BİLİŞİM HUKUK SEMPOZYUMLARI III
“UZAY, DİJİTAL EVREN VE HUKUK”

24 ARALIK 2025

BİLDİRİ ÖZETLERİ KİTABI

Layiha Yayınevi Press

HACETTEPE ÜNİVERSİTESİ HUKUK FAKÜLTESİ
HACETTEPE ÜNİVERSİTESİ
ADLİ BİLİŞİM ARAŞTIRMA VE UYGULAMA MERKEZİ
BİLİŞİM VE TEKNOLOJİ HUKUKU SEMPOZYUMLARI III
"UZAY, DİJİTAL EVREN VE HUKUK"
BİLDİRİ ÖZETLERİ KİTABI

24.12.2025

Editörler

Doç. Dr. Merve Ayşegül KULULAR İBRAHİM

Dr. Öğr. Üyesi Mehmet ÇOĞALAN

Layiha Yayınevi Press

Kitap Adı/*Book Title*: Bilişim ve Teknoloji Hukuku Sempozyumları III: Uzay, Dijital Evren ve Hukuk (Bildiri Özetleri Kitabı)/*Information and Technology Law Symposiums III: Space, the Digital Universe, and Law (Abstract Book)*
ISBN: 978-625-96572-2-6
DOI: 10.5281/zenodo.18081782

Editörler/*Editors*: Merve Ayşegül Kulular İbrahim (Assoc. Prof., Hacettepe University, Faculty of Law, Ankara/Türkiye, e-mail: kulularmerve@hacettepe.edu.tr, ORCID: 0000-0001-6556-0269)

Mehmet Çoğalan (Asst. Prof., Hacettepe University, Faculty of Law, Ankara/Türkiye, e-mail: mehmetcogalan@hacettepe.edu.tr, ORCID: 0000-0002-1185-2204)

Konu Kategorileri/*Subject Categories*
BISAC: LAW096000 Law/Science & Technology; LAW002000 Law/Air & Space
THEMA: LNU; LNT; GBC
DEWEY: 341.47 Law of OuterSpace

Keywords: Information Technology Law, Space Law, Technology Law, Cyber Law, Digital Universe.

Anahtar Kelimeler: Bilişim Hukuku, Uzay Hukuku, Teknoloji Hukuku Siber Hukuk, Dijital Evren.

Atıf Bilgisi/*Cite as*: *Bilişim ve Teknoloji Hukuku Sempozyumları III: Uzay, Dijital Evren ve Hukuk (Bildiri Özetleri Kitabı).* Layiha Yayınevi, 2025.

Layiha Yayınevi/*Layiha Press*
Yayıncı/*Publisher*: Alan Çalışmaları Derneği/*Area Studies Association* (Sahibata Mah. Başaralı Cad. 6 Rampalı Çarşı 236, Konya, Türkiye)
https://layiha.com.tr
layiha@bilimalani.org
Sertifika No./*Certificate Number*: 78122

Yayın No./*Publication Number*:
Dizi/*Series*: Bilimsel Toplantı
Tasarım ve Dizgi Editörleri/*Design and Layout Editors*: Mustafa Can Dağlı & Esranur Bulduk
Yayın Türü/*Publication Type*: Bildiri Özetleri/*Conference Abstracts*
Yayın Tarihi/*Publication Date*: December 2025
Yayın Yeri/*Place of Publication*: Konya, Türkiye
Yayın Dili/*Language*: Türkçe/*Turkish*
Baskı Sayısı/*Edition*: 1
Ebat/*Dimensions*: 17,6 x 25,01 cm
Sayfa Sayısı/*Page Count*: 74

Değerlendirme Süreci/*Review Process*: Eserde yer alan bildiri özetleri, Düzenleme ve Danışma Kurulu başta olmak üzere hakemler tarafından değerlendirilmiştir. / *The abstracts included in this book were evaluated by referees, primarily the Organizing and Advisory Board.*

Hacettepe Üniversitesi Hukuk Fakültesi
Bilişim ve Teknoloji Hukuku Sempozyumları III
"Uzay, Dijital Evren ve Hukuk"

DANIŞMA KURULU

Hacettepe Üniversitesi Hukuk Fakültesi
Bilişim ve Teknoloji Hukuku Sempozyumları III
"Uzay, Dijital Evren ve Hukuk"

DÜZENLEME KURULU

Prof. Dr. Beşir Fatih DOĞAN (Hacettepe Üniversitesi)

Doç. Dr. Merve Ayşegül Kulular (Hacettepe Üniversitesi)

Doç. Dr. Bayram DOĞAN (Sütçü İmam Üniversitesi)

Dr. Öğr. Üyesi Mehmet Çoğalan (Hacettepe Üniversitesi)

Öğr. Gör. Dr. Ahmet Talha ÖZEN (Hacettepe Üniversitesi)

Arş. Gör. Mustafa Can Dağlı (Hacettepe Üniversitesi)

Arş. Gör. Esranur Bulduk (Hacettepe Üniversitesi)

İÇİNDEKİLER

YAKIN YÖRÜNGE UYDULARI ÜZERİNDEN HABERLEŞME HİZMETLERİ: YETKİLENDİRME VE SİBER GÜVENLİK KAPSAMINDA DEĞERLENDİRME VE ÖNERİLER

EVALUATIONS AND SUGGESTIONS ON LOW ORBIT SATELLITES COMMUNICATION SERVICES IN THE CONTEXT OF LICENSING AND CYBER SECURITY

Bildiri Özeti

Ömer Fatih SAYAN[*]

Özet

Haberleşme teknolojilerinin hızla gelişmesi, her an her yerde bağlantıda olma ihtiyacı ve internete yüksek hızda erişim talepleri, sabit, mobil ve uydu şebekelerinin entegrasyonunu ve yüksek teknolojik hizmetlere imkan veren ve sürekli gelişen daha da kapsayıcı alternatif şebekelerin geliştirilmesini zorunlu kılmaktadır. Uydu sistemleri de özellikle coğrafi açıdan erişimin zor olduğu alanlar başta olmak üzere çeşitli haberleşme ihtiyaçlarına cevap verebilmektedir. Teknolojik gelişmeler ile birlikte, son dönemlerde Yakın Yörünge Uyduları (LEO) üzerinden haberleşme hizmeti sunulması ülkelerin gündeminde üst sıralarda yer almaktadır. Söz konusu sistemlerin mobil şebekeler ile entegrasyonuna yönelik çalışmalar da hız kazanmış durumdadır. Yaşanan gelişmeler ile birlikte, teknik ve hukuki çerçevede LEO uyduları ile ilgili düzenlemelerin yapılması kaçınılmaz olmaktadır. Yetkilendirme başta olmak üzere, kişisel verilerin korunması, kullanıcı hak ve menfaatlerinin gözetilmesi, siber güvenliğin sağlanması, sektörde sürdürülebilir rekabetin temini gibi hususlar, üzerinde hassasiyetle durulması gereken konuların başında gelmektedir. Bu çalışmada, LEO uyduları üzerinden haberleşme hizmeti sunulması teknik ve düzenleyici boyutları ile ele alınmakta, Türkiye için stratejik hususların altı çizilmektedir. Ayrıca, mobil cihazların doğrudan uydu ile entegrasyonu da bu çalışmada ele alınmış, ülkelerin düzenlemelerine yer verilmiş, özellikle Türkiye'nin yerli ve milli haberleşme politikalarıyla

[*] Dr., Ulaştırma ve Altyapı Bakanlığı Bakan Yardımcısı. E-posta: fatihsayan@gmail.com ORCID: 0009-0004-2092-0346

uyumlu olacak şekilde, uydu-karasal şebeke entegrasyonunun etkin bir biçimde hayata geçirilmesine vurgu yapılarak düzenleme ihtiyacı ile ilgili konularda önerilerde bulunulmuştur. Uydu sistemlerine yönelik olası siber saldırı ve tehdit türleri, çeşitli ülkelerde yaşanan siber saldırılar ve siber saldırıların etkileri hakkında değerlendirmeler yapılarak, siber güvenlik ile ilgili alınması gereken önlemlere yer verilmiştir.

Anahtar kelimeler: Alçak yörünge uyduları, Haberleşme, Bilişim hukuku, Lisanslama, Siber Güvenlik

Abstract

The rapid development of communication technologies, demand for connection anytime, anywhere, and increasing demand for high-speed access to the internet necessitate the integration of fixed, mobile and satellite networks. In that respect, development of more inclusive alternative networks that enable high-tech services are constantly developing. Satellite systems respond to communication needs in different areas, especially in areas where difficulty in access due to geography. With technological developments, the provision of communication services via Low Orbit Satellites (LEO) has recently been at the top of the agenda of countries. Studies on the integration of these systems with mobile networks have also gained momentum.

It is inevitable for countries to make necessary regulations regarding LEO satellites in both technical and legal dimensions. Issues such as authorization, protection of personal data, protection of user rights and interests, ensuring cyber security, and ensuring sustainable competition in the sector are among the issues that need to be considered throughly. In this study, the provision of communication services over LEO satellites is discussed with the technical and regulatory dimensions, and strategic issues for Türkiye are underlined.

In addition, the issue of Direct to Device is discussed, examples of regulation of several countries are given and some suggestions for Türkiye are made by emphasizing the effective implementation of satellite-terrestrial network integration in line with Türkiye's national communication policies. Siber security issues sorrounding satellite systems are explained with possible types of cyber attacks and threats against satellite systems, cyber attacks in various

countries and the effects of cyber attacks. Necessary measures and recommendation are given in this study on the subject.

Keywords: Low Earth Orbit Satellites, Communication, Information Technology Law, Licensing, Cybersecurity

UZAYIN TİCARİLEŞMESİ: STARLINK ÖRNEĞİ VE UZAY HUKUKU PERSPEKTİFİNDEN BİR DEĞERLENDİRME

THE COMMERCIALIZATION OF SPACE: THE STARLINK EXAMPLE AND AN ASSESSMENT FROM THE PERSPECTIVE OF SPACE LAW

Bildiri Özeti

Tamer SOYSAL[*]

Özet

Uydu takımyıldızı, küresel kapsama alanı sağlamak için birleştirilmiş bir sistem şeklinde çalışan homojen/hetorejen uzay araçları topluluğu olarak ifade edilir. Geniş bant internet erişimi sağlama yolunda ilk başarılı girişim, 2003 yılında Eutelsat tarafından e-Bird uydusunun fırlatılmasıyla gerçekleştirilmiştir. Süreç içinde Eutelsat'ın OneWeb; SpaceX'in Starlink ve Amazon'un Kuiper uydu takımyıldızları gönderilmiştir. 2019 yılında uydu fırlatmaya başlayan Starlink, başlangıçta 12.000 uydu planlaması yapmışken, bugün uydu sayısını 42.000 uyduya çıkarılması düşünülmektedir. Günümüzde 9.000 civarında starlink uydusunun uzayda bulunduğu ifade ediliyor. 10 yıl içinde, toplam uydu sayısının 100 binleri bulması beklenmektedir. Bu uydular alçak dünya yörüngesinde konuşlandırılmaktadır. Uzay hukukuna ilişkin temel uluslararası metinler, temel olarak devletlerin egemen olduğu bir düzen ön kabulü ile hareket edilerek hazırlanmıştır. Küresel internet bağlantısı, afet müdahalesi destekleri ve dijital uçurumu azaltma gibi faydaları bulunan bu uydu takımyıldızları bir takım önemli sorun alanları da oluşturmaktadır. Uzay artığı oluşturma, çevresel etkiler, uzayın gözetilmesine ilişkin sorunlar oluşturma yanında devlet dışı aktörler aracılığıyla uzay üzerinde özel mülkiyet benzeri ticari faydalar sağlanması en önemli konu olarak öne çıkmaktadır. Günümüzde 117 ülkenin taraf olduğu 1967 tarihli Dış Uzay Antlaşmasıyla uzayın sahiplenemezliği ilkesi kabul edilmiştir. Ayrıca uzayın keşfi ve kullanımının tüm devletlerin barış ve çıkarına uygun olarak tüm insanlığın yetkisinde olduğu

[*] Doç. Dr., Cumhuriyet Savcısı-Ankara Bölge Adliye Mahkemesi. E-posta: tamer.soysal@adalet.gov.tr ORCID: 0000-0001-6763-5041

belirtilmiştir. Öte yandan sorumluluk konusunda da Uzay Antlaşması'nın 6 ve 7 nci maddeleriyle temel olarak devletlerin sorumlu olduğu esası kabul edilmiştir. 1972 tarihli Uzay Sorumluluk Sözleşmesi'yle de aynı esaslar kabul edildiği görülmektedir.

Bildiri ile her geçen gün sayısı artan uydu takımyıldızları nedeniyle oluşabilecek çarpışma, çevre etkileri ve hatta askeri kullanım nedeniyle oluşabilecek zararlara karşı uluslararası uzay hukuku düzenlemeleri bağlamında bir değerlendirme yapılmaya çalışılacaktır. Bu kapsamda yeni bir uluslararası metnin gerekli olup olmadığı da tartışmaya açılacaktır.

Anahtar kelimeler: Uzay hukuku, Uzay Antlaşması, Uzay Sorumluluk Antlaşması, uzay enkazı, Starlink, Uydu Takımyıldızları, Zarar, Sorumluluk.

Abstract

A satellite constellation is defined as a collection of homogeneous/heterogeneous spacecraft operating as an unified system to provide global coverage. The first successful initiative to provide broadband internet access was launched in 2003 by Eutelsat with the launch of the e-Bird satellite. Since then, Eutelsat's OneWeb, SpaceX's Starlink, and Amazon's Kuiper satellite constellations have been launched. Starlink, which began launching satellites in 2019, initially planned for 12,000 satellites, but today it is considering increasing the number of satellites to 42,000. It is stated that there are currently around 9,000 Starlink satellites in space. Within 10 years, the total number of satellites is expected to reach 100,000. These satellites are deployed in low Earth orbit (LEO). Fundamental international treaties on space law have been drafted based on the premise that states have sovereignty over space. While these satellite constellations offer benefits such as global internet connectivity, disaster response support, and reducing the digital divide, they also raise a number of significant issues. The most important issues that stand out are the creation of space debris, environmental impacts, problems related to the monitoring of space, and the provision of commercial benefits similar to private property in space through non-state actors. The principle of the non-appropriability of space was accepted with the 1967 Outer Space Treaty, to which 117 countries are currently parties. It also states that the exploration and use of outer space shall be carried out for the benefit

and in the interest of all countries and shall be the province of all mankind. On the other hand, Articles 6 and 7 of the Outer Space Treaty essentially accept that states are responsible. The same principles are accepted in the 1972 Space Liability Convention.

The paper will attempt to assess the potential damage that could arise from collisions, environmental impacts, and even military use due to the increasing number of satellite constellations, within the context of international space law. In this regard, the necessity of a new international regulations will also be discussed.

Keywords: Space law, Outer Space Treaty, Space Liability Convention, space debris, Starlink, Satellite Constellations, Damage, Liability.

OTONOM UYDULARIN KARAR DÖNGÜSÜ VE UZAY HUKUKUNDA SORUMLULUK TARTIŞMALARI

THE DECISION-MAKING CAPABILITY OF AUTONOMOUS SATELLITES AND THE PARADIGM OF LEGAL RESPONSIBILITY IN OUTER SPACE

Bildiri Özeti

Gökhan KURT[*]

Özet

Bu çalışma ile, otonom uydu sistemlerine ait teknik karar döngüsü ile bu döngünün halihazırdaki mevcut uzay hukuku açısından ortaya çıkardığı sorumluluklar eksenindeki tartışmalar kapsamlı biçimde ele alınmıştır. Uydulara entegre edilen yapay zeka uygulamaları ile bu araçlar artık sadece veri toplayan pasif yapılar değil çevresini algılayabilen, elde ettiği verileri işleyebilen, bağımsız bir biçimde karar verebilen ve bu kararları da eyleme dönüştürebilen bilişsel sistemler olmaktadırlar. Bu tip tam otonom bilişsel sistemler uzay hukuku bakış açısından ele alındığında klasik uzay hukuku yaklaşımının dayandığı "insan merkezli sorumluluk" ilkesi sorgulanabilir bir hale dönüşmektedir. Özellikle de uydunun sensor birimlerinden alınan verilerin işlenmesi, hedeflerin belirlenmesi ve de eylem kararlarının otomatik olarak alınması esnasında meydana gelebilecek önemli algoritmik hatalar bilişsel riskler yaratabilecektir.

Bu çalışmada, otonom uydu sistemlerinin algılama, veri işleme, karar verme ve eylem aşamaları mühendislik perspektifinden incelenmiş, her bir aşamada meydana gelebilecek teknik hataların sonucunda hukuki sorumluluk doğuracak etkilere vurgu yapılmıştır. Uydunun veri işleme ve karar verme aşamalarında oluşan hataların failinin kim olacağı sorusu ile mevcut hukuki çerçeve sorguya açık hale getirilmiştir. Bu tip durumlarda mevcut hukuki çerçevenin net biçimde tanımlanamaması söz konusudur. Outer Space Treaty (1967) ve Liability Convention (1972) gibi temel metinler, insan denetiminde

[*] Dr., TÜBİTAK Uzay Teknolojileri Araştırma Enstitüsü. E-posta: gokhan83kurt@gmail.com ORCID: 0000-0002-1210-4013

yürütülen uzay faaliyetleri için yeterli bir dayanak sunarken; otonom sistemlerin özerk karar alma yetisi bu düzenlemelerin sınırlarını aşmaktadır.

Bu bağlamda uzay çalışmalarında önümüzdeki yıllarda başat teknoloji haline gelecek otonom uydu sistemleri için bu konu ön plana çıkarılmaktadır. Çalışmada herhangi hukuki bir model önerilmemekle birlikte, söz konusu teknolojik gelişmelerin hukuk sisteminde yaratacağı olası boşluklara dikkat çekilmek istenmektedir. Böylelikle hukuk uzmanlarına bu konuda yeni tartışma alanlarının açılması amaçlanmaktadır. Yapay zeka destekli otonom uydu sistemlerinin uzay ortamında gittikçe yaygınlaşmasıyla birlikte, veri güvenliği, yapay zeka etiği ve uluslararası sorumluluk ilkelerinin bütüncül bir biçimde yeniden ele alınması gerekliliği düşünülmektedir. Böyle bir farkındalık ile, hem uzayda güvenli olarak faaliyetlerin sürdürülmesi hem de gelecekte insan ile makinelerin ortak karar verdiği yeni çağın hukuk temellerinin düşünülmesi açısından kritik bir rol oynayacaktır. Bu tür çalışmalar, mühendislik temelli bulguların hukukla etkileşimin güçlendirmeyi hedefleyerek, disiplinler arası etkileşimi güçlendirecek ve hem bilimsel hem de hukuki gelişmelere yön verecektir.

Anahtar Kelimeler: Otonom uydu, yapay zeka, veri işleme, karar verme, uzay hukuku, sorumluluk

Abstract

This study comprehensively examines the technical decision-making cycle of autonomous satellite systems and the related discussions on legal responsibility within the framework of current space law. With the integration of artificial intelligence applications into satellites, these systems have evolved from being merely passive data collectors into cognitive entities capable of perceiving their environment, processing acquired data, making independent decisions, and translating those decisions into actions. When such fully autonomous cognitive systems are evaluated from the perspective of space law, the classical "human-centered responsibility" principle becomes increasingly questionable. In particular, during the processing of sensor data, target selection, and autonomous decision-making, significant algorithmic errors may occur, giving rise to cognitive risks.

In this study, the perception, data processing, decision-making, and action phases of autonomous satellite systems are analyzed from an engineering perspective, emphasizing the potential legal liabilities that may arise from technical errors in each stage. The question of who should be deemed responsible for errors occurring during the data processing and decision-making phases renders the current legal framework open to interpretation. In such cases, the existing legal regime remains insufficiently defined. While foundational texts such as the Outer Space Treaty (1967) and the Liability Convention (1972) provide a solid basis for space activities conducted under human supervision, the autonomous decision-making capability of these systems extends beyond the scope of these instruments.

In this context, the issue gains prominence as autonomous satellite systems are expected to become a dominant technology in future space operations. Although this study does not propose a specific legal model, it aims to highlight the potential gaps that such technological developments may create within legal systems. The intention is to open new fields of discussion for legal experts. As AI-supported autonomous satellites become increasingly prevalent in space, it will be essential to reconsider data security, AI ethics, and international liability principles in an integrated manner. Raising awareness in this regard will play a critical role in ensuring safe operations in outer space and in shaping the legal foundations of a new era in which humans and machines jointly make decisions.

Keywords: Autonomous satellite, artificial intelligence, data processing, decision-making, space law, liability

SAVUNMA SANAYİİ PERSPEKTİFİNDEN UZAY TABANLI YAPAY ZEKÂ SİSTEMLERİNİN HUKUKİ DEĞERLENDİRİLMESİ

A LEGAL ASSESSMENT OF SPACE-BASED ARTIFICIAL INTELLIGENCE SYSTEMS FROM THE PERSPECTIVE OF THE DEFENSE INDUSTRY

Bildiri Özeti

Elife Filiz GÖKDAŞ[*]

Özet

Uzay tabanlı yapay zekâ (YZ) sistemleri, yalnızca bilimsel ve sivil amaçlarla değil; keşif-gözlem (ISR), komuta-kontrol (C2), otonom görev planlama ve savunma operasyonlarında da giderek artan bir şekilde kullanılmaktadır. Uydu tabanlı görüntüleme, hedef sınıflandırma, veri analizi ve çarpışma önleme gibi uygulamalar, savunma sanayiinde operasyonel etkinliği artırırken aynı zamanda hukuki sorumluluk, etik uyumluluk ve denetim sorunlarını gündeme getirmektedir. Bu çerçevede uzay tabanlı YZ, teknolojik ilerlemenin yanı sıra, devletlerin ve özel aktörlerin uzay hukukundaki yükümlülüklerini yeniden yorumlamayı zorunlu kılan çok katmanlı bir olgu haline gelmiştir.

Savunma amaçlı uzay tabanlı YZ teknolojilerinin hukuki açıdan doğurduğu sorunların merkezinde, insan denetiminin azalmasıyla birlikte ortaya çıkan sorumluluk boşlukları yer almaktadır. Özellikle otomatik hedef tanımlama hataları, kriz anlarında otonom kararların uluslararası insancıl hukukla uyumluluğu ve veri güvenliği gibi meseleler, kimin "hukuken sorumlu" sayılacağı konusunda belirsizlik yaratmaktadır. Bu bağlamda "anlamlı insan denetimi" (meaningful human control) ilkesi, insan unsurunun karar süreçlerindeki konumunu korumak ve sorumluluk zincirini belirginleştirmek açısından kilit bir ilke olarak öne çıkmaktadır. Ancak mevcut düzenlemelerde bu ilkenin ne ölçüde uygulanabilir olduğu açık değildir.

[*] Avukat, Uzm. Arb. TOBBUYUM Uzay Hukuku Komisyon Uzmanı. E-posta: eliffilizgokdas@gmail.com ORCID: 0009-0009-5194-6916.

1972 tarihli Uzay Nesnelerinin Neden Olduğu Zararlardan Dolayı Uluslararası Sorumluluk Sözleşmesi (Liability Convention) ve 1967 tarihli Uzay Antlaşması (Outer Space Treaty), uzay faaliyetlerinde devletlerin sorumluluğuna dair temel çerçeveyi oluşturmakla birlikte, otonom YZ karar zincirleri nedeniyle ortaya çıkan dolaylı ve karmaşık neden-sonuç ilişkileri karşısında yetersiz kalmaktadır. Avrupa Uzay Ajansı (ESA), OECD ve NATO gibi kuruluşlar, yapay zekâya ilişkin etik ilkeler geliştirse de savunma ve güvenlik temelli uygulamalar için bağlayıcı, yeknesak bir mekanizma bulunmamaktadır. AB Yapay Zekâ Tüzüğü'nün (AI Act) askeri kullanımları kapsam dışında bırakması da çift kullanımlı (dual-use) sistemlerde hukuki belirsizlik yaratmaktadır.

Bu çalışma, savunma sanayii bağlamında uzay tabanlı YZ sistemlerinin hukuki uyumluluğunu artırmaya yönelik çözüm önerileri sunmaktadır. Bunlar arasında; tedarik sözleşmelerinde YZ'ye özgü garanti ve yazılım doğrulama hükümlerinin açıkça düzenlenmesi, operasyonel görevlerde insan müdahalesinin kapsamının teknik ve hukuki standartlara göre tanımlanması, sistem karar süreçlerine ilişkin kayıt ve izlenebilirlik yükümlülüklerinin oluşturulması, saha testleri ve bağımsız denetimlerle güvenilirliğin doğrulanması ve uluslararası düzeyde sorumluluk paylaşımına dair asgari hukuki standartların belirlenmesi bulunmaktadır. Sonuç olarak, savunma uygulamalarında uzay tabanlı YZ'nin hızla gelişen yapısı karşısında, uluslararası hukuk normlarının güncellenmesi ve "anlamlı insan denetimi" ilkesinin hem teknik hem hukuki boyutlarda standartlaştırılması gerekmektedir.

Anahtar Kelimeler: Yapay zekâ, Uzay hukuku, Savunma sanayii, Hukuki sorumluluk, Anlamlı insan denetimi

Abstract

Space-based artificial intelligence (AI) systems are increasingly utilized not only in civilian missions but also in intelligence, surveillance, reconnaissance (ISR), command-and-control (C2), autonomous mission planning, and defense operations. Applications such as satellite-based imaging, target classification, data analysis, and collision avoidance enhance operational efficiency while introducing new legal and ethical challenges related to accountability, transparency, and human oversight. Consequently, space-

based AI has become a multidimensional phenomenon requiring the reinterpretation of state and private actor obligations under space law.

The central legal issues surrounding defense-oriented space AI concern the diminishing role of human control and the resulting accountability gaps. Errors in automated target identification, compliance of autonomous actions with international humanitarian law, and data integrity concerns all raise uncertainty over who qualifies as the "legally responsible" actor. Within this context, the principle of meaningful human control plays a pivotal role in preserving human oversight and clarifying responsibility chains; yet, its practical implementation within existing legal regimes remains ambiguous.

While the 1972 Convention on International Liability for Damage Caused by Space Objects (Liability Convention) and the 1967 Outer Space Treaty establish foundational state responsibility norms, they prove insufficient when faced with the indirect and complex causalities produced by autonomous AI systems. International organizations such as ESA, OECD, and NATO have developed ethical frameworks for AI, but no harmonized, binding regime addresses defense-specific use. Moreover, the exclusion of military applications from the scope of the EU Artificial Intelligence Act perpetuates legal uncertainty for dual-use systems.

This paper proposes several practical approaches to enhance legal compliance in defense-related space AI operations: explicitly incorporating AI-specific warranty and software verification clauses into procurement contracts; clearly defining the scope of human intervention in accordance with technical and legal standards; establishing detailed record-keeping and traceability obligations; verifying system reliability through field testing and independent audits; and developing minimum international standards for liability sharing. Ultimately, bridging the gap between rapidly evolving space-based AI technologies and international legal norms requires the modernization of regulatory instruments and the institutionalization of meaningful human control both technically and legally.

Keywords: Artificial intelligence, Space law, Defense industry, Legal liability, Meaningful human control

ASTRONOTLARIN BEYİN DEĞİŞİMLERİ VE GELECEKTEKİ UZAY YERLEŞKELERİ: YAPAY ZEKÂ, NÖROBİLİM, UZAY HUKUKU VE İNSAN HAKLARI PERSPEKTİFİNDEN BİR DEĞERLENDİRME

ASTRONAUTS BRAIN CHANGES AND FUTURE SPACE SETTLEMENTS: AN AI, NEUROSCIENCE, SPACE LAW, AND HUMAN RIGHTS PERSPECTIVE

Bildiri Özeti

Najiba RAFIZADE[*]
Gözde SONAY[**]
Maral Gül EROL[***]
Ezgi Nur ÖZÇELEN [****]
İkbalnur ZORLU[*****]

Özet

Astronotların beyninde uzay görevleri sonucunda meydana gelen değişimler, gelecekte kurulması planlanan uzay yerleşkelerini şekillendiren temel unsurlardan biri hâline gelmektedir. Mikrogravite ortamı, yüksek seviyeli kozmik radyasyon ve uzun süreli izolasyon, insan beyninin bilişsel süreçleri, duygusal dengesi ve karar verme mekanizmaları üzerinde derin etkiler yaratmaktadır. Bu nedenle, insanlığın uzayda kalıcı yaşam alanları oluşturma hedefi sadece teknolojik inovasyonlarla değil, aynı zamanda nörobiyolojik verilerin dikkatle değerlendirilmesiyle mümkün olabilir. Uzayda uzun süre kalan bireylerin beyin yapısında görülen ventriküler genişleme, beyaz madde bağlantılarında değişim ve sıvı dağılımındaki kaymalar, gelecekteki sosyal

[*] Doktora Öğrencisi, Çalışma Ekonomisi ve Endüstri İlişkileri, Kocaeli Üniversitesi. E-posta: rafizade_najiba@yahoo.com ORCID: 0000-0002-8750-3916
[**] Dr., İstanbul Bakırköy Hava Harp Okulu Birinci Basamak Muayene Merkezi Askeri Sağlık Birimi. E-posta: gozdesonayy@gmail.com ORCID: 0000-0002-8100-0920
[***] Av. Ankara Barosu. E-posta: advocate_maral@hotmail.com ORCID: 0009-0004-8802-672X
[****] Öğrenci, Haliç Üniversitesi, Siyaset Bilimi ve Uluslararası İlişkiler. E-posta: ezgiozcelen@gmail.com ORCID: 0009-0003-7215-9133
[*****] Öğrenci, Atılım Üniversitesi, Hukuk. E-posta: ikbalnurzorlu@gmail.com ORCID: 0009-0000-0621-1202

yaşam modellerinin, çalışma düzenlerinin ve etik uygulamaların yeniden ele alınmasını zorunlu kılmaktadır. Bu durum, yalnızca sağlık risklerinin yönetilmesini değil; aynı zamanda bilişsel kapasite, karar verme yetisi ve psikolojik dayanıklılığın hukuki ve etik çerçevelerle uyumlu şekilde korunmasını da gerektirir. Buna ek olarak, uzayda ekip dinamiklerinin, liderlik süreçlerinin ve kişisel davranış kalıplarının da nörobiyolojik etkiler ışığında yeniden tanımlanması gerektiği görülmektedir. Bu bağlamda, uzay yerleşkelerinin tasarımında disiplinlerarası bir yaklaşım kaçınılmazdır. Nörobilim, etik, hukuk, yapay zekâ ve tıp bilimleri bir arada düşünülmeden uzun süreli yaşam stratejileri sürdürülebilir olamaz. Özellikle insan haklarının ve temel özgürlüklerin uzayda nasıl korunacağı, nörobiyolojik değişimlerin toplumsal düzeni nasıl etkileyeceği ve yapay zekâ destekli sistemlerin gözetim ile özerklik arasındaki dengeyi nasıl kuracağı önemli araştırma alanlarıdır. Bu çalışma, beyin yapısındaki nörolojik değişimlerin anlaşılmasında nörobilim ile yapay zekânın rolünü incelemekte; ayrıca uzay yaşamının sürdürülebilirliğini destekleyecek uyarlanabilir hukuk mekanizmalarının geliştirilmesine odaklanmaktadır. Tartışılan temel konular arasında yapay zekânın dinamik hukuk sistemlerinin oluşturulmasındaki işlevi, gelişmiş beyin görüntüleme teknolojilerinin yargı süreçlerine entegrasyonu ve mikrogravite koşullarında nöroplastisiteyi temel alan rehabilitasyon programlarının tasarımı yer almaktadır.

Anahtar kelimeler: uzay hukuku, nörobilim, nörohukuk, yapay zekâ, insan hakları, uzay yerleşkeleri

Abstract

The changes occurring in astronauts' brains as a result of space missions are becoming one of the fundamental factors shaping future planned space settlements. The microgravity environment, high levels of cosmic radiation, and prolonged isolation create profound effects on the human brain's cognitive processes, emotional balance, and decision-making mechanisms. Therefore, humanity's goal of creating permanent living spaces in space can be achieved not only through technological innovations but also through careful evaluation of neurobiological data. Ventricular enlargement observed in the brain structure of individuals who remain in space for extended periods, changes in white matter connections, and shifts in fluid distribution

necessitate a reconsideration of future social life models, work arrangements, and ethical practices. This situation requires not only the management of health risks but also the protection of cognitive capacity, decision-making ability, and psychological resilience in harmony with legal and ethical frameworks. Additionally, it is evident that team dynamics, leadership processes, and personal behavioral patterns in space must be redefined in light of neurobiological effects. In this context, an interdisciplinary approach in the design of space settlements is inevitable. Long-term survival strategies cannot be sustainable without considering neuroscience, ethics, law, artificial intelligence, and medical sciences together. Particularly important research areas include how human rights and fundamental freedoms will be protected in space, how neurobiological changes will affect social order, and how AI-supported systems will establish the balance between surveillance and autonomy. This study examines the role of neuroscience and artificial intelligence in understanding neurological changes in brain structure, while also focusing on the development of adaptive legal mechanisms to support the sustainability of space life. Key topics discussed include the function of artificial intelligence in creating dynamic legal systems, the integration of advanced brain imaging technologies into judicial processes, and the design of rehabilitation programs based on neuroplasticity under microgravity conditions.

Keywords: space law, neuroscience, neurolaw, artificial ıntelligence, human rights, space settlements

GNSS UYGULAMALARI İLE AFET MÜDAHALE OPERASYONLARININ GELİŞTİRİLMESİ

ENHANCING DISASTER RESPONSE OPERATIONS WITH GNSS APPLICATIONS

Bildiri Özeti

Abdurrahman ONAY*

Özet

Son birkaç on yılda doğal afetlerin sıklığı ve şiddeti, hızlı kentleşme, çevresel bozulma ve iklim değişikliğinin etkisiyle önemli ölçüde artmıştır. Bu karmaşık afetler; hazırlık, müdahale ve iyileştirme süreçlerinde çok disiplinli, teknoloji odaklı bir yaklaşım gerektirmektedir. Küresel Navigasyon Uydu Sistemleri (GNSS) — GPS (Amerika Birleşik Devletleri), GLONASS (Rusya), Galileo (Avrupa Birliği) ve BeiDou (Çin) — modern afet yönetim operasyonlarının vazgeçilmez araçları hâline gelmiştir. GNSS, yüksek hassasiyetli konumlama, zamanlama ve yön bulma olanağı sağlayarak, afet anında sahadaki ekiplerin ve yöneticilerin gerçek zamanlı olarak koordinasyon kurmalarına imkân tanır. GNSS uyduları Dış Uzay Andlaşması'nın I. Maddesi kapsamında uzaydaki faaliyetlerine serbestçe devam etmektedir.

Bu çalışma, GNSS teknolojilerinin afet müdahalesini güçlendirmek amacıyla dünya genelinde nasıl kullanıldığını incelemekte ve bu küresel uygulamaları Türkiye'nin Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) çatısı altındaki ulusal sistemiyle karşılaştırmaktadır. Ayrıca uzay hukukunun önemini vurgulamaktadır. Çeşitli vaka analizleri, iyi uygulama örnekleri ve performans değerlendirmeleri üzerinden, GNSS uygulamalarına ilişkin fırsatlar ve karşılaşılan zorluklar belirlenmiştir. Çalışmanın amacı, uydu tabanlı coğrafi istihbaratın (geospatial intelligence) afet dayanıklılığını güçlendirmek için stratejik öneriler sunmaktır. Japonya'nın GEONET sistemi ve ABD'nin FEMA GPS ağları gibi uluslararası örnekler, tehlike izleme ve hızlı müdahale süreçlerinde GNSS'in değerini ortaya koymaktadır. Türkiye'de ise TUSAGA-

* Avukat, Konya İl Afet ve Acil Durum Müdürlüğü. E-posta: avukat.onay@gmail.com ORCID: 0000-0001-8355-0734

Aktif (CORS-TR) ağı, AYDES Bilgi Sistemi ve AFAD'ın mobil GNSS çözümleri, güçlü bir coğrafi veri altyapısı oluşturmuştur. Bu sistemler, santimetre düzeyinde hassasiyetle hasar tespiti, kaynak takibi ve saha koordinasyonu sağlamaktadır.

Sonuç olarak, bulgular GNSS'in Coğrafi Bilgi Sistemleri (CBS), Uzaktan Algılama (UA) ve İnsansız Hava Araçları (İHA) gibi tamamlayıcı teknolojilerle bütünleştirilmesinin önemini vurgulamaktadır. Böylece, veri odaklı ve bütünleşik bir afet yönetimi ekosistemine ulaşmak mümkün olacaktır. Çalışma, Türkiye ve benzeri gelişmekte olan ülkeler için GNSS kullanımını güçlendirecek politika önerileri ve kapasite geliştirme stratejileri önermektedir.

Anahtar Kelimeler: Uzay, GNSS, Afetler, Uzay Hukuku.

Abstract

The frequency and severity of natural disasters have significantly increased over the last few decades as a result of rapid urbanization, environmental degradation, and climate change. These complex emergencies demand a multidisciplinary, technology-driven approach to enhance preparedness, response, and recovery. Global Navigation Satellite Systems (GNSS) — including GPS (United States), GLONASS (Russia), Galileo (European Union), and BeiDou (China) — have emerged as vital tools in modern disaster management operations. GNSS enables high-precision positioning, timing, and navigation, allowing first responders and emergency managers to coordinate effectively in real-time. GNSS satellites continue their activities in space freely within the scope of Article I of the Outer Space Treaty.

This study examines how GNSS technologies are used globally to enhance disaster response operations, and then compares these international applications with Turkey's national framework under the Disaster and Emergency Management Authority (AFAD). This study also highlights the importance of space law.Through a comprehensive review of case studies, best practices, and performance analyses, this paper identifies both opportunities and challenges associated with GNSS implementation. It aims to provide strategic insights for strengthening national disaster resilience through improved integration of satellite-based geospatial intelligence. Globally, GNSS-supported systems like Japan's GEONET and the United

States' FEMA GPS networks have proven invaluable for monitoring hazards and coordinating rapid interventions. In Turkey, initiatives such as the TUSAGA-Aktif (CORS-TR) network, AYDES Information System, and AFAD's mobile GNSS tools have created a resilient geospatial infrastructure. These systems enable centimeter-level accuracy for rapid damage assessment, resource tracking, and real-time field coordination.

Ultimately, the findings highlight the necessity of combining GNSS with complementary technologies such as Geographic Information Systems (GIS), Remote Sensing (RS), and Unmanned Aerial Vehicles (UAVs) to achieve a comprehensive, data-driven disaster management ecosystem. The paper concludes by recommending policy measures and capacity-building strategies for Turkey and similar developing nations to enhance GNSS utilization for effective disaster response.

Keywords: Space, GNSS, Disasters, Space Law

SİMÜLASYONDAN TEKLİĞE: UZAYDA DİJİTAL İKİZLERİN HUKUKİ VE ETİK BOYUTLARI

FROM SIMULATION TO SINGULARITY: LEGAL AND ETHICAL DIMENSIONS OF DIGITAL TWINS IN SPACE

Bildiri Özeti

Maral Gül EROL[*]

Özet

Günümüzde, bir yandan teknolojik tekilliğin potansiyel risklerine ilişkin farkındalık artarken, öte yandan dijital ikizlerin uzay araştırmalarındaki stratejik değeri giderek daha belirgin hâle gelmektedir. Dijital ikiz teknolojisi, fiziksel sistemlerin veya nesnelerin davranışını, performansını ve mevcut durumunu gerçek zamanlı olarak modelleyen veri odaklı sanal temsiller olarak tanımlanmaktadır. Uzay araştırmalarında dijital ikizler; görev simülasyonları, uzay araçlarının operasyonel analizi, bakım ve optimizasyon süreçlerinin geliştirilmesi ile astronot sağlık izleme uygulamalarında önemli bir rol oynamaktadır. Bu modeller, karmaşık sistem davranışlarının anlaşılmasını kolaylaştırmakta; operasyonel risklerin değerlendirilmesi, olası arızaların öngörülmesi ve süreçlerin verimliliğinin artırılması açısından kritik bir araç olarak kullanılmaktadır. Dijital ikizlerin yapay zekâ ile entegrasyonu, uzay teknolojilerinin yönetimi ve yönetişim süreçlerinde analiz, tahmin ve simülasyon kapasitesini önemli ölçüde genişletmektedir. Bu entegrasyon, çok kaynaklı veri yapılarına uyum sağlamayı, senaryo planlamasını ve sistem optimizasyonunu mümkün kılarak karar alma süreçlerine katkı sunmaktadır. Bununla birlikte, dijital ikiz teknolojilerinin geniş ölçekte kullanımı, veri güvenliği, veri yönetimi, sistem bütünlüğü ve sorumluluk paylaşımı gibi hukuki ve etik soruları gündeme getirmektedir. Büyük ölçekli veri işleme süreçlerinin doğası gereği ortaya çıkan siber güvenlik riskleri ile hassas bilgilerin korunmasına yönelik gereksinimler, ulusal düzenlemelere ve uluslararası standartlara uyumlu yönetişim mekanizmalarını zorunlu kılmaktadır. Ayrıca

[*] Av. Ankara Barosu. E-posta: advocate_maral@hotmail.com ORCID: 0009-0004-8802-672X

dijital ikizlerin ürettiği verilerin ve oluşturduğu analiz sonuçlarının fikri mülkiyet kapsamındaki hukuki statüsü net değildir. Bu belirsizlik, akademik, ticari ve endüstriyel uygulamalarda yeni düzenleme ihtiyaçlarını ortaya çıkarmaktadır. Hızla gelişen teknoloji, uluslararası düzenlemelerin uyarlanmasını ve iş birliği mekanizmalarının güçlendirilmesini zorunlu kılmaktadır. Bu çalışma, dijital ikizlerin uzay araştırmalarında doğurduğu hukuki ve etik meseleleri kapsamlı biçimde ele almakta; veri yönetişimi, sorumluluk paylaşımı ve çok disiplinli iş birliğinin gerekliliğini vurgulamaktadır.

Anahtar Kelimeler: Dijital İkiz, Yapay Zekâ, Uzay, Hukuk, Etik

Abstract

Today, while awareness of the potential risks associated with technological singularity continues to rise, the strategic value of digital twins in space research is becoming increasingly evident. Digital twin technology is defined as data-driven virtual representations that model the behavior, performance, and real-time status of physical systems or objects. In space research, digital twins play a significant role in mission simulations, operational analysis of spacecraft, the development of maintenance and optimization processes, and astronaut health monitoring applications. These models facilitate understanding of complex system behaviors and serve as critical tools for assessing operational risks, predicting potential failures, and improving procedural efficiency. The integration of digital twins with artificial intelligence significantly expands analytical, predictive, and simulation capacities within the management and governance of space technologies. This integration supports compatibility with multi-source data structures, enables scenario planning, and allows for system optimization, thereby contributing to more effective decision-making processes. Nevertheless, the large-scale use of digital twin technologies raises important legal and ethical questions, including data security, data governance, system integrity, and the allocation of responsibility. The nature of extensive data processing activities introduces cybersecurity risks and heightens the need for governance mechanisms aligned with national regulations and international standards to ensure the protection of sensitive information. Moreover, the legal status of the data generated and the analytical outputs produced by digital twins within the framework of intellectual property remains unclear. This uncertainty

underscores the need for updated regulatory approaches across academic, commercial, and industrial applications. The rapid advancement of technology necessitates the adaptation of international regulatory frameworks and the strengthening of cooperative mechanisms. This study examines the legal and ethical issues arising from the use of digital twins in space research and highlights the importance of data governance, responsibility sharing, and multidisciplinary collaboration.

Keywords: Digital Twin, Artificial Intelligence, Space, Law, Ethics

KIYMETLİ EVRAKIN DİJİTALLEŞMESİ: HUKUKİ VE TEKNİK GEREKLİLİKLER, MEVCUT TEKNOLOJİLER VE ÖNERİLER

DIGITIZATION OF NEGOTIABLE INSTRUMENTS: LEGAL AND TECHNICAL REQUIREMENTS, CURRENT TECHNOLOGIES, AND RECOMMENDATIONS

Bildiri Özeti

Işık ÖZER[*]

Ayşe Nilay ŞENOL[**]

Tuğçe TOMRUKÇU[***]

Özet

Uluslararası Ticaret Odası (ICC), Covid-19 salgınının başında Nisan 2020'de ticari faaliyetleri kesintisiz sürdürmek amacıyla ülkeleri kağıtsız ticarete geçmeye ve gerekli hukuki düzenlemeleri yapmaya çağırmıştır. Bu çağrı, konişmento, poliçe, bono, çek ve makbuz senedi gibi kıymetli evrakın dijital ortama aktarılması için yasal düzenleme çalışmalarının başlamasına veya bazı ülkelerde hız kazanmasına yol açmıştır. ICC, kağıt ve elektronik kıymetli evrakın işlevsel ve hukuki eşdeğerliğinin önemini vurgulamış ve tüm ülkelere UNCITRAL'in 2017 tarihli Elektronik Devredilebilir Kayıtlara İlişkin Model Yasasını (Model Law on Electronic Transferable Records/MLETR) örnek almalarını tavsiye etmiştir.

Çalışmamızda da kıymetli evrakın elektronik ortamda güvenilir biçimde düzenlenmesi ve (zilyetlik, mülkiyet, rehin hakkı kurulması, devredilmesi vb.) hukuki işlemlere konu olması için gerekli teknik ve hukuki gereklilikler, uluslararası standartlar ve güncel teknolojik uygulamalar ışığında

Bu çalışma, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından 223K518 numaralı proje ile desteklenmiştir. Projeye verdiği destekten ötürü TÜBİTAK'a teşekkürlerimizi sunarız.

[*] Doçent Doktor, Özyeğin Üniversitesi Hukuk Fakültesi, Ticaret Hukuku Anabilim Dalı E-posta: isik.ozer@ozyegin.edu.tr ORCID: 0000-0001-6588-8934

[**] Doçent Doktor, Özyeğin Üniversitesi Hukuk Fakültesi, Medeni Hukuk Anabilim Dalı E-posta: nilay.senol@ozyegin.edu.tr ORCID: 0000-0001-7144-9698

[***] Özyeğin Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Bölümü Doktora Öğrencisi E-posta: tugce.tomrukcu@ozu.edu.tr ORCID: 0000-0002-9957-8771

incelenmektedir. Bu kapsamda kıymetli evrakın elektronik ortama taşınmasında tekilliğin (uniqueness) ve bütünlüğün (integrity) sağlanması gibi gereklilikler ile uluslararası uyum (harmonization) ve genel güvenilirlik standartları (reliability standards) üzerinde durulacak ve bu gerekliliklerin hangi teknolojiler ile sağlanabileceği açıklanacaktır.

Kıymetli evrakın elektronik ortama taşınması için gerekli olan teknik gereklilikler üç grup altında incelenmektedir: (i) Merkezi kayıt sisteminde, elektronik kıymetli evrakın orijinal nüshası güvenilir bir kurum tarafından dijital imzalar, zaman damgası, anahtar yönetimi ve kontrollü erişim yöntemleri ile korunur. (ii) Tokenizasyona dayalı kayıt sisteminde, kıymetli evrakın kendisi yerine benzersiz kriptografik bir token üretilir ve sahiplik anahtar kontrolü ile doğrulanır. Hash-temelli bütünlük kontrolleri, akıllı sözleşmeler, kriptografik doğrulanabilirlik ve dijital imza teknolojileri önemli rol oynar. (iii) Hibrit sistemde ise sahiplik kanıtı dağıtık defter üzerinde tutulurken belgenin içeriği merkezi ya da dağıtık olarak saklanır. Her üç sistem de elektronik kıymetli evrakta dijital imzalar, zaman damgası vb. ortak teknik bileşenler kullanmakla birlikte, güvenin kaynağı ve sahiplik doğrulama yöntemleri bakımından farklılaşmaktadır. Merkezi kayıt sisteminde güven, tek bir kurumun işlemleri doğrulayıp saklayan kapalı altyapısına; tokenizasyona dayalı kayıt sisteminde dağıtık deftere, kriptografiye ve hibrit sistemde ise merkezi otoriteye ve kriptografiye dayanır.

O halde, kıymetli evrakın elektronik ortama taşınması, bütünlük ve teklik ilkelerinin gözetildiği, güvenilir ve uluslararası standartlarla uyumlu bir teknolojik ekosistemi gerektirmektedir. Çalışmamız, belirttiğimiz bu ilkeleri incelemekte ve bu ilkelerin hayata geçirilmesi için yararlanılan mevcut teknolojilerin güçlü ve sınırlı yönlerini karşılaştırmalı olarak ortaya koymaktadır.

Anahtar Kelimeler: Kıymetli evrak, Dijitalleşme, Tokenizasyon, Dağıtık defter, Güvenilirlik standartları

Abstract

In April 2020, amid the Covid-19 pandemic, the International Chamber of Commerce (ICC) urged countries to transition to paperless trade and adopt legal frameworks to ensure continuity of commercial activities. This initiative accelerated legislative efforts in several countries to digitalize negotiable

instruments, including bills of lading, promissory notes, bills of exchange, cheques, and warehouse receipts. The ICC emphasized the functional and legal equivalence of paper and electronic instruments and recommended that countries consider the UNCITRAL Model Law on Electronic Transferable Records (MLETR) as a reference framework which is published in 2017.

In this paper, the technical and legal requirements for the secure electronic issuance of negotiable instruments, as well as for their involvement in legal transactions (such as the establishment of possession, ownership, pledge rights, and the transfer of the instrument) are examined. The analysis considers international standards and current technological practices, focusing on ensuring uniqueness and integrity, achieving international harmonization, and adhering to general reliability standards, alongside the technologies that support these requirements.

Technical solutions for electronic transfer are classified into three models: (i) In centralized registries, the original instrument is safeguarded by a trusted institution using digital signatures, timestamps, key management, and controlled access. (ii) In token-based registries, a unique cryptographic token represents the instrument, with ownership verified through key control. Hash-based integrity checks, smart contracts, cryptographic verifiability, and digital signatures serve a pivotal function in ensuring security and authenticity. (iii) Hybrid systems maintain ownership proof on a distributed ledger while storing document content centrally or in a distributed manner. Although all three systems employ common technical components such as digital signatures and time stamps, they diverge in terms of the source of reliability and the methods used for verifying ownership: centralized systems depend on a single trusted institution, token-based systems on the reliability of distributed ledger and cryptography, and hybrid systems on a combination of centralized authorities and cryptographic mechanisms.

Therefore, the digitalization of negotiable instruments requires a reliable technologic ecosystem that upholds integrity and uniqueness while complying with international standards. This paper examines these principles and comparatively evaluates the strengths and limitations of existing technologies that facilitate their implementation.

Keywords: Negotiable Instruments, Digitization, Tokenization, Distributed Ledger, Reliability standards

EVLİLİK BİRLİĞİNİN TEMELİNDEN SARSILMASI BOŞANMA SEBEBİ BAĞLAMINDA METAVERSE TEKNOLOJİSİNİN DEĞERLENDİRİLMESİ

THE EVALUATION OF METAVERSE TECHNOLOGY IN THE CONTEXT OF SHAKING THE FOUNDATION OF THE MARRIAGE UNION AS A GROUND FOR DIVORCE

Bildiri Özeti

Doğa Ekrem DOĞANCI[*]

Merve ÖZAYDIN[**]

Özet

Gündelik hayatta karşılaşılabilecek ve önceden belirlenmesi mümkün olmayan birçok olay genel boşanma sebebine konu olabilir. Şayet bu olaylar evlilik birliğini temelinden sarsarsa ve buna bağlı olarak ortak hayatın devam etmesi eşlerden beklenemezse boşanmanın genel sebebi oluşur.

Genel boşanma sebeplerinden biri olan dar ve teknik anlamda evlilik birliğinin temelinden sarsılması boşanma sebebinde kanun koyucu "evlilik birliğinin temeli" kavramında hüküm içi boşluk bırakmıştır. Hukuki bir ihtilafta hakimin takdir hakkı dahilinde dikkate alacağı bu kavram, somut olay dahilinde evlilik birliğinin ekonomik, duygusal, cinsel vb. temellerine ilişkin olabilir.

Evlilik birliğinin temelini sarsan olgular, eşlerin analog hayattaki faaliyetlerinden kaynaklanabileceği gibi dijital ortamdaki faaliyetlerinden de kaynaklanabilir. Bu dijital ortamlardan biri de teknolojinin en gelişmiş ve en son yeniliklerinden biri olan Metaverse'tür. İnteraktif katılımını sağlayan Metaverse, çeşitli özellikleriyle diğer platformlardan ayrılmaktadır. Kullanıcılar, hayatlarını, zihnen orada hissettikleri Metaverse'e adapte edebilmektedir. Bu adaptasyon kullanıcıların beş duyu organına hitap edilerek ve kullanıcılara günlük hayattaki deneyimlerini Metaverse'te de yapabilme

[*] Doç. Dr., İzmir Katip Çelebi Üniversitesi, Hukuk Fakültesi, Özel Hukuk Anabilim Dalı. E-posta: dogaekrem.doganci@ikc.edu.tr ORCID: 0000-0002-8771-0907

[**] Yüksek Lisans Öğrencisi, İzmir Katip Çelebi Üniversitesi, Hukuk Fakültesi, Medeni Hukuk Anabilim Dalı. E-posta: merveozaydin51@gmail.com ORCID: 0009-0007-8193-9106

imkanı sunup kendilerini Metaverse'ün içerisinde hissetmelerini sağlayarak gerçekleştirilmektedir.

Kullanıcıların hayatları bir nevi Metaverse'e aktarılabilecekse, boşanma sebebi teşkil edebilecek çeşitli durumlar da Metaverse'te gündeme gelebilir. Metaverse'te bir sosyal medya platformudur. Bu bağlamda öncelikle genel olarak sosyal medya kullanımından dolayı meydana gelen evlilik birliğini temelinden sarsan durumlarla karşılaşılabilir. Bunun yanında özellikle Metaverse platformunda bu teknolojinin kullanımına özgü sebepler yüzünden evlilik birliğini temelinden sarsan durumlarla karşılaşılabilir.

Giriş bölümünde evlilik birliğinin temelinden sarsılması ve Metaverse teknolojisi hakkında genel bilgiler paylaşılacaktır. Takiben Metaverse teknolojisine özgü özellik taşıyan evlilik birliğinin temelinden sarsılmasına sebebiyet verecek durumlar ilgili Yargıtay kararları incelenerek aktarılacaktır. Sonuç bölümünde ise konuya ilişkin hukuki değerlendirmelerimiz paylaşılacaktır.

Anahtar Kelimeler: Metaverse, Metaverse Teknolojisi, Genel Boşanma Sebepleri, Yargıtay Kararları, Evlilik Birliğinin Temeli

Abstract

Events that may occur in life and cannot be predicted in advance may constitute grounds for divorce. If these events fundamentally undermine the marriage and, as a result, the continuation of the shared life cannot be expected from the spouses, this constitutes grounds for divorce. Among the general grounds for divorce, the legislature has left a legal gap in the concept of "the foundation of the marriage union" in the narrow and technical sense of the fundamental undermining of the marriage union as a ground for divorce. This concept, which the judge will consider within the scope of his or her discretion in legal disputes, may relate to the economic, emotional, sexual, etc. foundations of the marriage union in the specific case.

Factors that undermine the foundation of marriage can stem from spouses' activities in analog life as well as their activities in digital environments. One such digital environment is the Metaverse, one of the most advanced and cutting-edge innovations in technology. The Metaverse, which enables interactive participation, stands out from other platforms with its various features. Users can adapt their lives to the Metaverse, where they feel mentally

present. This adaptation is achieved by appealing to the users' five senses and allowing them to experience their daily lives in the Metaverse, enabling them to feel immersed within it. If users' lives can be transferred to the Metaverse in a way, situations that could constitute grounds for divorce may also arise in the Metaverse. The Metaverse is also a social media platform. In this context, situations that fundamentally undermine the marital union may arise due to reasons specific to the use of social media in general and the Metaverse platform in particular.

The introduction section will provide general information about the undermining of the foundation of marriage and Metaverse technology. Subsequently, Supreme Court decisions related to situations that could undermine the foundation of marriage specific to Metaverse technology will be examined and presented. In the conclusion section, our legal assessments on the subject will be shared.

Keywords: Metaverse, Metaverse Technology, General Grounds for Divorce, Supreme Court Decisions, Basis of Marriage

METAVERSE ŞİRKETLERİNİN HUKUKİ NİTELİĞİ: DİJİTAL EVRENLERDE SANAL TİCARİ İŞLETMELER

THE LEGAL NATURE OF METAVERSE COMPANIES: A COMMERCIAL LAW PERSPECTIVE ON VIRTUAL COMMERCIAL ENTERPRISES UNDER THE TURKISH COMMERCIAL CODE

Bildiri Özeti

Gülnur Ceren UÇAR[*]

Özet

Metaverse teknolojilerinin hızla gelişmesi, dijital evrenlerde kurulan sanal ticari işletmeleri hukuk düzeni açısından tartışılması gereken yeni bir alan haline getirmiştir. Bu çalışma, metaverse ortamında faaliyet gösteren girişimlerin Türk Ticaret Kanunu ("TTK") çerçevesindeki hukuki niteliğini inceleyerek, dijital evrende sürdürülen ekonomik faaliyetlerin "ticari işletme" kavramı ile ne ölçüde örtüştüğünü değerlendirmektedir. Metaverse'de mağaza açan, dijital hizmet sunan veya NFT ve diğer dijital varlıkları ticarete konu eden yapıların, klasik ticari işletme unsurları olan "gelir sağlamaya elverişlilik", "devamlılık" ve "bağımsızlık" ölçütlerini karşılayıp karşılamadığı çalışma kapsamında ayrıntılı olarak analiz edilmiştir.

Bu çerçevede, TTK m. 11'de yer alan ticari işletme tanımının, fiziksel bir mekâna bağlı olmayan tamamen dijital faaliyetleri kapsayacak şekilde yorumlanması gerektiği ileri sürülmektedir. Dijital evrende kullanılan ticaret unvanları, avatarlar aracılığıyla yürütülen faaliyetlerde temsil ve sorumluluk ilişkisi, metaverse işletmelerinin ticaret siciline tescil edilebilirliği ve elektronik ortamda tutulan kayıtların ticari defter niteliği gibi hususlar, ticaret hukuku bakımından yeni ve çözümlenmesi gereken meseleler olarak öne çıkmaktadır.

Çalışmada ayrıca, blokzincir tabanlı otonom organizasyon modelleri (DAO'lar) ile TTK'da düzenlenen şirket türlerinin karşılaştırılması yapılmış; sanal mal ve hizmetlerin hukuki niteliği, sözleşmesel ilişkilerin kurulması ve dijital evrende tüketici işlemlerinden doğan sorumluluk konuları ele alınmıştır.

[*] Arş. Gör., Altınbaş Üniversitesi Ticaret Hukuku ABD. E-posta: ceren.ucar@altinbas.edu.tr ORCID: 0000-0001-8814-6546

Metaverse platformlarının merkeziyetsiz yapısı nedeniyle ortaya çıkan yetki, denetim ve sorumluluk sorunları da değerlendirilmiş; mevcut hukuk düzeninin dijital ticari işletmelere tam anlamıyla cevap veremediği tespit edilmiştir.

Sonuç olarak, çalışma, metaverse'de gelişen ticari yapıların Türk Ticaret Hukuku bakımından değerlendirilmesinin hem kavramsal hem de düzenleyici anlamda önemli boşluklar içerdiğini ortaya koymakta; dijital evrenlerdeki ekonomik faaliyetleri kapsayacak yeni hukuki çerçevelerin geliştirilmesi gerektiğini vurgulamaktadır.

Anahtar Kelimeler: metaverse, dijital ticari işletme, ticaret hukuku, blockchain, TTK

Abstract

The rapid development of metaverse technologies has transformed virtual commercial enterprises operating within digital environments into a new legal phenomenon requiring comprehensive analysis. This study examines the legal nature of business activities conducted in the metaverse under the framework of the Turkish Commercial Code (TCC), focusing on the extent to which digital-world economic activities align with the traditional concept of a "commercial enterprise." The analysis explores whether businesses that open virtual stores, provide digital services, or trade NFTs and other digital assets within the metaverse satisfy the classical elements of a commercial enterprise, namely "profit-oriented activity," "continuity," and "organized structure."

In this context, the study argues that the definition of a commercial enterprise under Article 11 of the TCC must be interpreted in a manner capable of encompassing purely digital operations that do not rely on any physical location. Issues such as the use of trade names in digital environments, representation and liability through avatars, the possibility of registering metaverse businesses with the trade registry, and the status of electronically maintained records as commercial books are discussed as emerging legal questions requiring new doctrinal evaluation.

The study further compares blockchain-based decentralized autonomous organizations (DAOs) with company structures regulated under the TCC, addressing the legal nature of virtual goods and services, the formation and

validity of contractual relationships in digital spaces, and the allocation of liability arising from consumer transactions conducted within the metaverse. Additionally, the decentralized structure of metaverse platforms raises significant jurisdictional, supervisory, and liability challenges, revealing considerable gaps within existing legal frameworks.

Ultimately, this study demonstrates that the emerging commercial structures of the metaverse reveal conceptual and regulatory deficiencies within Turkish Commercial Law. It emphasizes the need for new legislative and doctrinal approaches capable of addressing economic activities carried out in digital universes and ensuring legal certainty in this evolving domain.

Keywords: metaverse, digital commercial enterprise, commercial law, blockchain, TCC

METAVERSE'ÜN HUKUKA ETKİSİ VE GLOBAL METAVERSE PAZARI

THE IMPACT OF THE METAVERSE ON LAW AND THE GLOBAL METAVERSE MARKET

Bildiri Özeti

Gökçen YÜCEL[*]

Özet

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, interneti Web 1.0'dan Web 4.0'a taşıyarak, bireylere mevcut gerçekliğin ötesine geçme imkânı sunan ve kelime anlamı "öte-evren" olan Metaverse'ü ortaya çıkarmıştır. Metaverse, fiziki dünyada yapılan çalışma, ticaret ve sosyal aktiviteler dâhil olmak üzere hemen her şeyin simülasyon yoluyla taklit edilebildiği, zaman ve mekândan bağımsız bir sanal yaşam vaat etmektedir. Hukuk, doğası gereği teknolojik ilerlemeleri takip etmek ve sosyal yaşamdaki yıkıcı etkileri sınırlayarak muhtemel boşlukları doldurmak üzere değişime uğrar. Bu nedenle, Metaverse gibi yıkıcı bir teknolojinin günümüz hukuk sistemleri üzerinde yaratabileceği muhtemel değişimlerin incelenmesi kritik bir önem taşımaktadır.

Bu çalışmada, öncelikli olarak Metaverse'ün mevcut hukuk sistemlerini zorlayan çok katmanlı sorunları incelenmektedir. Bu sorunlar arasında, bir gerçek kişiye bağlı olmayan, yapay zekâ tarafından kontrol edilen elektronik kişi avatarlarının hukuki kişiliği ve bunların ceza hukuku bağlamındaki durumu öne çıkmaktadır. Zira bir suçun işlenmesi sırasında yapay zekânın suçun manevi unsuruna sahip olup olmadığı tartışmalıdır. Benzer şekilde, farklı ülke vatandaşları arasında sanal ofislerde kurulan iş ilişkilerinde hangi ülkenin iş hukukunun uygulanacağı veya kripto paralarla yapılan sanal ürün satışlarından doğan vergi kayıplarının nasıl önleneceği gibi sınır ötesi nitelikteki sorunlar uluslararası düzenlemeleri zorunlu kılmaktadır.

Bu bağlamda çalışmada, blok zincir tabanlı işlemlerden doğan uyuşmazlıkların çözümü için usul ekonomisi ilkesi gereği, önce sanal mahkeme algoritmaları

[*] Kamu Hukuku Ana Bilim Dalı Doktora Öğrencisi, Bursa Uludağ Üniversitesi. E-posta: yucelgokcen26@gmail.com ORCID: 0000-0002-3566-4953

ve ardından gerçek hukukçuların avatarlarından oluşan sanal temyiz mahkemeleri tarafından yürütülen bir yargılama modeli önerilmektedir. Ancak temel hak ve hürriyetlerle doğrudan ilişkisi nedeniyle ceza yargılamasında karar mekanizmasının bir algoritmaya teslim edilmemesi gerektiği de vurgulanmaktadır.

Hukuki zorlukların ötesinde, Metaverse'ün ekonomik ve jeopolitik boyutları da stratejik bir yaklaşım gerektirmektedir. 2030 yılına kadar 824,53 milyar dolara ulaşması beklenen global Metaverse pazarından büyük pay alması beklenen ülkeler karşısında (ABD, Çin, İngiltere) özellikle gelişmekte olan diğer ülkelerin alması gereken teknik ve hukuki tedbirler değerlendirilmektedir. Vergi kaybı ve ucuz iş gücü istihdamı kaynaklı olası işsizlik gibi olumsuz etkilere karşı en önemli çözümün, ülkelerin kendi ulusal Metaverse evrenlerini inşa etmeleri olduğu vurgulanmaktadır.

Anahtar Kelimeler: Metaverse, Hukuki Kişilik, Vergilendirme, Sanal Mahkeme, Global Pazar

Abstract

The rapid advancements in information and communication technologies have propelled the internet from Web 1.0 to Web 4.0, giving rise to the Metaverse, which literally means "beyond-universe" and offers individuals the opportunity to transcend existing reality. The Metaverse promises a virtual life independent of time and space, where almost everything done in the physical world, including work, commerce, and social activities, can be simulated. Law, by its nature, evolves to follow technological advancements and fill potential gaps by limiting their disruptive effects on social life. Therefore, examining the potential changes that a disruptive technology like the Metaverse might bring to current legal systems is of critical importance.

This study primarily examines the multilayered problems the Metaverse poses to existing legal systems. Among these issues, the legal personality of electronic person avatars controlled by artificial intelligence and not linked to a real person, and their status in the context of criminal law, stand out; as it is debatable whether artificial intelligence possesses the mens rea element of a crime during its commission. Similarly, cross-border issues such as which country's labor law should apply to employment relationships established in

virtual offices between citizens of different countries, or how to prevent tax losses arising from the sale of virtual products transacted with cryptocurrencies, necessitate international regulations.

In this context, the study proposes a judicial model for the resolution of disputes arising from blockchain-based transactions, which, for the sake of judicial economy, would be conducted first by virtual court algorithms and then by virtual courts of appeal composed of avatars of real legal professionals. However, it is also emphasized that due to its direct relation to fundamental rights and freedoms, the decision-making mechanism in criminal justice should not be entrusted to an algorithm.

Beyond the legal challenges, the economic and geopolitical dimensions of the Metaverse also require a strategic approach. Technical and legal measures that other developing countries, in particular, should take against countries expected to capture a large share of the global Metaverse market, projected to reach $824.53 billion by 2030 (USA, China, UK), are evaluated. It is emphasized that the most important solution against negative effects such as tax loss and potential unemployment caused by the employment of cheap labor is for countries to build their own national Metaverse universes.

Keywords: Metaverse, Legal Entity, Taxation, Virtual Court, Global Market

AVRUPA BİRLİĞİ DİJİTAL DÜZENLEMESİNDE KAMU-ÖZEL ORTAKLIĞININ ROLÜ VE HUKUKUN ÜSTÜNLÜĞÜ İLKESİ AÇISINDAN DEĞERLENDİRİLMESİ

THE ROLE OF PUBLIC-PRIVATE PARTNERSHIPS IN EUROPEAN UNION DIGITAL REGULATION AND THEIR ASSESSMENT IN LIGHT OF THE PRINCIPLE OF THE RULE OF LAW

Bildiri Özeti

Esra DEMİR[*]

Özet

Avrupa Birliği'nde (AB) dijital düzenlemeler son yıllarda önemli bir ivme kazanmış ve birçok yeni düzenleme hayata geçirilmiştir. 2016 yılında kişisel verilerin korunmasına ilişkin düzenlemeler ile hareketlenen bu süreç, dijital pazarlar, dijital hizmetler ve yapay zeka gibi çeşitli alanlarda bir dizi düzenleme ile devam etmiştir.

AB yasa koyucusu dijital düzenleme alanında inovasyon ve koruma hedeflerine ulaşmayı amaçlayan idealist bir duruş sergilemektedir. Buna göre, bir yandan temel hak ve özgürlükleri korumayı diğer yandan teknolojik inovasyona elverişli bir ortam hazırlamayı amaçlamaktadır. İnovasyon ve korumanın birlikte gerçekleştirilmesi hedefine ulaşmak için ise risk temelli bir yaklaşım benimsemekte ve kamu ve özel sektör aktörlerinin iş birliğini gerektiren çeşitli enstrümanlar öngörmektedir.

Bu çalışma, AB'nin dijital düzenleme alanındaki bu eğiliminin rolüne ve hukukun üstünlüğü ilkesi açısından yansımalarına odaklanmaktadır. Genel olarak, kamu ve özel sektör aktörlerinin düzenlemeye ortak katılımının, inovasyon ve korumanın birlikte gerçekleştirilmesi açısından umut verici olduğu söylenebilecektir. Dijital teknolojilerin düzenlemenin konusunu oluşturduğu hususlarda geleneksel olarak yasa yapımında kullanılan teknik ve enstrümanlar arzu edilen sonuçları veremeyebilecektir. Bu sebeple bu geleneksel yasa yapımının kamu ve özel sektör aktörlerinden elde edilecek

[*] Dr. Öğretim Üyesi, Ankara Üniversitesi Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku Anabilim Dalı. E-posta: esrademir@ankara.edu.tr ORCID: 0000-0002-4416-1290

ortak bilgi birikimiyle düzenlenmesi dijital teknolojilerin daha etkili bir şekilde düzenlenmesini sağlama potansiyeline sahiptir. Nitekim, ikili hedefin gerçekleştirilmesi amacıyla, AB yasa koyucusu, AB Genel Veri Koruma Mevzuatı, Dijital Hizmetler Mevzuatı ve Yapay Zeka Mevzuatında davranış kuralları, sertifikasyon ve teknik standartlar gibi bağlayıcı olmayan enstrümanlar benimsemiştir. Gerçekten de özel sektörün sahip olduğu bilgi avantajı, sektöre özgü uygulanabilecek davranış kurallarının belirlenmesinde, sertifikasyon için gerekli kriterlerin geliştirilmesinde ve teknik standartların oluşturulmasında önemli bir rol oynamaktadır. Ancak bu yaklaşımın mükemmel olmadığı da unutulmamalıdır.

De jure bağlayıcılığı bulunmayan bu enstrümanların de facto olarak bağlayıcı hale gelmesi, özel sektör aktörlerinin, özellikle büyük teknoloji şirketlerinin, demokratik yollarla seçilmiş temsilcilerin düzenleyici faaliyetlerine katılımı demokrasi konusunda endişelere yol açmakta ve demokrasi ile teknokrasi arasındaki çizgiyi bulanıklaştırmaktadır. Bu bağlamda çalışma, demokrasinin korunmasında hukukun üstünlüğü ilkesinin temel gerekliliklerine saygı gösterilmesi için yasa koyucunun daha net bir yaklaşım benimsemesi gerektiğinin altını çizmektedir. Özel sektör aktörlerinin kararlarının rasyonelliği, alınan kararların öngörülebilirliği ve anlaşılabilirliği ve diğer ilgili paydaşların karar alma mekanizmasında söz sahibi olması, hukukun üstünlüğü prensibinin temelini oluşturan gücün keyfi kullanımının azaltılması açısından önem arz etmektedir.

Anahtar Kelimeler: Dijital düzenleme, Kamu-özel ortaklığı, Hukukun üstünlüğü, Demokrasi, Teknokrasi

Abstract

Digital regulation in the European Union (EU) has grown considerably in recent years, with the implementation of numerous new regulations. This process, which began in 2016 with regulations on the protection of personal data, has continued with a series of regulations such as digital markets, digital services and artificial intelligence.

In digital regulation, the EU legislator has adopted an idealistic stance, aiming to achieve both innovation and protection. In doing so, it seeks to protect fundamental rights and freedoms while creating an environment conducive to

technological innovation. To achieve this objective, it adopts a risk-based approach and envisages several instruments requiring cooperation between public and private sector actors.

This study focuses on the role of this trend in EU digital regulation and its implications for the rule of law. In general, joint participation by public and private sector actors in regulation holds promise in terms of innovation and protection. In areas where digital technologies are regulated, the techniques and instruments traditionally used in law-making may not deliver the desired results. Therefore, using the collective knowledge acquired by public and private sector actors in regulation could enable more effective ways. Indeed, in achieving the dual objective, the EU legislator has adopted non-binding instruments, such as codes of conduct, certification, and technical standards in the EU General Data Protection Regulation, the Digital Services Act, and the Artificial Intelligence Act. The knowledge advantage of the private sector plays an important role in determining sector-specific codes of conduct, developing the criteria necessary for certification, and setting technical standards. However, it should be noted that this approach is not flawless.

The de facto binding nature of these instruments, which are not de jure, raises concerns about democracy and blurs the line between democracy and technocracy, as private sector actors, particularly big technology companies, participate in the regulatory activities of democratically elected representatives. The study emphasises that legislators must adopt a clearer approach. The rationality of decisions, their predictability and comprehensibility, and the participation of other relevant stakeholders in the decision-making are important for reducing the arbitrary use of power, which is fundamental to the principle of the rule of law.

Keywords: Digital regulation, Public-private partnership, The rule of law, Democracy, Technocracy

AVRUPA İNSAN HAKLARI MAHKEMESİNİN ÖZEL VE AİLE HAYATINA SAYGI HAKKI IŞIĞINDA VERİ GÜVENLİĞİNE İLİŞKİN DENETİMİ

EUROPEAN COURT OF HUMAN RIGHTS' REVIEW OF DATA SECURITY IN LIGHT OF THE RIGHT TO RESPECT FOR PRIVATE AND FAMILIY LIFE

Bildiri Özeti

Deniz KARADAŞ[*]

Veri güvenliği, dijitalleşmenin de yaygınlaşmasıyla günümüzde gittikçe artan bir öneme sahiptir. Artan bu önemi sebebiyle veri güvenliğinin korunması Avrupa İnsan Hakları Mahkemesi (AİHM) olmak üzere uluslararası ve Türk Anayasa Mahkemesi olmak üzere ulusal birçok mahkemede dava konusu olmaya başlamıştır. Günümüzde her ne kadar Avrupa İnsan Hakları Sözleşmesinde (AİHS) henüz başlı başına bir hak olarak kendisine yer bulamasa da özel hayatın gizliliğini koruma altına alan "özel ve aile hayatına saygı hakkı" çerçevesinde AİHM kararlarına konu olmuştur. Bu bağlamda AİHM, özel ve aile hayatına saygı hakkını düzenleyen madde 8 hükmüne bir aykırılığın bulunup bulunmadığını takdir ederken kullandığı ve birçok hakka yapılan müdahalenin hukuka uygunluğu değerlendirirken öğretide üçlü test olarak adlandırılan kriterleri veri güvenliği hususuna özgü bir biçimde şekillendirmiştir. Buna göre, madde 8 hükmü çerçevesinde veri güvenliğinin sağlanması için öncelikle veri güvenliğine yapılan müdahalenin hukuki bir zemine sahip olup olmadığı araştırılmaktadır. Veri güvenliğine yapılan müdahale hukuka uygun bir şekilde gerçekleşmişse, testin bir sonraki aşaması olan ilgili müdahalenin meşru bir amacı haiz olup olmadığı değerlendirilmesidir. Bu değerlendirme yapılırken madde 8'in ikinci fıkrasında yer alan kamu güvenliği, kamu sağlığının korunması, diğer bireylerin haklarının korunması gibi meşru amaçların varlığı aranmaktadır. Testin son aşamasında ise ilgili müdahalenin demokratik bir toplumda gerekliliği hususu değerlendirilmektedir. Madde 8 hükmünün bir gereği olarak AİHM; mümkün

[*] Araştırma Görevlisi, Atılım Üniversitesi Hukuk Fakültesi, Anayasa Hukuku Anabilim Dalı. E-posta: deniz.karadas@atilim.edu.tr ORCID: 0009-0000-0223-8037

olan en az verinin toplanıp toplanmadığını, toplanan verinin mümkün olan en kısa sürede silinip silinmediğini, verilerin yalnızca toplandıkları amaç için kullanılıp kullanılmadığını, toplanan verinin doğru ve güncel tutulup tutulmadığını ve veri toplama sürecinin şeffaf olup olmadığını değerlendirmektedir. İşbu çalışmada veri güvenliğine özgü bu testin kapsamı ve AİHM'nin bu testi nasıl ele aldığı açıklanacaktır.

Anahtar Kelimeler: AİHM, AİHS m.8, üçlü test, veri güvenliğinin korunması, dijitalleşme

Data security is gaining increasing importance today with the widespread adoption of digitalization. Due to this growing importance, the protection of data security has started to become the subject of litigation in many international courts, including the European Court of Human Rights (ECHR), and national courts, including the Turkish Constitutional Court. Although it has not yet found a place for itself as a standalone right in the European Convention on Human Rights (ECHR), it has been the subject of ECHR judgments within the framework of the "right to respect for private and family life," which protects the privacy of private life. In this context, the ECHR, while assessing whether there is a violation of Article 8 concerning the right to respect for private and family life, has adapted the criteria, known in doctrine as the three-step test when evaluating the lawfulness of interference with many rights, in a manner specific to the issue of data security. Accordingly, to ensure data security within the framework of Article 8, it is first investigated whether the interference with data security has a legal basis. If the interference with data security has taken place lawfully, the next stage of the test is the assessment of whether the interference has a legitimate aim. In this assessment, the existence of legitimate aims, such as public security, the protection of public health, and the protection of the rights of others, listed in the second paragraph of Article 8, is sought. In the final stage of the test, the necessity of the interference in a democratic society is evaluated. As a requirement of Article 8, the ECHR assesses whether the minimum possible data has been collected, whether the collected data has been deleted as soon as possible, whether the data is used only for the purpose for which it was collected, whether the collected data is kept accurate and up-to-date, and

whether the data collection process is transparent. This study will explain the scope of this data security-specific test and how the ECHR addresses this test.

Keywords: European Court of Human Rights (ECHR), ECHR Article 8, three-step test, protection of data security, digitalization

DEVLETİN SİBER UZAYDAKİ MİLLİ GÜCÜNÜ MEYDANA GETİREN UNSURLARINA YÖNELİK SİBER SALDIRIDA BULUNMA SUÇU: "SİBER GÜVENLİK KANUNU" KAPSAMINDA BİR İNCELEME

THE CRIME OF CYBER ATTACK AGAINST THE ELEMENTS OF THE STATE THAT CONSTITUTE ITS NATIONAL POWER IN CYBERSPACE: AN EXAMINATION WITHIN THE SCOPE OF THE CYBER SECURITY LAW

Bildiri Özeti

Veysel TOPUZ*

Özet

Günümüzde dijitalleşme süreçlerinin hızla ilerlemesi, siber güvenliği küresel ölçekte kritik bir öncelik hâline getirmiştir. Hem bireylerin hem de kurumların dijital varlıklarını koruma gereksinimi, gelişmiş ülkelerde stratejik nitelikte siber güvenlik politikalarının oluşturulmasını ve bu alandaki teknolojik yatırımların artırılmasını zorunlu kılmıştır. Özellikle kritik altyapıların güvenliği ile kamu kurumlarının dijital varlıklarının korunması, güncel siber güvenlik stratejilerinin temel bileşenleri arasında yer almaktadır. Bu çerçevede, "Milli Teknoloji Hamlesi" kapsamında ülkemizde yürütülen teknolojik dönüşüm sürecinin de en önemli gereksinimlerinden birisi etkin ve güçlü bir siber güvenlik altyapısının tesis edilmesidir.

Günümüzde geleneksel harp tekniklerinin etkisini yitirmesiyle birlikte, çatışmalar hibrit ve asimetrik nitelikli boyutlara dönüşmüştür. Karşı devletlerin yürüttüğü siber operasyonların yanı sıra; terör örgütleri, organize suç ağları ve bireysel motivasyonla hareket eden siber aktörler; kamu kurumlarını, enerji ve finans sistemlerini, sağlık hizmetlerini, iletişim altyapılarını ve çeşitli teknolojik platformları hedef alan çok yönlü saldırılar gerçekleştirebilir hâle gelmiştir. Bu saldırıları önleyebilmek amacıyla birçok Devlet bu alanda kapsamlı düzenlemeler yapmaktadır. Uluslararası Telekomünikasyon Birliği tarafından 2024 yılında yayımlanan Küresel Siber Güvenlik Endeksi sonuçları

* Dr. Arş. Gör., İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku ABD. E-posta: veyseltopuz_35@hotmail.com ORCID: 0000-0002-9831-2816

incelendiğinde, "Rol Model Ülke" kategorisinde yer alan 46 Devletin yaklaşık %91'inde siber güvenlik alanında kapsamlı ve çerçeve bir normun yürürlükte bulunduğu; kişisel verilerin korunması, siber suçlarla mücadele ve kritik altyapıların güvenliğine ilişkin açık ve sistematik bir hukuki yapı oluşturulduğu görülmektedir. Buna karşın, ülkemiz söz konusu kategori içerisinde değerlendirilmesine rağmen uzun süre bu alanı bütüncül biçimde düzenleyen bir siber güvenlik kanunundan yoksun kalmıştır. Bu eksiklik, "12/03/2025 tarih ve 7545 sayılı Siber Güvenlik Kanunu'nun" yürürlüğe girmesiyle birlikte giderilmiş; böylece bu alanda münhasır bir Kanuna kavuşulmuştur.

Bahsi geçen Kanunun 16. maddesinde önemli cezai hükümler söz konusudur. Özellikle söz konusu maddenin 6. fıkrasında "Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlarına yönelik olarak siber saldırıda bulunma veya bu saldırı neticesinde elde ettiği her türlü veriyi siber uzayda bulundurma eylemi" cezalandırılmıştır. Bu hükmün uygulama sınırlarının, metinde geçen kavramların ceza hukukunda belirlilik ilkesi bağlamında öncelikle ortaya konulması gerekmektedir. Devamında, söz konusu suçun TCK'da yer alan benzer suçlarla olan içtima ilişkisinin nasıl çözüme kavuşturulacağının tartışılması gerekmektedir. Üstelik halihazırda casusluk, bilişim sistemlerine girme, sistemi engelleme, bozma veya verileri değiştirme fiillerinin TCK'da zaten suç olarak düzenlendiği bir normatif havuzda ayrıca bir de bu suç tipine ihtiyaç olup olmadığının da tartışılması gerekmektedir. Çalışmada söz konusu suç tipi, tüm tartışmalı yönleriyle incelenecektir.

Anahtar Kelimeler: siber güvenlik kanunu, siber saldırı, casusluk, bilişim sistemine girme, içtima.

Abstract

The rapid advancement of digitalization processes today has made cybersecurity a critical priority on a global scale. The need to protect the digital assets of both individuals and institutions has necessitated the development of strategic cybersecurity policies in developed countries and the increase of technological investments in this area. The security of critical infrastructures and the protection of the digital processes and assets of public institutions, in particular, are among the fundamental components of current cybersecurity strategies. Within this framework, one of the most crucial requirements of the technological transformation process underway in our country as part of the

National Technology Initiative is the establishment of an effective and robust cybersecurity infrastructure.

Today, as traditional warfare techniques have become less effective, conflicts have evolved into hybrid and asymmetrical dimensions. In addition to cyber operations conducted by opposing states, terrorist organizations, organized crime networks, and individually motivated cyber actors have become capable of launching multifaceted attacks targeting public institutions, energy and financial systems, healthcare services, communications infrastructures, and various technological platforms. To prevent these attacks, many states are implementing comprehensive regulations in this area. An examination of the results of the Global Cybersecurity Index published by the International Telecommunication Union in 2024 reveals that approximately 91% of the 46 states in the "Role Model Country" category have a comprehensive framework norm in place in the field of cybersecurity, and a clear and systematic legal structure has been established regarding the protection of personal data, the fight against cybercrime, and the security of critical infrastructures. Despite this, despite being classified as such, our country has long lacked a cybersecurity law that holistically regulates this area. This deficiency was remedied with the entry into force of the "Cyber Security Law No. 7545 dated 12/03/2025", thus an exclusive Law was achieved in this field.

Article 16 of the aforementioned law contains significant penal provisions. Specifically, the sixth paragraph of this article penalizes "the act of conducting a cyber attack against the elements that constitute the national power of the Republic of Türkiye in cyberspace, or of keeping in cyberspace any data obtained as a result of such an attack". The application limits of this provision, and the concepts mentioned in the text, must be determined primarily within the context of the principle of certainty in criminal law. Subsequently, it is necessary to discuss how the aforementioned crime's affiliation with similar crimes stipulated in the Turkish Penal Code (TCK). Furthermore, in a normative framework already regulated as crimes under the TCK, espionage, accessing information systems, obstructing or disrupting systems, or altering data, the need for an additional crime type must be discussed. This study will examine this crime type in all its controversial aspects.

Keywords: cyber security law, cyber attack, espionage, entering information systems, gathering.

TÜRKİYE'NİN YENİ 7545 SAYILI YENİ SİBER GÜVENLİK KANUNU: YAPI, KAPSAM VE ETKİLERİ

TÜRKİYE'S NEW CYBERSECURITY LAW NO. 7545: STRUCTURE, SCOPE, AND IMPLICATIONS

Bildiri Özeti

Cemre Çise KADIOĞLU KUMTEPE*

Özet

Bu çalışma, daha önce farklı mevzuat içinde dağınık şekilde yer alan siber güvenlik hükümlerini tek bir çatı altında toplayan 7545 sayılı yeni Siber Güvenlik Kanunu'nu (SGK) incelemekte ve bu düzenlemenin genel çerçevesini ortaya koymaktadır. SGK, çeşitli temel kurumsal yapılar oluşturmakta; kamu kurumlarına, özel sektör aktörlerine ve dijital ortamda faaliyet gösteren diğer kişi ve kuruluşlara kapsamlı yükümlülükler getirmektedir. Kanun, siber güvenliği ağırlıklı olarak ulusal güvenlik ekseninde konumlandırsa da, bireysel hakların korunmasına yönelik işlevini de kabul etmekte; siber altyapının yerlileştirilmesini ve yerli teknolojilerin geliştirilmesini teşvik etmektedir. SGK'nın bazı hükümleri, AB'nin NIS2 Direktifi ve Siber Dayanıklılık Yasası gibi düzenlemelerden etkilenildiğini göstermektedir. Keza, ve ulusal siber güvenlik stratejisi kapsamında da bu çerçeveyle uyumun hedeflendiği açıkça ifade edilmektedir.

Çalışma, SGK'nın birden çok alanı düzenlemesine dikkat çekmektedir. Kanun aynı anda siber olaylara karşı hazırlık bulunuşluk kapasitesini artırmayı ve kritik altyapıyı korumayı hedeflerken getirdiği bazı hükümler neticesinde piyasa denetimi ve içerik moderasyonuna zemin hazırlamaktadır. SGK, ifade özgürlüğü ile kişi hürriyeti üzerinde etkileri olabilecek idari ve cezai yaptırımlar öngörmesine rağmen birçok yükümlülük ve yaptırım ölçütü yeterince açık tanımlamamaktadır. Bu belirsizlik, SGK'nın Kişisel Verilerin Korunması Kanunu'na (KVKK) açık bir atıfta bulunmaması nedeniyle daha da derinleşmektedir. KVKK hala uygulanabilir olmasına karşın, SGK'nın mevcut

* Dr. Öğr. Üyesi, Ankara Üniversitesi, Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku Anabilim Dalı. E-posta: cckadioglu@ankara.edu.tr ORCID: 0000-0002-9573-727X.

gizlilik ve veri koruma düzenlemeleriyle ilişkisi açıkça ortaya konmamaktadır. KVKK kapsamındaki kabahatler ile Türk Ceza Kanunu'ndaki kişisel veri suçları ve siber suç düzenlemeleriyle örtüşen yaptırımlar nedeniyle ciddi bir hukuki belirsizlik yaratmaktadır. Benzer çatışmalar, siber güvenlik ürün ve hizmetlerine getirilen yükümlülükler bakımından rekabet hukuku yönünden de gündeme gelebilecektir.

AB başta olmak üzere uluslararası düzeyde dijital yönetişim alanında benimsenen düzenleyici sadeleşme eğilimlerinin aksine, SGK ek uyum ve bildirim yükümlülükleri getirerek hukuki karmaşıklığı artırmakta ve uyum çabalarından uzaklaştırmaktadır. Çalışma, SGK'nın amaçlarını, kapsamını, kurumsal mimarisini ve yaptırım rejimini inceleyerek SGK'nın genel düzenleyici yaklaşımını ortaya koymakta; SGK'nın uygulamadaki etkisinin değerlendirilmesi açısından ikincil mevzuat ile yargı içtihadının belirleyici olacağını savunmaktadır.

Anahtar Kelimeler: Siber güvenlik, dijital yönetişim, ulusal güvenlik, veri koruma, uyumlaştırma

Abstract

This article analyzes Türkiye's new Cybersecurity Law (TCL) No. 7545, which consolidates previously scattered cybersecurity provisions into a single instrument. The TCL creates several core institutional bodies and introduces broad duties for public authorities, private-sector entities, and other actors operating in digital environments. Although the law frames cybersecurity primarily through a national-security lens, it also acknowledges its role in safeguarding individual rights, emphasizing the localization of cyber infrastructure and the development of domestic cybersecurity technologies. Certain provisions reflect influences from instruments such as the EU's NIS2 Directive and the Cyber Resilience Act, which the national cybersecurity strategy aims to harmonize with.

The study highlights the TCL's multifaceted regulatory functions: strengthening cyber preparedness and protecting critical infrastructure, while also acting as a mechanism of market oversight and, potentially, content moderation. The law establishes administrative and criminal sanctions that may affect freedom of expression and personal liberty, yet several obligations

and enforcement standards remain insufficiently defined. This ambiguity is exacerbated by the absence of explicit references to the Personal Data Protection Law (PDPL). Although the PDPL continues to apply, the TCL's failure to clarify its interaction with existing privacy and data-protection rules creates uncertainty—particularly where overlapping sanctions arise under the PDPL and under the Turkish Criminal Code provisions on personal-data offences and cybercrimes. Similar conflicts may arise with competition law rules in terms of obligations imposed on cybersecurity companies and products.

Departing from international—particularly EU—trends toward regulatory simplification in digital governance, the TCL introduces additional compliance and reporting obligations, thereby increasing regulatory complexity and distancing Turkish law from harmonization efforts. By examining the law's aims, scope, institutional architecture, and sanctions regime, the study outlines the TCL's underlying regulatory approach and argues that forthcoming secondary legislation and judicial interpretation will be crucial for assessing the practical impact of this new framework.

Keywords: Cybersecurity, digital governance, national security, data protection, harmonization

RUHSAT USULÜNDE YENİ BİR UYGULAMA: YOUTUBE YAYINCILARINA RTÜK LİSANSI

A NEW IMPLEMENTATION WITHIN THE AUTHORIZATION REGIME: RTÜK LICENSING FOR YOUTUBE BROADCASTERS

Bildiri Özeti

Melikşah ÇIRAKOĞLU[*]

Özet

Kamu hizmeti, idarenin varlık sebeplerinden biridir. Bu çerçevede idare, çeşitli kamu hizmetlerini bizzat yerine getirmektedir. Öte yandan vatandaşların ihtiyaçları zamanla değiştiğinden, kamu hizmeti kavramı ve bu kavram içerisinde değerlendirilebilecek faaliyetlerin kapsamı da değişime uğramıştır. Bu noktada, bazı kamu hizmetlerinin özel teknik bilgi ve uzmanlık gerektirmesi veya kendine özgü yatırım ya da altyapıya ihtiyaç duyması nedeniyle; idare tarafından bizzat yerine getirilmesi yerine idarenin denetimi ve gözetimi altında özel hukuk kişilerince yürütülmesi gündeme gelmektedir.

İdare çeşitli usullerle kamu hizmetini özel hukuk kişilerine gördürebilmektedir. İmtiyaz ya da yap-işlet-devret yöntemlerinde olduğu gibi, idare ile özel hukuk kişisi arasında gerçekleştirilen sözleşme kapsamında kamu hizmetinin özel hukuk kişisi tarafından yürütülmesi mümkün olduğu gibi; ruhsat, lisans ya da izin olarak adlandırılan ve idarenin tek taraflı işlemiyle özel hukuk kişisini yetkilendirdiği yöntemle de bir kamu hizmeti özel hukuk kişisi tarafından yerine getirilebilmektedir.

Ruhsat usulü genellikle, "virtüel kamu hizmeti" olarak isimlendirilen hizmetlerin yerine getirilebilmesi amacıyla başvurulan yöntemlerden biridir. Bu tür kamu hizmetleri ulaşım, haberleşme ya da eğitim gibi toplumun ortak, sürekli ve zorunlu ihtiyaçlarını karşılayan ancak organik anlamda idare tarafından yerine getirilmemesi nedeniyle de "fonksiyonel kamu hizmeti" olarak adlandırılan faaliyetlerdir. Virtüel kamu hizmetlerinde idare, sadece

[*] Doktor Öğretim Üyesi, Ankara Sosyal Bilimler Üniversitesi, Hukuk Fakültesi, İdare Hukuku Anabilim Dalı. E-posta: meliksah.cirakoglu@asbu.edu.tr/meliksahcirakoglu@gmail.com. ORCID: 0000-0002-6248-3330

kolluk yetkilerini kullanarak denetim yapmamakta; bu yetkilerin ötesinde, yürütülen faaliyetin içeriğini düzenleyebilmekte ve denetleyebilmektedir.

Elektronik haberleşme ve internet hizmetleri, 5369 sayılı Evrensel Hizmet Kanunu çerçevesinde evrensel hizmet kapsamına alınmış faaliyetlerdir. Bilgi Teknolojileri ve İletişim Kurumu (BTK), bu faaliyetlerin özel hukuk kişilerince yerine getirilebilmesi amacıyla ruhsat ya da lisans vermek konusunda yetkilendirilmiştir.

Lisans usulü ile internet hizmetlerinin kesiştiği bir diğer alan ise; Radyo Televizyon Üst Kurulu'nun (RTÜK) YouTube isimli sosyal medya platformunda yayın yapan içerik üreticilerine lisans verme uygulamasıdır. 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun çerçevesinde gerçekleştirilen bu uygulama; lisans usulünün oldukça yeni bir şeklini ifade etmektedir. Bu nedenle; Kanun kapsamında RTÜK'e tanınan bu yetkinin aslında 5369 s. Kanun kapsamında BTK'ya tanınması gereken bir yetki olup olmadığı; söz konusu yetki çerçevesinde adı geçen platformda yayın yapan içerik üreticilerinden hangilerinin lisans uygulaması kapsamında olduğu; bunların lisans almaması durumunda ne gibi yaptırımların hangi şekilde uygulanacağı gibi konular yeterince netleşmemiştir. Bu çalışma, bahsi geçen konuları ele almayı ve bunların netleştirilmesine katkı sağlamayı amaçlamaktadır.

Anahtar Kelimeler: Kamu Hizmeti, Ruhsat Usulü, Radyo Televizyon Üst Kurulu, YouTube, Yayın Lisansı

Abstract

Public services constitutes a core justification for the existence of administrative authority. Traditionally, the administration has directly undertaken various public services; however, as societal needs have evolved, both the definition of public service and the range of activities encompassed by it have transformed. In this context, certain public services—due to their need for specialized expertise, technical capacity, or substantial infrastructure—may be performed not directly by the administration but by private-law entities operating under its supervision and control.

The administration may entrust the performance of public services to private entities through different mechanisms. This may be achieved contractually, as in concession or build-operate-transfer models, or through unilateral administrative acts—commonly referred to as licenses, permits, or authorizations—by which a private party is empowered to carry out a public service.

The authorization procedure is frequently used for activities described as "virtual public services." These services meet common, continuous, and essential societal needs—such as transportation, communications, or education—yet are not executed organically by the administration, thereby qualifying as "functional public services." In such cases, the administration exercises not merely police powers but may also regulate and supervise the substantive content of the activity.

Electronic communications and internet services are classified as universal services under the Universal Service Law No. 5369. The Information and Communication Technologies Authority (BTK) is authorized to issue licenses or authorizations enabling private entities to provide these services.

A more recent intersection of licensing procedures and internet-based activities concerns the Radio and Television Supreme Council's (RTÜK) licensing of content creators broadcasting on YouTube. Implemented pursuant to Law No. 6112, this practice represents a novel form of the authorization regime. As a result, significant legal uncertainties persist: whether this authority should instead lie with BTK under Law No. 5369; which YouTube content creators fall within the licensing obligation; and what sanctions may apply to those who fail to obtain a license. This study seeks to examine these issues and contribute to their clarification.

Keywords: Public Service, Authorization Procedure, RTÜK, YouTube, Broadcasting License

TELEKOMÜNİKASYON HİZMETLERİNİN YETKİLENDİRİLMESİ VE DENETLENMESİNDE BAĞIMSIZ İDARİ OTORİTELERİN ÖNEMİ: BTK ÖRNEĞİ

THE SIGNIFICANCE OF INDEPENDENT ADMINISTRATIVE AUTHORITIES IN THE AUTHORIZATION AND SUPERVISION OF TELECOMMUNICATION SERVICES: THE CASE OF BTK (INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY)

Bildiri Özeti

Beyzanur BAŞAK*

Özet

Telekomünikasyon hizmetleri, hak bağlamında haberleşme hürriyetinin bir uzantısı olup yüksek mahkeme kararlarınca bir kamu hizmeti olarak kabul edilmektedir. Bu hizmetler kamu hizmetleri olmasının yanı sıra özelleştirmeye açık, rekabetçi bir sektörde kullanıma sunulmaktadır. Özelleştirme ve serbestleştirmenin bir sonucu olarak piyasa üzerinde yetkilendirme ve denetleme sorunları ortaya çıkmaktadır. Bu sorunları gidermek adına bağımsız idari otoriteler etkin bir şekilde görev almakta ve baskı altında kalmadan yetkilendirme, düzenleme ve denetleme yoluna başvurabilmektedirler. Bu nedenle bağımsız idari otoriteler, elektronik haberleşme piyasasında etkin rekabetin, hukuki güvenliğin ve kamusal denetimin aynı anda sürdürülebilmesi için büyük önem arz etmektedir.

Bağımsız idari otorite niteliği taşıyan kamu tüzel kişiliğini haiz, idarî ve mali özerkliğe sahip özel bütçeli Bilgi Teknolojileri ve İletişim Kurumu (BTK), özellikle telekomünikasyon gibi teknik uzmanlık ve rekabet denetimi gerektiren alanlarda, idarenin hiyerarşik yapısından ve siyasal karar alma süreçlerinden görece bağımsız şekilde kamu gücü kullanan düzenleyici bir kurumdur. BTK bu çerçevede, elektronik haberleşme piyasasında rekabetin sağlanması, piyasa aksaklıklarının giderilmesi, kullanıcı haklarının korunması

* Ankara Yıldırım Beyazıt Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Tezli Yüksek Lisans Öğrencisi. E-posta: avbeyzanurbasak@gmail.com ORCID: 0009-0004-7698-3469

ve teknik standartların uygulanması görevlerini yerine getiren, sektörel düzenlemeyi kamu adına icra eden bağımsız bir düzenleyici otorite niteliğindedir. BTK telekomünikasyon hizmetlerinde düzenleme, denetim, uzlaştırma yetkilerini yukarıda belirtilen nedenlerle sektör üzerinde kullanmaktadır.

Bu çalışmada elektronik haberleşme sektöründe bağımsız düzenleyici otorite olarak BTK'nın telekomünikasyon araçları üzerindeki yetkileri ve bu yetki kullanımının hukuki çerçevesi değerlendirilmektedir. Aynı zamanda sektörel bakımdan BTK'nın uygulamadaki işlevselliğini analiz edilmektedir. Bu kapsamda çalışma, özellikle uzay tabanlı haberleşme hizmetlerinin giderek artan önemine rağmen BTK'nın literatürde sınırlı biçimde ele alınmış olmasından kaynaklanan boşluğu doldurmayı hedeflemektedir.

Anahtar Kelimeler: Telekomünikasyon Hukuku, Haberleşme , Bağımsız İdari Otoriteler, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Rekabet.

Abstract

Telecommunication services are considered an extension of the freedom of communication in the context of rights, and they are recognized as a public service by high court decisions. In addition to being public services, these services are offered within a competitive sector open to privatization. Consequently, privatization and liberalization result in authorization and supervision issues within the market. To address these challenges, independent administrative authorities are actively engaged and are able to undertake authorization, regulation, and supervision without being subject to pressure. Therefore, independent administrative authorities are of paramount importance for simultaneously sustaining effective competition, legal certainty, and public scrutiny within the electronic communication market.

The Information and Communication Technologies Authority (BTK), which possesses the nature of an independent administrative authority, has public legal personality, administrative and financial autonomy, and a special budget. BTK is a regulatory institution that exercises public power relatively independently of the hierarchical structure of the administration and political decision-making processes, particularly in areas requiring technical expertise and competition oversight, such as telecommunications.

Within this framework, BTK functions as an independent regulatory authority that executes sectoral regulation on behalf of the public, fulfilling duties such as ensuring competition in the electronic communication market, remedying market failures, protecting user rights, and implementing technical standards.

This study evaluates the powers of BTK, as an independent regulatory authority in the electronic communication sector, over telecommunication instruments, and the legal framework for the use of these powers. The study aims to analyze their practical functionality from a sectoral perspective. In this scope, the study intends to fill a gap stemming from the limited coverage in the literature regarding BTK's position in the field of space-based communication services, especially given the growing significance of these services.

Keywords: Telecommunication Law, Communication, Independent Administrative Authorities, Information and Communication Technologies Authority (BTK), Competition.

CEZA HUKUKU AÇISINDAN UYDULARA YÖNELİK SİBER SALDIRILAR

CYBER ATTACKS TARGETING SATELLITES FROM A CRIMINAL LAW PERSPECTIVE

Bildiri Özeti

Berke Celil AKTAŞ*

Özet

Uydular haberleşme, gözlem ve diğer hizmetlerin sürdürülmesini sağlayan sistemlerdir. Önemleri gün geçtikçe artarken bunlara yönelik saldırıların taşıdıkları riskler de büyümektedir. Rusya ile Ukrayna arasındaki çatışmada bunun örnekleri görülmektedir. Bu süreçte, bir Ukrayna uydusuna zararlı yazılımlarla yapılan saldırı sonucunda binlerce sivil ve askeri kullanıcının internete erişimi kopmuş ayrıca Almanya'daki iki bin rüzgâr tribününün işleyişi aksamıştır. Başka bir olayda ise siber saldırıyla uydu sinyallerine müdahale edilerek Ukrayna televizyonlarında Moskova'daki askeri geçit törenleri yayımlanmıştır.

Türkiye'nin uzayda toplam dokuz uydusu bulunmaktadır. Bunlardan altısı haberleşme, diğer üçü ise gözlem uydusudur. Bu uydulara yönelik olarak yukarıdaki örneklerdeki gibi bir saldırının gerçekleşmesi halinde bunun ceza hukuku açısından sonuçları incelenecektir.

Uydular 5237 sayılı Türk Ceza Kanunu (TCK) kapsamında bilişim sistemi, 7545 sayılı Siber Güvenlik Kanunu kapsamında ise Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren unsurlarındandır. Türkiye'nin uydularına yönelik yukarıda örnekleri verilen bir saldırı ile hangi suçların oluşacağı, uyduların türü göz önünde tutularak tespit edilmelidir.

Uyduların bir siber saldırıyla işlevsiz bırakılması, TCK'nın 244. maddesinde tanımlı olan bilişim sistemini engelleme ve Siber Güvenlik Kanunu'nun 16/6 hükmünde tanımlanan Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü

* Avukat, İstanbul Barosu Bilişim Hukuku Komisyonu Sekreteri, Bahçeşehir Üniversitesi Bilişim Hukuku Yüksek Lisans (2023), Marmara Üniversitesi Kamu Hukuku Doktora Öğrencisi E-posta: celil@celilaktas.av.tr ORCID: 0009-0006-1466-5216

meydana getiren unsurlarına yönelik olarak siber saldırıda bulunma suçlarını oluşturacaktır. Siber saldırıya uğrayan uydunun bir haberleşme uydusu olması halinde ise TCK'nın 124. maddesinde düzenlenen haberleşmenin engellenmesi suçunun üçüncü fıkradaki nitelikli hali oluşur. Uydular kamu hizmetine tahsis edilmiş eşyalardan olduklarından bunlara yönelik bir siber saldırı sonucunda yayınların aksaması halinde mala zarar verme suçunun TCK'nın 152. maddesinin 3. fıkrasında tanımlı nitelikli hali de sübut bulacaktır. Haberleşmenin böylece engellenmesinden tutuklular ve hükümlüler de etkileneceğinden TCK'nın 298. maddesinin ilk fıkrasında tanımlı suç da oluşacaktır.

Görüldüğü üzere, uydulara yönelik bir siber saldırı sonucunda birden fazla suç sübuta erecektir ve bunların olaya ayrı ayrı tatbiki mümkündür. Bu nedenle görünüşte içtimadan söz edilemeyecek ve fikri içtima hükümleri uygulanacaktır. Nitekim, Siber Güvenlik Kanunu'nun 16/6 hükmünde tanımlı suç ile TCK'daki suçlar arasında özel norm – genel norm ilişkisi bulunmamaktadır zira bu suçların unsurları ve korudukları hukuki değerler farklıdır. Çalışmada uydulara karşı bir siber saldırıda fikri içtima kurallarının nasıl uygulanacağı ve konuyla ilgili Yargıtay kararları incelenecektir.

Anahtar Kelimeler: Uydular, Siber Uzay, Siber Saldırı, Bilişim Sistemi, Fikri İçtima.

Abstract

Satellites are systems enabling communication, observation, and other services. As their importance grows daily, so do the risks posed by attacks against them. Examples of this can be seen in the conflict between Russia and Ukraine. In this process, a cyberattack by malware against a Ukrainian satellite disconnected thousands of civilian and military users from the internet and disrupted the operation of 2,000 wind turbines in Germany. In another incident, a cyberattack on satellite signals disrupted Ukrainian TV stations, causing them to broadcast military parades in Moscow.

In total, Türkiye has nine satellites in space. Six of these are communication satellites, and the other three are observation satellites. The consequences of the aforementioned attack on these satellites will be analysed from the perspective of criminal law.

Satellites are accepted as information systems under the Turkish Penal Code No. 5237 and as components that constitute the national power of the Republic of Türkiye in cyberspace under Cybersecurity Law No. 7545. The type of satellite shall be taken into account while deciding which crimes will apply due to the aforementioned attack on Türkiye's satellites.

Rendering a satellite inoperable through a cyberattack constitutes the crimes of preventing the functioning of a system as defined in Article 244 of the Turkish Penal Code and committing a cyberattack against the components of the national power of the Republic of Türkiye in cyberspace as defined in Article 16/6 of the Cybersecurity Law. If the targeted satellite is a communications satellite, then the qualified form of prevention of communications, as defined in the third paragraph of Article 124 of the Turkish Penal Code will apply. Since satellites are items for public service, if broadcasts are disrupted due to a cyberattack, the qualified form of the crime of damaging property, as defined in the third paragraph of Article 152 of the Turkish Penal Code will apply. Since detainees and convicts will also be affected by the prevention of communications in this manner, the crime defined in the first paragraph of Article 298 of the Turkish Penal Code will also apply.

As it is seen, in the case of a cyberattack targeting satellites, multiple crimes will be committed, and all of them can be applied. Therefore, there will be no unreal joinder of offences and provisions of conceptual aggregation will apply. Indeed, there is no special norm-general norm relationship between the crime defined in Article 16/6 of the Cybersecurity Law and the crimes in the Turkish Penal Code since the elements of these crimes and the legal goods they protect are different. In the paper, the application of the rules of conceptual aggregation in a cyberattack against satellites and the relevant decisions of the Court of Cassation will be examined.

Keywords: Satellites, Cyberspace, Cyber Attack, Information System, Conceptual Aggregation.

E-TİCARET SİTELERİNDE SAHTE YORUMLARA İLİŞKİN CEZA HUKUKU BAĞLAMINDA BİR DEĞERLENDİRME

A CRIMINAL LAW PERSPECTIVE ON FAKE REVIEWS IN E-COMMERCE: AN ASSESSMENT WITHIN THE SCOPE OF CRIMINAL LAW

Bildiri Özeti

Bedriye Bilkay ÖZBEK*

Özet

Dijitalleşmenin etkisiyle birlikte geleneksel ticaret anlayışında köklü değişiklikler meydana gelmiş ve tüketici davranışları bu değişimden önemli ölçüde etkilenmiştir. Ticaretin elektronik platformlara taşınmasıyla birlikte, mal ve hizmetlere erişim daha geniş bir yelpazede ve daha hızlı bir biçimde mümkün hale gelmiştir. Özellikle tüketicilerin "kullanıcı yorumları" ve "müşteri değerlendirmeleri" gibi ölçütlere anında ulaşabilmesi, sağlıklı ve şeffaf bir e-ticaret ortamı hedefinin temel taşlarından biri olmuştur.

Ancak son yıllarda e-ticaret piyasalarında yer alan "sahte kullanıcı yorumları", gerçekte var olmayan müşteri deneyimlerinin sunulması suretiyle, piyasa şeffaflığını ve güvenilirliğini ciddi biçimde zedelemektedir. Bu bağlamda, sahte kullanıcı yorumları aracılığıyla kötü niyetli satıcıların haksız ticari avantaj ve maddi kazanç elde ettiği gözlemlenmektedir. Bununla birlikte, bu sahte içerikler aynı zamanda Türk Ceza Kanunu'nda (TCK) tanımlanan bazı suç tiplerine de vücut vermektedir.

Sahte kullanıcı yorumları, ilk bakışta bilişim sistemleri üzerinden gerçekleştirilmeleri nedeniyle TCK'nın 243 ve 244. maddelerinde düzenlenen "bilişim sistemine girme" veya "verileri bozma, yok etme, değiştirme" suç tipleriyle ilişkilendirilebilir gibi görünse de, bu yorumlar genellikle sistemin işleyişine yönelik izinsiz bir müdahale içermemekte ve kullanıcı arayüzü üzerinden, sistemin izin verdiği şekilde yapılmaktadır. Dolayısıyla, TCK m.244 anlamında "veri bozma veya değiştirme" fiilinden söz etmek mümkün

* Araştırma Görevlisi, Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi, İdare Hukuku Anabilim Dalı. E-posta:bedriye.ozbek@asbu.edu.tr ORCID: 0000-0002-8725-1798

değildir. Buna karşılık, sahte yorumların amacı tüketiciyi aldatmak ve ekonomik menfaat sağlamaktır. Buna karşılık, sahte yorumların temel amacının tüketiciyi aldatmak ve ekonomik menfaat sağlamak olduğu dikkate alındığında, fiilin TCK m.158/1-f'de düzenlenen "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle nitelikli dolandırıcılık" suçunun unsurlarını taşıyabileceği değerlendirme konusu olabilmektedir. Zira fail, e-ticaret platformu gibi bir bilişim sistemini araç olarak kullanarak aldatıcı bir içerik üretmekte ve bu suretle haksız kazanç elde etmektedir. Bu nedenle, sahte kullanıcı yorumlarının cezai nitelendirilmesinde TCK m.158/1-f hükmü esas alınmalı; bilişim sistemine yönelik teknik müdahale içermeyen fiiller bakımından TCK m.244 kapsamında değerlendirme yapılmamalıdır.

Öte yandan, platform sağlayıcılar ve içerik üreticileri açısından da sorumluluk doğuran hükümler mevcuttur. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesine ilişkin 5651 sayılı Kanun kapsamında hem içerik sağlayıcıların hem de yer sağlayıcıların yükümlülükleri gündeme gelmektedir. Çalışmamız kapsamında, sahte kullanıcı yorumlarının Türk Ceza Kanunu hükümleri çerçevesinde suç teşkil edip etmediği detaylı şekilde incelenecek; ayrıca 5651 sayılı Kanun kapsamında erişimin engellenmesi ve içeriklerin yayından kaldırılması gibi önleyici tedbirler ekseninde hukuki değerlendirmesi yapılacaktır.

Anahtar Kelimeler: E-Ticaret, Ceza Yaptırımı, Bilişim Suçları, Çevrim İçi Platformlar, Sahte Yorumlar.

Abstract

With the impact of digitalization, traditional trade practices have undergone profound changes, and consumer behavior has been significantly affected by this transformation. As trade has moved to electronic platforms, access to goods and services has become possible across a wider range and in a much faster manner. In particular, consumers' ability to instantly access metrics such as "user reviews" and "customer evaluations" has become one of the fundamental pillars of a healthy and transparent e-commerce environment.

However, in recent years, "fake user reviews" appearing in e-commerce markets have seriously undermined market transparency and reliability by

presenting customer experiences that do not actually exist. In this context, it has been observed that malicious sellers gain unfair commercial advantages and financial profit through fake user reviews. Moreover, these fake contents also correspond to certain criminal offenses defined under the Turkish Penal Code (TPC).

At first glance, fake user reviews might seem related to the offenses of "unauthorized access to a computer system" or "altering, destroying, or corrupting data" as regulated under Articles 243 and 244 of the TPC, since they are conducted through information systems. However, these reviews generally do not involve unauthorized interference with the system's operation and are submitted through the user interface in a manner permitted by the system. Therefore, it is not possible to speak of "data alteration or corruption" within the meaning of Article 244. On the other hand, considering that the main purpose of fake reviews is to deceive consumers and obtain economic benefit, it may be evaluated that the act could carry the elements of the offense of "qualified fraud committed by using information systems, banks, or credit institutions as a means," regulated under Article 158/1-f of the TPC. The perpetrator uses an information system, such as an e-commerce platform, as a tool to produce deceptive content and thereby gains unjust profit. Consequently, the criminal characterization of fake user reviews should be based on Article 158/1-f of the TPC; acts that do not involve technical interference with the information system should not be evaluated under Article 244.

Furthermore, there are provisions that impose liability on platform providers and content producers. Under Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications, the obligations of both content providers and hosting providers come into play. Within the scope of our study, whether fake user reviews constitute a criminal offense under the provisions of the Turkish Penal Code will be examined in detail; additionally, preventive measures such as blocking access and removing content under Law No. 5651 will also be evaluated from a legal perspective.

Keywords: E-Commerce, Criminal Sanction, Cybercrimes, Online Platforms, Fake Reviews.

GÖRÜNMEYEN SINIRLAR: DİJİTAL EGEMENLİĞİN ULUSLARARASI HUKUKTAKİ YANSIMALARI

INVISIBLE BORDERS: REFLECTIONS OF DIGITAL SOVEREIGNTY IN INTERNATIONAL LAW

Bildiri Özeti

Pelin ÖZKAYA ÖKMEN*

Özet

Dijital çağ, devletlerin egemenlik anlayışını köklü biçimde dönüştürmüştür. Devletler artık yalnızca fiziksel toprakları üzerinde değil, veri, ağ altyapısı ve dijital platformlar üzerinde de yetki kullanma ihtiyacıyla karşı karşıyadır. Siber uzayın sınır aşan doğası, devletlerin egemenlik yetkilerinin sınırlarını karmaşıklaştırmakta, bu durum uluslararası hukukun uygulanabilirliği konusunda yeni bir tartışma alanı yaratmaktadır.

Dijital egemenlik, "devletlerin dijital altyapı, veri ve bilgi üzerindeki karar ve düzenleme yetkisi" olarak tanımlanmaktadır. Bildiri, dijital egemenlik kavramını uluslararası hukuk perspektifinden ele alarak, siber uzayda devlet yetkilerinin normatif sınırlarını belirlemeyi amaçlamakta ve bu çerçevede üç temel soruya yanıt aramaktadır:

1. Mevcut egemenlik ilkeleri siber uzaya ne ölçüde uygulanabilir?

2. Devletler siber güvenlik gerekçesiyle hangi sınırlar içinde hareket edebilir?

3. Bu alanda uluslararası hukuk hangi ölçüde bağlayıcı ve uygulanabilir bir etki yaratmaktadır?

Bu kapsamda bildiride, siber operasyonların egemenlik ihlali ve müdahale yasağı bağlamında nasıl değerlendirildiğine ilişkin "Tallinn Manual 2.0" ve "BM Açık Uçlu Çalışma Grubu (OEWG)" raporları temel belgeler olarak ele alınmakta, bu belgelerden yola çıkarak Avrupa Birliği'nin 'dijital egemenlik'

* Avukat, Arabulucu, Ankara Barosu, Hacettepe Üniversitesi Doktora Öğrencisi. E-posta: avpelinozkaya@gmail.com ORCID: 0000-0002-5429-2729

yaklaşımı, Çin'in 'bilgi egemenliği' modeli ve Türkiye'nin ulusal siber stratejisi karşılaştırmalı olarak incelenmektedir.

Bulgular, siber uzayın uluslararası hukuk kapsamında kabul edildiğini, ancak normatif düzeyde hâlen "soft law" düzeyinde işlediğini ve devletlerin siber uzaydaki davranışlarını şekillendiren ortak ilkelerin henüz tam anlamıyla kurumsallaşmadığını göstermektedir.

Sonuç olarak dijital egemenlik, teknik bir siber güvenlik meselesinden öte, uluslararası hukukun dijital ortamda uygulanabilirliğini ve dijital haklarla güvenlik arasındaki dengeyi sınayan bir alandır. Bildiri, bu alanda geliştirilecek normatif çerçevenin, hem devletlerin güvenlik kaygılarını hem de bireylerin dijital haklarını koruyacak biçimde, uluslararası işbirliği mekanizmalarıyla dengelenmesi ve güçlendirilmesi gerektiğini savunmaktadır.

Anahtar Kelimeler: Dijital Egemenlik, Siber Uzay, Uluslararası Hukuk, Siber Güvenlik, Uygulanabilirlik

Abstract

The digital age has profoundly transformed the notion of state sovereignty. States today face the need to exercise authority not only over their physical territories but also over data, network infrastructures, and digital platforms. The cross-border nature of cyberspace complicates the boundaries of state sovereignty, creating new debates on the applicability of international law in this domain.

Digital sovereignty is defined as "the authority of states to make decisions and regulations concerning digital infrastructure, data, and information." This paper examines the concept of digital sovereignty from the perspective of international law, aiming to identify the normative boundaries of state authority in cyberspace and addressing three central questions:

1. To what extent can existing principles of sovereignty be applied to cyberspace?

2. Within what limits can states act on the grounds of cybersecurity?

3. To what degree does international law produce binding and applicable effects in this field?

In this context, the paper takes the Tallinn Manual 2.0 and the UN Open-Ended Working Group (OEWG) reports as primary reference documents to assess how cyber operations are interpreted in relation to violations of sovereignty and the prohibition of intervention. Building on these frameworks, the study compares the European Union's approach to "digital sovereignty," China's model of "information sovereignty," and Turkey's national cyber strategy.

The findings show that cyberspace is accepted within the scope of international law, but it still operates at the normative level as 'soft law' and the common principles shaping the behavior of states in cyberspace have not yet been fully institutionalized.

Ultimately, digital sovereignty is not merely a technical cybersecurity issue but a field that tests the applicability of international law in the digital environment and the balance between digital rights and security. The paper argues that the normative framework to be developed in this area should balance and reinforce both state security concerns and the protection of individual digital rights through mechanisms of international cooperation.

Keywords: Digital Sovereignty, CyberSpace, International Law, CyberSecurity, Applicability.

İLETİŞİM AHLAKI YASASI BÖLÜM 230 KAPSAMINDA DERİN KURGU TEKNOLOJİSİYLE ÜRETİLEN ZARARLI İÇERİKLERİN SOSYAL MEDYA PLATFORMLARINDA YAYILMASININ ÖNLENMESİ

THE PREVENTION OF THE DISSEMINATION OF HARMFUL CONTENT PRODUCED THROUGH DEEPFAKE TECHNOLOGY ON SOCIAL MEDIA PLATFORMS UNDER SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

Bildiri Özeti

Fatih Tolga SÜMERLİ[*]

Özet

Bilişim teknolojilerinde yaşanan gelişmelerin gündelik hayata sunduğu araçlar çeşitlilik arz ederken bunlardan biri de günümüzde derin kurgu teknolojisi olmuştur. Kısaca gerçekliğin değiştirilmesi olarak ifade edilebilecek olan derin kurgu teknolojisi, sanat gibi yaratıcılığın önemli olduğu alanlarda çığır açan faydalı bir gelişme olarak görülmektedir. Buna mukabil bu teknolojinin kötü niyetli kullanımları sonucunda bireysel veya toplumsal ölçekte, kişilik haklarına saldırı ve dezenformasyon gibi ciddi tahribatlara yol açabilecek zararlı örnekleriyle de yaygın bir şekilde karşılaşılmıştır. Derin kurgu teknolojisinin kötü niyetli olarak kullanılması sonucunda yüksek derecede sorun teşkil edebilecek içeriklerin, bir de küresel bir sanal evren olan sosyal medyanın sahip olduğu kelebek etkisi gücüyle birlikte yayılma hızı konunun tartışılmasının önemini arttırmaktadır. Zararlı derin kurgu içeriklerin, sosyal medyada yayılmasının önlenmesi konusunun çalışmada ele alınmasının temel amacı, bu teknolojinin yaratabileceği yeni olumsuz sonuçların önlenmesi için doktrinde sunulan teknik çözüm önerilerinin hukuki düzenlemelerle birlikte yeniden değerlendirilmesidir. Çalışma özelinde incelenecek olan Amerika Birleşik Devletleri'nde 1996 yılında yürürlüğe giren İletişim Ahlakı Yasası (Communications Decency Act -CDA-) Bölüm 230, iki açıdan incelemeye

[*] Tezli Yüksek Lisans Öğrencisi, Ankara Sosyal Bilimler Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Anabilim Dalı. E-posta: tolgasumerli06@gmail.com ORCID: 0009-0004-3096-2021

değerdir: Birincisi, Bölüm 230'un b fıkrasının dördüncü bendinde ve c fıkrasının ikinci bendinde, zararlı çevrimiçi içeriğin engellenmesine yönelik filtreleme araçlarının hizmet sağlayıcılar tarafından geliştirilmesinden ve bu faaliyetlerinden dolayı sorumlu tutulmayacaklarından bahsedilmektedir. Söz konusu hükümlerin, zararlı derin kurgu içeriklerin sosyal medya platformlarında yayılmasının engellenebileceğine işaret eden tespit yazılımlarının platformlara entegre bir şekilde kullanılması biçiminde yorumlanması mümkündür. Öte yandan Bölüm 230'la ilgili olarak ikinci önemli husus, küresel sosyal medya içeriklerinin çoğu Facebook, X ve Youtube gibi ABD şirketleri tarafından barındırılmaktadır. Dolayısıyla İletişim Ahlâkı Yasası, her ne kadar bir ABD yasası olsa da hizmet sağlayıcıların Bölüm 230'a cevap olarak uygulamaya almak zorunda oldukları teknik yazılımlar ile küresel çapta bir temel oluşturarak olumlu etkiler sağlayacaktır.

Anahtar Kelimeler: Derin kurgu teknolojisi, yapay zeka, sosyal medya, iletişim ahlakı yasası, bölüm 230

Abstract

While the tools offered by developments in information technology to everyday life are diverse, one of them today is deepfake technology. Deepfake technology, which can be briefly described as the alteration of reality, is seen as a groundbreaking and beneficial development in fields where creativity is important, such as art. However, harmful examples of this technology's malicious use have also become widespread, potentially causing serious damage on an individual or societal scale, such as attacks on personal rights and disinformation. The use of deepfake technology for malicious purposes, combined with the butterfly effect power of social media as a global virtual universe, increases the speed at which highly problematic content can spread, increases the importance of discussing this issue. The main purpose of addressing the prevention of harmful deepfake content spreading on social media in this study is to re-evaluate the technical solutions proposed in the doctrine, along with legal regulations, in order to prevent the new negative consequences that this technology may create. Section 230 of the Communications Decency Act (CDA), which came into effect in the United States in 1996 and will be examined in this study, is noteworthy in two respects: First, Sections 230(b)(4) and (c)(2) state that service providers cannot

be held liable for developing filtering tools to block harmful online content or for their activities in this regard. These provisions can be interpreted as allowing platforms to integrate detection software to prevent the spread of harmful deepfake content on social media platforms. On the other hand, the second important point regarding Section 230 is that most global social media content is hosted by US companies such as Facebook, X, and YouTube. Therefore, although the Communications Decency Act is a US law, it will have positive effects by establishing a global foundation through the technical software that service providers are required to implement in response to Section 230.

Keywords: Deepfake technology, artificial intelligence, social media, communications decency act, section 230

ELEKTRİKLİ ARAÇLARDA İNTERNET KULLANIMI VE E-SIM TEKNOLOJİSİ

INTERNET USE AND E-SIM TECHNOLOGY IN ELECTRIC VEHICLES

Bildiri Özeti

Buşra Demir Yıldırım*

Özet

Elektrikli araçlar, 1800'lü yıllardan günümüze kadar önemli bir gelişim göstermiş ve çevreci beklentilerin artmasıyla yeniden ilgi görmeye başlamıştır. Batarya teknolojilerinin ilerlemesi ve şarj altyapısının yaygınlaşması, bu araçların günlük hayata daha iyi uyum sağlamasına imkan tanımıştır. Modern elektrikli araçlar artık sadece bir ulaşım aracı olmaktan çıkmış, internet bağlantısı sayesinde veri ileten ve uzaktan yönetilebilen akıllı sistemlere dönüşmüştür. Gerçek zamanlı trafik bilgisi, şarj durumu takibi, uzaktan kontrol gibi özellikler bu bağlantının temel işlevleri arasındadır. e-SIM teknolojisi ise fiziksel SIM kart ihtiyacını ortadan kaldırarak daha güvenli ve esnek bir iletişim imkanı sunmaktadır. Bu sayede yazılım güncellemeleri daha hızlı yapılmakta ve araç ile bulut sistemi arasındaki veri akışı kesintisiz hale gelmektedir.

Elektrikli araçlarda internet kullanımıyla birlikte e-SIM teknolojisinin yaygınlaşması, bu araçlara ilişkin teknik ve idari düzenlemelerin önemini artırmıştır. Mevzuatta elektrikli araçlarda internet ve e-SIM kullanımına ilişkin doğrudan bir yasaklama bulunmamakla birlikte, veri güvenliği, gizlilik ve ulusal güvenlik kaygıları çerçevesinde belirli sınırlamaların getirilebilmesi mümkündür. Bilgi Teknolojileri Kurumu, Türkiye'de veri güvenliği, kullanıcı bilgileri ve haberleşme sistemlerinin kontrolü gibi alanlarda belirli kurallar öngörmekte ve özellikle e-SIM'lerin yerli olarak yönetilmesini şart koşulmaktadır. Bu yaklaşım, bağlantı altyapısının güvenli şekilde işletilmesini

* Hâkim Yardımcısı, Ankara Sosyal Bilimler Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı. E-posta: busra.demiryildirim@student.asbu.edu.tr ORCID: 0009-0000-0589-7812

ve yazılım güncellemeleri, acil durum bildirimleri ve iletişim sistemlerinin sorunsuz çalışmasını amaçlamaktadır. BTK'nin e-SIM modüllerinin yalnızca yerli mobil işletmeciler tarafından programlanabilmesi, verinin ülke sınırları içinde tutulması ve araçlarda kullanılan e-Call sistemlerinde yerli SIM kartı ile yerleşik sunucu kullanımının zorunlu olması kararları önemli hukuki sonuçlar doğurmaktadır. Bu kararlar başta milli güvenlik, kamu düzeni, rekabet ve tüketici haklarının korunması bakımından etkili bir hukuki çerçeve sunmaktadır.

Sonuç olarak, elektrikli araçlarda internet ve e-SIM kullanımına ilişkin düzenlemeler ve uygulamalar birlikte değerlendirildiğinde, bu teknolojilerin hem araç güvenliği hem de kullanıcı deneyimi açısından önemli bir ihtiyaç haline geldiği görülmektedir. Bu kapsamda e-SIM'in yerli olarak yönetilmesi, verilerin ülke içinde tutulması ve haberleşme altyapısının güvenli şekilde işletilmesine yönelik yükümlülükler, söz konusu ihtiyacın hukuki dayanağını oluşturmaktadır. Veri güvenliğinin sağlanması, kullanıcı haklarının korunması ve siber güvenlik tedbirlerinin güçlendirilmesi, elektrikli araçların güvenli biçimde kullanılabilmesi için zorunludur.

Anahtar Kelimeler: Elektrikli araçlar, e-SIM teknolojisi, bağlantılı araçlar, veri güvenliği, bağlantı sistemleri.

Abstract

Electric vehicles have undergone significant development from the 1800s to the present and have regained attention with rising environmental expectations. Advances in battery technology and the expansion of charging infrastructure have enabled these vehicles to integrate more effectively into daily life. Modern electric vehicles have evolved from simple means of transportation into smart systems that transmit data and can be remotely managed through internet connectivity. Functions such as real-time traffic information, battery status monitoring, and remote control are central to this connection. e-SIM technology, by eliminating the need for a physical SIM card, provides more secure and flexible communication, allowing faster software updates and uninterrupted data flow between the vehicle and the cloud.

With the growing use of the internet in electric vehicles, the spread of e-SIM technology has increased the importance of technical and administrative regulations. Although current legislation does not explicitly prohibit internet or e-SIM use in electric vehicles, restrictions may be introduced due to concerns related to data security, privacy, and national security. The Information Technologies Authority sets rules in Türkiye regarding data security, user information, and the control of communication systems, and specifically requires e-SIMs to be managed domestically. This approach aims to ensure the secure operation of communication infrastructure and the uninterrupted functioning of software updates, emergency notifications, and communication systems. The BTK's decisions requiring that e-SIM modules be programmed only by domestic mobile operators, that data be stored within national borders, and that locally issued SIM cards and nationally located servers be used in e-Call systems have significant legal implications. These measures establish an effective legal framework particularly regarding national security, public order, competition, and consumer protection.

In conclusion, when regulations and practices concerning internet and e-SIM use in electric vehicles are evaluated together, these technologies appear essential for both vehicle safety and user experience. The obligations relating to domestic e-SIM management, data retention within the country, and the secure operation of communication infrastructure form the legal basis of this requirement. Ensuring data security, protecting user rights, and strengthening cybersecurity measures are necessary for the safe use of electric vehicles.

Keywords: Electric vehicles, e-SIM technology, connected vehicles, data security, communication systems.