BİLİŞİM VE TEKNOLOJİ HUKUKU DERNEĞİ

İSTANBUL MEDENİYET ÜNİVERSİTESİ

III. ULUSLARARASI BİLİŞİM VE TEKNOLOJİ HUKUKU SEMPOZYUMU

3RD INTERNATIONAL IT LAW SYMPOSIUM

29 – 30 KASIM / NOVEMBER 2024 - ISTANBUL

BİLDİRİ ÖZETİ KİTABI
ABSTRACT BOOK

EDİTÖR / EDITOR

Dr. Öğr. Üyesi (Asst. Prof. Dr) Şerafettin EKİCİ

www.bthukukusempozyumu.com

BİLİŞİM VE TEKNOLOJİ HUKUKU DERNEĞİ

İSTANBUL MEDENİYET ÜNİVERSİTESİ

III. ULUSLARARASI BİLİŞİM VE TEKNOLOJİ HUKUKU SEMPOZYUMU
III. INTERNATIONAL IT LAW SYMPOSIUM

29 – 30 Kasım /November 2024

ISTANBUL

BİLDİRİ ÖZETİ KİTABI
ABSTRACT BOOK

EDİTÖR / EDITOR
Dr. Öğr. Üyesi (Asst. Prof. Dr) Şerafettin EKİCİ

ISTANBUL / 2024

ISBN: 978-605-72218-2-7

SUNUŞ

Bilişim ve Teknoloji Hukuku Derneği ile İstanbul Medeniyet Üniversitesi işbirliği ile düzenlenmiş olan III. Uluslararası Bilişim ve Teknoloji Hukuku Sempozyumu, 29-30 Kasım 2024 tarihlerinde İstanbul'da gerçekleştirilmiştir.

Sempozyumda toplam oturumda birbirinden değerli kırk konuşmacı tebliğlerini dinleyicilerle buluşturmuşlardır.

Sempozyum öncesi hakemler tarafından kabul edilmiş olan tebliğlerin özetlerinden oluşan bu tebliğ özeti kitabının hukuk dünyasına hayırlı olmasını dileriz.

PRESENTATION

The III. International Symposium on Information and Technology Law, organized in collaboration with the Association of Information and Technology Law and Istanbul Medeniyet University, took place in Istanbul on November 29-30, 2024.

During the symposium, a total of forty distinguished speakers presented their papers in various sessions, engaging with the audience.

We hope that this book of abstracts, composed of the summaries of the presentations accepted by the reviewers prior to the symposium, will be beneficial to the legal community.

EDİTÖR / EDITOR
Dr. Öğr. Üyesi (Asst. Prof. Dr) Şerafettin EKİCİ

İÇİNDEKİLER / INDEKS

DÜZENLEME KURULU
ORGANIZING COMMITTEE

Prof. Dr. Özcan GÜNERGÖK	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Istanbul Medeniyet University Faculty of Law
Doç. Dr. Sezen KAMA IŞIK	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Istanbul Medeniyet University Faculty of Law
Dr. Öğr. Üyesi Şerafettin EKİCİ	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Istanbul Medeniyet University Faculty of Law
Dr. Öğr. Üyesi Meltem KAYA	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Istanbul Medeniyet University Faculty of Law
Dr. Öğr. Üyesi Hamza TÜZGEN	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Istanbul Medeniyet University Faculty of Law
Arş. Gör. Salih KARADENİZ	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Istanbul Medeniyet University Faculty of Law
Av. Muhammed Emre AVŞAR	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Adem GÜL	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Büşra ÖZELLİBEŞ	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Mehmet Melih GÜLSEREN	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Bahar ÖTE	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Raci Çetin YÜKSEKBAŞ	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Arif ALICI	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Enis KESKİN	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Meltem AVCI DEMİRCİ	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Nida ALTIN	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Ayşegül TUNÇ	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Gizem Gaye AK	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Betül TÜRKGÖZÜ	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Av. Ömer Can EKDİ	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Stj. Av. Aynur Feyza KABAN	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Stj. Av. Ahmet Can KURU	Bilişim ve Teknoloji Hukuku Derneği IT Law Society
Stj. Av. Züleyha KONUR	Bilişim ve Teknoloji Hukuku Derneği IT Law Society

BİLİM VE HAKEM KURULU
SCIENTIFIC AND REFEREE COMMITTEE

BİRİNCİ BÖLÜM:
BİLİŞİMİN TİCARET HUKUKUNA YANSIMALARI

6563 SAYILI ELEKTRONİK TİCARETİN DÜZENLENMESİ HAKKINDA KANUN KAPSAMINDA MOBİL UYGULAMA MAĞAZASI SAĞLAYICILARININ YÜKÜMLÜLÜKLERİ

Saranur SAKA*, Abdurrahman SAVAŞ**

Özet

Dünyada dijitalleşme çok hızlı bir şekilde ilerlemekte ve ticari işlemlerin yanı sıra kişisel ve hatta pek çok resmi işlem, akıllı telefonlar üzerinden gerçekleştirilmektedir. Bu durum akıllı cihazlarda kullanılan uygulamaların ve bu uygulamaların sunulduğu dijital mağazaların çoğalmasına neden olmuştur. Bu çoğalma ile birlikte dijital piyasalarda tekelleşme ve haksız rekabet ile ilgili sorunlar ortaya çıkmaya başlamıştır. Dijital piyasalarda tekelleşmeyi önlemek ve rekabet ortamını güçlendirmek için 1 Kasım 2022 tarihinde Avrupa Birliğinde Digital Markets Act (DMA) olarak isimlendirilen düzenleme yürürlüğe girmiş ve Mayıs 2023'den itibaren uygulanmaya başlamıştır. Bu düzenleme kapsamında nitelikleri itibari ile ağ bekçisi (*gatekeeper)* olarak isimlendirilen ve pazara hâkim durumda bulunan süjeler esas alınarak rekabeti engelleyici davranışları önleyici nitelikte hükümler getirilmiştir.

Ülkemizde de Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da (ETDHK), 1 Temmuz 2022 tarihinde yapılan değişikliklerle elektronik pazaryerleri kapsamında elektronik ticaret hizmet sağlayıcı ve elektronik ticaret aracı hizmet sağlayıcı kavramları getirilmiş ve bunlara farklı yükümlülükler yüklenmiştir.

ETDHK kapsamında getirilen bazı yeni yükümlülükler arasında haksız ticari uygulamaya ve tekelleşmeyi önleyici hükümlere ilişkin düzenlemeler önemlidir. Kanunun gerekçesinden de anlaşılacağı üzere, tekelleşmeyi önleyici hükümler düzenlenirken Avrupa Birliği Dijital Piyasalar Yasası (DMA) örnek alınmıştır. Ancak, ETDHK'de elektronik pazar yerindeki süjelere ilişkin *gatekeeper* nitelendirilmesine yönelik bir belirleme yapılmamış; sadece elektronik ticarete yönelik düzenlemeler yapılmıştır.

ETDHK Ek madde 1'de düzenlenen haksız ticari uygulamalara ilişkin hükümler elektronik ticaret aracı hizmet sağlayıcının aracılık hizmetini sunduğu elektronik ticaret hizmet sağlayıcıya yönelik faaliyetleri dikkate alınarak düzenlenmiştir. Doktrinde bu hükümlerin Avrupa Birliği 2019/1150 sayılı Çevrimiçi Aracılık Hizmetlerinin

* Arş. Gör., İstanbul Üniversitesi, Bilişim ve Teknoloji Hukuku Anabilim Dalı, ORCID-ID: 0009-0005-3452-9580, (saranur.saka@istanbul.edu.tr).

** Doç. Dr., İstanbul Üniversitesi, Bilişim ve Teknoloji Hukuku Anabilim Dalı, ORCID-ID: 0000-0002-3832-484X, (abdurrahman.savas@istanbul.edu.tr).

Ticari Kullanıcıları İçin Adil ve Şeffaf İşleyişin Sağlanması Hakkında Tüzük (P2B) düzenlemesiyle örtüştüğü belirtilmiştir. Maddenin ikinci fıkrasında ise sayılan hallerin birinci fıkrada belirtilen unsurları taşımasa bile haksız ticari uygulama olduğu karinesi getirilmiştir. Doktrinde haksız ticari uygulamaya ilişkin getirilen bu düzenlemenin daha çok 6098 sayılı Türk Borçlar Kanunu'nda düzenlenen Genel İşlem Koşulları denetimi ya da 6502 sayılı Tüketicinin Korunması Hakkında Kanunda düzenlenen haksız şartlar rejimine benzediği ifade edilmiştir.

Bu tartışmalar ışığında, ETDHK kapsamında mobil uygulama mağazalarının ve mobil uygulama mağazası sağlayıcılarının hukuki statülerinin tespit edilmesi ve bunların yükümlülüklerinin belirlenmesi gerekmektedir.

Anahtar Kelimeler: mobil uygulama mağazaları, mobil uygulama mağazası sağlayıcıları, elektronik ticaret aracı hizmet sağlayıcı, elektronik ticaret hizmet sağlayıcı, haksız ticari uygulamalar, ağ bekçisi.

OBLIGATIONS OF MOBILE APP STORE PROVIDERS UNDER THE LAW ON THE REGULATION OF ELECTRONIC COMMERCE NO.6563

Abstract

Digitalization is advancing rapidly in the world and commercial transactions, as well as personal and even many official transactions, are carried out via smartphones. This has led to the proliferation of applications used on smart devices and the digital stores where these applications are offered. In order to prevent monopolization in digital markets and to strengthen the competitive environment, the EU 2022/1925 Digital Markets Act (DMA) entered into force in the European Union on November 1st, 2022 and this regulation started to be implemented as of May 2023. In this regulation, provisions have been introduced to prevent anti-competitive behavior on the basis of the subjects who are called gatekeepers and who are in a dominant position in the market. With the amendments made to the Law on the Regulation of Electronic Commerce (E-Commerce Law) on July 1st, 2022, in Türkiye, the concepts of electronic commerce service provider and electronic commerce intermediary service provider were introduced within the scope of electronic marketplaces and different obligations were imposed on them. Among some of the new obligations introduced under the E-Commerce Law, regulations on unfair commercial practices and anti-monopolization provisions are important. The EU Digital Markets Act (DMA) was taken as an example while regulating the anti-monopolization provisions in the E-Commerce Law. However, the E-Commerce Law does not make any determination regarding the qualification of gatekeepers for the subjects in the electronic marketplace; only regulations have been made for electronic commerce.

The provisions regarding unfair commercial practices regulated in Annex Article 1 of the E-Commerce Law are regulated by taking into account the activities of the electronic commerce intermediary service provider towards the electronic commerce service provider for which it provides intermediary services. It is stated in the doctrine that these provisions overlap with the EU Regulation 2019/1150 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services (P2B). In the second paragraph of the Article, the presumption of unfair commercial practice is regulated even if the cases listed do not carry the elements specified in the first paragraph. It is stated in the doctrine that this article regulated on unfair commercial practice is more similar to the standardized terms regulated in Turkish Code of Obligations No.6098 or the unfair terms regime regulated in Consumer Protection Law No. 6502.

Considering these discussions, it is necessary to ascertain the legal status of mobile app stores and mobile app store providers and to determine their obligations under the E-Commerce Law.

Keywords: mobile app stores, mobile app store providers, electronic commerce intermediary service provider, electronic commerce service provider, unfair commercial practices, gatekeeper.

ELEKTRONİK CİHAZ SİGORTASI SİBER SALDIRI SONUCU CİHAZLARDA MEYDANA GELEN FİZİKİ ZARARLARI KARŞILAR MI?

Şerife Esra KİRAZ*

Özet

Günlük hayatın önemli bir parçası haline gelen teknoloji, iş yürütmekten, gündelik işleri yerine getirmeye, kamu hizmetlerinden yararlanmaktan, iletişim kurmaya pek çok olanda kullanılmaktadır. Bunun sonucunda siber risklere maruz kalma ihtimali artmaktadır. Siber risklerden bir tanesi olan siber saldırılar ise yetkilendirilmemiş kişilerce sistemdeki açıkların kullanılarak sisteme girilmesi ve buradaki verilere yönelik bir saldırı olarak tanımlanabilir. Siber saldırılar sonucunda söz konusu verilerin ele geçirilmesi, ifşası ya da itibara zarar verilmesi söz konusu olabilir.

Öte yandan siber saldırılar sadece veri ihlallerine yönelik sonuçlar doğurmamakta, cihazlara fiziksel zararlar da verebilmektedir. Siber saldırı sonucunda, elektronik cihaz sistemlerinin bozulması, sistem yavaşlaması, dolayısıyla elektronik cihazdan beklenen verimin alınamaması, bunun yanında elektronik bir şebekenin hedef alınması sonucu çıkabilecek bir yangın sonucu elektronik aletlerin zarar görmesi de mümkündür.

Siber saldırı sonucunda elektronik cihazlarda meydana gelebilecek fiziksel zararların nasıl giderilebileceği, bu türden risklere karşı hangi türden bir sigorta koruması sağlanabileceği hem elektronik cihaz kullanan büyük işletmeler, hem de nihai tüketici olarak ifade edebileceğimiz bireyler açısından önem arz eder. Zira, günümüzde giderek artan sayıda elektronik alet kullanılmakta, söz konusu aletler sadece cep telefonu, bilgisayar gibi cihazlarla sınırlı kalmayıp, akıllı ev aletlerini de içermektedir. Bu aletlerin de çoğu zaman wifi sistemine bağlanarak komut alması da düşünüldüğünde, siber saldırıların pek çok cihazı, kişiyi ve kurumu etkileyeceği yadsınamaz bir gerçektir.

Siber saldırılar ve buna ilişkin riskler sigorta sektörünün de dikkatini çekmekte, bu risklere yönelik sigortalar geliştirilmektedir. Türkiye'de, kendine has genel şartları düzenlenmemiş olsa da sigorta şirketlerine tarafından siber sigorta yapılmaktadır.

* Dr. Öğretim Üyesi, Çankırı Karatekin Üniversitesi Hukuk Fakültesi, Ticaret Hukuku ABD, ORCID ID 0000-0003-3163-8640, serifeesrakiraz@karatekin.edu.tr

Ancak, söz konusu sigortaların daha çok veri ihlalleri, verilerin çalınması, yayılması, ele geçirilen verilerle şantaj yapılması, veriler yoluyla kişi/kurum itibarının zarara uğraması gibi durumları kapsadığı görülmektedir. Dolayısıyla, siber sigortalar, siber saldırı sonucu elektronik cihazlarda meydana gelen fiziksel zararları kapsamamaktadır. Yapılan çalışmalarda da siber sigortaların kapsamının dar olduğu, siber risklerin ve zararların tamamının bu sigorta türü kapsamında korunmadığı görülmüştür.

Elektronik makine, teçhizat veya bilgi işletim sistemleri, Elektronik Cihaz Sigortası Genel Şartları'nda belirtilen zararlardan meydana gelen maddi ziya ve hasarlar dolayısıyla karşılaşılacak tamirat masrafları ve ikame bedelleri için sigortalanabilmektedir. Çalışmamız kapsamında siber saldırılar dolayısıyla bu makine ve teçhizatlarda meydana gelecek fiziksel zararlar, Genel Şartlar içinde yer alan "sabotaj", "kısa devre, yüksek voltaj ve endüksiyon akımının etkileri", "yangın ve bunlar sebebiyle yapılan söndürme, yıkma ve kurtarma ameliyelerinden" gerçekleşmiş sayılabilir mi sorusu cevaplandırılacaktır. Ayrıca, siber saldırıların "harp" ya da "terör olayları" gibi teminat kapsamı dışında sayılan hallerden olup olmadığı da incelenerek bir değerlendirme yapılacaktır.

Anahtar Kelimeler: Siber Saldırı, Siber Sigorta, Elektronik Cihaz Sigortası, Siber Risk, Teminat Kapsamı

DOES ELECTRONIC DEVICE INSURANCE COVER PHYSICAL DAMAGES TO DEVICES AS A RESULT OF CYBER-ATTACK?

Abstract

Technology, which has become an important part of daily life, is used in many areas such as conducting business, fulfilling daily tasks, benefiting from public services, and communicating. As a result, the possibility of exposure to cyber risks increases. Cyber-attacks which are one of the cyber risks, can be defined as an attack on the system and the data by unauthorised person who uses the vulnerabilities in the system. As a result of cyber-attacks, such data may be intercepted, disclosed or reputational damage may occur.

On the other hand, cyber-attacks do not only result in data breaches but can also cause physical damage to devices. As a result of a cyber-attack, it is possible that the electronic device systems may be disrupted, the system may slow down, thus the expected efficiency of the electronic device may not be obtained, as well as the electronic devices may be damaged by a fire that may occur due to targeting an electronic network.

It is important for both large enterprises using electronic devices and individuals who can be expressed as final consumers to reveal how physical damages to the

electronic devices as a result of a cyber-attack can be compensated and what kind of insurance protection can be provided against such risks. Regarding that an increasing number of electronic devices used, and these devices are not limited to devices such as mobile phones and computers, but also include smart home appliances. Considering that these devices often receive commands by connecting to the wifi system, it is an undeniable fact that cyber-attacks will affect many devices, individuals and institutions.

Cyber-attacks and related risks attract the attention of the insurance sector, and insurances are being developed for these risks. In Türkiye, cyber insurance is provided by insurance companies, although its specific general conditions are not regulated. However, it is seen that these insurances mostly cover situations such as data breaches, theft and dissemination of data, blackmailing with the captured data, and damage to the reputation of individuals and organizations through data. Therefore, cyber insurance does not cover physical damages to electronic devices as a result of a cyber-attack. Studies have shown that the scope of cyber insurance is narrow and not all cyber risks and damages are protected under this type of insurance.

Electronic machinery, equipment or information operating systems can be insured for repair costs and replacement costs to be incurred due to material loss and damages arising from losses specified in the General Terms and Conditions of Electronic Equipment Insurance. Within the scope of our study, the question of whether the physical damages to these machines and equipment due to cyber-attacks can be considered to have occurred due to 'sabotage', 'short circuit, high voltage and induction current effects', 'fire and extinguishing, demolition and rescue operations due to these', which are included in the General Conditions, will be answered. In addition, an assessment will be made by analysing whether cyber-attacks are considered as 'war' or 'terrorist incidents' which are not covered by the insurance.

Keywords: Cyber Attack, Cyber Insurance, Electronic Equipment Insurance, Cyber Risk, Coverage

SOSYAL MEDYA ETKİLEYİCİLERİ TARAFINDAN YAPILAN TİCARİ REKLAM VE HAKSIZ TİCARİ UYGULAMALAR HAKKINDA KILAVUZ'DA YER ALAN DÜZENLEMELERİN REKLAM HUKUKU AÇISINDAN DEĞERLENDİRİLMESİ

Abdurrahman Hamza TÜZGEN*

Özet

"Sosyal Medya Etkileyicileri Tarafından Yapılan Ticari Reklam ve Haksız Ticari Uygulamalar Hakkında Kılavuz" (Kılavuz) Reklam Kurulu'nun 04.05.2021 tarihli ve 309 sayılı toplantısında 2021/2 numaralı ilke kararı olarak kabul edilmiştir. İlgili Kılavuz, Tüketicinin Korunması Hakkında Kanun (TKHK), Ticari Reklam ve Haksız Ticari Uygulamalar Yönetmeliği (Reklam Yönetmeliği) ve 309 sayılı Reklam Kurulu toplantısında alınan karara dayanılarak hazırlanmıştır (Kılavuz md.3).

Kılavuz'da yer alan düzenlemelerin bir kısmı, kanun ve yönetmelikle paralellik göstermesine rağmen, Kılavuzda yer alan bazı maddelerin kanunda ve yönetmelikte açıkça belirtilmeyen yükümlülükler içerecek şekilde düzenlendiği görülmektedir. Bu durum, özellikle sosyal medya etkileyicileri olmak üzere, kılavuzdaki yükümlülüklere aykırı davranışlarda bulunan kişilerin idari yaptırımlarla karşılaşmalarına neden olmaktadır. Bu durum, ifade özgürlüğü bağlamında önemli bir sorun teşkil etmektedir. Zira, Avrupa İnsan Hakları Mahkemesi (AİHM) ve Anayasa Mahkemesi (AYM) kararlarında da ifade edildiği üzere, reklam faaliyeti ifade özgürlüğü kapsamında değerlendirilen bir haktır. Kılavuzda yer alan bazı düzenlemeler ile başta örtülü reklamlar olmak üzere, haksız reklamların önüne geçmek ve reklam hukuku alanına hakim olan ilkelere uyulmasını hedeflense de, reklam faaliyetlerinin Kılavuz ile kanunda öngörülenden daha fazla sınırlandırılması hukuk sistematiği açısından problemli bir durumdur. Normlar hiyerarşisinde kanundan daha alt seviyede yer alan bir düzenleme olan Kılavuzun, kanunda açıkça belirtilmeyen yükümlülükler getirmesi, nihayetinde tüketicinin korunmasından ziyade, tüketicilerin "bilgilenme" hakkının zarar görmesine sebep olmaktadır.

* Dr. Öğr. Üyesi, İstanbul Medeniyet Üniversitesi, ORCID: 0000-0002-4497-7302, hamza.tuzgen@medeniyet.edu.tr

Yukarıdaki açıklamaların yanında, Kılavuzda yer alan düzenlemeler hukuk sistematiği içerisinde doğru bir biçimde yer almış olsaydı dahi, bu düzenlemelerin sosyal medya etkileyicilerinin yaptıkları reklamların etkin denetimi açısından yeniden gözden geçirilmesi gerektiği göze çarpmaktadır. Bu bağlamda Kılavuzda yer alan bazı tanımlamaların hatalı şekilde yapıldığı, birtakım düzenlemelerin sınırlarının net çizilmediği ve kimi düzenlemelerin ise gerekli kapsayıcılıkta olmadığı göz çarpmaktadır.

Tüm bu açıklamalar doğrultusunda, Kılavuz ile hedeflenen gayeye ulaşılabilmesi adına, hukuk sistematiği açısından kısıtlamaların en azından bir kısmının kanun ile düzenlenmesi, tanımlamaların doğru bir biçimde yapılması ve hükümlerin sınırları ile kapsamlarının net şekilde ortaya konması gerekmektedir.

Anahtar Kelimeler: İfade Özgürlüğü, Reklam, Sosyal Medya, Sosyal Medya Etkileyicisi, Tüketicinin Korunması

EVALUATION OF THE REGULATIONS IN THE GUIDELINE ON COMMERCIAL ADVERTISEMENTS AND UNFAIR COMMERCIAL PRACTICES BY SOCIAL MEDIA INFLUENCERS IN TERMS OF ADVERTISING LAW

Abstract

'Guideline on Commercial Advertisements and Unfair Commercial Practices by Social Media Influencers' (Guideline) was adopted as principle decision numbered 2021/2 at the meeting of the Board of Advertisement dated 04.05.2021 and numbered 309. The Guideline was prepared based on the Law on the Protection of Consumers (TKHK), the Regulation on Commercial Advertisements and Unfair Commercial Practices (Advertisement Regulation) and the decision taken at the meeting of the Board of Advertising numbered 309 (Art. 3 of the Guideline).

Although some of the regulations in the Guideline are in parallel with the law and the regulation, it is observed that some of the articles in the Guideline are regulated in a way to include obligations that are not explicitly stated in the law and regulation. This situation leads to administrative sanctions for those, especially social media influencers, who violate the obligations in the guideline. This situation constitutes an important problem in the context of freedom of expression. This is because, as stated in the decisions of the European Court of Human Rights (ECtHR) and the Constitutional Court (AYM), advertising is a right that is evaluated within the scope of freedom of expression. Although some of the provisions in the Guideline aim to prevent unfair advertisements, particularly covered advertisements, and to comply with the principles governing the field of advertising law, it is problematic in terms of legal systematics that the Guideline restricts advertising activities more than stipulated

in the law. The fact that the Guideline, which is a regulation at a lower level than the law in the hierarchy of norms, imposes obligations that are not explicitly stated in the Law, ultimately causes damage to the right of consumers 'to be informed' rather than consumer protection.

In addition to the above explanations, even if the provisions in the Guideline were correctly included in the legal systematics, it is noteworthy that these regulations should be reviewed in terms of effective supervision of the advertisements made by social media influencers. In this context, it is observed that some of the definitions in the Guideline are incorrectly made, the boundaries of some provisions are not clearly defined and some provisions are not inclusive enough.

In line with all these explanations, in order to achieve the objective of the Guidelines, at least some of the restrictions should be regulated by Law, in terms of legal systematics, definitions should be made correctly, and the boundaries and scope of the provisions should be clearly defined.

Keywords: Freedom of Expression, Advertisement, Social Media, Social Media Influencer, Consumer Protection

YAPAY ZEKA SİSTEMLERİNİN ŞİRKETLERİN YÖNETİM KURULUNDA KULLANIMININ AVRUPA BİRLİĞİ YAPAY ZEKA KANUNU BAĞLAMINDA DEĞERLENDİRİLMESİ

Salih KARADENİZ*

Özet

Gelişen teknolojiler arasında en dikkat çekicilerden birisi hiç şüphesiz yapay zekâ teknolojisidir. Çeşitli kullanım alanlarının yanı sıra yapay zekâ teknolojileri, şirketlerin yönetimine de dâhil olmaya başlamıştır. Yapay zekâ, 2014 yılında ilk kez bir şirketin yönetim kuruluna atanmıştır! Yapay zekânın şirketlerin yönetimine sunacağı katkılar oldukça yüksektir. Faydalarıyla beraber birtakım olası sorunların çıkabileceği de literatürde değerlendirme konusu yapılmaktadır. Genel olarak yapay zekadan faydalanılması ile bu teknolojiden kaynaklı risklerin bertaraf edilmesi ve temel insan haklarının korunması amacıyla Avrupa Birliği, kapsamlı bir şekilde hazırladığı Yapay Zeka Kanunu'nu (AI ACT) 2024 yılında Resmi Gazetede yayımlamıştır.

Risk temelli yaklaşım esas alınarak hazırlanan AI ACT; yasaklı, yüksek riskli, sınırlı riskli ve minimum riskli yapay zeka sistemleri olarak ayrıma tabi tutulmuştur. Tebliğ konusu kapsamında olabilecek yasaklı yapay zeka sistemi kullanımı, AI Act m. 5/1-f. bendinde yer almaktadır. Bu bende göre, eğitim ve çalışma alanlarında gerçek kişilerin duygu tespitini yapan, diğer bir deyişle duygularını yorumlayan yapay zeka sistemleri yasaklanmıştır. Bu doğrultuda yapay zeka sistemlerinin şirketlerin yönetim kurulunda veya herhangi bir kademesinde duygu tanıma amacıyla kullanılması yasak kapsamında kabul edilebilecektir.

Yasaklı yapay zeka sistemlerinin yanı sıra şirketlerin yönetim kurulunda yapay zekanın kullanılması, AI ACT kapsamında yüksek riskli yapay zeka sistemleri açısından da değerlendirilmelidir. Ek 3'te düzenlenen yapay zeka sistemleri, yüksek riskli olarak kabul edilecektir (AI ACT m. 6/2). Örneğin bir şirketin herhangi bir kademesinde duygu tespiti yapan yapay zeka sistemini kullanması halinde, bu yapay zeka sistemi

* Araştırma Görevlisi, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku ABD, ORCID: 0000-0001-6586-3278, salih.karadeniz@medeniyet.edu.tr .

yüksek riskli kabul edilecek ve bu doğrultuda öngörülen yükümlülüklere uygun davranması gerekecektir. Diğer bir yüksek riskli yapay zeka sistemi ise istihdam, işçi yönetimi ve serbest mesleğe erişim başlığı altında düzenlenmiştir. AI ACT kapsamında kalan bir şirkette, yönetim kurulu üyesi olarak atanan veya üyelere yardımcı olması için kurulda yararlanılan yapay zeka, işçilerin alımında veya performanslarının değerlendirilmesinde kullanılıyorsa artık bu yapay zeka sistemi yüksek riskli olarak kabul edilecek ve şirket, "kullanıcı" olarak yükümlülüklere tabi olacaktır.

AI ACT, Avrupa Birliği tarafından çıkarılsa bile yasanın kapsam itibariyle genişliği göz önüne alındığında, yapay zeka sistemlerini şirket içerisinde herhangi bir kademede kullanmak isteyen şirketlerin, AI ACT'in kapsamında kalıp kalmadıklarını değerlendirmeleri önem arz etmektedir. Bu sebeple AI ACT'te yer alan kuralların şirketler bakımından dikkate alınması, gelecekteki olası regülasyonlar bakımından faydalı olabilecek niteliktedir. Bu nedenlerden hareketle tebliğ, yapay zekâ sistemlerinin şirketlerin yönetim kurulundaki rolünün Avrupa Birliği Yapay Zeka Kanunu bağlamında, hukuki çerçevesini çizmeyi amaçlamaktadır.

Anahtar Kelimeler: AI ACT, Yapay Zeka, Şirket Yönetim Kurulu, Şirketler Hukuku, Bilişim ve Teknoloji Hukuku.

EVALUATION OF THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS IN THE BOARD OF DIRECTORS OF COMPANIES IN THE CONTEXT OF THE EUROPEAN UNION AI ACT

Abstract

One of the most striking among the developing technologies is undoubtedly artificial intelligence technology. In addition to various fields of use, artificial intelligence technologies have also started to be included in the management of companies. Artificial intelligence was appointed to the board of directors of a company for the first time in 2014! The contributions of artificial intelligence to companies management are quite high. Along with its benefits, some possible problems are also evaluated in the literature. In order to utilize artificial intelligence in general and to eliminate the risks arising from this technology and to protect fundamental human rights, the European Union published its comprehensive Artificial Intelligence Act (AI ACT) in the Official Gazette in 2024.

AI ACT, which is prepared based on a risk-based approach, is divided into prohibited artificial intelligence systems, high risk, limited risk and minimum risk. The prohibited use of artificial intelligence systems that may be within the scope of the subject of the study is included in Art. 5/1-f. of the AI Act. According to this Article, artificial intelligence systems that detect the emotions of real persons, in other words, interpret

their emotions, are prohibited in the fields of education and work. Accordingly, the use of artificial intelligence systems for emotion recognition in the board of directors or at any level of companies may be considered within the scope of the prohibition.

In addition to prohibited AI systems, the use of AI in the board of directors of companies should also be assessed in terms of high-risk AI systems under the AI ACT. AI systems regulated in Annex 3 will be considered high-risk (Art. 6/2 of the AI ACT). For example, if a company uses an artificial intelligence system that detects emotions at any level of a company, this artificial intelligence system will be considered high-risk and will be required to comply with the obligations stipulated in this regard. Another high-risk AI system is regulated under the heading of employment, labor management and access to self-employment. In a company falling within the scope of the AI ACT, if the artificial intelligence appointed as a board member or utilized in the board to assist the members is used in the recruitment of workers or the evaluation of their performance, this artificial intelligence system will now be considered high-risk and the company will be subject to obligations as a "deployer".

Even if the AI ACT is enacted by the European Union, given the wide scope of the law, it is important for companies wishing to use artificial intelligence systems at any level within the company to assess whether they are covered by the AI ACT. For this reason, taking into account the rules in the AI ACT for companies may be useful in terms of possible future regulations. For these reasons, this paper aims to outline the legal framework of the role of artificial intelligence systems in the board of directors of companies in the context of the European Union Artificial Intelligence Act.

Keywords: AI ACT, Artificial Intelligence, Board of Directors, Company Law, Information and Technology Law.

İKİNCİ BÖLÜM:
YAPAY ZEKA HUKUKU

YAPAY ZEKÂNIN DENİZ TİCARET HUKUKUNA YANSIMALARI

Hacı KARA*

Özet

Yapay zekâ (YZ) *(Artificial Intelligence, AI)* bilgisayarların ve makinelerin insan zekasını ve problem çözme yeteneklerini taklit etmesini sağlayan teknolojiye verilen isimdir. Yapay zekâ kendi başına veya diğer teknolojilerle (örneğin, sensörler, coğrafi konum belirleme ve robotik işlemler v.s.) ile birlikte, (aksi takdirde insan zekâsı veya müdahalesi gerektirecek görevleri) yerine getirebilir. Dijital asistanlar, Küresel Konumlandırma Sistemi *(Global Positioning System, GPS)* rehberliği, otonom araçlar ve jeneratif yapay zekâ araçları (Open AI'nin Chat GPT'si gibi) günlük haberlerde ve günlük hayatımızda yer alan yapay zekâ örneklerinden sadece birkaçıdır.

Bilgisayar biliminin bir alanı olarak yapay zekâ, makine öğrenimi ve derin öğrenmeyi kapsar (ve genellikle bunlarla birlikte anılır). Bu disiplinler, insan beyninin karar verme süreçlerinden sonra modellenen, mevcut verilerden 'öğrenebilen' ve zaman içinde giderek daha doğru sınıflandırmalar veya tahminler yapabilen yapay zekâ algoritmalarının geliştirilmesini içerir.

Yapay zekâ pek çok hype döngüsünden geçmiştir. Ancak şüpheciler için bile ChatGPT'nin piyasaya sürülmesi bir dönüm noktasına işaret ediyor gibi görünmektedir. Üretken yapay zekâ en son bu kadar büyük göründüğünde, atılımlar bilgisayarla görme alanındaydı, ancak şimdi ileriye doğru sıçrama doğal dil işleme (NLP) alanındadır. Bugün, üretken Yapay Zekâ sadece insan dilini değil, görüntüler, video, yazılım kodu ve hatta moleküler yapılar dâhil olmak üzere diğer veri türlerini de öğrenebilir ve sentezleyebilir.

Yapay zekâ uygulamaları her geçen gün artmaktadır. Ancak iş dünyasında yapay zekâ araçlarının kullanımıyla ilgili heyecan arttıkça, yapay zekâ etiği ve sorumlu yapay zekâ ile ilgili konuşmalar kritik önem kazanmaktadır.

* Prof. Dr., İstanbul Medeniyet Üniversitesi, Hukuk Fakültesi, Deniz Ticaret Hukuku Anabilim Dalı Öğretim Üyesi, ORCID: 0000-0002-8255-6277.

Bu çalışmada yapay zekânın denizciliğe ve deniz ticaretine etkileri incelenecektir. Bu yazıda sadece insansız ticari gemiler ele alınacaktır. Akıllı gemi endüstrisinin askeri kullanımı ise bu yazıda tartışılmayacaktır.

Anahtar kelimeler: Yapay zekâ, yapay zekânın denizcilik sektöründe kullanılması, yapay zekâ etiği, hukuk ve yapay zekâ, ChatGPT'nin hukukta kullanılması.

REFLECTIONS OF ARTIFICIAL INTELLIGENCE ON MARITIME LAW

Abstract

Artificial intelligence, or AI, is the technology that enables computers and machines to mimic human intelligence and problem-solving abilities. AI can perform tasks (tasks that would otherwise require human intelligence or intervention) on its own or in combination with other technologies (e.g. sensors, geolocation, robotics, etc.). Digital assistants, Global Positioning System (GPS) guidance, autonomous vehicles and generative AI tools (such as Open AI's Chat GPT) are just a few examples of AI in the news and in our daily lives.

As a field of computer science, AI encompasses (and is often referred to as) machine learning and deep learning. These disciplines involve the development of AI algorithms that are modeled after the decision-making processes of the human brain, can 'learn' from available data and make increasingly accurate classifications or predictions over time.

AI has gone through many hype cycles. But even for skeptics, the launch of ChatGPT seems to mark a turning point. The last time generative AI looked this big, the breakthroughs were in computer vision, but now the leap forward is in natural language processing (NLP). Today, generative AI can learn and synthesize not only human language but also other types of data, including images, video, software code and even molecular structures.

The applications of artificial intelligence are increasing every day. But as excitement about the use of AI tools in business grows, conversations about AI ethics and responsible AI are becoming critical.

This study will examine the impact of AI on maritime and maritime trade. Only unmanned commercial vessels will be discussed in this paper. The military use of the smart ship industry will not be discussed in this paper.

Keywords: Artificial intelligence, use of artificial intelligence in maritime sector, ethics of artificial intelligence, law and artificial intelligence, use of ChatGPT in law.

FİNANSAL TAVSİYE SUNULMASINA YÖNELİK ROBO-DANIŞMANLIK HİZMETLERİNİN HUKUKİ NİTELİĞİ

Yiğit Türker ÇOBAN*

Özet

Sermaye piyasalarında, hatta genel olarak finansal piyasalarda yapay zekânın kullanım alanı gün geçtikçe genişlemektedir. Robo-danışmanlık hizmetleri de finansal piyasalarda yapay zekâ tabanlı uygulamaların bir görünümüdür. Günümüzde müşteriler ve yatırımcılar, bir internet sayfası veya mobil uygulama üzerinden, hiçbir insan müdahalesi bulunmaksızın veya sınırlı bir insan müdahalesi çerçevesinde, yapay zekâ ile desteklenen bir bilgisayar algoritmasından finansal tavsiyeler alabilmektelerdir. Robo-danışmanlık olarak nitelendirilen söz konusu hizmet türü, ülkemizde de yaygın bir uygulama alanına sahiptir. Ne var ki, mevzuatımızda "robo-danışmanlık" kavramına oldukça sınırlı bir biçimde yer verilmiş olup, bu hizmetin niteliği tam anlamıyla açıklığa kavuşturulmuş değildir. Öte yandan, Avrupa Birliği ve üye ülkeleri, Birleşik Devletler, Singapur, Hong Kong, Avusturalya gibi birçok yabancı hukuk sisteminde robo-danışmanlık hizmetleri, kanunkoyucunun, düzenleyici idari otoritelerin ve literatürün incelemelerine konu olmuştur. Ülkemizde de Sermaye Piyasası Kurulu'nun 2019 ilâ 2022 yıllarına ilişkin faaliyet raporlarında ve 2022-2026 Stratejik Planı'nda, robo-danışmanlık uygulamalarının mevzuattaki yerinin tespit edilmesi hedef olarak belirlenmiştir. Ne var ki, kanaatimizce, yeterli düzeyde somut adımlar henüz atılmamıştır. Robo-danışmanlık hizmetlerinin hukuki niteliğinin belirlenmesi çeşitli açılardan önem arz etmektedir. Söz konusu hizmetlerin aracı kurumlar, bankalar ve sermaye piyasası kurumu niteliğinde olmayan finansal teknoloji şirketleri tarafından sunulduğu görülmektedir. Bu bağlamda, bir robo-danışmanlık hizmet sağlayıcısının Sermaye Piyasası Kurulu'ndan izin almasının gerekli olup olmadığı, robo-danışmanlık hizmetinin hangi hükümlere tabi olduğu, yapay zekâ tabanı dikkate alınarak hukuki ve

* Dr, Araştırma Görevlisi, Yeditepe Üniversitesi Hukuk Fakültesi Ticaret Hukuku Anabilim Dalı; ORCID: 0000-0003-3958-3285; E-posta adresi: y.turkercoban@hotmail.com, yigit.coban@yeditepe.edu.tr.
Research Assistant, Yeditepe University Faculty of Law Department of Commercial Law; ORCID: 0000-0003-3958-3285; E-mail: y.turkercoban@hotmail.com, yigit.coban@yeditepe.edu.tr.

idari sorumluluk rejimlerinin nasıl tespit edileceği sorularını cevaplamak için öncelikle robo-danışmanlık hizmetinin hukuki niteliği tespit edilmelidir.

Türkiye'de bulunan robo-danışmanların, özellikle yatırım fonlarına, bunun yanında mevduat veya döviz yatırımlarına ilişkin tavsiye sunduğu belirtilebilir. Bu kapsamda, söz konusu hizmetlerin özellikle sermaye piyasası hukuku bağlamında, gerekli olduğu ölçüde ise bankacılık mevzuatı kapsamında değerlendirilmesi gerekmektedir. Özellikle, robo-danışmanlar tarafından sunulan tavsiyelerin, III-37.1 sayılı Yatırım Hizmetleri ve Faaliyetleri ile Yan Hizmetlere İlişkin Esaslar Hakkında Tebliğ çerçevesinde yatırım danışmanlığı faaliyeti olarak nitelendirilip nitelendirilemeyeceği önem arz etmektedir. Tebliğ kapsamında, yatırım danışmanlığı faaliyetinin doğması için, ticari veya mesleki bir faaliyet çerçevesinde, sermaye piyasası araçları veya ihraççılar hakkında, belirli bir müşteriye veya gruba yönelik olarak, yönlendirici nitelikte bilgi, araştırma, yorum veya tavsiye sunulması gerekmektedir. Şu var ki, Tebliğ'in 45'inci maddesinin 5 ve 6'ncı fıkralarında, belirli yatırım fonlarına ilişkin olarak tavsiye sunulması faaliyeti, yatırım danışmanlığının kapsamından muaf tutulmuştur. Robo-danışmanların çoğunlukla yatırım fonlarına ilişkin tavsiye sunması nedeniyle söz konusu istisnalar, bu hizmet türü açısından ayrı bir öneme sahiptir.

O hâlde çalışmamızın ana konusunu tavsiye sunulmasına yönelik robo-danışmanlık hizmetlerinin hukuki niteliğinin, sermaye piyasası hukuku bağlamında ne olduğu, özellikle yatırım danışmanlığı sayılıp sayılamayacağı noktasındaki de lege lata incelemelerimiz ve de lege ferenda değerlendirmelerimiz oluşturacaktır. Çalışmamızda inceleyeceğimiz başlıca alt sorunları ise karma tavsiye sunan robo-danışmanların sermaye piyasası hukuku kapsamında değerlendirilip değerlendirilmeyeceği, müşteri gruplarını profilleme şeklinde çalışan yapay zekâ algoritmalarının "belirli bir müşteriye yönelik" tavsiye sunup sunamayacağı, internet üzerinden sunulan robo-danışmanlık uygulamalarının geleneksel yatırım faaliyetlerinden farklı bir biçimde değerlendirilip değerlendirilmeyeceği, insan iletişiminin zayıfladığı bu noktada müşterinin uygunluk ve yerindelik testleri ile müşterilere yapılan uyarıların yeniden ele alınmasının gerekip gerekmediği ve netice itibariyle robo-danışmanlık hizmetlerinin III-37.1 sayılı Tebliğ m. 45/f. 5-6 istisnaları karşısındaki durumu oluşturacaktır.

Anahtar Kelimeler: algoritmik yatırım; robo-danışmanlar; robo-danışmanlık; yatırım danışmanlığı; yatırım tavsiyeleri

LEGAL NATURE OF ROBO-ADVISORY SERVICES FOR THE PROVISION OF FINANCIAL ADVICE

The use of artificial intelligence in capital markets, and even in financial markets in general, is expanding day by day. Robo-advisory services are also a kind of AI-based practices in financial markets. Today, clients and investors can receive financial advice from a computer algorithm based on artificial intelligence through a website or mobile application, with no or limited human intervention. This type of service, namely robo-advisory, is also widely practiced in Türkiye. However, the concept of "robo-advisory" has been included in our legislation in a very limited manner, and the legal nature of this service has not been fully clarified. On the other hand, in many foreign legal systems, such as the European Union and its member states, the United States, Singapore, Hong Kong, and Australia, robo-advisory services have been the subject of scrutiny by lawmakers, regulatory authorities, and the literature. In Türkiye, the Capital Markets Board's annual reports for the years 2019 to 2022 and the Strategic Plan for 2022-2026 set the goal of determining the place of robo-advisory in the legislation. However, in our opinion, sufficient concrete steps have not yet been taken. Determining the legal nature of robo-advisory services is vital from various perspectives. It is observed that such services are provided by intermediaries, banks, and FinTech firms which are not capital market institutions. In this context, in order to answer the questions of whether a robo-advisory service provider is required to be authorized by the Capital Markets Board, which provisions the robo-advisory service is subject to, and how to determine the legal and administrative liability regimes considering the artificial intelligence base, the legal nature of the robo-advisory service should first be determined.

It can be noted that robo-advisors in Turkey offer advice, in particular, on investment funds, besides deposits and foreign currency investments. In this context, such services should be evaluated particularly in the context of capital markets law and, to the extent necessary, in the context of banking legislation. In particular, it is essential to consider whether the advice provided by robo-advisors can be qualified as investment advisory under the III-37.1 Communiqué on Principles Regarding Investment Services, Activities and Ancillary Services. Within the scope of the Communiqué, in order for an investment advisory activity to arise, information, research, comments or recommendation on capital market instruments or issuers, directed to a particular client or group of clients, must be provided within the framework of a commercial or professional activity. However, paragraphs 5 and 6 of Article 45 of the Communiqué exempt the provision of advice on certain investment funds from the scope of investment advisory. As robo-advisors mostly provide advice on investment funds, these exemptions are of particular importance for this type of service.

Therefore, the main subject of this research will be our de lege lata analysis and de lege ferenda assessment of the legal nature of robo-advisory services for the provision of advice in the context of capital markets law, and, in particular, whether they can be considered investment advisory services. The main sub-issues that will

be examined in this research are whether robo-advisors providing mixed advice can be considered within the scope of capital markets law, whether artificial intelligence algorithms working in the form of profiling customer groups can provide advice "for a particular customer", whether robo-advisory services offered via the internet should be evaluated differently from traditional investment activities, whether the suitability and appropriateness tests and the warnings given to the clients should be reconsidered at this point where human communication is weakened, and consequently, how robo-advisory services should be considered in accordance with the exemptions regulated at Art. 45 / para. 5-6 the Communiqué No. III-37.

Keywords: algorithmic trading; robo-advisors; robo-advisory; investment advisory; investment advice

YARGIDA YAPAY ZEKÂ KULLANIMININ HUKUKİ DENETİMİ VE YARGI ETİĞİ İLKELERİ BAKIMINDAN İNCELENMESİ

Ahmet Haşim ALAGÜNEY*

Özet

Yapay zekâ teknolojileri, her geçen gün iş yükü artan yargı organlarının karar verme süreçlerinde hız ve verimlilik sağlama potansiyeli ile dikkat çekmektedir. Ancak bu teknolojilerin yargıya entegrasyonu, önemli hukuki ve etik zorluklar doğurmaktadır. Yargıda Yapay Zekâ teknolojilerinin kullanımı önyargı, şeffaflık, izlenebilirlik ve hesap verebilirlik gibi konularda önemli riskler taşımaktadır.

Bu çalışmanın temel amacı, Yapay Zekâ destekli hukuk teknolojilerinin yargıda kullanımının hukuki denetimi konusunu ele almak ve yargı etiği ilkeleri çerçevesinde bir inceleme yapmaktır. Bu doğrultuda, çalışmada Bangalor Yargı Etiği İlkeleri arasında sayılan bağımsızlık, tarafsızlık, doğruluk, dürüstlük, eşitlik, ehliyet ve liyakat gibi temel yargı etiği ilkelerinin Yapay Zekâ sistemlerine entegrasyonu ele alınacaktır. Avrupa Konseyi Avrupa Adaletin Etkinliği Komisyonu (CEPEJ) tarafından hazırlanan "Yapay Zekanın Yargı Sistemlerinde ve Çevrelerinde Kullanımına İlişkin Avrupa Etik Şartı" ve "Avrupa Birliği Yapay Zekâ Yasası" düzenlemeleri ışığında yargı süreçlerinde Yapay Zekâ kullanımına ilişkin oluşturulan mevcut hukuki denetim mekanizmaları irdelenecektir.

Çalışmada ayrıca Yapay Zekâ sistemlerinin yargı süreçlerindeki mevcut rolü ve gelecekteki potansiyel kullanım alanlarının neler olduğu, yargıda yapay zekanın kullanımının faydaları ve taşıdığı riskler ele alınacak, Yapay Zekâ sistemlerinde kullanılan algoritmaların şeffaflık, izlenebilirlik ve hesap verebilirlik gibi özellikleri taşıyıp taşımadığı hususları incelenecektir. Çalışmada ayrıca etik ihlallerin önlenmesi ve hukuki denetimin etkin bir şekilde sağlanabilmesi için çözüm önerilerine yer verilecek, Yapay Zekanın yargı süreçlerinde kullanımına yönelik etik ve hukuki standartların nasıl geliştirilebileceği ve bu alandaki reform ihtiyaçları tartışılacaktır.

Anahtar Kelimeler: Yapay Zekâ, Hukuk Teknolojileri, Yargı Etiği, AB Yapay Zekâ Yasası, Avrupa Etik Şartı.

* Avukat Dr., ORCID numarası, mail,

LEGAL OVERSIGHT OF ARTIFICIAL INTELLIGENCE USE IN THE JUDICIARY AND EXAMINATION IN TERMS OF PRINCIPLES OF JUDICIAL ETHICS

Abstract

Artificial intelligence technologies attract attention with their potential to provide speed and efficiency in the decision-making processes of judicial bodies, whose workload increases day by day. However, the integration of these technologies into the judiciary brings significant legal and ethical challenges. The use of Artificial Intelligence technologies in the judiciary carries significant risks in terms of bias, transparency, traceability and accountability.

The main purpose of this study is to examine of legal supervision of the use of AI-supported legal technologies in the judiciary and to analyse them within the framework of judicial ethics principles. In this context, the study will focus on the integration of the core principles of judicial ethics such as independence, impartiality, integrity, honesty, equality, competence and merit, which are listed among the Bangalore Principles of Judicial Ethics, into Artificial Intelligence systems. In the light of the 'European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment' prepared by the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe and the 'European Union Artificial Intelligence (AI) Act', the existing legal control mechanisms regarding the use of Artificial Intelligence in judicial processes will be analysed.

Moreover, the study will examine the current role of Artificial Intelligence systems in judicial processes and their potential future areas of use, the benefits and risks of the use of artificial intelligence in the judiciary, and whether the algorithms used in Artificial Intelligence systems have features such as transparency, traceability and accountability. The study will also include suggestions for solutions to prevent ethical violations and ensure effective legal oversight, and discuss how ethical and legal standards can be developed for the use of Artificial Intelligence in judicial processes and the reform needs in this field.

Key Words: Artificial Intelligence, Legal Technologies, Judicial Ethics, EU Artificial Intelligence Act, European Ethical Charter.

YAPAY ZEKÂ VE BÜYÜK VERİ ANALİTİĞİNDE VERİ HUKUKU: MAHREMİYET VE DİJİTAL HAKLARIN KORUNMASI

Esra Fatma FAZLIOĞLU*

Özet

Yapay Zekâ (YZ) ve büyük veri teknolojilerinin hızla ilerlemesi, veri gizliliği ve bireylerin dijital hakları konusunda önemli etik ve hukuki ikilemler yaratmıştır. Büyük veri analitiği, sağlık, güvenlik ve pazarlama gibi alanlarda avantajlar sağlasa da kişisel verilerin işlenmesi sürecinde önemli gizlilik ihlallerine neden olmaktadır. Bu çalışma, YZ destekli büyük veri analitiğinin gizlilik üzerindeki etkilerini veri koruma hukuku bağlamında incelemekte ve mevcut yasal düzenlemelerin yeterliliğini değerlendirmektedir.

Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR), veri koruma alanındaki en kapsamlı mevzuatlardan biri olarak birçok ülke için küresel bir kıstas niteliği taşımaktadır. GDPR, veri minimizasyonu, anonimleştirme ve kişisel verilerin işlenmesi sırasında bireylerin açık rızasının alınması gibi temel kavramları vurgulamaktadır. Ancak, bu ilkelerin büyük veri analitiği ve YZ uygulamaları bağlamında yeterliliği sorgulanmaktadır. Anonimleştirilmiş veri setlerinin, birden fazla veri setinin birleştirilmesi yoluyla yeniden bireylerle ilişkilendirildiği "yeniden tanımlama" kavramı, büyük bir endişe kaynağı oluşturmaktadır. Bu süreç, anonimleştirmenin beklenenden çok daha az koruma sağladığını ve veri gizliliği açısından ciddi riskler yarattığını göstermektedir.

Yeniden tanımlama, gizlilik açısından ciddi tehditler oluşturmaktadır ve GDPR gibi düzenlemelerin yetersiz kaldığı durumlarda sonuçları ağır olabilir. Anonimleştirme yöntemlerinde kaydedilen ilerlemelere rağmen, yeniden tanımlama tehdidinin artması, bireylerin gizlilik haklarını tehlikeye atmakta ve kişisel verilerin kötüye kullanılmasına yol açabilmektedir. YZ destekli sistemlerin bireyleri profilleyerek ayrımcı sonuçlar

* Avukat, Marmara Üniversitesi Bilişim Yüksek Lisans Öğrencisi, ORCID: 0000-0002-5874-6994, email: efazlioglu@marun.edu.tr

üretme kapasitesi de önemli bir endişe kaynağıdır. Bu nedenle, bireylerin dijital haklarını koruyacak güçlü ve etkili veri koruma hukuku düzenlemeleri gereklidir.

Bu çalışma, Avrupa Birliği'nin önerdiği Yapay Zekâ Yasası (AI Act) ile Genel Veri Koruma Tüzüğü (GDPR) arasındaki ilişkiyi incelemektedir. AI Act, YZ teknolojilerinin güvenli, etik ve şeffaf bir şekilde kullanılmasını sağlamak amacıyla risk temelli bir çerçeve benimsemektedir. AI Act, YZ sistemlerini risk seviyelerine göre sınıflandırmakta ve özellikle büyük veri analitiği ile uğraşan yüksek riskli sistemler için veri minimizasyonu, anonimleştirme ve şeffaflık protokollerini zorunlu kılmaktadır. Bu düzenlemeler, kişisel verilerin işlenmesi sırasında bireylerin gizliliğinin korunmasını hedeflemektedir.

AI Act ile GDPR'nin birleştirilmesi, bireylerin veri korumasını sağlamak açısından büyük önem taşımaktadır. AI Act, YZ teknolojilerinin kişisel verileri nasıl işlemesi gerektiğine dair düzenlemeler getirmekte ve GDPR ile uyumlu olarak, bireylerin rızası olmadan veri işlenmesini sınırlamaktadır. Şeffaflık ve hesap verebilirlik ilkeleri, bireylerin haklarını korumak ve otomatik karar verme süreçlerinde insan denetimini sağlamak açısından temel unsurlardır ve YZ uygulamaları için vazgeçilmezdir.

Bu çalışmanın yöntemi, YZ ve büyük veri analitiği ile ilgili ulusal ve uluslararası hukuki belgelerin incelenmesine dayanmaktadır. Bu analiz, Avrupa Birliği'nin GDPR ve AI Act çerçevesinde kişisel verilerin korunmasına ve gizlilik ihlallerinin önlenmesine yönelik oluşturduğu yasal çerçevelere odaklanacaktır. YZ ve büyük veri analitiği bağlamında bireylerin gizlilik haklarının korunması, güçlü ve kapsamlı düzenlemeler gerektirmektedir. AI Act ve GDPR'nin entegre olarak uygulanması, bu teknolojilerin güvenli ve sorumlu kullanımında önemli bir ilerlemeyi temsil etmektedir.

Anahtar Kelimeler: Yapay Zekâ (YZ), Büyük Veri Analitiği, Veri Koruma Hukuku, Genel Veri Koruma Tüzüğü (GDPR), Mahremiyet ve Dijital Haklar

DATA LAW IN ARTIFICIAL INTELLIGENCE AND BIG DATA ANALYTICS: PROTECTION OF PRIVACY AND DIGITAL RIGHTS

Abstract

The swift advancement of artificial intelligence (AI) and big data technologies has engendered substantial ethical and legal dilemmas around data privacy and individual digital rights. Although big data analytics provides benefits in fields like healthcare, security, and marketing, it also poses significant privacy infringements throughout the handling of personal data. This paper analyzes the influence of AI-driven big data analytics on privacy in the context of data protection law and evaluates the sufficiency of current legislative rules.

The European Union's General Data Protection Regulation (GDPR) is among the most extensive legislation in data protection, acting as a benchmark for numerous countries globally. The GDPR underscores essential concepts including data minimization, anonymization, and the necessity of getting explicit agreement from individuals when processing personal data. The adequacy of these principles in relation to big data analytics and AI applications is under scrutiny. The notion of re-identification, wherein anonymized data sets are linked back to individuals via the amalgamation of several data sets, presents a considerable concern. This procedure demonstrates that anonymization provides significantly less security than anticipated and poses substantial risks to data privacy.

Re-identification poses significant threats to privacy, and when legislation like the GDPR are inadequate, the repercussions can be severe. Notwithstanding progress in anonymization methods, the escalating threat of re-identification jeopardizes individuals' privacy rights and may result in the exploitation of personal data. The capacity of AI-driven systems to profile individuals and produce discriminatory results is a significant worry. Consequently, robust and efficient legislative frameworks for data protection are essential to preserve individuals' digital rights.

This paper analyzes the relationship between the European Union's proposed Artificial Intelligence Act (AI Act) and the General Data Protection Regulation (GDPR). The AI Act employs a risk-based framework to guarantee the safe, ethical, and transparent utilization of AI technologies. It categorizes AI systems according to their risk level, requiring data reduction, anonymization, and transparency protocols, especially for high-risk systems involved in big data analytics. These regulations seek to safeguard individuals' privacy during the handling of their personal data.

The amalgamation of the AI Act with the GDPR is crucial for safeguarding individuals' data protection. The AI Act establishes legislation governing the processing of personal data by AI technologies and, in accordance with the GDPR, restricts data processing without individual consent. The principles of openness and accountability are essential for safeguarding individual rights and ensuring human oversight in automated decision-making processes, which are foundational for AI applications.

This study's methodology relies on the examination of national and international legal documents related to AI and big data analytics. This analysis will focus on the legislative frameworks instituted by the European Union's GDPR and AI Act concerning personal data protection and the mitigation of privacy infringements. The safeguarding of individual privacy rights within the realm of AI and big data analytics necessitates robust and comprehensive rules. The combined implementation of the AI Act and GDPR signifies a substantial advancement in the secure and responsible utilization of these technologies.

Keywords: Artificial Intelligence (AI), Big Data Analytics, Data Protection Law, General Data Protection Regulation (GDPR), Privacy and Digital Rights

ÜÇÜNCÜ BÖLÜM:
KRİPTO VARLIK HUKUKU

KRİPTO VARLIK HİZMET SAĞLAYICILARI VE KRİPTO VARLIK HİZMET SAĞLAYICI MENSUPLARININ HUKUKİ SORUMLULUĞUNDA TEMEL ESASLAR

Harun ERYİĞİT*

Özet

Kripto varlıklar ortaya çıktıklarından bu yana birçok ülkede kripto varlıklara yönelik açık düzenlemeler bulunmamakta olup uluslararası kurumların yeknesak bir uygulama seti oluşturma çalışmaları devam etmektedir. Ülkemizde ise bu konuda en somut adım 26 Haziran 2024 tarihinde kabul edilen ve 2 Temmuz 2024 tarihli ve 32590 sayılı resmi gazetede yürürlüğe giren "Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun" ile atılmış, kripto varlıklar açık bir şekilde pozitif hukuk düzenlemelerimizin bir parçası haline gelmiştir.

Sermaye piyasası kanununda yapılan bu değişiklik ile birlikte kripto varlık saklama hizmeti sağlayan kuruluşları ve bu 6362 sayılı Kanuna dayanılarak yapılacak düzenlemelerde kripto varlıkların ilk satış ya da dağıtımı dâhil olmak üzere kripto varlıklarla ilgili olarak hizmet sağlamak üzere belirlenmiş diğer kuruluşlar kripto varlık hizmet sağlayıcısı olarak nitelendirilmiş ve bu kapsamda geniş bir sorumluluk rejimi oluşturulmuştur.

Kripto varlık hizmet sağlayıcılarının hukuka aykırı faaliyetleri ile nakit ödeme ve/veya kripto varlık teslim yükümlülüklerini yerine getirememesinden kaynaklanan zararlardan kripto varlık hizmet sağlayıcıları sorumludur. Zararın kripto varlık hizmet sağlayıcılarından tazmin edilememesi veya edilemeyeceğinin açıkça belli olması hâlinde; kripto varlık hizmet sağlayıcı mensupları kusurlarına ve durumun gereklerine göre zararlar kendilerine yükletilebildiği ölçüde sorumlu olup, şahsi sorumlulukla ilgili olarak bu Kanunun 110/B maddesi uygulanır denilmiştir. 110/B maddesi uyarınca kripto varlık hizmet sağlayıcının 6362 sayılı Kanun'un 110/A maddesi kapsamında zimmet sayılan karar ve işlemler gerçekleştirdiği tespit edilen yönetim kurulu başkan

* Doç. Dr., İstanbul Medipol Üniversitesi Hukuk Fakültesi, Ticaret Hukuku Anabilim Dalı, https://orcid.org/0000-0002-6066-1287, heryiigt@medipol.edu.tr.

ve üyeleri, diğer mensupları, hukuken veya fiilen yönetim veya kontrolünü elinde bulundurmuş olan gerçek kişi ortaklarının müşterilere verdikleri zararla sınırlı olarak zimmete geçirildiği tespit edilen tutardan öncelikli olarak karşılanmasını sağlamak amacıyla şahsi sorumlulukları yoluna gidilerek, Kurulun talebi üzerine doğrudan şahsen iflaslarına mahkemece karar verilebilecektir.

Getirilen bu düzenlemeler gerek içeriği gerekse de uygulanacağı çevrenin tespiti bakımından bir takım soru işaretlerini beraberinde getirmektedir. Bu soru işaretlerinin giderilmesi adına kripto varlık hizmet sağlayıcıları ve kripto varlık hizmet sağlayıcı mensuplarının hukuki sorumluluğunda temel esasların tespiti amaçlanmaktadır.

Anahtar Kelimeler: Kripto, Kripto Varlıklar, Kripto Varlık Hizmet Sağlayıcı, Platform, RWA

FUNDAMENTAL PRINCIPLES OF LEGAL LIABILITY FOR CRYPTO ASSET SERVICE PROVIDERS AND MEMBERS OF CRYPTO ASSET SERVICE PROVIDERS

Abstract

Since the inception of crypto assets, a notable absence of explicit regulatory frameworks has characterized many jurisdictions, while international institutions are actively working to establish a uniform set of practices. In the Turkish context, a significant legislative advancement occurred with the enactment of the "Law on Amending the Capital Markets Law" on June 26, 2024, which entered into force on July 2, 2024, as published in the official gazette (number 32590). This law explicitly integrates crypto assets into the corpus of positive legal regulations in Turkey.

The amendments to the Capital Markets Law categorize entities providing crypto asset custody services, along with other organizations designated to facilitate services related to crypto assets—including initial sales or distributions—under the umbrella of crypto asset service providers. This classification has led to the establishment of an expansive liability regime.

According to the provisions set forth, crypto asset service providers bear responsibility for damages resulting from unlawful activities, as well as for failures to meet obligations pertaining to cash payments and/or crypto asset deliveries. In instances where compensation for damages by the crypto asset service providers is evidently unattainable, the members of these service providers may be held liable to the extent that damages can be attributed to them based on their respective faults and the relevant circumstances. Article 110/B of the Law delineates the parameters of personal liability in such cases. Specifically, if it is determined that the chairman and members of the board of directors of a crypto asset service provider have engaged

in decisions and transactions constituting embezzlement as defined in Article 110/A of Law No. 6362, their personal liability will be invoked to ensure that the amounts identified as embezzled, limited to the damages incurred by clients, are prioritized for restitution. Furthermore, upon the Board's request, a court may issue a declaration of personal bankruptcy for these individuals.

The introduction of these regulatory measures gives rise to several questions concerning both the content and the contextual applicability of the law. In light of these uncertainties, it is essential to establish foundational principles governing the legal liability of crypto asset service providers and their members.

Key Words: Crypto, Crypto Assets, Crypto Asset Service Providers, Platforms, RWA.

KRİPTO VARLIK ARZI AÇISINDAN HALKTAN PARA TOPLAMA EYLEMLERİNE İLİŞKİN SUÇLAR VE NORM ÇATIŞMALARI ÜZERİNE BİR DEĞERLENDİRME

Aslıhan KART ALTUN*

Özet

Türk Ticaret Kanunu'nun ("TTK") 552 ve 562. maddelerinde Sermaye Piyasası Kanunu ("SPKn") hükümleri saklı kalmak kaydıyla, bir şirket kurmak veya şirketin sermayesini artırmak amacıyla yahut vaadiyle halka her türlü yoldan çağrıda bulunularak para toplanması suç olarak düzenlenmiştir. Genel hüküm olarak bu madde mihenk alındığında sırasıyla önce SPKn'nun tanımı ile "*sermaye piyasası araçlarının satın alınması için her türlü yoldan yapılan genel bir çağrıyı ve bu çağrı devamında gerçekleştirilen satış*" anlamına gelen halka arza, sonrasında 109. maddesi ile düzenlenen usulsüz halka arz ve izinsiz sermaye piyasası faaliyetleri suçlarına ve 104. maddesinde yer alan piyasa bozucu eylemler kabahatlerine gidilmekte; devamında yeni bir düzenleme olarak SPKn 35B/ 6 hükmünde düzenlenen kripto varlıkların satış ya da dağıtımının yapılması suretiyle halktan para toplama eylemlerinin genel hükümlere atfına varılmakta; en nihayetinde Türk Ceza Kanunu'ndaki ("TCK") dolandırıcılık suçları başta olmak üzere suçlarla ilgili bir başka genel düzenlemeye geri dönülmektedir.

Konu, tüm bu hükümler çerçevesinde ele alındığında ise kripto varlık arzı konusunda da genel hükümlere atıf kurulduğundan, öncelikle, TTK'da düzenlenen halktan para toplama suçu incelenmeli ve örneğin yeni TTK ile re'sen takip olunacak bir suç olarak düzenlenmekte iken 2012 yılında yapılan değişiklik sonucunda hala re'sen mi takip edileceği yoksa şikâyete bağlı mı olduğunun belirsizliği, ilk sorun olarak karşımıza çıkmaktadır.

İkinci olarak, SPKn hükümleri uyarınca düzenlenen suç ve kabahatler olarak usulsüz halka arz, izinsiz sermaye piyasası faaliyetleri ve piyasa bozucu eylemlerden kimlerin

* Dr. Kart Avukatlık Bürosu, ORCID No. 0000-0002-9263-630X, aslihankart@gmail.com

sorumlu olacağı ve mezkûr suç ve kabahatler arasında ortaya çıkması muhtemel içtima sorunları da incelenmeye değer diğer bir hususdur ki söz konusu içtimaın hem suçların kendi arasında hem de suç ve kabahatler arasında doğabilme ihtimalleri ayrı ayrı dikkate alınarak belirlenmesi gerekmektedir.

Son olarak, SPKn'nun md. 35B/ 6 fıkrasında "*kripto varlıkların satış ya da dağıtımının yapılması suretiyle halktan para toplayanlar ile bunlara fon sağlayanlar arasındaki ilişkiler genel hükümlere tabidir*" denilerek ve getirilen müteselsil sorumluluklar ile kripto varlık hizmet sağlayıcıların faaliyetleri konusunda doğrudan SPKn hükümlerine değil, genel hükümlere yapılan atıf ele alınmalıdır.

Çalışmada konu edilen, halktan para toplama eylemlerine ilişkin suçlar açısından SPKn, TTK ve TCK hükümleri arasında doğacak norm çatışmasından hareketle genel - özel (*lex specialis ilkesi*), önceki - sonraki (*lex posterior ilkesi*) kanun ilişkileri ve çapraz norm çatışmaları incelenmeye değer bir başka husus olarak kendilerini göstermektedir.

Bu doğrultuda çalışma kapsamında TTK, SPKn ve TCK çemberinde gelişen bu ilişkiler incelenerek hukuki sorun tespitleri ile muhtemel çözüm önerileri getirilmesi amaçlanmaktadır. Aslında çok sayıda soru işaretinin ortaya konulmaya çalışılacağı bu çalışma kapsamında sermaye piyasası alanında halktan para toplama eylemleri ile bağlantılı olan suç ve kabahatler ve bunların kripto varlık hizmet sağlayıcıların halktan para toplamaya ilişkin eylemleri ile ilişkileri ile SPKn md. 35B/ 6 uyarınca genel hükümlere atıflar nedeniyle TTK'da düzenlenen halktan para toplama suçu ve TCK'nin ilgili olabilecek hükümleri üzerinden bir tartışma sağlanacaktır.

Anahtar Kelimeler: sermaye piyasası, kripto varlık arzı, halka arz, halktan para toplama, usulsüzlük.

AN EVALUATION ON THE CRIMES AND NORM CONFLICTS RELATED TO THE ACTS OF COLLECTING MONEY FROM THE PUBLIC IN TERMS OF CRYPTO ASSET OFFERING

Abstract

Without prejudice to the provisions of the Capital Market Law ("CML"), in Articles 552 and 562 of the Turkish Commercial Code ("TCC") make it a criminal offence to collect money by any means by appealing to the public in any way, with the intention or promise of establishing a company or increasing the capital of the company. When this general provision is based on as a cornerstone, firstly on the public offer, which is defined in the CML as "A general invitation to purchase capital market instruments and the sale carried out in response to following this invitation"; afterwards the offences of improper public offer and unauthorized capital market activity regulated in Article 109 and the misdemeanors of market abuse actions regulated in Article 104. Then,

as a new regulation, the acts of collecting money from the public through the sale or distribution of crypto assets are referred by Article 35B/ 6 of the CML to the general provisions. Ultimately, it is returned to another general regulation related to crimes, in particular fraud crimes, the Turkish Penal Code ("TPC").

In the context of all these provisions and as the reference is also made to the general provisions on crypto-asset offerings, the offence of collecting money from the public will be analysed and by way of example the first question arises that, while the offence of collecting money from the public which is regulated in the TCC is prosecuted ex officio; the amendment made in 2012 raises the question of whether this offence will be an indictable offence or an offence prosecuted on complaint.

Secondly, in accordance with the provisions of the CML, it is worth analyzing, who will be criminally responsible for the crimes and misdemeanors of improper public offer, unauthorized capital market activity and market abuse actions and the probable conceptual aggregation between these crimes and misdemeanors. It shall be determined by separately considering that the conceptual aggravation types may arise both among the crimes and between the crimes and misdemeanors.

Finally, the reference to general provisions, not directly to the provisions of the CML, is addressed in the Article 35B/ 6 of the CML which provides that "the relations between those who collect money from the public through the sale or distribution of crypto-assets and those who provide funds to them shall be subject to general provisions", and with the joint and several liability introduced with respect to the activities of crypto-asset service providers.

With regard to crimes related to the collecting money from the public, the general - special (lex specialis principle), prior - subsequent (lex posterior principle) legal relations and cross-norm conflicts are another issue to be examined, based on the normative conflict that may arise between the provisions of the CML, TCC and TPC.

The purpose of this study is to examine these relationships that have developed in the circle of the TCC, the CML and the TPC, to identify legal problems and to propose possible solutions. In fact, within the scope of this study, in which many question marks will attempt to clarify many questions be revealed, the crimes and misdemeanors related to the acts of collecting money from the public in the field of capital markets and their relationship to the acts of crypto-asset service providers in collecting money from the public and the crime of collecting money from the public regulated under the TCC will be examined with reference to the general provisions pursuant to Article 35B/6 of the CML and a discussion of the provisions of the TPC that may be relevant.

Keywords: capital market, cyrpto asset offering, collecting money from the public, improperty.

DİJİTAL ZİLYETLİK: DİJİTAL VARLIKLARDA KONTROL KAVRAMI

Rabia ÖZKAN TAŞ*

Özet

Dijital dönüşüm, yürürlükteki hukukta kabul edilen tanımlamalardan farklı mal ve hizmet türlerini de beraberinde getirmiştir. Son yıllarda gerek bir ödeme aracı olarak gerek bir hak veya şeyi temsil ederek gerek de kendi başlarına değerli şeyler olarak dijital varlıkların kullanım yoğunluğu büyük bir ivmeyle artmaktadır. Özünde sayısal verilerin diziliminden müteşekkil dijital varlıklar, fiziksel bir mevcudiyete sahip olmayan soyut varlıklardır. Buna karşın dijital varlıkların fiziksel varlıklarla birçok ortak yönü de bulunmaktadır. Dijital varlıklar da tıpkı fiziksel varlıklar gibi hukuki işlemlere konu olmakta, devredilmekte ve hatta çalınabilmektedir. Dolayısıyla dijital varlıklar ekonomik hacmi giderek büyüyen bir pazar oluşturmakta ve hukuki önemleri gün geçtikçe artmaktadır. Buna karşın dijital varlıkları konu alan işlemler veya bunların sonuçları bakımından mevcut hukukumuzda bir belirlilik bulunmamakta ve bu durum dijital varlıklara ilişkin hukuki güvenliğin sarsılmasına sebep olmaktadır. Bu durumun önüne geçmek ve dijital varlıklar üzerindeki birtakım esaslı hususlara ilişkin belirlilik sağlamak amacıyla UNIDROIT tarafından 2023 yılının Eylül ayında Dijital Varlıklar ve Özel Hukuk hakkında birtakım prensipler (*UNIDROIT Principles on Digital Assets and Private Law*) yayımlanmıştır. UNIDROIT Prensipleri'ne göre dijital varlıklar, kontrole tabi olabilen elektronik kayıtlardır. Bu varlıklar üzerinde münhasır şekilde kullanma, yararlanma ve tasarruf etme ve bu varlıkların kullanılmasından elde edilen faydanın önemli bir kısmından üçüncü kişilerin faydalanmasını engelleme yetkisi olarak tanımlanan kontrol kavramı UNIDROIT Prensipleri açısından kritik öneme sahip bir kavram olarak karşımıza çıkar.

Dijital bir varlık üzerindeki hakimiyetin belirlenmesini ifade eden kontrol kavramı, ilgili Prensipler kapsamında fonksiyonel açıdan zilyetlik benzeri bir olgu olarak ele alınmıştır. Nitekim zilyetlik, bir hukuki durum olarak kendisine sonuç bağlanmış fiili hakimiyeti ifade eder. Bu işlevsel noktadan hareketle UNIDROIT Prensipleri'nde kontrolün de fiziki boyutu eksik olmakla beraber tıpkı zilyetlik gibi kendisine hukuki

* Araştırma Görevlisi, Balıkesir Üniversitesi Medeni Hukuk Anabilim Dalı, ORCID: 0000-0002-6419-8429

sonuçlar bağlanmış bir olgu olduğu kabul edilmiştir. Dijital varlıklar üzerinde ayni etkili bir hakkın tesisi fikrini temel alan UNIDROIT Prensipleri, gerek dijital varlıklar üzerinde böyle bir hakkın iyiniyetli edinimi gerek üçüncü kişilere karşı ileri sürülebilmesi açısından kontrol kavramını esas almaktadır. Bu kapsamda kontrol kavramının, taşınır eşyalar üzerindeki zilyetliğe benzer sonuçlar doğurduğunu belirtmek yanlış olmayacaktır.

UNIDROIT Prensipleri'nde dijital varlıkları alelade elektronik kayıtlardan ayıran ana unsur olarak karşımıza çıkan kontrol kavramının ifade ettiği anlam ve ihtiva ettiği içerik bu çalışmanın ana konusunu oluşturmaktadır. Kontrol kavramı ekseninde hangi elektronik kayıtların dijital varlık kapsamında olduğu ve e-postalar, oyun içi itemler gibi Prensipler kapsamında incelemeye alınmayan dijital varlıklar bakımından kontrolün söz konusu olup olamayacağı değerlendirilecektir. Bunun yanında saklama hizmetleri bakımından hizmet sağlayıcı ve müşterinin kontrollerinin ne yönde ve hangi boyutlarda olduğu tartışılacak ve UNIDROIT Prensipleri çerçevesinde dijital varlıklar üzerinde hak sahipliği ile kontrol sahibi olmak arasında yapılan ayrımın sınırları ve önemi tespit edilmeye çalışılacaktır.

Anahtar Kelimeler: *Dijital Varlık, Zilyetlik, Kontrol, UNIDROIT, Blokzincir*

DIGITAL POSSESSION: THE CONCEPT OF CONTROL IN DIGITAL ASSETS

Abstract

The digital transformation has brought distinctive types of goods and services, different from the current law's recognitions. In recent years, the intensity of digital assets, whether as a means of payment, as a representation of a right or thing, or as valuable things of their own, has been increasing rapidly. Digital assets, essentially a sequence of numeric data, are intangible assets without physical existence. Nevertheless, digital assets have many commonalities with physical assets. Digital assets, like physical assets, can be subject to legal transactions, transferred, and even stolen. Therefore, digital assets constitute a market with a growing economic volume, and their legal importance increases as time passes. However, there is no certainty in our current law regarding the transactions involving digital assets or their consequences, and this situation causes legal insecurity in these transactions, which are based on digital environment. To prevent this ambiguity and to provide certainty regarding certain fundamental aspects of digital assets, UNIDROIT published the UNIDROIT Principles on Digital Assets and Private Law in September 2023. According to the UNIDROIT Principles, digital assets are electronic records that may be subject to control. The concept of control has critical importance in the UNIDROIT Principles, which is defined as the exclusive ability to prevent others from obtaining substantially

all of the benefit from the digital asset, the ability to obtain substantially all of the benefit from the digital asset, and the exclusive ability to transfer these abilities.

The concept of control, which refers to the determination of dominance over a digital asset, has been addressed as a phenomenon functionally similar to possession under the Principles. Possession is a factual matter, and its presence gives rise to legal consequences. Because of the functional similarity, UNIDROIT acknowledges control is a factual situs that has legal outcomes on digital assets without the physical facet of possession. The UNIDROIT Principles aim to establish a right in rem for digital assets. Therefore, the Principles approach the concept of control as a condition of innocent acquisition and assertion against third parties of such a right. In this context, it can be said that the concept of control has similar consequences to the possession of movable property.

The main subject of this study is the meaning and content of the concept of control, which is the main element that distinguishes digital assets from any electronic records in the UNIDROIT Principles. In terms of the concept of control, this study evaluates which electronic records are considered digital assets and whether control is possible for digital assets such as e-mails and in-game items that are not in the scope of the Principles. In addition, this study aims to discuss the direction and extent of the control of the service provider and the customer in custody services. Finally, the limits and importance of distinguishing rights and control over digital assets will be determined within the framework of the UNIDROIT Principles.

Key Words: *Digital Assets, Possession, Control, UNIDROIT, Blockchain*

KRİPTO VARLIK HİZMET SAĞLAYICILARIN PERSONELLERİNİN FİLLERİNDEN SORUMLULUĞU

Uğur KARACA*

Özet

7518 Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun (Kanun) ile kripto varlık piyasasına ilişkin düzenleme yapılmıştır. Söz konusu düzenleme ile kripto varlıklar ve kripto varlık hizmet sağlayıcılar tanımlanmış, kripto varlık hizmet sağlayıcılara ilişkin esaslar belirlenmiş, kripto varlık hizmet sağlayıcıların denetimi ve sorumluluğuna ilişkin hükümler ihdas edilmiştir. Getirilen hükümler arasında şüphesiz en dikkat çekeni Kanun'un 9. maddesi ile Sermaye Piyasası Kanunu(SPK)'na eklenen *"Kripto varlık hizmet sağlayıcıların denetimi ve uygulanacak yaptırımlar"* başlıklı 99/B maddesidir. Söz konusu maddenin 4. fıkrasında kripto varlık hizmet sağlayıcıların; bilişim sistemlerinin işletilmesi, her türlü siber saldırı, bilgi güvenliği ihlalleri gibi fiillerden veya personelin her türlü davranışından kaynaklanan kripto varlık kayıplarından, 6098 sayılı Kanunun 71 inci maddesi kapsamında sorumlu olacağı öngörülmüştür.

Kanun koyucu kripto varlık hizmet sağlayıcılar katı bir sorumluluk rejimine tabi tutmuştur. Nitekim 6098 sayılı Kanunun 71. maddesi Türk Borçlar Kanunu(TBK)'ndaki en ağır sorumluluk türüdür. Öyle ki kripto varlık hizmet sağlayıcılar, personellerinin her türlü fillerinden kaynaklanan kripto varlık kayıplarından tehlike sorumluluğu kapsamında sorumlu olacaktır. Ancak söz konusu düzenleme birtakım soruları da beraberinde getirmiştir. Örneğin söz konusu düzenleme kapsamında her somut olayda tehlike sorumluluğunun şartlarının varlığı değerlendirilecek midir, kripto varlık hizmet sağlayıcılar teknolojinin en yeni ve gelişmiş araçlarından faydalansa dahi yine de bir zarar doğma ihtimali var mıdır, SPK m. 99/B-4'te öngörülen fiiller tipik tehlike olarak değerlendirilebilecek midir? Yine personellerin fillerinin kripto varlık kayıplarının yanı sıra başkaca zararlara neden olması halinde nasıl bir sorumluluk rejimi işletilecektir ve dahası zarar kalemleri arasında böyle bir ayrım yapılması isabetli midir?

* Araştırma Görevlisi, İstanbul Üniversitesi Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku Anabilim Dalı, E-posta: ugur.karaca@istanbul.edu.tr ORCID: 0000-0002-6076-0787

Çalışmamız kapsamında öncelikle TBK m. 71'de düzenlenen genel tehlike sorumluluğunun şartları kısaca açıklanacak, akabinde kripto varlık hizmet sağlayıcıların söz konusu şartları sağlayıp sağlamadığı değerlendirilecektir. Bu kapsamda özellikle kripto varlık hizmet sağlayıcıların personellerinin fillerinin tipik tehlike oluşturup oluşturmadığı üzerinde durulacaktır. Ardından kripto varlık kayıpları dışındaki zararlar bakımından kripto varlık hizmet sağlayıcıların sorumluluğu incelenecektir. Bu bağlamda SPK m. 99/B-4 gereği kripto varlık hizmet sağlayıcıların, personellerinin fillerinin neden olduğu kripto varlık kayıplarından tehlike sorumluluğu kapsamında sorumlu olmasının yerindeliği değerlendirilecektir. Yapılacak değerlendirmelerde SPK m. 99/B-4 düzenlemesi AB Kripto Varlık Piyasaları Tüzüğü (MiCA) ile karşılaştırmalı olarak ele alınacaktır.

Anahtar Kelimeler: Kripto Varlık Kaybı, Kripto Varlık Hizmet Sağlayıcı, Tehlike Sorumluluğu, Tipik Tehlike, 3. Kişilerin Fillerinden Sorumluluk

RESPONSIBILITY OF CRYPTO ASSET SERVICE PROVIDERS FOR THE ACTIONS OF THEIR PERSONNEL

Abstract

Regulation regarding the crypto asset market has been introduced through the Law on the Amendment of the Capital Markets Law No. 7518 (Law). With the said regulation, crypto assets and crypto asset service providers have been defined, principles regarding crypto asset service providers have been established, and provisions related to the supervision and responsibility of crypto asset service providers have been introduced. Undoubtedly, the most notable provision is Article 99/B, titled "Supervision of Crypto Asset Service Providers and Applicable Sanctions", which was added to the Capital Markets Law(CML) through Article 9 of the Law. Paragraph 4 of the aforementioned article stipulates that crypto asset service providers will be held liable, under Article 71 of Law No. 6098, for crypto asset losses arising from the operation of their information systems, any form of cyber-attacks, information security breaches, or any behaviour of their personnel.

The legislator has subjected crypto asset service providers to a strict liability regime. As a matter of fact, Article 71 of the Law No. 6098 is the most severe type of liability in the Turkish Code of Obligations (TCO). As such, crypto asset service providers will be liable for the loss of crypto assets arising from all kinds of actions of their personnel within the scope of hazard liability. However, this regulation has also brought along some questions. For instance, within the scope of the this regulation, will the existence of the conditions of hazard liability be evaluated in each concrete case, even if crypto asset service providers make use of the newest and most advanced tools of technology, is there still a possibility that a damage may arise, can the acts stipulated in Article

99/B-4 of the Capital Markets Law be considered as typical hazards? Similarly, if the actions of personnel cause other damages in addition to crypto asset losses, what kind of liability regime will be applied, and moreover, is it appropriate to make such a distinction between different categories of damages?

Within the scope of our study, we will first briefly explain the conditions of general strict liability as regulated under Article 71 of the TCO, and then assess whether crypto asset service providers meet these conditions. In this context, particular emphasis will be placed on whether the actions of the personnel of crypto asset service providers constitute a typical risk. Subsequently, the liability of crypto asset service providers with respect to damages other than crypto asset losses will be examined. In this context, according to Article 99/B-4 of the CML, the appropriateness of crypto asset service providers being liable for the losses of crypto assets caused by the acts of their personnel within the scope of hazard liability will be evaluated. "In the evaluations to be conducted, the provisions of Article 99/B-4 of the CML will be analysed in comparison with the EU Markets in Crypto-Assets Regulation (MiCA).

Keywords: Crypto Asset Loss, Crypto Asset Service Provider, Hazard Liability, Typical Risk, Liability for the Actions of Third Parties

DÖRDÜNCÜ BÖLÜM:
BİLİŞİMİN KAMU HUKUKUNA YANSIMALARI

TRANSHÜMANİZMİN POPÜLER ÜRÜNLERİNDEN BİRİ OLAN NEURALINK TEKNOLOJİSİNİN İNSAN HAKLARI TEORİSİ BAĞLAMINDA DEĞERLENDİRİLMESİ

Yasin AYDOĞDU*

Özet

İnsanların doğal sınırlarını aşarak fiziksel, zihinsel, psikolojik ve sosyal açıdan bireyi daha güçlü bir seviyeye eriştirmeyi amaçlayan transhümanizm düşüncesinin fikri kökenleri Antik Yunanda Aristoteles'e kadar dayanmakla beraber, günümüzdeki anlamıyla transhümanizmin ortaya çıkışı 20. Yüzyılın ikinci yarısına denk gelmektedir. 1950'li yıllarla beraber bilgisayar, yapay zekâ, robotik ve sentetik biyolojinin gelişimi ile insan vücudundaki bazı eksiklikler ve hastalıklardan kaynaklanan dezavantajlı durumu gidermeye yönelik geliştirilen teknolojik araçlar transhümanizm düşüncesinin bilimsel olarak güçlenmesine hizmet etmiştir. Öyle ki, bu gelişmeler, transhümanistlerin hastalanmayan, yaşlanmayan ve hatta ölümsüz bir insan türü geliştirilebileceğine yönelik inançlarının ütopik olmaktan çıkararak bilimsel zeminde tartışılmasına yol açmıştır.

21. Yüzyılda yapay zekâ başta olmak üzere bilişim teknolojilerindeki hızlı gelişim transhümanizmin bir düşünce ve felsefe olmasından öte geçerek kendine özgü bir endüstri oluşturmasına yol açmıştır. Öyle ki, daha önce bilim kurgu yapımlarında karşımıza çıkan bazı araçlar günümüzde artık belirli teknoloji şirketleri tarafından geliştirilebilmektedir. Bu şirketler arasında son yıllarda yaptığı çalışmalarla adından sıklıkla söz ettiren Neuralink de vardır. Daha önce bir grup nörolog tarafından geliştirilen ancak ABD'li ünlü girişimci ve iş insanı Elon Musk tarafından satın alınmasının ardından dünya genelinde tanınırlığa erişen Neuralink, insan beynine takılan çip şeklinde bir implant ile beyin nöronlarına erişim sağlanarak alzheimer, parkinson, görme bozuklukları, hafıza kaybı gibi hastalıkları iyileştirmek ve hatta omurga yaralanmalarından kaynaklanan kalıcı felci ortadan kaldırmak gibi tedavi

* Dr. Öğretim Üyesi, Eskişehir Osmangazi Üniversitesi Hukuk Fakültesi, ORCID: 0000-0003-3248-5199, e-posta: yasinaydogdu@ogu.edu.tr

amaçlarının yanı sıra bilgisayar ve gelişmiş yapay zekâ teknolojilerinden faydalanarak insan beynini daha ileri seviyeye getirmeyi amaçladığını belirtmektedir. Belirli hayvanlar üzerindeki deneyleri başarıyla tamamlayan Şirket, şu sıralar gönüllü insanlar üzerinde bu teknolojiyi test etmektedir. Bu gelişmeler karşısında endişe duyan ve farklı gerekçelerle karşı çıkan bir kesim bulunmakla beraber, aksine bu ve benzeri çalışmaları destekleyen ve testlerin başarılı sonuçlanmasını heyecanla bekleyen bir kesim daha vardır.

Çalışmada öncelikle transhümanizm düşüncesinin mevcut durumu, savunucularının argümanları ve bu düşünceye yönelik eleştiri ve kaygılara değinilecektir. Ardından transhümanizmin son yıllardaki en popüler araçlarından biri olan Neuralink teknolojisi hakkında bilgiler verilerek, bu teknolojinin mevcut durumu ile yakın gelecekte erişeceği düzey üzerinden insan sağlığına olumlu ve olumsuz etkileri ele alınacaktır. Nihayetinde konunun etik ve sosyolojik yönü üzerinde kısaca durulduktan sonra Neuralink teknolojisinin hak ve özgürlükler ile insan hakları teorisinin temel ilkeleri bağlamında değerlendirmesi yapılacaktır. Değerlendirmede insanın sırf insan olarak doğmasından kaynaklı olarak sahip olduğu hak ve özgürlüklerden hangilerinin bu gelişmelerden ne düzeyde etkileneceği ve insan türü arasında bir ayrımcılığın ortaya çıkıp çıkmayacağı eşitlik ilkesi üzerinden ele alınacaktır.

Anahtar Kelimeler: Transhümanizm, Neuralink, İnsan Hakları Teorisi, Robot, Yapay Zekâ.

EVALUATION OF NEURALINK TECHNOLOGY THAT ONE OF THE POPULAR PRODUCTS OF TRANSHUMANISM IN THE CONTEXT OF HUMAN RIGHTS THEORY

Abstract

Although the intellectual origins of the idea of transhumanism, which aims to achieve a higher physical, mental, psychological and social level by exceeding the natural limits of human, date back to Aristotle in ancient Greece, the emergence of transhumanism in its current sense coincides with the second half of the 20th century. The development of computers, artificial intelligence, robotics and synthetic biology in the 1950s, and the technological tools developed to overcome the disadvantages caused by certain deficiencies and diseases of the human body, have served to strengthen the idea of transhumanism scientifically. In fact, these developments have transformed the transhumanist belief that a human species that does not get sick, does not age, and is even immortal, can be developed from utopian to scientific.

In the 21st century, the rapid development of information technologies, especially artificial intelligence, has meant that transhumanism has gone from being an idea

and a philosophy to becoming an industry in its own. So much so that some of the tools previously seen in science fiction productions can now be developed by certain technology companies. One such company is Neuralink, which has made a name for itself in recent years. Neuralink, which was originally developed by a group of neurologists but gained worldwide recognition after being acquired by the famous US entrepreneur and businessman Elon Musk, says it aims to take the human brain to a more advanced level by using computer and advanced artificial intelligence technologies, as well as treatment purposes such as improving diseases such as Alzheimer's, Parkinson's, visual impairment, memory loss and even eliminating permanent paralysis caused by spinal injuries, by providing access to brain neurons through a chip-shaped implant inserted into the human brain. Having successfully completed experiments on certain animals, the company is now testing the technology on human volunteers. While some people are concerned about these developments and oppose them for various reasons, there is another group of people who support these and similar studies and eagerly await the successful outcome of the tests.

In the study, firstly, the current status of the idea of transhumanism, the arguments of its advocates, and the criticisms and concerns about this idea will be discussed. Then, by providing information on Neuralink technology, one of the most popular tools of transhumanism in recent years, the positive and negative effects of this technology on human health will be discussed through its current status and the level it will reach in the near future. Finally, after a brief discussion of the ethical and sociological aspects of the subject, the Neuralink technology will be evaluated in the context of rights and freedoms and the basic principles of human rights theory. In the evaluation, it will be discussed which of the rights and freedoms that human beings have by virtue of their birth as human beings will be affected by these developments, and to what extent, and whether discrimination between human species will arise through the principle of equality.

Keywords: Transhumanism, Neuralink, Human Rights Theory, Robot, Artificial Intelligence.

METAVERSE PLATFORMLARINDAKİ İŞLEMLERİN VERGİLENDİRİLMESİ PROBLEMİ

Arzu KALYON*, Ayşe Nur YAYLA**

Özet

Metaverse'de sayısız vergilendirebilir işlemlerin vergiye tabi olmadığı ve bunun da vergi adaletini zedelediği düşüncesi son yıllarda tartışılmaya başlanmıştır. Metaverse dünyanın dört bir yanından insanın bir araya gelerek ekonomik ve ticari ilişkilerini sürdürdüğü dijital bir evren olma yolunda ilerlemektedir. Dijital ortamda gerçekleşen ve vergiye tabi olmayan bir çok faaliyetin vergilendirilmesi ve buna ilişkin vergi düzenlemelerin oluşturulması yeni bir "vergi cenneti" yaratılmaması için önemlidir.

Metaverse'de ekonomik anlamda işlemler yapıldığında, gerçek dünyada bir gelir elde edilmektedir. Metaverse'de elde edilen bu gerçek gelirin kime ait olduğunu belirlemek yani öncelikle kimin vergilendirileceğini, sanal dünyanın arkasındaki gerçek veya tüzel kişiyi ortaya çıkarmak gerekecektir. Bu konuda server sağlayıcılarından veya benzer teknolojilerden yararlanılması düşünülebilir. Daha sonra ise, verginin yasallığı ilkesi ve belirlilik ilkesi gereğince, dijital ortamda vergiyi doğuran olayın ve matrahın tanımının yapılması zaruridir.

Ancak, vergilendirme zamanı bakımında ise klasik Gelir Vergisi ve Kurumlar Vergisi Kanunu'nda olduğu gibi bunun beyan esasına göre değil de "anında" vergilendirme sistemi ile yapılması daha etkin bir vergilendirme olacaktır. Ayrıca, kanun koyucu tarafından sanal mülkiyet tanımının da yapılması gerekmektedir.

Dijital ortamda elde edilen gelirin hangi ülkenin vergilendirme yetkisinde olduğunun doğru belirlenmesi de çifte vergilendirme bakımından önem taşımaktadır. Bir diğer önemli konu ise elde edilen gelirin niteliğinin belirlenmesi olacaktır. Örneğin, Dijital ortamda, dijital kodla alım satımı yapılan sanat eserleri, süreklilik unsuru var ise Gelir Vergisi Kanunu'nun 65. Maddesi uyarınca serbest meslek kazancı olarak nitelendirilebilecektir. Ancak, serbest meslek faaliyeti arızi olarak yapılmakta ise, elde edilen gelir serbest meslek kazancı olarak değil, Gelir Vergisi Kanunu 80. Madde diğer kazanç ve iratlar kapsamında değerlendirilecektir.

Vergi düzenlemelerin, dijital dünyadaki gelişmeleri yakalaması ve buna ilişkin çözümler bulması zaruridir. Nitekim, Anayasa'nın 73. Maddesinde de "herkes" in mali gücüne göre vergilendirilmesi öngörülmüştür. Metaverse'de ödeme aracı olarak

* Doktor Öğretim Üyesi, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, https://orcid.org/0000-0001-6289-6189, arzu.kalyon@medeniyet.edu.tr

** Ar. Gör., İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, https://orcid.org/0009-0005-6591-676X, aysenur.yayla@medeniyet.edu.tr

kullanılan kripto paralar, dijital jetonlar vb. vergiyi doğuran olayın takibi için önemlidir. Her ne kadar Metaverse teknolojisinde NFT, kripto para birimleri gibi dijital varlıkların vergilendirilmesi zor olsa da, dijital ortamda yapılan ve kazanç sağlanan işlemlerin vergiye tabi olması için bir an önce çalışmalarımıza başlamamız gerekmektedir.

Anahtar Kelime: Metaverse, vergi, dijital varlık, çifte vergilendirme, vergilendirme yetkisi

THE PROBLEM OF TAXATION OF TRANSACTIONS ON METAVERSE PLATFORMS

Abstract

The tax justice, has started to be discussed in recent years that numerous taxable transactions in the Metaverse are not taxed. Metaverse is on its way to becoming a digital universe where people from all over the world come together and maintain their economic and commercial relations. It is important to tax many non-taxable activities that take place in the digital environment and to establish tax regulations related to this in order not to create a new "tax haven".

When economic transactions are made in the metaverse, an income is obtained in the real world. It will be necessary to determine to whom this real income obtained in the metaverse belongs, that is, first of all, it will be necessary to reveal who will be taxed and the real or legal person behind the virtual world. In this regard, it may be considered to use server providers or similar technologies. Then, in accordance with the principle of legality of tax and the principle of certainty, it is essential to define the event and base that gives rise to the tax in the digital environment.

However, in terms of taxation time, it will be a more effective taxation to do this with an "instant" taxation system, not on a declaration basis, as in the classical Income Tax and Corporate Tax Law. In addition, the definition of virtual property must also be made by the legislator.

It is also important in terms of double taxation to correctly determine which country has the taxation authority of the income obtained in the digital environment. Another important issue will be to determine the nature of the income obtained. For example, works of art traded with digital codes in the digital environment, if there is an element of continuity, are subject to Article 65 of the Income Tax Law. In accordance with the article, it can be qualified as self-employment earnings. However, if the self-employment activity is carried out incidentally, the income obtained is not considered as self-employment income, but as income under Section 80 of the Income Tax Act. The item will be evaluated within the scope of other earnings and revenues.

It is imperative that tax regulations catch up with the developments in the digital world and find solutions for this. As a matter of fact, Article 73 of the Constitution. In the article, it is stipulated that "everyone" will be taxed according to his financial power. Cryptocurrencies, digital tokens, etc., which are used as a means of payment in the metaverse, are important for the follow-up of the event that gives rise to the tax.

Although it is difficult to tax digital assets such as NFTs and cryptocurrencies in Metaverse technology, we need to start working as soon as possible to ensure that transactions made and earned in the digital environment are subject to tax.

Keyword: Metaverse, tax, digital asset, double taxation, taxation jurisdiction

KRİPTOGRAFİ HUKUKU BAĞLAMINDA ÖZEL HAYATIN GİZLİLİĞİ VE NEMO TENATUR İLKESİ

Özgür TAŞDEMİR*

Özet

Bilişim çağında, gündelik toplumsal ilişkilerden, devletlerin yürüttüğü güvenlik hizmetlerine kadar birçok bireysel veya kamusal faaliyet dijital alana taşınmıştır. Nesnelerin interneti, yapay zekâ, beyin makine arayüzü ve gözetim teknolojilerinin gelişimiyle gündelik hayatın daha da fazla dijitalleşeceği, özel veya kamusal verilerin öneminin artacağı açıktır. Bu gelişmeler ışığında kriptografinin de "kişisel veri" kavramı gibi gelecekte hukukçuların gündemlerinden birini oluşturacağını tahmin edebiliriz. Çünkü verilerin gizliliği ve siber güvenlik ancak şifreleme teknolojileri ile sağlanabilmektedir. Bu nedenle, Türkiye'de henüz az sayıda insanın duyduğu kriptografi hukukuna değinmek gerekir. Kriptografi hukuku, şifreleme teknolojilerinin üretim süreçlerini, kimler tarafından, nasıl ve hangi şartlar, sınırlar altında kullanılabileceğini, ithalat ve ihracatını düzenleyen hukuk kurallarını barındıran, kamu hukukunun bir dalıdır. Veri gizliliği ve güvenliğiyle ilişkisi nedeniyle bilişim hukukunun altında değerlendirilebilir.

Kriptografi hukuku, silahlı kuvvetlerce ve gizli servislerce kullanılan şifreleme teknolojilerinin, milli güvenlikle ilgili görülerek, ihracatlarının düzenlenmesiyle doğar. Örneğin, hukuk sistemimizde kriptografiye dair bulabileceğimiz ilk düzenlemeler Wassenaar Düzenlemesine dayanır. Buna karşın bu hukuk alanında karşılaşılabilecek en önemli sorunlar özel kişilerce şifreleme teknolojilerinin kullanımıyla karşımıza çıkar. Bireyler ve devlet arasındaki, mahremiyet ve güvenlik dengesi adalete dayanmalıdır. Suç delillerini karartmak amacıyla şifreleme teknolojilerinden yararlanılabilmekte ve suç örgütleri devlet otoritelerine karşı önemli bir koz kazanmaktadır. Örneğin Çin, özel şahıslarca şifreleme teknolojilerinin kullanımını kısıtlamaktadır. Bir şifrelemenin delil etmek amacıyla kırılamaması durumunda, sanığın şifreleme anahtarını vermesinin gerekip gerekmediği, bunun nemo tenetur ilkesi çerçevesinde meşruiyeti

* Dr. Öğretim Üyesi, Yozgat Bozok Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, (okucuk-tasdemir@gmail.com), Orcid Id: https://orcid.org/0000-0001-5327-1822

başka bir tartışma konusudur. Devletlerin, hangi koşullarda, "arka kapılar" aracılığıyla şifrelenmiş iletişimlere (Örn. WhatsApp) müdahil olabilecekleri, bireylerin hangi sınırlar içinde şifreleme programlarıyla kişisel verilerini koruyabilecekleri, özel hayatın gizliliği çerçevesinde ele alınabilecek bir başka sorundur. Iphone telefonlara erişim sağlanmasıyla ilgili Apple ve FBI arasındaki mahkemeye taşınmış uyuşmazlıklar, tartışma konumuz açısından önemli örneklerdir. Sunumumuzda, kriptografi hukukunun, uluslararası düzenlemeler ve karşılaştırmalı hukuk ışığında incelemesi yapılacak, KVKK ile CMK'nın 134'üncü ve 135'inci maddeleri çerçevesinde Türk hukukundaki yeri değerlendirilecektir.

Anahtar Kelimeler: Kriptografi, Kriptografi Hukuku, Kriptografik Adalet, Özel Hayatın Gizliliği, Nemo Tenatur

IN THE CONTEXT OF CRYPTOGRAPHY LAW: PRIVACY AND THE PRINCIPLE OF NEMO TENETUR

Abstract

In the digital era, numerous aspects of both individual and public activities, ranging from everyday social interactions to state security services, have transitioned into the digital realm. With the advent of the Internet of Things, artificial intelligence, brain-machine interfaces, and surveillance technologies, it is evident that daily life will become increasingly digitized, thereby amplifying the significance of both personal and public data. According to these developments, it is foreseeable that cryptography, much like the concept of "personal data," will become a prominent subject of legal discourse. Because data privacy and cybersecurity can only be safeguarded through encryption technologies. Therefore, it is imperative to address the subject of cryptography law, which remains relatively unfamiliar to many in Turkey. Cryptography law constitutes a branch of public law that encompasses the legal frameworks governing the development, utilization, and regulation of encryption technologies, specifying who may use such technologies, under what conditions, and within what limitations. It also governs the import and export of these technologies. Due to its intrinsic link with data privacy and security, cryptography law may be regarded as a subfield of information technology (IT) law.

The legal imperative for regulating cryptography emerged from the need to control the export of encryption technologies used by military forces and intelligence agencies, as these are considered crucial to national security. For instance, the initial regulations concerning cryptography in our legal system can be traced to the Wassenaar Arrangement. However, the most significant challenges in this area arise in relation to the use of encryption technologies by private individuals. The delicate balance between privacy and security in the relationship between individuals and the

state must be established on principles of justice. Encryption technologies may serve as concealment for criminal evidence and provide considerable leverage for criminal organizations against state authorities. As an illustrative example, China imposes strict limitations on the use of encryption technologies by private individuals.

In cases where encryption cannot be breached for evidentiary purposes, a critical legal question emerges regarding whether judicial authorities, within the framework of the nemo tenetur principle, may compel an accused person to surrender the encryption key. Furthermore, the conditions under which states may intervene in encrypted communications (e.g., WhatsApp) through the implementation of "backdoors" and the extent to which individuals can protect their personal data through encryption programs represent further issues that can be examined within the broader context of the right to privacy. The legal disputes between Apple and the FBI regarding access to iPhone data serve as notable examples that are pertinent to this discussion. This presentation will examine cryptography law within the context of international regulations and comparative legal frameworks, and will assess its standing within Turkish law, particularly in relation to Law on the Protection of Personal Data (KVKK) and Articles 134 and 135 of the Turkish Criminal Procedure Code.

Keywords: Cryptography, Cryptography Law, Cryptographic Justice, Privacy, Nemo Tenatur

BEŞİNCİ BÖLÜM:
BİLİŞİMİN CEZA HUKUKUNA YANSIMALARI

KRİPTO VARLIK HİZMET SAĞLAYICILAR TARAFINDAN İŞLENEN ZİMMET SUÇU

Murat BALCI*

Özet

Merkeziyetsiz bir yapı arz eden blokzincir teknolojisi ve bu teknoloji kullanılarak ortaya çıkarılan kripto varlıklar, günümüzde oldukça yaygınlaşmıştır. Yakın geçmiş zamanda ortaya çıkan bu varlık türü, kanun koyucuların da radarına girmiştir. Bu doğrultuda kripto varlıklara ilişkin yasal düzenleme getiren ülkelerden biri de Türkiye olmuştur. T.C. Merkez Bankası tarafından çıkarılan "Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik" sonrası, ihtiyacın daha da arttığını gören kanun koyucu, 7518 sayılı "Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun" ile bu alana ilişkin özel bir takım kanuni düzenlemeler getirmiştir. Kamuoyunda "Kripto Varlık Yasası" olarak bilenen bu düzenlemede, kripto varlık hizmet sağlayıcıları temel alınmıştır. Kanunda kripto varlık hizmet sağlayıcıları çeşitli açılardan düzenlendikten sonra aynı zamanda "Kripto Varlık Hizmet Sağlayıcılarda Zimmet" başlığı altında yeni bir suç tipi öngörülmüştür.

Çalışmada Sermaye Piyasası Kanunu (SPK) m. 110/A da düzenlenen kripto varlık hizmet sağlayıcılar tarafından işlenen zimmet suçu üzerinde durulacaktır. SPK'nın 110/A maddesi düzenlemesi öncesinde TCK'nın 155'nci maddesinde düzenlenen güveni kötüye kullanma suçu kapsamında değerlendirilebilecek fiiller özel olarak düzenlemeye tabi tutulmuş cezaları da ağırlaştırılmıştır. SPK m. 110/A kapsamında düzenlenen suç tipi, 5411 Sayılı Bankacılık Kanunu'nun 160'ncı maddesinde yer alan hükmü temel almıştır. Hüküm kripto varlık hizmet sağlayıcılara uyarlanarak formüle edilmiştir.

Tebliğde suç tipinde geçen temel kavramlar, suçla korunan hukuki değer, suçun unsurları, suçun özel görünüş şekilleri, etkin pişmanlık ve yaptırım konuları üzerinde durulacak ve detaylı bir değerlendirme yapılacaktır.

Anahtar Kelimeler: Kripto Varlık, Kripto Varlık Hizmet Sağlayıcı, Zimmet Suçu, Bilişim Suçları, Sermaye Piyasası Kanunu.

* Prof. Dr, Polis Akademisi Başkanı, ORCID: 0000-0002-8506-7911.

THE CRIME OF EMBEZZLEMENT COMMITTED BY CRYPTO-ASSET SERVICE PROVIDERS

Abstract

The decentralized blockchain technology and crypto assets created using this technology have become quite widespread today. This type of asset, which has emerged in the recent past, has also entered the radar of lawmakers. Accordingly, Turkey has been one of the countries to introduce legal regulations on crypto assets. After the "Regulation on the Non-Use of Crypto Assets in Payments" issued by the Central Bank of the Republic of Turkey, the legislator, seeing that the need has increased even more, has introduced some special legal regulations in this field with the "Law Amending the Capital Markets Law" numbered 7518. This regulation, publicly known as the "Crypto Asset Law", is based on crypto asset service providers. After regulating crypto asset service providers in various aspects, a new type of crime under the title of "Embezzlement in Crypto Asset Service Providers" has been stipulated in the Law.

This study will focus on the crime of embezzlement committed by crypto asset service providers regulated under Article 110/A of the Capital Markets Law (CMB). Prior to the regulation of Article 110/A of the CMB, the acts that can be considered within the scope of the crime of abuse of trust regulated under Article 155 of the TCC were subject to special regulation and their penalties were aggravated. The type of offense regulated under Article 110/A of the CML is based on the provision of Article 160 of the Banking Law No. 5411. The provision has been formulated by adapting it to crypto asset service providers.

In the present communiqué, the basic concepts of the crime type, the legal value protected by the crime, the elements of the crime, the special forms of appearance of the crime, effective remorse and sanctions will be emphasized and a detailed evaluation will be made.

Keywords: Crypto Asset, Crypto Asset Service Provider, Embezzlement, IT Crimes, Capital Markets Law.

CEZA MUHAKEMESİNDE SEGBİS UYGULAMASINA İLİŞKİN SORUNLAR VE ÇÖZÜM ÖNERİLERİ

Can CANPOLAT*

Özet

23 – 24 Mart 2000'de yapılan Lizbon Zirvesi'nde, AB, on yıllık ekonomik ve politik hedefleri için elektronik dönüşümü temel alan bir plan açıklamıştır. Planda, bilgiye dayalı ekonominin yarattığı değişimi yakalamak için küresel bilgi altyapılarını oluşturmak ve eğitim sistemini modern ihtiyaçlara göre dönüştürmek temel gaye olarak ifade edilmiştir. Türkiye, 2001'de bu planı e-Türkiye adı altında hayata geçirmek için projelendirmeler yapmış, 2006 yılında e-devlet uygulaması hayata geçirilmiştir. E-Türkiye'nin en önemli görünümlerinden biri Ulusal Yargı Ağı Projesi'dir (UYAP). Bu çerçevede Adalet hizmetlerinin aşamalı olarak elektronik ortama taşınması hedeflenerek UYAP'ı hayata geçirmek üzere sorumlu kurum olan Adalet Bakanlığı ile Havelsan A.Ş. arasında protokoller imzalanmıştır. Proje ile Adalet Bakanlığı'na bağlı merkez ve taşra teşkilatlarının tümünde elektronik adalet hizmeti verecek şekilde bir altyapı kurulmuştur.

Bu çerçevede ortaya çıkan adalete erişimin kolaylaştırılması sürecinde, yani E-Devlet ve UYAP'ın ana zeminini oluşturan düşüncenin bir parçası ve aşaması olarak muhakeme safahatında yapılan işlemlerin, imkan bulunduğu ölçüde ses ve görüntü kaydeden cihazlarla tespit edilmesi düşüncesi ön plana çıkmıştır. Böylece kayıtların sonradan incelenerek tereddütlü hususların açıklığa kavuşturulması sağlanabilecek ve daha da önemlisi, denetim muhakemesinde kovuşturmanın kanuna uygun yürütülüp yürütülmediği değerlendirilebilecektir. Bu açıdan CMK'daki hükümler incelendiğinde, Ses ve Görüntü Bilişim Sistemi (SEGBİS) kullanımının takdire bırakıldığı ve zorunlu tutulduğu bazı düzenlemelere yer verildiği görülmektedir.

Tebliğde, CMK'da yer verilen düzenlemeler mucibince kayda alınan muhakeme işlemleri yönünden tatbikatta gündeme gelen meseleler; "CMK m. 219'a göre duruşmanın

* Doçent Doktor, Yalova Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, ORCID: 0000-0002-8729-0359, canpolat@yalova.edu.tr

SEGBİS aracılığıyla kayda alınması halinde, bilirkişi eliyle metne dönüştürülen tutanağın usulüne uygun imza edilmemesi yahut geç imzalanması", "SEGBİS aracılığıyla yapılan tanık dinleme işlemlerinde CMK'nın emredici düzenlemelerinin gözetilmemesi" ve "yargılama safahatındaki hakim değişiklikleri" başlıkları altında, çeşitli ihtimaller de göz önünde bulundurularak değerlendirilmiştir. Tahkik edilen sorunların çözümü için hukuk devleti prensibinin içselleştirilerek bu prensibe uygun yargılama yapılması gerektiği, tatbikatın bu yönde şekillenebilmesi için yargının uygun bir zemine ve iş gücüne kavuşturulması gerektiği vurgulanmıştır. Keza ceza muhakemesine, müdafi veya vekil sıfatıyla katılan avukatların, usul hukukuna hakim olmaları, bu hususlar nazarında savunma yapmalarının önemine işaret edilmiştir.

Anahtar Kelimeler: SEGBİS, savunma hakkı, silahların eşitliği ilkesi, adil yargılanma hakkı, nitelikli usul adaleti.

PROBLEMS AND SOLUTION SUGGESTIONS REGARDING SEGBIS (AUDIO AND VIDEO INFORMATION SYSTEM) IN CRIMINAL PROCEDURE

Abstract

At the Lisbon Summit held on March 23 – 24, 2000, the European Union (EU) announced a ten-year plan focusing on economic and political objectives based on electronic transformation. The plan highlighted the importance of establishing global information infrastructures and transforming educational systems to meet modern needs in order to capture the changes brought about by a knowledge-based economy. In 2001, Turkey initiated efforts to implement this plan under the project known as e-Turkey, and in 2006, the e-Government application was launched. One of the most significant components of e-Turkey is the National Judicial Network Project (UYAP). Within this framework, protocols were signed between the Ministry of Justice and Havelsan A.Ş. to progressively digitize justice services. Through this project, an electronic infrastructure was established to enable the entire central and provincial organizations under the Ministry of Justice to provide digital judicial services.

In the course of this process, the idea of recording procedural stages with audio and video devices has come to the fore as part of the broader goal of facilitating access to justice, which is a foundational element of both e-Government and UYAP. Thus, by examining such records afterward, it becomes possible to clarify any ambiguities, and more importantly, to assess whether the prosecution process was conducted in accordance with legal procedures during appellate reviews.

When examining the provisions of the Turkish Code of Criminal Procedure (CMK), it is evident that the use of SEGBIS is left to discretion in some instances and mandated

in others. In practice, several issues have arisen concerning procedural actions recorded under the provisions of the CMK. These issues have been evaluated under headings such as: “In cases where the hearing is recorded via SEGBİS in accordance with Article 219 of the CMK, the failure or delayed signing of the transcript converted into text by an expert” “Failure to comply with the mandatory provisions of the CMK in witness hearings conducted via SEGBIS” and “Judge changes during the trial process” considering various possibilities.

It has been emphasized that to resolve these issues, judicial processes must be conducted in accordance with the principle of the rule of law, and that the judiciary must be provided with appropriate infrastructure and workforce to ensure this. Furthermore, it has been underlined that lawyers participating in criminal proceedings as defense counsel or legal representatives must be proficient in procedural law and conduct their defense with these considerations in mind.

Key words: The usage of audio and video information system (SEGBIS), right to defense, principle of equality of arms, right to fair trial, procedural justice.

YAPAY ZEKA VE CEZA YARGILAMASI: AB YAPAY ZEKA TÜZÜĞÜ IŞIĞINDA YÜKSEK RİSKLİ SİSTEMLERİN KULLANILMASI

Kenan Evren YAŞAR*

Özet

İnsanlar asırlardır bilgi ile ilişki içindedir. İlk başta insan bilginin ne olduğunu bilmeden tecrübe yoluyla, doğa ile temas ettikçe bilgi edinmeye başladı. İlerleyen zamanlarda bilgi doğa ile sınırlı kalmadı ve doğadan edinilen bilgi insan tarafından soyutlanmaya başlandı. İnsanoğlunun bilgiyi sevmesi de bu aşamadan sonra gerçekleşti. Antik Yunan filozofları bilgilerin peşine düştü, stoacılar soyut bilgiyi tartışılabilir, şüpheli hale getirdi. Tek tanrılı dinler bilgiyi kadir-i mutlak olan ilahi kudrete havale ettiler. Aydınlanma filozofları bilgiyi ilahi bilgi, doğa bilgisi ve beşerî bilgi şeklinde tasnif ettiler ve bu alanlardaki bilgilerin nitelikleri itibariyle birbirinden farklı olduğunu ortaya koydular. Bu ayrım sonrasında beşerî bilgi hızlı bir şekilde gelişme gösterdi, çoğaldı, genişledi. Bilginin konusu dünyayı aşarak uzaya ulaştı. Artık insanoğlu asırlardır uzaktan izlediği, merak ettiği ve bir kısım korkularının kaynağı olan uzayın bilgisini edinmekteydi. Uzayın bilgisi iletişimin hızlanmasının önünü açtı. Uzaya dair bilgiler ile insanoğlu bilgisayar çağına geçişi hızlandırdı. Bilgi iletişimin konusu olmaktaydı. İletişime imkân tanıyan araç ise bilgisayar ve bilgisayarları birbirine bağlayan internet teknolojisi oldu. Bu aşamadan sora bilgi artık bir veriydi ve hiçbir veri kaybolmuyor bilgisayarlar aracılığı ile saklanabiliyor ve istendiği zaman yer değiştirebiliyordu.

Veri haline gelen bilgi artık şüphesiz hukukun konusu olmalıydı. Artık iki bloklu dünyada blokların birbirinden sakladıkları ve birbiriyle yarışta kullandıkları bilgilerden değil herkes hakkında oluşturulan, toplanan ve hatta depolanan yani kaybolması zorlaşan bilgiden söz ediliyordu. Bu bilgilerin toplanmasının ardından tasnif edilmesi ve değerli, kullanılabilir verilere dönüştürülmesi gerekmektedir. Bu ihtiyaç yapay zekanın arkasında yatan asıl nedendir.

Bilginin askeri, siyasi boyutu ve dolayısıyla insan hakları boyutu bulunmaktadır. Biz bu çalışmamızda verinin insan haklarını ilgilendiren yönü ile ilgileneceğiz. Veri

* Dr. Öğr. Üyesi, Yalova Üniversitesi Hukuk Fakültesi, ORCİD: 0000-0001-7839-2321

mademki insana dair o halde öncelikle insan hakları ile ilişkilendirilmesi gerekmektedir. Kişilere ait olan verilerin gelişen teknoloji ile hızlı ve yaygın bir şekilde toplanıp işlenmesi insan haklarının önemli bir konusudur. Avrupa Genel Veri Koruma Tüzüğü bu aşamada devreye girdi ve 6 yıllık bir hazırlık süreci sonrasında kişisel verilerin korunması amacına matuf bir şekilde yürürlüğe girdi. Gelinen son aşamada ise artık verilerin toplanmasının regüle edilmesi de yeterli güvenceyi sağlamamaktadır. Zira yapay zekâ teknolojisi ile toplanan verilerden derin öğrenme yoluyla makineler yeni veriler ve analizler gerçekleştirmeye başladı. Yapay zekâ ile toplanan verilerden yeni veri üretme veya toplanan verilerden insan müdahalesi olmadan sonuçlar çıkarma mümkün hale geldikçe de sorun insan hakları boyutuyla daha tehlikeli hal almaya başladı.

Bu aşamada konu ile ilgili şu sorular güncel sorulardır; (1) Yapay zekanın yeniden ürettiği bilgilerin kaynağındaki bilgiler nasıl korunmalıdır? (2) Yapay zekâ bilgi üretme kapasitesi dolayısıyla hukuki veya cezai sorumluluğun süjesi olabilir mi? (3) Yapay zekânın kendisi verilerin girildiği bir ortamda muhakeme yapabilir mi? (4) Bilgi işleme ve üretme aracı olarak yapay zekanın üretmiş olduğu bilgilerin kullanım alanlarını sınırlandırmak gerekir mi?

Bu ve benzeri sorulara felsefi, özel hukuk ve kamu hukuku alanında cevaplar aranmaktadır. Çalışmamız kapsamında özellikle son soruya cevap bulmaya çalışacağız. Yapay zekanın ürettiği bilgilerin kullanım alanları sınırlandırılabilir mi, sınırlandırılabilirse nasıl? Özel olarak da yapay zekâ tarafından üretilen verilerin ceza muhakemesinde kullanmak mümkün mü? Kullanımın mümkün kılındığı hallerde temel hak ve özgürlüklere müdahale sınırı nasıl belirlenecektir?

Çalışmamız kapsamında bu sorulara "Yapay Zekâ Hakkında Uyumlaştırılmış Kurallar Getiren ve Bazı Birlik Yasama Tasarruflarını Değiştiren (AB) 2024/1689 sayılı Tüzük" çerçevesinde nasıl cevap verildiğini tüzüğün risk temelli anlayışını da izah ederek ele almaktayız.

Çalışmamızın giriş kısmında yapay zeka sistemleri tarihsel olarak anlatılacak, yapay zekanın maddi ceza hukuku ve ceza muhakemesi hukuku ilişkisine değinilecek, yapay zekanın suçun önlenmesi ve suçun tespiti için kullanım yöntemleri ele alınacak, önleyici kolluk ve adli kolluk açısından yapay zeka sistemlerinin kullanımı izah edilecek, AB Yapay Zeka Tüzüğü'nde yer alan risk temelli yaklaşım anlatılacak, tüzük kapsamında kabul edilemez risk, yüksek risk taşıyan yapay zeka sistemlerinin kullanımının sınırları hakkında bilgi verilecektir. Ceza muhakemesinde kullanılabilecek olan yapay zekâ sistemlerinin yüksek riskli olarak kabul edildiği ve hangi şartlar altında kullanılabileceği incelenecektir.

Anahtar Kelimeler: Veri, Yapay Zekâ, Önleyici Kolluk, Adli Kolluk, Risk Temelli Yaklaşım

ARTIFICIAL INTELLIGENCE AND CRIMINAL PROCEDURE: THE USE OF HIGH-RISK SYSTEMS IN LIGHT OF THE EU ARTIFICIAL INTELLIGENCE REGULATION

Abstract

Humankind has been in a relationship with knowledge for centuries. Initially, humans began acquiring knowledge without understanding its essence, primarily through experience and contact with nature. Over time, knowledge expanded beyond nature, and the information derived from nature was abstracted by humans. It was at this stage that humanity began to cherish knowledge. Ancient Greek philosophers pursued knowledge, Stoics rendered abstract knowledge debatable and skeptical, while monotheistic religions attributed knowledge to the omnipotent divine power. Enlightenment philosophers classified knowledge into divine, natural, and human categories, emphasizing the distinct characteristics of each. This differentiation accelerated the development of human knowledge, which grew rapidly in scope and scale. Knowledge transcended the world, extending into space. Humanity began to acquire information about the space it had observed, wondered about, and feared for centuries.

The knowledge of space facilitated advancements in communication. Through space exploration, humanity accelerated the transition to the computer age. Knowledge became a subject of communication, with computers and the internet serving as tools that enabled this communication. At this stage, information became data—data that could be preserved indefinitely and transferred as needed via computers.

Data, as a form of information, undoubtedly became a matter of law. No longer limited to classified, competitive information in a bipolar world, data began to refer to information collected, stored, and categorized about everyone—data that was increasingly difficult to lose. Following collection, this data required classification and transformation into valuable, actionable insights. This necessity underpins the development of artificial intelligence (AI).

Knowledge inherently possesses military, political, and human rights dimensions. This study focuses on the intersection of data and human rights. If data pertains to individuals, it must first and foremost be linked to human rights. The rapid and widespread collection and processing of personal data by emerging technologies represent a significant human rights issue. The General Data Protection Regulation (GDPR) addressed this concern, coming into force after six years of preparation to ensure the protection of personal data. However, regulating data collection alone no longer provides adequate safeguards. With AI technologies, machines began generating new data and analyses through deep learning from collected data. As AI systems increasingly produce new information or derive conclusions from data without human intervention, the human rights implications become increasingly perilous.

At this stage, several pressing questions arise:

- How can the source information from which AI generates new data be protected?
- Can AI, given its capacity to produce information, be considered a subject of legal or criminal liability?
- Can AI engage in reasoning within environments where data is entered?
- Should the areas of application for information generated by AI as a tool for data processing and production be restricted?

Philosophical, private law, and public law domains seek answers to these and similar questions. This study particularly examines the final question: Can the use of information generated by AI be restricted, and if so, how? Specifically, can data produced by AI be utilized in criminal procedures? If permitted, how will the boundaries of intervention in fundamental rights and freedoms be delineated?

This study explores how these questions are addressed within the framework of Regulation (EU) 2024/1689, titled "Harmonized Rules on Artificial Intelligence and Amending Certain Union Legislative Acts." It elucidates the regulation's risk-based approach and examines the boundaries of unacceptable and high-risk AI systems outlined therein.

In the introduction, the study provides a historical overview of AI systems, discusses the relationship between AI and substantive and procedural criminal law, and explores the use of AI for crime prevention and detection. It explains the application of AI systems in preventive and judicial policing. The study delves into the risk-based approach of the EU AI Regulation, detailing the limits on unacceptable and high-risk AI systems under the regulation. Lastly, it analyzes high-risk AI systems deemed suitable for use in criminal procedures and the conditions under which they may be employed.

Keywords: Data, Artificial Intelligence, Preventive Policing, Judicial Policing, Risk-Based Approach

ÖNLEYİCİ KOLLUK FAALİYETİ OLARAK TAHMİNE DAYALI POLİSLİK (PREDICTIVE POLICING-PREDPOL) UYGULAMASI ve CEZA HUKUKU İLKELERİ BAĞLAMINDA KABUL EDİLEBİLİRLİK SORUNU

Derya TEKİN*, Veysel TOPUZ**

Özet

Tahmine dayalı (öngörücü) kolluk uygulamaları, suç işleme potansiyeli taşıyan bireylerin suç şüphesi oluşturabilecek davranışlarının ya da suç işleme niyetlerinin analitik yöntemlerle tahmin edilerek suç işlenebilirliği hakkında önceden bilgi sağlamayı amaçlayan bir kolluk faaliyetidir. *PredPol* olarak adlandırılan tahmine dayalı polislik uygulaması bundan yıllar önce 2002 yapımı Azınlık Raporu (*Minority Report*) filminde etkileyici bir şekilde sergilenmiştir. Filmde, psişik yeteneklere sahip kâhinler ve çeşitli teknolojik cihazlar aracılığıyla cinayetler daha işlenmeden önce kolluk güçlerinin müdahalesiyle önlenmeye çalışılmaktadır. 2000'li yılların başlarında bu fikirler bilim kurgu olarak algılansa da, günümüzde yapay zekâ teknolojisindeki ilerlemeler, tahmine dayalı polisliğin şu anki durumu ve gelecekte ne seviyelere ulaşabileceği konusunda bize bazı ipuçları sunmaktadır. Yapay zekâ tabanlı öngörücü kolluk uygulamaları, geleneksel önleyici yöntemlerin ötesinde, büyük veri ve öğretilmiş veri kaynakları kullanarak geliştirilmiş algoritmalarla çalışan sistemleri ifade eder. Bu sistemler, makine öğrenimi ve derin öğrenme teknikleriyle, suçların meydana geleceği yer ve zamanları, suç mağduru olma olasılığı en yüksek bireyler ya da demografik grupları tahmin edebilir. Ayrıca suç potansiyeli ve riskini matematiksel ve istatistiksel yöntemlerle belirleyerek, genel suç potansiyelini analiz etmenin yanı sıra, belirli bireylerin suç işleme riskini de hesaplama imkânı sunar.

Suçlulukla mücadelede suçluların cezalandırılmasının yanı sıra, suçların henüz işlenmeden önlenmesi büyük önem taşımaktadır. Önleyici mekanizmalarla henüz işlenmeden suçların önlenmesi kamunun büyük faydasına olacaktır. Ceza muhakemesi, suç işlendikten sonra devreye giren adli bir süreçken, suçun önlenmesine yönelik faaliyetler idari bir nitelik taşır. Bu bağlamda, suçun önlenmesi ile ilgili görev ve sorumluluk idareye aittir. Ceza hukuku araçlarıyla suçla mücadele ise, suçun işlenmeye başlamasıyla mümkün olur. Önceki aşama hazırlık evresi olarak adlandırılır ve ceza

* Dr. Öğretim Üyesi, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku ABD. ORCID: https://orcid.org/0000-0001-9877-8336

** Arş. Gör., İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku ABD. ORCID: https://orcid.org/0000-0001-9877-8336

hukukunda hazırlık hareketleri genellikle cezalandırılmadığı için, uygun eylemlerle doğrudan icra edilmediği sürece bir kişinin cezalandırılması mümkün değildir. Türk hukuku bakımından da bir eylemin ceza hukuku sorumluluğunu doğurması TCK m. 35 bağlamında doğrudan doğruya icraya başlama ölçütüne bağlanmıştır. Benzer şekilde CMK m. 160 gereğince Cumhuriyet savcısı tarafından soruşturmaya başlanabilmesi için bir suçun işlendiği izlenimi veren bir halin ya da en azından bir emarenin mevcut olması gerekir. Bununla birlikte, günümüzde suçla etkin mücadele edilebilmesi için bazı durumlarda daha da erken müdahaleye ihtiyaç olduğu da bir gerçektir. İşte tahmine dayalı polislik uygulaması tam da bu noktada devreye girmekle birlikte, bu uygulama pek çok tartışmayı da beraberinde getirmektedir. Suçun işlenmesinin önlenmesi suretiyle kamu düzeninin sağlanmasına ilişkin menfaat ile temel hak ve hürriyetlerin (özel hayatın gizliliği, masumiyet karinesi, lekelenmeme hakkı gibi) korunması çatışan en temel iki menfaattir. Bu çalışmada, tahmine dayalı polislik uygulamasının Türk kolluk uygulamasında kullanıldığı bir varsayımda, bu menfaatlerin nasıl etkileneceği ve Türk ceza muhakemesi hukuku bakımından hangi olası sorunlarla karşılaşılabileceği ortaya konulacaktır.

Konunun, ayrıca AB Yapay Zeka Tüzüğü bağlamında da değerlendirilmeye elverişli olduğu söylenebilir. Avrupa Komisyonu tarafından 21 Nisan 2021 tarihinde sunulan ve Yapay Zeka (YZ) sistemlerinin piyasaya arzı, hizmete sunulması ve bazı uygulamaların yasaklanmasına dair kuralları belirleyen "Yapay Zeka Hakkında Uyumlaştırılmış Kurallar Getiren ve Bazı Birlik Yasama Tasarruflarını Değiştiren (AB) 2024/1689 sayılı Tüzük", 12 Temmuz 2024 tarihinde AB Resmi Gazetesi'nde yayımlanmıştır. Bu tüzüğün ikinci bölümü "yasaklanan yapay zekâ uygulamaları" başlığını taşımaktadır. Tüzüğün 5. maddesinin 1-d alt bendine göre gerçek bir kişinin suç işleme riskini değerlendirmek veya tahmin etmek amacıyla gerçek kişilerin risk değerlendirmelerini yapmak için bir YZ sisteminin piyasaya sürülmesi, bu özel amaç için hizmete sunulması veya kullanılması yasaktır. Çalışmada söz konusu bu düzenleme de değerlendirmeye tabi tutulacaktır.

Anahtar Kelimeler: yapay zekâ, tahmine dayalı polislik, öngörücü polislik, hazırlık hareketleri, önleyici kolluk

PREDICTIVE POLICING (PRED-POL) PRACTICE AS PREVENTIVE POLICE ACTIVITY and THE PROBLEM OF ACCEPTABILITY IN THE CONTEXT OF THE PRINCIPLES OF CRIMINAL LAW

Abstract

Predictive policing is a law enforcement activity that aims to provide advance information about the likelihood of crime by analytically predicting the criminal

behavior or criminal intentions of individuals with the potential to commit crimes. Predictive policing, referred to as PredPol, was impressively demonstrated years ago in the 2002 movie Minority Report. In the movie, psychically gifted clairvoyants and various technological devices are used to prevent murders before they are committed through the intervention of law enforcement. Although these ideas were perceived as science fiction in the early 2000s, today, advances in artificial intelligence technology offer us some clues about the current state of predictive policing and the levels it can reach in the future. Artificial intelligence-based predictive law enforcement applications refer to systems that go beyond traditional preventive methods and work with algorithms developed using big data and taught data sources. With machine learning and deep learning techniques, these systems can predict the times and places where crimes will occur, and the individuals or demographic groups most likely to be victims of crime. In addition, by determining the crime potential and risk with mathematical and statistical methods, it offers the opportunity to analyze the general crime potential as well as calculate the risk of certain individuals committing crimes.

In addition to punishing criminals in the fight against crime, it is of great importance to prevent crimes before they are committed. Preventing crimes before they are committed through preventive mechanisms will be of great benefit to the public. While criminal procedure is a judicial process that comes into play after a crime has been committed, activities aimed at crime prevention are administrative in nature. In this context, the duty and responsibility for crime prevention belongs to the administration. The fight against crime with the tools of criminal law is possible only after the crime has been committed. The previous stage is called the preparatory stage, and since preparatory acts are generally not punishable in criminal law, it is not possible to punish a person unless they are directly executed with appropriate actions. In terms of Turkish law, the criminal liability of an act is subject to the criterion of direct execution in the context of Article 35 of the TCC. Similarly, pursuant to Article 160 of the Criminal Procedure Code, in order for the public prosecutor to initiate an investigation, there must be a situation or at least an indication that gives the impression that a crime has been committed. However, it is also a fact that today, in order to fight crime effectively, there is a need for even earlier intervention in some cases. This is precisely where the practice of predictive policing comes into play, but this practice brings with it many controversies. The interest of maintaining public order by preventing the commission of crime and the protection of fundamental rights and freedoms (such as the right to privacy, the presumption of innocence, the right not to be stained) are two of the most fundamental conflicting interests. This study will reveal how these interests will be affected and what possible problems may be encountered in terms of Turkish criminal procedure law in a hypothetical situation where predictive policing is used in Turkish law enforcement practice.

It can be said that the issue is also suitable to be evaluated in the context of the EU Artificial Intelligence Regulation. The "Regulation (EU) No 2024/1689 Introducing Harmonized Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (EU) 2024/1689", which was submitted by the European Commission on 21 April

2021 and sets out the rules on the placing of Artificial Intelligence (AI) systems on the market, putting them into service and prohibiting certain applications, was published in the Official Journal of the EU on 12 July 2024. The second part of this regulation is entitled “prohibited artificial intelligence applications”. According to subparagraph 1-d of Article 5 of the Regulation, it is prohibited to place an AI system on the market, make it available for this specific purpose or use it to carry out risk assessments of natural persons in order to assess or predict the risk of a natural person committing a crime. This regulation will also be evaluated in this study.

Keywords: artificial intelligence, predictive policing, smart policing, preparatory actions, preventive law enforcement

ALTINCI BÖLÜM:
BİLİŞİMİN FİKRİ MÜLKİYET HUKUKUNA YANSIMALARI

YAPAY ZEKANIN TELİF HAKLARI İLE İMTİHANI

Cahit SULUK*

Özet

Pek çok yönüyle insanı ikame etmek üzere tasarlanan yapay zekanın belki de en büyük imtihanı telif haklarıdır. Üretken yapay zekanın telif haklarıyla temasında temelde üç boyut vardır:

i) Yapay zekanın eğitimi (training): Bu işlem yürütülürken telife tabi içerik çoğaltma ve çıkarmaya (extraction) tabi tutulmakta ve işlemi yapan telif suçlamasına muhatap olmaktadır.

ii) Yapay zeka üretimine insanın katkısı (input): Yapay zekanın geliştirdiği ürünler üzerinde insanın eser sahipliğinin bulunup bulunmadığı sorunu çıkmaktadır.

iii) Yapay zeka ürünleri (output): Yapay zekanın geliştirdiği ürünler, başkalarına ait telife tabi fikri ürünlerle benzeştiğinde telif ihlali gündeme gelmektedir. Bu ürünlerin hukuken korunup korunmayacağı ise ayrı bir gündem maddesidir.

Bilebildiğimiz kadarıyla bugüne kadar dünya genelinde yapay zeka / telif kesişimi pozitif düzenlemelere konu olmamıştır. Bu tespitimiz Avrupa Birliğinde yeni kabul edilen Yapay Zeka Kanunu (AIA) için de geçerlidir. Ancak bir yandan literatürde yoğun bir hukuk işçiliği yapılırken diğer yandan daha şimdiden bu konuda pek çok telif davası açılmış, her geçen gün de yenileri açılmaktadır.

Tebliğde yukarıda zikredilen sorunlar hem mevcut hukuki rejim *(de lege lata)* hem de olması gereken hukuk *(de lege ferenda)* boyutlarıyla ele alınacaktır. Özellikle de yapay zekanın geliştirdiği ürünlerin telife tabi olup olmayacağı, eğer olacaksa hak sahibinin kim olacağı gibi oldukça tartışmalı hususlar irdelenecektir.

Anahtar Kelimeler: Yapay Zeka, Üretken Yapay Zeka, Yapay Zeka Ürünleri, Telif Hakları, Yapay Zekanın Gerçekleştirdiği Telif İhlali.

* Doç. Dr., İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, Fikri Mülkiyet Hukuku Anabilim Dalı Öğretim Üyesi, ORCID: 0000-0002-8952-9247, suluk@suluk.com.tr,

TESTING ARTIFICIAL INTELLIGENCE WITH COPYRIGHTS

Abstract

Perhaps the biggest challenge of artificial intelligence, which is designed to replace humans in many aspects, is copyright. Generative AI's involvement in copyright essentially has three dimensions:

i) Training of artificial intelligence *(training):* While this process is carried out, copyrighted content is subjected to duplication and extraction and the person who performs the process will be accused of copyright infringement.

ii) Human contribution to the production of artificial intelligence *(input):* The problem arises whether there is human ownership of the products/works developed by artificial intelligence.

iii) Artificial intelligence products *(output):* When the products developed by artificial intelligence are similar to copyrighted intellectual products belonging to others, copyright infringement comes to the fore. Whether these products will be legally protected is a separate agenda item.

As far as we know, the artificial intelligence / copyright intersection has not been subject to positive regulations worldwide to date. This finding is also valid for the Artificial Intelligence Law (AIA) newly adopted in the European Union. However, while there is intense legal work being done in the literature, many copyright cases have already been filed on this issue, and new ones are added every day.

In the paper, the problems mentioned above will be discussed in terms of both the current legal regime *(de lege lata)* and the law that should exist *(de lege ferenda)*. In particular, highly controversial issues such as whether the products developed by artificial intelligence will be subject to copyright and, if so, who will be the rightful owner, will be examined.

Keywords: Artificial Intelligence, Generative Artificial Intelligence, Artificial Intelligence Products, Copyrights, Copyright Infringement by Artificial Intelligence.

BİLGİSAYAR PROGRAMLARINDA TERSİNE MÜHENDİSLİK PATENT VE TELİF HUKUKU AÇISINDAN DEĞERLENDİRME

Pelin KARAASLAN*

Özet

Bu tebliğde, tersine mühendislik kavramı ve bilgisayar programlarındaki uygulamaları, patent ve telif hukuku boyutuyla ele alınacaktır. Tersine mühendislik, bir ürünün, sistemin veya cihazın mevcut halinden yola çıkarak, onun nasıl çalıştığını, hangi bileşenlerden oluştuğunu ve tasarımını anlamak amacıyla yapılan bir analiz sürecidir. Yazılım sektörü özelinde ise tersine mühendislik, bir yazılımın işleyişini anlamak ve analiz etmek amacıyla mevcut kodun veya yazılım yapısının geri çözümlenmesi işlemlerini ifade eder. Bu süreç, bir yazılımın derlenmiş halinden, kaynak koduna veya kaynak koda yakın bir formata geri dönüştürülmesi (dekompilasyon), kodun analiz edilmesi, algoritmaları ve veri yapılarını çözümleme gibi işlemleri kapsar. Bu uygulama, yazılımın işlevlerini, algoritmalarını ve veri yapısını anlamak, güvenlik açıklarını tespit etmek, hata ayıklamak, birlikte çalışabilirliği sağlamak, lisans ihlallerini tespit etmek veya eski yazılımların bakımını yapmak gibi çeşitli amaçlarla kullanılabilir. Ancak tersine mühendislik uygulamasının bilgisayar programları üzerinde hak sahibi olmayan üçüncü kişilerce gerçekleştirilmesi, fikri mülkiyet hukuku alanında bazı problemlere yol açabilir.

Bilgisayar programları, FSEK kapsamında "eser" olarak korunan fikri ürünlerdir (FSEK m. 2/1). Bu kapsamda eseri çoğaltma ve işleme gibi haklar münhasıran eser sahibine aittir (FSEK m. 21 vd.). Bilgisayar programının tersine mühendislik yoluyla analiz edilmesi, özellikle de dekompilasyon işlemleri, bu hakların ihlal edilmesi riskini taşır. Zira dekompilasyon işlemi, münhasıran eser sahibinin yetkisinde olan kodun çoğaltılması ve kod formunun çevirisi fiillerinin gerçekleştirilmesini gerektirir. Bununla birlikte FSEK, bilgisayar programları üzerindeki tersine mühendislik faaliyetlerine üçüncü kişiler açısından sınırlı bir serbesti tanır. FSEK m. 38/6, ara işlerlik sağlamak amacıyla sınırlı kalmak üzere, dekompilasyon işlemini serbest bırakır.

* Doç. Dr., Eskişehir Osmangazi Üniversitesi Hukuk Fakültesi Fikri Mülkiyet Hukuku Anabilim Dalı, pgkaraaslan@gmail.com; ORCID: 0000-0001-5695-192X.

Bilgisayar programlarına yönelik tersine mühendislik işlemi, patent hukuku açısından da önem arz eden bir konudur. Esasen bilgisayar programları, hukukumuzda "buluş" kavramı dışında tutularak patentlenemeyecek yaratımlar arasında gösterilmiştir (SMK m. 82/2-c). Bununla birlikte Türk ve AB Hukukunda artan bir eğilimle, bilgisayar programlarının buluş sayılmayacağı prensibinin mutlak olarak kabul edilemeyeceği, bilgisayar programlarının teknik karakter gösterme ihtimali zayıf olduğundan bu tutumun sergilendiği, buna karşın gelişen teknoloji ile birlikte bu karaktere sahip bilgisayar programlarının ortaya çıktığından söz etmenin mümkün olduğu ve bunu sağlayan bilgisayar programlarının patentlenmesi gerektiği kabul edilmektedir. Bu bağlamda, TÜRKPATENT tarafından da benimsenerek kabul gören genel görüş, bilgisayar programının patentlenebilmesi için "ileri teknik etki" göstermesi gerektiğidir. Bu şekilde elde edilebilecek olan patent hakkı da sahibine münhasır kullanım yetkileri sağlamaktadır. Bu yetkilere getirilen sınırlandırmalardan biri olan "deneme serbestisi", patentli bilgisayar programları açısından önem taşımaktadır. Zira "deneme serbestisi" ilkesi çerçevesinde, patentli bir buluş üzerinde araştırma ve geliştirme amacıyla yapılan çalışmalar, patent hakkı sahibinin izni olmadan gerçekleştirilebilir. Yazılım patentleri bakımından bu düzenleme, yazılım geliştirme ve iyileştirme amacıyla üçüncü kişilere ait patentli yazılımlar üzerinde tersine mühendislik yapılmasına olanak tanır.

Bu tebliğde öncelikle, FSEK'te öngörülen dekompilasyon serbestisi ile patent hukukunda öngörülen deneme serbestisi kapsam ve koşulları bakımından incelenecek, ardından tarafımızca çelişkili bulunan bir duruma değinilecektir. Şöyle ki, patent hukukunda düzenlenen deneme serbestisi, FSEK'e kıyasla, tersine mühendislik için daha geniş bir serbestlik tanımaktadır ve bu da farklı fikri mülkiyet koruma türleri arasında bir denge sorunu doğurmaktadır. Salt telif hakkıyla korunabilecek yazılımlara göre daha ileri teknik etki gösteren patentli yazılımların daha geniş bir serbestiye tabi tutulması, fikri mülkiyet hukukunda çözüm bekleyen bir sorun olarak öne çıkmaktadır.

Anahtar Kelimeler: bilgisayar programı, patent, telif, dekompilasyon, deneme serbestisi

REVERSE ENGINEERING IN COMPUTER PROGRAMS: AN EVALUATION FROM THE PERSPECTIVES OF PATENT AND COPYRIGHT LAW

Abstract

This paper explores the concept of reverse engineering and its application to computer programs from the perspectives of patent and copyright law. Reverse engineering involves analyzing a product, system, or device to understand its functionality, components, and design by deconstructing its current form. In the software sector, reverse engineering refers to the process of deconstructing existing code or software

structures to analyze a program's functionality. This includes converting compiled software back into source code or a source-code-like format (decompilation), analyzing the code, and deciphering algorithms and data structures. Such activities are employed for understanding software functions, identifying security vulnerabilities, debugging, ensuring interoperability, detecting license violations, or maintaining legacy software. However, reverse engineering by third parties who do not own the rights to the software can create legal issues under intellectual property law.

Computer programs are protected as "works" under the Law on Intellectual and Artistic Works (FSEK). Rights such as reproduction, adaptation, and distribution are exclusively reserved for the copyright holder (Arts. 21 et seq. of FSEK). Reverse engineering, particularly decompilation, carries the risk of infringing these rights since it involves acts like reproducing the code and translating its form—rights that belong solely to the copyright owner. Nevertheless, FSEK provides limited exceptions for reverse engineering activities for interoperability purposes only. Specifically, Article 38/6 of FSEK allows decompilation solely to achieve interoperability between independently created programs, provided certain conditions are met.

Reverse engineering of computer programs also holds significance in patent law. Generally, computer programs are excluded from the definition of "invention" and considered unpatentable under Turkish law (Art. 82/2-c of the Industrial Property Code - SMK). However, there is a growing recognition in Turkish and EU law that this exclusion should not be absolute. It is acknowledged that, with technological advancements, computer programs exhibiting a technical character may emerge and should be eligible for patent protection. The general consensus, also adopted by the Turkish Patent and Trademark Office (TÜRKPATENT), is that a computer program must demonstrate an "advanced technical effect" to be patentable. A patent grants exclusive rights to its holder, but the "experimental use exception" limits these rights. Under this exception, research and development on a patented invention can be conducted without the patent holder's consent. For software patents, this allows reverse engineering on patented software by third parties for development and improvement purposes.

This paper will compare the scope and conditions of the decompilation exception under FSEK and the experimental use exception under patent law. It argues that the experimental use exception in patent law provides a broader allowance for reverse engineering than FSEK, highlighting a balance problem between different types of intellectual property protection. This discrepancy raises an unresolved issue in intellectual property law: the broader freedom granted to patented software, which demonstrates a higher technical effect, compared to software that could be protected solely by copyright.

Keywords: computer program, patent, copyright, decompilation, experimental use exception

DİJİTAL VİDEO OYUNLARININ ESER NİTELİĞİ ÜZERİNE BİR DEĞERLENDİRME

Esra KARATAŞ*

Özet

Gün geçtikçe talebi artan ve pazar payı genişleyen dijital video oyunları günümüzde çocukların olduğu kadar yetişkinlerin de vazgeçilmez eğlence aracıdır. Peki severek ve eğlenerek oynadığımız dijital video oyunları eser midir ve Fikir ve Sanat Eserleri Kanunu kapsamında koruma sağlanabilir mi? Bunun için öncelikle dijital video oyunlarının ve eserin unsurlarını irdelememiz gerekmektedir.

Eser kavramının tanımını ne kanun koyucu ne de telif haklarına ilişkin ilk uluslararası nitelikteki sözleşme olan Bern Sözleşmesi yapmıştır. Kanun koyucu eserin ayırdına varmamızı sağlayacak olan unsurları saymış ve sınırlı sayıda olacak şekilde eser kategorilerini belirlemiştir. Kanuna göre sahibinin hususiyetini taşıyan ve kanunda sayılan eser kategorilerinden birine dâhil olan her nevi fikri ürünler eserdir. Ayrıca fikri ürünün maddi şey üzerinde somutlaşmış olması da gerekmektedir. Dijital video oyunları genellikle bilgisayar, telefon, tablet gibi teknolojik ürünlerin üzerinde bilgisayar programı olarak somutlaşmakta ve gerçek kişinin fikri çabası sonucu meydana gelmektedir. Ancak dijital video oyunları sadece bilgisayar programı olarak nitelenemez. Kullanıcı ile oyun arasındaki etkileşimi arttıran görsel ve işitsel unsurlarla ve senaryo ile diyaloglarla bezeli teknik unsurlardan oluşmaktadır. Burada dijital video oyunlarının eser olarak nitelendirilebilmesi için sınırlı sayıda sayılan eser kategorilerinden birine dahil olup olmadığı sorunu karşımıza çıkmaktadır.

Bu hususta doktrinde farklı görüşler bulunmaktadır. Dijital video oyununun temelinde bilgisayar programının yer alması sebebiyle ilim ve edebiyat eseri olduğunu ileri sürenler olduğu gibi görsel ve işitsel unsurlar içermesi nedeniyle güzel sanat eseri veya sinema eseri olarak niteleyenler de bulunmaktadır. Bir görüşe göre ise dijital video oyunları multimedya eser olarak da nitelenmektedir. Kanunumuzda sadece dört eser kategorisi- ilim ve edebiyat eseri, musiki eseri, sinema eseri ve güzel sanat eseri- bulunduğu ve multimedya eseri adı altında bir kategoriye yer verilmediği göz

* Arş. Gör., Kocaeli Üniversitesi Hukuk Fakültesi, Medeni Hukuk Anabilim Dalı, E-posta: esra.karatas@kocaeli.edu.tr, ORCID Numarası: 0000-0002-8657-6718.

önüne alındığında ancak yeni bir düzenleme ile multimedya ürünleri için ayrı bir eser kategorisinin oluşturulması gerektiği de belirtilmiştir.

Burada dikkat edilmesi gereken husus dijital video oyunlarının hususiyet yönünden eser niteliğini haiz olup olmadığıdır. Multimedya eseri kapsamında da değerlendirilen dijital video oyunları için ayrı bir kategori oluşturulmasına gerek yoktur. Her somut oyun kapsamında hususiyet içeren unsurlar dahil olduğu eser kategorisinde korunabilir. Bu çalışmamızda doktrinde yer alan görüşler ışığında dijital video oyunlarının hangi eser kategorisinde değerlendirilebileceği ile multimedya eserler hakkındaki farklı görüşler irdelenecektir.

Anahtar Kelimeler: Dijital Video Oyunu, Eser, Bilgisayar Programı, Hususiyet, Multimedya Eserler.

AN EVALUATION OF THE WORK QUALIFICATION OF DIGITAL VIDEO GAMES

Abstract

Digital video games, which are increasingly in demand and expanding their market share, have become an essential source of entertainment for children and adults. So, are the digital video games we enjoy and play for fun considered works of art, and can they be protected under the Law on Intellectual and Artistic Works? To address this, we must first examine the elements of digital video games and their works.

Neither the legislator nor the first international treaty on copyright, the Berne Convention, has defined the concept of a work. The legislator has listed the elements that allow us to recognize work and has defined categories of works in a limited manner. According to our law, any intellectual product that possesses the originality of its owner and falls into one of the categories specified by law is considered a work. It is also required that the intellectual product is embodied in a tangible form. Digital video games generally materialize as computer programs on technological products such as computers, phones, and tablets, and they are created as a result of an individual's intellectual effort. However, digital video games cannot be classified solely as computer programs. They consist of technical elements enriched with visual and auditory components, as well as narratives and dialogues that enhance interaction between the user and the game. This raises the question of whether digital video games can be classified as works, specifically whether they fall into one of the limited categories of works defined by law.

In this regard, there are differing views in the literature. Some argue that digital video games are considered literary and artistic works due to their foundation in computer programming, while others classify them as fine arts or cinematic works

because they contain visual and auditory elements. According to one opinion, digital video games can also be classified as multimedia works. Given that our law recognizes only four categories of works—literary and artistic works, musical works, cinematic works, and fine arts—and does not include a category for multimedia works, it has been suggested that a new regulation is necessary to create a separate category for multimedia products.

The key point to consider is whether digital video games possess the originality of a work. If they are evaluated within the framework of multimedia works, there may not be a need to establish a separate category for them. Every specific game can be protected within the category of works that includes its originality elements. In this study, we will explore the views in the literature regarding which category digital video games can be evaluated under, as well as the differing opinions on multimedia works.

Keywords: Digital Video Game, Work, Computer Program, Originality, Multimedia Works.

AÇIK KAYNAK KODLU VE ÖZGÜR YAZILIM (FOSS) SÖZLEŞMELERİNİN FİKRİ MÜLKİYET HUKUKU BAKIMINDAN DEĞERLENDİRİLMESİ

Vildan GÜLSEV*

Özet

FOSS (Free and Open Source Software) yazılımları günümüzde birçok kişi ve ticari şirket tarafından herhangi bir ücret ödemeksizin ve kamuya açık platformlardan erişilerek kullanılabilen yazılım türleridir. Ayrıca, bu yazılımlarda kaynak koduna ulaşılması serbest olduğundan yazılım üzerinde değişiklik yapılması ve geliştirilerek üçüncü kişilere lisanslanması da mümkündür. FOSS yazılım örnekleri olarak en yaygın kullanılan GPL (General Public License), Apache License, MIT Licence, Berkeley License, yazılım lisansları verilebilir. FOSS lisanslarında amaç, yazılımların birçok kişi tarafından geliştirilmesini sağlamak ve yazılımların geliştirilmesinin teşvik edilmesidir. Bunun için FOSS sağlayıcıları, kamuya ücretsiz olarak yazılım sunarken aynı zamanda yazılımlarını fikri mülkiyet hukuku çerçevesinde yazılım değiştirilmesi ve dağıtımını kontrol edebilirler. Örneğin, FOSS sağlayıcı, sunduğu bir yazılımın ticari amaçlar için kullanılmasını ve yazılımdan ticari çıkar elde edilmesini engelleyebilir. Burada amaç, yazılımların gelişmesini teşvik ederken emek sahibinin de haklarını korumaktır. FOSS lisansının diğer yazılım türlerinden farklılıklarından biri de, "copyleft" ilkesine göre yazılım üzerinde yapılan değişikliklerin aynı lisans altında dağıtılmasını zorunlu kılmasıdır. Bu sayede yazılım üzerinde değişiklik yapan herkesin emeği aynı lisansın altında toplanmış olmaktadır.

FOSS yazılım lisans sözleşmeleri, genelde tarafların müzakeresine açık olmayan tek taraflı bir sözleşme olarak düzenlenmektedir. Yazılımı kullanacak olan kişi, yazılım dosyasının içerisinde yer alan "Licence" belgesinde yazılımı kullanımına ilişkin hangi hakların belirlendiğini bulabilir ve akabinde yazılımı kullanması işbu kurallara uymayı kabul ettiği anlamına gelmektedir. Ancak, bu sözleşme içerisinde gizlilik, uygulanacak hukuk vb. diğer sözleşme unsurlarına yer verilmemektedir. Çalışmamızda, öncelikle açık kaynak kodlu ve özgür yazılımların (FOSS) temel felsefesinden ve türlerinden

* İstanbul Medeniyet Üniversitesi, Bilişim ve Teknoloji Hukuku Tezli Yüksek Lisans Öğrencisi,
ORCID ID: 0009-0004-5728-3950

bahsedeceğiz. Akabinde FOSS yazılım lisans sözleşmelerinin; sözleşme niteliğinin tartışılması, sözleşmelerin fikri mülkiyet hukuku kuralları ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu çerçevesinde değerlendirilmesi amaçlanmaktadır. #yazılım #lisanssözleşmesi #FOSS #açıkkaynakkod #fikrimülkiyet

EVALUATION OF OPEN SOURCE AND FREE SOFTWARE (FOSS) CONTRACTS IN TERMS OF INTELLECTUAL PROPERTY LAW

Abstract

FOSS (Free and Open Source Software) software is a type of software that can be used today by many individuals and commercial companies without paying any fees and by accessing public platforms. In addition, since the source code of this software it is freely available, it is also possible to modify and develop the software and license it to third parties. The most widely used GPL (General Public License), Apache License, MIT License, Berkeley License, software licences can be given as examples of FOSS software. The aim of FOSS licences is to encourage the development and use of software by many people. For this, FOSS providers can offer software to the public for free of charge while at the same time controlling the modification and distribution of their software under intellectual property law. For example, a FOSS provider can prevent the use of its software for commercial purposes and the commercial exploitation of the software. The aim is to protect the rights of workers while encouraging software development. One of the differences of the FOSS license from other types of software is that it obliges the modifications made to the software to be distributed under the same license according to the "copyleft" principle. In this way, the work of anyone who makes changes to the software is collected under the same licence.

FOSS software licence agreements, on the other hand, are generally arranged as a unilateral contracts that cannot be negotiated by the parties. The person using the software can find out what rights to use the software are defined in the "Licence" document included in the software file, and subsequently using the software means that he agrees to comply with these rules. However, this agreement does not include other contractual elements such as confidentiality, applicable law, etc.

In our study, we will first talk about the basic philosophy and types of Open Source and Free Software (FOSS). Subsequently, it is aimed to discuss the contractual nature of FOSS software licence agreements, and to evaluate them in the context of intellectual property rules and the Law No. 5846 on Intellectual and Artistic Works.

#FOSS #licenceagreement #opensource #law #software

YEDİNCİ BÖLÜM:
VERİ HUKUKU

MOBİL OYUNLARDA İŞLENEN ÇOCUKLARA AİT KİŞİSEL VERİLERDE YASAL TEMSİLCİNİN RIZASI

Meryem SOLMAZ*

Özet

Kişisel verilerin korunması, Anayasa md. 20 ile güvence altına alınan ve medeni hukuk boyutuyla kişilik hakkı kapsamına dâhil olan bir haktır. Hakkın kapsamı ve niteliği dolayısıyla kişisel verilerin korunması talebi ve buna bağlı olarak kişisel verilerin işlenmesine yönelik rıza, doktrinde kişiye sıkı sıkıya bağlı hak olarak tanımlanmaktadır. Kişisel verilerin işlenmesi, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") kapsamında sıkı şartlara bağlanmış ise de anılan Kanun, çocukların kişisel verilerini özel olarak düzenlememiş ve kişisel verilerin işlenmesine yönelik rızaya ilişkin bir yaş sınırı öngörmemiştir. Bu durum, medeni hukuk prensipleri çerçevesinde küçüğün kişisel verilerinin korunması hususunda verinin işlenmesine yönelik rızanın küçüğün rızası ile mi yoksa yasal temsilcinin rızası ile mi olacağına ilişkin değerlendirmeyi zorunlu kılmaktadır. Zira mobil oyunlar özelinde sanal platformlar, küçüklerin risk altında olduğu ve kişisel verilerinin zarar görme tehlikesi altında bulunduğu yerlerdir. Özellikle ülkemizde yaygın olarak tercih edilen mobil oyunların büyük oranda uluslararası şirketlere ait olduğu ve bu oyunlar üzerinden işlenen verilerin çoğunlukla yurt dışına aktarıldığı hakikati göz önünde bulundurulduğunda; 10 Temmuz 2024 tarihinde yürürlüğe giren "Kişisel Verilerin Yurt Dışına Aktarılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" hükümleri çerçevesinde küçüklerin kişisel verilerinin işlenmesine ve yurtdışına aktarılmasına ilişkin rıza konusu önem kazanmaktadır.

Mobil oyun sektörü, küçüklerin kişisel verilerinin korunması konusunda hem Türkiye'de hem de dünyanın pek çok ülkesinde gittikçe büyüyen bir risk olarak karşımıza çıkmakta, bu şekildeki sanal platformlar üzerinden elde edilen veriler çoğu zaman ticarî meta olarak kullanılmaktadır. Ülkemizde çocukların kişisel verilerinin işlenmesine ve bu süreçte yasal temsilcinin rızasının alınmasına ilişkin özel bir düzenleme bulunmamaktadır. Mukayeseli hukuk perspektifinden bakıldığında ise 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nde ("GDPR") 16 yaş sınırının öngörüldüğü, pek çok Avrupa ülkesinin bu düzenlemeyi kendi iç hukuklarına aktardığı, yine Amerika Birleşik Devletleri ("ABD") gibi bazı ülkelerde bunun özel mevzuatla düzenlendiği görülmektedir. Bununla birlikte hem Türkiye gibi küçüklerin

* Doktor Öğretim Üyesi, İbn Haldun Üniversitesi Hukuk Fakültesi, ORCID: 0000-0001-7546-7957, meryem.bilici@ihu.edu.tr

kişisel verilerine ilişkin özel düzenleme olmayan ülkelerde hem de ABD ve Avrupa ülkeleri gibi konuyu düzenleyen ülkelerde, sanal platformlar ve özellikle mobil oyunlar üzerinden işlenen kişisel verilere ilişkin yasal temsilcinin sürece nasıl ve hangi aşamada dâhil olması ve rızanın hangi yöntemlerle alınması gerektiği tartışılmaktadır.

Bu tebliğ, yukarıda kısaca açıklanan hukukî problemin ve küçüklerin karşı karşıya kaldığı riskin analiz edilmesinin ve buna ilişkin farklı ülke uygulamalarından faydalanarak hukukî çözümlerin sunulmasının amaçlandığı bilimsel araştırma projesi kapsamında hazırlanmıştır. Bu çerçevede kişisel verilerin korunması hakkının medeni hukuk boyutuyla nitelendirilmesi, küçüklerin kişisel verilerinin işlenmesine ilişkin yasal temsilci rızasının gerekliliği ve bu rızanın hangi aşamada ve ne suretle temin edilebileceği (örneğin mobil oyunun açılması için öncelikle yasal temsilcinin e-posta adresine onay maili gönderilmesi gibi) hususları mukayeseli hukuk perspektifiyle ortaya konulmaktadır. Ayrıca proje kapsamında Kişisel Verileri Koruma Kurumu'nda ("Kurum") çalışan uzmanlar ile yapılan mülakat ve bu vesileyle elde edilen Kurum yaklaşımı da tebliğ çerçevesinde sunulmaktadır. Belirtmek gerekir ki yapılan çalışmalar ve elde edilen sonuçlar; Türkiye'deki mevcut mevzuat tahtında küçüklerin kişisel verilerinin özellikle sanal platformlarda korunmasına ilişkin yeterli koruyucu düzenlemelerin olmadığını, konuya ilişkin toplumsal bilincin artırılmasına yönelik çalışmaların yanı sıra küçüklerin kişisel verilerinin korunmasına ve yasal temsilcinin daha aktif olarak sürece dâhil edilmesine ilişkin özel bir düzenlemenin gerektiğini ve Kurum'un da bu eğilimde olduğunu göstermektedir.

Anahtar Kelimeler: KVKK, Veri Koruma, Mobil oyunlar, Çocukların kişisel verileri, Yasal temsil.

CONSENT OF LEGAL REPRESENTATIVE FOR PERSONAL DATA OF CHILDREN PROCESSED IN MOBILE GAMES

Abstract

Protection of personal data is a right guaranteed by Article 20 of the Turkish Constitution and is included within the scope of personality rights in civil law. Due to the scope and nature of the right, the request for personal data protection and, accordingly, the consent to the processing of personal data is defined as a strictly personal right in the doctrine. Although the processing of personal data is subject to strict conditions under Law No. 6698 on the Protection of Personal Data ("LPPD"), the said law does not specifically regulate the personal data of children and does not stipulate an age limit for consent to the processing of personal data. This situation necessitates the evaluation of whether the consent for the processing of the minor's personal data will be with the consent of the minor or with the consent of the legal representative within the framework of the civil law principles. This is because virtual

platforms, in particular mobile games, are places where minors are at risk and their personal data are under the threat of damage. Considering the fact that mobile games, which are widely preferred in our country, are mostly owned by international companies and the data processed through these games are often transferred abroad; the issue of consent regarding the processing and transfer of personal data of minors abroad within the framework of the provisions of the "Regulation on Procedures and Principles Regarding the Transfer of Personal Data Abroad", which entered into force on 10 July 2024, gains importance.

The mobile gaming sector is a growing risk both in Türkiye and in many countries of the world in terms of the protection of minor's personal data, and the data obtained through such virtual platforms are often used as commercial commodities. In our country, there is no special regulation on the processing of personal data of minors and obtaining the consent of the legal representative in this process. From a comparative law perspective, it is seen that the European Union General Data Protection Regulation ("GDPR") No. 2016/679 stipulates an age limit of 16 years, that many European countries have adopted this regulation into their domestic laws, and that it is regulated by special legislation in some countries such as the United States of America ("USA"). However, both in countries such as Turkey, where there is no special regulation on the personal data of minors, and in countries such as the USA and European countries that regulate the issue, it is discussed how and at what stage the legal representative should be involved in the process regarding the personal data processed through virtual platforms and especially mobile games, and by which methods the consent should be obtained.

This paper has been prepared within the scope of the scientific research project, which aims to analyze the legal problem briefly explained above and the risks faced by minors and to present legal solutions by referring to the practices of different countries. Within this framework, the characterization of the right to protection of personal data from the perspective of civil law, the necessity of the consent of the legal representative regarding the processing of minors' personal data, and at what stage and by what means this consent can be obtained (such as sending a confirmation e-mail to the legal representative before downloading the mobile game) are put forward from the perspective of comparative law. In addition, the interviews conducted with the experts working at the Personal Data Protection Authority ("Authority") within the scope of the project and the approach of the Authority obtained thereby are also presented in the paper. It should be noted that the studies conducted and the results obtained show that there are not sufficient protective regulations regarding the personal data of minors, especially on virtual platforms, under the current legislation in Türkiye, and that a special regulation on the protection of personal data of minors and the more active involvement of the legal representative in the process is required in addition to efforts to raise public awareness on the subject, and that the Authority is also in this position.

Keywords: GDPR, Data protection, Mobile games, Children's personal data, Legal guardianship.

VERİ MAHREMİYETİ KAPSAMINDA YAPAY ZEKÂNIN ULUSAL ve ULUSLARARASI DÜZENLEMELER AÇISINDAN DEĞERLENDİRİLMESİ

Özge DEMİRDELEN*, Şevval CEYHAN**

Özet

Veri mahremiyeti, yapay zekânın (YZ) gelişimi ve kullanımıyla doğrudan ilişkilidir. YZ sistemleri, büyük miktarda veriyi işleyerek öğrenmekte ve kararlar da alabilmektedir. Bu nedenlerle de birlikte, veri güvenliği ve gizliliği, hem ulusal hem de uluslararası düzeyde önemli bir konu haline gelmektedir. Devletler, YZ'nin etik kullanımı ve veri mahremiyetini korumak amacıyla stratejiler geliştirmektedir. Örneğin, YZ uygulamalarında şeffaflık ve hesap verebilirlik sağlamak için kılavuzlar oluşturulmaktadır. Sağlık, finans gibi hassas sektörlerde YZ'nin veri kullanımı için, kişisel verilerin korunmasını ve etik kullanımı teşvik etmeyi hedefleyen, özel düzenlemeler bulunmaktadır.

Devletlerin bazıları ilgili kişilerin verilerinin korunması için yasal düzenlemeler yaparken; birçok uluslararası kuruluş, YZ'nin insan haklarına uygun şekilde geliştirilmesi ve uygulanması gerektiğine dair beyanlar yayınlamaktadır. Avrupa Birliği (AB) kapsamında Genel Veri Koruma Tüzüğü (GDPR)'nde ise, YZ uygulamalarının, kişisel verilerin korunmasına yönelik yüksek standartlara uyması gerektiği belirtilmekte ve ilgili kişilerin verileri üzerindeki hakları güçlendirilmektedir. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), yayımladığı yönergelerle YZ ile ilgili veri mahremiyeti ilkelerini belirleyen veri yönetimi ve etik kullanımı konularında standartlar oluşturmayı hedeflemektedir. Bu yönergeler, YZ uygulamalarında kullanıcıların mahremiyetini koruma amacını taşımaktadır. OECD'nin yönergeleri, YZ sistemlerinin şeffaflık, hesap verebilirlik ve adalet gibi ilkeleri benimsemesini teşvik etmektedir. Sonuç olarak, bu yönergeler, sürdürülebilir bir dijital dönüşüm için temel bir çerçeve sunmaktadır. AB Komisyonu tarafından yayımlanan 2018 yılındaki "Avrupa Birliği Yapay Zekâ Bildirgesi" ve 2019 yılındaki "Güvenilir Yapay Zekâ için Etik Kılavuz İlkeleri ve Değerlendirme Listesi" ile gelişen YZ teknolojilerinde kişisel veri mahremiyetinin korunması açısından önem arz eden temel hak ve etik değerleri tanımlanmaktadır. Aynı zamanda YZ teknolojilerinde veri mahremiyetinin korunmasının önemi vurgulanmaktadır. AB, güvenilir YZ sistemlerinin benimsenmesi ve olası zararlara karşı güvenliğin

* Dr., Çağ Üniversitesi Hukuk Fakültesi Milletlerarası Özel Hukuk ABD Öğretim Üyesi (ozgedemirdelen@cag.edu.tr, ORCID-ID: 0000-0001-9046-5124).

** Av., Adana Barosu, Çağ Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Yüksek Lisans Öğrencisi (Tezli) (avsevvalceyhan@gmail.com, ORCID- ID: 0000-0002-5608-4958).

sağlanması amacıyla 01 Ağustos 2024 tarihinde yürürlüğe giren "Avrupa Birliği Yapay Zekâ Yasası"nı yayımlamıştır.

Ülkemiz ise, Avrupa Konseyi (AK) Yapay Zekâ Geçici Komitesi'ne aktif şekilde katılım sağlamakta, YZ etiği ve veri mahremiyeti hususlarını gözeterek, yasal çerçevenin oluşturulma çalışmalarına devam etmektedir. Stanford Üniversitesi tarafından yayımlanan YZ'nin etkilerini detaylıca değerlendiren "2024 Yapay Zekâ Endeksi Raporu"nda Türkiye 160 ülke arasında 47. sırada yer almaktadır. Bu süreçte, büyük ölçekli iş yapan şirketlerin pazarlama stratejileri açısından verilere olan ihtiyacının arttığı, yapay zekâ aracılığıyla verilerin daha kolay ve detaylı şekilde analiz edilebildiği tespit edilmiştir. "Ulusal Yapay Zekâ Stratejisi 2021-2025" ile İlgili 2021/18 Sayılı Cumhurbaşkanlığı Genelgesi ile, ülkemiz YZ stratejisi yayımlayan ülkeler arasında yerini almıştır. Strateji kapsamında; uluslararası düzeyde yürütülen güvenilir ve sorumlu YZ ile sınır ötesi veri paylaşımı alanındaki çalışmalara ülkemizin aktif şekilde katılım sağlaması, veri mahremiyetini desteklemek amacıyla teknoloji ve hukuk alanlarında uzman kişilerin bir araya gelerek, iş birliği yapması ve etik çerçeve hazırlanması kararlaştırılmıştır. Kişisel Verileri Koruma Kurumu (KVKK) ise, ilgili kişileri ve diğer bağlantılı kişileri bilgilendirici nitelikte "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler"i yayımlamıştır.

Milletlerarası özel hukuk çerçevesinde, veri aktarımı ve uyum sorunları da gündeme gelmektedir. Uluslararası iş birliği ve standartların belirlenmesi bir başka zorluktur. Veri işleme ve analiz süreçleri, düzenlemelerin kapsamı, ülkelerin farklı yaklaşımları, veri transferi ve yargı yetkisi meseleleri, veri mahremiyeti ihlalleri ve sonuçları, YZ ve veri mahremiyeti ilişkisi ele alınması gereken konulardır. Çalışmamızda, veri mahremiyeti kapsamında YZ meselesi ulusal ve uluslararası düzenlemeler açısından incelenip değerlendirmeler yapılacaktır.

Anahtar Kelimeler: Kişisel Veri, Milletlerarası Özel Hukuk, Veri Mahremiyeti, Veri Güvenliği, Yapay Zeka.

EVALUATION of ARTIFICIAL INTELLIGENCE IN TERMS of NATIONAL and INTERNATIONAL REGULATIONS WITHIN THE SCOPE of DATA PRIVACY

Abstract

Data privacy is directly related to the development and use of artificial intelligence (AI). AI systems process large amounts of data to learn and make decisions. As a result, data security and privacy have become important issues at both national and international levels. Governments are developing strategies to ensure the ethical use of AI and protect data privacy. For example, guidelines are being created to

ensure transparency and accountability in AI applications. In sensitive sectors such as healthcare and finance, there are specific regulations aimed at promoting the protection of personal data and ethical usage.

While some governments are making legal regulations to protect individuals' data, many international organizations are issuing statements emphasizing that AI should be developed and implemented in accordance with human rights. Within the framework of the European Union (EU), the General Data Protection Regulation (GDPR) stipulates that AI applications must comply with high standards for the protection of personal data and strengthen the rights of individuals over their data. The Organisation for Economic Co-operation and Development (OECD) aims to establish standards on data management and ethical use by defining data privacy principles related to AI through its published guidelines. These guidelines aim to protect users' privacy in AI applications. The OECD's guidelines encourage AI systems to adopt principles such as transparency, accountability, and fairness. As a result, these guidelines provide a fundamental framework for sustainable digital transformation. The "EU AI Declaration" published by the European Commission in 2018 and the "Ethical Guidelines and Assessment List for Trustworthy AI" in 2019 define fundamental rights and ethical values that are crucial for protecting personal data privacy in evolving AI technologies. They also emphasize the importance of safeguarding data privacy in AI technologies. To promote the adoption of trustworthy AI systems and ensure safety against potential harms, the "EU AI Act," which came into force on August 1, 2024, has been published.

Our country actively participates in the Council of Europe (CoE) Ad Hoc Committee on Artificial Intelligence, continuing efforts to create a legal framework while considering AI ethics and data privacy. The "2024 AI Index Report," published by Stanford University, ranks Turkey 47th among 160 countries in evaluating the effects of AI. During this process, it has been identified that large-scale companies have an increasing need for data in their marketing strategies, as AI enables easier and more detailed data analysis. With the "National Artificial Intelligence Strategy 2021-2025", our country has joined the ranks of nations publishing AI strategies through Presidential Decree No. 2021/18. Under this strategy, it has been decided that Turkey will actively participate in international efforts on trustworthy and responsible AI and cross-border data sharing, with experts from technology and law collaborating to support data privacy and develop an ethical framework. The Personal Data Protection Authority (PDPA) has also published recommendations on "Protecting Personal Data in the Field of Artificial Intelligence" to inform relevant individuals and other connected parties.

Within the framework of private international law, issues of data transfer and compliance also come to the forefront. Another challenge is the establishment of international cooperation and standards. Topics that need to be addressed include data processing and analysis processes, the scope of regulations, different approaches of countries, data transfer and jurisdiction issues, data privacy violations and their

consequences, as well as the relationship between AI and data privacy. In our study, the issue of AI in the context of data privacy will be examined and evaluated in terms of national and international regulations.

Keywords: Personal Data, Private International Law, Data Privacy, Data Security, Artificial Intelligence.

KİŞİSEL SAĞLIK VERİLERİNİN BİLİŞİM SİSTEMLERİYLE İŞLENMESİ VE CEZA SORUMLULUĞU

Atacan KÖKSAL*

Özet

6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre kişisel veri, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili her türlü bilgidir. Kişinin adı, doğum yeri, kimlik numarası, cinsiyeti, fotoğrafı, e-posta adresi, IP adresi kişisel veriye örnek verilebilir. Aralarında sağlık verilerinin de bulunduğu özel nitelikli kişisel veriler Kanun'un 6/1. maddesinde sayılmıştır. Buna göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Çalışmanın konusunu oluşturan kişisel sağlık verisi, kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgilerdir. Örneğin, kişinin sağlık durumuna ilişkin reçete, sağlık raporu, ilaç bilgisi, teşhis ve tedaviler kişisel sağlık verisidir.

Kişisel verinin işlenmesi ise, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder. İşlemede önem arz eden veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir. İşlemenin bilişim sistemi olarak da değerlendirilebilecek bir veri kayıt sistemi vasıtasıyla yapılması, Kanunun kapsamı yönünden önemlidir. Nitekim Kanun'un kapsama ilişkin 2. maddesine göre, "*Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt*

* Arş. Gör. Dr., Ankara Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Elemanı, ORCID: 0000-0003-1880-5176, e-posta: koksala@ankara.edu.tr

sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır".

Kişisel verilere ilişkin suçlar bakımından 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140 ıncı madde hükümleri uygulanır. Bu suçlar, kişisel verilerin kaydedilmesi suçu, verileri hukuka aykırı olarak verme veya ele geçirme ile verileri yok etmeme suçlarıdır. Bu çalışmada, yargı uygulaması ve Kişisel Verileri Koruma Kurulu kararları ışığında kişisel sağlık verilerinin işlenmesindeki ceza sorumluluğu incelenecektir.

Anahtar Kelimeler: Kişisel Sağlık Verisi, Bilişim Sistemi, İşleme, Veri Kayıt Sistemi, Özel Nitelikli Kişisel Veri.

PROCESSING OF DATA CONCERNING HEALTH THROUGH INFORMATION SYSTEMS AND CRIMINAL RESPONSABILITY

Abstract

According to the Personal Data Protection Law No. 6698 personal data means any information relating to an identified or identifiable natural person. Data subject's name, place of birth, identity number, gender, photo, e-mail address, IP address can be given as examples of personal data. Special categories of personal data, including data concerning health, are listed in Article 6/1 of the Law. Accordingly, personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data are deemed to be special categories of personal data. The personal health data which is the subject of the study is any information relating to the physical and mental health of an identified or identifiable natural person and information related to the health service provided to the person. For example, prescriptions, health reports, medication information, diagnoses and treatments related to a person's health status are data concerning health.

Processing of personal data means any operation which is performed on personal data, wholly or partially by automated means or non-automated means which provided that form part of a data filing system, such as collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization, preventing the use thereof. The data filing system, which is important in processing, is the system where personal data are processed by being structured according to specific criteria. It is important that the processing is carried out by means of a data filing system, which can also be considered as an information system, in terms of the scope of the Law. In fact, according to Article 2 of the Law on scope, "*The provisions of this Law shall apply to natural persons whose personal data*

are processed and to natural or legal persons processing such data wholly or partially by automated means or by non-automated means which provided that form part of a data filing system".

Articles 135 to 140 of Turkish Penal Code No. 5237 shall be applied to the crimes concerning personal data. These crimes are recording of personal data, illegally obtaining or giving data and destruction of data. In this study, criminal responsability related to data concerning health will be examined in the light of judicial practice and decisions of the Personal Data Protection Board.

Keywords: Data Concerning Health, Information System, Processing, Data Filing System, Special Categories of Personal Data.

OKULLARDA ÇOCUK MAHREMİYETİ (SOSYAL MEDYADA ÖĞRENCİ GİZLİLİĞİNİN KORUNMASI)

Cennet ALAS ŞEKERBAY*

Özet

Sosyal medyanın hayatın her alanında giderek daha önemli bir yer tutmaya başlaması gerçeği karşısında okullar ve öğretmenler tarafından da sosyal medya uygulamaları her zamankinden daha fazla kullanılmaya başlamıştır. Bu kullanım tanıtım, pazarlama, iletişim, eğitim gibi çeşitli süreçlerin parçası olabilmektedir. Bununla birlikte çocuklar giderek karmaşıklaşan bir sektörün finansman ortamında içerik tüketmekte, hizmetlere erişmekte ve hatta çocukların yer aldığı fotoğraf ve videolar bu ortamın bir parçası olarak içeriğin kendisini oluşturmaktadır. Elbette sosyal medyanın okullar ve öğretmenler tarafından kullanımının çeşitli faydaları bulunmakla birlikte yetişkinler tarafından kurgulanan ve kullanılan sosyal medya uygulamalarında ayırt etme gücü dahi bulunmayan çocukların tüketici ya da içeriğin kendisi olarak yer almaları bir takım mahremiyet kaygılarını gündeme getirmektedir. Bu bakımdan 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uyum sağlanması, yasal yükümlülüklerin yerine getirilmesi ve konuya özgü sektörel ilkelerin belirlenmesi önemlidir. En temel yaklaşım olarak öğrencilerin geri bildirimleri alınarak fotoğraf, video ya da diğer kişisel bilgilerinin dünyaya yayılması konusundaki endişeleri dikkate alınmalı, onlara kendilerini daha güvende hissetmeleri için yapabilecekleri anlatılmalı, her öğrencinin isteklerine kısaca kişisel verilerinin korunması hakkına saygı gösterilmelidir.

Anahtar Kelimeler: Kişisel Veri, Mahremiyet, Öğrenci Verisi, Okul Verisi, Sosyal Medya

* Kişisel Verileri Koruma Kurumu Kurul Üyesi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Fikri Mülkiyet Hakları Teknoloji Politikaları ve İnovasyon Yönetimi Doktora Öğrencisi, ORCID: 0000-0001-7215-9764

CHILDREN'S PRIVACY IN SCHOOLS (PROTECTING STUDENTS' PERSONAL DATA ON SOCIAL MEDIA)

Abstract

As social media becomes increasingly important in all areas of life, social media applications are being used by schools and teachers more than ever before. This use can be part of different processes such as advertising, marketing, communication and education. However, children consume content and access services in the financial environment of an increasingly complex sector. Moreover, photos and videos of children are the content itself as part of this environment. The use of social media by schools and teachers undoubtedly has many advantages. On the other hand, the fact that children, who do not even have the power of judgement, participate as consumers or as the content itself in social media applications designed and used by adults raises some privacy concerns. In this respect, it is important to comply with Law No. 6698 on the Protection of Personal Data, to fulfil legal obligations and to establish sectoral principles in this area. The most basic approach should be to seek students' feedback, address their concerns about their photos, videos or other personal information being shared with the world, and tell them what they can do to feel safer, the wishes of each student must be respected, in short, their right to the protection of their personal data.

Keywords: Personal Data, Privacy, Student Data, School Data, Social Media

SEKİZİNCİ BÖLÜM:
DİJİTAL BAĞIMLILIK

DİJİTAL OYUN BAĞIMLILIĞI

Osman Tolga ARICAK*

Özet

Bu bildirinin amacı, çocuk ve gençlerle çalışan uzmanlara dijital oyun bağımlılığının ne olduğunu, DSM-5 ve ICD-11 tanılama sistemlerinde tanılama kriterlerinin neler olduğunu, tanılamadaki benzerlik ve farklılıklarını ortaya koymaktır.

Dünya genelinde artan istatistiklere bağlı olarak Amerikan Psikiyatri Birliği problemli dijital oyun oynama davranışının psikiyatrik bir bozukluk olabileceği konusunda temkinli; fakat ciddi adımlar atmaya başlamıştır. Bu konuda atılan adımlar kısa sürede meyvesini vermiş ve Amerikan Psikiyatri Birliği, 2013 yılında yayınladığı DSM'nin beşinci baskısı üçüncü kısmında "hakkında daha fazla araştırmaya ihtiyaç duyulan" bir bozukluk olarak 'internet oyun oynama bozukluğunu' tanımlamıştır. Kitapta her ne kadar bozukluğun ismi 'internet oyun oynama bozukluğu' olarak geçmekteyse de, 'Alt Tipler' başlığı altında 'internete bağlı olmayan bilgisayar oyunlarının da' bu gruba dâhil edilebileceğini belirtmiştir.

Dünya Sağlık Örgütü de 2014 yılından bu yana 2018 yılında yayımlanan 'Hastalıkların Uluslararası Sınıflandırılması' el kitabının 11. Baskısında, hem çevrimiçi hem de çevrimdışı "oyun oynama bozukluğu" kavramını tanımlamış ve tanı kriterlerini sıralamıştır.

Dijital oyun bağımlılığı üzerine şu ana kadar yapılan en geniş ölçekli çalışmaların, Avrupa ve Uzakdoğu Asya ülkelerinde gerçekleştirildiği görülmektedir. Yapılan araştırmalar oyun bağımlılığı için yaygınlık oranını, Batı ülkeleri genelinde %1-10 arası, Güney Amerika ve Afrika ülkeleri genelinde %1-9 arası, Uzakdoğu Asya ülkeleri genelinde ise %10-15 arası olarak vermektedir. DSM-5, bir Asya ülkesinden elde edilen oranları paylaşmış; 15-19 yaş arası erkeklerin %8.4'nün, kızların ise %4.5'nin DSM-5'teki oyun oynama bozukluğu için belirlenen dokuz ölçütten beşini taşıdığını belirtmiştir.

* Prof. Dr., Boğaziçi Üniversitesi Eğitim Fakültesi Öğretim Üyesi, https://orcid.org/0000-0001-8598-5539 tolga.aricak@bogazici.edu.tr

Bu bildiride özellikle Dünya Sağlık Örgütü'nün 2014'ten bu yana bu konudaki çalışmalarının özetlenmesi amaçlanmaktadır. Bu çalışma, literatür derlemesi tarzı bir yöntemle gerçekleştirilmiştir. Aynı zamanda yazarın son sekiz yıldır Dünya Sağlık Örgütü bünyesinde gerçekleştirdiği çalışmaların ve deneyimlerin bir özeti niteliğindedir.

Anahtar Kelimeler*:* Dijital oyun bağımlılığı, İnternet Oyun Oynama Bozukluğu

DIGITAL GAME ADDICTION

Abstract

The purpose of this report is to elucidate the concept of digital game addiction for specialists working with children and adolescents, as well as to outline the diagnostic criteria in the DSM-5 and ICD-11 systems, highlighting their similarities and differences.

In response to increasing statistics worldwide, the American Psychiatric Association has cautiously begun to take significant steps regarding problematic digital gaming behavior, which may be considered a psychiatric disorder. These efforts have quickly borne fruit, leading the American Psychiatric Association to define "Internet Gaming Disorder" as a condition that "Conditions for Further Study" in the third section of the fifth edition of the DSM, published in 2013. Although the disorder is referred to as "Internet Gaming Disorder" in the book, it notes under the heading "Subtypes" that "non-Internet computerized off-line games" can also be included in this group.

Since 2014, the World Health Organization (WHO) has defined the concept of "Gaming Disorder" in both predominantly online and predominantly offline contexts in the 11th edition of the International Classification of Diseases (ICD), published in 2018, and has outlined its diagnostic criteria.

The largest-scale studies conducted to date on digital game addiction have taken place in European and East Asian countries. Research indicates that the prevalence of gaming addiction is between 1-10% in Western countries, 1-9% in South American and African countries, and 10-15% in East Asian countries. The DSM-5 reported findings from an Asian country, indicating that 8.4% of males and 4.5% of females aged 15-19 met five of the nine criteria established for gaming disorder.

This report specifically aims to summarize the WHO's work on this subject since 2014. It has been conducted as a literature review and also serves as a summary of the author's experiences and studies conducted within the WHO over the past eight years.

Key Words: Digital game addiction, Internet Gaming Disorder

DİJİTAL OYUNLARIN KUMARLA İLİŞKİSİ: RİSKLER VE ÖNLEME YOLLARI

Süreyyanur KİTAPÇIOĞLU*

Özet

Günümüzde internet hizmetleri ve akıllı telefonların yaygınlaşması, teknolojik gelişmelerle birlikte insanların günlük yaşamını büyük ölçüde değiştirmiştir. Özellikle oyun ve kumar endüstrileri bu dijital dönüşümden önemli ölçüde etkilenmiş ve bireylerin bu sektörlerle etkileşimini artırmıştır (Derevensky ve Griffiths, 2019). Oyun sektörünün hızlı büyümesi gençlerin dijital oyunlara olan ilgisini artırırken, kumar sektörü daha yavaş ilerlemiş ve dijital ortamda kumara yönelik ilgiyi çekmek için yeni stratejiler geliştirmeye başlamıştır (Delfabbro ve King, 2020). Bu stratejiler arasında, dijital oyunlara kumar benzeri içeriklerin entegre edilmesi yer almaktadır. Özllikle loot box gibi oyun içi satın alma unsurları gençlerde bağımlılık riskini yükseltmektedir (Drummond ve Sauer, 2018; King ve Delfabbro, 2020). Özellikle kumar unsurlarının oyun sektörüne dâhil edilmesi, ticari kazancı artırırken gençlerde bağımlılık geliştirme riskini de arttırmaktadır.

Dijital Oyunlarda Kumar Benzeri İçerikler

Oyunlarda yer alan kumar benzeri unsurlar, kullanıcıları uzun süre oyunda kalmaya ve daha fazla harcamaya teşvik eden mekaniklere sahiptir. Bu içerikler, kumarın bir biçimi olarak tartışılan loot box'lar ve oyun içi satın alma gibi özellikleri içermektedir (King ve Delfabbro, 2020; Macey ve Hamari, 2018). Araştırmalar, oyun içi satın alma işlemlerinin bazı kullanıcılar için risk oluşturabileceğini, aşırı harcamaya, bağımlılık yapıcı davranışlara ve kumarın normalleşmesine yol açabileceğini belirtmektedir (King ve Delfabbro, 2018; King ve Delfabbro, 2020). Özellikle genç oyuncular arasında yaygın olan loot box satın alımları, onları ödül kazanma arzusuyla oyuna bağlayarak aşırı oyun oynama davranışlarına yol açabilmektedir.

* Klinik Psikolog, Doktora Öğrencisi, Hasan Kalyoncu Üniversitesi, https://orcid.org/0000-0001-6608-2772 sureyyakitapcioglu@gmail.com

E-spor Bahisleri ve Sosyal Kumarhaneler

E-spor bahisleri, video oyunu yarışmalarının sonuçlarına bahis koyma pratiğini ifade etmektedir. Bu durum dijital platformların yaygınlaşmasıyla birlikte popüler hale gelmiştir. E-spor bahislerinin bağımlılık riskini artıran bir etken olduğu ve gençlerin kumar bağımlılığı geliştirmesine katkıda bulunabileceği öne sürülmektedir (Zendle, 2020). Öte yandan, sosyal kumarhane oyunları, gerçek parayla şans oyunları oynama fırsatı sunarak oyuncuları kumarın eğlenceli bir etkinlik olduğu yanılgısına düşürebilmektedir. Bu oyunların kullanıcıları daha sonra geleneksel kumara yönelebilmekte ve bu da bağımlılık riskini artırabilmektedir (Gainsbury ve ark., 2016).

Ganimet Kutuları ve Jetonlu Bahisler

Ganimet kutuları, oyuncuların rastgele ödüller kazandığı oyun içi ögelerdir ve kullanıcıları ödül kazanma beklentisiyle daha fazla harcama yapmaya yönlendirebilmektedir. Bu mekaniklerin, kumarla benzer özellikler taşıması nedeniyle bağımlılık yapıcı etkileri olabileceği öne sürülmektedir (Drummond ve Sauer, 2018). Ayrıca jetonlu bahis gibi oyun içi aktiviteler, kullanıcıları oyun içerisinde elde ettikleri sanal ödüllerle tatmin ederek, onları kumara karşı duyarsızlaştırabilir ve bağımlılık riskini artırabilmektedir (Zendle, 2020).

Kumar Endüstrisinin Dijitalleşmesi ve Gençlere Erişimi

Kumar endüstrisi, dijitalleşme ile birlikte gençleri hedef alan içeriklerle geniş bir kitleye erişim sağlama imkanı bulmuştur. Sosyal medya, influencer işbirlikleri ve spor sponsorlukları gibi stratejilerle kumar reklamları, gençler için normalleştirilmekte ve erişilebilir hale getirilmektedir (Wardle ve ark., 2024). Dijital oyunlarda kumar unsurlarının normalleştirilmesi, gençlerin bu tür içeriklere duyarlı hale gelmesine yol açabilir ve bu nedenle, toplum sağlığı açısından gençleri koruyucu önlemler gerekmektedir. The Lancet Public Health Komisyonu, kumarın halk sağlığı sorunu olarak ele alınması gerektiğini belirterek daha güçlü düzenlemelerin ve koruyucu politikaların önemine dikkat çekmektedir (Wardle ve ark., 2024).

Halk Sağlığı ve Düzenleme Gereksinimi

Dijital oyunların kumar unsurları içermesi, gençlerin kumara daha fazla maruz kalmalarına yol açarak bağımlılık riskini artırmaktadır. Bu risklerin önlenmesi adına dijital oyunlarda kumar benzeri mekaniklerin sınırlandırılması, yaş sınırlamalarının uygulanması ve oyun içi satın alımların düzenlenmesi gibi politikaların oluşturulması gerekmektedir. Özellikle sosyal medya ve dijital platformlarda kumar içerikli reklamların sınırlandırılması, gençlerin bu tür içeriklere daha az maruz kalmasını sağlayacaktır (Wardle ve ark., 2024).

Önleme Yolları ve Bilinçlendirme

Gençlerin dijital oyunlarda kumar benzeri içeriklere maruz kalmalarının önlenmesi için ailelerin ve eğitimcilerin bu konuda farkındalık kazanmaları önemlidir. Özellikle ailelerin, çocuklarını dijital oyunların içerdiği riskler konusunda bilinçlendirmeleri ve çocukların oyun alışkanlıklarını yakından takip etmeleri gerekmektedir. Aynı zamanda oyun geliştiricilerin ve dağıtıcıların da bu konuda sorumluluk almaları, oyun içi satın alımların ve kumar benzeri unsurların sınırlandırılması adına etkili olacaktır. Ayrıca, çocukların oyun bağımlılığı ve kumar bağımlılığına karşı korunması için halk sağlığı açısından etkili politikaların geliştirilmesi önem arz etmektedir.

Sonuç

Dijital oyunların kumar unsurları içermesi, gençlerde oyun ve kumar bağımlılığı riskini artırarak halk sağlığını tehdit etmektedir. Bu nedenle, dijital oyun içeriklerinin sıkı düzenlemelerle denetlenmesi ve gençlerin kumar riskinden korunması için kapsamlı önlemler alınması gerekmektedir. Teknolojik gelişmelerle birlikte büyüyen oyun endüstrisinin, toplum sağlığı üzerindeki etkilerinin değerlendirilmesi ve bu etkilerin sınırlandırılması için politika yapıcıların aktif rol alması gereklidir. Özellikle dijital oyunlarda yer alan kumar unsurlarının düzenlenmesi ve gençlerin bu riskli içeriklerden korunması, toplum sağlığını korumak adına kritik öneme sahiptir.

Anahtar Kelimeler: Dijital oyun bağımlılığı, İnternet Oyun Oynama Bozukluğu, Kumar bağımlılığı

THE INTERRELATIONSHIP BETWEEN DIGITAL GAMES AND GAMBLING: RISKS AND PREVENTIVE STRATEGIES

Abstract

The widespread availability of internet services and smartphones, coupled with technological advancements, has fundamentally transformed daily life. This digital shift has had a profound impact, particularly on the gaming and gambling industries, fostering increased engagement with these sectors (Derevensky & Griffiths, 2019). While the rapid expansion of the gaming sector has intensified interest among young users, the gambling industry has experienced comparatively slower growth, prompting the development of new strategies to enhance digital engagement with gambling content (Delfabbro & King, 2020). These strategies have prominently included the integration of gambling-like mechanisms into digital games, where in-game purchasing features, such as loot boxes, have raised addiction risks, particularly among youth (Drummond & Sauer, 2018; King & Delfabbro, 2020). Consequently, incorporating gambling

features within the gaming sector not only augments commercial profitability but also amplifies addiction risks among younger demographics.

Gambling-like Elements in Digital Games

Digital games increasingly incorporate elements that closely mirror gambling, driving prolonged user engagement and promoting additional spending. These mechanisms encompass features like loot boxes and other in-game purchases, which have garnered attention as potential gateways to gambling behaviors (King & Delfabbro, 2020; Macey & Hamari, 2018). Empirical evidence suggests that such in-game purchasing options can be especially risky for certain users, leading to excessive spending, addictive behaviors, and the normalization of gambling, particularly among young users incentivized by reward-based mechanics (King & Delfabbro, 2018; King & Delfabbro, 2020).

Esports Betting and Social Casino Games

The practice of esports betting, wherein users wager on competitive gaming outcomes, has surged in popularity alongside the growth of digital platforms. This form of betting has been identified as a significant risk factor, contributing to addictive behaviors and potentially leading to gambling addiction among youth (Zendle, 2020). Social casino games, in contrast, provide simulated gambling experiences that involve real monetary stakes, luring players into perceiving gambling as a recreational activity. Studies indicate that participants in these social casino games may later transition to traditional gambling, thereby elevating their risk of addiction (Gainsbury et al., 2016).

Loot Boxes and Token-based Betting

Loot boxes, which offer players randomized rewards through paid transactions, closely resemble gambling mechanics and encourage repeated spending due to the anticipation of obtaining valuable items. This resemblance to gambling has raised concerns over the potential for addiction (Drummond & Sauer, 2018). Furthermore, token-based betting in games can reward players with virtual prizes, potentially desensitizing them to gambling while simultaneously increasing their susceptibility to addiction (Zendle, 2020).

Digitalization of the Gambling Industry and Youth Accessibility

Digitalization has enabled the gambling industry to reach a wider audience, particularly young people, through tailored content. By leveraging social media, influencer partnerships, and sports sponsorships, gambling advertisements are increasingly normalized and accessible to youth (Wardle et al., 2024). The normalization of gambling elements in digital games increases young people's susceptibility to such

content, thus highlighting the need for protective public health measures. The Lancet Public Health Commission underscores the importance of addressing gambling as a public health issue and advocates for stronger regulatory and preventive policies to mitigate these risks (Wardle et al., 2024).

Public Health Imperatives and Regulatory Requirements

The inclusion of gambling elements in digital games exposes young individuals to heightened risks of engaging with gambling, thus increasing addiction susceptibility. Effective prevention strategies necessitate limiting gambling-like features in games, enforcing age restrictions, and regulating in-game purchases. In addition, curtailing gambling advertisements on social media and digital platforms may further reduce youth exposure to gambling (Wardle et al., 2024).

Preventive Measures and Awareness

Mitigating youth exposure to gambling-like elements in digital games requires raising awareness among parents and educators. Parental vigilance regarding digital gaming risks and monitoring children's gaming habits are essential. Additionally, developers and distributors bear responsibility for restricting in-game purchases and gambling-like features. The development of effective public health policies is paramount to safeguarding children from gaming and gambling addiction.

Conclusion

The integration of gambling elements into digital games significantly increases addiction risks among young players, posing a public health threat. As such, it is imperative to impose stringent regulations on digital game content and implement comprehensive measures to protect youth from gambling-related risks. Policymakers should play an active role in assessing and mitigating the public health impacts of the rapidly expanding gaming industry. Notably, regulating gambling elements within digital games and protecting young individuals from such hazardous content is critical for safeguarding public health.

Key Words: Digital game addiction, Internet Gaming Disorder, Gambling

PROBLEMLİ PORNOGRAFİ KULLANIMI: TANIMLAR, ETKİLER, ARAŞTIRMA

Eren Murat DİNÇER*

Özet

Son yıllarda internetin yaygınlaşmasıyla birlikte pornografi kullanımı, özellikle gençler ve yetişkinler arasında giderek artan bir sıklıkla görülmektedir. Araştırmalar, pornografik içeriğe erişimin kolaylaşmasıyla birlikte, bireylerin pornografi tüketim alışkanlıklarının arttığını ve bunun birçok farklı yaş grubunda yaygın bir pratik haline geldiğini göstermektedir.

Problemli pornografi kullanımı (PPK), bireyin pornografiye karşı kontrol edemediği bir dürtü geliştirmesi ve bu durumun işlevselliğini, ilişkilerini veya genel yaşam kalitesini olumsuz yönde etkilemesi olarak tanımlanmaktadır. Ancak, PPK'nin tanımı ve sınıflandırılması konusundaki tartışmalar sürmektedir. Bazı araştırmacılar, PPK'yi bağımlılık çerçevesinde değerlendirirken, diğerleri onu daha çok bir alışkanlık ya da zorlayıcı bir davranış modeli olarak ele almaktadır. Bu tartışmalar, PPK'nin doğası, nedenleri ve sonuçları hakkında daha fazla araştırma yapılmasını gerektirmektedir.

PPK'nin bireyler üzerindeki etkileri geniş bir yelpazeye yayılmaktadır. Bu etkiler arasında cinsel işlev bozuklukları, düşük benlik saygısı, ilişkisel çatışmalar ve duygu düzenleme güçlükleri yer almaktadır. Ayrıca, PPK'nin kişinin sosyal hayatı ve akademik/mesleki performansı üzerindeki olumsuz etkileri de dikkat çekmektedir. Bu etkiler, bireyin problemli kullanım döngüsünü sürdürmesine ve günlük yaşamını olumsuz etkilemesine neden olabilir.

PPK'yi ölçmek için geliştirilen çeşitli ölçekler bulunmaktadır, ancak bu ölçeklerin geçerlilik ve güvenilirlikleri konusundaki tartışmalar devam etmektedir. Güncel ölçüm araçları, bireyin pornografi kullanımının sıklığını, süresini ve bu kullanımın psikososyal etkilerini değerlendirmeyi amaçlamaktadır. Ancak, kültürel faktörler ve bireysel farklılıklar, bu ölçüm araçlarının genellenebilirliğini sınırlayabilir.

* Dr., erenmuratdincer@gmail.com https://orcid.org/0000-0002-7837-0832

Gelecekteki çalışmaların, PPK'nin farklı yaş ve kültürel gruplardaki yaygınlığını ve etkilerini incelemesi önemlidir. Ayrıca, pornografi kullanımını etkileyen faktörler, PPK'nin bilişsel ve nörolojik temelleri ve etkili müdahale stratejilerinin geliştirilmesi gibi konular daha fazla araştırma gerektirmektedir. Özellikle, PPK'nin uzun vadeli etkileri ve iyileşme süreçleri üzerine yapılacak çalışmalar, alana önemli katkılar sağlayabilir.

Anahtar Kelimeler: Problemli porno kullanımı; davranışsal bağımlılıklar; pornografi; ruh sağlığı

PROBLEMATIC PORNOGRAPHY USE: DEFINITIONS, EFFECTS, RESEARCH

Abstract

In recent years, the prevalence of pornography use has been increasing, particularly among adolescents and adults, with the widespread availability of the internet. Research shows that as access to pornographic content becomes easier, individuals' pornography consumption habits have increased, making it a common practice across various age groups.

Problematic pornography use (PPU) is defined as the development of an uncontrollable urge toward pornography, which negatively impacts an individual's functionality, relationships, or overall quality of life. However, debates continue regarding the definition and classification of PPU. Some researchers view PPU within the framework of addiction, while others consider it more as a habit or a compulsive behavior pattern. These discussions highlight the need for further research on the nature, causes, and consequences of PPU.

The effects of PPU on individuals span a wide range, including sexual dysfunctions, low selfesteem, relational conflicts, and difficulties in emotion regulation. Additionally, the negative impacts of PPU on a person's social life and academic/professional performance are significant. These effects can perpetuate the cycle of problematic use and negatively influence daily life.

Various scales have been developed to measure PPU, but debates about the validity and reliability of these scales continue. Current assessment tools aim to evaluate the frequency and duration of pornography use, as well as its psychosocial effects. However, cultural factors and individual differences may limit the generalizability of these tools.

Future studies should focus on examining the prevalence and effects of PPU across different age and cultural groups. Furthermore, topics such as factors influencing pornography use, the cognitive and neurological foundations of PPU, and the

development of effective intervention strategies require further research. Especially, studies on the long-term effects of PPU and recovery processes can provide significant contributions to the field.

Keywords: Problematic pornography use; behavioral addictions; pornography; mental health

DOKUZUNCU BÖLÜM:
BİLİŞİMİN DİĞER GÜNCEL YANSIMALARI

GELİŞEN TEKNOLOJİ İLE DOĞACAK ÇOCUĞU TASARLAMAK SURETİYLE ONUN KİŞİLİK HAKKINA HENÜZ DOĞMADAN MÜDAHALE EDİLMESİ

Sera REYHANİ YÜKSEL*

Özet

Doktrinde kişilik hakkı farklı şekillerde tanımlanmış olsa da kişilik hakkını en genel haliyle, yaşam, beden bütünlüğü, onur ve saygınlık gibi kişi varlığı değerleri üzerinde var olan, kişiye sıkı sıkıya bağlı, herkese karşı ileri sürülebilen ve herkes tarafından ihlal edilebilecek olması nedeniyle mutlak, zamanaşımı veya hak düşürücü süreye tabi olmayan, devredilemeyen ve vazgeçilemeyen, mirasçılara geçmeyen, tekelci bir niteliğe sahip, haczedilemez/iflas masasına girmez nitelikte, zamanla gelişen ve değişen bir niteliğe sahip olması dolayısıyla esnek, şahıs varlığına dahil bir hak olarak tanımlamak mümkündür.

Çocukların hiç şüphesiz kendilerine ait ve korunmaya değer bir kişilikleri bulunmaktadır. Çocuğun korunmaya değer bu kişiliği onun henüz doğumundan önce anne ve babasının kendi genlerine müdahalesine maruz kalmamasını da kapsamına almalıdır. Ancak gelişen teknoloji beraberinde anne ve babaların çocuklarını programlayabilmesi imkanını getirmiştir. Doğacak çocukların ileride herhangi bir sağlık sorunu yaşamamasını sağlayamaya yönelik olması sebebiyle teknolojinin getirdiği bu imkân olumlu olarak görülebilirse de yaratacağı sakıncalar da göz ardı edilemez. Mesela bu doğacak çocuğun cinsiyetine yönelik bir müdahaleye neden olduğunda cinsiyet dağılımında dengesizlik dahil olmak üzere birçok soruna yol açabilir. Bunun dışında doğacak çocuğun başka birçok fiziksel, bilişsel veya psikolojik özelliğine müdahale gerçekleştirilebilir. Anne ve babanın çocuğunun sarışın, mavi gözlü olmasını istediği bir durumda bunu sağlamaları mümkün olabilecektir. Üstelik sadece bebeklerin cinsiyeti, boyu, saç ve göz rengi değil, karakteri bile önceden belirlenebilir hale gelmektedir. Halbuki bir çocuğun, anne ve babasının kendisi için yaptığı

* Doç. Dr, Tekirdağ Namık Kemal Üniversitesi Hukuk Fakültesi, Medeni Hukuk Anabilim Dalı Öğretim Üyesi, sereyhani@hotmail.com, Orcid İd:0000-0002-7969-6949.

seçimlerin dışına çıkabilmesi de kişiliğini ortaya koymasının bir yoludur. Zeki, özgür ruhlu, yaratıcı, karizmatik, uzun boylu, normal kiloda olması istenilen bir çocuğun özelliklerine bu denli müdahale edilmesi onun bağımsız bir kişi olarak var olmasının önünde bir engeldir ve kişilik hakkına müdahale oluşturur. Dolayısıyla bu konuda var olan ve göz ardı edilemez etik ve ahlaki kaygılar bir yana, çocuğun kişilik hakkının korunması bakımından da durum olumsuz sonuçlara sebep olabilecek niteliktedir. İnceleme konumuz bağlamında öncelikle teknolojik gelişmeler sonucu ortaya çıkan "tasarım bebek" kavramı açıklanacak, sonrasında tasarım bebek olgusunun çocuğun kişilik hakkına müdahale anlamında yaratacağı hukuki sorunlar üzerinde durulacaktır.

Anahtar Kelimeler: Tasarım bebek, kişilik, kişilik hakkı, kişiliğin korunması, genetik müdahale

VIOLATION OF PERSONAL RIGHTS OF AN UNBORN BABY WHEN THE BABY IS DESIGNED WITH ADVANCING TECHNOLOGY

Abstract

Although there are several definitions of personal rights, in general it can be defined as a right that a person has over their own body based on the integrity of body, life, honour and dignity, closely tied to the person, which is absolute, exclusive, non-seizable and is not subject to statute of limitations or final term; which may not be transferred or renounced, may not be inherited, may not be sold, traded or distributed by a bankrupt entrepreneur, flexible since it develops and changes over time.

A child undoubtedly has their own personality worthy of protection. Protection of a child's personality should also include nonexposure to gene editing by its parents before it is even born. However advancing technology allows parents to design and program their babies. Although this opportunity brought by the technology can be considered as a positive development since it prevents potential health problems in children before they are born, problems this can cause cannot be ignored. For example when the technology allows parents to choose the gender of their unborn children, this can cause many problems including sex-ratio imbalances. In addition to this, many of the physical, cognitive abilities or personality traits of the unborn child can be altered. For example, it will be possible for their parents to make their baby blonde and blue eyed. Moreover, not only the sex, height, hair and eye colours but also personality of the baby can also be altered. However, children's freedom to make their own choices instead of their parents' is a way to manifest their personality. Altering personality traits of a child to make them smart, free-spirited, creative, charismatic, tall with normal weight prevents the child from becoming an independent person and is considered as a violation of personal rights. Therefore in addition to ethical and moral

concerns which cannot be ignored, this can also have consequences for the protection of personal rights of the child. In this paper, we will first explain the "designer baby" concept created with the advances in technology and then discuss legal consequences of the designer baby concept since it may be considered as a violation of personal rights.

Keywords: Designer baby, personality, personal right, protection of personal rights, gene editing

YAŞLI BİREYLERİN SOSYAL ROBOT KULLANIMINDA AYDINLATMA YÜKÜMLÜLÜĞÜ VE AÇIK RIZA

Deniz Onur ARAS*

Özet

Teknoloji ve tıptaki gelişmelerle birlikte yaşam sürelerinin uzaması, kişiye daha fazla deneyim yaşama şansı sunmaktadır. Dünya genelinde yaş ortalaması yükseldikçe, sağlık hizmetlerine ve yaşlı bakımına olan ihtiyacı her geçen gün daha da artırmaktadır. Bu artan talebe yanıt vermekte zorlanan sağlık hizmetlerinde maliyetler artmakta, yaşlı bireylerin yetersiz fiziki ve psikolojik destekle baş başa kalmaktadır. Dünyada azalan doğum oranları, artan bireyselleşme ve aile yaşam alanlarının küçülmesi ile geniş ailelerin giderek kaybolması, yaşlı bakımı ve yalnızlaşma sorununu beraberinde getirmektedir. Yaşlı bakım evleri hem hizmetleri hem de sosyal alanları konusunda bir nebze de olsa çözüm olabilecekken, bakım evlerinin kalitesi, insan istihdamındaki problemler ve hizmet kalitesinin denetiminin zor olması bu sorunu başka bir boyuta taşımaktadır.

Zamanının çoğunu yalnız geçiren ve kronik hastalıklarla uğraşan yaşlı bireyin mental kapasitesi de bir süre sonra hızlı bir çöküşe geçebilecektir. Bu sorunlara çözüm üretmeye çalışan Japonya, Fransa, Almanya vb. ülkeler robotikten faydalanmaktadır. Birçok çeşidi olan robotların kullanılmasıyla birlikte hasta bakımı gerçekleştirebilmekte, günlük faaliyetlere yardımcı olunmakta, ilaç saatleri düzenlenmekte ve sosyal etkileşim arttırılmaktadır. Bu robotlar farklı özellikleriyle muhtelif ebatlara ve görevlere ilişkin karmaşıklık düzeylerine ulaşabilmektedir. Yaşlı bakım evlerinde de bu tip robotlar kullanılabilmekteyse de yaşlı bireylerin sosyal robotları evlerinde kullanma alışkanlıkları giderek artmaktadır.

Bazı ülkelerde uzun yıllardan beri yaşlı bireyler tarafından kullanan sosyal robotlar, ülkemizde de kullanım alanı bulmaya başlamıştır. Bu robotlar şuan itibariyle gerek kişisel, gerekse huzurevleri tarafından temin edilebilmektedir. Ülkemizde ve Dünyada

* İzmir Ekonomi Üniversitesi Araştırma Görevlisi Doktor, Deniz Onur Aras, Orcid: 0009-0007-6861-565X, Mail: deniz.aras@ieu.edu.tr

kullanımın yaygınlaşması, bu robotların bireylere mental veya fiziksel zararlar verebileceği zararların çeşidi değişmekte ve etkilenen kişi sayısı artmaktadır. Bu robotlar doğrudan maddi zararlar sebebiyet verebileceği gibi, manipülasyon yöntemleriyle kişiye mental olarak zarar verebilecektir. Bu durum halihazırda kalp, tansiyon demans, Alzheimer vb. gibi kronik hastalıklarla uğraşan yaşlı bireylerin daha büyük kayıplar yaşamasına sebebiyet verebilir.

Aslında sosyal robotların yaşlı bakımında kullanılmasında farklı hukuk dallarını ilgilendirebilecek birçok risk olmasına rağmen, bu risklerin henüz bir bölümü anlaşılabilmiştir. Kaldı ki risk doğuran olayların meydana gelmesindeki çeşitlilik özellikle yapay zekanın denkleme daha çok girmeye başladığı ve teknolojilerinin karmaşıklaştığı dönemde artış gösterecektir. Bu risklerin de yaşlı bireylere aktarılması gerekmektedir. Halihazırda analiz edilen riskler dahi ilgili mevzuatlarda muhtelif sorunlara sebebiyet verebilecek düzeydedir. Konumuz bakımından ise hareket sensörleri, görsel ve işitsel kayıt cihazları, yüz tanıma sistemleri, ağır fiziki yapıları, var olabilecek yapay zeka ajanları gibi öğeler robotların çok geniş bir kişisel ve özel nitelikteki veriyi elde edebilmesine sebebiyet vermektedir. Kullanıcılarının çoğunluğu yaşlı bireylerden oluşan bu robotların meydana getirebileceği risklere ilişkin aydınlatma ve elde edilebilecek verilere ilişkin açık rızanın ne şekilde alınacağı ise sorunlu bir alan olabilecektir. Çalışmamızda da yaşlı bireylerin kullanacağı sosyal robotlar için hem kişisel hem de özel nitelikli kişisel verilerin işlenebilmesi için alınması gerek açık rızada dikkat edilmesi gereken hususlar değerlendirilecektir.

Anahtar Kelimeler: Sosyal Robot, Yaşlı Bakım, Aydınlatma Yükümlülüğü, Açık Rıza

OBLIGATION OF ENLIGHTENMENT AND EXPLICIT CONSENT IN THE USE OF SOCIAL ROBOTS BY ELDERLY INDIVIDUALS

Abstract

Advancements in technology and healthcare have led to longer life expectancies, allowing individuals to enjoy more experiences throughout their lives. However, as the global population ages, the demand for healthcare and elderly care services is growing at a rapid pace. Healthcare systems are finding it increasingly difficult to meet this rising demand, resulting in higher costs and insufficient physical and psychological support for elderly individuals. Contributing factors, such as declining birth rates, increasing individualism, shrinking living spaces, and the waning presence of extended family structures, further exacerbate the challenges of elderly care and isolation.

Although nursing homes could provide partial solutions with their services and social environments, issues such as the quality of care, employment challenges, and

difficulties in monitoring service standards introduce new dimensions to this problem. Elderly individuals who spend most of their time alone and deal with chronic illnesses may experience rapid mental decline over time. Countries like Japan, France, and Germany have started to utilize robotics as a solution to these issues. Different types of robots are being used to provide patient care, assist with daily activities, schedule medication times, and increase social interaction. These robots, varying in size and complexity depending on their functions, are increasingly being used in nursing homes as well as in elderly individuals' homes.

In some countries, social robots have been used by elderly individuals for many years, and their usage is now becoming more common in Türkiye. These robots are currently available for both personal use and for use in nursing homes. As the use of these robots expands, both in Türkiye and globally, the potential for mental or physical harm they may cause increases, along with the number of people affected. These robots can cause direct physical harm, and through manipulation techniques, they can cause mental distress as well. This could lead to severe consequences for elderly individuals already struggling with chronic conditions such as heart disease, hypertension, dementia, or Alzheimer's.

Although there are various risks associated with the use of social robots in elderly care, which could fall under different branches of law, only a few of these risks have been understood so far. As artificial intelligence becomes more integrated and these technologies become increasingly complex, the variety of risks will continue to grow. These risks must also be communicated to the elderly individuals who will be using these robots. Even the risks identified so far pose potential challenges to the existing legal frameworks.

In terms of the topic at hand, components such as motion sensors, visual and audio recording devices, facial recognition systems, heavy physical structures, and potential AI agents allow these robots to collect extensive personal and sensitive data. How to inform elderly users about these risks and how to obtain their explicit consent regarding the use of these data are areas that remain problematic. This study will evaluate the considerations that need to be taken into account when obtaining explicit consent for the processing of both personal and sensitive personal data in the context of social robots used by elderly individuals.

Keywords: Social Robot, Elderly Care, Obligation of Enlightment, Explicit Consent

TÜRK HUKUKUNDA ŞEBEKELER ÜSTÜ HİZMET VE ŞEBEKELER ÜSTÜ HİZMET SAĞLAYICIYA GENEL BAKIŞ

Raci ÇETİN YÜKSEKBAŞ*

Özet

İnternet teknolojisinin, yirmi birinci yüzyılda küresel bazda pek çok paradigmayı değiştirdiği görülmektedir. Dünyada yaşanan bu paradigma değişimlerinden bir tanesi de, kuşkusuz iletişim ve telekomünikasyon alanında gerçekleşmiştir. Yüzyılımızın başında geleneksel kablolu iletişim, yerini büyük oranda şebekeler vasıtasıyla yapılan kablosuz mobil iletişime terk etmiştir. Mobil iletişim operatörlerinin klasik sesli iletişimin yanında internet hizmetini de sunmaları ve özellikle 3G teknolojisinin ortaya çıkmasıyla, internet teknolojisine cep telefonları vasıtasıyla da erişim mümkün hale gelmiş ve internet teknolojisi toplumun geniş kesimlerine yayılmıştır. İnternet teknolojisinin kendine özgü niteliği, sesli, yazılı ve görüntülü iletişim ile diğer medya unsurlarının internet üzerinden aktarılmasını olanaklı kıldığından, zamanla iletişimin internet üzerinden yapılması düşüncesi doğmuştur. Buna dair düşünceler, sosyal medya şirketlerinin çeşitli medya unsurlarını, herhangi bir mobil operatörden destek almadan ve yalnızca internet kullanarak taraflar arasında iletilmesi ile güçlenmiştir.

İşte bu şekilde, mobil iletişim operatörlerinin sunmakta olduğu şebeke, kablo, mobil istasyon vb. altyapıyı kullanmaksızın ve bu operatörün müdahalesi olmaksızın her türlü iletişim ve medya aktarımın son kullanıcıya yalnız internet üzerinden sağlandığı şebekeler üstü hizmet (*Over-The-Top Services*) kavramı ortaya çıkmıştır. Facebook Messenger, WhatsApp, Telegram, Discord ve Signal başta olmak üzere çeşitli şirketlerce geliştirilen mobil uygulamalarla şebekeler üstü hizmet ve şebekeler üstü iletişim kavramı, kronolojik bakımdan çok kısa olarak kabul edilebilecek bir sürede bir iletişim devrimine imza atmış ve giderek şebekelerle sağlanan çağdaş mobil iletişim hizmetlerinin dahi önüne geçmeye başlamıştır.

* Avukat, İstanbul Medeniyet Üniversitesi, Lisansüstü Eğitim Enstitüsü, Özel Hukuk Ana Bilim Dalı, Bilişim ve Teknolojileri Hukuku Bilim Dalı Mezunu. E-posta: raci@yuksekbas.av.tr , Orcid: 0009-0006-2420-291X

Şebekeler üstü hizmet vasıtasıyla medya aktarımı ve her türlü iletişimin mümkün hale gelmesi karşısında küresel bazda olduğu gibi Türkiye Cumhuriyetinde de buna ilişkin uygulama ve hizmetler yaygınlaşmıştır. Ülkemizde, bu yeni nesil iletişim hizmetinin kamu düzeni, milli güvenlik ve sosyal yapının korunması gibi amaçlarla düzenlenmesi için mevzuat çalışmaları yapılmıştır. Bu bağlamda 5809 sayılı Elektronik Haberleşme Kanunu'nda 7418 sayılı Kanun ile yapılan değişikliklerle şebekeler üstü hizmet ve şebekeler üstü hizmet sağlayıcı kavramları mevzuatımıza dahil olmuştur.

Şebekeler üstü hizmet ve şebekeler üstü hizmet sağlayıcı, Elektronik Haberleşme Kanunu kapsamına alınarak aynı zamanda Bilgi Teknolojileri ve İletişim Kurumu'nun da idari gözetim ve denetimi altına alınmış; hizmet sağlayıcılara çeşitli yükümlülükler, sorumluluklar ve yaptırımlar öngörülmüştür. Bu çalışmamızda, yapılan yeni düzenleme kapsamında şebekeler üstü hizmet kavramı, şebekeler üstü hizmet sağlayıcının yükümlülükleri ve sorumlulukları incelenecek; yeni normların Türk pozitif mevzuatı bakımından değerlendirilmesine gayret edilecektir.

Anahtar Sözcükler: Elektronik Haberleşme, Şebekeler Üstü Hizmet, Telekomünikasyon, Sosyal Medya, İletişim.

AN OVERVIEW OF OVER-THE-TOP SERVICES AND OVER-THE-TOP SERVICE PROVIDERS IN TURKISH LAW

Abstract

After It is observed that internet technology has brought about numerous paradigm shifts on a global scale in the twenty-first century. One of these paradigm shifts is undoubtedly in the field of communication and telecommunications. At the beginning of our century, traditional wired communication has largely given way to wireless mobile communication conducted through networks. With mobile communication operators offering internet services in addition to traditional voice communication, and particularly with the emergence of 3G technology, access to internet technology through mobile phones became possible, leading to the widespread adoption of internet technology across large segments of society. Since the unique nature of internet technology allows the transmission of voice, written, and visual communication, along with other media elements over the internet, the idea of conducting communication via the internet gradually emerged. These ideas were further strengthened by social media companies facilitating the transmission of various media elements between parties without relying on any mobile operator's support and using only the internet.

In this way, the concept of Over-The-Top (OTT) services emerged, where all forms of communication and media transmission are provided to the end user solely over the

internet, without using the network, cable, mobile stations, or any other infrastructure offered by mobile communication operators, and without their intervention. Through mobile applications developed by various companies, such as Facebook Messenger, WhatsApp, Telegram, Discord, and Signal, the concept of OTT services and OTT communication has sparked a communication revolution within a chronologically brief period, progressively surpassing even modern mobile communication services provided through networks.

As media transmission and all forms of communication became possible through OTT services, these services and applications have also gained prevalence in the Republic of Turkey, as they have on a global scale. Legislative efforts have been made in our country to regulate this new generation of communication services for purposes such as maintaining public order, national security, and preserving the social structure. In this context, the concepts of OTT services and OTT service providers have been incorporated into our legislation with amendments to the Electronic Communications Law No. 5809 by Law No. 7418.

The Over-The-Top (OTT) services and OTT service providers have been brought under the scope of the Electronic Communications Law and placed under the administrative oversight and supervision of the Information and Communication Technologies Authority (ICTA). Various obligations, responsibilities, and sanctions have been imposed on service providers. In this study, the concept of OTT services, as well as the obligations and responsibilities of OTT service providers under the new regulation, will be examined, and an effort will be made to assess these new norms in terms of the applicable Turkish legal framework.

Keywords : *Electronic Communications, Over-The-Top (OTT) Services, Telecommunications, Social Media, Communication.*

BUTURUGA V. ROMANIA: İNSAN HAKLARI AVRUPA MAHKEMESİ'NDE SİBER ZORBALIK ADINA YENİ BİR BAŞLANGIÇ

Saba Şahika TAHMAZ ÜZELTÜRK*

Özet

Teknolojinin ortaya çıkmasından beri üzerinde çalışılan siber zorbalığın İnsan Hakları Avrupa Mahkemesi tarafından ilk görünümü olan 2020 tarihli *Buturugă v. Romanya* davası, bu önemli konunun mahkeme nezdinde ele alındığı ilk örnektir. İnsan Hakları Avrupa Sözleşmesi'nin 3. ve 8. maddesi kapsamında ele alınan kararda siber zorbalığın kadın ve kız çocuklarına karşı şiddette kabul edilen bir şiddet türü olduğu ve bu şiddetin özel hayatın siber platformlarda ihlal edilmesi, mağdurun bilgisayarına haksız erişim, veri ve görüntülerin alınması, paylaşılması ve manipülasyonunu içerdiği ortaya konmuş ve karar kilit karar olarak arşivlere girmiştir.

Aile içi şiddet kapsamında ele alınan karar hem 3. maddede düzenlenen "İşkence Yasağı" hükmü hem de 8. maddede düzenlenen "Özel ve Aile Hayatına Saygı Hakkı" bakımından tartışılmıştır. Karara konu olan olayda *Buturugă*, eski eşi hakkında aile içi şiddet ve elektronik yazışmaların gizliliği iddialarıyla Mahkeme'ye başvurmuş ve bu konuda taraf devletin ceza soruşturmalarının yetersiz olduğunu ve kişisel alanının korunmadığını belirtmiştir. Mahkeme, esas itibarıyla taraf devlet olan Romanya'nın pozitif yükümlülüklerini yerine getirmediğini ve bu nedenle Sözleşme'nin 3. ve 8. maddelerini ihlal ettiği sonucuna varmıştır.

Çalışma, siber zorbalığın İHAS ve İHAM içtihatları nezdinde ileride yer alacak sorunları öngörmeye çalışacak ve bunlara bir çözüm bulmayı amaçlayacaktır. Bu kapsamda öncelikle siber zorbalık kavramından ve kapsamından bahsedilecek, daha sonrasında *Buturugă* kararıyla birlikte, peşinden gelen *Volodina v. Rusya* ve kısmen *Giuliano Germano v. İtalya* kararlarından bahsedilecektir. Bu kararların ortaya konmasından sonra, Mahkeme tarafından beklenen ise siber zorbalık kapsamını ne kadar genişleteceği olacaktır. Bu nedenle Mahkemenin siber zorbalığa bakış açısının

* Yeditepe Üniversitesi Hukuk Fakültesi Doktora Bursiyeri, Avukat, ORCID: 0000-0002-5632-7817, sabauzelturk@gmail.com

ne olduğunu hem de ileride hangi boyutlarda çözümler üretmeye başlayacağını değerlendirilecektir.

Anahtar Kelimeler: Siber Zorbalık, İnsan Hakları Avrupa Mahkemesi, İnsan Hakları Avrupa Sözleşmesi, Buturugă v. Romanya, Aile İçi Şiddet

BUTURUGA V. ROMANIA: A NEW BEGINNING FOR THE EUROPEAN COURT OF HUMAN RIGHTS ON CYBERBULLYING

Abstract

Since the emergence of technology, cyberbullying has been studied and the 2020 case of *Buturugă v. Romania* by the European Court of Human Rights is the first example of this important issue being addressed by the Court. Within the scope of Articles 3 and 8 of the European Convention on Human Rights, it was revealed by the Court that cyberbullying is an aspect of violence accepted as violence against women and girls and that this violence includes cyber breaches of privacy, intrusion into the victim's computer and the capture, sharing and manipulation of data and images which led the case to be published as a key case.

The decision, which was addressed within the scope of domestic violence, was discussed both in terms of the "Prohibition of Torture" regulated in Article 3 and the "Right to Respect for Private and Family Life" regulated in Article 8. In the incident that is the subject of the decision, *Buturugă* applied to the Court with allegations of domestic violence and privacy of electronic correspondence against her ex-husband and stated that the criminal investigations of the signatory state in this regard were inadequate and that her personal space was not protected. The Court found that Romania, as a signatory state, had failed to fulfill its positive obligations and was therefore breached Articles 3 and 8 of the Convention.

The study will try to foresee the problems that will take place in the future in terms of the ECHR and ECtHR jurisprudence regarding cyberbullying and will aim to find a solution. In this context, first of all, the concept and scope of cyberbullying will be discussed, and then the *Buturugă* case will be discussed along with the *Volodina v. Russia* case[*] and some parts of the *Giuliano Germano v. Italy* case[**]. After these decisions are presented, the Court will most likely expand the scope of cyberbullying. Therefore, the questions of how the Court views cyberbullying and to what extent it will begin to produce solutions in the future will try to be answered.

Keywords: Cyberbullying, European Court of Human Rights, European Convention on Human Rights, Buturugă v. Romania, Domestic Violence

* *Volodina v. Russia (No.2),* Application no 40419/19, 14.09.2021.
** *Giuliano Germano* v. Italy, Application no. 10794/12, 22.06.2023.

www.bthukukusempozyumu.com

BİLİŞİM VE TEKNOLOJİ HUKUKU DERNEĞİ

İSTANBUL MEDENİYET ÜNİVERSİTESİ