Sınar, 'Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)', *Kişisel Verileri Koruma Dergisi*, cilt: 2, sayı: 1, 2020, s. 47.

5651 sayılı Kanun kapsamında, internet ortamında sunulan çeşitli hizmetlerin düzenlenmesi ve bu hizmetler yoluyla işlenen suçlarla mücadele edilmesi amaçlanmaktadır. Bu çerçevede, internet aktörleri; içerik, yer, erişim sağlayıcılar ve toplu kullanım sağlayıcılar, belirli sorumluluklar altına alınmışlardır. Kanunun getirdiği düzenlemeler, internet ortamında işlenen suçlarla etkin bir şekilde mücadele edilmesi ve bireylerin haklarının korunması hedeflenmektedir. Özellikle, internet üzerinden erişilen içeriklerin kontrolü ve denetimi noktasında, 5651 sayılı Kanun'un önemi büyüktür. İnternet ortamında yayınlanan içeriklerin suç unsuru taşıması veya bireylerin haklarını ihlal etmesi durumunda, erişimin engellenmesi, içeriğin kaldırılması gibi hukuki yollar sunulmaktadır. Bu süreçler, bireylerin şikayet ve ihbarlarını temel alarak işletilmekte ve bu şekilde kullanıcıların internet ortamında güvenliği artırılmaktadır.<sup>114</sup>

Ayrıca, eğer bir kullanıcı, hesabının güvenliğini ihmal ederek başka bir kullanıcının zarar görmesine neden olursa, zarar gören kullanıcı, zararını tazmin etmek için hukuki yollara başvurabilir. Bu, özellikle oyun içi varlıkların veya hesapların haksız yere transfer edilmesi gibi durumlarda geçerli olabilir. Oyun hesaplarının güvenliği ihmal edildiğinde, kullanıcının sadece oyun içindeki değerli varlıklarını kaybetmesiyle sınırlı kalmaz. Oyun hesapları genellikle e-posta adresleri, kredi kartı bilgileri ve diğer kişisel bilgilerle ilişkilidir. Bu nedenle, hesabın ele geçirilmesi, kişisel verilerin ifşa edilmesi veya kötüye kullanılması riskini de artırır. Bu tür bir veri ihlali, kullanıcıyı kimlik hırsızlığı, mali dolandırıcılık ve diğer bilişim suçlarına karşı savunmasız bırakabilir.

Çevrimiçi oyun hesaplarının güvenliğini sağlamak, sadece oyun içi varlıkları korumak için değil, aynı zamanda hukuki sorumlulukları ve potansiyel hukuki sonuçları önlemek için de hayati öneme sahiptir. Bu bağlamda, kullanıcıların, hesap güvenliği konusunda bilinçli ve proaktif olmaları hem dijital hem de hukuki riskleri en aza indirmek için kritik bir öneme sahiptir.

---

<sup>114</sup>chromeextension://efaidnbmnnnibpcajpcgglefindmkaj/https://www.guvenliweb.org.tr/dosya/nH58 Q.pdf, 'Bilgi Teknolojileri ve İnternetin Bilinçli, Güvenli Kullanımı', E.T: 24 Kasım 2023.

### 3. ÇEVİRİMİÇİ OYUN HESAPLARININ VE KARAKTERLERİNİN ELE GEÇİRİLMESİ: YÖNTEMLER VE MOTİVASYONLAR

Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, günümüzde siber suç dünyasının önemli bir boyutunu temsil etmektedir. Bu durumun hem teknik hem de motivasyonel boyutları vardır. Öncelikle, çeşitli yöntemlerle ele geçirilen bu hesaplardan, ekonomik bir kazanç elde edilebilir. Bununla birlikte, bu eylemler genellikle hukuksal anlamda karmaşıklıklar doğurmakta ve dünyanın farklı bölgelerinde farklı şekillerde ele alınmaktadır. Siber suçlular genellikle çeşitli teknikler kullanarak bir oyun hesabını ele geçirirler. Bu teknikler genellikle kullanıcının kimlik bilgilerini ele geçirmeyi hedefler. Phishing<sup>115</sup> saldırıları, kimlik avı, brute force<sup>116</sup> saldırıları ve keylogger<sup>117</sup> gibi zararlı yazılımlar bu teknikler arasında en yaygın olanlarıdır. Bu suçları işleyenlerin motivasyonları genellikle ekonomiktir. Çevrimiçi oyun hesapları ve karakterleri, oyun içi eşyalar ve diğer değerli varlıklar içerebilir. Bu varlıklar gerçek dünyada para karşılığı satılabilir. Dolayısıyla bir hesabı ele geçirmek, suçlulara hızlı ve kolay bir gelir kaynağı sağlayabilir. Türkiye ile Çin, Güney Kore ve ABD gibi batı ülkeleri arasında bu konuda çeşitli farklılıklar bulunmaktadır. Örneğin, Türkiye'de, çevrimiçi oyun hesaplarının ele geçirilmesi genellikle 5237 sayılı TCK'da "Bilişim Alanında Suçlar" başlığı altında toplanmıştır. Ancak çevrimiçi oyun hesaplarının çalınması konusu ile ilgili olarak özel bir açıklama bulunmamaktadır. Bununla birlikte, hukuki süreçler genellikle zaman alıcı ve karmaşıktır. Bu durum, suçluların cezasız kalmasına neden olabilmektedir. Bu suçların küresel doğası, yargılama ve cezalandırma sürecini karmaşık hale getirebilir. Özellikle, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi hem kullanıcıları hem de oyun şirketlerini doğrudan etkileyen karmaşık bir sorundur. Oyun şirketlerine de bu konuda büyük bir sorumluluk düşmektedir. Şirketler, kullanıcı hesaplarını güvence altına almak için güçlü güvenlik önlemleri almalı, kullanıcıları olası tehditlere karşı bilinçlendirmeli ve eğitmelidir. Ayrıca, hesap ele geçirme vakalarına karşı hızlı ve etkili bir yanıt verme kapasitesine sahip olmalıdırlar. Bu sayede, çevrimiçi oyun

<sup>115</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

<sup>116</sup>B. Erol, 'Ağ Trafik Özelliklerinin Analizini Yaparak Anormalliklerin Tespit Edilmesi', Yüksek Lisans Tezi, *İstanbul Aydın Üniversitesi Fen Bilimleri Enstitüsü*, İstanbul, 2019.

<sup>117</sup>M. Dama, 'Windows Fonksiyonları Kullanılarak Özgün Bir Casus Yazılım Tasarımı ve Alınabilecek Önlemler', Yüksek Lisans Tezi, *Gazi Üniversitesi Bilişim Enstitüsü*, Ankara, 2014.

dünyası daha güvenli bir yer haline gelebilir ve kullanıcılar, eğlencelerini endişe etmeksizin devam ettirebilirler.

### 3.1. Hesap Ele Geçirme Yöntemleri ve Teknikleri

Dijital çağın hızla ilerleyen akışında, çevrimiçi oyunlar sadece eğlence sektöründe değil, aynı zamanda kişisel kimlik, sosyal etkileşim ve ekonomik ilişkilerin kesişim noktasında önemli bir rol oynamaktadır. Çevrimiçi oyun<sup>118</sup> hesaplarının ve karakterlerinin güvenliği, bu çok katmanlı etkileşim ağında bireysel oyuncuların oyun şirketlerine dek geniş bir yelpazede aktörler için kritik bir önem arz etmektedir. Oyun hesaplarının ele geçirilmesi, ekonomik kayıpların yanı sıra, kişisel veri ihlalleri ve oyun içi sosyal etkileşimlerin bozulmasına kadar varan geniş çaplı olumsuz sonuçlara yol açabilmektedir. Bu tür saldırılar, çeşitlilik gösteren yöntemlerle gerçekleştirilebilir ve hukukun dijital sınırlar içerisinde etkin bir şekilde uygulanmasını zorunlu kılar.

Literatür kaynaklarına göre, çevrimiçi oyunlar ve onların destekleyici bileşenleri üzerinde gerçekleşen etkileşimler, temelde oyuncuları oyunlarla ya da oyuncuları birbirleriyle bağlantılandırmaktadır. Bu etkileşimler, oyuncuların diğer oyuncularla kurduğu sosyal ilişkiler ve bunların gerçek hayata yansımaları gibi farklı biçimlerde ortaya çıkabilmektedir. Oyuncular, oyun karakterleri ya da avatarlarını yaratırken, kendi kimlik ve benliklerini belirli oranlarda bu sanal varlıklara aktarmakta, hatta bazen yarattıkları karakterler, ulaşmak istedikleri ama gerçek hayatta ulaşamadıkları benlik ve kimliklerin bir yansıması olabilmektedir.<sup>119</sup> Ticari ilişkiler açısından ise, oyunlara yatırılan gerçek paralarla oyun paralarının satın alınması ya da oyun eşyalarının tüketilmesi gibi etkileşimler, oyun içi ile sınırlı kalmamakta, geliştirilen hesaplar belirli fiyatlara diğer oyunculara satılabilmekte ve böylece oyun eşyası, gerçek para, sanal para ve gerçek eşya arasında geniş bir etkileşim ağı oluşmaktadır.<sup>120</sup> Çevrimiçi oyun hesaplarının ele geçirilmesi ile ilgili olarak yöntemlerin birçoğuna ve bu yöntemlerin hukuki yönlerini inceleyeceğiz.

---

<sup>118</sup>A. B. Kaya, 'Çevrimiçi Oyun Bağımlılığı Ölçeğinin Geliştirilmesi: Geçerlik ve Güvenirlilik Çalışması', Yüksek Lisans Tezi, *Gaziosmanpaşa Üniversitesi Eğitim Bilimleri Enstitüsü*, Tokat, 2013.

<sup>119</sup>Fidan, a.g.e., s. 37.

<sup>120</sup>Fidan, a.g.e., s. 38.

### 3.1.1. Phishing (Oltalama) Yöntemi

Phishing ya da Türkçe karşılığıyla "Oltalama", siber suçluların sahte web siteleri oluşturarak kullanıcıları bu sitelere yönlendirip, kişisel bilgilerini ele geçirmeye çalıştığı bir siber saldırı yöntemidir.<sup>121</sup> Bu saldırılar genellikle e-posta, SMS veya sosyal medya yoluyla gerçekleştirilir. Kullanıcılara gönderilen mesajlarda genellikle acil eylem gerektiren bir durum olduğu belirtilir ve kullanıcının belirtilen sahte siteye giriş yapması istenir.<sup>122</sup>

Phishing saldırıları, birçok ülkede "Bilişim Sistemine İlişkin Suçlar" başlığı altında değerlendirilir. Türkiye'de ise TCK madde 243 ile bilişim sistemine girme suçuyla düzenlerken; TCK madde 244 ile bilişim sisteminden veri hırsızlığını düzenlemektedir. Phishing saldırıları, bu maddeler kapsamında değerlendirilebilir. Ayrıca 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında, kişisel verilerin izinsiz toplanması ve işlenmesi suç sayılmaktadır. Phishing saldırıları sonucu ele geçirilen kişisel verilerin izinsiz olarak toplanması, bu kanun kapsamında ciddi yaptırımlarla karşılaşabilir.

Phishing saldırıları, siber güvenlik dünyasında sürekli gelişen ve evrilen bir tehdit olarak karşımıza çıkmaktadır. Bu tür saldırıların hukuki boyutları hem bireylerin hem de kurumların haklarını koruma altına almayı amaçlamaktadır. Ancak, en etkili korunma yöntemi, kullanıcıların bu tür tehditlere karşı bilinçlenmesi ve eğitilmesidir.

### 3.1.2. Keylogging ( Keylogger ) Yöntemi

Keylogging ya da diğer adıyla "Keylogger", kullanıcının bilgisayarına ya da mobil cihazına yüklenen ve klavye tuş vuruşlarını kaydeden yazılımlardır.<sup>123</sup> Bu yazılımlar, kullanıcının şifrelerini, banka bilgilerini, kişisel mesajlarını ve diğer özel bilgilerini ele geçirebilir. Keyloggerlar genellikle kötü amaçlı yazılımlar, virüsler veya truva atları aracılığıyla cihazlara bulaşır. Keylogging eylemi, birçok ülkede "Özel Hayatın Gizliliğinin İhlali" suçu kapsamında değerlendirilir. Türkiye'de 5237 sayılı

---

<sup>121</sup>Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.

<sup>122</sup>Ş. Ahi, 'Gelişmiş Sosyal Mühendislik Saldırıları Analizi ve Tespiti', Yüksek Lisans Tezi, *Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü*, Gebze, 2020.

<sup>123</sup>Dama, a.g.e., s. 16.

TCK madde 134 ile kişisel verilerin hukuka aykırı olarak kaydedilmesini suç olarak tanımlamaktadır. Aynı kanunun 134/2. maddesi ise bu verilerin yayılmasını suç olarak kabul eder. Keylogger yazılımları aracılığıyla elde edilen bilgilerin kaydedilmesi ve yayılması, bu maddeler kapsamında değerlendirilebilir. Ayrıca, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında, kişisel verilerin izinsiz toplanması ve işlenmesi suç sayılmaktadır. Keylogger yazılımları aracılığıyla elde edilen kişisel verilerin izinsiz olarak toplanması, bu kanun kapsamında ciddi yaptırımlarla karşılaşabilir.

Özellikle güvenlik yazılımlarının düzenli olarak güncellenmesi, şüpheli e-posta eklerinin açılmaması ve bilinmeyen kaynaklardan yazılım indirilmemesi gibi basit önlemler, keylogger saldırılarına karşı koruma sağlar.<sup>124</sup>

### 3.1.3. Çevrimiçi Oyunlarda Hesap Paylaşımı Yöntemi

Çevrimiçi oyunlarda hesap paylaşımı, bir kullanıcının oyun hesabının kullanıcı adı, şifresi ve diğer erişim bilgilerini başka bir kullanıcıyla paylaşması eylemidir. Bu paylaşım, genellikle oyun içi avantaj elde etmek, belirli bir seviyeye ulaşmak ya da oyun içi eşyaları transfer etmek amacıyla yapılır. Ancak, bu tür bir paylaşım, hesabın ele geçirilmesi riskini beraberinde getirir.

Çoğu çevrimiçi oyunun Kullanıcı Sözleşmesi veya Hizmet Şartlarında, hesap bilgilerinin üçüncü şahıslarla paylaşılması yönünde hükümler bulunmaktadır.<sup>125</sup> Bu tür bir paylaşımın gerçekleşmesi durumunda, söz konusu sözleşme hükümlerine aykırı hareket edilmiş olur. Bu aykırılık, hesabın askıya alınması, banlanması veya diğer yaptırımların uygulanmasına neden olabilir. Hesap paylaşımı sonucu kişisel verilerin izinsiz olarak üçüncü şahıslarla paylaşılması, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında suç teşkil edebilir. Bu durumda, veri sorumlusu olan oyun şirketi KVKK'nın ikinci bölüm, kişisel verilerin işlenmesi ile ilgili maddeleri gereğince yaptırımlarla karşılaşabilir.

<sup>124</sup>G. Canbek, 'Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme', Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2005.

<sup>125</sup>[chromeextension://efaidnbmnnnnibpcjpcglclefindmkaj/https://i.dell.com/sites/csdocuments/Legal\\_Docs/en/DellEULA\\_English.pdf](chromeextension://efaidnbmnnnnibpcjpcglclefindmkaj/https://i.dell.com/sites/csdocuments/Legal_Docs/en/DellEULA_English.pdf), 'EULA Sözleşmesi', E.T: 01 Kasım 2023.

Oyun şirketlerinin, kullanıcılarına sundukları Kullanıcı Sözleşmesi veya Hizmet Şartlarında hesap paylaşımı ile ilgili maddeleri açık ve anlaşılır bir şekilde belirtmeleri, hukuki bir yükümlülüktür.<sup>126</sup> Ayrıca, kişisel verilerin korunması konusunda da gerekli önlemleri almak ve bu önlemleri kullanıcılara bildirmek, şirketlerin hukuki yükümlülükleri arasındadır.

#### 3.1.4. Güvenlik Açıkları Yöntemi

Çevrimiçi oyunlarda güvenlik zafiyetleri, bilgisayar yazılımları veya ağ sistemlerindeki korunmasız bölümleri ifade eder. Bu zafiyetler, siber suçluların sistemlere yetkisiz erişim elde etmesine ve zarar verici faaliyetlerde bulunmasına olanak tanır.<sup>127</sup> Özellikle çevrimiçi oyun platformlarında, bu tür zafiyetlerin tespit edilmesi, kullanıcı hesaplarının tehlikeye girmesine sebep olabilir. Siber saldırganlar, bu güvenlik açıklarından faydalananarak, oyun içi varlıkları çalabilir, hesap bilgilerini değiştirebilir ya da kullanıcıların kişisel verilerine ulaşabilirler. Bilişim sistemlerine izinsiz müdahale, pek çok ülkede yasalarla düzenlenmiş bir suçtur. Örneğin, Türkiye'de 5237 sayılı TCK madde 243 bilişim sistemlerine yetkisiz erişimi suç olarak nitelendirmekte ve yaptırımlar öngörmektedir. Bu çerçevede, bir çevrimiçi oyun hesabına yetkisiz erişim elde etmek, yukarıda bahsi geçen yasal düzenlemelere tabi tutulabilir. Siber güvenlik zafiyetleri konusunda rol alan temel paydaşlar; yazılım geliştiricileri, sızıntıları keşfeden güvenlik araştırmacıları, zafiyetleri alım satım yapan piyasalar, son kullanıcılar, güvenlik ihlallerini raporlayan medya organları ve düzenleyici otoriteler olarak sıralanabilir.<sup>128</sup>

#### 3.1.5. Çevrimiçi Oyunlarda Sosyal Mühendislik Yöntemi

Sosyal mühendislik, teknolojik becerilere dayanmayan, insanların duygusal ve sosyal zayıflıklarını hedef alan bir dolandırıcılık tekniğidir ve bu yöntem, bireyleri

---

<sup>126</sup><https://www.resmigazete.gov.tr/eskiler/2022/12/20221229-5.html>, 'Elektronik Ticaret Aracı Hizmet Sağlayıcı ve Elektronik Ticaret Hizmet Sağlayıcılar Hakkında Yönetmelik Resmî Gazete Sayı: 32058', E.T: 31 Ekim 2023.

<sup>127</sup>O. Bozoklu ve C. Z. Çil, 'Yazılım Güvenlik Açığı Ekosistemi ve Türkiye'deki Durum Değerlendirmesi', *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, cilt: 3, sayı: 1, 2017, s. 7.

<sup>128</sup>Bozoklu ve Çil, a.g.e., s. 8

aldatarak manipüle etmek için psikolojik etkileme taktiklerini kullanır.<sup>129</sup> Çevrimiçi oyun platformlarında, sosyal mühendislik sıkça karşılaşılan bir saldırı biçimi olup, kullanıcıları değerli oyun içi varlıklarını paylaşmaya, kişisel hesap bilgilerini ifşa etmeye ya da zararlı yazılımları bilgisayarlarına yüklemeye ikna etmek için kullanılır. Bu saldırılar genellikle, kendilerini oyunun destek personeli olarak tanıtan dolandırıcılar, dostluk teklifleri veya cazip ödüller vaat ederek gerçekleştirilir.

Bilgisayar ve ağ güvenliği perspektifinden bakıldığında, sosyal mühendislik, güvenlik mekanizmalarını etkisiz kılarak kullanıcıların veya sistem yöneticilerinin ayrıcalıklarına sızma stratejisidir. Bu yaklaşım, insan psikolojisini ve davranış biçimlerini, güvenlik sistemlerindeki zafiyetler olarak görür ve bu zafiyetleri sömürmeyi hedefler. Sosyal mühendislik saldırıları, etki altına alma, zorlama, yanıltıcı ilişkiler kurma ve hedef kişilerin sorumluluk, etik, dürüstlük veya sadakat duygularını sarsma gibi çeşitli manipülatif yöntemler içerir.<sup>130</sup> Bu yöntemlerin amacı, hedef kişileri gizli bilgileri ifşa etmeye veya yetkisiz erişim sağlamaya yönlendirmektir.

### **3.1.6. Brute Force (Kaba Kuvvet) Saldırıları Yöntemi**

Brute force saldırısı, deneme-yanılma yöntemiyle kullanıcı hesaplarına erişim sağlama girişimini ifade eder ve bu yöntem, bir hacker'ın, çeşitli şifre kombinasyonlarını sistematik bir şekilde deneyerek bir kullanıcının hesabına girmesini amaçlar.<sup>131</sup> Brute force veya Kaba Kuvvet saldırıları, özellikle güçlü olmayan şifrelerle korunan hesaplar üzerinde etkili olabilir ve genellikle otomatize edilmiş yazılımlar yardımıyla kısa sürede sayısız kombinasyon test edilir. Bu tip bir saldırı, pek çok ülkedeki yasalar altında "Bilişim Sistemine İlişkin Suçlar" kategorisinde ele alınır. Örneğin, Türkiye'deki 5237 sayılı TCK madde 243, bilişim sistemlerine yetkisiz erişimi açıkça suç saymaktadır. Dolayısıyla, brute force yöntemiyle bir hesaba izinsiz erişim sağlamak, söz konusu mevzuat kapsamında yargılanabilir bir suçtur.

<sup>129</sup>N. Yalçın ve A. Avşar, "Sosyal Mühendislik Atakları ve Alınması Gereken Önlemler", 20. Akademik Bilişim 2018 Konferansı Bildirileri, Malatya, 1-3 Şubat 2018, s. 77.

<sup>130</sup> Yalçın ve Avşar, a.g.e., s. 77.

<sup>131</sup>Erol, a.g.e., s.32.

Brute Force Attack, Türkçede Kaba Kuvvet Saldırıları olarak bilinir ve temel olarak, kimlik doğrulama mekanizmalarında kullanılan kullanıcı adı ve şifre değerlerini belirlenmiş potansiyel sınırlar içerisindeki tüm olası karakter, uzunluk ve çeşitleri üzerinde denemeler yaparak gerçekleştirilir.<sup>132</sup> Bu saldırı türü, önceden belirlenmiş bir aralıkta sistematik bir yaklaşımla tüm mümkün kombinasyonları deneyerek doğru erişim bilgilerini bulmayı amaçlar.

### 3.1.7. Denial of Service (Hizmet Dışı Bırakma) Saldırıları Yöntemi

Denial of Service (DoS) saldırısı, bir bilgisayar sisteminin ya da ağ servisinin işlevsiz hale getirilmesi amacıyla yapılan zararlı bir girişimdir. Bu tür saldırılar, hedeflenen sisteme ya da ağa muazzam miktarda trafik ya da bilgi yükleyerek gerçekleştirilir, böylece bu sistemlerin normal hizmet verme kapasiteleri aşılır ve geçici ya da kalıcı olarak kullanılamaz hale getirilir. Söz konusu saldırıların odak noktası, genellikle internete bağlı hizmetlerin sağlandığı ana bilgisayarlar ve ilgili ağ kaynaklarıdır.<sup>133</sup> Bu tür bir saldırı sonucu, sistemlerin hizmet dışı kalması nedeniyle, etkilenen işletme veya bireyler önemli iş ve gelir kayıpları yaşayabilirler, ayrıca itibarlarında ciddi zararlar meydana gelebilir.

Denial of Service saldırıları, bilgisayar suçları kapsamında değerlendirilmekte ve birçok ülkede yasal yaptırımlara tabi tutulmaktadır. Örneğin, Türkiye hukuk sistemi içerisinde, 5237 sayılı TCK madde 244, bilgi sistemlerinin işleyişini kasıtlı olarak bozan ya da engelleyen eylemleri suç olarak tanımlamakta ve bu tür saldırılar bu çerçevede cezai yaptırımlara maruz kalmaktadır. Bu nedenle, DoS saldırılarına maruz kalan işletmeler ve bireyler, mevcut hukuki yollara başvurarak, haklarını arayabilirler. Diğer taraftan, bu tür siber saldırılara karşı etkin önlemler almak da büyük önem arz etmektedir. İşletmeler, ağ trafiğini sürekli izleyerek anormal aktiviteleri tespit etmek, aşırı yüklenmeye karşı koruma sağlamak, yedek sunucu sistemleri kurmak ve dağıtık ağ yapıları oluşturmak gibi stratejilerle kendilerini koruyabilirler. Aynı zamanda, kullanıcı sözleşmelerinde ve hizmet şartlarında bu tür saldırılara karşı alınan önlemleri

---

<sup>132</sup>İ. Kara, 'Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi', *Sakarya University Journal Of Computer And Information Sciences*, cilt: 2, sayı: 2, 2019, s. 62.

<sup>133</sup>E. Masum, 'Dağıtık Servis Dışı Bırakma Saldırılarının İncelenmesi ve Korunma Yöntemleri', Yüksek Lisans Tezi, *Ankara Üniversitesi Sağlık Bilimleri Enstitüsü*, Ankara, 2017.

ve kullanıcı haklarını net bir şekilde belirtmeleri, hem hukuki açıdan korunaklı olmalarını sağlar hem de kullanıcılarına karşı şeffaflığı temin eder.

### 3.1.8. Çoklu Hesap Kullanımı (Multi-Accounting) Yöntemi

Çoklu Hesap Kullanımı ya da Multi-Accounting, bir oyuncunun birden fazla hesap oluşturarak oyun içinde avantaj elde etmeye çalıştığı bir yöntemdir. Bu, özellikle rekabetçi oyunlarda diğer oyunculara karşı haksız bir avantaj sağlamak, belirli ödülleri birden fazla kez kazanmak veya oyunun ekonomik dengesini bozmak amacıyla yapılır.

Çoğu online oyunun Kullanıcı Sözleşmesi veya Hizmet Şartları<sup>134</sup>, çoklu hesap kullanımını yasaklar. Bu tür bir eylem, sözleşmeye aykırılık teşkil eder ve oyuncunun hesaplarının askıya alınmasına veya kalıcı olarak banlanmasına (banned)<sup>135</sup> neden olabilir. Ayrıca, eğer bu eylem sonucunda oyuncu maddi bir kazanç elde ederse, bu durum TCK madde 158/1/f ile dolandırıcılık suçu kapsamında değerlendirilebilir. Oyun şirketleri, çoklu hesap kullanımını tespit etmek ve önlemek için çeşitli teknolojik araçlar ve yöntemler kullanabilirler. Bu tür bir eylemin tespit edilmesi durumunda, şirketin hukuki yollara başvurma hakkı bulunmaktadır.

Yukarıda tüm tehlikeli yöntemleri ile belirtildiği üzere çevrimiçi oyun platformları, teknolojinin sunduğu sınırsız imkanlarla birlikte, bireyler için sosyal, ekonomik ve eğlenceli bir alan oluşturmaktadır. Fakat bu alandaki büyüme, oyun hesaplarının ele geçirilmesi gibi güvenlik sorunlarına ve hukuki meydan okumalara da yol açmıştır. Özellikle oyun hesaplarının güvenliği, bireysel oyuncuların ve oyun şirketlerinin en öncelikli meselelerinden biri haline gelmiştir. Bu durum, hukukun bu alanda nasıl bir rol üstlenmesi gerektiği sorusunu beraberinde getirmiştir. Bireysel oyuncuların hakları ve oyun şirketlerinin sorumlulukları, hukuki normlar ve standartlarla belirlenmelidir. Ancak bu sorunun çözümü, yalnızca ulusal bir perspektifte değil, küresel bir yaklaşımla ele alınmalıdır. Çünkü çevrimiçi oyunlar, ulusal sınırların ötesinde bir etkileşim ve etki yaratmaktadır. Bu bağlamda, hukukun temel amacı, sadece suçları tanımlamak ve cezalandırmak değil, aynı zamanda

<sup>134</sup>[https://documentation.my.games/terms/mygames\\_tou](https://documentation.my.games/terms/mygames_tou), 'My Games EULA Sözleşmesi.', E.T: 16 Kasım 2023

<sup>135</sup><https://www.playstation.com/tr-tr/support/account/suspensions-psn/>, 'Hesap Askıya Almalar ve Yasaklamalar', PlayStation, E.T: 31 Ekim 2023.

çevrimiçi oyun deneyiminin adil, güvenli ve keyifli olmasını sağlamaktır. Hukukçuların ve oyun şirketlerinin, bu alandaki tehditlere karşı etkili koruma stratejileri geliştirmesi ve bu tehditleri anlaması kritik bir öneme sahiptir. Çevrimiçi oyunlarla ilgili hukuki düzenlemelerin, teknolojik gelişmelere ve yeni saldırı yöntemlerine hızla adapte olması gerekmektedir. Bu hem bireylerin haklarını koruyacak hem de oyun şirketlerinin sorumluluklarını yerine getirmelerini sağlayacak bir yaklaşımın benimsenmesini zorunlu kılmaktadır.

### 3.2. Saldırganların Motivasyonları ve Hedefleri

Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi siber suçların, şimdilik çok üzerine düşülmeyen bir alt başlığı olarak karşımıza çıkar. Bu eylemin arkasında olduğundan ilk dem vurabileceğimiz motivasyon ekonomik kazançtır. Saldırgan bu kazancı oyun içi varlıkları satma veya gerçek para birimleriyle değiştirme yoluyla elde etmeyi hedefler. Bu eylem adil oyun ilkesini bozmakla kalmayıp ayrıca, oyun içi alımların da dengesini bozar. Uzun vadede oyunu diğer oyuncular tarafından da kullanılamaz hale getirebilir. İkincil ve daha fazla karşılaşıldığı için tehlikeliliği diğer ihlallere göre daha çok anlaşılmış olan motivasyon ise, kişisel verilerin ihlali, saldırganların çevrimiçi oyun hesaplarındaki hassas bilgilere erişerek kimlik hırsızlığı yapması veya bu bilgileri satmasıdır.

Finansal sıkıntılar, bir saldırganın hayatında önemli bir etken olabilir ve bu tür maddi zorluklar, suç işlemeye iten finansal bir motivasyon kaynağı haline gelebilir. Örneğin, bilgi karşılığında verilen rüşvet, bir başka şirkette iş teklifi almak veya maddi bir rekabet avantajı sağlamak gibi faktörler, finansal motivasyonun somut örneklerindendir. Makroekonomik koşulların kötüleşmesi, aşırı borçlanma veya maddi hırs gibi faktörler, kuruluşların içindeki bireylerin davranışlarını etkileme potansiyeline sahiptir. Öte yandan, politik motivasyonlar, bir devlete veya kuruma zarar verme, korku ve tedirginlik yaratma, başka bir devlet veya şirket adına casusluk yapma gibi hedefleri içerebilir.<sup>136</sup> Kişisel motivasyonlar ise saldırganların bireysel

---

<sup>136</sup>H. İ. Ulus ve M. Demirci, 'Kurum İçi Saldırıların Tespiti ve Önlenmesi için Sunucu İzleme Uygulaması', *Gazi Üniversitesi Fen Bilimleri Dergisi*, cilt: 6, sayı: 3, 2018, s. 511.

hırslarını, bilgiye olan susuzluklarını veya adaletsizlik algıları sonucunda ortaya çıkan intikam alma arzularını kapsar.

Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi gibi saldırılar çeşitli motivasyon ve amaçları içerebilir ve bu faktörlerin anlaşılması, etkili bir hukuki ve güvenlik stratejisi geliştirmede kritik önem taşır. Kimi saldırganlar, bireysel zevklerini tatmin etmek veya başkalarını rahatsız etmek amacıyla hesapları ele geçirebilir. Bu tip saldırganlar sıklıkla "troller"<sup>137</sup> olarak anılır ve genellikle psikolojik tatmin peşinde koşarlar.

Çevrimiçi oyun hesaplarının ele geçirilmesi konusu, hukuki bir bakış açısından ele alındığında, önemli bir motivasyon ve hedef çeşitliliği sunar. Bu suçlar, bir oyun hesabının değerini anlamak ve manipüle etmek için genellikle teknik yetenek ve spesifik bilgi gerektirir. Bu suçlar maddi kazanç, kişisel zevk veya hatta sosyal statü kazanma motivasyonlarına dayanabilir. Suçlular genellikle kıymetli hesapları hedef alır, ancak zaman zaman yalnızca kişisel bir anlaşmazlığı çözme veya bir rakibi alt etme motivasyonu ile hareket ederler.

Siber suçlarla mücadelede öncelikle bu suçların işlenmesinin önlenmesi, işlenmeleri halinde failerin tespiti ve cezalandırılması, mağdurun eski hale getirilmesi amaçlanmaktadır. Bir başka önemli olan konu da oyun geliştiricileri ile platform sağlayıcıları için güvenlik standartlarının belirlenmesi olmalıdır. Çevrimiçi oyun hesaplarının ele geçirilmesi, rekabet avantajı sağlama amacıyla gerçekleştirilen eylemlerden, ekonomik kazançla yönelik suçlara evrilmiştir. Bu durum, siber güvenlik ve hukuk alanında önemli konuları gündeme getirirken, bireysel oyuncuların yanı sıra genel toplum güvenliği için de ciddi tehditler oluşturmaktadır.<sup>138</sup> İlgili konuların daha ayrıntılı incelemesi detaylı bir şekilde aşağıda ele alınmıştır.

---

<sup>137</sup>B. Mercimek, N. D. Yaman, A. Kelek ve H. F. Odabaşı, 'Dijital Dünyanın Yeni Gerçeği: Troller', *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, cilt 6, sayı 1, 2016, s. 67-77.

<sup>138</sup>D. Şenol ve E. B. Karataşoğlu, 'Siber Suçlara Sosyolojik Bakış', *Academic Social Resources*, cilt: 7, sayı: 33, 2022, s. 44.

### 3.2.1. Ekonomik Kazanç: Oyun İçi Varlıklar ve Para Aklama

Çevrimiçi oyunlar, dijital dünyanın en etkileyici ve karlı alanlarından biri haline gelmiştir. Bu platformlar, oyun içi varlıklar ve sanal para birimleri üzerinden ciddi bir ekonomik döngü yaratmıştır. Ancak, bu döngü aynı zamanda, yasadışı faaliyetlerden elde edilen gelirlerin aklanması için de bir fırsat sunmaktadır. Bu durum, hukuki açıdan ciddi sorunları beraberinde getirmekte ve uluslararası hukuk düzeninin yeni mücadele alanlarından birini oluşturmaktadır.

Masum bir bilgisayar oyunu olarak görünen araç, aslen kara paranın aklanması son derece kolaylaştıran bir faaliyete dönüşme tehlikesini bünyesinde barındırmaktadır. İlk olarak, yasadışı gelirler, oyun içi varlıklar veya sanal para birimleri çevrimiçi oyunlar aracılığıyla sistem içerisine dahil edilebilir. Bu süreç, yasadışı gelirlerin kaynağının gizlenmesi ve oyun içi ekonomiye yerleştirilmesi anlamına gelir. Oyun içi alımlar, genellikle düşük düzeyde finansal denetimlere tabi olduğundan, yasadışı gelirlerin sisteme sızdırılması için ideal bir yol oluşturur. İkinci aşama, bu gelirlerin çeşitli işlemler aracılığıyla ayrıştırılmasıdır. Çevrimiçi oyunlar, global bir kullanıcı kitlesine sahip olduğundan, bu platformlar üzerinden yapılan transferler, uluslararası sınırları kolayca aşabilir ve izlerini kaybettirebilir. Oyun içi varlıkların satışı, takas edilmesi veya farklı oyunlara transfer edilmesi, bu gelirlerin izini bulanıklaştıran bir yöntemdir. Son aşama olan bütünleştirme ise, yasadışı gelirlerin oyun içi veya dışı yasal ekonomik faaliyetlerle karıştırılması sürecidir. Bu aşamada, oyun içi kazançlar gerçek dünya ekonomisine transfer edilir ve yasadışı gelirlerin kökeni daha da gizlenir. Örneğin, bir oyuncu yüksek miktarlarda oyun içi para kazandığını iddia ederek, bu gelirleri yasal bir işletmenin geliri gibi gösterebilir.<sup>139</sup>

Bu süreçler, oyuncuların oyun içinde gerçek veya oyun parası kullanarak eşya ve avantajlar satın alıp satabildiği oyun içi alım-satım işlemleri yoluyla şekillenen ekonomileri etkilemekle kalmaz; aynı zamanda finansal suçlarla mücadelede uluslararası hukuk düzeninin karşılaştığı zorlukları da artırır. Bu, oyun ekonomilerinin oyun dışı gerçek para ekonomileriyle olan etkileşimi nedeniyle oluşan çeşitli hukuki ve düzenleyici sorunları beraberinde getirir.

---

<sup>139</sup>E. Gürel ve Ç. Şahin, "Dijital Dünyada Kara Para Aklama: Örnek Olaylar", *Üçüncü Sektör Sosyal Ekonomi Dergisi*, cilt: 57, sayı: 3, 2022, s. 2289-2305.

Mevcut finansal düzenlemeler, dijital oyun dünyasının hızlı değişimine ve karmaşıklığına uyum sağlamakta zorlanmaktadır. Dolayısıyla, çevrimiçi oyunlar üzerinden gerçekleştirilen para aklama faaliyetleri hem ulusal hem de uluslararası hukuk düzenleyicileri için yeni stratejiler ve düzenlemeler geliştirmeyi gerektirir. Bu bağlamda, çevrimiçi oyun platformları ve oyun içi ekonomiler, yasadışı faaliyetlerin izini sürmek ve önlemek için daha sıkı düzenlemelere tabi tutulmalıdır. Danimarka polislerinin çevrimiçi oyunlarda kurduğu özel bir ekip, zorbalıkla mücadele ederek güvenli bir ortam yaratmayı hedeflemektedir. Bu ekip, oyun içinde aktif olarak faaliyet göstererek, kötü niyetli davranışları tespit etme ve önleme konusunda önemli bir rol oynamaktadır. Bu uygulama, çevrimiçi ortamlarda güvenliği artırma çabalarında çığır açan bir adım olarak değerlendirilmektedir.<sup>140</sup> Oyun geliştiricileri ve platform işletmecileri, finansal suçlarla mücadelede aktif rol almalı ve kullanıcılarının işlemlerini daha yakından izlemelidir. Bu hem oyun ekosistemlerinin sağlığını korumak hem de genel finansal güvenliği sağlamak adına kritik bir öneme sahiptir.<sup>141</sup> Çevrimiçi oyunlar ve oyun içi ekonomiler, modern dünyanın vazgeçilmez bir parçası haline gelmiştir. Ancak, bu yeni ekonomik alanların, para aklama gibi yasadışı faaliyetlere karşı daha etkin bir şekilde korunması gerekmektedir. Bu, sadece oyun sektörünün değil, tüm toplumun finansal güvenliğini sağlamak adına elzem bir adımdır.

### 3.2.2. Kişisel Verilerin İhlali ve Kimlik Hırsızlığı

Çevrimiçi oyunlar sadece gençlerin değil, her yaştan bireyin ilgisini çeken bir eğlence biçimi haline gelmiştir. Bu platformlar, oyunculara sanal dünyalarda etkileşim kurma ve maceralara atılma olanağı sunarken, aynı zamanda kişisel veri güvenliği açısından önemli riskler taşımaktadır. İşte bu sebeple, çevrimiçi oyunlar ve bu oyunların kişisel veri güvenliği üzerindeki etkilerini detaylıca incelemek gerekmektedir.

---

<sup>140</sup><https://www.merlininkazani.com/polisler-de-oyun-oynar-hatta-yayin-bile-acar-haber-123470>,

‘Polisler de Oyun Oynar, Hatta Yayın Bile Açır’, E.T: 12 Nisan 2024.

<sup>141</sup>Gürel ve Şahin, a.g.e., s. 2297.

Öncelikle, çevrimiçi oyunlarda kişisel veri güvenliğinin neden önemli olduğunu anlamak gerekmektedir. Kullanıcılar, oyun içinde genellikle gerçek isimleri, e-posta adresleri, ödeme bilgileri gibi hassas bilgilerini paylaşır. Bu bilgilerin kötü niyetli kişilerin eline geçmesi, ciddi maddi kayıplara ve kimlik hırsızlığına yol açabilir. Sentetik kimlik hırsızlığı, bireylerin gerçek ve sahte bilgileri harmanlayarak yaratılan, tamamen yeni kimliklerdir. Bu tür kimlikler, özellikle finansal sistemleri hedef alarak yasa dışı faaliyetlerde bulunmak için kullanılmakla birlikte çevrimiçi oyunlarda da sıklıkla kullanılmaya uygundur.<sup>142</sup> Sentetik kimlik hırsızlığı, bu alanda yükselen bir tehdit olarak karşımıza çıkmakta, hırsızlar bu yöntemle tamamen yeni ve sahte kimlikler oluşturarak yasa dışı faaliyetlerde bulunabilmektedir.

Çevrimiçi oyunlarda güvenliğin sağlanmasında birkaç temel unsur bulunmaktadır. İlk olarak, oyun ve uygulama geliştiricileri, yazılımların güvenlik açıklarını sürekli olarak izlemeli ve güncellemelidir. Ancak bu, güvenlik sorumluluğunun sadece geliştiricilerde olduğu anlamına gelmez. Kullanıcılar da kişisel verilerini korumak için proaktif adımlar atmalıdır.<sup>143</sup> Çevrimiçi oyunlar, kullanıcı deneyimini zenginleştirirken aynı zamanda belirli güvenlik risklerini de beraberinde getirir. Bu bağlamda oyun geliştiricilerinin yazılımlarını sürekli güncel tutmaları siber güvenlik açısından elzemdir. Her ne kadar bu tür güncellemeler yasal olarak zorunlu olmasa da sektörel etik ve sorumluluk çerçevesinde bu güncellemelerin düzenli olarak yapılması beklenir. Virüs yazılımlarında olduğu gibi bu süreçlerin amacı yazılımın ve son kullanıcıların korunmasını sağlamaktır. Geliştiriciler yazılımlarını güncelleyerek hem ticari varlıklarını koruma altına alır hem de kullanıcı deneyimini olumsuz yönde etkileyebilecek güvenlik açıklarını minimize ederler. Kullanıcılar ise çevrimiçi platformlarda karşılaşılabilecekleri güvenlik tehditlerine karşı bireysel önlemler almakla yükümlüdürler. Oyun içi güncellemelerin zamanında kabul edilmesi ve gerekli güvenlik tedbirlerinin alınması kullanıcının kendi veri güvenliğini sağlamasında kritik rol oynar. Oyun şartnameleri ve End User License Agreement (EULA) – Son Kullanıcı Lisans Anlaşması kullanıcıların oyunları belirli şartlar altında kullanmalarına izin verirken, oyunun telif hakları ve kaynak kodları yalnızca üretici

<sup>142</sup><https://blog.codevist.com/sentetik-kimlik-hırsızlığı-nedir-567d73cddb99>, ‘Sentetik kimlik hırsızlığı nedir?’, E.T: 12 Nisan 2024.

<sup>143</sup>B. Yalçınkaya, A. Ünal, B. Yılmaz ve F. Özdemirci, ‘Bilgi Yönetimi ve Bilgi Güvenliği’, *Ankara Üniversitesi Yayınları*, cilt: 1, sayı:5, 2019, s. 494.

şirkete ait olmaya devam eder. Bu çerçevede kullanıcıların kendilerine tanınan kullanım haklarını aşmamaları ve bu hakların ihlali durumunda karşılaşılabilecekleri yasal sonuçlar hakkında bilinçli olmaları büyük önem taşır. Bu bilinçlendirme hem kullanıcıları koruma altına alır hem de fikri mülkiyet haklarının gereği gibi idare edilmesini sağlar.

Kullanıcıların alabileceği önlemler arasında, şifre yönetimi önemli bir yer tutmaktadır. Güçlü ve benzersiz şifreler kullanmak, farklı oyun ve uygulamalar için farklı şifreler belirlemek, kişisel verilerin korunmasında önemli bir rol oynar. Ayrıca, iki faktörlü kimlik doğrulama yöntemlerini etkinleştirmek, hesap güvenliğini önemli ölçüde artırır. İki faktörlü kimlik doğrulama<sup>144</sup>, kullanıcıların hesaplarına erişim sağlarken güvenliklerini artırmak amacıyla iki aşamalı bir doğrulama sürecidir. Bu süreç, genellikle kullanıcı adı ve parola ile giriş yaptıktan sonra, kişinin telefonuna bir doğrulama kodu gönderilmesi şeklinde işler. Bu ikinci adım, hesap güvenliğine önemli bir katkı sağlar ve yetkisiz erişim riskini azaltır. İki faktörlü kimlik doğrulamanın uygulanması, siber güvenlik önlemleri arasında etkin bir yöntem olarak kabul edilir ve kullanıcıların dijital varlıklarını korumada kritik bir rol oynar. Öte yandan, kullanıcıların verdiği uygulama izinleri de büyük önem taşır. Çoğu oyun ve uygulama, çeşitli bilgilere erişim izni ister. Kullanıcıların, bu izinleri dikkatli bir şekilde incelemesi ve gereksiz izinleri reddetmesi gerekir. Özellikle, kişisel verilerin işlenmesi ve paylaşılması konusunda kullanıcılara net bilgilendirme yapılmalıdır.

Bu bilgilendirme süreci özellikle dijital platformlar ve oyunlar söz konusu olduğunda kullanıcıların bilinçli onayını almayı hedefler. Ancak pratikte çoğu kullanıcı hızla ilerleyip oyunun veya uygulamanın keyfini çıkarabilmek amacıyla bu bilgilendirme ve onam süreçlerini dikkatlice incelemeden geçiştirmekte ve hemen kabul etmektedir. Bu durum onam sürecinin asıl amacını sorgulamayı gerektirir çünkü gerçek bir bilinçlendirme ve onay kullanıcının sunulan bilgileri anlaması ve bu bilgilere dayanarak bilinçli bir tercih yapabilmesi anlamına gelir. Onay sürecinin yalnızca bir kerelik olması ve oyunun ilk kurulumu ile sınırlı kalması, bu sürecin etkinliğini daha da azaltmaktadır. Eğer gerçekten bilinçli bir onam sağlanmak isteniyorsa kullanıcıların bu bilgilere sürekli erişimi olmalı ve zaman zaman bu

---

<sup>144</sup><https://www.innova.com.tr/blog/iki-faktorlu-kimlik-dogrulama-2fa-internette-guvende-kalin>, ‘İki Faktörlü Kimlik Doğrulama (2FA): İnternette Günde Kalın’, E.T: 12 Nisan 2024.

konular hakkında hatırlatmalar yapılmalıdır. Ancak oyun ve uygulama sahipleri genellikle bu tür bir süreklilik sağlama yönünde bir yükümlülük hissetmemektedirler. Bu durum onamın sadece bir formalite olarak algılanmasına yol açar ve aslında bu onay sürecinin yeterince etkili olmadığını gösterir. Öte yandan onay sürecini daha etkileşimli ve oyunun bir parçası haline getirerek kullanıcıların dikkatini çekmek ve onları bilgilendirmek mümkün olabilir. Ancak bu oyunun akışını ve kalitesini bozabileceği için geliştiriciler bu tür bir değişikliği tercih etmeyebilir. Dolayısıyla kullanıcıların gerçekten bilinçli bir onam verip vermedikleri konusunda ciddi şüpheler bulunmaktadır. Bilinçli bir onam süreci için kullanıcılara verilen bilgilerin anlaşılır ve erişilebilir olması ve bu bilgilere dayanarak verilen kararların kullanıcılar tarafından iyi anlaşıldığının teyit edilmesi gerekmektedir. Bu hem oyun ve uygulama geliştiricilerinin sorumluluğunu artırır, hem de kullanıcıların bilinçli karar verme sürecine olan katılımlarını güçlendirir.

Çevrimiçi oyunlarda karşılaşılabilecek bir diğer tehlike ise, phishing saldırıları ve kötü amaçlı yazılımlardır. Oyuncular, oyun içi mesajlar veya e-posta yoluyla sahte bağlantılara yönlendirilebilir. Bu nedenle, gelen bağlantı ve e-postalara karşı dikkatli olmak ve yalnızca güvenilir kaynaklardan indirme yapmak önem taşır. Son olarak, mobil cihazlarda oyun oynayan kullanıcılar için ek güvenlik önlemleri de bulunmaktadır. Mobil cihazlar, kişisel bilgilerin saklandığı birer dijital cüzdan gibidir. Bu cihazlarda bulunan uygulamaların izinlerini düzenli olarak kontrol etmek ve kullanılmayan uygulamaları silmek, kişisel verilerin güvende tutulmasına yardımcı olur.<sup>145</sup> Çevrimiçi oyunlarda kişisel veri güvenliği, yalnızca teknolojik önlemlerle sağlanamaz. Bu süreç hem geliştiricilerin hem de kullanıcıların bilinçli ve sorumlu davranışlarına bağlıdır. Teknoloji gelişse de kişisel verilerin korunması konusunda her zaman proaktif olmak, sanal dünyada güvenli bir şekilde gezinmenin anahtarıdır.

### **3.2.3. Rekabet Avantajı ve Oyun İçi Manipülasyon**

Çevrimiçi oyunlarda rekabet avantajı elde etmek ve oyunun normal işleyişini manipüle etmek amacıyla hesap ele geçirme, siber suç dünyasında giderek artan bir trend haline gelmiştir. Bu tür eylemler, oyunların temel prensiplerine ve adil oyun anlayışına doğrudan bir saldırı teşkil eder. Saldırganların bu motivasyonları, oyun içi

---

<sup>145</sup>Yalçinkaya, Ünal, Yılmaz ve Özdemirci, a.g.e., s. 498.

dengeleri bozarak, diğer oyuncuların deneyimlerini olumsuz etkileyen ve oyunun bütünlüğünü zedeleyen sonuçlar doğurur.

Dijital oyunların evrimi, basit televizyon konsollarından günümüzün çok yönlü çevrimiçi platformlarına kadar uzanmaktadır. Bu süreçte rekabet avantajı sağlama amacıyla hesap ele geçirme, genellikle oyuncuların daha yüksek seviyelere ulaşmak, nadir bulunan eşyaları elde etmek veya oyun içi para biriktirmek gibi amaçlarla gerçekleştirilmektedir. Bu gelişim, çeşitli cihazlar aracılığıyla erişilebilen geniş bir oyun yelpazesi sunarak, kullanıcıların oyun deneyimlerini zenginleştirmiştir. Ancak bu ilerleme, özellikle çocuklar ve ergenler arasında dijital oyun bağımlılığının artmasına yol açmıştır. Bu bağımlılık, gerçek dünyadan uzaklaşma, sorumlulukların ihmal edilmesi ve diğer aktivitelerin göz ardı edilmesi gibi davranışları içerir. Hukuki açıdan, rekabet avantajı sağlamak amacıyla hesap ele geçirme gibi eylemler, kişisel verilerin korunması, gizlilik ihlalleri, telif hakkı ihlalleri, dolandırıcılık ve haksız rekabet gibi sorunları beraberinde getirir. Oyun geliştiricileri ve platform sağlayıcıları, bu tür eylemleri önlemek için gerekli güvenlik önlemlerini almakla yükümlüdür. Bu durum, siber güvenlik ve hukuk alanında önemli konuları gündeme getirirken, bireysel oyuncuların yanı sıra genel toplum güvenliği için de ciddi tehditler oluşturmaktadır.<sup>146</sup>

Siber suçlarla mücadelede hukukun rolü, bu tür eylemleri caydırmak, failleri tespit etmek ve cezalandırmak, mağdurlara adalet sağlamak ve oyun geliştiricileri ile platform sağlayıcıları için güvenlik standartlarını belirlemek şeklinde kritik bir öneme sahiptir. Hukuki düzenlemeler, siber suçlara karşı etkili önlemler almayı, suçluları tespit etmeyi ve cezalandırmayı amaçlar. Ayrıca, oyun geliştiricileri ve platform sağlayıcıları için güvenlik standartlarını belirleyerek, bu tür saldırıların önlenmesine yardımcı olur. Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, sadece bireysel oyuncular için değil, genel olarak siber güvenlik ve hukuk için önemli bir konudur. Bu tür eylemlerin arkasındaki motivasyonlar ve hedefler, ekonomik kazanç, kişisel veri ihlali ve rekabet avantajı sağlama gibi çeşitli faktörlerle ilişkilidir. Hukukun bu alandaki rolü, suçları önleme, suçluları adalet önüne çıkarma ve mağdurlara koruma sağlama yönündedir. Bu, siber suçlarla mücadelede hukukun kritik önemini vurgular ve oyun geliştiricileri ile platform sağlayıcıları için güvenlik standartlarının belirlenmesini gerektirir.

---

<sup>146</sup>A. Ünsal ve İ. Ulutaş, 'Bilgisayar Oyun Bağımlılığı Ölçeğinin Okul Öncesi Dönem Çocuklarına Uyarlanması', *Aksaray Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, cilt: 3, sayı: 2, 2019, s. 326.

#### **4. HUKUKİ BOYUT: SORUMLULUKLAR VE YAPTIRIMLAR**

Türk Ceza Kanunu'nda çevrimiçi oyun hesabının ve oyun karakterinin ele geçirilmesi gibi eylemler, çeşitli maddeler altında değerlendirilmektedir. Bu tür eylemler, genellikle bilişim sistemine girme, sistemleri engelleme, veri gönderme, verileri yok etme veya değiştirme ve banka veya kredi kartlarının kötüye kullanılması gibi suç tipleri kapsamında incelenir. Ayrıca, çevrimiçi oyunlar söz konusu olduğunda, ispat sorunu ve delil toplama yöntemleri gibi konular da büyük bir zorluk teşkil etmektedir. Hukuki yaptırımlar ve cezai müeyyideler, zarar gören tarafların tazminat hakkı, uluslararası iş birliği ve sınır ötesi suçlar gibi konular da bu çerçeve içerisinde ele alınmaktadır. Bu bağlamda, adli bilişim ve çevrimiçi oyunlarla ilgili hukuki sorumluluklar ve yaptırımlar, ilerleyen bölümlerde daha ayrıntılı bir şekilde incelenecektir.

##### **4.1. TCK Nezdinde “Çevrimiçi Oyun Hesabının ve Oyun Karakterinin Ele Geçirilmesinin Bilişim Suçları Kapsamında Değerlendirilmesi” Eylemlerinin Değerlendirilmesi**

Günümüzde teknoloji ve internet kullanımının hızla artmasıyla birlikte çevrimiçi platformlar ve sosyal medya üzerinden gerçekleştirilen etkileşimler de artmaktadır. Özellikle çevrimiçi oyunlar, milyonlarca kullanıcıyı bir araya getiren dinamik platformlar olarak öne çıkar. Ancak bu sanal platformlarda yaşanan bazı olumsuz durumlar, hukuki sorunları da beraberinde getirir. Çevrimiçi oyun hesaplarının ve karakterlerinin kötü niyetli kişilerce ele geçirilmesi, bu sorunlardan biridir ve TCK nezdinde değerlendirilmesi gereken ciddi bir konudur.

Hesapların ele geçirilmesi sürecinde, finansal kazanç umuduyla hareket eden saldırganlar, ele geçirilen hesapları satışa çıkarabilir veya hesapta bulunan değerli öğeleri satabilirler. Bu tür eylemler, TCK madde 141 Hırsızlık ve TCK madde 142 Nitelikli Hırsızlık ile TCK madde 157 Dolandırıcılık ve TCK madde 158 Nitelikli Dolandırıcılık suçlarını içerebilir. Ancak çevrimiçi ortamda gerçekleştirilen bu eylemler hukuk kurallarına tam anlamıyla uymaz. Bu hukuk çerçevesinin teknolojik gelişmeleri ve siber suçların sürekli değişen doğasını anlamak ve bu durumlarla başa çıkmak için sürekli olarak güncellenmesini gerektirir.

Bununla birlikte, çevrimiçi ortamda gerçekleştirilen bu eylemlerin hukuki bir boşluk yarattığı görülür. Çünkü dijital ortamın kendine özgü yapısı, geleneksel hukuk kurallarının uygulanabilirliğini zorlaştırır. Bu durum, özellikle yargı mensuplarının bu konularda teknik bilgiye sahip olmamaları nedeniyle, dijital adli tıp konularında sürekli eğitim gereksinimini ortaya çıkarır. Çünkü dijital olayların delillerinin doğru bir şekilde toplanması ve yorumlanması, teknik bir anlayış gerektirir.

Sonuç olarak, Türkiye'deki hukuk sisteminin, çevrimiçi oyun hesaplarının ele geçirilmesi gibi siber suçlarla daha etkin bir şekilde mücadele edebilmesi için gelişmesi gerekmektedir. Bu, hem suçluların etkili bir şekilde cezalandırılması hem de potansiyel suçluların caydırılması için kritik öneme sahiptir. Hukuk çerçevesinin güncellenmesi, sadece yasaların yazımıyla sınırlı kalmamalı, aynı zamanda yargı mensuplarının bu yeni ve karmaşık suç tiplerini anlamalarını sağlayacak eğitim programlarını da kapsamalıdır. Bu tür bir yaklaşım, çevrimiçi oyun hesaplarının korunmasına ve bu alandaki suçların azaltılmasına önemli ölçüde katkı sağlayacaktır.

#### **4.2. “Çevrimiçi Oyun Karakteri Ele Geçirme” Eyleminin Türk Ceza Kanunu’ndaki Uygun Suç Tipleri Açısından Değerlendirilmesi**

Dijital çağın akla gelen ilk sorunu Internet üzerinden gerçekleştirilen yasa dışı faaliyetlerin önlenmesidir. Özellikle, internet üzerinden gerçekleştirilen ve bilişim teknolojilerinin kullanıldığı suçlar, modern hukukun önemli bir sorunsalını teşkil etmektedir.<sup>147</sup> Bu bağlamda, Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" olarak adlandırılan bu suç tipleri, yasal düzenlemelerle kontrol altına alınmaya çalışılmaktadır.

Çevrimiçi oyun hesaplarının ele geçirilmesi ve bu tür olayların hukuki boyutunu incelemek, Türkiye ve diğer birçok ülkede hukukçular ve yasa yapıcılar için büyük bir meydan okuma olmuştur. Bunun sebebi, dijital dünyanın karmaşık ve sürekli değişen doğası hem kanun koyucuların hem de yargı mensuplarının bu alandaki bilgi ve becerilerinin sınırlı olmasıdır. Ayrıca, mevcut kanunların bu tür durumları ele alma şekli, çevrimiçi suçlarla etkin bir şekilde başa çıkmak için genellikle yetersiz

---

<sup>147</sup>V. Ö. Özbek, ‘İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları’, *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 69, sayı: 1-4, 2001, s. 106.

kalmaktadır. Bu noktada, kolluk kuvvetlerinin rolü özellikle önemlidir. Yasa koyucuların internet tabanlı suçlarla mücadelede yeterince etkili olamadığı durumlarda, kolluk kuvvetleri mevcut yasal çerçeve içerisinde hareket etme sorumluluğuna sahiptir. Ancak, mevcut yasaların eksikliği veya yetersizliği söz konusu olduğunda, kolluk kuvvetlerinin hukuki sınırlar dışına çıkması veya yasa dışı faaliyetlerde bulunması kesinlikle uygun değildir. Bu tür bir durumda, kolluk kuvvetleri, yasal boşlukları dolduracak şekilde yasama organı ile iş birliği yaparak, eksik yasal düzenlemelerin tamamlanması için gerekli adımları atmalı ve mevcut yasal çerçevede kalmak koşuluyla suçla mücadele etmelidir. Böylece, hem yasalara uygun hareket edilmiş olur hem de çevrimiçi suçlarla daha etkin bir mücadele mümkün hale gelir. Bu süreçte, kolluk kuvvetlerinin görevi, yasal sınırların dışına çıkmadan, mevcut yasaların imkân verdiği ölçüde suçla mücadeleyi sürdürmek ve yasal boşlukların giderilmesi için yasama organıyla iş birliği yapmaktır. Bu iş birliği, müdahale edilen suçlarda eksik görülen hususların teklif yoluyla bildirilmesi, yeni yasal düzenlemelerin hazırlanması ve mevcut yasaların dijital suçlar karşısında daha etkili hale getirilmesi için gerekli olan bilgi, tecrübe ve teknik donanımın sağlanmasını kapsar. Bu süreçte, kolluk kuvvetlerinin ve hukukçuların katkılarıyla yasaların uygulanabilirliği artırılarak, çevrimiçi suçlarla mücadelede daha sağlam bir hukuki zemin oluşturulacaktır.

Hesap ele geçirme vakalarının hukuki boyutu, mevcut hukuki çerçevenin dijital dünyanın hızla değişen ve karmaşıklaşan gereksinimlerini karşılamakta zorlandığını göstermektedir. Bu, yasa yapıcıları ve kolluk kuvvetlerini, dijital dünyayı daha iyi anlama ve hukuki çerçeveyi bu yeni ve karmaşık alanı etkin bir şekilde düzenleyecek şekilde güncelleme ihtiyacına itmektedir. Hukukçular, yasa yapıcılar ve kolluk kuvvetleri, dijital dünyanın hızla değişen doğasını takip etmek ve buna uyum sağlamak için sürekli çaba sarf etmek zorundadırlar. Yasa koyucuların yeni ve karmaşık dijital suçları anlamak ve bu suçları etkin bir şekilde düzenleyecek yasalar ve düzenlemeler oluşturmak için çabaları, dijital dünyanın karmaşık doğasına rağmen hukuki çözümler üretmek için önemli bir adımdır.

Bu çözümlerden biri, çevrimiçi hesap ele geçirme suçunun cezai boyutunu açıkça tanımlayan ve belirleyen daha spesifik yasaların oluşturulmasıdır. Örneğin, Türkiye'deki mevcut TCK'da belirtilen bilişim alanında suçların düzenlenmiş olduğu

Kanunlar çevrimiçi hesap ele geçirmeyi açıkça bir suç olarak tanımlamamaktadır. Bunun yerine, bu tür suçlar genellikle genel suçlar çerçevesinde değerlendirilmekte ve yargılanmaktadır. TCK ilgili maddeleri çerçevesinde, suçun maddi unsurunun hareket ögesinin eyleme tam olarak tekabül etmediği durumlarda, genellikle hırsızlık, nitelikli dolandırıcılık gibi daha genel suç tipleri üzerinden yaptırım uygulanmaktadır. Çevrimiçi oyun hesaplarının ve oyun karakterlerinin izinsiz ele geçirilmesi suçu, maddi unsurları açısından incelendiğinde, bu suçun temelini oluşturan hareket, bu tür hesap veya karakterlere yetkisiz olarak erişim sağlanması ve kontrolünün ele alınmasıdır. Gerçek sahibinin hesap veya karakter üzerindeki kontrolünün kısıtlanması veya tamamen yitirilmesi gerçekleşir. Bu durum, hesap sahibinin maddi ve manevi zararlara uğramasına neden olabilir.

İllyet bağı bakımından, yetkisiz erişimin doğrudan bu zararların ve kontrol kaybının sebebi olduğu açıktır. Hesabın veya karakterin ele geçirilmesi, çevrimiçi oyun içi varlıkların kaybına veya oyun içi kazanımların başka bir şahıs tarafından gasp edilmesine yol açar. Bu durum, oyun sahibinin hem ekonomik hem de sosyal etkileşimlerde ciddi kayıplar yaşamasına sebep olur. Bu tür suçlar, mevcut kanunlar altında genellikle hırsızlık, nitelikli dolandırıcılık gibi daha genel suç tipleri üzerinden değerlendirilse de çevrimiçi oyun ortamlarının özgül nitelikleri ve bu platformlarda gerçekleşen etkileşimlerin karmaşıklığı, bu tür eylemlerin daha spesifik bir hukuki çerçeve içerisinde ele alınmasını gerektirir. Bu tür suçların daha etkin bir şekilde ele alınabilmesini ve önlemler alınmasını sağlayacaktır.

Çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi suçu hâlâ yeni ve özelleşmiş bir alan olduğundan, mevcut yasalar altında bu tür eylemlerin cezalandırılması konusunda belirsizlikler bulunabilir. Suçta ve cezada kanunilik ilkesi, herhangi bir kişinin yalnızca yasalarla önceden belirlenmiş bir suçu işlemesi halinde cezalandırılabileceğini belirtir. Bu ilke aynı zamanda, cezaların ve suç tanımlarının açık ve önceden belirlenmiş olmasını gerektirir. Çevrimiçi oyun hesaplarının izinsiz ele geçirilmesi gibi davranışlar için özel bir yasal düzenleme bulunmaması durumunda, hakimler bu tür suçları genel suçlar çerçevesinde, örneğin hırsızlık ve nitelikli dolandırıcılık gibi mevcut suç tipleri altında değerlendirebilirler. Ancak, bu tür bir uygulama kıyas yasağına aykırı olabilir. Kıyas yasağı, yasalarda açıkça tanımlanmayan bir davranışın, benzer görünen başka bir suç tipi altında

cezalandırılmasını engeller. Eğer hakimler, çevrimiçi oyun hesaplarının izinsiz ele geçirilmesi suçunu, yasalarda açıkça tanımlanmamışsa ve direkt olarak uygulanabilecek bir yasa maddesi bulunmuyorsa, genel suç tipleri altında değerlendiriyorlarsa, bu durum suçta ve cezada kanunilik ilkesi ve kıyas yasağına potansiyel olarak aykırı bir uygulama olabilir.

Karşılıksız yararlanma<sup>148</sup> suçu bağlamında ele alındığında, TCK mad. 163'ün açıklamaları dikkate alındığında, bu madde malvarlığına karşı işlenen suçlar çerçevesinde cezalandırılan fiilleri kapsar. Ancak karşılıksız yararlanma fiilinin ceza gerektiren bir fiil olarak ele alınıp alınamayacağı ve eğer ceza hukuku kapsamında ele alınacaksa ayrı bir suç tipi mi yoksa benzer nitelikteki hırsızlık, dolandırıcılık veya bilişim alanındaki suç tipleri içinde mi düzenleneceği soruları yasal belirsizlikler yaratmaktadır.

Karşılıksız yararlanma suçu, temelde bir malvarlığına yönelik haksız yarar sağlama fiili olarak tanımlanabilir. Ancak, bu suçun ceza hukuku kapsamında ayrı bir suç tipi olarak ele alınması gerekip gerekmediği konusu tartışmalıdır. TCK mad. 163 bu suçu net bir şekilde tanımlar ve hırsızlık, dolandırıcılık gibi diğer malvarlığına karşı suçlarla benzer özellikler taşısa da kendi başına ayrı bir kategori olarak ele alınır. Karşılıksız yararlanma, özellikle otomatik makineler<sup>149</sup> aracılığıyla sunulan hizmetlerden yararlanmayı kapsar ve bu durum hırsızlık veya dolandırıcılıktan farklıdır çünkü bu suçlar doğrudan bir malın zimmete geçirilmesi veya aldatma yoluyla bir kazanç sağlama eylemini içerir. Diğer yandan bilişim suçlarıyla ilişkilendirilmesi ise daha çok çevrimiçi platformlarda gerçekleşen yararlanma faaliyetlerinde söz konusu olabilir. Çevrimiçi oyun hesaplarının izinsiz ele geçirilmesi gibi modern suç tipleri karşılıksız yararlanma kavramını teknolojik boyutta genişletir. Ancak burada dikkat edilmesi gereken TCK'nın bu tür modern suçlar için özel düzenlemelere ihtiyaç duymasıdır. Mevcut kanun maddeleri genellikle fiziksel dünyada gerçekleşen yararlanmaları ele alırken, çevrimiçi ortamlarda meydana gelen suç tipleri için yetersiz kalabilir.<sup>150</sup>

---

<sup>148</sup>B. Işık, 'Karşılıksız Yararlanma Suçu', *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 29, sayı: 3, 2021, s. 2052.

<sup>149</sup>Işık, a.g.e., s. 2063.

<sup>150</sup>Işık, a.g.e., s. 2056-2058.

TCK mad. 163 karşılıksız yararlanma suçunu açıkça tanımlamış olmasına rağmen, bu suçun yargı pratiğindeki uygulanışında ve yeni teknolojik suç tiplerine adaptasyonunda belirsizlikler mevcuttur. Bu nedenle kanun koyucunun bu suç tipini ve ilgili yasal düzenlemeleri, teknolojik gelişmeleri ve modern suç tiplerini göz önünde bulundurarak güncellemesi büyük önem taşımaktadır. Böylece hem yasal açıklık kapatılmış olur hem de karşılıksız yararlanma suçu daha etkin bir şekilde cezalandırılabilir. Ayrıca tezimizin konusu olan çevrimiçi oyunlarda meydana gelen hesapların ve hesap karakterlerinin çalınması suçunun açık ve net bir şekilde cezalandırılması sağlanacaktır.

Bu alandaki hukuki düzenlemelerin sınırları belirsiz kalmakta, internet, demokratik ve hatta anarşik bir platform olarak değerlendirilmektedir. İnternetin bu evrensel doğası, vatandaşlara anonim bir şekilde, kimliklerini açığa çıkarmadan, düşüncelerini özgürce ifade etme imkânı sunar.<sup>151</sup> Bu bağlamda, internetin yarattığı yeni iletişim kanalları, küresel köyün küçük ama etkili mekanlarına dönüşürken, sesli ve görüntülü iletişim, çevrimiçi oyunlar, özel yaşamın paylaşılması, e-ticaret gibi birçok yeniliği beraberinde getirmiştir. Bunlar hem olumlu hem de olumsuz sonuçlar doğurarak toplumun yeni alışkanlıklar edinmesine öncülük etmiştir. Siber alanın yüzyılımızın en hızla evrilen ve global bir boyuta ulaşan sektörlerinden biri olduğu açıktır. Bu dinamik ortamda, kolluk kuvvetlerinin etkin bir varlık sergileyebilmesi, siber dünyanın özgün yapısını ve bu alandaki suçlarla mücadelede karşılaşılan spesifik zorlukları derinlemesine kavramayı zorunlu kılar. İnternet, geçtiğimiz yirmi yıl içerisinde coğrafi sınırları aşarak hızla büyüyen ve geleneksel yargı alanlarını genişleten bilişim sektörü olarak kendini göstermiştir. Bu sebeple, siber suçlarla mücadelede kolluk kuvvetlerinin daha yetkin bir role bürünebilmesi için teknik bilgi ve becerilerin sürekli olarak güncellenmesi, kullanılan araçların etkin şekilde işlev görmesi ve yeni teknolojik gelişmelerle taktiklerin devamlı izlenmesi gerekmektedir. Bu bağlamda, kolluk kuvvetlerinin siber suçlarla mücadeledeki etkinliğini artırmak ve dijital dünyanın getirdiği zorluklarla baş edebilmek adına, teknik ve hukuki çerçevenin sürekli olarak yenilenmesi, bilgi ve becerilerin artırılması ve zamanın gerektirdiği

---

<sup>151</sup>U. Taşçı ve A. Can, 'Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014', *Fırat Üniversitesi Sosyal Bilimler Dergisi*, cilt: 25, sayı: 2, 2015, s. 230.

teknolojik donanımların temin edilmesi elzemdir. Ancak bu şekilde siber alanda hukukun üstünlüğü ilkesi etkin bir şekilde tecelli edebilir.<sup>152</sup>

Türkiye'nin hukuk sistemi, çevrimiçi hesap ele geçirme eylemlerine yönelik daha detaylı ve spesifik düzenlemelere ihtiyaç duymaktadır. Gerekli düzenlemelerin yapılması ve eğitim programlarının hayata geçirilmesi ile çevrimiçi hesap ele geçirme vakalarına karşı daha etkili bir önleyici ve mücadeleci yaklaşım sergilenebilir. Özellikle TCK Onuncu Bölümde yer alan ve bilişim suçları ile direkt ve dolaylı olarak ilişkilendirilen bazı kanun maddelerini aşağıda inceleyeceğiz.

#### **4.2.1. Bilişim Sistemine Girme (TCK md.243)**

Bu madde bireylerin veya kuruluşların bilgi işlem kaynaklarına yönelik hukuka aykırı müdahaleleri yasaklamakta ve bu tür eylemleri gerçekleştiren kişilere ciddi cezai yaptırımlar öngörmektedir. Bilişim sistemlerine izinsiz giriş, sadece sisteme fiziksel olarak zarar vermekle sınırlı olmayıp, veri hırsızlığı, kötü amaçlı yazılım yayma ve diğer zararlı faaliyetleri de içerebilecek geniş bir yelpazeyi kapsar. Bu madde, bilişim teknolojilerinin hayatımızın her alanına nüfuz ettiği günümüz dünyasında, bireylerin ve kurumların dijital varlıklarını koruma altına almayı amaçlamaktadır. Bilişim sistemlerine izinsiz erişim, kişisel verilerin, finansal bilgilerin ve diğer hassas verilerin çalınması, bozulması veya yok edilmesi gibi ciddi sonuçlar doğurabilir. Bu sebeple, TCK madde 243, bu tür eylemleri caydırıcı bir unsur olarak ele alır ve potansiyel suçlulara karşı açık bir uyarı niteliği taşır.

TCK madde 243'un temel gerekçesi, bilişim sistemlerinin bütünlüğünü ve güvenliğini sağlamak, aynı zamanda bilişim suçlarına karşı etkili bir mücadele mekanizması oluşturmaktır. TCK madde 243, bilişim sistemlerine izinsiz erişim ile ilgili genel hükümler içermekte olup, özellikle çevrimiçi oyun hesapları ve oyun karakterlerinin ele geçirilmesi gibi spesifik durumlar açıkça metinde yer almamaktadır. Ancak, bu tür davranışlar, madde kapsamında değerlendirilebilecek izinsiz erişim faaliyetleri olarak kabul edilebilir. Bu madde, izinsiz erişimin maddi unsurları olarak, bilişim sistemlerine yetkisiz olarak girilmesini ve bu sistemler

---

<sup>152</sup> Taşçı ve Can, a.g.e., s. 229.

üzerinde kontrol sağlanmasını içerir. Bu durum, çevrimiçi oyun hesaplarının ele geçirilmesiyle paralellik göstermektedir.

TCK madde 243 kapsamında genel suç, "bilgi sistemlerine izinsiz giriş" suçunu tanımlayarak bu alanda genel bir çerçeve sunar. Genel suçlar<sup>153</sup>, belirli bir alan veya sektörle sınırlı olmaksızın farklı bilgi sistemleri için geçerlidir. Dolayısıyla, bu madde bilgi sistemlerine izinsiz giriş, veri hırsızlığı, kötü amaçlı yazılım yayma gibi geniş bir yelpazedeki zararlı faaliyetleri kapsar. Bu tür eylemler, özellikle çevrimiçi oyun hesapları gibi dijital varlıkların ele geçirilmesi ve kontrol edilmesi olaylarını da içerir. Genel hükümler içerdiği için, bilgi suçları alanında işlenen pek çok eylemi tanımlama yeteneğine sahiptir. TCK madde 243, bu bağlamda dolandırıcılık, hırsızlık, gasp veya şantaj gibi suçların bilgi sistemleri üzerinden işlenmesini tamamlayıcı bir nitelik kazanır. Tamamlayıcı suç, diğer suç türlerini destekleyen veya tamamlayan bir suç olarak tanımlanır.<sup>154</sup> Örneğin, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, sıklıkla hırsızlık veya dolandırıcılık gibi diğer suçlarla birlikte işlenir. Bu durumda, madde 243, bilgi sistemlerine izinsiz girişin getirdiği tehlikeli boyutları ve zararı tanımlayarak diğer suçlarla birlikte uygulanabilir. Bu şekilde, bilgi suçlarıyla ilgili başka suçların işlenmesi halinde madde 243, ek bir hukuki dayanak sağlar.

Özetle, TCK madde 243, bilgi sistemlerine izinsiz giriş eylemleriyle ilişkili geniş kapsamlı suçları ele alır ve başka suçların işlenmesinde tamamlayıcı bir rol oynayarak bilgi alanındaki yasa dışı faaliyetlere karşı kapsamlı bir koruma sağlar. TCK madde 243'un bu bağlamda önemi, sadece bilgi suçlarını cezalandırmakla kalmayıp, aynı zamanda dijital ortamda güvenliğin ve istikrarın sağlanması yönünde caydırıcı bir etki yaratmaktadır. Böylece hem bireylerin hem de şirketlerin dijital varlıklarının korunması güçlenmiş olur. Bu madde, bilgi suçlarıyla mücadelede önemli bir yasal araç olarak hem bireysel hem de kurumsal düzeyde güvenlik ve güvenilirliği desteklemektedir.

---

<sup>153</sup>F. Erem, 'Suçun Konusu ve Hümanist Doktrin', *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, cilt:25, sayı: 1-2, Mart-Nisan 1968, s. 14.

<sup>154</sup>S. Bayındır, 'İş ve Çalışma Hürriyetinin İhlali Suçu (TCK m. 117/1)', *D.E.Ü. Hukuk Fakültesi Dergisi*, cilt 21, Özel Sayı, 2019, s. 157.

#### **4.2.2. Madde 244: Bilişim Sistemini Engelleme, Bozma, Veri Gönderme, Verileri Yok Etme veya Değiştirme**

Bilişim suçları, günümüz dijital çağında bireylerin ve kuruluşların karşılaştığı en büyük tehditlerden biridir. TCK madde 244, bilişim sistemlerine izinsiz erişimle bunların işleyişine zarar verilmesini, yetkisiz veri gönderilmesini, içerdiği verilerin izinsiz değiştirilmesi veya yok edilmesini yasaklar ve bu tür eylemler için cezai yaptırımlar öngörür. Bilişim sistemlerine saldırılar, kişisel veya kurumsal verilerin yok edilmesi, değiştirilmesi, izinsiz paylaşılması ya da manipüle edilmesi gibi geniş kapsamlı zararlar doğurur. Bu bağlamda çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, bilişim suçları arasında önemli bir yer tutar.

Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, bir kullanıcının izni olmaksızın dijital varlıklarının veya karakterlerinin ele geçirilmesi ve manipüle edilmesi anlamına gelir. Dijital varlıklar, kullanıcıların büyük çaba ve mali yatırımlarla geliştirdiği çevrimiçi oyun hesapları veya karakterlerdir. Bu varlıklar, kullanıcının izni olmaksızın ele geçirildiğinde hem maddi kayıp hem de manevi zarar meydana gelir. Bu zararlar arasında finansal kayıplar, kişisel veri ihlali ve sosyal çevrede güven kaybı yer alır. TCK madde 244, genel anlamda bilişim sistemlerine yetkisiz erişimi suç sayar. Bu açıdan genel bir suçtur, çünkü sadece belirli bir tür bilişim sistemiyle sınırlı kalmayıp, farklı türdeki sistemlere erişimi düzenler. Örneğin, bir kurumsal bilgi sistemi ya da bireysel çevrimiçi oyun hesabı fark etmeksizin izinsiz giriş yapıldığında bu maddeye dayanarak cezai yaptırım uygulanabilir. Tamamlayıcı suç olarak TCK madde 244, dolandırıcılık, hırsızlık veya şantaj gibi suçlara destek verir ve onların işlenmesi sırasında bilişim sistemlerine izinsiz giriş yapılmasını kapsar.<sup>155</sup> Örneğin çevrimiçi oyun hesaplarının ele geçirilmesi ile birlikte bu varlıkların haksız kazanç sağlamak amacıyla kullanılması durumunda, hırsızlık veya dolandırıcılık suçlarının tamamlayıcısı olarak ele alınır.

Bu suçta korunan hukuki yarar, bireylerin dijital varlıklarının ve verilerinin bütünlüğü ve gizliliğidir. Bilişim sistemlerine izinsiz erişim, kullanıcıların özellikle

---

<sup>155</sup>R.Y. Yazıcıoğlu, “5237 s. TCK.nun 244/4’üncü Maddesinde Düzenlenen “Bilişim Sistemi Marifetiyle Haksız Çıkar Sağlanması” Suçu ile md.142/2-e ve 158/1-f Maddesinde Düzenlenen “Bilişim Sistemlerinin Kullanılması Suretiyle” “Hırsızlık” ve “Dolandırıcılık” Suçlarının İşlenmesi Sorunsalı Üzerine Düşünceler”, *Suç ve Ceza Dergisi*, sayı:4, 2009, s.4-8.

maddi zarar görmesine yol açar. Örneğin, çevrimiçi oyun hesaplarının ele geçirilmesi durumunda, kullanıcılar yatırım yaptıkları dijital varlıklarını kaybedebilir. Bu tür olaylar, doğrudan finansal kayıplara neden olur. Dolayısıyla, TCK madde 244'ün amacı, bilişim sistemlerini koruyarak bu dijital varlıkların güvenliğini sağlamak ve kullanıcıların maddi haklarını korumaktır. Bu yönüyle, yasa kapsamındaki yaptırımlar, dijital varlıkların güvenli bir şekilde korunmasını garanti altına almayı hedefler. Gerekçe olarak, bilişim suçlarının karmaşıklığı ve dijital varlıkların korunması ihtiyacı gösterilebilir. Bu tür suçlar sürekli olarak gelişmekte olup, bireylerin ve kuruluşların dijital varlıklarına tehdit oluşturmaktadır. Dolayısıyla TCK madde 244, bireylerin ve kuruluşların dijital ortamda güvenle var olabilmelerini sağlamak ve bilişim suçlarının sonuçlarını engellemek amacıyla cezai yaptırımlar getirmektedir. Bu yaptırımlar, bilişim suçlarına karşı caydırıcı ve adil bir koruma mekanizması olarak işlev görür.

#### **4.2.3. Madde 245: Banka veya Kredi Kartlarının Kötüye Kullanılması**

Türk Ceza Kanunu'nun (TCK) 245. maddesi, finansal işlemler ve kişisel finansal bilgilerin kötüye kullanılmasını önlemek amacıyla düzenlenmiştir. Bu madde, banka ve kredi kartları gibi finansal araçların izinsiz kullanımını yasaklar ve bu tür eylemlere karşı ciddi cezai yaptırımlar öngörür. Çevrim içi oyun hesaplarının ve karakterlerinin ele geçirilmesi durumunda, özellikle bu hesaplar finansal değer taşıyorsa, TCK 245 kapsamında değerlendirilmesi mümkündür.<sup>156</sup>

Çevrim içi oyunlarda kullanılan oyun içi para birimleri, genellikle oyuncuların kredi kartları veya banka kartları kullanarak gerçek parayı oyun içine aktarmasıyla meydana gelmektedir. Bu süreç, çevrim içi oyun hesaplarının ve karakterlerinin finansal bir değer taşımasına ve bu hesapların kötüye kullanılması durumunda maddi zararlara yol açmasına neden olur. Çevrim içi oyun hesaplarının izinsiz ele geçirilmesi, bu maddi değerlerin kötü niyetli kişiler tarafından kullanılması anlamına gelir ve TCK madde 245 altında düşünüldüğünde, banka ve kredi kartı bilgilerinin kötüye kullanılmasına paralel bir durum teşkil eder.

---

<sup>156</sup>V. Ö. Özbek, 'Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)', *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 9, Özel Sayı, 2007, s. 1024.

Bu suçta korunan hukuki yarar, finansal işlemler ve bireylerin kişisel finansal bilgilerinin güvenliğidir. Çevrim içi oyunlarda, gerçek para kullanılarak oyun içi para birimleri satın alınması, bu para birimlerinin ve diğer dijital varlıkların korunmasını zorunlu kılar. Çevrim içi oyun hesaplarının izinsiz ele geçirilmesi durumunda, bu dijital varlıkların kötüye kullanılması hem bireysel kullanıcıları hem de ekonomik sistemleri olumsuz etkileyebilir. Bu nedenle, TCK madde 245'in koruma amacı, finansal güvenliği sağlamak ve bireylerin mali kaynaklarını güvence altına almaktır.

Gerekçe olarak çevrim içi oyun hesaplarının ele geçirilmesi, finansal değer taşıyan dijital varlıklara yönelik bir tehdit oluşturur. Bu hesaplar aracılığıyla yapılan işlemler genellikle kredi kartı veya banka bilgilerini içerir, dolayısıyla bu bilgilerin kötüye kullanılması, geniş çaplı finansal zararlara yol açabilir. TCK madde 245'in getirdiği yasal düzenlemeler, bu tür kötüye kullanımları önlemeyi amaçlar, böylece hem bireysel hem de kurumsal düzeyde finansal güvenlik sağlanır.<sup>157</sup>

TCK madde 245, genel bir suç olarak finansal bilgilerin kötüye kullanılmasını yasaklar. Bu madde, finansal araçların kötüye kullanılmasını kapsayarak geniş bir yelpazede uygulanabilir. Tamamlayıcı suç olarak ise, özellikle çevrim içi oyun hesaplarının ele geçirilmesi gibi durumlarla birlikte değerlendirildiğinde, bu suçların dolandırıcılık veya hırsızlık gibi diğer finansal suçlarla birleştiği durumları kapsar. Bu hesapların kötüye kullanılması, doğrudan finansal zararlara sonuçlanabilir ve bu zararlar, TCK madde 245'in koruma kapsamına girer. Sonuç olarak, çevrim içi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi, TCK madde 245'in ruhuna uygun olarak değerlendirilmeli ve finansal güvenlik ile kişisel bilgilerin korunması amacıyla genişletilmesi veya uygun şekilde yorumlanması gerekir. Bu durum, yasal düzenlemelerin dijital çağın gerekliliklerine göre güncellenmesini ve hukuki yorumların genişletilmesini gerektirir, böylece etkili bir koruma sağlanabilir.

#### **4.2.4. Madde 245/A: Yasak Cihaz veya Programlar**

TCK madde 245/A, günümüzün sürekli gelişen dijital dünyasında bilişim sistemlerinin güvenliğini tehdit eden ciddi sorunlarla mücadele etmek amacıyla

---

<sup>157</sup> Özbek, a.g.e., s. 1025-1026.

tasarlanmıştır. Bu madde, bilişim sistemlerine izinsiz erişim sağlama, bu sistemlerdeki verilere izinsiz olarak müdahale etme veya bilişim sistemlerini izinsiz kullanma amacıyla hazırlanmış olan her türlü cihaz, bilgisayar programı veya diğer araçların üretimi, satışı, ithali, nakli veya bu araçların sair şekillerde temini, dağıtımı veya bulundurulmasını yasaklar. Bu düzenleme, bilişim suçlarıyla mücadelede önemli bir adım olup, bu tür eylemleri gerçekleştiren kişilere cezai yaptırımlar uygulanmasını sağlar.<sup>158</sup>

Bu suçta korunan hukuki yarar, bilişim sistemlerinin bütünlüğü ve işleyişinin korunmasıdır. Bilişim sistemlerine yönelik saldırılar, sadece maddi kayıplara yol açmakla kalmaz, aynı zamanda bireylerin ve kurumların işleyişini temelden sarsabilir. Özellikle çevrimiçi oyun hesaplarının ele geçirilmesi gibi eylemler, bilişim sistemlerinin güvenilirliğine ve verilerin gizliliğine yönelik tehditler oluşturur. Bu durumlar, bilişim suçlarının kapsamında değerlendirilir ve maddi değerlerin yanı sıra sistem güvenliğinin korunması açısından da önem taşır.

TCK madde 245/A'nın temel gerekçesi, bilişim sistemlerinin korunmasını sağlamaktır. Çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi, genellikle bilişim sistemlerine yönelik saldırılarla ilişkilidir. Bu tür eylemler, genellikle bilişim sistemlerine izinsiz erişim sağlamak veya bu sistemlerdeki verilere izinsiz olarak müdahale etmek amacıyla hazırlanmış programlar veya araçlar kullanılarak gerçekleştirilir. Yasal düzenlemelerin bu tür teknolojik araçları net bir şekilde tanımlaması ve bu araçların kullanımını engellemesi, suçların önlenmesi ve bilişim sistemlerinin güvenliğinin sağlanması açısından kritik önem taşır.

TCK madde 245/A, genel bir suç tanımı sağlar çünkü bilişim sistemlerine yönelik her türlü izinsiz erişimi kapsar. Aynı zamanda tamamlayıcı suç niteliği taşır, çünkü bilişim sistemlerine zarar vermek amacıyla yapılan diğer suçlarla birlikte değerlendirilebilir. Örneğin, çevrimiçi oyun hesaplarının ele geçirilmesi, sadece finansal zararlarla sınırlı kalmayıp, aynı zamanda bilişim sistemlerinin işleyişine zarar verme potansiyeli taşıdığı için, bu madde altında değerlendirilebilir. Bu çerçevede, TCK madde 245/A'nın etkin uygulanması, bu tür suçların önlenmesinde ve bilişim

---

<sup>158</sup>İ.S. Kaya ve A. Çakır, 'Yasak Cihaz veya Programlar Suçu', *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, cilt: 19, sayı: 38, 2020, s. 35.

sistemlerinin korunmasında önemli bir role sahiptir. TCK madde 245/A'nın uygulanması, çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi gibi modern bilişim suçlarının etkin bir şekilde ele alınmasını sağlar. Bu madde, bilişim sistemlerine yönelik saldırıları caydırma ve cezalandırma yoluyla, bilişim suçlarıyla mücadelede önemli bir yasal araç olarak işlev görür.

#### **4.2.5. Madde 246: Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması**

TCK madde 246'nın sunduğu çerçeve, bilişim teknolojilerinin hızla evrimleştiği çağımızda, tüzel kişilerin karşı karşıya kaldığı suçlarla mücadelede önemli bir yasal araç sunmaktadır. Bu madde, şirketler, dernekler, vakıflar gibi tüzel kişiliklere sahip organizasyonların temsilcileri veya çalışanları tarafından işlenen bilişim suçları bağlamında, söz konusu tüzel kişilere uygulanacak güvenlik tedbirlerini detaylandırır. Bu, özellikle günümüzde tüzel kişiliklerin bilişim teknolojilerine olan bağımlılığının artmasıyla daha da büyük bir önem kazanmıştır. Bilişim suçları, siber saldırılar, veri ihlalleri ve benzeri faaliyetler, tüzel kişiliklerin itibarına, finansal durumuna ve işleyişine zarar verebilecek potansiyele sahiptir.<sup>159</sup>

Bu bağlamda, TCK madde 246'nın sağladığı yaptırımlar ve tedbirler, tüzel kişiliklerin bu tür suçlara karşı korunmasını sağlamak amacıyla hayati öneme sahiptir. TCK madde 246 kapsamında öngörülen güvenlik tedbirleri, tüzel kişinin faaliyetlerinin durdurulması, belirli haklardan yoksun bırakılması gibi geniş bir yelpazeye sahiptir. Bu tedbirlerin amacı, suç teşkil eden faaliyetlerin önlenmesi, tekrarının engellenmesi ve tüzel kişiliklerin hukuka uygun hareket etmelerinin teşvik edilmesidir. Örneğin, bir şirketin çalışanı tarafından işlenen bir bilişim suçu nedeniyle, şirketin internet üzerinden hizmet verme yetkisinin geçici olarak askıya alınması söz konusu olabilir. Bu hem caydırıcı bir etki yaratmakta hem de şirketi iç kontrol ve denetim mekanizmalarını güçlendirmeye yönlendirmektedir. Bu noktada, çevrimiçi oyun hesaplarının ve oyun karakterlerinin ele geçirilmesi, günümüzde önemli bir sorun haline gelmiştir. Bilişim suçu kapsamında değerlendirilebilecek bu tür eylemler, kişisel mülkiyet haklarının ihlali olarak görülebilir ve tüzel kişiliklerin de dahil olduğu bir

---

<sup>159</sup>Y. Erdoğan, 'Bilişim Sistemine Girme ve Kalma Suçu', *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 12, Özel Sayı, 2010, s. 1423-1424.

çerçevede incelenmelidir. Özellikle, bir şirketin çevrimiçi oyun hizmeti sunması ve bu platform içerisinde kullanıcıların hesap veya karakterlerinin yetkisiz kişilerce ele geçirilmesi durumunda, bu şirketin sorumluluğu gündeme gelir. TCK madde 246'nın uygulama alanı, eğer bu tür bir olay şirketin yetersiz güvenlik önlemleri veya ihmalden kaynaklanıyorsa, tüzel kişiye yönelik güvenlik tedbirlerinin devreye sokulmasını mümkün kılar.<sup>160</sup>

Bu çerçevede, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, modern hukuk sistemlerinde genellikle 'hırsızlık' kategorisine girmemekle birlikte, bilişim suçları arasında değerlendirilir. Bu tür eylemler, kişilerin mülkiyet haklarını dijital ortamda ihlal etmektedir ve bu nedenle ciddi yasal sonuçlar doğurabilir. Ancak, mevcut yasaların bu tür suçlara özgü detayları kapsayacak şekilde güncellenmesi gerekmektedir. TCK madde 246 gibi maddeler, tüzel kişiliklere yönelik sorumlulukları netleştirse de çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesine özel olarak odaklanan yasal düzenlemelerin eksikliği, bu alandaki yasal boşlukları işaret etmektedir.

TCK madde 246'nın sağladığı güvenlik tedbirleri, tüzel kişiliklerin bilişim suçlarına karşı korunmasında önemli bir role sahiptir. Ancak, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi gibi modern bilişim suçlarına özel düzenlemelerin yapılması ve mevcut yasaların bu tür suçlara uygun şekilde güncellenmesi gerekmektedir. Bu hem bireylerin hem de tüzel kişiliklerin dijital ortamda daha güvenli bir şekilde faaliyet göstermelerini sağlayacak, aynı zamanda bilişim suçlarına karşı daha etkili bir mücadele ortamı oluşturacaktır.

#### **4.2.6. Madde 142/2/e: Nitelikli Hırsızlık/Bilişim Sistemlerinin Kullanılması Suretiyle**

TCK madde 142/2/e kapsamında tanımlanan "Nitelikli Hırsızlık/Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık" suçu, hukukun dijitalleşen dünyaya adaptasyonunun bir yansıması olarak değerlendirilebilir. Bu suç tipi, bilişim sistemlerinin, yani internet üzerinden erişilebilen her türlü elektronik veri işleme ve

---

<sup>160</sup>Erdoğan, a.g.e., s. 1425.

saklama sistemlerinin, hukuka aykırı şekilde kullanılarak bir kişinin başkasına ait malvarlığı değerlerini elde etmesini kapsar. Özellikle internet bankacılığı, elektronik ticaret platformları gibi sistemler üzerinden gerçekleştirilen izinsiz transferler ve benzeri eylemler, modern hırsızlık yöntemleri olarak kabul edilir. Günümüzde bilişim teknolojileri ve internetin yaygınlaşmasıyla birlikte, hırsızlık suçunun işlenme yöntemleri de çeşitlenmiştir. Dolayısıyla, hukuk sistemleri de bu yeni suç tiplerine karşı yaptırımlarını güncellemiş ve ağırlaştırmıştır. Nitelikli hırsızlık suçu, bu yeni suç tiplerine verilecek cezai yaptırımların ağırlığını belirleyen önemli bir kriter haline gelmiştir. Bilişim sistemlerinin kullanılması suretiyle işlenen hırsızlık suçları, geleneksel hırsızlık suçlarına göre daha geniş bir mağdur kitlesine ulaşabilme potansiyeline sahiptir ve bu suçların işlenme hızı da geleneksel yöntemlere göre çok daha yüksektir. Bu nedenlerle, bilişim sistemleri aracılığıyla işlenen hırsızlık suçlarına karşı daha caydırıcı cezai yaptırımların uygulanması gerekliliği ortaya çıkmıştır.<sup>161</sup>

Bu bağlamda, çevrimiçi oyun hesaplarının ve oyun içi karakterlerin izinsiz olarak ele geçirilmesi eylemi de nitelikli hırsızlık suçu kapsamında değerlendirilmelidir. Çünkü çevrimiçi oyun hesapları ve karakterleri, özellikle oyun içi satın almalar ve karakter gelişimine yapılan yatırımlar göz önünde bulundurulduğunda, gerçek malvarlığı değerleri içerir. Oyun içi eşyalar, karakterler veya hesaplar üzerindeki kontrolün, bilişim sistemleri aracılığıyla yetkisiz kişiler tarafından ele geçirilmesi, hukuka aykırı bir malvarlığı devrine ve dolayısıyla nitelikli hırsızlık suçunun işlenmesine yol açar. Ancak, bu tür hırsızlık olaylarının nitelikli hırsızlık suçu olarak değerlendirilebilmesi için, çevrimiçi oyun hesaplarının ve oyun içi karakterlerin "malvarlığı değeri"<sup>162</sup> taşıdığının hukuki olarak kabul edilmesi gerekmektedir. Mevcut hukuk sistemlerinin çoğu, fiziksel olmayan varlıkların malvarlığı değeri taşıyıp taşımadığı konusunda net bir ayırım yapmamaktadır. Bu durum, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesinin, nitelikli hırsızlık kapsamında değerlendirilip değerlendirilemeyeceği konusunda belirsizliklere neden olmaktadır.

---

<sup>161</sup>E. Şen, 'Hırsızlık Suçları', *Ankara Barosu Dergisi*, sayı: 3, 2012, s. 323-324.

<sup>162</sup>S. Yılmaz, 'Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu', *Ankara Barosu Dergisi*, sayı: 2, 2011, s. 79.

Dijital para<sup>163</sup> birimleri veya oyun içi satın alımlar, kullanıcıların gerçek dünya kaynaklarını, zamanlarını ve emeklerini harcayarak elde ettikleri değerlerdir. Bu varlıklar, fiziksel olmasalar da sahipleri için önemli bir ekonomik ve duygusal değere sahiptir. Dolayısıyla, bu varlıkların izinsiz olarak ele geçirilmesi, sadece dijital bir kaybı değil, aynı zamanda gerçek dünya emeğinin ve yatırımının da kaybını ifade eder. Bu nedenle, dijital dünyada gerçekleşen hırsızlık eylemlerinin, fiziksel dünyadaki hırsızlık eylemleriyle eş değer olarak görülmesi ve buna göre cezalandırılması gerekmektedir. Bilişim sistemleri aracılığıyla işlenen hırsızlık suçlarının tanımı, dijital varlıkların da malvarlığı değeri taşıdığını kabul edecek şekilde genişletilmeli ve netleştirilmelidir. Bu hem mevcut yasal boşlukların doldurulması hem de çevrimiçi ortamlarda gerçekleşen ekonomik aktivitelerin korunması açısından kritik öneme sahiptir. Dijital ortamlarda gerçekleştirilen hırsızlık eylemlerine karşı uygulanacak hukuki yaptırımların belirlenmesi, bu tür suçların önlenmesinde etkili bir araç olacaktır. Bu suç türünde korunan hukuki yarar, bireylerin ve kurumların mali varlıklarının güvenliğidir. Bilişim sistemleri aracılığıyla yapılan hırsızlık eylemleri, bu varlıkların bütünlüğünü ve güvenliğini tehdit eder. Bu tür suçlar, bireylerin mali güvenliğini doğrudan etkileyebilecek ve geniş çapta maddi zararlara neden olabilecek potansiyel taşır. Madde 142/2/e'nin temel gerekçesi (TCK mad. 142'nin ikinci fıkrası) bilişim sistemlerinin hırsızlık amacıyla kötüye kullanılmasını önlemek ve bu yolla bireylerin mali güvenliğini korumaktır. Bilişim sistemlerinin hızla geliştiği ve yaygınlaştığı günümüzde, bu tür sistemlerin güvenliğinin sağlanması, mali suçlarla mücadelede hayati önem taşır. Bilişim sistemleri aracılığıyla gerçekleştirilen hırsızlık eylemleri, geleneksel hırsızlık suçlarına göre daha geniş çapta etkiler yaratabilir ve daha zor tespit edilebilir, bu nedenle bu suç türüne özel düzenlemeler ve caydırıcı cezalar getirilmiştir. Madde 142/2/e (TCK md.142'nin 2.fıkrası) genel bir suç tanımı sağlamakla birlikte, özellikle bilişim sistemleri kullanılarak yapılan hırsızlık eylemlerini kapsayan tamamlayıcı bir suç niteliğindedir. Bu madde, diğer hırsızlık suçlarının yanı sıra, özel olarak bilişim sistemlerinin kullanıldığı durumları ele alır ve bu suçların başka suçlarla birlikte işlenip işlenmediğini değerlendirirken önemli bir hukuki dayanak sunar.

---

<sup>163</sup>M. Çatlı ve S. Şimşek, 'Dijital Para ve Egemenlik', *Türkiye Adalet Akademisi Dergisi*, cilt: 12, Sayı: 48, 2021, s. 151-184.

Ayrıca, dijital dünyada gerçekleşen hırsızlık eylemlerine karşı mücadelede, bilişim suçlarına özgü araştırma ve takip yöntemlerinin geliştirilmesi, uluslararası iş birliğinin güçlendirilmesi ve bilişim suçlarıyla mücadelede uzmanlaşmış birimlerin kurulması gibi adımlar da önem taşımaktadır. Bilişim suçlarına özgü zorluklar, geleneksel hırsızlık suçlarından farklı olduğundan, bu suçlarla mücadelede özel yetkinlik ve teknolojilere ihtiyaç duyulmaktadır. Çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz olarak ele geçirilmesi, modern toplumun karşı karşıya olduğu önemli bir hukuki ve etik sorundur. Dijital ortamdaki malvarlığı değerlerinin korunması, hukuk sisteminin güncellenmesi ve bilişim teknolojilerine özgü suçlarla mücadele yöntemlerinin geliştirilmesi gerektiğini ortaya koymaktadır. Bu tür suçların etkin bir şekilde önlenmesi ve cezalandırılması, dijital dünyada güvenliğin ve adaletin sağlanması için elzemdir.

#### **4.2.7. TCK Madde 158 Nitelikli Dolandırıcılık 1.Fıkrasının f Bendi Bilişim Sistemlerinin, Banka veya Kredi Kurumlarının Araç Olarak Kullanılması Suretiyle**

TCK madde 158/1/fnin hükümleri, çağımızın suç şekillerinden biri olan ve teknolojinin getirdiği imkanlarla gerçekleştirilen dolandırıcılık eylemlerine özel bir önem atfetmektedir. Bu madde, bilişim sistemlerinin veya banka ve kredi kurumlarının dolandırıcılık amacıyla araç olarak kullanılmasını, suçun nitelikli hallerinden biri olarak tanımlamaktadır. Bu tanım, teknolojinin hızla geliştiği ve bilişim sistemlerinin hayatımızın her alanına nüfuz ettiği günümüzde, dolandırıcılık suçlarının da bu sistemler üzerinden işlenmesine yönelik ciddi bir yasal müeyyideyi içermektedir. Böylece, internet üzerinden sahte bir web sitesi kurarak insanlardan kredi kartı bilgilerini alıp bu bilgileri yasadışı amaçlarla kullanma gibi eylemler, bu madde kapsamında değerlendirilir.<sup>164</sup> Nitelikli dolandırıcılık kapsamında değerlendirilen eylemler, sadece finansal bilgilerin çalınmasıyla sınırlı kalmamakta, aynı zamanda kişisel verilerin izinsiz kullanımı, sahte kimlik oluşturma ve bu kimlikler üzerinden dolandırıcılık yapma gibi geniş bir yelpazeyi kapsamaktadır. Bu suçların işleniş

---

<sup>164</sup>F. Korkmaz, ‘Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi’, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 69 sayı: 3, 2020, s. 1423-1424.

biçiminde, bilişim sistemlerinin ve banka veya kredi kurumlarının, dolandırıcılık faaliyetlerini kolaylaştıran bir araç olarak kullanılması esastır. Dolandırıcılar, teknolojinin sunduğu anonimlik<sup>165</sup> ve hızdan faydalanarak, geleneksel dolandırıcılık yöntemlerine kıyasla çok daha geniş bir hedef kitleye ulaşabilmekte ve bu sayede suçun etki alanını genişletebilmektedir.

Bu suç türünde korunan hukuki yarar, bireylerin ve kurumların finansal güvenliği ve mali bütünlüğüdür. Bilişim sistemleri veya banka/kredi kurumlarının dolandırıcılık amacıyla kullanılması, geniş çapta maddi kayıplara ve finansal istikrarsızlığa neden olabilir. Bu tür dolandırıcılık eylemleri, finansal sistemin güvenilirliğine zarar verir ve bireylerin ekonomik haklarını tehdit eder. Madde 158/1/f'nin temel gerekçesi, finansal sistemlerin ve bilişim altyapısının dolandırıcılık amacıyla kötüye kullanılmasını önlemektir. Finansal işlemlerin dijitalleşmesi, dolandırıcıların yeni yöntemlerle suç işlemelerine olanak tanıdığından, bu tür suçlara karşı etkin mücadele ve caydırıcı cezaların uygulanması zorunluluktur. Yasal düzenlemeler, bilişim sistemlerinin ve finansal altyapının korunmasını sağlayarak, dolandırıcılık suçlarının önüne geçmeyi amaçlar. Madde 158/1/f, genel bir suç tanımı sağlamakla birlikte, özellikle finansal altyapı ve bilişim sistemlerinin dolandırıcılık amacıyla kullanılması durumlarını kapsayan tamamlayıcı bir suç niteliğindedir. Bu madde, dolandırıcılık suçlarının diğer formlarıyla birlikte değerlendirildiğinde, finansal dolandırıcılık eylemlerinin daha geniş bir yelpazede incelenmesine olanak tanır ve bu suçların başka hukuki maddelerle birlikte işlenip işlenmediğini belirlerken önemli bir hukuki dayanak sunar.

Çevrimiçi oyun hesaplarının ve oyun karakterlerinin ele geçirilmesi, günümüzde ciddi bir sorun haline gelmiştir ve bu tür eylemler, hırsızlık ve dolandırıcılık suçlarıyla yakından ilişkilidir. Oyun içi varlıkların ve karakterlerin, gerçek dünya değerine sahip olması, bu alanı dolandırıcılar için cazip bir hedef haline getirmiştir. Çevrimiçi oyun hesaplarının ele geçirilmesi, kullanıcı adı ve şifre bilgilerinin çalınması veya sosyal mühendislik yoluyla elde edilmesi gibi yöntemlerle gerçekleştirilebilir. Bu hesapların ele geçirilmesi ve kontrolünün başka bir kişiye aktarılması, maddi değer taşıyan oyun içi varlıkların izinsiz bir şekilde kullanılması

---

<sup>165</sup>S. Kaya, 'Sosyal Medyada Anonim Olmanın Söylemler Üzerindeki Etkisinin Haber Yorumları Üzerinden İncelenmesi', *İletişim Kuram ve Araştırma Dergisi*, sayı: 60, 2022, s. 169-171.

anlamına gelir. Bu durum, TCK madde 158/1/f kapsamında değerlendirildiğinde, bilişim sistemlerini kullanarak dolandırıcılık yapmanın nitelikli hallerinden biri olarak görülebilir. Çünkü bu tür eylemler, bilişim sistemlerinin dolandırıcılık amacıyla araç olarak kullanılması ve maddi değer taşıyan dijital varlıkların izinsiz kullanımıyla doğrudan ilişkilidir. Ancak, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi durumunun tam olarak nitelikli dolandırıcılık suçu kapsamına girip girmediği, mevcut yasal tanımların ve hukuki yorumların sınırları içinde tartışmalı bir konu olabilir. Bilişim sistemlerinin kullanımı, dolandırıcıların mağdurları yüz yüze gelmeden aldatmalarını mümkün kılar. Dolandırıcılar genellikle, mağdurların güven duyduğu ve tanıdık bildikleri platformları hedef alır. Örneğin, bir çevrimiçi oyun platformunda bir kullanıcının hesap bilgileri phishing saldırıları yoluyla ele geçirilebilir. Burada dolandırıcı sahte bir güvenlik uyarısı veya güncelleme talebi yollayarak kullanıcıdan hassas bilgilerini (kullanıcı adı, şifre vb.) tekrar girmesini isteyebilir. Kullanıcı bu talebi meşru bir istek olarak algıladığında bilgilerini dolandırıcıya teslim etmiş olur.<sup>166</sup> Dolandırıcılık suçunun bu yöntemi diğer suç türlerinden ayrılan bazı özelliklere sahiptir. Öncelikle dolandırıcılık suçunda mağdurun malvarlığına zarar verme niyeti ve bu zararın mağdurun rızası ile gerçekleşmesi gereklidir. İkincil olarak bilişim sistemlerinin kullanılması, dolandırıcının kimliğini gizleyerek faaliyetlerini daha da gizli bir hale getirir. Bu durum suçun tespit edilmesini ve faillerin adalete teslim edilmesini zorlaştıran bir faktördür.

Bu suç türüyle mücadele etmek, sadece yasal düzenlemelerin güncellenmesiyle sınırlı kalmamalı, aynı zamanda bilişim suçlarına özgü yeni soruşturma yöntemleri ve tekniklerin geliştirilmesini de içermelidir. Örneğin, çevrimiçi platformlar kullanıcılarının güvenliğini artırmak için iki faktörlü kimlik doğrulama gibi güvenlik önlemlerini standart hale getirebilir. Ayrıca bu tür suçların izini sürmek ve failleri tespit etmek için daha sofistike veri analizi yöntemleri ve yapay zekâ teknolojilerinden yararlanılabilir.

Çevrimiçi oyun hesaplarının ele geçirilmesi gibi dolandırıcılık suçları hem bilişim teknolojilerinin ilerlemesiyle birlikte evrilmekte hem de yeni yasal ve teknik

---

<sup>166</sup>Korkmaz, a.g.e., s. 1427.

mücadele stratejilerini zorunlu kılmaktadır. Bu tür eylemlerin nitelikli dolandırıcılık olarak değerlendirilebilmesi için, yasal düzenlemelerde daha açık tanımlamalara ve özellikle çevrimiçi oyun varlıklarının hukuki statüsüne ilişkin net bir çerçeveye ihtiyaç duyulmaktadır. Dolandırıcılık suçunun bu yeni formunun hukuki olarak tanınması ve cezalandırılması, teknolojinin getirdiği yeni suç biçimlerine karşı etkili bir mücadele stratejisinin oluşturulmasında kritik bir öneme sahiptir. Bu bağlamda, mevcut yasal düzenlemelerin bu tür modern dolandırıcılık yöntemlerini kapsayacak şekilde güncellenmesi, suçla mücadelede önemli bir adım olacaktır.

#### **4.2.8. TCK Madde 228/3: Kumar Oynanması İçin Yer ve İmkân Sağlama / Suçun Bilişim Sistemleri Kullanılması Suretiyle İşlenmesi**

TCK madde 228/3, Türk Ceza Kanunu içinde spesifik olarak kumar oynanması için yer ve imkân sağlama suçunu ele alır. Bu madde, kumarın fiziksel veya dijital ortamlarda teşvik edilmesini ve kolaylaştırılmasını cezalandırmayı amaçlar. Ancak, çevrimiçi oyun hesapları ve karakterlerinin izinsiz olarak ele geçirilmesi, ilk bakışta TCK madde 228/3'ün doğrudan kapsamı dışında gibi görünebilir. Bu tür eylemler, genellikle bilişim sistemlerini kullanarak yapılan hırsızlık, dolandırıcılık veya mala zarar verme gibi farklı suç tipleri altında değerlendirilir.<sup>167</sup> Buna rağmen, bilişim sistemleri aracılığıyla işlenen suçların geniş yelpazesi göz önüne alındığında, dijital ortamlarda kumar oynanmasını kolaylaştıran platformlar aracılığıyla, dolaylı yoldan çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi ve bu varlıkların kumar oyunlarında kullanılması durumları TCK madde 228/3 ile ilişkilendirilebilir. Bu, özellikle çevrimiçi oyunlar içindeki varlıkların, gerçek para değeri taşıyan ve kumar oyunlarında kullanılabilen dijital mülkiyet olarak kabul edilmesi durumunda daha da belirginleşir. Ancak, bu tür bir uygulamanın gerçekleştirilmesi için mevcut yasal tanımların genişletilmesi ve güncellenmesi gerekmektedir.

Çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz olarak ele geçirilmesi eylemi, bilişim suçları kapsamında değerlendirildiğinde, bu suç tiplerinin tanımlarının ve yasal yaptırımlarının netleştirilmesi gerektiği ortaya çıkar. Bu bağlamda, TCK

---

<sup>167</sup>B. Babayiğit, 'Kumar Oynama ve Kumar Oynanması İçin Yer ve İmkân Sağlama Fiilleri', *Türkiye Adalet Akademisi Dergisi*, sayı: 34, 2018, s. 309.

madde 228/3'ün doğrudan uygulanabilirliği olmasa da dijital mülkiyetin korunması ve çevrimiçi ortamlardaki suçlarla mücadele bağlamında yasal çerçevenin genişletilmesi ve derinleştirilmesi ihtiyacı bulunmaktadır. Çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz olarak ele geçirilmesi, mevcut yasal düzenlemeler çerçevesinde doğrudan TCK madde 228/3 altında değerlendirilemese de bu eylemlerin dijital mülkiyetin izinsiz ele geçirilmesi ve bilişim suçları kapsamında ele alınması gerektiğini vurgular. Bu durum, Türk Ceza Kanunu ve ilgili yasal mevzuatta dijital mülkiyetin korunmasına yönelik açık tanımların ve yaptırımların oluşturulmasını zorunlu kılar.<sup>168</sup> Dolayısıyla, çevrimiçi oyun hesapları ve karakterlerinin korunması, mevcut yasal çerçevenin genişletilmesi, suçun nitelikli halinin bilişim sistemleri ile tanımlanması ve teknolojik gelişmelere uygun hale getirilmesi ile mümkün olacaktır.

#### **4.3. Hukuki Yaptırımlar ve Cezai Müeyyideler**

Bilişim suçları, günümüzde teknolojinin hızla gelişimi ile paralel olarak artan bir suç türüdür ve çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi bu kapsamda değerlendirilen suçlar arasında yer alır. Bu tür olaylar, bilişim sistemlerine izinsiz erişim, verileri hukuka aykırı olarak ele geçirme veya yok etme gibi faaliyetleri içerir ve TCK madde 243 altında suç teşkil eder. Bilişim suçlarına ilişkin hukuki çerçeve, mağdurların haklarını korumayı ve suçlulara karşı etkin bir mücadele yöntemi geliştirmeyi amaçlar.

Yargıtay 13. Ceza Dairesi'nin 08.1.2020 tarihli kararında<sup>169</sup> 2019/9265 Esas, 2020/258 Karar sayılı hükmünde, internet ortamında oynanan bir oyun içindeki karakterin hukuka aykırı şekilde ele geçirilmesi vakası ele alınmıştır. Kararda, mağdurun oyun karakterinin ele geçirilmesi eylemi dolayısıyla sanığın hırsızlık suçundan beraatine karar verilmesi yerine, oyun karakterinin ekonomik bir değere sahip olmasına rağmen taşınır mal niteliği taşımadığı, ancak alınıp satılabilen ve maddi değere sahip bir veri olarak kabul edilmesi gerektiği vurgulanmıştır. Bu bağlamda, sanığın eyleminin TCK madde 244 ikinci fıkrasında tanımlanan “var olan verileri başka bir yere gönderme” ve dördüncü fıkrasında belirtilen “haksız bir çıkar sağlama”

---

<sup>168</sup>Babayiğit, a.g.e., s. 299.

<sup>169</sup>Yargıtay 13. Ceza Dairesi, E.2019/9265, K.2020/258

hareketlerinden birini oluşturduğu ve dolayısıyla bilişim suçu teşkil ettiği sonucuna varılmıştır. Yüksek Mahkeme'nin bu kararı, sanal oyun karakterlerinin ve diğer sanal mülklerin, hukuka aykırı olarak ele geçirilmesinin, TCK madde 142/2-e'de düzenlenen bilişim suretiyle hırsızlık olarak değil, aynı Kanun'un 244/4 maddesinde düzenlenen verileri hukuka aykırı olarak ele geçirme suçu kapsamında değerlendirilmesi gerektiğine işaret etmektedir. Bu yaklaşım, çevrimiçi oyun hesaplarının izinsiz ele geçirilmesi gibi eylemlerin, ekonomik değeri olan verilerin izinsiz olarak ele geçirilmesi veya değiştirilmesi şeklinde bilişim suçları kapsamında değerlendirilmesini sağlamakta, çevrimiçi oyunlar ve sanal mülklerin hukuki zemindeki yerini güçlendirmekte ve bilişim suçlarına karşı mücadelede önemli bir adım olarak kabul edilmektedir.<sup>170</sup> Bu içtihat gibi verilmesini destekleyeceğimiz kararlar sanal dünyada gerçekleştirilen eylemlerin somut dünyadaki hukuki sonuçlar doğurabileceğini ve modern hukukun bu yeni gerçekliklere nasıl yanıt verdiğini göstermektedir.

Çevrimiçi oyunlarda karakterlerin ele geçirilmesi, fiziki mülkiyetin çalınmasıyla karşılaştırıldığında, hukukun dijital varlıklara yönelik yaklaşımının önemli ölçüde farklılaşması gerektiğini ortaya koyar. Fiziki mülkiyetin çalınması, somut varlıkların hukuka aykırı olarak bir kişiden diğerine geçişini ifade ederken, dijital mülkiyetin, özellikle çevrimiçi oyun karakterleri gibi, ele geçirilmesi durumunda ise, maddi olmayan varlıkların izinsiz el değiştirmesi söz konusudur.

Dijital mülkiyetin özgül doğası, onun ekonomik değer taşımasına rağmen fiziki bir varlık olmamasını içerir; bu da hukukun, dijital mülkiyetin korunması konusunda yeni mekanizmalar geliştirmesini gerektirir. TCK madde 244'e göre, çevrimiçi oyun karakterlerinin izinsiz ele geçirilmesi, verileri hukuka aykırı olarak ele geçirme suçu olarak değerlendirilmelidir. Bu, oyun karakterlerinin sadece oyun içinde değil, gerçek dünyada da ekonomik değer taşıdığı ve bu nedenle korunması gerektiği anlayışını yansıtır. Fiziki ve dijital mülkiyet arasındaki bu temel farklılık, hukukun dijital çağın gereksinimlerine uyum sağlaması ve dijital varlıkların izinsiz kullanımını caydırıcı bir şekilde ele alması gerekliliğini gösterir. Çevrimiçi oyunlardaki karakterlerin ele geçirilmesinin, bilişim suçları çerçevesinde değerlendirilerek, hem bireylerin dijital

---

<sup>170</sup>Yargıtay 13. Ceza Dairesi, E.2016/2155, K.2017/10403

mülkiyet haklarının korunması hem de dijital ekonominin sağlıklı bir şekilde işleyişi için gerekli hukuki düzenlemelerin yapılması zorunludur. Bu yaklaşım, dijital varlıkların benzersiz doğasını tanıyarak, onlara uygun hukuki koruma sağlamayı amaçlar ve böylece fiziki ve dijital mülkiyet arasındaki karşılaştırmalı analiz, hukukun dijital çağdaki evrimini teşvik eder.

Bilişim teknolojilerinin hayatımıza entegre olmasıyla birlikte, çevrimiçi oyunlar günlük yaşantımızın ayrılmaz bir parçası haline gelmiştir. Bu oyunlar, sadece eğlence amaçlı değil, aynı zamanda sosyal bir etkileşim ve ekonomik bir değer taşıyan platformlar olarak da önem kazanmıştır. Oyun içerisinde elde edilen karakterler ve sanal eşyalar, zaman ve emek harcanarak kazanıldığı için gerçek ekonomik değerler ifade edebilir. Bu durum, çevrimiçi oyunlar içerisinde gerçekleştirilen hırsızlık ve dolandırıcılık eylemlerinin, fiziki dünyadaki suçlarla benzer yasal sonuçlar doğurmasına yol açmıştır.<sup>171</sup> TCK madde 245/A bilişim sistemlerine yönelik suçlarla mücadelede önemli bir araç olarak karşımıza çıkmaktadır. Çevrimiçi oyunlarda çalınan karakterler veya sanal eşyalar, somut varlıklar olarak değerlendirilmesi ve mülkiyet hakkına dayandırılması gereken önemli bir hukuki meseledir. Bu bağlamda, Kişisel Verilerin Korunması Kanunu'nda (KVKK) soyut verilerin korunması ve kişilik haklarının güvence altına alınması gibi prensipler dikkate alındığında, bilgisayar ortamında yaratılan sanal varlıkların da benzer bir korumaya tabi tutulması gerektiği ortaya çıkmaktadır. Nitekim, bilgisayar sistemlerinden elde edilen veriler nasıl kişisel haklar çerçevesinde korunuyorsa, sanal karakterler ve eşyalar da bu kapsamda değerlendirilmelidir. Burada karşılaşılan en büyük engel, hukuki düzenlemelerde ve toplumsal algıda sanal varlıklara yönelik geleneksel yaklaşımların aşılması olabilir. Bu, sanal varlıkların somut mülkiyet nesneleri gibi korunmasının önündeki temel psikolojik ve hukuki engelleri belirlemekte ve bu engellerin üstesinden gelinmesi için yeni yasal düzenlemelerin yapılmasını zorunlu kılmaktadır.

Çevrimiçi oyunlar içerisinde elde edilen karakterler ve sanal eşyalar, kullanıcılar tarafından gerçek para ile satın alınabildiği veya oyun içi etkinliklerle kazanıldığı için, bu varlıkların ekonomik bir değere sahip olduğu açıktır. Dolayısıyla, bu varlıkların izinsiz olarak ele geçirilmesi, sahiplerine maddi zararlar verebilir. Bu

---

<sup>171</sup>H. Demir, 'Bilişim Suçları Uygulamaları', *Ankara Batı Adliyesi Dergisi*, cilt: 4, sayı: 7, Ocak-Haziran 2022, s. 14.

bağlamda, çevrimiçi oyun içerisinde çalınan karakter veya sanal eşyaların, fiziki olmayan varlıklar olmalarına rağmen, maddi bir değer taşıdığı ve bu sebeple cezai yaptırımlara tabi tutulabileceği görüşü giderek kabul görmektedir. TCK madde 158/1/f kapsamında bilişim sistemlerinin kullanılması suretiyle işlenen dolandırıcılık ve TCK madde 142/2/e kapsamında hırsızlık suçları nitelikli suçlar olarak kabul edilmekte ve bu suçlar için ağır cezai yaptırımlar öngörülmektedir. Ancak, çevrimiçi oyun içerisinde çalınan karakter veya sanal eşyaların hukuki statüsünün net bir şekilde tanımlanması ve bu suçlar için spesifik yasal düzenlemelerin yapılması, hukuk sistemimizde henüz tam anlamıyla gerçekleşmemiştir. Bu nedenle, yargı organları, mevcut yasal çerçeve içerisinde bu tür suçlara ilişkin kararlar verirken, somut olayın koşullarını ve sanal varlıkların ekonomik değerini dikkate alarak değerlendirme yapmaktadır.

Çevrimiçi oyunlar içerisinde işlenen suçlara yönelik cezai müeyyidelerin belirlenmesinde, sanal varlıkların gerçek ekonomik değerlerinin yanı sıra, bu suçların bireyler üzerindeki psikolojik ve sosyal etkileri de göz önünde bulundurulmalıdır. Çünkü, çevrimiçi oyunlar sadece maddi bir yatırım değil, aynı zamanda oyuncuların zaman ve duygusal bağlılıklarını da içermektedir. Bu sebeple, çevrimiçi oyunlar içerisinde çalınan karakter veya sanal eşyaların cezai müeyyidelerinin belirlenmesi, sadece maddi zararların tazmininden daha geniş bir perspektifi kapsamalıdır. Bu bağlamda, bilişim suçlarına yönelik mevcut yasal düzenlemelerin güncellenmesi ve bu tür suçlara özgü cezai yaptırımların geliştirilmesi, dijital çağda bireylerin haklarının korunması için önemli bir adımdır. Bu süreçte, hukukçular, yargı organları ve yasama organlarının, teknolojik gelişmeleri yakından takip ederek, çevrimiçi oyunlar gibi dijital platformlarda güvenliği sağlamak ve bilişim suçlarıyla etkin bir şekilde mücadele etmek için iş birliği içerisinde çalışmaları gerekmektedir.

#### **4.4. Soruşturma ve Kovuşturma Aşamasında İspat Sorunu**

Sübut, hukukun temel kavramlarından biri olarak iddia edilen bir durumun doğruluğunu delillerle ortaya koyma sürecidir. Bu süreç, medeni usul hukukunda özellikle önem arz eder ve tarafların, hâkim önünde iddia ve savunmalarına dayanak teşkil eden vakıaların doğruluğunu ispatlama çabasını içerir. Genel anlamda sübut; tarafların, bir uyuşmazlık konusu olan maddi vakıaların gerçekliğini, hâkimde uygun

bir kanaat oluřturacak řekilde, delil, karine ve hukuki argümanlar sunarak göstermeleri sürecidir. Hukuk davalarında ispatın amacı, dava konusu uyuzmazlıęa iliřkin, hâkimin bilgisi dıřında kalan ve davadan önce gerçekteřen vakıaların doęruluęu konusunda hâkimde bir kanaat oluřturmaadır. Bu örneęin, çevrimiçi oyunlarda karakter ve sanal eřyaların izinsiz ele geçirilmesi gibi biliřim suçları bağlamında büyük bir meydan okumayı temsil eder. Fiziki suçlara kıyasla, dijital ortamda gerçekteřen bu tür suçlarda delillerin toplanması, korunması ve sunulması, dijital ortamın soyut ve karmařık yapısı nedeniyle zorlařmaktadır.<sup>172</sup> Dijital ortamda suçların doęası gereęi, delillere ulařma süreci fiziki suçlara kıyasla çok daha karmařık ve zorlayıcıdır. Öncelikle, dijital delillerin soyut ve deęiřken yapısı, bu tür delillerin toplanmasını, korunmasını ve adli süreçlerde kullanılmasını zorlařtırır. Dijital deliller, sıklıkla elektronik verilerin geçici ve kolayca deęiřtirilebilir olması sebebiyle, koruma ve doęrulama gereksinimlerini artırır. Bir dięer zorluk, dijital suç mahallinin genellikle sanal olması ve fiziksel bir konumla sınırlı olmamasıdır. Bu durum, suçun iřlendięi yeri tespit etmeyi ve delilleri somutlařtırmayı zorlařtırır. Dijital deliller genellikle hızla yok edilebilir veya manipüle edilebilir, bu da delil toplama sürecinin sadece hızlı deęil, aynı zamanda dikkatli bir řekilde yürütölmesini gerektirir. Ayrıca, dijital delillerin doęası gereęi gecikmesinde sakınca bulunan hallerin sürekli var oluřu, koruma tedbirlerinin yetersiz kalabileceęini de göstermektedir. Bu sebeple, hâkim kararı öncesi süreçte alınacak koruma tedbirleri, delillerin deęiřtirilmesine veya yok edilmesine karřı yeterince etkili olmayabilir. Dijital delillerin korunması ve doęruluklarının sürdürölabilirlięi, hukuk sistemlerinde önemli ve acil bir yeniden deęerlendirmeyi gerektirmektedir. Üstelik, dijital ortamda iřlenen suçlar genellikle uluslararası sınırları ařabilir. Bu, farklı yargı bölgeleri arasında iř birlięi ve koordinasyon ihtiyacını doęurur, ancak bu süreç çeřitli hukuki ve pratik engellere tabidir. Yargı alanları ve veri koruma yasaları arasındaki farklılıklar, delil toplama ve paylařma sürecini karmařıklařtırabilir.

Çevrimiçi oyun platformlarında yařanan hırsızlık ve dolandırıcılık vakaları, mülkiyetin ve izinsiz transferin somut fiziki delillere dayanmaması nedeniyle, adli makamlar için ciddi bir ispat problemi oluřturur. Bu tür suçların soruřturulması ve kovuřturulması sırasında, sanal varlıkların mülkiyetine dair kanıtların sunulması,

---

<sup>172</sup>Demir, a.g.e., s. 40.

hukuki süreçlerde yeni yöntemlerin ve yaklaşımların geliştirilmesini gerektirir. Bir hukuk davasında başarı, kanun tarafından kabul edilen koşul vakıalara uygun somut vakıaların ispatına bağlıdır. Ancak, medeni yargıda bir hususun ispatsız kalması, hâkimin hüküm verme zorunluluğunu ortadan kaldırmaz. Bu, özellikle çevrimiçi suçların ispatlanması bağlamında, adli süreçlerde esneklik ve derinlemesine bir dijital bilgi anlayışı gerektiren bir durumdur. Dolayısıyla, hukuk normları, somut olarak gerçekleşmedikçe uygulanmaz ve hukuki sonuç doğmuş sayılmaz. Bu, çevrimiçi oyunlarda karakter ve sanal eşyaların izinsiz ele geçirilmesi gibi durumlar için de geçerlidir; burada ispat, hakkını dayandırdığı vakıaların doğruluğunu göstermek ve adil bir karar elde etmek için kritik öneme sahiptir.<sup>173</sup>

#### **4.4.1. Çevrimiçi ve Fiziki Suçlar Arasındaki İspat Mekanizmalarının Karşılaştırılması**

Fiziki ve çevrimiçi suçların delil toplama süreçleri arasındaki farklar, hem suçun doğasını hem de yargı sürecini derinden etkileyen önemli unsurlardır. Fiziki suçlarda, delil toplama genellikle görgü tanıklarının ifadeleri, video kayıtları, parmak izleri ve DNA gibi somut kanıtlar üzerine kurulurken, çevrimiçi suçlarda bu süreç büyük ölçüde elektronik verilere dayanır. Bu veriler, sunucu logları, IP adresleri, dijital iletişim kayıtları ve kullanıcı aktivite raporları gibi çeşitli kaynaklardan elde edilen bilgilerden oluşur. Bu tür elektronik delillerin toplanması, analizi ve korunması, özel bilgi ve teknik beceri gerektiren karmaşık bir süreçtir. Öte yandan, bir eylemin suç olarak tanımlanabilmesi için yasal bir temele sahip olması gerektiği, ceza hukukunun temel ilkesidir. TCK md.2’de yer alan kanunilik ilkesine göre, yasanın açıkça suç olarak tanımlamadığı bir eylem için ceza verilemez. Bu, suçun yasal unsuru olarak bilinen ve tipiklik veya kanuni unsur adı verilen ilk suç unsurunun zorunlu bir sonucudur. Buna göre, bir eylemin suç sayılabilmesi için, yasanın özel hükümleri arasında ya da ceza hükümlü özel bir yasada yer alan belli bir maddedeki tanıma uygun olması gerekmektedir. İşlenen eylem ile yasal hüküm arasında bu şekilde bir uygunluk yoksa, eylem kanuni unsur eksikliği nedeniyle suç sayılmayacaktır. Dolayısıyla hem fiziki hem de çevrimiçi suçlarda delil toplama ve suçun yasal tanımının anlaşılması,

---

<sup>173</sup>Demir, a.g.e., s. 41.

adil bir yargılama sürecinin temel taşlarındandır. Bu süreçler, suçun doğasına göre özelleşmiş bilgi ve beceriler gerektirir ve adaletin sağlanmasında kritik bir rol oynar.<sup>174</sup>

Her iki suç türünde de delillerin yasallığı, doğruluğu ve bütünlüğü, suçun ispatı için kritik önem taşır. Ancak, çevrimiçi suçlarda delillerin toplanması, saklanması ve sunulması, fiziki suçlara kıyasla daha karmaşık teknik zorluklar içerir. Çevrimiçi delillerin doğası gereği daha kolay değiştirilebilir veya yok edilebilir olması, bu delillerin korunması ve adil bir yargılama sürecinde kullanılabilmesi için özel önlemler gerektirir. Çevrimiçi ve fiziki suçlar arasındaki ispat mekanizmalarının karşılaştırılması, her iki alanın da kendine özgü zorluklar ve gereksinimler sunduğunu göstermektedir. Fiziki suçlarda somut delillere dayalı geleneksel ispat yöntemleri kullanılırken, çevrimiçi suçlarda elektronik verilerin analizi ve korunması öne çıkar. Her iki durumda da adaletin sağlanabilmesi için delillerin doğru ve adil bir şekilde toplanması, analiz edilmesi ve sunulması esastır.

#### **4.4.2. Çevrimiçi Oyun Platformlarından Toplanan Verilerin Rolü**

Çevrimiçi oyun platformları ve servis sağlayıcıları tarafından toplanan verilerin, sanal hırsızlık veya dolandırıcılık gibi suç soruşturmalarında hayati öneme sahip olduğu bir gerçektir. Bu platformlar, kullanıcıların giriş-çıkış kayıtları, IP adresleri, işlem geçmişi ve etkileşimlerini içeren detaylı veri kümeleri sağlayarak, suçların kanıtlanması ve faillerin tespit edilmesinde kritik bir rol oynar. Ancak, bu verilerin toplanması, saklanması ve işlenmesi, sadece yüksek teknik uzmanlık gerektirmekle kalmaz, aynı zamanda gizlilik ve veri koruma yasalarıyla uyumlu olmayı da zorunlu kılar. 20. yüzyılın ikinci yarısından itibaren gelişen dijital oyun sektörü, oyunların tasarımı ve oynanışı üzerinde önemli bir dönüşüm yaratmış, yeni medyanın hipermetinsellik, etkileşimlilik ve multimedya biçimselliği gibi özellikleriyle dijital oyunları zenginleştirmiştir.<sup>175</sup> Bu gelişmeler, oyun zamanı ve mekanı, oyun oynama eylemi ve geliştirme süreçlerini dönüştürürken, dijital oyunların yaratıcı endüstrilerin bir parçası olarak endüstriyel bir yapı içinde üretilmesi, onları

<sup>174</sup>U. Alacakaptan, *Suçun Unsurları*, Ankara Üniversitesi Hukuk Fakültesi Yayınları No: 372, Ankara, 1975, s. 8.

<sup>175</sup>S. Sezgin, 'Türkiye'de Dijital Oyun Endüstrisi ve Yaratıcı Emek', Doktora Tezi, *Ankara Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2019.

geleneksel oyunlardan ayıran bir özellik olarak öne çıkar. Dolayısıyla, çevrimiçi platformlardan toplanan verilerin kullanımı, dijital çağda suçla mücadelede önemli bir araç haline gelmiş olup, hukuki çerçeveler ve etik standartlarla uyumlu bir şekilde yönetilmesi gerekmektedir.

#### **4.4.3. Çevrimiçi Oyunlarda Veri Manipülasyonu ve Yok Edilmesi**

Sanal suçların soruşturulması ve ispatlanması sürecinde, verilerin manipülasyonu veya yok edilmesi adli süreçlerde karşılaşılan önemli bir engel teşkil etmektedir. Suçlular, izlerini silmek amacıyla teknik yöntemler kullanarak delilleri değiştirebilir veya tamamen ortadan kaldıracırlar. Bu durum, adli makamların elde edilen verilerin kaynağını ve toplanma yöntemlerini dikkatlice incelemesini zorunlu kılar. Çünkü hukuka aykırı yollarla elde edilen veriler, adli süreçlerde delil olarak kabul edilmeyebilir ve böylece geçersiz sayılabilir.

Öte yandan, veri manipülasyonu, verileri daha anlaşılır ve işlenebilir hale getirmek için kullanılan bir düzenleme sürecidir. Bu süreç, çalışan bilgilerinin alfabetik sıralama gibi basit yöntemlerle düzenlenmesinden, web sitesi trafiğinin analizine, muhasebe kayıtlarının düzenlenmesine ve borsa tahminlerine kadar geniş bir yelpazede uygulanabilir.<sup>176</sup> Ancak, adli bağlamda veri manipülasyonu, verilerin gerçekliğini ve bütünlüğünü koruma konusunda hassas bir denge gerektirir. Adli inceleme süreçlerinde, verilerin manipülasyonu sadece meşru ve kabul edilebilir yöntemlerle yapıldığından ve verilerin toplanma sürecinin hukuka uygun olduğundan emin olmak adli makamlar için hayati önem taşır. Bu, veri manipülasyonunun adli süreçlerde delil olarak kabul edilebilirliğini sağlamak için titizlikle yönetilmesi gerektiğini vurgular.

Veri manipülasyonu, veriler üzerinde yapılan değişiklikler, güncellemeler veya yeniden düzenlemeleri ifade eder ve çevrimiçi oyunlarda hem olumlu hem de olumsuz amaçlarla uygulanabilir. Pozitif yönlerden biri, oyun deneyimini geliştirmek ve oyun içi dengeleri sağlamaktır. Örneğin, geliştiriciler oyuncu davranış verilerini analiz ederek oyun mekaniklerini, öge dengelerini veya zorluk seviyelerini ayarlayabilirler.

---

<sup>176</sup>www.questionpro.com, ‘Veri Manipülasyonu Nedir? Teknikler ve Örnekler’, E.T: 22 Ocak 2024.

Bu, oyunun daha adil ve eğlenceli hale gelmesini sağlar. Öte yandan, veri manipölasyonu ve yok edilmesi, hile yapma veya oyunun adil oynanışını bozma niyetiyle de kullanılabilir. Hileciler oyunun kodunu değiştirebilir, oyun içi kaynakları arttırabilir veya rakiplerine karşı haksız avantajlar elde edebilirler. Bu tür manipölasyonlar oyunun bütünlüğünü bozar ve diğer oyuncuların deneyimini olumsuz etkiler.

Veri yok edilmesi ise, genellikle hile yapma veya oyun içi ekonomiyi bozma girişimleri sırasında ortaya çıkar. Örneğin, bir hileci, oyun içi nesnelerin veya kaynakların izlerini silmek için veri tabanındaki kayıtları silebilir. Bu tür faaliyetler, oyunun dengesini bozabilir ve diğer oyuncular için adaletsiz bir oyun ortamı oluşturabilir. Çevrimiçi oyunlarda veri manipölasyonu ve yok edilmesiyle mücadele etmek için geliştiriciler, çeşitli güvenlik önlemleri ve izleme sistemleri kullanır. Bu sistemler, anormal veri değişikliklerini, oyuncu istatistiklerindeki şüpheli sapmaları tespit edebilir ve hile yapma girişimlerine karşı proaktif tedbirler alabilir. Ayrıca, oyun geliştiricileri düzenli güncellemeler<sup>177</sup> ve yama notları<sup>178</sup> aracılığıyla güvenlik açıklarını kapatır ve hile programlarının oyun üzerindeki etkisini azaltır. Çevrimiçi oyunlarda veri manipölasyonu ve yok edilmesi hem geliştiriciler hem de oyuncular için önemli bir konudur. Geliştiricilerin oyunun adil ve eğlenceli kalmasını sağlamak için bu tür faaliyetlere karşı dikkatli olmaları ve etkili önlemler alması gerekmektedir.

#### 4.4.4. Çözüm Önerileri

Çevrimiçi oyun suçlarının soruşturma ve kovuşturma aşamalarında karşılaşılan ispat sorunlarının üstesinden gelmek için hem ulusal hem de uluslararası düzeyde bütüncül stratejiler geliştirilmelidir. Bu bağlamda, çeşitli çözüm önerileri şunlardır:

Yasal çerçevenin güçlendirilmesi; çevrimiçi oyunlar ve sanal varlıkların giderek artan popülaritesi, bu alanda ortaya çıkan suçlarla mücadelede yasal çerçevenin güçlendirilmesinin önemini vurgulamaktadır. Yasal düzenlemelerin eksikliği veya yetersizliği, ispat sorunlarının çözümünü zorlaştıran temel engellerden

---

<sup>177</sup><https://playvalorant.com/tr-tr/news/game-updates/>, 'Riot Games Oyun Güncellemeleri', E.T: 25 Ocak 2024.

<sup>178</sup><https://playvalorant.com/tr-tr/news/game-updates/>, 'Riot Games VALORANT 8.02 Yama Notları', E.T: 25 Ocak 2024.

biri olarak karşımıza çıkmaktadır. Bu bağlamda, çevrimiçi oyunlar ve sanal varlıkların hukuki statüsünü açıkça tanımlayacak, dijital dünyanın özgül dinamiklerini dikkate alan ve teknolojik gelişmeleri öngören yasal düzenlemelerin yapılması, ispat süreçlerinde karşılaşılan zorlukların üstesinden gelinmesinde kritik bir rol oynayabilir. Bu tür düzenlemeler hem ulusal hem de uluslararası düzeyde iş birliğini ve uyumu teşvik ederek, çevrimiçi oyun suçlarına karşı etkili bir mücadele stratejisi geliştirmenin temelini oluşturacaktır. Bu yolla, hukuk sisteminin çevrimiçi oyunlara özgü suçlar karşısında daha donanımlı hale gelmesi ve adaletin sağlanmasında önemli bir adım atılması mümkün olacaktır.

Teknik kapasitenin yetersiz olması; çevrimiçi oyun suçlarının soruşturma ve kovuşturma aşamalarında karşılaşılan zorluklar, özellikle dijital delillerin toplanması, analizi ve korunması konusundaki teknik kapasitenin yetersizliği nedeniyle önemli ispat sorunlarına yol açmaktadır. Bu bağlamda, adli makamların bu tür delillerle etkin bir şekilde başa çıkabilmesi için gerekli teknik kapasiteye sahip olmalarının önemi büyüktür. Bu, sadece ilgili personelin eğitilmesiyle değil, aynı zamanda teknolojik araç ve yöntemlerin geliştirilmesi ve bu alanda kullanılacak kaynakların tahsis edilmesiyle mümkün olabilir. Bu kapasitenin artırılması, çevrimiçi oyunlar ve sanal varlıklarla ilgili suçların daha etkili bir şekilde tespit edilmesi, soruşturulması ve kovuşturulmasına imkân tanıyacak, böylece bu alandaki hukuki boşlukların kapatılmasına ve ispat sorunlarının üstesinden gelinmesine katkı sağlayacaktır. Bu yolla hem ulusal hem de uluslararası düzeyde bütüncül stratejilerin geliştirilmesi, çevrimiçi oyun suçlarıyla mücadelede kritik bir öneme sahip olacaktır, zira dijital çağın getirdiği zorluklar karşısında adli makamların donanımlı olması, hukukun üstünlüğünün korunması ve bireylerin haklarının savunulması için elzemdir.

Uluslararası iş birliğinin teşviki; çevrimiçi oyun suçlarının sınır ötesi doğası, uluslararası iş birliği ve bilgi paylaşımı mekanizmalarının güçlendirilmesini zorunlu kılar. Bu tür suçlar, tek bir ülkenin yargı yetkisi içinde kalmayıp, birden fazla ülkeyi etkileyebilecek karmaşık yapılar oluşturduğundan, suçların etkin bir şekilde soruşturulması ve kovuşturulması için ülkeler arası koordinasyon ve iş birliği hayati önem taşımaktadır. Bu bağlamda, çeşitli uluslararası kurum ve kuruluşlar arasında bilgi paylaşımını kolaylaştıracak mekanizmaların oluşturulması, dijital delillerin sınır ötesi toplanması, analizi ve korunması konusunda standartların belirlenmesi

gerekmektedir. Bu tür bir iş birliği, aynı zamanda yasal çerçevelerin uyumlaştırılmasına ve ortak mücadele stratejilerinin geliştirilmesine olanak tanıyacak, böylece uluslararası düzeyde çevrimiçi oyun suçlarına karşı daha etkili bir mücadele yürütülebilecektir. Bu süreç, aynı zamanda ulusal yargı makamlarının kapasitelerinin artırılmasını destekleyecek, çünkü uluslararası iş birliği, suçla mücadelede en iyi uygulamaların ve teknolojik yeniliklerin paylaşılmasını teşvik edecektir. Bu nedenle, uluslararası iş birliğinin teşviki, çevrimiçi oyun suçlarına karşı koymada bütüncül ve çok yönlü bir stratejinin temel taşı olarak görülmelidir.

Farkındalığın artırılması; çevrimiçi oyunlar ve sanal varlıkların güvenliğini tehdit eden suçlarla mücadelede hayati bir stratejidir. Kullanıcıların çevrimiçi güvenlik konusunda bilinçlendirilmesi ve etkili korunma yöntemleri hakkında eğitilmesi, bu tür suçların önlenmesine önemli ölçüde katkı sağlayabilir. Eğitim programları, seminerler ve bilgilendirme kampanyaları aracılığıyla gerçekleştirilecek bu bilinçlendirme faaliyetleri, kullanıcıları potansiyel tehditler karşısında uyararak, güvenli çevrimiçi davranışlar geliştirmelerine yardımcı olur. Ayrıca, kişisel bilgilerin korunması, şüpheli etkinliklerin nasıl tanınacağı ve rapor edileceği gibi konularda sağlanacak eğitim, kullanıcıları sadece bilgilendirmekle kalmayıp, aynı zamanda aktif birer savunma hattı olarak da güçlendirir. Bu yaklaşım, çevrimiçi oyun ekosistemini daha güvenli bir alan haline getirerek, suçların önlenmesinde proaktif bir rol oynar ve bireyleri potansiyel tehditlere karşı daha dirençli kılar.

Çevrimiçi oyunların büyüdü dünyasında yükselen suç dalgaları, hukukun sınırlarını zorlarken, adaletin dijital çağın karmaşasında yolunu bulması için bütüncül bir vizyon gerekmektedir. Yasal çerçevelerin güçlendirilmesi, teknik kapasitenin artırılması, uluslararası iş birliğinin derinleştirilmesi ve farkındalığın üst seviyeye taşınması, bu mücadelede dört temel direği oluşturur. Her biri, çevrimiçi oyun suçlarına karşı koymada kritik öneme sahip bu unsurlar, adaletin terazisini dijital dünyanın lehine eğmek ve bireylerin sanal varlıklarını korumak için bir araya gelmelidir. Bu stratejik yaklaşım, hukukun üstünlüğünü dijital çağın ötesine taşıyacak, bireylerin haklarını korurken, suçlulara karşı etkili bir kalkan oluşturacaktır. Bu yolculukta, her adım, hukuki profesyonelliğin ve teknolojik yeniliklerin mükemmel bir uyum içinde dans ettiği bir senfoniye dönüşmelidir; böylece adaletin dijital ufukta parlaması için gerekli zemin hazırlanır. Bu çaba, sadece bugünün değil, yarının da

güvenliğini sağlayacak, çevrimiçi oyun dünyasını daha adil, daha güvenli bir yer haline getirecek bir hukuk anlayışının temelini atmaktadır.

#### 4.5. Delile Ulaşma Yöntemleri

Çevrimiçi oyun hesapları ve karakterlerinin yetkisiz kişiler tarafından ele geçirilmesi, dijital çağın getirdiği bilişim suçları arasında öne çıkan, hem bireysel kullanıcıların kişisel veri güvenliğini tehdit eden hem de geniş çapta ekonomik ve sosyal etkilere sahip bir sorundur. Bu tür vakaların aydınlatılması ve faillerin adalete teslim edilmesi süreci, CMK md.134 gibi mevcut hukuki düzenlemelere dayanmakta, ancak bu düzenlemelerin siber suçlarla mücadelede yeterli olup olmadığı tartışmalıdır. Olay yeri incelemesi ve elektronik delillerin toplanması, kolluk kuvvetlerinin teknolojik ve hukuki bilgi birikimini gerektirirken, bu süreçte delillerin bütünlüğünün korunması kritik önem taşır. Etkili bir mücadele, sadece yasal düzenlemelerle değil, aynı zamanda kolluk kuvvetleri ve adli makamların sürekli eğitimi ile teknolojik gelişmelere uyum sağlamasıyla mümkündür, bu da bireylerin dijital varlıklarının korunmasını ve çevrimiçi oyun ekosisteminin sağlıklı büyümesini destekler.<sup>179</sup>

Olay yerine ilk müdahale eden ekiplerin, delil toplama sürecine başlamadan önce, kullanacakları teknolojik araçları hazırlamaları, kendi güvenliklerini ve olay yerinin güvenliğini sağlamaları gerekmektedir. Bu temel adımların ardından hem elektronik hem de elektronik olmayan delillerin bütünlüğünü koruma altına almak önceliklidir.<sup>180</sup> Delillerin toplanması süreci, şüphelinin dijital izlerinin detaylı bir şekilde incelenmesiyle başlar. Bu, IP adresleri, giriş-çıkış kayıtları ve hesap aktiviteleri gibi dijital verilerin analizini kapsar. Çevrimiçi oyun sağlayıcılarının bu bilgileri sistemsel olarak kaydetmesi, soruşturma sürecinde kritik öneme sahiptir. Elde edilen veriler, şüphelinin dijital ortamda bıraktığı izleri takip ederek, suçun işlenme zamanı, kullanılan IP adresleri ve gerçekleştirilen işlemleri ortaya çıkarır. Ayrıca, oyun içi iletişim kayıtları da suçun aydınlatılması ve faillerin tespit edilmesinde önemli rol oynar. Oyuncular arasındaki mesajlaşmalar, takas işlemleri ve karakter etkileşimleri,

<sup>179</sup>M. V. Dülger, 'Adli Bilişim ve Ülkemizde Uygulaması', *H Plus Dergisi* 6. Baskı, cilt: 11, sayı: 1, 2015, s. 22.

<sup>180</sup>Y. Başlar, 'Elektronik Delilin Toplanması ve Muhafazası', *Hacettepe Hukuk Fakültesi Dergisi*, cilt: 10, sayı: 1, Ankara 2020, s. 83.

faillerin kimliklerinin belirlenmesine ve olayın yeniden oluşturulmasına yardımcı olabilir. Bu bilgiler, özellikle hesap veya karakter çalınması vakalarında, faillerin niyetini ve eylemlerini anlamada kritik önem taşır. Bu kapsamlı yaklaşım, adli sürecin sağlam bir temel üzerine kurulmasını sağlar ve suçun aydınlatılmasına katkıda bulunur.

Dijital delillerin toplanmasının yanı sıra, mağdurların ve tanıkların ifadeleri de önemlidir. Bu kişilerin hesap ele geçirme olayı hakkında sağlayabileceği bilgiler, dijital delillerle birleştirildiğinde, olayın bütün yönleriyle aydınlatılmasına olanak tanır. Mağdurların hesap güvenliği ile ilgili aldıkları önlemler, hesaplarını nasıl kullandıkları ve hesaplarının ele geçirilmesinden önce yaşadıkları olaylar, faillerin yöntemlerini ve amaçlarını ortaya çıkarmada yardımcı olabilir. Bununla birlikte, çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi olaylarında delil toplamanın önünde ciddi engeller de bulunmaktadır. Bu engellerin başında, çoğu zaman faillerin kimliklerini gizlemek için kullandıkları teknikler gelir. VPN<sup>181</sup> kullanımı, IP adresini maskeleyme<sup>182</sup>, hesap bilgilerini phishing<sup>183</sup> yöntemleriyle ele geçirme gibi yöntemler, faillerin izini sürmeyi zorlaştırır. Ayrıca çevrimiçi oyun hesaplarının uluslararası bir alanda bulunması, farklı ülkelerin hukuk sistemleri arasındaki uyumsuzlukları da beraberinde getirir. Bu durum, delil toplama ve faillerin yargı önüne çıkarılması sürecini karmaşıktırabilir. Delil toplama yöntemlerinin etkinliği, aynı zamanda ilgili yasal çerçevelere ve bilişim suçlarıyla mücadeledeki uluslararası iş birliklerine de bağlıdır. Çevrimiçi oyun hesaplarının ele geçirilmesine yönelik suçların çözülmesi, sadece teknik bir mesele değil, aynı zamanda yasal ve diplomatik bir çaba gerektirir. Bu nedenle, bilişim suçlarıyla mücadelede ulusal ve uluslararası düzeyde iş birliğinin artırılması, etkili bir yasal çerçevenin oluşturulması ve teknik altyapının güçlendirilmesi büyük önem taşır.

---

<sup>181</sup>Aydoğdu, a.g.e., s. 2-5.

<sup>182</sup>Millî Eğitim Bakanlığı, *Bilişim Teknolojileri Alt Ağlar*, Seçkin Yayıncılık, Ankara, 2012, s. 9-10.

<sup>183</sup>Arslan, a.g.e., s. 348-358.

#### 4.6. Zarar Gören Taraflar ve Tazminat Hakkı

Türk hukuk sistemi zarar gören tarafların haklarını Türk Borçlar Kanunu madde 49’da belirtilen hükümler doğrultusunda düzenler. Ancak, çevrimiçi oyun hesaplarının hukuka aykırı ele geçirilmesi durumlarında, dijital alanda mülkiyet hakkının tanımlanması ve zararın nasıl hesaplanacağı gibi konularda belirsizlikler vardır. Bu belirsizlikler hukukun dijital dünyayla ayak uyduramamasından ve dijital mülkiyet hakkının henüz tam anlamıyla Türk hukukunda tanımlanmamış olmasından kaynaklanmaktadır. Maddî zarar, malvarlığında meydana gelen eksilme veya artmanın engellenmesi sonucunda oluşur ve genellikle somut maddi değerlerle ölçülebilirken, manevi zarar, kişilik haklarını koruma kapsamına giren değerlerin ihlalden kaynaklanan ve maddi bir karşılığı olmayan zararlardır.<sup>184</sup>

Çevrimiçi oyunlarda zararların hesaplanması, bu alanın kendine özgü karmaşıklıkları nedeniyle özellikle zordur. Maddi zararlar, oyun içi eşyaların veya hizmetlerin kaybı gibi somut unsurları içerirken, manevi zararlar oyun deneyiminin bozulması, itibarın zedelenmesi gibi soyut konseptleri kapsar. Oyun içi varlıkların gerçek dünya para birimiyle doğrudan bir karşılığı olmadığı durumlarda, maddi zararın değerini belirlemek karmaşılaşır. Manevi zararlar ise oyunun sosyal ve psikolojik boyutları göz önünde bulundurulduğunda daha da subjektif bir hâl alır. Bu nedenle, çevrimiçi oyunlarda zararların hesaplanması hem maddi hem de manevi zararların özgün doğasını ve çevrimiçi ortamın spesifik dinamiklerini dikkate alan detaylı bir yaklaşım gerektirir. Hukukçular için bu, özellikle dikkatli ve derinlemesine bir değerlendirme yapmayı gerektiren bir süreçtir.

Hukuk pratiğinde TBK madde 49 kapsamında zarar gören tarafın tazminat talep etme hakkı temel bir prensip olarak kabul edilir. Bununla birlikte, özellikle dijital dünya ve çevrimiçi platformlarda meydana gelen zararların tazmin edilme sürecinde, tazminatın miktarının ve kapsamının belirlenmesi konusunda belirgin bir standart bulunmamaktadır. Dijital mülkiyet hakları, geleneksel mülkiyet anlayışından farklı olarak, daha soyut ve dinamik bir yapıya sahiptir. Bu durum tazminat taleplerinin değerlendirilmesini zorlaştırmakta ve hukuki belirsizliklere yol açmaktadır. Bu

---

<sup>184</sup>V. Kafes, ‘Ceza Hukukunda Mağdurun Zararının Giderilmesi’, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 60, sayı: 1, 2011, s. 93.

kapsamda, dijital mülkiyet haklarının daha detaylı ve somut bir şekilde tanımlanması ve düzenlenmesi gerekmektedir. Çünkü dijital ortamda meydana gelen zararlar, fiziksel dünyadaki zararlardan farklı olarak, somut olmayan varlıklara, itibara veya kullanıcı deneyimine yönelik olabilmektedir. Bu nedenle, dijital dünyanın özgün dinamikleri ve karmaşıklıkları göz önünde bulundurularak, zarar görenlerin tazminat haklarının somut standartlar çerçevesinde düzenlenmesi, hukuki süreçlerin adil ve tutarlı bir şekilde işlemlerini sağlayacak ve dijital mülkiyet haklarının daha etkin bir biçimde korunmasına katkıda bulunacaktır. Hukukçular için bu hem yasal düzenlemelerin hem de yargısal kararların<sup>185</sup>, dijital ortamın özgünlüğünü ve karmaşıklığını dikkate alan bir perspektiften şekillendirilmesi gerektiği anlamına gelmektedir. Teknolojik gelişmelerin getirdiği yeniliklerin hukuki bir çerçevede ele alınması, vatandaşların dijital dünyadaki haklarının daha etkin bir şekilde korunmasını sağlayacak ve dijital çağın getirdiği zorluklara karşı hukukun adaptasyonunu ve gelişimini destekleyecektir. Bu sürecin hem hukukçular hem de tüm vatandaşlar için yeni bir dönemin başlangıcı olacağı kuşkusuzdur.

#### **4.7. Uluslararası İş Birliği ve Sınır Ötesi Suçlar**

Türkiye, adli yardımlaşma alanında kapsamlı bir genel yasal düzenlemeye sahip olmamakla birlikte, bu eksiklik çok-terafı ve iki-terafı uluslararası antlaşmalar ile bunlara dayalı ulusal düzenlemeler aracılığıyla giderilmeye çalışılmaktadır. Bu durum, özellikle yurtdışı muhakemeleri ve adli yardım talepleri gibi konularda Türk ulusal makamlarının izlemesi gereken belirgin bir prosedürün olmamasına yol açmakta, adli yardımlaşmanın çeşitli yönlerini düzenleyen spesifik hükümler ancak belirli antlaşma ve düzenlemelerle sınırlı kalmaktadır. Örneğin, TCK madde 18’de geri vermeyle ilgili kurallar, Anayasa ve Türk Ceza Kanunu’nda ele alınmış, ancak genel bir çerçeve oluşturulmamıştır. Bu bağlamda, farklı türdeki iş birliğini kapsayacak özel bir düzenlemenin yararlı olacağı ifade edilmektedir. Aynı zamanda, çevrimiçi oyun hesaplarının ve karakterlerinin yetkisiz ele geçirilmesi, bilişim suçları kapsamında değerlendirilen ve sadece bireysel zararla sınırlı kalmayıp ulusal ve uluslararası güvenlik sorunlarına dönüşebilen bir problem olarak dikkat çekmektedir. Bu tür

---

<sup>185</sup>Yargıtay 13. Ceza Dairesi, 2016/2155 Esas No, 2017/10403 Karar No.

suçların önlenmesinde uluslararası iş birliğinin arttırılması, günümüzdeki teknolojik gelişmeler ve siber güvenlik tehditlerinin boyutu göz önünde bulundurulduğunda, giderek daha fazla önem kazanmaktadır.<sup>186</sup>

Bu iki ana konu, Türkiye'nin hem adli yardımlaşma mekanizmalarını hem de bilişim suçlarıyla mücadelede uluslararası iş birliği ve uyum süreçlerini güçlendirme gerekliliğini ortaya koymaktadır. Özellikle bilişim suçları alanında uluslararası iş birliğinin ve koordinasyonun geliştirilmesi, bu tür suçlarla etkin bir şekilde mücadele etmek ve ulusal güvenliği korumak adına kritik önem taşımaktadır. Bu kapsamda, Türkiye'nin ilgili mevzuatını sürekli olarak güncelleyerek ve uluslararası standartlarla uyumlu hale getirerek, adli yardımlaşma ve siber suçlarla mücadelede daha etkin bir rol üstlenmesi gerekmektedir.

Bilişim teknolojilerinin hızla gelişmesi ve internet kullanımının yaygınlaşması, çevrimiçi oyun sektörünü de büyümüşür. Bu büyüme, yeni ekonomik fırsatlar sunarken, bilişim suçlarının da çeşitlenmesine ve artmasına neden olmuştur. Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, bu suçların en yaygın örneklerinden biridir. Oyun içi eşyalar, karakterler ve hesaplar, gerçek para değerine sahip olabilmekte ve suçlular için cazip bir hedef haline gelmektedir. Bu tür suçlar, genellikle kimlik hırsızlığı<sup>187</sup>, dolandırıcılık ve kötü amaçlı yazılım kullanımı<sup>188</sup> gibi yöntemlerle gerçekleştirilmektedir. Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, sadece maddi zararlara neden olmakla kalmayıp, mağdurların kişisel ve finansal bilgilerinin tehlikeye girmesine de yol açabilir. Bu durum, bireylerin ötesinde, ulusal güvenlik meselelerini de beraberinde getirebilir. Örneğin, ele geçirilen hesaplar üzerinden yürütülen dolandırıcılık ve kimlik hırsızlığı faaliyetleri, terör finansmanı gibi daha geniş çaplı suçların işlenmesine zemin hazırlayabilir.

Bu tür suçların uluslararası boyutu, farklı ülkelerin yargı alanlarını aşarak gerçekleşmesi nedeniyle, suçluların takibi ve yargılanması önemli zorluklar içermektedir. Çevrimiçi oyun hesaplarının ele geçirilmesi gibi suçlar, genellikle sınır ötesi bir nitelik taşımakta ve bu da suçluların yakalanmasını ve adalete teslim

---

<sup>186</sup>Önok,a.g.e., s. 1247.

<sup>187</sup>Bayzıt, a.g.e., s. 635-659.

<sup>188</sup>N. K. Torun ve T. Torun, 'Kötü Amaçlı Yazılımların E-Ticaret İçerisinde Siber Güvenlik Açısından İncelenmesi', *Sakarya İktisat Dergisi*, cilt: 11, sayı: 1, 2022, s. 3-4.

edilmesini güçleştirmektedir. Bu bağlamda, uluslararası iş birliği, bu tür bilişim suçlarıyla mücadelede kritik bir öneme sahiptir. Uluslararası iş birliğinin temeli, çeşitli ülkeler arasında bilgi alışverişi, suçluların iadesi ve ortak yargı mekanizmalarının oluşturulması gibi unsurları içermektedir. Bu iş birliği INTERPOL, Europol gibi uluslararası polis teşkilatları ve Birleşmiş Milletler gibi küresel kuruluşlar tarafından desteklenmektedir.<sup>189</sup> Ayrıca, çeşitli ülkeler arasında imzalanan ikili ve çok taraflı anlaşmalar, bu tür suçlarla mücadelede hukuki bir zemin oluşturmaktadır.<sup>190</sup> Öte yandan, uluslararası iş birliğinin etkinliği, katılan ülkelerin hukuk sistemleri, teknolojik kapasiteleri ve siyasi iradeleri gibi faktörlere bağlıdır. Bu faktörler arasındaki farklılıklar, iş birliğinin zorluklarını da beraberinde getirebilir. Bu nedenle, uluslararası iş birliğini güçlendirmek için ülkelerarası anlayışın ve koordinasyonun artırılması, ortak standartların ve prosedürlerin belirlenmesi gerekmektedir.

Buna ek olarak, çevrimiçi oyun sektörü ve ilgili teknoloji şirketleri ile hükümetler ve uluslararası kuruluşlar arasında iş birliği, bu suçlarla mücadelede önemli bir rol oynamaktadır. Sektörün, güvenlik önlemlerini artırması, kullanıcıların bilinçlendirilmesi ve suçluların tespiti için gerekli verilerin paylaşılması, suçların önlenmesi ve suçluların adalet karşısına çıkarılmasında kritik öneme sahiptir. Çevrimiçi oyun hesaplarının ve karakterlerinin ele geçirilmesi, günümüzde ciddi bir bilişim suçu tehdidi oluşturmaktadır. Bu tehditle mücadele etmek, sadece ulusal düzeyde değil, uluslararası iş birliği ve koordinasyon gerektirmektedir. Uluslararası iş birliği, sınır ötesi bilişim suçlarıyla etkili bir şekilde mücadele etmek için hayati öneme sahiptir. Bu iş birliği hem hukuki mekanizmaların güçlendirilmesi hem de teknolojik ve bilgi altyapısının iyileştirilmesi yoluyla sağlanabilir. Bu çabaların başarısı, uluslararası toplumun bu konudaki kararlılığı ve iş birliği yapma kapasitesine bağlıdır.

---

<sup>189</sup>Önok,a.g.e., s. 1234-1241.

<sup>190</sup>C. Aliusta ve R. Benzer, 'Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci', *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, cilt: 4, sayı: 2, 2018, s. 37.

## SONUÇ

Çevrimiçi oyun hesaplarının ve karakterlerinin izinsiz ele geçirilmesi, dijital çağın beraberinde getirdiği en ciddi bilişim suçlarından biri olarak günümüzde büyük bir sorun teşkil etmektedir. Bu suç türü, bireysel kullanıcıların kişisel ve finansal güvenliğini tehdit ederken, aynı zamanda oyun geliştiricileri ve genel olarak dijital ekosistemi de olumsuz yönde etkilemektedir. Bu bağlamda, çevrimiçi oyun hesapları ve karakterlerinin korunması, sadece bireysel bir sorumluluk değil, aynı zamanda teknoloji sağlayıcıları ve hukuk sistemlerinin de ortaklaşa üstlenmesi gereken bir görev haline gelmiştir.

İzinsiz erişim vakalarının artışı, kullanıcıların kişisel bilgilerinin korunması ve dijital varlıklarının güvenliği konusunda yeni stratejilerin geliştirilmesini zorunlu kılmıştır. Bu suçların üzerine gidilmesi sürecinde, dijital delillerin toplanması, korunması ve analiz edilmesi gibi bir dizi zorlukla karşılaşmaktadır. Özellikle, dijital delillerin geçici doğası, soruşturma sürecini karmaşıklaştıran en önemli faktörlerden biridir. Bu delillerin zamanında toplanamaması veya yanlış şekilde işlenmesi, suçların aydınlatılmasını ve failerin adalet karşısına çıkarılmasını güçleştirebilir. Örneğin, bir çevrimiçi oyun platformunda kullanıcı hesabının izinsiz ele geçirilmesi vakası ele alındığında, failer genellikle IP adreslerini gizlemek veya sahtelemek, VPN hizmetleri kullanmak gibi yöntemlerle izlerini kaybettirirler. Bu durum, suçun gerçekleştiği anda ilgili IP adreslerinin, giriş loglarının ve diğer ilgili verilerin hızla tespit edilip, kaydedilmesini gerektirir. Ancak, bu bilgiler zamanla üzerine yazılabilir, silinebilir veya manipüle edilebilir, bu da soruşturmayı zorlaştırır. Ayrıca, dijital delillerin uluslararası sınırlar içinde aktarılması, farklı ülkelerin veri koruma yasalarına tabi olması gibi hukuki engeller de mevcuttur. Bir diğer örnek ise, bir kullanıcının kimlik avı saldırısı sonucu oyun içi varlıklarının çalınması olayıdır. Bu durumda, saldırganın kullandığı sahte e-posta adresleri, kimlik avı siteleri ve bu sitelere yönlendirme yapan linkler, dijital delil olarak toplanabilir. Ancak, bu tür delillerin etkin bir şekilde toplanabilmesi için, olayın fark edildiği andan itibaren hızlı bir şekilde harekete geçilmesi ve teknik uzmanlığa sahip kişiler tarafından soruşturmanın yürütülmesi gerekmektedir. Saldırganlar tarafından kullanılan yöntemler sürekli evrildiğinden, adli bilişim tekniklerinin ve araçlarının da bu değişime ayak uydurabilmesi önem taşımaktadır. Bu örnekler, izinsiz erişim vakalarının soruşturulmasında karşılaşılan

zorlukların sadece birkaçını yansıtmaktadır. Dijital delillerin toplanması, korunması ve analiz edilmesi sürecinde yaşanan zorluklar, bu tür suçlarla mücadelede etkili yöntemlerin ve stratejilerin geliştirilmesini zorunlu kılmaktadır. Bu bağlamda, adli bilişim uzmanları, hukuk profesyonelleri ve teknoloji sağlayıcılarının iş birliği içinde çalışması, suçların aydınlatılmasını ve faillerin adalet önüne getirilmesini kolaylaştıracak çözümler üretme yolunda kritik bir öneme sahiptir.

Dijital delil toplama sürecinde, adli bilişim uzmanları, izinsiz erişim olaylarının aydınlatılması için oyun sunucularından, kullanıcı etkinlik kayıtlarından ve ağ trafiği analizlerinden elde edilen verilere başvururlar. Bu veriler, suçun işlendiği zaman diliminde gerçekleşen olayları detaylı bir şekilde ortaya koymak için kritik öneme sahiptir. Örneğin, bir oyun sunucusundan elde edilen kullanıcı giriş ve çıkış kayıtları, hesabın izinsiz kullanıldığına dair belirgin kanıtlar sunabilir. Bu kayıtlar, hesabın ele geçirilme zamanını, suçun gerçekleştiği coğrafi konumu (IP adresi üzerinden) ve hatta saldırganın kullandığı cihaz bilgilerini içerebilir. Bir diğer örnek olarak, ağ trafiği analizi, saldırganın kullanıcı hesabına nasıl erişim sağladığını belirlemekte kullanılabilir. VPN kullanımı, TOR ağları veya başka anonimleştirme servislerinin kullanılması gibi izleri barındıran ağ trafiği kayıtları, saldırganın izini sürmede değerli ipuçları sağlayabilir. Bu tür analizler, saldırganın kullandığı yöntemlerin ve araçların belirlenmesinde yardımcı olurken, aynı zamanda ileride benzer saldırıların önlenmesine yönelik güvenlik önlemlerinin geliştirilmesinde de kritik rol oynar. Bununla birlikte, toplanan bu verilerin işlenmesi sırasında, bireylerin mahremiyet haklarının korunması ve kişisel verilerin güvenliğinin sağlanması gerekmektedir. Örneğin, bir kullanıcının giriş kayıtlarının incelenmesi sırasında, sadece soruşturma ile doğrudan ilgili olan bilgilere erişilmesi ve bu bilgilerin yasal çerçeveler dahilinde işlenmesi önem taşır. Bu hem adli bilişim uzmanlarının hem de hukuk profesyonellerinin, veri koruma yasaları ve mahremiyet standartları konusunda derinlemesine bir bilgiye sahip olmalarını gerektirir. Ayrıca, elde edilen delillerin mahkemede kullanılabilir olması için, toplama ve işleme süreçlerinin yasalara uygun olarak yürütülmesi zorunludur.

Hukuki çerçeve ile ilgili olarak, çevrimiçi oyun hesapları ve karakterlerinin izinsiz ele geçirilmesi vakalarına karşı daha etkili mücadele stratejileri geliştirilmesi

gerekmektedir. Mevcut yasaların güçlendirilmesi ve güncellenmesi, bu tür suçlarla mücadelede kritik öneme sahiptir.

Özellikle, bilişim suçlarına özgü delil toplama yöntemleri, cezai yaptırımlar ve mağdurların haklarını koruyan yasal düzenlemelerin oluşturulması, etkili bir mücadele için olmazsa olmazlardır. Aynı zamanda, uluslararası iş birliği, sınır ötesi suçlarla mücadelede önemli bir rol oynamaktadır. Farklı ülkeler arasında bilgi paylaşımını ve iş birliğini kolaylaştıracak anlaşmaların yapılması ve uluslararası düzeyde koordinasyonun sağlanması, bu suçlarla mücadelede önemli bir adım olacaktır. Örneğin, bir oyuncunun hesabının izinsiz şekilde ele geçirilmesi ve bu hesap üzerinden gerçekleştirilen işlemler, diğer oyuncuların haklarının ihlal edilmesine neden olabilir. Bu tür bir durumda, hukuki çerçeve, mağdur oyuncunun haklarını koruyacak ve failleri cezalandıracak mekanizmaları içermelidir. Bu, bilişim suçlarına özel olarak tasarlanmış delil toplama prosedürlerini, suçlulara yönelik caydırıcı cezaları ve mağdurların zararlarının telafi edilmesini kapsayan düzenlemeleri içerebilir. Aynı zamanda, bu tür suçlar sıklıkla uluslararası sınırları aşan bir nitelik taşıdığından, uluslararası iş birliği hayati öneme sahiptir. Farklı ülkelerin hukuk sistemleri arasında bilgi ve delil paylaşımını kolaylaştıracak anlaşmaların yapılması, sınır ötesi suçların etkili bir şekilde soruşturulmasını ve faillerin adalet önüne çıkarılmasını sağlar. Örneğin, bir saldırganın farklı bir ülkede bulunan bir sunucuyu kullanarak bir oyuncunun hesabını ele geçirmesi durumunda, ilgili ülkeler arasındaki iş birliği, saldırganın tespit edilmesi ve gerekli yasal işlemlerin başlatılması için kritik olacaktır. Bu kapsamda, bilişim suçlarına yönelik uluslararası düzeyde kabul görmüş standartların ve iş birliği protokollerinin geliştirilmesi, suçlarla mücadelede önemli bir adım olarak görülmektedir. Bu tür bir iş birliği hem teknik hem de hukuki alanlarda uluslararası düzeyde koordinasyonun sağlanmasına yardımcı olacak ve çevrimiçi oyun hesaplarının ve karakterlerinin korunmasına yönelik etkili stratejilerin geliştirilmesine olanak tanıyacaktır. Bu yaklaşım hem bireysel kullanıcıların hem de oyun geliştiricilerinin dijital varlıklarını korumalarına yardımcı olacak ve bilişim suçlarına karşı daha güçlü bir savunma mekanizması oluşturulmasını sağlayacaktır.

Bireysel kullanıcıların dijital güvenlik bilincinin artırılması da bu mücadelede önemli bir yer tutmaktadır. Kullanıcıların, güçlü şifreler kullanması, iki faktörlü kimlik doğrulama sistemlerini aktif hale getirmesi ve düzenli olarak hesap güvenlik

kontrolleri yapması, hesap güvenliğini artırarak izinsiz erişim vakalarını önleyebilir. Bu bağlamda, kullanıcı eğitimi ve farkındalık programlarının yaygınlaştırılması, dijital güvenlik bilincinin artırılmasında kritik bir rol oynamaktadır.

Oyun geliştiricileri ve platform sağlayıcıları tarafından alınacak güvenlik önlemleri de bu suçlarla mücadelede önemli bir yer tutmaktadır. Gelişmiş güvenlik önlemlerinin uygulanması, şüpheli giriş denemelerini tespit eden algoritmalar, düzenli güvenlik güncellemeleri ve kullanıcıları güvenlik tehditleri konusunda bilgilendiren sistemler, kullanıcı hesaplarının korunmasına yönelik etkili yöntemler arasında yer alır. Ayrıca, oyun geliştiricileri, kullanıcı verilerinin korunmasına yönelik şeffaf politikalar geliştirerek, kullanıcıların güvenliğini kazanmalı ve bu alandaki yasal yükümlülüklerini yerine getirmelidir. Örneğin, bir oyun geliştiricisi, oyununun güvenliğini artırmak için çok faktörlü kimlik doğrulama sistemlerini devreye sokabilir. Bu sistem, kullanıcıların hesaplarına giriş yaparken sadece şifrelerini değil, aynı zamanda bir telefon uygulaması üzerinden alınan tek seferlik bir kodu da girmelerini gerektirir. Bu yöntem, izinsiz erişim girişimlerini önemli ölçüde azaltabilir. Bir başka örnek, oyun içi algoritmaların kullanılmasıdır. Bu algoritmalar, şüpheli davranışları tespit edebilir ve otomatik olarak güvenlik ekibine bildirimde bulunabilir. Örneğin, bir kullanıcının hesabından beklenmedik bir coğrafi konumdan giriş yapılması veya olağandışı bir varlık transferi gerçekleştirilmesi, bu algoritmalar tarafından tespit edilebilir ve hızlı bir müdahaleye olanak tanır. Oyun geliştiricileri ayrıca, düzenli güvenlik güncellemeleri yayınlayarak ve kullanıcıları güvenlik tehditleri konusunda bilgilendirerek de önemli bir rol oynarlar. Güvenlik güncellemeleri, bilinen zafiyetleri giderir ve oyunun güvenliğini artırır. Kullanıcıları bilgilendirme ise, onların güvenlik tehditlerine karşı daha bilinçli olmalarını sağlar. Örneğin, geliştiriciler, kullanıcıları kimlik avı saldırılarına karşı uyarabilir ve güvenli şifre oluşturma teknikleri hakkında bilgi verebilir. Geliştiricilerin kullanıcı verilerinin korunmasına yönelik şeffaf politikalar geliştirmesi de büyük önem taşır. Bu politikalar, kullanıcı verilerinin nasıl toplandığını, kullanıldığını ve korunduğunu açıkça belirtmelidir. Şeffaflık, kullanıcıların güvenliğini kazanmak ve geliştiricilerin yasal yükümlülüklerini yerine getirmek için kritik bir unsurdur. Örneğin, bir oyun platformu, kullanıcı sözleşmesinde veri işleme pratiklerini detaylı bir şekilde açıklayabilir ve kullanıcıların kendi verileri üzerinde kontrol sahibi olmalarını sağlayacak araçlar sunabilir.

Geleceğe yönelik arařtırmaların, çevrimiçi oyun hesapları ve karakterlerinin izinsiz ele geçirilmesine karşı daha sofistike mücadele yöntemleri geliştirilmesi noktasında odaklanması kaçınılmazdır. Bu bağlamda, bilişim teknolojilerinin sürekli evrimi, mevcut hukuki çerçevelerin bu dinamik ortama uyum sağlamasını zorunlu kılmaktadır. Yapay zekâ (AI) ve makine öğrenimi gibi teknolojilerin suç tespiti ve önlenmesinde nasıl stratejik bir avantaj sağlayabileceği, hukuki arařtırmaların merkezinde yer almalıdır. Bu teknolojilerin entegrasyonu hem suçların proaktif olarak önlenmesinde hem de detaylı soruşturma süreçlerinde devrim yaratabilir. Yapay zekâ destekli güvenlik sistemlerinin kullanımı, çevrimiçi oyun platformları için vazgeçilmez bir güvenlik katmanı haline gelmiştir. Bu sistemler, kullanıcı davranışlarını öğrenerek, herhangi bir anormallikte güvenlik ekiplerine anında bildirimde bulunabilir. Örneğin, coğrafi konum anomalileri veya alışılmadık oyun içi işlemler, potansiyel izinsiz erişim vakaları olarak sınıflandırılabilir. Bu, izinsiz erişim teşebbüslerinin erkenden tespit edilip, gerekli önlemlerin alınmasını sağlar. Makine öğrenimi algoritmalarının büyük veri setleri üzerindeki analiz kabiliyeti, suç desenlerini ve eğilimlerini tespit etmede kritik bir role sahiptir. Bu analizler, suç faaliyetlerinin ardındaki motivasyonları ve yöntemleri anlamada derinlemesine bir perspektif sunar. Bu bilgiler, soruşturma ekiplerinin daha stratejik ve odaklanmış soruşturma yöntemleri geliştirmesine olanak tanır. Bilişim teknolojilerindeki hızlı gelişmeler, hukukun teknolojik yeniliklere adaptasyonunu zorunlu kılmaktadır. Yeni suç türlerinin ortaya çıkışı, mevcut yasal düzenlemelerin sürekli olarak revize edilmesini gerektirir. Bu evrim, fail ile mağdur arasındaki fiziksel sınırları ortadan kaldırarak suçun işlenmesini kolaylaştırmış ve bilgisayar korsanlığını sınır tanımayan, illegal amaçlar için kullanılan bir suça dönüştürmüştür. Bu süreç, hukuki düzenlemelerin teknolojik ilerlemelerle uyumlu hale getirilmesini ve kullanıcı haklarının korunmasını sağlar. Uluslararası iş birliği, sınır ötesi suçlarla mücadelede hayati bir öneme sahiptir. Farklı ülkeler arasındaki koordinasyon ve bilgi paylaşımı, suçların önlenmesi ve faillerin adalete teslim edilmesi süreçlerini güçlendirir. Bu iş birliği, özellikle çevrimiçi oyun hesaplarının izinsiz ele geçirilmesi gibi küresel nitelikteki suçlarla mücadelede önemli bir avantaj sağlar. Sonuç olarak, gelecekteki arařtırmalar, yapay zekâ ve makine öğrenimi gibi ileri teknolojilerin suçla mücadeledeki potansiyelini keşfetmeli, hukuki düzenlemelerin bu teknolojik

gelişmelere adaptasyonunu teşvik etmeli ve uluslararası iş birliğinin önemini vurgulamalıdır. Bu çok yönlü yaklaşım, çevrimiçi oyun hesapları ve karakterlerinin izinsiz ele geçirilmesiyle mücadelede yeni bir paradigmaya yol açabilir ve suçların önlenmesi ile etkin soruşturma ve kovuşturma süreçlerine katkıda bulunabilir. Bu hukuk ve teknolojinin sinerjisinden maksimum fayda sağlama yönünde stratejik bir adımdır.

Çalışmamız kapsamında ele aldığımız, toplumsal barışı bozma potansiyeline sahip tehlikeleri ve suç eylemlerini daha etkin bir şekilde önleyebilmek ve bu suçların soruşturmalarını güçlendirebilmek adına, suçun belirgin modus operandi'sini karşılayacak özel bir kanun maddesinin gerekliliğinin belirlenmesi önem arz etmektedir. Bu bağlamda, Türk Ceza Kanunu'nun Onuncu Bölümü olan 'Bilişim Alanında Suçlar' bölümüne eklemeyi önerdiğimiz madde aşağıdaki gibidir.

Türk Medeni Kanunu'na Eklenmesi Teklif Edilen Madde;

Madde “...” - Dijital Mülkiyetin Tanımlanması ve Korunması

(1) Dijital mülkiyet, bir kişinin dijital bir platformda, uygulamada veya oyun içi öğeler, hesaplarda, dijital içerikler (kitaplar, müzik, film, yazılımlar) ve hizmetlerde sahip olduğu hakları ve menfaatleri kapsar. Bu mülkiyet, çevrimiçi hesapları, oyun içi varlıkları, dijital para birimlerini, sanal malları ve dijital içerikleri içerir.

(2) Dijital mülkiyet, fiziki mülkiyetle aynı korumayı ve hakları sağlar. Dijital mülkiyetin hukuka aykırı bir şekilde ele geçirilmesi, fiziki mülkiyetin hukuka aykırı ele geçirilmesi ile aynı cezai yaptırımları içerir.

(3) Dijital mülkiyetin devri, sahibinin açık rızası olmadan gerçekleştirilemez. Bu tür bir devir, rızasız bir şekilde gerçekleştirildiği takdirde, yasalara aykırı kabul edilir ve cezai yaptırımlar uygulanır.

(4) Dijital mülkiyet üzerindeki kullanıcı verilerinin korunması ve gizliliğin sağlanması için gerekli tedbirler alınır. Bu bağlamda, kişisel verilerin işlenmesi, saklanması ve üçüncü taraflarla paylaşılması sıkı düzenlemelere tabidir.

(5) Uluslararası iş birliği ve koordinasyon, dijital mülkiyetin korunması ve yasa dışı faaliyetlerin engellenmesi amacıyla teşvik edilir. Bu amaçla, Türkiye, ilgili

uluslararası anlaşmalar çerçevesinde diğer ülkelerle iş birliği yapar ve gerekli mekanizmaları kurar.

Bu örnek madde dijital mülkiyetin tanımını açıkça yapmakta ve dijital mülkiyetin korunması için yasal düzenlemeleri belirtmektedir. Fiziki mülkiyet ile dijital mülkiyet arasında eşitlik ilkesi oluşturulmuştur. Bu madde ayrıca dijital mülkiyetin rızasız devrinin yasaklandığını da belirtmektedir. Ayrıca dijital mülkiyetin hukuka aykırı bir şekilde ele geçirilmesi durumunda aşağıda bir örnek kanun maddesi oluşturulmuştur. Bu maddede dijital mülkiyetin hukuka aykırı ele geçirilmesini suç olarak tanımlanmaktadır:

Türk Ceza Kanunu'na Eklenmesi Teklif Edilen Madde;

Madde “...” - Dijital Mülkiyetin Hukuka Aykırı Ele Geçirilmesi

(1) Bir kişinin dijital mülkiyetini, o kişinin rızası olmaksızın, hile, tehdit, zor kullanma veya herhangi bir yasadışı yöntemle ele geçiren, kullanılabilir hale getiren, kullanma hakkını elinde bulunduran, yok eden, zarar veren, değiştiren, bu hakları kullanmasını engelleyen kişi, “...” yıldan “...” yıla kadar hapis cezası ile cezalandırılır.

(2) Suçun, banka veya kredi kartlarının, e-posta hesaplarının, sosyal medya hesaplarının, çevrimiçi oyun hesaplarının veya benzeri dijital platformlardaki mülkiyet haklarını içerdiği hallerde, verilecek ceza “...” oranında artırılır.

(3) Dijital mülkiyet haklarının hukuka aykırı olarak ele geçirilmesi veya kullanılması sonucunda mağdurun uğradığı zararın tazmini için hukuki süreç başlatılabilir.

Bu yasa maddesi, dijital mülkiyet haklarının hukuka aykırı bir şekilde ele geçirilmesini suç olarak tanımlamakta ve bu eylemi gerçekleştirenlerin cezalandırılmasını sağlamaktadır. Ayrıca, suçun belirli dijital platformlarda gerçekleştirilmesi durumunda cezanın arttırılması da öngörülmüştür. Son olarak, mağdurların uğradıkları zararın tazminini talep etme hakkı da yasa maddesi içerisinde belirtilmiştir.

## KAYNAKÇA

- A. Ünsal ve İ. Ulutaş, 'Bilgisayar Oyun Bağımlılığı Ölçeğinin Okul Öncesi Dönem Çocuklarına Uyarlanması', *Aksaray Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, cilt: 3, sayı: 2, 2019, s. 326.
- Ahi, Ş. 'Gelişmiş Sosyal Mühendislik Saldırıları Analizi ve Tespiti', Yüksek Lisans Tezi, *Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü*, Gebze, 2020.
- Akarıslan, H. 'Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Kavramı', Yüksek Lisans Tezi, *Polis Akademisi Güvenlik Bilimleri Enstitüsü*, Ankara, 2011.
- Akcan, Ö. 'Adli Bilişim Veri İncelemelerinin Araştırılması', Yüksek Lisans Tezi, *Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü*, İstanbul, 2021.
- Akıncı, A. N. 'Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi', *Çalışma Raporu 6, Türkiye Cumhuriyeti Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü*, Ankara, 2017, s. 7.
- Alacakaptan, U. 'Suçun Unsurları', *Ankara Üniversitesi Hukuk Fakültesi Yayınları No: 372*, Ankara, 1975, s. 8.
- Aldoori, A. 'Uluslararası Hukukta Siber Suçla Mücadele', Yüksek Lisans Tezi, *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2020.
- Aliusta, C. ve Benzer, R. 'Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci', *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, cilt: 4, sayı: 2, 2018, s. 37.
- Ankara Kalkınma Ajansı 'Dijital Oyun Sektörü Raporu', Ankara, 2017, s. 19.
- Arslan, Ç. 'Dijital Delil ve İletişimin Denetlenmesi', *Ceza Hukuku ve Kriminoloji Dergisi*, cilt: 3, sayı: 2, 2015, s. 256.

- Arslan, Y. 'Oltalama Saldırıları Farkındalık Tatbikatı Örneği', *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, cilt: 9, sayı: 3, 2021, s. s. 348-358.
- Aslay, F. 'Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi', *International Journal of Multidisciplinary Studies and Innovative Technologies*, cilt: 1, sayı: 1, 2017, s. 25.
- Avrupa Birliği, 'Avrupa Birliği Genel Veri Koruma Tüzüğü', *Resmî Gazete*, Ankara, 25 Mayıs 2018.
- Aydoğdu, N. 'Sanal Özel Ağ (VPN) Bağlantı Mantığı (VPN Teknolojisi) ve TOKEN Güvenliğinin PİN Kodu ile Arttırılması', Yüksek Lisans Tezi, *Beykent Üniversitesi Fen Bilimleri Enstitüsü*, İstanbul, 2014.
- Babayiğit, B. 'Kumar Oynama ve Kumar Oynanması İçin Yer ve İmkân Sağlama Fiilleri', *Türkiye Adalet Akademisi Dergisi*, sayı: 34, 2018, s. 309.
- Babayiğit, B. 'Kumar Oynama ve Kumar Oynanması İçin Yer ve İmkân Sağlama Fiilleri', *Türkiye Adalet Akademisi Dergisi*, sayı: 34, 2018, s. 309.
- Başlar, Y. 'Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri', *TBB Dergisi*, cilt: 148, 2020, s. 49.
- Başlar, Y. 'Elektronik Delilin Toplanması ve Muhafazası', *Hacettepe Hukuk Fakültesi Dergisi*, cilt: 10, sayı: 1, Ankara 2020, s. 83, 10.32957/hacettepehdf.690592.
- Bayındır, S. 'İş ve Çalışma Hürriyetinin İhlali Suçu (TCK m. 117/1)', *D.E.Ü. Hukuk Fakültesi Dergisi*, cilt 21, Özel Sayı, 2019, s. 157.
- Bayzıt, T. 'Kimlik Hırsızlığının Türk Ceza Hukuku ve Karşılaştırmalı Hukuk Bakımından Değerlendirilmesi', *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, cilt: XIX, sayı: 2, 2022, s. 637.
- Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, 'Bireysel Siber Güvenlik Önlemleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Ankara, 2023, s. 1-9.
- Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı, 'Çevrimiçi Oyunlara İlişkin Güvenlik Riskleri', *Ulusal Siber Olaylara Müdahale Merkezi (USOM)*, Kasım 2014, s. 3.

Bilgi Teknolojileri ve İletişim Kurumu, ‘Dijitalleşen Dünyada Bilişim Suçları ve Mücadele Yöntemleri’, *Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı*, Ankara, 2022, s. 18.

Bozoklu, O. ve Çil, C. Z. ‘Yazılım Güvenlik Açığı Ekosistemi ve Türkiye’deki Durum Değerlendirmesi’, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, cilt: 3, sayı: 1, 2017, s. 7.

Bucak, Y. ‘Adli Bilişim ve Türk Ceza Muhakemesi Hukukunda Bilgisayarda Arama’, Yüksek Lisans Tezi, *Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü*, İstanbul, 2019.

Canbek, G. ‘Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme’, Yüksek Lisans Tezi, *Gazi Üniversitesi Fen Bilimleri Enstitüsü*, Ankara, 2005.

Canbek, G. ve Sağiroğlu, Ş. ‘Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma’, *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi*, cilt 22, sayı 1, 2007, s. 125.

Ceylan Özgüven Ü. ve Eroğlu, Ş. ‘Elektronik Kaynaklarda Telif Hakkı ve Lisans Sözleşmeleri Üzerine Bir Değerlendirme: Bartın Üniversitesi Örneği’, *Bilgi Yönetimi Dergisi*, cilt: 6, sayı: 2, 2023, s. 197-216.

Ceylan, H. H. ve Köse, B. ‘Tüketicilerin Gri Pazar Ürün Tercihleri Üzerine Bir Araştırma’, *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, Karaman, cilt: 20, sayı: 34, 2018, s. 2.

Çakır, S. ve Kesler, M. ‘Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımları’, *Akademik Bilişim 12 - XIV. Akademik Bilişim Konferansı Bildirileri*, Uşak, 1-3 Şubat 2012, s. 472.

Çatlı, M. ve Şimşek, S. ‘Dijital Para ve Egemenlik’, *Türkiye Adalet Akademisi Dergisi*, cilt: 12, Sayı: 48, 2021, s. 151-184.

#### Çeviri Kitap

Dama, M. ‘Windows Fonksiyonları Kullanılarak Özgün Bir Casus Yazılım Tasarımı ve Alınabilecek Önlemler’, Yüksek Lisans Tezi, *Gazi Üniversitesi Bilişim Enstitüsü*, Ankara, 2014.

- Delogu, *Suç Genel Teorisinde 'Alet'*, (Çev. D. Soyaslan), Rivista Italiana di Diritto Procedura Penale, Nuova Serie, Ankara, 1989, s. 251-282.
- Demir, H. 'Bilişim Suçları Uygulamaları', *Ankara Batı Adliyesi Dergisi*, cilt: 4, sayı: 7, Ocak-Haziran 2022, s. 14.
- Demirtaş, S. 'Alman Ceza Kanunu'nda Kurala İlişkin Örnekler Müessesesi: Kanunilik İlkesi Açısından Bir Değerlendirme', *Türkiye Adalet Akademisi Dergisi*, cilt: 13, sayı: 49, Ocak 2022, s. 434-440.
- Doğan, D. ve Özocak, G. 'Dijital Oyunlar, Multimedya Yaratımlar ve Güncel Hukuki Problemler', *Özocak Blog*, Haziran 2013, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://ozocak.com/Dosyalar/88cd5f.pdf, E.T: 22 Şubat 2024.
- Durmuş, M. E. 'Bilgisayar Oyunlarının Türk Hukukunda Korunması', Yüksek Lisans Tezi, *İstanbul Şehir Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2020.
- Dülger, M. V. 'Adli Bilişim ve Ülkemizde Uygulaması', *H Plus Dergisi* 6. Baskı, cilt: 11, sayı: 1, 2015, s. 22.
- Egeli, H. 'Türk Anayasa Hukukunda Mülkiyet Hakkının Kullanımının Durdurulması', *Liberal Düşünce Dergisi*, cilt: 27, sayı: 105, 2022, s. 223-236.
- Erdağ, A. İ. 'Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)', *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, cilt XIV, 2010, s. 276-300.
- Erdoğan, Y. 'Bilişim Sistemine Girme ve Kalma Suçu', *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 12, Özel Sayı, 2010, s. 1423-1424.
- Erem, F. 'Suçun Konusu ve Hümanist Doktrin', *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, cilt:25, sayı: 1-2, Mart-Nisan 1968, s. 14.
- Eren, M. A. 'Dijital Deliller ve Delil Yasakları', Doktora Tezi, *Hacettepe Üniversitesi Adli Bilimler Bölümü*, İstanbul, 2023.
- Ergün, B. 'Türkiye ile Avrupa Birliği Arasında Hizmet Ticaretinin Karşılıklı Olarak Serbestleştirilmesi', Doktora Tezi, *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2009.

- Erol, B. ‘Ağ Trafik Özelliklerinin Analizini Yaparak Anormalliklerin Tespit Edilmesi’, Yüksek Lisans Tezi, *İstanbul Aydın Üniversitesi Fen Bilimleri Enstitüsü*, İstanbul, 2019.
- Fidan, B. ‘Çevrimiçi Oyun Oynayan Kişiler ile Oyun Karakterleri Arasındaki Bağlar ve Tüketici Davranışları İlişkisi: Metin2 Ve League Of Legends Örnekleri’, Yüksek Lisans Tezi, *Ankara Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2020.
- Gökalp, Ö. M. *Bilgisayar Ağları ve Adli Bilişim*, Gazi Üniversitesi Gazi Bilişim Enstitüsü, Ankara, 2021
- Gönenç, E. ‘Adli Bilişim ve Elektronik Delillerin Hukuk Yargılamasındaki Yeri’, Yüksek Lisans Tezi, *İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2015.
- Gürel E. ve Şahin, Ç. ‘Dijital Dünyada Kara Para Aklama: Örnek Olaylar’, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, cilt: 57, sayı: 3, 2022, s. 2289-2305, <https://doi.org/10.15659/3.sektor-sosyal-ekonomi.22.09.1890>.
- Işık, B. ‘Karşılıksız Yararlanma Suçu’, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 29, sayı: 3, 2021, s. 2052.
- İleri, Ç. ‘Dijital Miras’ - Alman Federal Mahkemesi’nin ‘Facebook’ Kararı Üzerine Bir İnceleme’, *TBB Dergisi*, sayı: 146, 2020, s. 137-150.
- Kafes, V. ‘Ceza Hukukunda Mağdurun Zararının Giderilmesi’, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 60, sayı: 1, 2011, s. 93.
- Kara, İ. ‘Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi’, *Sakarya University Journal Of Computer And Information Sciences*, cilt: 2, sayı: 2, 2019, s. 62.
- Karakuş, S. ve Turan, S.G. ‘Yetişkinlerin Siber Zorbalık Davranımları ile Dijital Vatandaşlık Becerileri Arasındaki İlişkinin İncelenmesi’, *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, sayı: 49, 2021, s. 410.
- Kaya, A. B. ‘Çevrimiçi Oyun Bağımlılığı Ölçeğinin Geliştirilmesi: Geçerlik ve Güvenirlik Çalışması’, Yüksek Lisans Tezi, *Gaziosmanpaşa Üniversitesi Eğitim Bilimleri Enstitüsü*, Tokat, 2013.

- Kaya, İ.S. ve Çakır, A. ‘Yasak Cihaz veya Programlar Suçu’, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, cilt: 19, sayı: 38, 2020, s. 35.
- Kaya, S. ‘Sosyal Medyada Anonim Olmanın Söylemler Üzerindeki Etkisinin Haber Yorumları Üzerinden İncelenmesi’, *İletişim Kuram ve Araştırma Dergisi*, sayı: 60, 2022, s. 169-171, <https://doi.org/10.47998/ikad.1067590>.
- Kaynakçioğlu, U. ‘Ceza Muhakemesinde Dijital Deliller’, Yüksek Lisans Tezi, *Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2015.
- Kızıltan, M.B. ‘5237 Sayılı Türk Ceza Kanunu’nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları’, Yüksek Lisans Tezi, *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul, 2007.
- Kirova, M. C. ‘Fikir ve Sanat Eserleri Kanunu’nda Manevi, Mali veya Bağlantılı Haklara Tecavüz Suçu’, Yüksek Lisans Tezi, *Antalya Bilim Üniversitesi Lisansüstü Eğitim Enstitüsü*, Antalya, 2023.
- Korkmaz, F. ‘Dolandırıcılık Suçunun Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi’, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 69 sayı: 3, 2020, s. 1423-1424.
- Livingstone, S. ve Third, A. ‘Çevrim İçi Zorbalık: Nedir ve Nasıl Önlenir ?’ *UNICEF*, Ankara, 2020, s. 5.
- Masum, E. ‘Dağıtık Servis Dışı Bırakma Saldırılarının İncelenmesi ve Korunma Yöntemleri’, Yüksek Lisans Tezi, *Ankara Üniversitesi Sağlık Bilimleri Enstitüsü*, Ankara, 2017.
- Mercimek, B., Yaman, N. D., Kelek, A. ve Odabaşı, H. F. ‘Dijital Dünyanın Yeni Gerçeği: Troller’, *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, cilt 6, sayı 1, 2016, s. 67-77.
- Millî Eğitim Bakanlığı, ‘Bilişim Teknolojileri Alt Ağlar’, *Seçkin Yayıncılık*, Ankara, 2012, s. 9-10.
- Nacar, F. B. ‘Avrupa Birliği Ülkeleri ve Türkiye’de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları’, Yüksek Lisans Tezi, *Atılım Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2010.

- Orta, M. 'Bilişim Suçlarında Adli Analiz', Doktora Tezi, *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü*, Konya, 2015.
- Öğün, M. N. ve Kaya, A. 'Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler', *Güvenlik Stratejileri Dergisi*, cilt: 9, sayı: 18, 2013, s. 153.
- Önok, M. 'Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği', *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, cilt 19, sayı 2, 2013, s.1239.
- Özbek, V. Ö. 'Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)', *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 9, Özel Sayı, 2007, s. 1024.
- Özbek, V. Ö. 'İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları', *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*, cilt: 69, sayı: 1-4, 2001, s. 106.
- Özen, M. ve Özocak, G. 'Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)', *Ankara Barosu Dergisi*, 2015/1, s. 51.
- Özkaya, P. 'Dijital Dünyada Çevrimiçi Riskler, Bilişim Suçları ve Mağdur Çocuk', *Türkiye Adalet Akademisi Dergisi*, cilt: 14, sayı: 53, Ocak 2023, s. 13-42.
- Sezgin, S. 'Türkiye'de Dijital Oyun Endüstrisi ve Yaratıcı Emek', Doktora Tezi, *Ankara Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2019.
- Sınar, H. 'Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)', *Kişisel Verileri Koruma Dergisi*, cilt: 2, sayı: 1, 2020, s. 47.
- Şen, E. 'Hırsızlık Suçları', *Ankara Barosu Dergisi*, sayı: 3, 2012, s. 323-324.
- Şenol, D. ve Karataşoğlu, E. B. 'Siber Suçlara Sosyolojik Bakış', *Academic Social Resources*, cilt: 7, sayı: 33, 2022, s. 44.

- Şimşek, S. ‘Mülkiyet Hakkının Kapsamı, Sınırlandırma Nedenleri ve Şartları Açısından 1982 Anayasası ve Avrupa İnsan Hakları Sözleşmesi: Karşılaştırmalı Bir Analiz -I’, *TBB Dergisi*, sayı: 91, 2010, s. 188.
- Taşçı, U. ve Can, A. ‘Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014’, *Fırat Üniversitesi Sosyal Bilimler Dergisi*, cilt: 25, sayı: 2, 2015, s. 230.
- Torun, N. K. ve Torun, T. ‘Kötü Amaçlı Yazılımların E-Ticaret İçerisinde Siber Güvenlik Açısından İncelenmesi’, *Sakarya İktisat Dergisi*, cilt: 11, sayı: 1, 2022, s. 3-4.
- Tunca, S. ‘Modern Çağda Siber Güvenlik Kavramı’, *Dumlupınar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, sayı: 3, 2015, s. 3.
- Türkiye Cumhuriyeti Dijital Dönüşüm Ofisi, ‘Video Oyun Endüstrisi’, Ankara, 2022, s. 15.
- Ulus, H. İ. ve Demirci, M. ‘Kurum İçerisi Saldırıların Tespiti ve Önlenmesi için Sunucu İzleme Uygulaması’, *Gazi Üniversitesi Fen Bilimleri Dergisi*, cilt: 6, sayı: 3, 2018, s. 511, <https://doi.org/10.29109/gujsc.351365>.
- Uysal, E.H. ‘Fikrî Mülkiyet Hukukunda Bilgisayar Oyunlarının Korunması’, Yüksek Lisans Tezi, *Ankara Sosyal Bilimler Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara, 2021.
- Ünal, Y. ve Selçuk, N. ‘Elektronik Bilgi Kaynakları İçin Entelektüel Mülkiyet ve Dijital İçerik Hakları, Düzenleme ve Dijital Ödeme Sistemleri’, *Bilgi Dünyası*, cilt: 1, sayı: 1, 2000, s. 180-191.
- Wood, C. C. ‘Computer Security Alert’, *CSI Members-Only Web / Audio Conference on Incident Response*, New York, Temmuz 2009.
- Yalçın, N. ve Avşar, A. ‘Sosyal Mühendislik Atakları ve Alınması Gereken Önlemler’, *20. Akademik Bilişim 2018 Konferansı Bildirileri*, Malatya, 1-3 Şubat 2018, s. 77.
- Yalçınkaya, B., Ünal, A., Yılmaz, B. ve Özdemirci, F., ‘Bilgi Yönetimi ve Bilgi Güvenliği’, *Ankara Üniversitesi Yayınları*, cilt: 1, sayı:5, 2019, s. 494.

Yargıtay 13. Ceza Dairesi, 2016/2155 Esas No, 2017/10403 Karar No.

Yazıcıoğlu, R.Y. ‘5237 s. TCK.nun 244/4’üncü Maddesinde Düzenlenen “Bilişim Sistemi Marifetiyle Haksız Çıkar Sağlanması” Suçu ile md.142/2-e ve 158/1-f Maddesinde Düzenlenen “Bilişim Sistemlerinin Kullanılması Suretiyle” “Hırsızlık” ve “Dolandırıcılık” Suçlarının İşlenmesi Sorunsalı Üzerine Düşünceler’, *Suç ve Ceza Dergisi*, sayı:4, 2009, s.4-8.

Yeşilyurt, H. ‘Adli Bilişim Soruşturma Metotlarının Standartlaştırılması ve Etkinlik-Verimlilik Perspektifinde Değerlendirilmesi’, *Adli Bilimler Dergisi*, cilt: 13, sayı: 3, Eylül 2024, s. 3.

Yılmaz, S. ‘Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu’, *Ankara Barosu Dergisi*, sayı: 2, 2011, s. 79.

## İnternet Kaynakları

chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://afyonluoglu.org/PublicWebFiles/cyber/legislation/2001Avrupa%20Birli%C4%9Fi%20Siber%20Su%C3%A7lar%20S%C3%B6zleşmesi-TR.pdf, ‘Avrupa Birliği Siber Suçlar Sözleşmesi - Budapeşte Sözleşmesi’, E.T: 30 Ekim 2023.

chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://i.dell.com/sites/csdocuments/Legal\_Docs/en/DellEULA\_English.pdf, ‘EULA Sözleşmesi’, E.T: 01 Kasım 2023.

chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.guvenliweb.org.tr/dosya/nH58Q.pdf, ‘Bilgi Teknolojileri ve İnternetin Bilinçli, Güvenli Kullanımı’, E.T: 24 Kasım 2023.

Herzfeld, O. ‘What Is The Legal Status Of Virtual Goods?’, <https://www.forbes.com/sites/oliverherzfeld/2012/12/04/what-is-the-legal-status-of-virtual-goods/?sh=51076f8b108a>, E.T: 30 Ekim 2023.

<https://ansiklopedi.tubitak.gov.tr/ansiklopedi/antropoloji>, ‘Antropoloji’, E.T: 25 Mart 2024.

- <https://ansiklopedi.tubitak.gov.tr/ansiklopedi/ontolojivarlikbilim>, '*Varlığı ve var olanları nelik ve nasıllıkları bakımından inceleyen felsefe dalıdır. Felsefenin ana disiplinlerinden biri olan metafiziğin alt dalıdır.*', E.T: 25.03.2024.
- <https://ansiklopedi.tubitak.gov.tr/ansiklopedi/psikoloji>, '*Psikoloji, düşünme, hatırlama, öğrenme, problem çözme, muhakeme gibi zihinsel süreçler ile davranışları bilimsel olarak inceleyen bir bilim dalıdır.*', E.T: 25.03.2024.
- <https://bilgem.tubitak.gov.tr/sge/>, '*Siber Güvenlik Eğitimleri*', E.T: 13.09.2023.
- <https://blog.codevist.com/sentetik-kimlik-hirsizligi-nedir-567d73cddb99>, '*Sentetik Kimlik Hırsızlığı Nedir?*', E.T: 12 Nisan 2024.
- <https://diabgm.adalet.gov.tr/Home/SayfaDetay/avrupa-konseyyine-genel-bir-bakis27022020030011>, '*Avrupa Konseyine Genel Bir Bakış*', E.T.: 26.10.2023.
- [https://documentation.my.games/terms/mygames\\_tou](https://documentation.my.games/terms/mygames_tou), '*My Games EULA Sözleşmesi*', E.T: 16 Kasım 2023
- <https://kalkinmaguncesi.izka.org.tr/index.php/2021/02/02/kuresel-pazarlara-giden-yol-dijital-oyun-sektoru/>, '*Küresel Pazarlara Giden Yol: Dijital Oyun Sektörü*', E.T: 27 Ekim 2023.
- <https://law.stackexchange.com/questions/8992/is-legal-to-sell-virtual-goods>, '*Is Legal To Sell Virtual Goods?*', E.T: 30 Ekim 2023.
- <https://mbkaya.com/bilisim-suc-istatistik-turkiye-siber-guvenlik/>, '*Bilişim Suç İstatistikleri - Türkiye Siber Güvenlik*', E.T: 25 Ekim 2023.
- <https://playvalorant.com/tr-tr/news/game-updates/>, '*Oyun Güncellemeleri Valorant*' E.T: 25 Ocak 2024.
- <https://playvalorant.com/tr-tr/news/game-updates/valorant-8-02-yama-notlari/>, '*Valorant 8.02 Yama Notları*', E.T: 25 Ocak 2024.
- <https://turkiye.un.org/tr>, '*Birleşmiş Milletler Türkiye*', E.T.: 26.10.2023.
- [https://www.ab.gov.tr/ab-hukuku-ve-ceviri-daire-baskanligi\\_51631.html](https://www.ab.gov.tr/ab-hukuku-ve-ceviri-daire-baskanligi_51631.html), '*AB Hukuku ve Çeviri Daire Başkanlığı Türkiye Cumhuriyeti Avrupa Birliği Başkanlığı*', E.T: 15.10.2023.

<https://www.bloomberght.com/cin-de-yuksek-mahkeme-dijital-varlik-haklarinin-korunmasi-cagrisinda-bulundu-2260616>, '*Çin'de Yüksek Mahkeme Dijital Varlık Haklarının Korunması Çağrısında Bulundu*', E.T: 30 Ekim 2023.

<https://www.btk.gov.tr/siber-guvenlik-kurulu>, '*Bilgi Teknolojileri ve İletişim Kurumu Siber Güvenlik Kurulu*', E.T: 13.09.2023.

<https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22congress%22%3A118%7D>, '*Legislation Search*', E.T: 30 Ekim 2023.

<https://www.dell.com/eula>, '*Son Kullanıcı Lisans Sözleşmesi (EULA)*', E.T: 30 Ekim 2023.

<https://www.egm.gov.tr/siber>, '*Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele*', E.T: 13.09.2023.

<https://www.epicgames.com/help/tr/fall-guys-c9505712380315/teknik-destek-c9505744757531/son-kullanici-lisans-sozlesmesi-eula-a9505740271131>, '*Son Kullanıcı Lisans Sözleşmesi (EULA)*', E.T: 30 Ekim 2023.

<https://www.icertis.com/contracting-basics/the-importance-of-the-end-user-license-agreement/>, '*The Importance Of The End-User License Agreement*', E.T: 30 Ekim 2023 – 02 Ocak 2024.

<https://www.innova.com.tr/blog/iki-faktorlu-kimlik-dogrulama-2fa-internette-guvende-kalin>, '*İki Faktörlü Kimlik Doğrulama (2FA): İnternette Güvende Kalın*', E.T: 12 Nisan 2024.

<https://www.jandarma.gov.tr/asayis/siber-sucmucdbskligi>, '*Jandarma Genel Komutanlığı Siber Suçlarla Mücadele*', E.T: 13.09.2023.

<https://www.merlininkazani.com/polisler-de-oyun-oyinar-hatta-yayin-bile-acar-haber-123470>, '*Polisler de Oyun Oynar, Hatta Yayın Bile Açar*', E.T: 12 Nisan 2024.

<https://www.playstation.com/tr-tr/support/account/suspensions-psn/>, '*Hesap Askıya Almalar ve Yasaklamalar*', E.T: 31 Ekim 2023.

<https://www.questionpro.com/blog/tr/veri-manipulasyonu-nedir-teknikler-ve-ornekler/>, '*Veri Manipülasyonu Nedir? Teknikler ve Örnekler*', E.T: 22 Ocak 2024.

<https://www.resmigazete.gov.tr/eskiler/2022/12/20221229-5.htm>, '*Elektronik Ticaret Aracı Hizmet Sağlayıcı ve Elektronik Ticaret Hizmet Sağlayıcılar Hakkında Yönetmelik Resmî Gazete Sayı: 32058*', E.T: 31 Ekim 2023.

<https://www.trthaber.com/haber/dunya/guney-kore-nft-oyunlarini-yasaklayacak-640720.html>, '*Güney Kore NFT Oyunlarını Yasaklayacak*', E.T: 29 Ekim 2023.

<https://zhuanlan.zhihu.com/p/260383465>, '*Zhihu*', E.T: 30 Ekim 2023.

Simav, Ö. '*Geç Saatlere Kadar Oyun Yasak*', <https://www.hurriyet.com.tr/aile/yazarlar/oznur-simav/gec-saatlere-kadar-oyun-yasak-401410>, E.T: 29 Ekim 2023.

Yayla, T. '*Sanal Hırsızlık*', <https://talhayayla.av.tr/sanal-mulkiyet/>, E.T: 29 Ekim 2023.