BİLİŞİM VE TEKNOLOJİ HUKUKU DERNEĞİ

İSTANBUL MEDENİYET ÜNİVERSİTESİ

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

BİLDİRİ ÖZETİ KİTABI
ABSTRACT BOOK

19 - 20 - 21 KASIM /NOVEMBER 2022
ISTANBUL

EDİTÖRLER / EDITORS

Dr. Öğr. Üyesi (Asst. Prof. Dr) Şerafettin EKİCİ
Dr. Öğr. Üyesi (Asst. Prof. Dr) Ekrem SOLAK
Av. (Atty) Muhammed Emre AVŞAR

www.bthukukusempozyumu.com

BİLİŞİM VE TEKNOLOJİ HUKUKU DERNEĞİ

İSTANBUL MEDENİYET ÜNİVERSİTESİ

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

19 – 20 – 21 Kasım /November 2022

ISTANBUL

BİLDİRİ ÖZETİ KİTABI
ABSTRACT BOOK

EDİTÖRLER / EDITORS
Dr. Öğr. Üyesi (Asst. Prof. Dr) Şerafettin EKİCİ
Dr. Öğr. Üyesi (Asst. Prof. Dr) Ekrem SOLAK
Av. (Atty) Muhammed Emre AVŞAR

ISTANBUL / 2022

ISBN: 978-605-72218-1-0

SUNUŞ

Bilişim Ve Teknoloji Hukuku Derneği ile İstanbul Medeniyet Üniversitesi işbirliği ile düzenlenmiş olan II. Uluslararası Bilişim Ve Teknoloji Hukuku Sempozyumu, 19 – 20 – 21 Kasım 2021 tarihlerinde İstanbul'da gerçekleştirilmiştir.

Sempozyum'da, Türkiye'den on dokuz ve yurt dışından beş üniversite olmak üzere yirmidört farklı üniversiteden ve iş dünyasından, toplam altmışdört konuşmacı ve oturum başkanı akademik katkı sunmuştur.

Sempozyumda sunulan akademik tebliğlerin özetlerinden oluşan bu özet kitabın, bilişim hukuku camiasına ve ülkemize hayırlı olmasını diler, Sempozyum'a sunumları ile katkı yapan tüm katılımcılarımıza teşekkür ederiz.

PRESENTATION

The II. International Informatics and Technology Law Symposium, organized in cooperation with the Informatics and Technology Law Association and Istanbul Medeniyet University, was held in Istanbul on 19 - 20 - 21 November 2021.

In the Symposium, a total of sixty-four speakers and session chairmen from twenty-four different universities, nineteen from Turkey and five from abroad, and from the business world, made academic contributions.

We wish that this abstract book, which consists of abstracts of academic papers presented at the symposium, will be beneficial to the informatics law community and our country, and we would like to thank all our participants who contributed to the Symposium with their presentations.

EDİTÖRLER / EDITORS
Dr. Öğr. Üyesi (Asst. Prof. Dr) Şerafettin EKİCİ
Dr. Öğr. Üyesi (Asst. Prof. Dr) Ekrem SOLAK
Av. (Atty) Muhammed Emre AVŞAR

İÇİNDEKİLER

SUNUŞ / PRESENTATION 3
DÜZENLEME KURULU / ORGANIZING COMMITTEE..... 9
BİLİM VE HAKEM KURULU / SCIENTIFIC AND REFEREE COMMITTEE.....11

DİJİTALLEŞMENİN GETİRDİĞİ TELİF SORUNLARI VE ÇARE ARAYIŞLARI
Cahit SULUK 13

NFT'LERİN BİLET OLARAK KULLANILMASININ HUKUKİ DEĞERLENDİRMESİ
Dr. Süleyman KIRAN 15

YAPAY ZEKÂNIN ÜRETTİĞİ TASARIMLARDA HUKUKİ SORUMLULUK
Hasan Kadir YILMAZTEKİN 17

ELEKTRONİK KIYMETLİ EVRAK VE HUKUKİ NİTELİĞİ- ALMAN, İSVİÇRE VE TÜRK HUKUKU İLE KARŞILAŞTIRMALI BİR DEĞERLENDİRİLME
Doç. Dr. Emrullah KERVANKIRAN 21

GEMİ TİCARETİNDE KRİPTO PARA BİRİMİ KULANILMASI
Doç. Dr. Hacı KARA 25

GAYRİMENKUL SERTİFİKASI VE KİRA SERTİFİKALARININ AKILLI SÖZLEŞMELERLE ARACISIZ DEVRİNİN BİNA İNŞAAT MALİYETLERİNİN FİNANSMANINA VE MÜLKİYET HAKKI DEVRİNE ETKİSİ VE VERGİ AVANTAJLARI
Memduh ASLAN 29

DAO'LARIN MASAK MEVZUATI VE ADİ ŞİRKET HÜKÜMLERİ AÇISINDAN DEĞERLENDİRİLMESİ
Av. Cemal ARAALAN 35

MEDENİ USUL HUKUKUNDA YARGILAMANIN HIZLANDIRILMASI VE ADALETE ERİŞİM HAKKI BAKIMINDAN ÇEVRİM İÇİ MAHKEMELER VE YAPAY ZEKANIN KULLANIMI
Gökçe KARABEL - Dilek AYDEMİR 41

YAPAY ZEKÂNIN CEZA MUHAKEMESİNDE İDDİA VE HÜKÜM MAKAMINDA BULUNMASINA İLİŞKİN DÜŞÜNCELER
Dr. Şaban Cankat TAŞKIN 45

YARGI KARARLARININ GEREKÇELENDİRİLMESİNDE YAPAY ZEKANIN ROLÜ
Mehmet ÇATLI 47

BLOKZİNCİR TEKNOLOJİSİNDEKİ VERİLERİN DELİL NİTELİĞİNİN HUKUK YARGILAMASI BAKIMINDAN İNCELENMESİ
Dr. Elif Irmak BÜYÜK 49

BİLİŞİM TEKNOLOJİSİNDE BİR SUİSTİMAL ÖRNEĞİ: BİLİŞİM SİSTEMLERİNİN KULLANILMASI SURETİYLE DOLANDIRICILIK SUÇLARI
Ali Tanju SARIGÜL 51

TÜRK CEZA HUKUKUNDA YENİ BİR SUÇ TİPİ OLARAK BİLİŞİM SİSTEMLERİ ARACILIĞIYLA İŞLENEN ISRARLI TAKİP SUÇU
Dr. Öğr. Üyesi Nurten ÖZTÜRK 55

"BİLİŞİM YOLUYLA" SUÇTAN KAYNAKLANAN MALVARLIĞI DEĞERLERİNİN AKLANMASI SUÇUNA GÜNCEL BİR ÖRNEK: TWITCH BIT SCAM OLAYLARI
Arş. Gör. İlkay ELBEY 59

KRİPTO PARA MADENCİLİĞİ VE CEZA HUKUKU SORUMLULUĞU
Osman Gazi ÜNAL 63

ÇOCUKLARIN SİBER ALANDA CİNSEL AMAÇLAR İÇİN TEŞVİKİ (CYBER-GROOMING)
Prof. Dr. E. Eylem AKSOY RETORNAZ 65

SOSYAL MEDYANIN DEZENFORMASYONLA İMTİHANI
Güneş OKUYUCU ERGÜN 67

SİBER ZORBALIKLA MÜCADELEDE YENİ ARAYIŞLAR: OKULLARDA ONARICI ADALET MEKANİZMALARININ KULLANILMASI
Zeynep ARDIÇ 71

BİR SOSYAL MÜHENDİSLİK YÖNTEMİ OLARAK PHISHING (OLTA AVCILIĞI)
Veysel TOPUZ 75

KİŞİSEL VERİLERE İLİŞKİN ÖNEMLİ KORUMA: DİJİTAL TEHDİTLER KARŞISINDA ÇOCUK
Şevval Ceyhan - Özge Demirdelen 79

SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ YÖNETİMİNE DAİR DÜZENLEMELERE GENEL BİR BAKIŞ
Alper IŞIK 81

PLATFORM REGÜLASYONU VE AVRUPA BİRLİĞİ DİJİTAL PİYASALAR DÜZENLEMESİ (DIGITAL MARKET ACT) ÜZERİNE DEĞERLENDİRMELER
Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK 85

KRİPTO VARLIK PİYASALARINA İLİŞKİN AB TÜZÜK TEKLİFİ ve MEVZUATIMIZ İÇİN DÜZENLEME ÖNERİLERİ
Av. Deniz BAYTEMÜR KÖKSAL 89

KARŞILAŞTIRMALI HUKUKTAKİ GELİŞMELER IŞIĞINDA DEEPFAKE TEKNOLOJİSİNİN REGÜLASYONU VE TÜRK HUKUKU İÇİN ÖNERİLER
Sinem ÖZYİĞİT 93

VERGİ İDARESİNİN DİJİTAL DÖNÜŞÜMÜ
Ahmet Emrah GEÇER 97

DİJİTAL PAZARLAMA VE SATIŞ YOLU İLE KAZANÇLARIN VERGİLENDİRİLMESİ VE GÜNCEL GELİŞMELER
Arzu KALYON 101

GELİR VERGİSİ VE KURUMLAR VERGİSİ YÖNÜNDEN HİZMET OLARAK YAZILIM (SAAS) ÖDEMELERİNİN NİTELENDİRİLMESİ
Alperen Asım KORUK 103

YAPAY ZEKÂ ÜZERİNDEN GERÇEKLEŞTİRİLEN İRADE AÇIKLAMALARININ İRADE ÖZERKLİĞİ KAPSAMINDA AÇIKLANABİLİRLİĞİ SORUNU
Mustafa AKSU 107

OTONOM SİLAH SİSTEMLERİ VE CEZA SORUMLULUĞU
Murat BALCI 113

YAPAY ZEKA DESTEKLİ SİLAHLARIN HUKUKSAL YAPISI
Av. Dr. Ahmet Çağrı YILMAZ 115

AVRUPA KOMİSYONU'NUN YAPAY ZEKADA SÖZLEŞME DIŞI SORUMLULUĞA İLİŞKİN 28.9.2022 TARİHLİ ÖNERİSİNİN DEĞERLENDİRİLMESİ
Halil Emre GÜRLER 119

HUKUKTA YAPAY ZEKA KULLANIMI - HAKİM YAPAY ZEKA
Salih KARADENİZ 123

THE MAIN CHALLENGES OF E-ELECTIONS: PROS AND CONS (Case Study of Georgia)
Prof. Dr. Mariam JIKIA 125

LEGAL FIGHT AGAINST RANSOMWARE-RELATED CRIMES IN THE UNITED STATES
Kerime TOPRAK 127

THE ROLE OF IT IN ACTIVATING ANTICORRUPTION POTENTIAL OF CIVIL SOCIETY
Dr. Roza JUMABEKOVA - Dr. Bagdat AUYESHOVA 129

AMERİKAN HUKUKUNDA SOSYAL MEDYA PLATFORMLARININ DÜZENLENME VE DENETLENME SORUNSALI
Dr. Samet TATAR 131

ARTIFICIAL INTELLIGENCE IN DIGITAL ECONOMY FROM INDONESIA INTEREST IN MULTIDISCPLINARY APPROACH
Firdausi FIRDAUS 135

DİJİTAL VARLIKLARIN KORUNMASI VE ULUSLARARASI YATIRIM HUKUKU
Neriman KILIÇ 137

ELEKTRONİK DEFTER, BEYANNAME VE FATURALAR ÜZERİNDEN TRANSFER FİYATLANDIRMASINA YÖNELİK EMSAL VERİ TABANI OLUŞTURULMASI
Arş. Gör. Simay DOĞMUŞ 139

SUSTAINABILITY AND DIGITALISATION: CHALLENGES AND OPPORTUNITIES FOR CORPORATE GOVERNANCE
Meltem KARATEPE KAYA 143

THE ASSESSMENT OF THE EU PRODUCT LIABILITY REGIME IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE AND RELATED EMERGING TECHNOLOGIES: A NEW ERA?
Furkan BULUT 145

CAN ARTIFICIAL INTELLIGENCE (AI) BE AN INVENTOR? AN INTERNATIONAL ANALYSIS IN LIGHT OF 'DABUS' DECISIONS
Fatmanur CEBECİ ÇORUM 149

DÜZENLEME KURULU
ORGANIZING COMMITTEE

Dr. Öğr. Üyesi Şerafettin EKİCİ *Asst. Prof. Dr. Serafettin EKICI*	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi *Istanbul Medeniyet University Faculty of Law*
Dr. Öğr. Üyesi Ekrem SOLAK *Asst. Prof. Dr. Ekrem SOLAK*	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi *Istanbul Medeniyet University Faculty of Law*
Av. Muhammed Emre AVŞAR *Atty. Muhammed Emre AVSAR*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Dr. Öğr. Üyesi Sezen KAMA IŞIK *Asst. Prof. Dr. Sezen KAMA ISIK*	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi *Istanbul Medeniyet University Faculty of Law*
Dr. Öğr. Üyesi Serkan KAYA *Asst. Prof. Dr. Serkan KAYA*	Boğaziçi Üniversitesi Hukuk Fakültesi *Bogazici University Faculty of Law*
Dr. Öğr. Üyesi Dilek AYDEMİR *Asst. Prof. Dr. Dilek AYDEMİR*	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi *Istanbul Medeniyet University Faculty of Law*
Dr. Öğr. Üyesi Meltem KAYA *Asst. Prof. Dr. Meltem KAYA*	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi *Istanbul Medeniyet University Faculty of Law*
Dr. Öğr. Üyesi Ahmet Emrah GEÇER *Asst. Prof. Dr. Ahmet Emrah GECER*	İstanbul Medeniyet Üniversitesi Hukuk Fakültesi *Istanbul Medeniyet University Faculty of Law*
Av. Adem GÜL *Atty. Adem GUL*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Av. Büşra ÖZELLİBEŞ *Atty. Busra OZELLIBES*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Av. Büşra ALTUNAY *Atty. Busra ALTUNAY*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Av. Mehmet Melih GÜLSEREN *Atty. Mehmet Melih GÜLSEREN*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Av. Bahar ÖTE *Atty. Bahar OTE*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Av. Raci Çetin YÜKSEKBAŞ *Atty. Raci Cetin YUKSEKBAS*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Av. Ahmet Semih BAŞYİĞİT *Atty. Ahmet Semih BASYIGIT*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*
Av. Ali ERŞİN *Atty. Ali ERSIN*	Bilişim ve Teknoloji Hukuku Derneği *IT Law Society*

BİLİM VE HAKEM KURULU
SCIENTIFIC AND REFEREE COMMITTEE

DİJİTALLEŞMENİN GETİRDİĞİ TELİF SORUNLARI VE ÇARE ARAYIŞLARI

Cahit SULUK*

ÖZET

Fikri ürünlerin hukuken korunması 13. yüzyıldaki imtiyazlara kadar eskiye dayanır. Ancak modern anlamda yasa koyucular sanayileşmeyle birlikte fikri ürünleri hukuken koruma altına almaya başlamıştır. Bu çerçevede ilim-edebiyat, müzik, senama ve güzel sanat eserleri telif yasalarıyla korunmaktadır. *Münhasır nitelikteki bu koruma* modeli günümüzün şartlarıyla örtüşmemektedir. Şöyle ki bilgi çağını idrak ettiğimiz bugünlerde fikri ürünler dijitalleşti ve bu durum yeni telif sorunlarını beraberinde getirdi.

Son yıllarda takipçisi olduğumuz AB'de bu soruna ilişkin çare arayışları hız kazandı. Bu çerçevede pek çok analiz, rapor, akademik ve yasal çalışma yürütülmektedir. Yasal çalışmaların bazıları sonuçlandırılmıştır. Bunlar arasında 2019/790 sayılı Dijital Tek Pazar Yönergesi dikkat çekicidir. Ancak çalışmalar bu yönergeyle sınırlı olmayıp dijital içerik korumasına yönelik başkaca metinler de hazırlanmaktadır. Bu çare arayışları telif hukukumuzu da doğrudan etkilemektedir. Çünkü aday bir ülke olarak Türkiye, AB müktesebatını iç hukukuna peyder pey aktarmaktadır.

Tebliğde, bilişim teknolojilerindeki gelişmelerin çıkardığı telif sorunları ve bu sorunlara yönelik özellikle AB ve Türk hukukunda çare arayışları üzerinde durulacaktır.

Anahtar Sözcükler: Bilişim Hukuku, Telif Hakları, Dijitalleşme ve Telif Sorunları, AB ve Türk Hukukunda Çare Arayışları.

COPYRIGHT ISSUES RAISED BY DIGITALIZATION AND SEARCH FOR REMEDIES

ABSTRACT

Legal protection of intellectual products goes back to privileges granted in the 13th century. However, in the modern sense, the legal protection of intellectual products by legislators starts with the industrial revolution. In this context, works of science-

* Doç. Dr., İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, Orcid: https://orcid.org/0000-0002-8952-9247 suluk@suluk.com.tr

literature, music, script and fine arts are protected by copyright laws. This *exclusive protection* model does not align with today's conditions. In other words, in this age of information, intellectual products have become digital, which has brought new copyright problems.

We have been following the developments in the EU in recent years, where the search for a solution to this problem has gained momentum. In this framework, the EU carries out various analyses, reports, academic and legal studies. Some of the legal studies have been finalized. Among them, the Digital Single Market Directive No. 2019/790 is noteworthy. However, the studies are not limited to this directive, and other texts for content protection are also being prepared. This search for remedies directly affects the Turkish copyright law since Turkey, as a candidate country, gradually transfers the EU acquis to its domestic law.

This paper will emphasize copyright issues caused by the developments in information technologies as well as the search for solutions for these problems, especially in the EU and Turkish law.

Keywords: IT Law, Copyright, Digitalization and Copyright Issues, Remedies in EU and Turkish Law.

NFT'LERİN BİLET OLARAK KULLANILMASININ HUKUKİ DEĞERLENDİRMESİ

Dr. Süleyman KIRAN*

ÖZET

Kripto varlıklar kısa zaman içinde Dünya'da olduğu gibi Türkiye'de geniş bir kullanıcı çevresine kavuşmuştur. Bu ise, hukuki ilişkilerin düzenlenmesi ihtiyacını doğurmuştur. 30/4/2021 tarihinde yürürlüğe giren Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik ile Türkiye'de ödemelerde kripto varlık kullanılması yasaklanmıştır.

Bir kripto varlık türü olan NFT (Non-Fungible Token)'lar ise son günlerde bir hayli öne çıkmaktadır. NFT'ler blok zincir teknolojisi kullanılarak herhangi bir şeyin türünün tek örneği olduğunu ispat edici niteliği haiz kriptografik dijital varlıklardır. Diğer kripto varlıklarda olduğu gibi el değiştirebilmeleri mümkündür. Sanat alanında yoğun bir şekilde görünür olmuşlardır. Bununla birlikte, kullanım alanları sanat ile sınırlı değildir.

Konser, festival veya spor müsabakası etkinliklerinin biletlerinin NFT olarak satılmasının bazı avantajları bulunmaktadır. Şöyle ki; NFT biletleri satın alan seyirciler/ katılımcılar/ taraftarlar, bu biletlerin hem orijinal olduğunu hem de meşru bir organizatör tarafından satıldığını anlayabileceklerdir. Biletler ikinci el piyasasında NFT olarak satıldığında organizatörler, mekân, sanatçılar ve sporcular belli bir oranda komisyon kazanabilecektir. Bazı NFT'ler ile birtakım imtiyazlara sahip olunabilecektir. Bu biletlerin konser alanında bazı ayrıcalıklı yerlere girme ya da sevdiğiniz sanatçıdan imzalı bir poster edinme gibi imkanlar sunabilecektir. Ayrıca bu NFT'ler sahiplerine aralarında yapılacak bir çekilişle, mekânda kullanılacak bir hediye çeki veya konser sonrası kulis ziyareti gibi heyecan verici imkânlar sağlayabilecektir. Bunlara ek olarak NFT biletler; konaklama, uçak ya da otobüs bileti ve araç kiralama gibi üçüncü parti hizmetlere de imkân verebilir. Bu örnekleri arttırabilmek mümkündür. Tüm bu avantajlara karşısında, NFT biletlerin kullanılması ve halde hukuki değerlendirilmesinin yapılması kaçınılmazdır.

Anılan yönetmelik, kripto varlıkların "ödeme" için kullanılmasını yasaklamaktadır. Bu halde biletin hukuki niteliğinin tespiti uygun olacaktır. Biletin hukuki niteliğinin tespitinden sonra NFT olarak basılmasının önünde hukuki bir engel olup olmadığı

* AnCom Hukuk & Danışmanlık, skiran@ancomlaw.com, ORCID: 0000-0003-4784-6233

hususu bildiride temel inceleme konusu olacaktır. Hukuki bir engel olduğu sonucuna varılırsa bunlara ilişkin çözüm önerilerinde bulunulması hedeflenmektedir.

Anahtar Kelimeler: NFT, Kripto Varlık, Blokzincir, Bilet, Ödeme.

LEGAL EVALUATION OF USING NFTS AS TICKETS

ABSTRACT

Crypto assets have gained a wide user base in Turkey as well as in the world in a short time. This has led to the need to regulate legal relations. With the Regulation on the Non-Use of Crypto Assets in Payments, which entered into force on 30/4/2021, the use of crypto assets in payments is prohibited in Turkey.

NFT (Non-Fungible Token), a type of crypto asset, has come to the fore in recent days. NFTs are cryptographic digital assets that can prove that anything is one-of-a-kind using blockchain technology. Like other crypto assets, they can change hands. They have been intensely visible in the field of art. However, its uses are not limited to art.

There are some advantages to selling tickets for concerts, festivals or sporting events as NFTs. Namely; Spectators/participants/fans who purchase NFT tickets will be able to understand that these tickets are both original and sold by a legitimate organizer. Organizers, venues, artists and athletes will be able to earn a commission at a certain rate when tickets are sold as NFT on the second-hand market. With some NFTs some privileges may be obtained. These tickets will offer opportunities such as entering some privileged places in the concert venue or obtaining a signed poster from your favorite artist. In addition, these NFTs will be able to provide their owners with exciting opportunities such as a gift certificate to be used in the venue or a backstage visit after the concert, through a lottery. In addition to these, NFT tickets; It may also provide third-party services such as accommodation, flight or bus tickets, and car rental. It is possible to increase these examples. In the face of all these advantages, it is inevitable to use NFT tickets and make a legal evaluation.

The regulation prohibits the use of crypto assets for “payment” purposes. In this case, it would be appropriate to determine the legal nature of the ticket. After determining the legal nature of the ticket, the issue of whether there is a legal obstacle to printing it as NFT will be the main issue in our examination. If it is concluded that there is a legal obstacle, it is aimed to propose solutions to them.

Keywords: NFT, Cryptoasset, Blockchain, Ticket, Payment.

YAPAY ZEKÂNIN ÜRETTİĞİ TASARIMLARDA HUKUKİ SORUMLULUK

Hasan Kadir YILMAZTEKİN*

ÖZET

Yapay zekânın, günümüzde, hayatın içinde geniş ve önemli bir yer tuttuğu artık kabul edilen bir olgudur. Yapay zekâ teknolojileri, birkaç sert kışın ardından, bugün, konunun uzmanı olan ve olmayan tüm herkesin ilgisini çekmektedir. Herkesin gündeminde olan yapay zekâ ne anlama gelmektedir?

Yapay zekâ kavramı, ilk duyulduğunda, genellikle fütüristik temalar düşünülmektedir. Mesela, insan dostu androidler veya katil robotlar gibi bilim kurgu tasvirleri akıllara gelmektedir. Fakat yapay zekâ, "belirli bir çevrede var olan, hareket eden ve algılayan öznelerin incelendiği" bir alan olarak görüldüğü takdirde, çok daha geniş bir bilim ve teknoloji alanı olarak kabul etmek ve gündelik hayatımıza tesir eden birçok uygulamadan bahsetmek mümkün olmaktadır. Apple'ın Siri'sinden Tesla'nın sürücüsüz arabasına, güvenlik kameralarına yerleştirilen yüz tanıma sistemlerinden Amazon'un Alexa'sına, Netflix'in film tavsiye eden sistemlerinden Google'ın arama motoruna kadar uzanan yapay zekâ taşıyan araçlarla donatılmış bir dünyada yaşandığı artık bilinmektedir.

Yapay zekâ ile çalışan teknolojinin varlığı, hayatı giderek artan bir şekilde kolaylaştırmaktadır. Yapay zekâ, aynı zamanda sunduğu teknolojik yeniliklerle, ekonomiyi ve insan refahını şekillendirmektedir. Bu teknolojiler, üretim verimliliğini artırıcı ve aynı zamanda maliyeti azaltıcı araçlar olarak kullanılmaktadır. Bu özelliği sebebiyle, yapay zekâ destekli ticari sektörler gittikçe daha da yaygınlaşmaktadır. Tanı tıbbı, taşıma, yatırım, terapi, istihbarat toplama, alternatif uyuşmazlık çözme, sözleşme hazırlama, millî savunma, bankacılık ve daha birçok benzer alanda yapay zekânın giderek artan bir rol oynadığını görmek mümkündür. Hatta bu sistemlerin gelişimine ekonomik anlamda ciddi kabul edilebilecek yatırımlar yapılmaktadır.

Yapay zekâya bu ikinci baharı getiren çeşitli sebepler bulunmaktadır. Makine öğrenmesi alanında son zamanlarda büyük gelişmeler kaydedilmiştir. Büyük verinin elde edilebilirliği ve muazzam büyüklükteki hacmi, yapay zekâ sistemlerinin eğitimini kolaylaştırmıştır. Bilgisayar işlemcilerinin hızları fevkalade artmıştır. Bulut depolama

* Hâkim, Dış İlişkiler Dairesi Başkanı, Türkiye Adalet Akademisi, Fikrî Mülkiyet Hukuku Doçenti, hkytekin@gmail.com, https://orcid.org/0000-0003-1050-4272.
Judge, Head of Department of Foreign Relations, Justice Academy of Türkiye, Associate Professor of IP Law. hkytekin@gmail.com, https://orcid.org/0000-0003-1050-4272.

sistemleri, bu verileri depolamak için devasa alanlar sunmaktadır. Artık internete erişmek ise çok daha kolay ve hızlıdır.

Yapay zekâ, beraberinde bazı sorunları da getirmektedir. Yükselen bu yeni teknolojiler, kamusal tartışmaların ve siyasi endişelerin merkezinde yer almaktadır. Toplumun bazı kesimleri, endişelerini yüksek sesle "robotlar dünyayı ele geçiriyor." şeklinde dile getirmektedir.

Moda endüstrisi, yapay zekâdan en çok etkilenen alanlar olarak karşımıza çıkmaktadır. Günümüzde yapay zekâ teknolojileri, fikrî mülkiyet hukukunun konusu olabilecek birçok tasarım meydana getirebilmektedir.

Yapay zekâ taşıyan araçlar ve cihazlar, moda endüstrisinde manken, kumaş ve giysi tasarımı için günümüzde yaygın bir biçimde kullanılıyor.

Yapay zekâ ile oluşturulan tasarımlardan bahsettiğimizde, aslında tasarımcının kim olduğuna dikkat edilmemektedir. Daha çok satan kıyafetler, daha çok rağbet gören ve moda olan tasarımlar ve müşteri beklentilerini karşılamak gibi, inovasyonun meyvelerine odaklanılmaktadır. Tasarımcılar, ürünlerini satışa arz etmeden önce kıyafet ve aksesuarın her bir parçasını tasarlarken veya yaratırken çok fazla emek, yetenek, zaman ve para harcarlar. Gerçekten bir moda endüstrisinde bir tasarım oluşturmak, zahmetli bir süreçtir. Model taslağı oluşturmak kıyafet yapımında ilk ve en önemli adımdır. Tasarımcı, moda tasarımına kağıt üzerinde genel bir taslak çizerek başlar; buna stiller, elementler ve renkleri ekler; her şeyi gözden geçirir ve rötuşlar yapar ve son olarak tasarımını terzilere teslim eder. Yapay zekâ, bu zahmetli ve zaman alıcı süreci hızlandırır. Üretici ters ağlar (*generative adversial networks*) olarak bilinen bir yapay zekâ tekniği yardımıyla kıyafet tasarımlarını yeniden şekillendirmeyi hedefleyen moda markası the Fabricant buna örnek olarak gösterebiliriz.

Moda endüstrisinde yapay zekânın verimlilik özelliğine odaklanıldığından genellikle yaptığı tasarımların hukukî sonuçları göz ardı edilmektedir. Bir yapay zekânın moda tasarımlarını yaratmadaki kapasitesi ve kabiliyeti, meydana getirdiği moda tasarımlarının başkasının tasarımlarına saldırı teşkil etmesi hâlinde kimin sorumlu olacağı sorusunu gündeme getirmektedir. Yapay zekâ taşıyan cihaz programcısıyla sözleşme yapan moda tasarımcısı mı sorumlu olacaktır? Programcı mı olacaktır? Yoksa yapay zekâ cihazının kendisi mi olacaktır? Veya o tasarım ortak bir saldırı mı teşkil edecektir?

Bu çalışmada, yapay zekâ tarafından meydana getirilen tasarımların yol açtığı saldırı hâllerinde kimlerin sorumlu olacağı konusu AB ve Türk hukuku bağlamında ele alacaktır.

Çalışmada özellikle, yapay zekâ tarafından meydana getirilen tasarımlarda, bu teknolojiler etrafındaki ilgili "insan" aktörlerden kimlerin sorumlu olabileceklerini tespit etmek için bir çözüm yöntemi ve model bir hukuk normu önerilmektedir.

Anahtar kelimeler: Tasarımlar, yapay zekâ, sorumluluk, moda, fikrî mülkiyet.

CIVIL LIABILITY DERIVING FROM AI-GENERATED DESIGNS

Artificial intelligence (AI) now infiltrates our culture. After a couple of difficult winters, AI today is a word on everybody's lips, and it attracts everyone's attention regardless of whether they are experts or not. What does AI that is on the everyone's agenda mean?

When we think of the notion of AI, we generally tend to associate it with futuristic themes. For instance, science fiction depictions such as killer robots or human-friendly androids come to our minds. However, if we see AI as 'the study of agents that exist in an environment and perceive and act,' it is possible to consider it as a much broader field of science and technology and to talk about many applications that have an impact on our daily lives. From Apple's Siri to Amazon's Alexa, Tesla's auto-driving cars to facial recognition systems in CCTV cameras, Netflix's film offering services to Google's search engine, we live in a world of AI goods.

The advent of AI-powered technologies increasingly affects people's lives across the globe. As a tool for productivity and cost-efficiency, AI also shapes our economy and welfare. AI-assisted commercial industries are becoming more and more common. It is possible to see that AI increasingly plays an important role in diagnostic medicine, transportation, investment, therapy, intelligence, alternative dispute resolution, contracts, national defence, banking and many other similar fields. Substantial economic investments have been channelled into the development of these technologies.

There are various reasons that have paved the way for another spring for AI. Remarkable innovations have recently been made in the field of machine learning. The availability and the enormous volume of big data has facilitated the training of AI systems. The speed of computer processors has exponentially increased. Cloud storage systems offer huge areas to manage this data. Internet access is now much easier and faster.

However, AI does not come without any problems. The upsurge of these novel technologies is at the centre of public debate and policy considerations. Some segments of the society have vocally raised their concern that 'robots are taking over.'

Fashion is one of the industries that AI can profoundly impact. AI tools and devices are currently being used in the fashion industry to create fashion models, fabric and jewellery designs, and clothing.

When we talk about AI-generated designs, we instead focus on the fruits of innovation –more best-selling apparels, more fashionable designs and more fulfilment of customer expectations – without paying heed to who the designer is. Designers invest a lot of talent, time and finances in designing and creating each article of clothing and accessory before they release their work to the public. Pattern drafting is the first and most important step in dressmaking. Designers typically start with a general sketch on paper; add styles, elements and colours; revise and refine everything; and finally

deliver their design to dressmakers. AI accelerates this time-consuming and labour-intensive process. The Fabricant, which aims at redesigning fashion designs with tha AI technique called generative adversial networks, can be shown as an example to this.

When only focussed on efficiency of AI systems, its full legal consequences in fashion industry are often forgotten. An AI device's ability to generate fashion designs raises the question of who will be liable for infringement deriving from use of third-party material in AI-generated fashion designs. Will it be the fashion designer who hires or contracts with the AI programmer? Will it be the programmer? Will it be the AI itself? Or will humans and computers be jointly liable?

This study examines the question of who would be held liable for AI-generated designs when they cause infringement within the context of EU and Turkish laws.

More specifically, in this study, a three-step test, which could be used to unleash the "human" infringers (actors) around AI-generated fashion designs, and a model norm will be proposed.

Key words: Designs, artificial intelligence, liability, fashion, intellectual property.

ELEKTRONİK KIYMETLİ EVRAK VE HUKUKİ NİTELİĞİ- ALMAN, İSVİÇRE VE TÜRK HUKUKU İLE KARŞILAŞTIRMALI BİR DEĞERLENDİRİLME

Doç. Dr. Emrullah KERVANKIRAN*

ÖZET

Teknolojinin baş döndürücü bir hızla ilerlediği ve her geçen gün insan yaşamını ve toplumsal hayatı derinden etkilediği günümüz dünyasında, hukuk kurallarının da teknolojik gelişmelere kayıtsız kalamayacağı görülmüş ve ülke mevzuatları hızla dijitalleşmeye doğru evrilmeye başlamıştır. Dünyadaki bu gelişmelere paralel olarak, son yıllarda ülkemizdeki mevzuat çalışmaları da teknolojik gelişmeler ekseninde yürütülmekte, kanunlarımızda dijitalleşmenin etkisi kendisini önemli ölçüde hissettirmektedir. Bütün dünyada ticari hayatın temel ve vazgeçilmez unsurlarından birisi olan Kıymetli Evrak Hukuku' da bu gelişmelerden nasibini almaya başlamıştır. Bu alanda çıkarılmış olan önemli kanunlardan birisi Almanya'da 03.06.2021 tarihinde yürürlüğe giren "Elektronik Kıymetli Evrak Hukuku" dur (Gesetz über elektronische Wertpapiere- eWpG). Diğer bir kanun ise 01.08.2021 tarihinde yürürlüğe giren ve birden fazla hukuk dalını elektronik kayıt sisteminde yer vererek, bunların birbiriyle uyumunu düzenleyen Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technick verteilter elektronischer Register adlı kanundur. Ülkemizde ise benzer bir çalışma 2015 yılından itibaren Türkiye Bankalar Birliği'nin çatısı altında hazırlanmış ve yasalaşarak 1 Ocak 2020 tarihinde yürürlüğü girmesi beklenmekte iken, şimdiye kadar henüz TBMM'nin gündemine getirilmemiş olan Elektronik Çek ve Bono Kanunu Tasarısı'dır.

Ülkemizde böyle bir kanun tasarısının yapılmasının amacı, elektronik çek ve bono sisteminin oluşturulması ile kayıt dışı ekonomiyle etkin bir mücadele aracına kavuşulmuş olması yanında, çek ve bononun sahteciliğe konu edilmesinin önlenmesi, teknolojinin sunduğu imkânlar ile çek ve bononun tüm tedavül sürecinin ilgililer tarafından izlenebilmesi ve böylece piyasada çek ve bonoya olan güvenin artırılması hedeflenmektedir. Dolaysıyla bu haliyle tasarıda yeni kıymetli evrak türleri icat edilerek yeni ödeme ve kredi araçları meydana getirilmiş değildir. Yeni kanun tasarısı ile Türk Ticaret Kanunu ve Çek Kanunu'nda düzenlenmiş olan çek ve bononun teknoloji yardımıyla elektronik ortamda düzenlenmesi, devredilmesi ve ödenmesi söz

* İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Ticaret Hukuku Anabilim Dalı, emrullah.kervankiran@medeniyet.edu.tr, ORCID-ID: 0000-0002-3704-7887

konusu olmakta, böylelikle klasik çek ve bono varlığını korumakla beraber bir dijital dönüşüme uğramaktadır. Ancak, her ne kadar bu alanda bir dijitalleşme kaçınılmaz olsa da, elektronik kıymetli evrakın hukuk niteliği, şimdiye kadar genel geçer kıymetli evrak teorisi ile açıklanamamaktadır.

Diğer taraftan, son yıllarda karşılıksız çıkan çeklerin sayısının artması ve bunlar için öngörülen yaptırımların yetersizliği, toplumda çeke duyulan güvenin sarsılmasına yol açmış, bu durum karşısında çeke duyulan güveni artırmaya yönelik yeni yasal düzenlemeler yapılması ihtiyacı ortaya çıkmıştır. Bu doğrultuda 09.08.2016 tarihinde yürürlüğe giren 6728 sayılı *Yatırım Ortamının İyileştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılmasına İlişkin Kanun* ile çeklerin karşılıksız çıkmasına ve çeke duyulan güvenin artırılmasına yönelik tedbirler alınmıştır. Bu kanun kapsamında kabul edilen karekodlu çek uygulaması ile çekin dijitalleşmesi sürecine ilişkin önemli bir adım atıldığı söylenebilir.

Açıklanan nedenlerle çek ve bononun teknoloji temelinde yeniden ele alınması ihtiyacı ortaya çıkmış, elektronik çek ve bono uygulamasının hayata geçirilmesiyle bir taraftan uygulamada karşılaşılan karşılıksız çek, çekte sahtecilik ve kayıt dışılık gibi sorunların önüne geçilebileceği düşünülmüş, diğer taraftan da çek ve bononun tedavül yeteneğinin daha da artırılması ve takibinin kolaylaştırılması hedeflenmiştir. Bu tebliğ kapsamında, Alman, İsviçre ve Türk hukukundaki düzenlemelere mukayeseli olarak yer verilerek, kıymetli evrakın genel geçer klasik ilkeleri ile uyumlu olup olmadıkları inceleme konusu yapılacaktır.

Anahtar Kelimeler: elektronik çek, elektronik bono, kıymetli evrak, dijitalleşme, kare kodlu çek

ELECTRONIC NEGOTIABLE INSTRUMENTS AND LEGAL NATURE OF ELECTRONIC NEGOTIABLE INSTRUMENTS A COMPARATIVE STUDY WITH GERMAN, SWISS AND TURKISH LAW

ABSTRACT

In today's world, it is a well-known fact that technology is advancing at a rapid pace and affecting human and social life more deeply with each passing day. It has been observed by many judicial systems in the world that the rules of law cannot remain indifferent to technological developments. For this reason, digitalization has begun to be taken into account in local legislation. In line with the mentioned developments in the world, law making activities in our country have been carried out in the axis of technological developments in recent years and the impact of digitalization makes itself felt significantly. Negotiable Instruments Law, which is one of the basic and

indispensable elements of commercial life all over the world, has started to get its share from these developments. One of the important regulations enacted in this field is the "Electronic Negotiable Instruments Law" (Gesetz über elektronische Wertpapiere-eWpG) which entered into force on 03.06.2021 in Germany. Another regulation called "Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technick verteilter elektronischer Register" is entered into force on 01.08.2021 and includes an electronic registration system for more than one branch of law and regulates their compatibility with each other. The Draft Law on Electronic Checks and Promissory Notes, which has been prepared under the supervision of The Banks Association of Türkiye since 2015 and was expected to enter into force on January 1, 2020, has not yet been brought to the agenda of the Grand National Assembly of Turkey, is a similar regulation to aforementioned German and Swiss regulations.

The purpose of drafting such a law in our country is to have an effective means of combating the subterranean economy with the establishment of an electronic check and promissory notes system. In addition, it is aimed to prevent the use of checks and promissory notes as fraudulent instruments, to monitor the entire circulation process of checks and promissory notes by the means of technology, and thus to increase the confidence in the market in checks and promissory notes. Therefore, new types of negotiable instruments are not invented and new payment and credit instruments are not created under the draft law. With the draft law, it will be possible to electronically arrange, transfer and pay the checks and promissory notes regulated under the Turkish Commercial Code and the Check Law with the help of technology. Thus, thanks to the draft law, these checks and promissory notes will be transformed digitally, while maintaining the existence of classic checks and promissory notes. However, although digitalization is inevitable in this field, the legal nature of electronic negotiable instruments cannot be explained by the generally accepted negotiable instruments theory until now.

On the other hand, the increase in the number of bounced checks in recent years and the inadequacy of the sanctions against bounced checks have led to the loss of public confidence in checks. For this reason, the need for new legal regulations to increase the public confidence in the check has emerged. In this regard, with the *Amendment of Certain Laws for the Improvement of Investment Environment* dated 9 August 2016 and numbered 6728 measures were taken to prevent checks from being bounced and to increase public confidence in checks. It can be stated that an important step has been achieved regarding the digitalization process of the check with the QR code check application regulated within the scope of this law.

For the reasons explained above, the need to reconsider checks and promissory notes on the basis of technology has emerged. With the implementation of electronic checks and promissory notes, it was thought that problems such as bounced checks, forgery and the subterranean economy could be prevented, and on the other hand, it was aimed to further increase the circulation capacity of checks and promissory notes and to facilitate their monitoring. Within the scope of this article, the regulations in

German, Swiss and Turkish law will be compared and whether they are compatible with the generally accepted classical principles of negotiable instruments will be examined.

Keywords: electronic check, electronic promissory note, negotiable instruments, digitalization, check with QR code

GEMİ TİCARETİNDE KRİPTO PARA BİRİMİ KULANILMASI

Doç. Dr. Hacı KARA*

ÖZET

Gemi ve deniz araçlarının mülkiyetinin geçmesinin yollarından biri de devren iktisaptır. Gemi ve deniz araçlarının devren iktisabı Türk Ticaret Kanun'unun 1001'inci maddesi ile düzenlenmiştir. Bu madde gereğince gemi siciline kayıtlı olan bir Türk gemisinin devren iktisabı için gemi sahibi ile iktisap edenin, mülkiyetin iktisap edene devri hususunda anlaşmış olmaları ve geminin zilyetliğinin (gemi üzerindeki tasarruf hakkının) iktisap edene geçirilmesi şarttır. Mülkiyetin devrine ilişkin sözleşmelerin yazılı şekilde yapılması ve imzaların noterce onaylı olması zorunludur. Ancak bir kolaylık yapılmış ve sözleşmenin gemi sicil müdürlüğünde de yapılabilmesi kabul edilmiştir.

Gemi ve deniz araçlarının alım satımında genelde nakit para ya da kredi kullanılmaktadır. Çoğunlukla da kredi kuruluşlarınca temin olunan parayı teminat altına almak için gemi ipoteği kullanılmaktadır. Ayrıca, geminin veya deniz araçlarının finansal kiralamaya ve kira sözleşmesine (çıplak gemi kirası, *bareboat charter*) konu olması da mümkün olabilmektedir. Genelde finansal kira ve kiralama sözleşmesi sonunda, ödenen kiraların toplam bedeli satış bedeli toplamına eşit olması halinde mülkiyetin devralan kiracıya ait olması kararlaştırılmaktadır.

Ama günümüzde kripto paranın milli paranın yerine geçmesi ya da alım-satımın kripto para birimi ile yapılması konusunda taraflar anlaşabilmektedir. Kripto para, merkezi bir otorite tarafından kontrol edilmeyen ve herhangi bir başka otoriteye ihtiyaç duyulmadan kişiden kişiye değer aktarımına izin veren, çevrimiçi ağlar yani internet aracılığıyla finansal işlemleri gerçekleştirmek için kriptografik işlemler kullanan, bir dijital para türü, değişim ve takas aracı olarak tanımlanmaktadır. Taraflar karşılıklı olarak borçlarını ifa ederler ve ücrete dair hiçbir çekişme ortaya çıkmaz ise bunun mümkün olması kabul edilebilir görünmektedir. Asıl sorun taraflar arasında ihtilaf çıkması halinde ortaya çıkmaktadır. Acaba bu durumda tarafların sözleşmede kararlaştırdıkları kripto para ile ödeme yükümlülüğü ücretin kararlaştırılması ve/veya ifası olarak kabul edilecek midir veya ödemenin milli para birimi ile mi yapılması gerekecektir? Dünyada tüm bu hususlar tartışma konusu yapılmaktadır.

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

Bu çalışmada kripto para ile gemi ya da deniz aracı satın almak mümkün müdür; taraflar arasındaki sözleşmeye dair hüküm geçerli kabul edilecek midir ve kripto para ile ifa nasıl mümkün olabilir, gibi hususlar incelenecektir. Ceza hukukuna dair konular ise bu çalışmanın konusu değildir.

Anahtar kelimeler: Gemi alım-satımı, deniz ticareti, kripto para, sanal para ve ticarette sanal para kullanımı.

USING CRYPTO CURRENCY IN PURCHASE AND SELLING OR LEASE AGREEMENTS OF SHIPS OR MARINE VEHICLES

ABSTRACT

Transfer agreement of ownership of ships and marine vehicles is one of the ways of transferring ownership. Transferring of ownership of ships and marine vehicles is regulated by Article 1001 of the Turkish Commercial Code. According to this article, for the transfer of a Turkish ship registered to the ship registry, the owner and the acquirer must have agreed on the transfer of ownership to the acquirer, and transfer of the possession of the ship (right of disposition on the ship) must be transferred to the acquirer. Contracts regarding the transfer of ownership must be made in writing and the signatures must be notarized. However, a convenience has been made and it has been accepted that the contract can also be made at the ship registry directorate.

Cash or credit is generally used in the purchase and sale or lease agreements of ships and marine vehicles. Ship mortgages are mostly used to secure the money provided by credit institutions. In addition, it is possible for the ship or marine vessels to be subject to financial leasing and bareboat charter. In general, at the end of the finance lease and leasing agreement, if the total price of the rents paid is equal to the sum of the sales price, it is decided that the ownership will belong to the transferee tenant.

However, nowadays, the parties can agree on whether the crypto currency should replace the national currency, or whether the purchase and sale should be made with the crypto currency. Cryptocurrency is defined as a type of digital currency, exchange, and exchange tool that is not controlled by a central authority and allows the transfer of value from person to person without the need for any other authority through online networks, namely the internet, and that uses cryptographic transactions to perform financial transactions. If the parties mutually perform their debts and no dispute, arises about the wage, it seems acceptable that using crypto currency is possible. The main problem arises when there is a conflict between the parties. In this case, will the obligation to pay with crypto money agreed by the parties in the contract be considered as the determination, and/or performance of the fee, or will the payment have to be made in national currency? All these issues are discussed in the world.

In this study, is it possible to buy a ship or sea vehicle with crypto money; Will the provision of the contract between the parties be considered valid and how it is possible to perform with crypto money will be examined. Issues related to criminal law are not the subject of this study.

Keywords: Ship sales, maritime trade, crypto money, virtual money and the use of virtual money in trade.

GAYRİMENKUL SERTİFİKASI VE KİRA SERTİFİKALARININ AKILLI SÖZLEŞMELERLE ARACISIZ DEVRİNİN BİNA İNŞAAT MALİYETLERİNİN FİNANSMANINA VE MÜLKİYET HAKKI DEVRİNE ETKİSİ VE VERGİ AVANTAJLARI

Memduh ASLAN*

ÖZET

Blok zinciri teknolojisinin geleceğe yönelik öngörülerinden biri de, taşınmazların devrinin güvenle yapılacağına yöneliktir. Blok zinciri, sadece kayıt güvenliğini sağlamakta, işlem güvenliği ise blok zinciri üzerinde değişiklik yapacak olan işlemleri yapan işleticinin güvenilirliğine bağlı olmaktadır. Taşınmaz mallar, tapu siciline kaydedilmek zorundadır. Mülkiyet devri ise, ancak sicile kayıt ile geçerli olabilir. Diğer taraftan, Türkiye genelinde tapu ve kadastro kayıtlarındaki mülkiyet verilerinin elektronik ortama aktarılması ve işlemlerin elektronik ortamda yürütülmesi, takip ve kontrolünün etkin ve hızlı bir şekilde yapılması amacıyla Tapu ve Kadastro Bilgi Sistemi (TAKBİS) oluşturulmuştur. Adalet Bakanlığı protokolleri kapsamında hacizlerin elektronik olarak tesis ve terkin edilmesi de sistem üzerinden yapılabilmektedir. Tapu ile bankalar arasında protokoller ile ipotek tesisi/terkini, satış-ipotek işlemleri elektronik ortamda başlatılmıştır. TAKBİS veri tabanının bir blok zinciri sisteminde tutulması halinde tapu devir işlemlerinin de akıllı sözleşmelere konu edilebilmesi mümkündür. Tapu kayıtları üzerinde işlem yetkisi verilen bankalar, noterler ve Adalet Bakanlığı aracılığı ile tapuya gitmeden tapu işlemleri yapılabilir hale gelmiştir.

Tapu devir işlemlerinin münhasıran tapu müdürü huzurunda yapılma zorunluluğu, 7413 sayılı Kanunun 11. maddesi ile 1512 sayılı Noterlik Kanununun 60/3 maddesinde yapılan değişiklik ve eklenen 61/A maddesi ile, taşınmaz satış vaadi sözleşmesi yapmak ve bu sözleşmeyi taraflardan birinin talep etmesi, harç ve giderleri ödemesi hâlinde tapu bilişim sistemi vasıtasıyla tapu siciline şerh vermek ile taşınmaz satış sözleşmesi yapmak noterlerin görevleri arasında sayılmıştır. Bu değişiklik, bilişim sisteminin kurulduğunun Adalet Bakanlığı resmi internet sitesinde duyurulduğu tarihten itibaren uygulanmaya başlanacaktır. 7413 sayılı Kanunun 14. maddesi ile 1512 sayılı Kanuna eklenen Geçici 21. maddenin ikinci fıkrasına göre ise, anılan bilişim sisteminin 01/01/2023 tarihine kadar kurulacaktır. Buna göre, taşınmaz satış sözleşmesi taraflarca imzalandığı anda

* Doç. Dr., Kocaeli Üniversitesi Hukuk Fakültesi, ORCID ID: orcid.org/0000-0002-9512-3876 memduhaslan@gmail.com,

noter, tapu bilişim sisteminden (TAKBİS) yevmiye numarası alarak sözleşmeyi bu sisteme kaydedecek ve tapu müdürlüğünce taşınmazın tapu siciline tescili sağlanacaktır. Tapuya güven esası çerçevesinde noterlerce yapılacak taşınmaz satış sözleşmesine ilişkin işlem güvenliğinden noterler sorumlu tutulmuştur. Zararın devlet tarafından ödenmesi hâlinde sözleşmeyi düzenleyen notere rücu edilebilecektir. Taşınmaz satış işlemlerinin noterler tarafından yapılacak olması nedeniyle ödeme hizmeti sunan kuruluşlar ile yapılacak anlaşmalar çerçevesinde araç devir ve tescillerinde olduğu gibi taşınmaz satış bedelleri de satışın yapıldığı anda satıcının hesabına geçebilecektir. Bu işlemlerin bizzat noter tarafından yapılmasının gerekmesi ve tarafların satış iradesinin varlığının kontrol edilmesi sorumluluğunun notere ait olması nedeni ile taşınmaz satış işleminin taraflarca elektronik ortamda gerçekleştirilmesi mümkün gözükmemektedir. Bu doğrultuda akıllı sözleşmenin tetiklenmesi bizzat noter tarafından yapılabilecektir.

Sermaye piyasası mevzuatı uyarınca herhangi bir sermaye piyasası aracı alım işlemini organize piyasalardan yapmak isteyen bir yatırımcının bu talebini yerine getirebilmek için mevcut durumda yatırım kuruluşu, borsa, takas kurumu, saklama kurumu gibi aktörlere ihtiyaç duymakta ve işlemler anlık olarak sonuçlanmamakta, işlemi takip eden ikinci iş gününde (T+2) takas gerçekleşmektedir.[1]

Uluslararası Menkul Kıymetler Hizmetleri Birliği Raporuna göre, alım-satım işlemlerinin gerçekleştirilmesi, takası, merkezi karşı taraf işlemleri ve saklanması için hizmet veren bir yapı bulunmadığı gibi, dağıtık defter alt yapısı belirli bir süre daha klasik piyasa yapıları ile birlikte varlığını devam ettirecektir.[2]

Blok zinciri sistemini popüler hale getiren temel unsur, özellikle, kripto paralar ile finans sistemine yeni bir alternatif olmasından kaynaklanmaktadır. Zira konvansiyonel bankacılık ve finans sistemine alternatif yollar aranmaktadır. Günümüzde teknolojinin hızlı gelişmesinin yanında para transferlerinde kullanılan yöntemler, yetersiz ve yüksek maliyetli kalmıştır.[3] Blok zinciri finansal teknoloji alanında da önemli gelişmeleri beraberinde getirmiştir. Kripto paralara bir karşılık olmasa bile elektronik para ve daha ileri boyutta dijital paralar üzerinde hukuki zemin oluşmakla birlikte bu konuda devletler ulusal bazda teknolojik araştırma ve geliştirme faaliyeti içerisindedirler. Katılım bankacılığının gelişmesi ve faizsiz finansman arayışları, sukuk uygulamalarının da mevzuatımızda yer almasını gerektirmiştir. 6362 sayılı Sermaye Piyasası Kanununun 61. maddesinde kira sertifikaları, 61/A maddesinde ise gayrimenkul sertifikaları düzenlenmiştir. Kira sertifikaları, varlık kiralama şirketleri tarafından ihraç edilebilmektedir. Varlık kiralama şirketinin kiralamaya konu edeceği varlıklar ise ağırlıklı olarak taşınmazlardır. Kira sertifikaları aracılığıyla kira geliri elde eden yatırımcı esasen kira süresince sertifika üzerinden geçici olarak ilgili varlığın sertifikaya isabet eden kısmına da dolaylı olarak malik olmaktadır. Kira sertifikaları için varlığın meydana getirilmiş olması gerekirken, gayrimenkul sertifikaları gayrimenkulün inşasının tamamlanmasına kadar inşaatın finansmanı için ihraç edilen ve inşaatın tamamlanması ile itfa edilen sertifikalardır. Gayrimenkul sertifikaları da elde bulunduğu sürece temsil

1 Dağlı, (2021), s. 69.
2 ISSA Raporu, (2019), s. 54.
3 Özkul, Baş, (2020), s. 58.

edilen yapının sahiplik hakkını vermektedir. Gayrimenkul sertifikası şimdiye kadar sadece Mavera 3 Projesinde kullanılmıştır. Sertifikaların kaydileştirilerek elektronik kayıt altında el değiştirmelerinin mümkün olması nedeniyle akıllı sözleşmelere de konu olabilecek mahiyettedirler. Kısa ve orta vadeli yatırım araçları olarak karşımıza çıkan bu iki sertifika türünün birlikte uygulanması halinde uzun vadeli yatırım aracı haline gelmeleri de mümkündür. Temsil ettiği varlıkların dolaylı sahiplik haklarını da vermesi nedeni ile tapuda tescile gerek kalmadan bu sertifikalar aracılığıyla gayrimenkul yatırımları yapmak mümkün hale gelebilecektir.

Hukuki altyapımız incelendiğinde sertifikaların elektronik ortamda devredilmesinin önünde yasal bir engel bulunmadığı gibi, mevzuatımız dijital dönüşümü de desteklemektedir. Ticari işlemler sonucunda ortaya çıkan sözleşmelerde taraflara yüklenen edimlerin koşullar oluştuğunda akıllı sözleşmeler ile icrasını sağlayabilecek hukuki düzenlemelerin yanında kamu tarafından belirli kurallara, izne ve denetime tabi, ödemeler için banka ve elektronik para kuruluşları, finansman için bankalar, finansman ve faktöring şirketleri, şirket hisse senetleri için merkezi kayıt kuruluşu, kira sertifikaları için varlık kiralama şirketleri, ticari mallar için umumi mağazalar, tarım ürünleri için lisanslı depolar gibi güvenli saklama noktaları bulunmaktadır.

Çalışmamızda herhangi bir ek yasal düzenleme veya yeni bir kuruluşa ihtiyaç olmadan Elektronik Sertifika Trampa Sistemi® üzerinden Varlık Kiralama Şirketlerinin gayrimenkul sertifikası ve kira sertifikasının birlikte kullandığı bir modelleme ile inşa edilecek gayrimenkulün finansmanı ve sistemde bulunan gayrimenkullerin tapu devrine ihtiyaç duymadan mülkiyet hakkının elde edilmesi ve bütün veya parçalı(belirlenen birim alan üzerinden) olarak başkasına aracısız devredilmesine, sertifikaların aynen ifaya opsiyonu ile klasik gayrimenkul mülkiyetine dönüştürme olanağına ilişkin yeni yol ve yöntemlerin mevcut uygulamalar ile karşılaştırılması yapılarak vergi avantajları ile ortaya konulacaktır.

Anahtar Kelimeler: Gayrimenkul Sertifikası, Kira Sertifikası, Akıllı Sözleşme, Sermaye Piyasası, Varlık Kiralama Şirketi

EFFECTS AND TAX BENEFITS OF TRANSFERRING REAL ESTATE CERTIFICATES AND LEASE CERTIFICATES VIA SMART CONTRACTS WITHOUT AGENTS ON FINANCING BUILDING CONSTRUCTION COSTS AND OWNERSHIP RIGHTS TRANSFER

ABSTRACT

One of the future predictions of blockchain technology is that the transfer of real estate will be done safely. The blockchain only provides record security, while transaction

security depends on the reliability of the operator that makes the transactions that will make changes on the blockchain. Due to Turkish Legislation Immovable properties must be registered in the land registry. The transfer of ownership can only be valid with registration in the registry. On the other hand, the Land Registry and Cadastre Information System (TAKBİS) was established in order to transfer the property data in the land registry and cadastre records to electronic environment, to carry out the transactions in the electronic environment, to follow and control them effectively and quickly. Within the scope of the protocols of the Ministry of Justice, electronic establishment and abandonment of foreclosures can also be done through the system. Mortgage establishment/leaving, sales-mortgage transactions were initiated electronically with protocols between the title deed and banks. If the TAKBİS database is kept in a blockchain system, it is possible to subject the title transfer transactions to smart contracts. Deed transactions can be made without going to the title deed through banks, notaries and the Ministry of Justice, which are authorized to process title deeds.

The obligation to carry out the transfer of title deeds exclusively in the presence of the title deed manager, the amendment made to the article 60/3 of the Notary Law No. 1512 with the 11th article of the Law No. In case of paying the expenses, giving annotations to the land registry through the land registry information system and making a real estate sales contract are among the duties of the notaries. This change will be implemented as of the date of the announcement of the establishment of the information system on the official website of the Ministry of Justice. According to the second paragraph of the Temporary Article 21 added to the Law No. 1512 with Article 14 of the Law No. 7413, the said information system will be established until 01/01/2023. Accordingly, once the immovable sales contract is signed by the parties, the notary public will obtain a journal number from the land registry information system (TAKBİS) and record the contract in this system, and the immovable will be registered in the land registry by the land registry directorate. Notary publics are held responsible for the transaction security regarding the real estate sales contract to be made by the notary publics within the framework of trust in the title deed. In case the damage is paid by the state, it can be recourse to the notary who issued the contract. Since real estate sales transactions will be carried out by notaries, within the framework of agreements to be made with institutions providing payment services, immovable sales prices will be transferred to the seller's account at the time of sale, as is the case with vehicle transfers and registrations. Since these transactions have to be carried out by the notary public and the responsibility of checking the existence of the parties' will to sell belongs to the notary, it does not seem possible to carry out the sale of the immovable by the parties electronically. In this direction, the triggering of the smart contract can be done by the notary public.

In accordance with the capital market legislation, an investor who wants to purchase any capital market instrument from organized markets currently needs actors such as investment institutions, stock exchanges, clearing houses, custodians, and the transactions are not concluded instantly, on the second business day following the

transaction. (T+2) swap takes place. [4]According to the Report of the International Association of Securities Services, there is no structure that provides services for the execution, clearing, central counterparty transactions and custody of purchase and sale transactions, and the distributed ledger infrastructure will continue to exist together with the classical market structures for a certain period of time.[5]

The main factor that makes the blockchain system popular is that it is a new alternative to the financial system with cryptocurrencies. Because alternative ways to the conventional banking and financial system are sought. Today, besides the rapid development of technology, the methods used in money transfers have remained inadequate and costly. [6]Blockchain has also brought important developments in the field of financial technology. Even if there is no response to cryptocurrencies, there is a legal basis for electronic money and more advanced digital currencies, and states are engaged in technological research and development activities on a national basis. The development of participation banking and the search for interest-free financing necessitated the inclusion of sukuk practices in our legislation. Lease certificates are regulated in Article 61 of the Capital Markets Law No. 6362, and real estate certificates are regulated in Article 61/A. Lease certificates can be issued by asset leasing companies. The assets to be leased by the asset leasing company are mainly immovables. The investor, who earns rental income through lease certificates, also indirectly owns the part of the related asset that corresponds to the certificate temporarily over the certificate during the lease term. While the asset must be created for lease certificates, real estate certificates are certificates that are issued to finance the construction until the completion of the construction of the real estate and are redeemed upon completion of the construction. Real estate certificates also give ownership of the represented building as long as they are available. The real estate certificate has only been used in the Mavera 3 Project so far. Since certificates can be dematerialized and exchanged under electronic record, they are also subject to smart contracts. It is also possible for these two types of certificates, which appear as short and medium-term investment instruments, to become long-term investment instruments if they are applied together. Since it gives indirect ownership rights to the assets it represents, it will be possible to make real estate investments through these certificates without the need for registration in the land registry.

When our legal infrastructure is examined, there is no legal obstacle to the transfer of certificates in the electronic environment, and our legislation also supports digital transformation. Banks and electronic money institutions for payments, banks for financing, financing and factoring companies, company stocks , subject to certain rules, permission and control by the public, as well as legal arrangements that can ensure the execution of the obligations imposed on the parties in contracts resulting from commercial transactions with smart contracts when the conditions are met. central

4 Dagli, (2021), p. 69.
5 ISSA Report, (2019), p. 54.
6 Özkul, Baş, (2020), p. 58.

registrar, asset rental companies for lease certificates, public stores for commodities, licensed warehouses for agricultural products.

In our study, without the need for any additional legal regulation or a new institution, financing of the real estate to be built with a modeling used together with the real estate certificate and lease certificate of the Asset Leasing Companies via the Electronic Certificate Barter System® and obtaining the ownership right of the real estates in the system without the need for title deed transfer and The new ways and methods regarding the partial (over the determined unit area) transfer to another person without an intermediary, the possibility of converting the certificates into traditional real estate property with the option to perform exactly, will be compared with the existing practices and will be presented with tax advantages.

Keywords: Real Estate Certificate, Lease Certificate, Smart Contract, Capital Market, Asset Leasing Company

DAO'LARIN MASAK MEVZUATI VE ADİ ŞİRKET HÜKÜMLERİ AÇISINDAN DEĞERLENDİRİLMESİ

Av. Cemal ARAALAN*

Kripto varlıkların yüksek kazanç getirilerinden dolayı popüler hale gelmesi neticesinde, bu varlıkların altyapısını oluşturan blokzincir teknolojisinin de kullanım alanları giderek artmaktadır. Blokzincir teknolojisinin sağladığı yarar ile yeni nesil finansman alanında da merkeziyetsiz bir yapı öne çıkarak "Merkeziyetsiz Finans" anlamına gelen DeFi *(Decentralized Finance)* kavramı doğmuştur. DeFi'nin özünü blockzincir teknolojisi ile çalışan akıllı sözleşmeler oluşturmaktadır. Akıllı sözleşmeler sayesinde aracısız olarak "Merkeziyetsiz Finans" gerçekleştirilmektedir. Günümüz ekosistemi içerindeki geleneksel finansal sistemlerde bankacılık, ticaret, nakit akışı uygulamalarının neredeyse çoğunluğu bankalar veya borsalar aracılığıyla ilerlemektedir. Diğer bir anlatımla merkezi finans sistemlerinde bireylerin paraları bankalar ya da temel gayesi para kazanmak olan şirketler nezdinde tutulmakta ve kişilerin sermaye ve finansal hizmetlere ulaşımı için birtakım aracı kurumların varlığı gerekmektedir. Nitekim merkezi finans sistemlerde paranın kontrolü bireylerin kendisinde değil, aracı otoritededir. Merkezi olmayan finans sistemleri (DeFi) ise bireylerin finansal süreçlerini yürütmeleri esnasında gelişen teknolojik yöntemleri kullanarak aracı kurum/kuruluş veya kişileri ortadan kaldırır. Tüm bu anlatılanlardan hareketle kısaca DeFi, kredi alma/verme, merkeziyetsiz borsa, sigorta, alışveriş, pazaryeri ve benzeri finansal işlevleri sağlayan ve temelinde akıllı sözleşmeler, merkeziyetsiz uygulamalar ve konsensus protokollerine dayanan finansal yapıdır.

DeFi denilen finansal yapının bir ürünü olan ve İngilizce'de Decentralized Autonomous Organization denilen kısaca DAO kelimesi ise, dijital ortamda kurulu olan, işleyiş ve bu organizasyona ilişkin kuralları kod şeklinde belirlenen, otonom ve şeffaf olarak çalışan topluluklara verilen isimdir. Türkçeye "merkezi olmayan özerk kuruluşlar" şeklinde tercüme edilebilecek DAO'lar, özünde genel itibariyle Ethereum blokzincir ağında oluşturulan bir akıllı sözleşme uygulaması olup DAO'ların işletme kuralları önceden bilgisayarlar tarafından belirlenmekte ve karar verme yetkisi geleneksel ortaklıklara kıyasla herhangi bir kişinin elinde olmayıp hiyerarşik bir yönetim yapısı da bulunmadığından, bu kuruluşlardaki yönetim ve karar alma süreçlerinin gayri merkezi olduğu kabul edilmektedir. DAO'ların kuruluşundaki temel amaç, blokzincir ağındaki paydaşların paylarına göre oy hakkına sahip olacak hissedarlar tarafından kontrol edilen bir yatırım kuruluşu inşa etmek olup DAO'lar akıllı sözleşmeler vasıtasıyla

* Çetinkaya Avukatlık Bürosu- Kıdemli Danışman, cemal@arcavukatlik.com, ORCID No: 0000-0003-3800-3752

yatırımcılarından fon toplayarak, bu fonlarla yatırımlarda bulunur ve elde edilen karı sistem tarafından belirlenen belirli bir algoritmaya göre dağıtmaktadır. DAO'ların yatırımcılarının ve bu projeyi başlatan yazılımcılarının (developer) kim oldukları dijital bir anahtar ile tespit edilmekle beraber, bu kişilerin gerçek dünyada kim oldukları genel olarak tespit edilemez niteliktedir. Zira DAO'larda temsiliyet kripto cüzdan adresleri üzerinden kurgulanmaktadır. Hatta öyle ki bu adresler insanlara ait olabileceği gibi; robotlara, cihazlara ya da başka merkeziyetsiz otonom kuruluşlara dahi ait olabilir. Başka bir ifade ile dünya, yatırımcıların her zaman gerçek veya tüzel kişi olmadığı yeni bir organizasyon yapısı ile tanışmaktadır.

Türkiye'de ilk kez kripto varlıklar 16.04.2021 tarihinde Resmî Gazete'de yayımlanarak yürürlüğe giren Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik (*"Yönetmelik"*) ile tanımlanmıştır. Yönetmelik m. 3'de kripto varlık, *"dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen* ***gayri maddi varlıklar****"* şeklinde tanımlanmıştır. Bu tanımdan hareketle, öncelikle netleştirilmesi gereken husus DAO'ların kripto varlık hizmet sağlayıcı olup olmadıklarının hukuken tespit edilmesidir. MASAK'ın Kripto Varlık Hizmet Sağlayıcıları Rehberi'nde kripto varlık hizmet sağlayıcıları, **"kripto varlıkların alım satımlarına elektronik işlem platformları üzerinden aracılık eden platformlar"** olarak tanımlanmaktadır. Yukarıda yer verilen Türk hukukundaki "kripto varlık" ve "kripto varlık hizmet sağlayıcı" tanımları açısından dikkat çekici bir husus özellikle kripto varlık tanımı MASAK'ın 1991 tarihinden itibaren üyesi olduğu Mali Eylem Görev Gücü (Financial Action Task Force; kısaca *"FATF"*) ile uyumludur.

Kripto varlık hizmet sağlayıcı olmanın en önemli sonucu, MASAK mevzuatı kapsamında yer verilen çeşitli yükümlülüklere (müşterinin tanınmasına ilişkin esaslar, şüpheli işlem bildirimi, bilgi ve belge verme yükümlülüğü, muhafaza ve ibraz yükümlülüğü vb.) tabi olunmasıdır.

Türk hukukuna bakıldığında, yapısal olarak DAO'ların sermaye şirketleri olan anonim ve limited şirketler ile kollektif ve komandit şirket ve kooperatiflerle özelliklerinin karşılaştırılmasına ve bu bağlamda DAO'lara ilişkin özel bir düzenlemeye ihtiyaç olup olmadığının tespitinin fayda sağlayacağı düşünülmektedir. Kısacası, DAO'lara ilişkin spesifik bir düzenleme bulunmadığı ve özellikle Türk Ticaret Kanunu ("TTK") ve sair mevzuat gereğince ticaret şirketlerine ilişkin belirli bir yapının ve detaylı birtakım kuruluş prosedürlerinin öngörülmesi sebebiyle DAO'ların sermaye şirketi olarak nitelendirilmesi mümkün gözükmemektedir. Bu noktada Türk Borçlar Kanunu ("TBK") m. 620/f. 2 ve TTK 214 gereğince DAO'ların hukuken tasnif edilebileceği tek seçenek adi şirket olabileceğidir. TBK m. 620/f. 1 uyarınca adi şirket, iki ya da daha fazla kişinin emeklerini ve mallarını ortak bir amaca erişmek için birleştirmeyi üstlendikleri bir sözleşme olarak tanımlanmaktadır. DAO'ların yapısına bakıldığında temelde iki ya da daha fazla kişinin ortak bir amaç için bir araya geldikleri görülmekle beraber adi şirketlerde bu kurumun düzenleniş ve sorumluluk rejimi itibariyle yapının

ortakların birbirini tanıması esasına dayalı olmasına rağmen DAO'larda kişilerin çoğu kez birbirini tanıması mümkün gözükmemektedir. Genel itibariyle adi şirket görünümü sergilemekle beraber özellikle DAO'larda yatırımcıların ve proje sahiplerinin anonim olması ve kimliklerinin bilinmemesi sebebiyle adi şirket hükümlerinin tam anlamıyla uygulanamayacağı düşünülmektedir.

Tebliğimizde özellikle DAO'ların MASAK mevzuatı kapsamında kripto varlık hizmet sağlayıcı olup olmadığı ve hukuken adi şirket hükümleri çerçevesinde değerlendirilip değerlendirilemeyeceği detaylı şekilde irdelenecektir.

Anahtar Kelimeler: gayri merkezi özerk organizasyonlar, gayri merkezi finans, MASAK, adi şirket, kripto varlıklar

LEGAL OVERVIEW ON DAO'S WITHIN THE FRAMEWORK OF TURKISH ANTI-MONEY LAUNDERING LEGISLATION AND THE ORDINARY COMPANY PROVISIONS

ABSTRACT

While crypto assets have become popular due to their high earnings returns, the use of blockchain technology, which forms the infrastructure of these assets, is gradually increasing. Considering the benefit of blockchain technology, a decentralized structure has also triggered to the importance in the field of new generation finance, and the concept of DeFi (Decentralized Finance). The essence of DeFi is smart contracts that functions with blockchain technology. Thanks to smart contracts, "Decentralized Finance" became popular without intermediaries. Almost the majority of banking, trade and cash flow applications in traditional financial systems within today's ecosystem proceed through banks or exchanges. In other words, in central financial systems, individuals' money is kept by banks or companies whose main purpose is to make money, and the presence of some intermediary institutions is required for individuals to access capital and financial services. As a matter of fact, the control of money in central financial systems is not the under the control of individuals but subject to intermediary authority. Decentralized financial systems (DeFi), on the other hand, eliminate intermediary institutions/organizations or individuals by using technological methods developed during the financial processes of individuals. In brief, DeFi is a financial structure based on smart contracts, decentralized applications and consensus protocols, which provides financial functions such as lending/issuing, decentralized exchange, insurance, shopping, marketplace and similar financial functions.

DAO ("Decentralized Autonomous Organization"), which is a product of DeFi in English, is the the autonomous and transparent communities established in the digital environment, whose operation and rules regarding this organization are

determined in the form of code. DAOs are essentially in the form of smart contract created in the Ethereum blockchain network and the operating rules of DAOs are predetermined by computers and the decision-making authority is not in the hands of any one person which differs from traditional partnerships. It is accepted that the management and decision-making processes in these organizations are decentralized. The main purpose of the establishment of DAOs is to build a shareholder-controlled investment mechanism that will have voting rights according to the shares of the stakeholders in the blockchain network. Although the investors of DAOs and their developers (developers) who created this mechanism are identified with a digital key, it is generally undetectable who these people are in the real world. This is because the representation in DAOs is established through crypto wallet addresses. In other words, the world is currently introduced with a new organizational structure where investors are anonymous.

In Turkey, crypto assets were firstly defined by the Regulation on Not Using Crypto Assets in Payments ("Regulation"), which was published in the Official Gazette on 16.04.2021. In accordance with Article 3 of the Regulation, crypto-assets are defined as "intangible assets that are created virtually and distributed over digital networks using distributed ledger technology or similar technology, but that do not qualify as fiat money, deposit money, electronic money, payment instruments, securities or other capital market instruments". Taking this definition into consideration, the first issue to be clarified first is to determine whether DAOs are crypto asset service providers or not within the framework of Turkish Financial Crimes Investigation Board ("MASAK") Legislation. In MASAK's Directory of Crypto Asset Service Providers, crypto asset service providers are defined as "platforms that mediate the buying and selling of crypto assets through electronic trading platforms". In terms of the definitions of "crypto-asset" and "crypto-asset service provider" in the Turkish law given above, it is noteworthy that the definition of crypto-assets is compatible with the definitions of the Financial Action Task Force ("FATF") which MASAK has been a member since 1991.

The most important result of being a crypto asset service provider is to be subject to various obligations included in the MASAK legislation (the mandatory rules regarding customer recognition, suspicious transaction reporting, obligation to provide information and documents, obligation of preservation and submission, etc.).

In Turkish law, it is beneficial to compare the structural features of DAOs with joint stock companies and limited liability companies, as well as with collective and limited partnership companies and cooperatives, and to determine whether there is a need for a special regulation regarding DAOs in this context. In brief, it does not seem possible to qualify DAOs as capital companies, since there is no specific regulation regarding DAOs and due to specific structure and detailed establishment procedures for commercial companies are stipulated under the Turkish Commercial Code ("TCC"). Based on the provisions such as Article 620/para. 2 of Turkish Code of Obligations ("TCO") and Article 214 of TCC, the only option in which DAOs can be

legally classified is to be ordinary companies. As per Article 620/para. 1, an ordinary company is defined as a contract in which two or more persons undertake to combine their labor and assets to achieve a common purpose. Looking into the structure of DAOs, it is seen that two or more people come together for a common purpose. Nevertheless, even though DAOs seems to be similar with the appearance of two or more persons for the purpose of achieving common purpose, it is considered that the provisions of ordinary companies under Turkish law cannot be fully implemented due to the anonymity and unknown identities of investors and project owners in DAOs.

In this Symposium, I will give a speech on whether DAOs are crypto asset service providers within the scope of MASAK legislation and whether they can be legally evaluated within the framework of ordinary company provisions.

Keywords: Decentralised anonymous organisations, decentralised finance, MASAK, ordinary company.

MEDENİ USUL HUKUKUNDA YARGILAMANIN HIZLANDIRILMASI VE ADALETE ERİŞİM HAKKI BAKIMINDAN ÇEVRİM İÇİ MAHKEMELER VE YAPAY ZEKANIN KULLANIMI

Gökçe KARABEL* - Dilek AYDEMİR**

Teknolojik gelişmelerin Medeni Usul Hukuku bakımından ilk ve en etkili yansıması uluslararası pek çok ödüle de sahip olan UYAP sisteminin kurulması ile olmuştur. Elektronik imza ve elektronik tebligat yanında Medeni Yargılama Hukuku bakımından dijitalleşme konusundaki en çarpıcı örneklerden birisi olarak karşımıza, özellikle 2020'de yapılan kanun değişikliği ile e-duruşma (HMK m.149) çıkmaktadır. Alternatif uyuşmazlık çözüm yöntemleri bakımından daha uzun zamandır gündemde olan klasik uyuşmazlık yöntemlerinde özellikle duruşmaların icrasında teknolojiden faydalanılması, belli hallerde ise, özellikle tüketici uyuşmazlıkları bakımından, uyuşmazlığın tamamen online çözülmesi yönündeki eğilim mahkeme yargılamasına da taşınmıştır. Belli uyuşmazlıklar bakımından dava şartı olarak uygulanan arabuluculuğun icrası da artık çoğunlukla teknolojik imkanlar kullanılarak yapılmakta; yüz yüze yapılmamaktadır. Yine Sigortacılık Tahkim Merkezi ve kural olarak Tüketici Hakem Heyetleri de yargılamalarını dosya üzerinden gerçekleştirmektedir. Her ne kadar belli uyuşmazlıklar bakımından alternatif uyuşmazlık çözüm sistemleri uygulanıyor olsa da merkezi bir alternatif uyuşmazlık çözüm sistemi mevcut olmadığı gibi genel manada küçük miktarlı ve nispeten daha az karmaşık uyuşmazlıklar bakımından (ör: kira, kat mülkiyeti, komşuluk, küçük miktarlı para alacakları, basit çekişmesiz yargı işleri) özel bir uyuşmazlık çözüm usulü öngörülmüş değildir.

Uyuşmazlık çözümünde yapay zekanın ve teknolojinin yansımalarına baktığımızda ise, şirketlerin ve uyuşmazlık çözüm kurumlarının yanında artık devletlerin de yargı hizmetinin bir ayağı olarak çevrim içi uyuşmazlık çözüm modellerini uyguladığını görmek mümkündür. Bu konuda, bazı açılardan Hollanda, İsrail, Avusturya, AB Küçük Talep Prosedürüne İlişkin Regülasyon (EC 861/2007) gibi örnekler yanında tebliğde özellikle Birleşik Krallık'ta uygulanan "Small Claim Procedure" ve Kanada'da uygulanan "Civil Resolution Tribunal" sistemi incelenmiştir. Bu sistemlerde temel amaç tarafların avukata ihtiyaç duymaksızın dava yöneticileri ve ayrıntılı rehberler

* Uludağ Üniversitesi Hukuk Fakültesi, Medenî Usul Ve İcra İflas Hukuku Anabilim Dalı Öğretim Üyesi, gokcekarabel@uludag.edu.tr, ORCID NO: 0000-0002-1787-165X

** Uludağ Üniversitesi Hukuk Fakültesi, Medenî Usul Ve İcra İflas Hukuku Anabilim Dalı Öğretim Üyesi, gokcekarabel@uludag.edu.tr, ORCID NO: 0000-0002-1787-165X

yardımıyla ve ayrıntılı formlar üzerinden uyuşmazlığı e-müzakere, e-arabuluculuk ve e-tahkim ya da e-mahkeme yargılaması ile çözmelerini sağlamaktır. Öte yandan sistemlere başvurunun iradi olduğunu da vurgulamak gerekir. Çin örneği de hem online uyuşmazlık çözümü hem de yapay zekanın karar merciinde olması açısından dikkat çekici bir örnektir. Yapay zeka konusunda en çok tartışılan konu da yapay zekanın karar mercii olması ihtimalidir. Bunun dışında, özellikle karar taslağı oluşturulması, mevzuat ve spesifik ilmi ve kazai içtihat tespiti gibi konularda hâkime yardımcı yapay zeka (örneğin, ABD'de COMPAS) ve taraflara ve avukatlara yardımcı yapay zeka (örneğin, DoNotPay, Legalzoom, Lexmachina, Cascrunch) çalışmaları karşımıza çıkmaktadır.

Yapay zekanın gelişimi dikkate alındığında, yargılamanın her aşamasında hâkime yardımcı bir rol oynayabileceği kolaylıkla söylenebilirse de yapay zekanın, soyut düşünme ve empati yeteneği olmadığı için "mevzu hukuku uygulayarak vicdani kanaatine göre karar vermesi" aşamasına henüz gelmediğini de vurgulamak gerekir. Konuya ilişkin gerek AB gerekse G20 gibi uluslararası organizasyonların yayınlamış olduğu ilke ve kurallarda da bu nokta vurgulanmaktadır. Dava stratejisi belirleme, davayı kazanma ihtimalini tespit etme gibi konularda taraflara yardımcı yapay zeka sistemlerinin gün geçtikçe arttığını söylemek mümkündür. Öte yandan bu girişimlere karşı açılmış "yetkilendirilmedikleri halde hukuk hizmeti verildiği" ve "tailormade" çözümler üretildiği yönünde davalar da mevcuttur.

Bu tebliğde, uluslararası hukukta çevrimiçi uyuşmazlık çözüm sistemlerinden örnekler verilecek; yapay zekanın kullanım alanları örnekler üzerinden değerlendirilecek ve sonuç kısmında ise yargıya erişim hakkı ve usul ekonomisi ilkesi dikkate alınarak çevrimiçi uyuşmazlık çözüm sistemlerinin özellikle karmaşık olmayan küçük miktarlı uyuşmazlıklar için Türk Hukuku bakımından uygulanabilirliği incelenecek ve bu minvalde ve ayrıca diğer uyuşmazlıkların makul sürede sonuçlandırılmasına hizmet etmesi bakımından UYAP sisteminde yapılabilecek değişikliklere ilişkin önerilerimiz sunulacaktır.

Anahtar Kelimeler: Çevrimiçi mahkeme, çevrimiçi alternatif uyuşmazlık çözümü, yapay zeka, küçük talep usulü, UYAP.

THE USE OF ONLINE COURTS AND ARTIFICIAL INTELLIGENCE TO ACCELERATE CIVIL PROCEDURE TRIAL AND THE RIGHT TO ACCESS TO JUSTICE

ABSTRACT

The most effective reflection of technological developments in terms of Civil Procedure Law has been with the establishment of the UYAP system. In addition to electronic signature and electronic notification, e-trial is one of the most striking

examples of digitalization in terms of civil procedure law, especially with the revision made in 2020 (HMK art.149). The tendency to use technology especially in the execution of hearings in terms of alternative dispute resolution methods and the tendency to resolve the dispute completely online has also been carried to court proceedings. The execution of mediation is now mostly carried out using technological means. Moreover, The Commission of Arbitration of Insurance and The Committees of Consumer Arbitration also conduct the proceedings over the file. Although alternative dispute resolution systems are applied in terms of certain disputes, there is no centralized alternative dispute resolution system for small and relatively fewer complex claims (eg. rental, strata disputes, small amount of money, ex-parte proceeding).

When we look at the reflections of artificial intelligence and technology in dispute resolution, it is possible to see that states now apply online dispute resolution models as a pillar of the judicial service. In this regard examples such as Netherlands, Israel, Austria, EU Regulation on Small Claims Procedure (EC 861/2007) as well as the "small claim procedure" applied in the United Kingdom and the "Civil Resolution Tribunal" system applied in Canada were examined in the paper. The main purpose of these systems is to enable the parties to resolve the dispute via negotiation, facilitation or tribunal decision with the help of case managers and detailed guides and detailed forms without the need for a lawyer. The case of China is also a remarkable example in terms of both online dispute resolution and artificial intelligence being the decision maker. The most debated issue on artificial intelligence is the possibility of artificial intelligence being the decision maker. Apart from this, we come across artificial intelligence that assists the judge (the example of COMPAS in the USA) and artificial intelligence that assists the parties and lawyers (such as DoNotPay, Legalzoom, Lexmachina, Casecrunch) especially in drafting decisions, legislation and case law determination.

Considering the development of artificial intelligence, it can easily be said that it can play a role in helping the judge at every stage of the trial, but it should be emphasized that artificial intelligence has not yet reached the stage of "deciding according to its conscientious opinion by applying the law," since it does not have the ability to think abstractly and empathize. However, it is possible to say that artificial intelligence systems that assist the parties are increasing day by day.

In this paper, examples of online dispute resolution systems in international law will be given and the usage areas of artificial intelligence will be evaluated through examples. As a conclusion, the applicability of online dispute resolution systems in terms of Turkish Law will be discussed. In this regard, our suggestions regarding the changes that can be made in the UYAP system will be presented.

Keywords: online court, online dispute resolution, small claim procedure, artificial intelligence, UYAP.

YAPAY ZEKÂNIN CEZA MUHAKEMESİNDE İDDİA VE HÜKÜM MAKAMINDA BULUNMASINA İLİŞKİN DÜŞÜNCELER

Dr. Şaban Cankat TAŞKIN*

ÖZET

Geçtiğimiz günlerde sosyal medyada gördüğüm bir haber çok dikkatimi çekti. Haberde Pekin İnternet Mahkemesi'nin yapay zekâlı hakimleri yargılamada kullanmaya başladığı ifade ediliyordu.

Başka bir haberde de Çin'de yapay zekâlı savcıların ceza muhakemesi sistemine dahil edilmesinin düşünüldüğü, böylece iddianame hazırlama sürecinde yapılan hataların önlenmesinin amaçlandığı belirtilmekteydi.

Bu çalışmada, yapay zekâlı hakimlerin ve savcıların ceza muhakemesine ilişkin işlemleri yapmasının ve yapay zekâlı hakimlere sanıklara ceza verme yetkisi tanınmasının ceza hukukunun ve ceza muhakemesi hukukunun temel ilkeleriyle bağdaşıp bağdaşmadığı değerlendirilmiştir.

Keza çalışmada ceza yargılamasında yapay zekâlı hakim ve savcılara yer verilmesinin ortaya çıkarabileceği ceza hukuku sorunları ile uygulamada ortaya çıkabilecek olası sorunlar değerlendirilmiştir.

Anahtar Sözcükler: yapay zekâ, yapay zekâlı hakim, yapay zekâlı savcı, ceza muhakemesi hukukunun ilkeleri, ceza hukukunun ilkeleri

---

THOUGHTS ON ARTIFICIAL INTELLIGENCE AT THE CLAIMING AND SENTENCING AUTHORITY IN CRIMINAL PROCEDURE LAW

ABSTRACT

A news I saw on social media recently caught my attention. In the news, it was stated that the Beijing Internet Court had started to use artificial intelligence judges in the trial.

* İstanbul Aydın Üniversitesi Hukuk Fakültesi Ceza Hukuku ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi, E-posta : sctaskin@gmail.com, Orchid ID: https://orcid.org/0000-0001-6312-472X

In another report, it was stated that in China, artificial intelligence prosecutors were considered to be included in the criminal procedure system, thus preventing the mistakes made during the preparation of the indictment.

In this study, it has been evaluated whether the artificial intelligence judges and prosecutors' handling of criminal procedure and the authorization of artificial intelligence judges to sentence the defendants are compatible with the basic principles of criminal law and criminal procedure law.

Likewise, in the study, the criminal law problems that may arise from the use of artificial intelligence judges and prosecutors in criminal proceedings and possible problems that may arise in practice are evaluated.

Keywords: artificial intelligence, artificial intelligence judge, artificial intelligence prosecutor, principles of criminal procedure law, principles of criminal law

YARGI KARARLARININ GEREKÇELENDİRİLMESİNDE YAPAY ZEKANIN ROLÜ

Mehmet ÇATLI*

ÖZET

Yargı kararlarının gerekçeli olması anayasal bir hak olarak kabul edilmiştir. Buna göre ülkedeki tüm mahkemelerin kararlarının gerekçeli olması bir zorunluluktur. Bu anayasal ilkeye aykırı mahkeme kararları, Avrupa İnsan Hakları Mahkemesinin çeşitli ihlal kararlarına konu olmaktadır. Yargı kararlarının gerekçelendirilmesi ile ilgili gerek fakülteler bazında gerek adalet bakanlığı bazında muhtelif çalışmalar yapılmaktadır. Bu çalışmada özellikle yapay zekanın yargı kararlarının gerekçelendirilmesinde sahip olabileceği role ilişkin çeşitli yaklaşımlara değinilecektir. Öncelikle, gerekçelendirmede, (argümantasyon) hukukun ortaya koyduğu temel ilkeler ortaya konulmaya çalışılacaktır. Devamında bu temel ilkeler ışığında yapay zekanın etkin olarak kullanılabileceği alanlar ve yargılamaya sunabileceği katkılar değerlendirilecektir.

Anahtar Kelimeler: Yapay zekâ ve Hukuk, Dijital hukuk uygulamaları, Gerekçelendirme, Bilişim hukuku

---

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE JUSTIFICATION OF JUDICIAL DECISIONS

ABSTRACT

Justification of judicial decisions is accepted as a constitutional right. Accordingly, it is imperative that the decisions of all courts in the country are justified. Court decisions contrary to this constitutional principle are the subject of various violation decisions of the European Court of Human Rights. Various studies are carried out on the basis of faculties and the ministry of justice regarding the justification of judicial decisions. In this study, various approaches regarding the role of artificial intelligence in justifying judicial decisions will be discussed. First of all, in justification, the basic principles of

* Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi, Genel Kamu Hukuku, Dr. Öğretim Üyesi, Orcid ID: 0000-0001-7998-8434

(argumentation) law will be tried to be put forward. Afterwards, in the light of these basic principles, the areas where artificial intelligence can be used effectively and its contributions to the judging will be evaluated.

Keywords: Artificial intelligence and law, Digital law practices, Argumentation, IT law

BLOKZİNCİR TEKNOLOJİSİNDEKİ VERİLERİN DELİL NİTELİĞİNİN HUKUK YARGILAMASI BAKIMINDAN İNCELENMESİ

Dr. Elif Irmak BÜYÜK*

ÖZET

Blokzincir teknolojisi, blokların birbirine zincir gibi bağlandığı dağıtık bir veri tabanıdır. Her ne kadar blokzincir teknolojisinden bahsedildiğinde akla öncelikli olarak kripto paralar ve finans sektörü gelse de, siber güvenliğin sağlanması, kitle fonlaması, dijital belgelerin oluşturulması ve korunması, sağlık sektöründe ilaçların dağıtımı ve takibi, tapu sicilinde işlemlerin gerçekleştirilmesi, oy verilmesi gibi kamusal hizmetlerin de dahil olduğu birçok farklı alanda bu teknoloji altyapısı kullanılmaktadır. Blokzincir teknolojisinin dünyadaki kullanım alanının gün geçtikçe çeşitlenip gelişmesiyle birlikte bu teknolojinin insan hayatına daha da sirayet edeceği ve gündelik hayatımızdaki birçok işlemde karşımıza çıkacağı aşikardır. Bu doğrultuda hukuk yargılamasında görülen bir uyuşmazlıkla bağlantılı olarak blok zincir altyapısındaki çeşitli işlemlerin ve kayıtların delil olarak ibraz edilmesi de pekâlâ söz konusu olabilecektir. Bu aşamada hayatımıza nispeten yeni giren ve hukuki açıdan birçok noktada muğlaklığı olan blokzincir teknolojisinde yer alan verilerin ispat hukuk açısından da değerlendirilmesi önem arz etmektedir. İspat faaliyetinin sağlıklı işleyişini ve kavramların hukuki belirliliğini sağlamak adına söz konusu verilerin pozitif düzenlemelerimize göre delil niteliği, nasıl ibraz edileceği, ibraz edilen delillerin nasıl değerlendirileceği ele alınması gereken konulardandır.

Diğer kullanıcılar fark etmeksizin blokzincir altyapısında bir verinin eklenmesinin, silinmesinin veya değiştirilmesinin mümkün olmaması, işlemlerde dijital imzalama kriptografik mekanizmasının kullanılması, söz konusu işlemlerin güvenliğini arttıran ve verilerin geriye yönelik takibini sağlayan bir yapı ortaya koymaktadır. Bahsedilen bu hususlar blokzincirde bulunan verileri delil niteliği ve kuvveti bakımından özel olarak incelemeyi gerekli kılmaktadır. Çalışmamızda blokzincirdeki verilerin genel olarak özelliklerinden bahsedildikten sonra, bu verilerin medeni yargı alanında mevcut ispat sistemimiz içinde hangi kurumlara karşılık gelebileceği değerlendirilecek ve karşılaştırmalı hukuk düzenlemeleri ve yargı kararları da ele alınarak konuyla ilgili kişisel görüş ve önerilerde bulunulacaktır.

Anahtar kelimeler: Blokzincir teknolojisi, veri, ispat hukuku, delil niteliği, hukuk yargılaması.

* Dr. Ar. Gör, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi, Medeni Usul ve İcra İflas Hukuku Anabilim Dalı, elifirmak.kilic@medeniyet.edu.tr. ORCID: 0000-0002-4088-6227.

EXAMINATION THE EVIDENTIAL VALUE OF DATA IN BLOCKCHAIN TECHNOLOGY IN TERMS OF CIVIL PROCEDURE

ABSTRACT

Blockchain technology is a distributed database where blocks are linked together like a chain. Although in the first place cryptocurrencies and the financial sector come to mind when blockchain technology is mentioned, this technology is used in many different areas such as providing cyber security, crowdfunding, creating and protecting digital documents, distribution and tracking of drugs in the health sector, realization of land registry transactions and voting.

As the usage area of blockchain technology in the world diversifies and develops day by day, it is obvious that this technology will spread to human life even more and will appear in many transactions in our daily lives. In this respect, it will be possible to present various transactions and records in the blockchain infrastructure as evidence in connection with a dispute in civil proceedings. At this stage, it is important to evaluate the data in the blockchain technology, which has entered our lives relatively recently, in terms of law of evidence. In order to ensure the healthy functioning of the proof activity and the legal certainty of the concepts, the issues such as the evidential nature of these data according to our positive regulations, the presentation and evaluation method of the evidences a need to be addressed.

The digital signatures using structure of blockcahin database that makes impossible to add, delete or change a data without other users notice, introduces a mechanism that increases the security of the transactions and ensures the retrospective tracking of the data. These mentioned issues make it necessary to examine the data in the blockchain specifically in terms of evidence quality and strength. In our study, after the general characteristics of the data in the blockchain are mentioned, it will be evaluated which institutions these data can correspond to in our current proof system in the field of civil jurisdiction, and personal opinions and suggestions will be made by considering comparative legal regulations and judicial decisions.

Keywords: Blockchain technology, data, the law of evidence, the evidential value, civil procedure.

BİLİŞİM TEKNOLOJİSİNDE BİR SUİSTİMAL ÖRNEĞİ: BİLİŞİM SİSTEMLERİNİN KULLANILMASI SURETİYLE DOLANDIRICILIK SUÇLARI

Ali Tanju SARIGÜL*

ÖZET

Karmaşıklaşan yaşam ilişkileri karşısında, bilişim sistemlerinin gelişmesine paralel olarak, ekonomik suçların yaygın bir biçimde işlendiğine her geçen gün daha fazla tanık olmaktayız. Ekonomik suçlar çoğunlukla örgütlü bir biçimde işlenmekte, toplumda maalesef çok sayıda mağdur yaratmaktadır.

Ekonomik suçlar arasında en fazla karşılaştığımız suçlardan biri kuşkusuz dolandırıcılık suçudur. 5237 sayılı Türk Ceza Kanunu'nda dolandırıcılık suçunun tipik fiili *"hileli davranışlarla bir kimseyi aldatıp, mağdurun veya başkasının zararına olarak kendisine veya başkasına yarar sağlamak"* olarak tanımlanmıştır. Suçun nitelikli hallerinden birini de *"bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi"* oluşturmaktadır (TCK m. 158/1-f).

Bilişim teknolojisi; sesli-görüntülü haberleşme, elektronik imzanın kabulü ve internet bankacılığı ile para transferi gibi sunduğu imkânlar sayesinde günümüzde ticari ilişkilerin ve toplumsal yaşamın vazgeçilmez bir parçası olmuştur. Ancak bilişim teknolojisinin sunduğu bu imkânlar, Kanun'un ilgili madde gerekçesinde de vurgulandığı üzere; dolandırıcılık suçunun işlenmesinde önemli bir kolaylık sağlamaktadır. Gerçekten günümüzde phishing (şifre avcılığı) ve cryptolocker (fidye virüsleri) gibi bazı yöntemler kullanılarak dolandırıcılık ya da bilişim suçlarından herhangi birinin kolaylıkla işlenebildiğini görmekteyiz.

Bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen dolandırıcılık suçunun oluşabilmesi için, gerçek kişilerin iradelerini sakatlamaya yönelik hileli davranışların bilişim sistemi aracılığıyla gerçekleştirilmesi gerekir. Bu suç, malvarlığına karşı işlenen suçlar arasında dolandırıcılık suçunun nitelikli hali olarak düzenlenmiştir. Söz konusu suçun tipiklik unsurları, Kanun'da bilişim alanında suçlar arasında yer verilen *"sistemi*

* Dr. Öğr. Üyesi, Hasan Kalyoncu Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi, E-posta: atanju.sarigul @ hku.edu.tr, ORCID ID: https://orcid.org/0000-0002-4112-0311.

engelleme, bozma, verileri yok etme ya da değiştirmek suretiyle haksız çıkar sağlanması (TCK m. 244/4)" suçunun unsurları ile benzerlik göstermektedir.

Tebliğde; öncelikle bilişim sistemleri yoluyla işlenen dolandırıcılık suçlarında sık karşılaşılan yöntemlerden örnekler vermek suretiyle bahsedilecek, suç vasfı bakımından tartışılacaktır. Tebliğde ayrıca, TCK m. 158/1-f, m. 142/2-e ve 244/4. maddeleri, tipiklik unsurları itibariyle karşılaştırılmak suretiyle aralarındaki içtima ilişkisi ortaya konulmaya çalışılacaktır.

Anahtar Sözcükler: Bilişim Sistemi, Bilişim Teknolojisi, Bilişim Suçu, Ceza Hukuku, Dolandırıcılık Suçu.

A TYPE OF MISUSE IN INFORMATION TECHNOLOGY: FRAUD CRIMES BY USING INFORMATION SYSTEMS

ABSTRACT

In the face of complex life relations, we are witnessing more and more economic crimes being committed in parallel with the development of information systems. Economic crimes are mostly committed in an organized manner, unfortunately creating many victims in the society.

Undoubtedly, fraud is one of the most common economic crimes. In the Turkish Penal Code No. 5237, the typical act of fraud is defined as *"deceiving a person with fraudulent behavior and providing benefit to himself or someone else at the expense of the victim or someone else"*. One of the qualified cases of the crime is that it is committed by using information systems as a tool (TCK Art. 158/1-f).

Today information technology has become an indispensable part of commercial relations and social life, thanks to the opportunities it offers such as audio-visual communication, acceptance of electronic signature, and money transfer via internet banking. However, these possibilities offered by information technology, as emphasized in the justification of the relevant article of the Law; It provide an important convenience in committing the crime of fraud. Indeed, nowadays, we see that any of the fraud or computer crimes can be committed easily by using some methods such as phishing (password hunting) and using crypto lockers (ransomware).

In order for the crime of fraud by the use of information systems as a tool to occur, fraudulent acts aimed at injuring the will of real persons must be carried out through the information system. This crime is regulated as the qualified form of fraud crime among the crimes committed against property. The typicality elements of the aforementioned crime are similar to the elements of the crime of *"obstructing the system, disrupting, destroying or changing the data (TCK Art. 244/4)"*, which is among the crimes in the field of informatics.

In the Presentation; first of all, the most common methods of fraud crimes committed through information systems will be mentioned by giving examples, and the examples will be discussed in terms of crime. Also in the Presentation, Turkish Penal Code articles 158/1-f, 142/2-e and 244/4 will be discussed comparatively in terms of typicality elements and the interrelationship between them will be tried to be revealed.

Keywords: Information System, Information Technology, Computer Crime, Criminal Law, Fraud Crime.

TÜRK CEZA HUKUKUNDA YENİ BİR SUÇ TİPİ OLARAK BİLİŞİM SİSTEMLERİ ARACILIĞIYLA İŞLENEN ISRARLI TAKİP SUÇU

Dr. Öğr. Üyesi Nurten ÖZTÜRK*

ÖZET

27 Mayıs 2022 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren 7406 sayılı Türk Ceza Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile TCK'da önemli değişiklikler yapılmıştır. Bunlardan biri de ısrarlı takibin 123/A maddesiyle Kanun'a eklenmesi olmuştur. Böylece karşılaştırmalı hukukta pek çok ülke kanununda cezalandırılan fiiller Türk hukukunda da müstakil bir suç olarak yaptırım altına alınmıştır. Israrlı takip esasında cinsel taciz ve aile içi şiddetle de yakından bağlantılıdır. Israrlı takip suçuyla ısrarlı bir şekilde; fiziken takip etmek ya da haberleşme ve iletişim araçlarını, bilişim sistemlerini veya üçüncü kişileri kullanarak temas kurmaya çalışmak suretiyle bir kimse üzerinde ciddi bir huzursuzluk oluşmasına ya da kendisinin veya yakınlarından birinin güvenliğinden endişe duymasına neden olma cezalandırılmıştır. Ayrıca suçun çocuğa ya da ayrılık kararı verilen veya boşandığı eşe karşı işlenmesi, mağdurun okulunu, iş yerini, konutunu değiştirmesine ya da okulunu veya işini bırakmasına neden olması, hakkında uzaklaştırma ya da konuta, okula veya iş yerine yaklaşmama tedbirine karar verilen fail tarafından işlenmesi halleri cezanın artırılmasını gerektiren nitelikli haller olarak düzenlenmiştir. Suçun soruşturulması ve kovuşturulması şikâyete bağlı olup ısrarlı takip suçu altı aydan 2 yıla kadar hapis cezasıyla yaptırım altına alınmıştır. Böylelikle TCK'da Hürriyete Karşı Suçlar bölümünde seçimlik hareketli yeni bir suç tipi düzenlenmiştir. Söz konusu seçimlik hareketlerden biri de bilişim sistemi aracılığıyla ısrarlı takip fiillerinin gerçekleştirilmesidir.

Bilişim ve teknoloji alanında yaşanan gelişmeler yeni suç türleri ortaya çıkardığı gibi klasik suç türlerinin de bilişim suretiyle işlenmesine de neden olmuştur. Günümüzde haberleşme, iletişim ve bilişim alanında yaşanan gelişmelerle bu sistemlerin yoğun ve yaygın olarak kullanılması kişilerin iletişiminde de kolaylıkları beraberinde getirmiştir. TUİK verilerine göre 2021 yılında internet kullanım oranı 16-74 yaş aralığında %82,6 olmuştur.[1]

* Erzincan BY Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, nozturk@erzincan.edu.tr, Orcid-id: 0000-0001-5500-4250.

1 https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437, E.T. 19.07.2022.

İnternetin, bilişim sistemlerinin günlük birçok faaliyetin gerçekleştirilmesinde kullanılmasının yanında farklı suç tipleri de bu alan vasıtasıyla işlenmektedir. Israrlı takip niteliğindeki fiiller de sıklıkla bilişim sistemleri aracılığıyla gerçekleştirilmektedir. Nitekim daha kolay ve çabuk bir haberleşme imkânının yanında failler sosyal medya, farklı uygulamalar, programlar aracılığıyla mağdurlarla etkileşime geçebilmektedir. Örneğin tweet atmak, durum paylaşımı yapmak, yer bildiriminde bulunmak ısrarlı takip suçuna konu olabilecektir. Yine günümüzde pek çok cihazda bulunan GPS ile kişilerin bulundukları konumların takip edilmesi de mümkündür.

Çalışmada bilişim sistemi özelinde ısrarlı takip suçu ele alınacak olup günümüzde bu tür fiillerin cezalandırılması gerekliliği üzerinde durulacaktır.

Anahtar kelimeler: ısrarlı takip, bilişim sistemi, internet, sosyal medya, ceza

STALKING THROUGH INFORMATION SYSTEMS AS A NEW TYPE OF CRIME IN TURKISH CRIMINAL LAW

ABSTRACT

With the Law No. 7406 on the Amendment of the Turkish Penal Code and Some Laws, which was published in the Official Journal on May 27, 2022, significant changes were made in the Turkish Penal Code. One of them was the addition of stalking to the Law with article 123/A. Thus, the acts punished in the laws of many countries in comparative law are also sanctioned as an independent crime in Turkish law. Stalking is also closely linked to sexual harassment and domestic violence. With the crime of stalking; it is punished persistently to cause serious unrest on a person or to worry about the safety of herself/himself or one of her/his relatives by following her/him physically or trying to contact by using communication and communication tools, information systems or third parties. In addition, if the crime is committed against the child or the spouse with whom a separation decision has been made or divorced, it causes the victim to change her/his school, workplace, residence or quit her/his school or job, and is committed by the perpetrator who is condemned with restraining order or is banned to approach the house, school or workplace, amount of penalty will be increased. The investigation and prosecution of the crime depends on the complaint, and the crime of stalking is sanctioned with imprisonment from six months to 2 years. Thus, a new optional act crime type has been regulated in the TPC, in the section of Crimes Against Liberty. One of these elective actions is the committing of stalking actions through the information system.

Developments in the field of informatics and technology have led to new types of crime, as well as the classic crime types to be committed by means of informatics. Today, with the developments in the field of communication, and informatics, the intensive and widespread use of these systems has brought convenience in the communication

of people. According to Turkish Statistical Institute data, the rate of internet usage in the age group of 16-74 in 2021 was 82.6%. In addition to the use of the Internet and information systems in the realization of many daily activities, different types of crimes are also committed through these systems. Actions in the nature of stalking are also often carried out through information systems. As a matter of fact, in addition to an easier and faster communication opportunity, the perpetrators can interact with the victims through social media, different applications and programs. For example, tweeting, sharing status, reporting location may be the subject of stalking. It is also possible to track the location of people with GPS, which is available in many devices today.

In the study, the crime of stalking through the information system will be discussed, and the necessity of punishing such acts will be emphasized today.

Keywords: stalking, information system, internet, social media, punishment

“BİLİŞİM YOLUYLA” SUÇTAN KAYNAKLANAN MALVARLIĞI DEĞERLERİNİN AKLANMASI SUÇUNA GÜNCEL BİR ÖRNEK: TWITCH BIT SCAM OLAYLARI

Arş. Gör. İlkay ELBEY*

ÖZET

Twitch (ya da Twitch.tv), elektronik spor ve video oyunu odaklı canlı görüntü akışlı sosyal medya platformudur. Geçtiğimiz aylarda Twitch platformuna ait kullanıcı bilgilerinin de dahil olduğu veri seti internete sızdırılmıştır. Sızdırılan veriler arasında yer alan yayıncıların Twitch üzerinden kazandığı gelirleri gösteren tablolar incelendiğinde, bazı yayıncıların takipçi ve destekçi sayılarıyla uyuşmayan olağandışı boyutta Bit adı verilen sanal emtia geliri elde ettiği tespit edilmiştir.

Araştırmalar ve bazı yayıncıların itirafları, bu gelirlerin aşağıdaki aşamalar sonucunda elde edildiği ortaya çıkarmıştır:

1) Banka veya kredi kartı bilgilerinin ele geçirilmesi

2) Kullanıcılar tarafından ele geçirilen kart bilgileri ile Bit alınması

3) Kullanıcılar tarafından anlaşmalı yayıncılara Bit bağışı yapılması

4) Anlaşmalı yayıncıların Twitch’ten aylık gelirini edindiğinde bir kısmını kullanıcılara göndermesi

Ortaya çıkan tablo, yaklaşık 150 yayıncının dahil olduğu yaklaşık 9.8 milyon dolar hacimli, somut vakaların özelliklerine göre banka veya kredi kartlarının kötüye kullanılması veya bilişim suretiyle dolandırıcılık suçları ile başlayan, suçtan kaynaklanan malvarlığı değerlerini aklama suçu ile sonuçlanan bir suç yoluna işaret etmektedir. Banka veya kredi kartları bilgilerinin bazılarının daha önce alışveriş için kullanılan bazı sitelerde kayıtlı kullanıcı bilgilerinin sitelerin hacklenmesi yoluyla elde edilmiş olması bilişim yoluyla işlenen başka öncül suçları da tartışmaya açmaktadır. Suçtan kaynaklanan malvarlığı değerlerinin aklanmasında kripto paraların kullanılması ise olayın bilişim hukuku bakımından önem gösteren bir başka yönünü oluşturmaktadır.

* Araştırma Görevlisi, Kocaeli Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, ORCID ID: 0000-0001-7238-2392, E-posta: ilkay.elbey@kocaeli.edu.tr

Çalışmamızın amacı, Twitch'te yaşanan olayların ceza sorumluluğu bakımından değerlendirilmesidir. İlk bölümde incelemeye konu olayın gerçekleştiği yayın platformu olan Twitch hakkında çalışmamızda gerektiği ölçüde bilgiler verilecektir. Twitch, Bit, Bit scam gibi kavramlar açıklanarak Twitch'te gelir elde etme yolları ortaya konulacaktır. İkinci bölümde Twitch'te yaşanan olayların ceza sorumluluğu bakımından incelenmesi amaçlanmaktadır. İncelemeye konu olayda faillerin Türk Ceza Kanununda yer alan banka veya kredi kartlarının kötüye kullanılması (m.245), bilişim suretiyle dolandırıcılık (m.158/1-f) ve suçtan kaynaklanan malvarlığı değerlerini aklama (m.282) suçları odağında ceza sorumluluğu değerlendirilecektir. Üçüncü bölümde ise bilişim hukukuyla bağlantılı Twitch olayları odağından ortaya çıkan bazı sorulara yanıtlar aranacaktır.

Anahtar kelimeler: Twitch, Bit, banka veya kredi kartlarının kötüye kullanılması, bilişim suretiyle dolandırıcılık, suçtan kaynaklanan malvarlığı değerlerini aklama.

A CURRENT EXAMPLE OF THE CRIME OF LAUNDERING ASSETS RESULTING FROM CRIME (MONEY LAUNDERING) "THROUGH INFORMATICS": TWITCH BIT SCAM INCIDENTS

ABSTRACT

Twitch (or Twitch.tv), is a live streaming social media platform focused on electronic sports and video gaming. In the past months, a data set, including user information of the Twitch platform, has been leaked to the Internet. Deciphering the tables showing the income earned by broadcasters on Twitch, which are among the leaked data, it was found that some broadcasters received an unusually large amount of virtual commodity income called Bit, which does not match the number of followers and supporters.

Research and the confessions of some publishers have revealed that these revenues are obtained as a result of the following stages:

1) Obtaining bank or credit card information

2) Receiving Bits with card information obtained by users

3) Donation of Bit by users to contracted publishers

4) Contracted broadcasters send part of their monthly income from Twitch to users when they receive it

The resulting picture with a volume of about $ 9.8 million, in which about 150 broadcaster are involved, indicates the path of crime which according to the characteristics of concrete incidents starting with the crimes of abuse of bank or credit cards or crime of committing fraud by using ınformatics systems as a tool,

ending with the crime of laundering assets resulting from crime. The fact that some of the bank or credit card information has been obtained through hacking of user information registered on some sites previously used for shopping opens up the discussion other premise crimes committed through informatics technology. The use of crypto currencies in laundering constitutes another aspect of the incident that shows importance in terms of informatics law.

The purpose of our study is to evaluate the incidents on Twitch in terms of criminal liability. In the first section, will be provided to the extent necessary in our study information about Twitch, the broadcasting platform where the incident subject to review took place. Concepts such as Twitch, Bit, Bit scam will be explained and ways to earn income on Twitch will be revealed. In the second part, it is aimed to examine the events on Twitch in terms of criminal liability. The responsibility of the perpetrators will be evaluated in the incident subject, focusing on the contained in the Turkish Criminal Code that the crimes of abuse of bank or credit cards (art. 245), crime of committing fraud by using ınformatics systems as a tool (art. 158/1-f), the crime of laundering assets resulting from crime (money laundering) (art. 282) In the third section, answers will be sought to some questions related to informatics law arising from the focus of Twitch events,

Keywords: Twitch, Bit, the abuse of bank or credit cards, committing fraud by using informatic systems as a tool, laundering assets resulting from crime.

KRİPTO PARA MADENCİLİĞİ VE CEZA HUKUKU SORUMLULUĞU

Osman Gazi ÜNAL*

ÖZET

Satoshi Nakamoto'nun 2008 yılında yayımlamış olduğu "Bitcoin: Eşten-eşe Elektronik Nakit Ödeme Sistemi" adlı makalesiyle ileri sürdüğü kripto para veya kripto varlıklar dünyamıza büyük bir devrim getirmiştir. Bu makalede merkezi olmaktan uzak, çevrimiçi ve iki kişinin kolaylıkla transfer edebileceği bir elektronik ödeme sistemi izah edilmiştir. Bu ödeme ise kripto paralar yoluyla yapılmaktadır. Kripto para özel bir algoritma temelli olup şifreleme metotlarıyla koruma altına alınan, dağıtımı için dijital anahtarlara gereksinim duyan, dönüştürülebilir dijital bir değiş tokuş aracıdır. Kripto paralar sayesinde ödemeler; dünyanın herhangi bir yerine, üçüncü kişilerin müdahalesi olmaksızın, daha hızlı ve hesap kayıtlarının anonim olmasıyla güvenli bir şekilde yapılabilmektedir. Bu işlemler herkese açık olarak görüntülenmekle birlikte kaydedilir ve tüm bu işlemler blok zincir olarak adlandırılır.

Kripto paralar iki şekilde elde edilebilmektedir. İlk olarak belli bir meblağ karşılığında internet sitelerinden ve buna özgü oluşturulan borsalardan kripto para temin edilebilmektedir. İkinci olarak kripto madencilik yoluyla kripto paralar çıkarılabilmektedir. Günümüzde kripto paraların alımı satımı ve borsa işlemleriyle ilgili ceza hukukuna yansıyan akademik çalışmalara rastlamak mümkündür. Buna karşılık kripto para madenciliği ile ilgili akademik çalışmalar oldukça azdır. Bu yüzden konunun bu kısmının araştırılmasına ihtiyaç vardır. Bilinmelidir ki kripto madencilik bu varlıkların elde edilmesinde adeta dijital bir darphane görevi görmektedir. Bu darphane tamamen kullanıcıların kazım gücüne bağlı olarak değişmekte ve herhangi bir merkez bankasına tabi tutulmamaktadır.

Çalışmada, öncelikle kripto paraların Türk hukuk sistemindeki konumu tartışmaya açılacak, daha sonra kripto madenciliğin çalışmasıyla ilgili genel bilgilere yer verilecektir. Bu madencilik sistemleri kendi içerisinde CPU, GPU, ASIC, Hard Disk, bulut madencilik ve musluk siteleri olmak üzere 6 alt türe ayrılmaktadır. Dünyada olduğu gibi ülkemizde de bu madencilik türleriyle kripto para elde edilebilmektedir. Bu türlerin ayrı ayrı incelenmesi konunun anlaşılması için önemlidir. Türlere göre madencilik ekipmanlarının alınmasının, elde bulundurulmasının, kazım yapılmasının, işletilmesinin ve neden olduğu sonuçların bir cezai sorumluluğu doğurup doğurmadığı hususu çalışmamızın asıl konusunu oluşturmaktadır. Ayrıca bu noktada hangi suçların işlenebileceği ya da yeni bir suç tipi ihdasına ihtiyaç olup olmadığı sorunu da incelenmiş olacaktır.

* Osman Gazi ÜNAL, Dr. Araştırma Görevlisi, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Anabilim Dalı, osman.unal@hbv.edu.tr, ORCID NO: 0000-0002-3101-0645.

Anahtar Kelimeler: Kripto para, kripto para madenciliği, blok zincir, madencilik türleri, ceza hukuku sorumluluğu.

THE CRYPTOCURRENCY MINING AND CRIMINAL LAW LIABILITY

ABSTRACT

Cryptocurrency or crypto assets, which Satoshi Nakamoto presented with his article titled "Bitcoin: A Peer-to-Peer Electronic Cash System" published in 2008, has revolutionized to our world. At this article, a decentralized, online and easily transferable electronic payment system is explained. This payment is carried through cryptocurrencies. Cryptocurrency is a convertible digital exchange instrument that based on a special algorithm, protected by encryption methods, requiring digital keys for its distribution. Payments through cryptocurrencies; it is able to be enabled anywhere in the world, without the intervention of third parties, faster and securely with anonymous account records. Along with these transactions are publicly viewed, they are recorded and all these are called blockchain.

Cryptocurrencies can be earned in two ways. First of all, they can be obtained from websites and stock exchanges specifically created for a certain amount. Secondly cryptocurrencies can be extracted through cryptomining. Nowadays, it is possible to find a number of new academic studies that are reflected in the criminal law regarding the purchase and sale of cryptocurrencies and stock exchange transactions. In contrast, academic studies on cryptomining are quite scare. For this reason, this part of the subject needs to be researched. It should be known that cryptomining acts like a digital mint in earning this assets. This mint changes completely depending on the mining power of users and is not subject to any central bank.

In this study, firstly, the position of cryptocurrencies in the Turkish legal system will be discussed, and then general information on work of cryptomining will be given. This mining systems are divided into 6 sub-types as CPU, GPU, ASIC, Hard Disk, cloud mining and faucet websites. Cryptocurrency can be earned with these types of mining in our country as well as in the world. Examining these sub-types separately is important for understanding the topic. The main issue of our study is whether the acquisition, possession, operation and consequences of mining equipment according to sub types lead to criminal law liability. In addition, at this point, the problem of which offences can be committed or whether there is a need to form for a new type of crime will be examined.

Keywords: Cryptocurrency, cryptomining, blockchain, mining types and criminal law liability.

ÇOCUKLARIN SİBER ALANDA CİNSEL AMAÇLAR İÇİN TEŞVİKİ (CYBER-GROOMING)

Prof. Dr. E. Eylem AKSOY RETORNAZ*

ÖZET

Gelişen teknolojiler, bireyler arası iletişim yöntemlerini dönüşüme uğratarak, siber alana taşımıştır. Akıllı telefonlar, tabletler ve bilgisayarlar aracılığıyla görüntü ve anlık mesajlaşmalar bu yeni iletişim biçiminin önemli bir parçası haline gelmiştir.

Türkiye İstatistik Kurumu 2021 yılı 6-15 Yaş Grubu Çocuklarda Bilişim Teknolojileri Kullanımı Araştırması'na göre internet kullanımı, 6-15 yaş grubundaki çocuklar için 2013 yılında %50,8 iken 2021 yılında %82,7'e yükselmiştir. Düzenli İnternet kullanan çocukların %31,3' ü interneti sosyal medya için kullandığını belirtilmiştir. Sosyal medyayı kullanan 6-15 yaş grubundaki çocukların %77,7' sinin her gün, %16,5' inin haftada en az bir defa, %5,8' inin ise haftada bir defadan az sosyal medya kullandığı tespit edilmiştir.

İletişimin siber alana taşınması çocukları hedef alan bazı davranış biçimlerini ve siber şiddeti de beraberinde getirmiştir. Siber alanda, çocuklar gittikçe artan bir biçimde siber alanda cinsel istismar ve cinsel taciz davranışlarına maruz kalmaktadır. Hemen hemen tüm sosyal ağlarda kullanıcıların sahte çevrimiçi profiller oluşturması mümkündür. İnternete erişimle büyüyen çocuklar, pedofillerin potansiyel hedefi haline gelmektedir.

Bu tebliğde siber alanda çocukların cinsel amaçlar için teşviki (cyber grooming) kavramı açıklanmaya çalışılacak ardından karşılaştırmalı hukukta siber alanda çocukların cinsel amaçlar için teşvikiyle mücadeleye ilişkin düzenlemeler ve Türk ceza hukukundaki durum incelenecektir.

Anahtar kelimeler: Siber cinsel teşvik, kışkırtma, cinsel istismar, cinsel taciz

* Galatasaray Üniversitesi Hukuk Fakültesi Bilişim ve Teknoloji Hukuku Anabilim Dalı Başkanı

ONLINE SOLICITATION OF CHILDREN FOR SEXUAL PURPOSES (CYBER GROOMING)

ABSTRACT

As the age of using technological devices and internet decreases, children become easy targets for cybercrimes. Their vulnerability and innocence on the one hand and the accessibility and anonymity of the internet on the other creates opportunities for the commitment of sexual offences against children in cyber space. One such offence is cyber grooming, which is very dangerous because of the gravity of its possible consequences on a child's life, but also because of the significantly vague scope of application arising from the difficulties to detect the real intent of the groomer. Although international legislation has influenced some national legal systems to criminalize child grooming as a separate offence, Turkish law has not initiated such a reaction yet. However, there exists other courses of action to criminalize cyber grooming in order to prevent such threats to a child's physical and moral well-being.

Keywords: Cyber grooming, solicitation, sexual abuse, sexual harassment

SOSYAL MEDYANIN DEZENFORMASYONLA İMTİHANI

Güneş OKUYUCU ERGÜN*

ÖZET

Dijital teknoloji alanındaki gelişmeler, sosyal medyayı bilgiye ulaşmanın, bilgiyi yaymanın ve kendini ifade etmenin önemli bir aracı haline getirmiştir. Gündelik yaşamın vazgeçilmez bir parçasına dönüşen sosyal medya, düşüncenin, bilginin ve haberlerin mesafelere ve sınırlara bağlı olmaksızın hızla yayılmasını sağlaması sayesinde kamuoyu oluşturmak ve kamuoyunu şekillendirmek bakımından çok etkili olabilmektedir. Ancak doğru ve gerçek bilgiler kadar; yanlış veya yanıltıcı bilgiler ve haberler de sosyal medya aracılığıyla aynı şekilde hızla ve kolayca yayılabilmektedir. Bu yanlış veya yanıltıcı bilgiler ve haberler, bireylere ilişkin olabileceği gibi, toplumu ilgilendiren konulara ilişkin de olabilir. Söz konusu yanlış yahut yanıltıcı bilgilerin ya da haberlerin manipülatif amaçlarla ortaya atılması ise, dezenformasyon olarak adlandırılmaktadır. Seçimler, iklim değişikliği, Corona virüs salgını gibi geniş kitleleri ilgilendiren konular, sosyal medyada dezenformasyonla karşılaşılan alanların tipik örneklerindendir. Kitlelerin bu şekilde manipüle edilmesinin kamu düzeni, kamu güvenliği, halk sağlığı gibi hususlarda yaratabileceği sakıncalar nedeniyle dezenformasyon, tüm dünyada olduğu gibi, ülkemizde de son zamanlarda çok konuşulan konulardan biri haline gelmiştir. Bu konuda bir yasa tasarısının da gündemde olduğu bilinmektedir. Ancak dezenformasyonun suç olarak düzenlenebilip düzenlenemeyeceği ve eğer düzenlenecekse bunun koşulları oldukça tartışmalıdır.

Kimi durumlarda yalan, yanlış ya da yanıltıcı nitelikteki paylaşımlar; hakaret, tehdit, cinsel taciz, özel hayatın gizliliğini ihlal, kişisel verilere ilişkin suçlar, iftira, halkı kin ve düşmanlığa tahrik veya aşağılama, suç işlemeye tahrik gibi suçlar şeklinde ortaya çıksa da hiçbir suça vücut vermedikleri haller de söz konusu olabilir. İşte bu gibi durumların ayrıca suç olarak düzenlenmesi ve bu düzenlemenin uygulamada ne gibi sorunlara yol açacağı soru işaretlerini de beraberinde getirmektedir. Özellikle dezenformasyon gibi belirsiz bir kavrama dayanarak suç ihdas edilmesinin doğurabileceği sakıncalar tereddütlere neden olmaktadır. Bir paylaşımın dezenformasyon amaçlı olup olmadığının belirlenmesindeki zorluklara ek olarak, bu belirlemenin hangi ölçütlere dayanarak kim tarafından yapılacağı da tartışmalıdır. Dezenformasyon içerikli paylaşımların

* Doç. Dr., Ankara Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, ORCID: https://orcid.org/0000-0001-5401-2312, E-Posta: okuyucu@law.ankara.edu.tr

denetimi için ayrı bir kurumsal mekanizmanın kurulması ve dezenformasyonun ancak organize, örgütlü ve belirli bir amaca yönelik olma ölçütüne dayanarak yaptırıma bağlanması şeklindeki çözüm önerilerinin de konuyla ilgili sorunları tam anlamıyla çözmeye yetmeyeceği ortadadır. Bu yöndeki düzenlemelerin uygulamada ifade ve basın özgürlüğünün sınırlanmasına yönelik olarak kullanılması ihtimali endişelere yol açmaktadır. Sosyal medya esas itibariyle haber alma hakkının, basın, iletişim ve ifade özgürlüğünün bir yansımasıdır ve dolayısıyla sosyal medya ve dezenformasyonla ilgili olarak yapılacak düzenlemelerin Avrupa İnsan Hakları Sözleşmesi'nin ifade özgürlüğünü düzenleyen 10. maddesine uygun olması gerekir. Avrupa İnsan Hakları Mahkemesi'nin içtihadı incelendiğinde, Mahkemenin ifade hürriyetinin internet ortamında kullanımı ile diğer haklar ve gereklilikler arasındaki hassas dengeyi itina ile gözetmeye çalıştığı görülmektedir. Bu noktada çelişen menfaatler arasında böyle bir hassas dengenin kurulmasının hem çok önemli hem de bir o kadar zor olduğu belirtilmelidir. Ayrıca söz konusu düzenlemelerin bir sansür ve otosansür mekanizmasına dönüşerek baskı aracı haline gelmemesi gerektiği önemle vurgulanmalıdır.

Anahtar Kelimeler: Sosyal Medya, Dijital Teknolojiler, Dezenformasyon, İfade Özgürlüğü, Basın Özgürlüğü

DISINFORMATION AS A CHALLENGE FOR SOCIAL MEDIA

ABSTRACT

Developments in the field of digital technology have made social media an important tool for reaching and disseminating information and expressing oneself. Social media, which has become an indispensable part of daily life, can be very effective in creating and shaping public opinion, thanks to its rapid dissemination of thought, information and news regardless of distances and borders. However, as much as accurate and correct information; false or misleading information and news can also spread quickly and easily through social media. These false or misleading information and news may relate to individuals as well as to issues of public concern. The disclosure of false or misleading information or news for manipulative purposes is called disinformation. Issues that concern large masses such as elections, climate change, and the Corona virus epidemic are typical examples of areas where disinformation is encountered on social media. Disinformation has become one of the most talked-about topics in our country, as it is all over the world, due to the disadvantages that such manipulation of the masses may cause in matters such as public order, public safety, and public health. It is known that a draft law on this subject is also on the agenda. However, whether disinformation can be regulated as a crime and if it will be, the conditions for it are highly controversial.

Although in some cases, false, incorrect or misleading posts may occur in the form of insults, threats, sexual harassment, violation of privacy, crimes related to personal data, slander, incitement to hatred and hostility, humiliation, or incitement to commit a crime, there may also be cases where they do not constitute any crime. Regulating such situations as crimes, and the problems that such regulation may cause in practice, raise questions. In particular, the inconveniences of creating a crime based on an ambiguous concept such as disinformation cause hesitations. In addition to the difficulties in determining whether a post is for disinformation purposes, it is also controversial by whom and based on what criteria this determination would be made. It is obvious that the suggested solutions such as the establishment of a separate institutional mechanism for the control of disinformation content sharing and sanctioning the disinformation only based on the criterion of being structured, organised and for a specific purpose will not be sufficient to fully solve the associated problems. The possibility of using regulations in this direction to limit the freedom of expression and press in practice raises concerns. Social media is essentially a reflection of the right to receive information, the freedom of press, communication and expression, and therefore, the regulations to be made regarding social media and disinformation must comply with Article 10 of the European Convention on Human Rights, which regulates the freedom of expression. When the case-law of the European Court of Human Rights is examined, it can be seen that the Court carefully tries to keep the delicate balance between the use of the freedom of expression on the internet and other rights and requirements. At this point, it should be noted that establishing such a delicate balance between conflicting interests is both very important and difficult. In addition, it should be emphasized that the said regulations should not turn into a censorship or self-censorship mechanism or become a tool of pressure.

Keywords: Social Media, Digital Technologies, Disinformation, Freedom of Expression, Freedom of the Press

SİBER ZORBALIKLA MÜCADELEDE YENİ ARAYIŞLAR: OKULLARDA ONARICI ADALET MEKANİZMALARININ KULLANILMASI

Zeynep ARDIÇ*

ÖZET

Bilişim çağı olarak değerlendirilen 21. yüzyılda teknolojinin sunduğu olanaklar sınırsızdır. Hayatın diğer alanlarında olduğu gibi eğitim alanında da teknolojik alet ve platformların ciddi etkilerinin olduğu bilinmektedir. Kovid-19 salgınının eğitimde dijitalleşmeyi hızlandırması teknolojinin eğitim alanında sunduğu olanaklara dikkat çekilmesini sağlamıştır. Ancak bu olanaklar bazı risk ve tehlikeleri de beraberinde getirmektedir; siber zorbalık da bunlardan biridir. Bir kişi ya da grubun bilgi iletişim teknolojilerini kullanarak başka bir kişi ya da gruba yönelik korkutma, yıldırma, üzme veya itibarını zedeleme amaçlı davranışları siber zorbalık olarak tanımlanmaktadır. Siber zorbalık olarak nitelenen davranışlar öğrenciler açısından ciddi tehlikeler barındırmaktadır. Fiziksel ve ruhsal rahatsızlıklara neden olan siber zorbalıkla mücadele etmek bu davranışları önlemeyi amaçladığı gibi söz konusu davranış biçimleri ortaya çıktığında bunlarla yüzleşmeyi ve olumsuz sonuçları ortadan kaldırmayı da gerektirmektedir. Bu bağlamda klasik ceza adaletinin bir yansıması olan geleneksel disiplin mekanizmalarına başvurmak etkin bir çözüm yolu olmaktan uzaktır. Bu mekanizmalara alternatif olarak onarıcı disiplin uygulamalarının benimsenmesi Avustralya, İngiltere, Kanada, Yeni Zelanda gibi ülkelerde denenmiş ve oldukça olumlu sonuçlara ulaşılmasına vesile olmuştur.

Geleneksel ceza adaletine bir alternatif olarak kurgulanan onarıcı adalet mekanizmaları sadece suç, suçlu ve ceza odaklı bir yaklaşımdansa, ortaya çıkan bireysel ve toplumsal zararı ortadan kaldırmak, faili rehabilite ederek tekrar suç işlemesini önlemek, mağdurun gördüğü zararı tazmin etmek gibi daha geniş ve uzun vadeli amaçları bünyesinde barındırmaktadır. Bu bağlamda, siber zorbalık davranışlarında bulunan çocukları cezalandırmaya değil meydana gelen zararı ortadan kaldırmaya yönelen onarıcı disiplin uygulamalarının benimsenmesi umut vaat eden yenilikçi bir yöntem olarak karşımıza çıkmaktadır. Aile konferansı, akran arabuluculuğu, fail ve mağdur panelleri başta olmak üzere pek çok farklı mekanizmayı kapsayan onarıcı disiplin uygulamaları, ceza vererek kısa vadede sorunları ortadan kaldırmayı amaçlayan geleneksel disiplin mekanizmalarından farklıdır. Siber zorbalık sonucunda

* İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Öğretim Görevlisi

ortaya çıkan mağduriyetin giderilmesi için bu durumdan etkilenen aktörler başta olmak üzere diğer öğrencileri, ebeveynleri ve ilgili kurum personelini sürece dâhil etmesi bu yaklaşımın kilit noktasıdır. Ayrıca sadece ortaya çıkan zararın giderilmesi değil uzun vadede benzer davranışların yeniden ortaya çıkmasını da engellemeyi amaçlayan bu süreçlerin ülkemizde de benimsenmesi faydalı olacaktır. Bu çalışma siber zorbalıkla mücadele etmede onarıcı disiplin mekanizmalarının nasıl bir işlev göreceğini incelemeyi ve bu uygulamaların benimsenmesi halinde ne gibi kazanımlar elde edilebileceğini göstermeyi amaçlamaktadır.

Anahtar Kelimeler: siber zorbalık, onarıcı adalet, onarıcı disiplin mekanizmaları

NEW SEARCHES IN FIGHTING AGAINST CYBERBULLYING: USING RESTORATIVE JUSTICE MECHANISMS IN SCHOOLS

ABSTRACT

In the 21st century, which is considered as the information age, the possibilities offered by technology are unlimited. It is known that technological tools and platforms have serious impacts in the field of education as in other areas of life. The fact that the Covid-19 epidemic accelerated the digitalization of education has drawn attention to the opportunities offered by technology in the field of education. However, these possibilities also bring some risks and dangers; Cyberbullying is one of them. Cyberbullying is defined as the behavior of a person or a group using information and communication technologies to intimidate, demoralise, upset or damage another person or group. Behaviors described as cyberbullying pose serious dangers for students. Fighting against cyberbullying, which causes physical and mental disorders, aims to prevent these behaviors and also requires facing them and eliminating the negative consequences when these behaviors occur. In this context, resorting to traditional disciplinary mechanisms, which is a reflection of traditional criminal justice, is far from being an effective solution. The adoption of restorative discipline practices as an alternative to these mechanisms has been tried in countries such as Australia, England, Canada, and New Zealand and has led to very positive results.

Restorative justice mechanisms, which are designed as an alternative to traditional criminal justice, have broader and long-term objectives such as eliminating the individual and social harm that occurs, preventing re-offending by rehabilitating the perpetrator, and compensating the victim's harm, rather than an approach focused only on crime, criminal and punishment. In this context, the adoption of restorative discipline practices that aim at eliminating the harm, rather than punishing children who engage in cyberbullying behaviors, emerges as a promising innovative method. Restorative disciplinary practices, which cover many different mechanisms, especially family conference, peer mediation, perpetrator and victim panels, are different from

traditional disciplinary mechanisms that aim to eliminate problems in the short term by punishing them. The key point of this approach is to involve other students, parents and relevant institution personnel, especially the actors affected by this situation, in order to eliminate the victimization that arises as a result of cyberbullying. In addition, it would be beneficial to adopt these processes in our country, which aim not only to eliminate the damage but also to prevent the re-emergence of similar behaviors in the long term. This study aims to examine how restorative discipline mechanisms will function in fighting cyberbullying and to show what gains can be achieved if these practices are adopted.

Keywords: cyberbullying, restorative justice, restorative discipline mechanisms

BİR SOSYAL MÜHENDİSLİK YÖNTEMİ OLARAK PHISHING (OLTA AVCILIĞI)

Veysel TOPUZ*

ÖZET

Sosyal mühendislik kişi veya kurumlara ait bilgi ve dokümanları haksız çıkar sağlamak amacıyla teknoloji yoluyla ya da insan zafiyetlerinden yararlanarak ele geçirme yöntemleri veya organizasyonları olarak tanımlanabilir.

Günümüzde hem mobil teknoloji alanında hem de bilişim sistemlerinde yaşanan hızlı gelişmeler ve kullanılan cihazların da altyapılarının gelişmesi sebebiyle sosyal mühendislik saldırıları oldukça artmıştır.

Öğretide sosyal mühendislik yöntemleri temeli bilgisayar ve teknolojiye dayanan sosyal mühendislik ile temeli insan zafiyetlerine dayanan sosyal mühendislik yöntemleri olmak üzere ikiye ayrılır.

Sosyal mühendisler kişilere ait bilgileri onlara fark ettirmeden elde etmeye çalıştıkları için değişik saldırı teknikleri kullanmakta, insanları sorularla veya farklı yöntemlerle kandırmaya çalışmaktadırlar.

Kurumlara çalışan olarak sızmak, çalışanlarla arkadaş olmak, teknik servisten arıyormuş gibi görünerek bilgi toplamak, hedef kişiyle dost olunarak kişilerin zaaf ve düşkünlüklerinden yararlanmak, kurum içerisine fiziksel olarak sızmak, omuz sörfü veya çöpleri karıştırmak, phishing, pharming, vishing, spam saldırıları, ekran ve tuş kaydediciler en fazla bilinen sosyal mühendislik yöntemleridir.

Hem küresel anlamda hem ülkemiz özelinde istatistiklere bakıldığında internet üzerinden gerçekleştirilen saldırıların çok büyük bir yoğunluğunu phishing saldırılarının oluşturduğu görülmektedir. Türkçeye oltalama (olta saldırısı), yemleme olarak çevrilebilen phishing, İngilizce "password" ve "fishing" sözcüklerinin birleştirilmesiyle oluşturulan ve bilişim sistemleri üzerinden gerçekleştirilen bir saldırı yöntemini ifade eder.

Olta saldırılarında finansal kurum ve kuruluşlar veya resmi kurumlar veya alışveriş sitelerinden gönderilmiş izlenimi oluşturulan acil ve çok önemli konular içeriyormuş görüntüsü oluşturan sahte e-postalar atılır. Bu mesajlarda kişilerin şifre, parola, müşteri

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

numarası, kullanıcı adı, kredi kartı numarası veya güvenlik kodları isteniyormuş gibi yazılarak, kişilerin bu linklere tıklaması sağlanmaya çalışılmaktadır.

Biz de çalışmamızda bilişim hukukunun interdisipliner bir çalışma alanı da olduğunu göz önüne alarak, hem Türk ceza hukuku doktrininde kavramsal olarak pek fazla söz konusu edilmeyen sosyal mühendislik kavramı hem de bilhassa internet dolandırıcılığı yöntemi olarak kullanılan phishing yöntemi hakkında bilgi vereceğiz.

Anahtar Kelimeler: Phishing, olta avcılığı, internet dolandırıcılığı, sosyal mühendislik

PHISHING AS A SOCIAL ENGINEERING METHOD

ABSTRACT

Social engineering can be defined as methods or organizations to seize information and documents belonging to individuals or institutions through technology or by taking advantage of human vulnerabilities in order to gain unfair advantage.

Today, social engineering attacks have increased considerably due to the rapid developments in both the field of mobile technology and information systems and the development of the infrastructure of the devices used.

Social engineering methods are divided into two as social engineering based on computers and technology, and social engineering methods based on human vulnerabilities.

Since social engineers try to obtain information about people without them noticing, they use different attack techniques and try to deceive people with questions or different methods.

Infiltrating institutions as employees, making friends with employees, collecting information by pretending to be calling from technical service, taking advantage of people's weaknesses and fondness by being friendly with the target person, physically infiltrating the institution, shoulder surfing or messing with garbage, phishing, pharming, vishing, spam attacks, screen and keystroke attacks loggers are the most well-known social engineering methods.

When we look at the statistics both globally and in our country, it is seen that phishing attacks constitute a very large density of attacks carried out over the internet. Phishing, which can be translated as phishing and baiting, refers to an attack method created by combining the English words "password" and "fishing" and carried out over information systems.

In phishing attacks, fake e-mails are thrown that appear to contain urgent and very important issues. In these messages, password, password, customer number, user name, credit card number or security codes are written as if they are requested, and people are trying to click on these links.

In our study, we will provide information about both the concept of social engineering, which is not mentioned much conceptually in the Turkish criminal law doctrine, and especially the phishing method, which is used as a method of internet fraud.

Keywords: Phishing, internet fraud, social engineering

KİŞİSEL VERİLERE İLİŞKİN ÖNEMLİ KORUMA: DİJİTAL TEHDİTLER KARŞISINDA ÇOCUK

Şevval Ceyhan* - Özge Demirdelen**

ÖZET

Sosyal medyanın kullanımı neticesinde kişisel verilerin paylaşılması yaygınlaşmaktadır. Yapılan paylaşımların doğurduğu veya doğurabileceği hukukî anlamın ve sonuçların tam olarak önceden algılaması veya bilmesi ya da tahmin edebilmesi her zaman mümkün değildir. Bu durum kişisel verilerin korunması açısından çeşitli riskleri ortaya çıkarmaktadır. Paylaşılan kişisel verilerle taciz, siber zorbalık, uygunsuz materyallere erişim ve doğrudan pazarlamanın olumsuz etkilerine maruz kalma başlıca risklerden bazılarıdır. Özellikle teknolojik gelişmelerin odağında yer alan çocuklar, dijital ortamların yaygınlığı, algı düzeyleri ve yaşları itibariyle kişisel verilerini paylaşmalarının neticesini öngörememektedirler. Karşılaşacakları dijital tehditlerin neticesinde çocukların kendi haklarını bilmemesi ve ailelerin dijital ortamdaki faaliyetlerde gözetimlerinde yetersiz kalması, çocukları dijital ortamlardaki tehditlere karşı savunmasız hale getirmektedir. Pandemi ile hayatımıza giren uzaktan iletişim çocukların, başta eğitim olmak üzere, sosyalleşme, oyun oynama, eğlenme ve iletişim kurma faaliyetlerini de internet aracılığıyla gerçekleştirmesinde önemli artışa sebep olmuştur. Bu husus da çocukların kişisel verilerine ilişkin olası tehditlere karşı gereken hassasiyetin gösterilmesini ve verilerinin korunmasını gerektirmektedir. Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR) bu konuda özel hükümler içermektedir. GDPR'daki özel hüküm sayesinde AB ülkelerinde örnek teşkil edecek kararlar da verilmektedir. İrlanda Veri Koruma Komisyonu'nun Eylül 2020'de başlattığı soruşturma neticesinde Instagram'a çocukların telefon numaralarının ve e-posta adreslerinin kamuya açık hale gelmesine yol açarak, GDPR'ı ihlal etmesi gerekçesiyle vermiş olduğu 405 milyon Euro tutarındaki para cezası bu kapsamdaki önemli örnek kararlardan birisidir. Kişisel verilerinin korunması kapsamında çocuklar açısından mevzuatımızda ise eksiklikler bulunmaktadır. Kişisel Verilerin Korunması Kanunu (KVKK)'nda konuya dair herhangi bir özel hüküm yer almamaktadır. Bu eksikliğin giderilmesinin yanı sıra önlemlerin alınması ve çocukların menfaatlerinin gözetilmesi açısından ailelerin ve çocukların dijital ortamları daha iyi tanıyabilmesi ve dijital tehditlere karşı korunabilmesi için bu alanda bilgilendirilmeleri de ciddi önem arz etmektedir. Çalışma kapsamında; kişisel verilerin korunması konusu çerçevesinde dijital ortamlarda çocuklara karşı risk teşkil eden konular

* Çağ Üniversitesi, Özel Hukuk Tezli Yüksek Lisans Öğrencisi, ORCID: 0000-0002-5608-4958, avsevvalceyhan@gmail.com
** Çağ Üniversitesi, Milletlerarası Özel Hukuk ABD Araştırma Görevlisi, ORCID: 0000-0001-9046-5124, ozgedemirdelen@cag.edu.tr

değerlendirilecektir. Risklere karşı alınabilecek önlemler, ulusal ve uluslararası düzenlemeler ile kararlar çerçevesinde incelenecektir.

Anahtar Sözcükler: Çocuk, Dijital Tehdit, Kişisel Veri, KVKK, GDPR

IMPORTANT PROTECTION REGARDING PERSONAL DATA: THE CHILD FACING DIGITAL THREATS

ABSTRACT

As a result of the use of social media, the sharing of personal data is becoming widespread. It is not always possible to fully anticipate, know or predict the legal meaning and consequences of the sharing. This situation creates various risks in terms of the protection of personal data. Harassment with shared personal data, cyberbullying, access to inappropriate materials and exposure to the negative effects of direct marketing are some of the main risks. Especially children, who are at the center of technological developments, cannot foresee the result of sharing their personal data in terms of the prevalence of digital environments, their level of perception, and age. As a result of the digital threats they will face, the children's ignorance of their rights and the inadequacy of their families in the supervision of their activities in the digital environment make children vulnerable to the threats in the digital environment. Distance communication, which has entered our lives with the pandemic, has led to a significant increase in children's realization of activities such as education, socialization, playing games, entertainment, and communication via the internet. This issue requires showing the necessary sensitivity against possible threats to the personal data of children and protecting their data. The General Data Protection Regulation (GDPR) of the European Union contains special provisions in this regard. Thanks to the special provision in the GDPR, exemplary decisions are also made in EU countries. As a result of the investigation initiated by the Irish Data Protection Commission in September 2020, the fine of 405 million Euros imposed on Instagram for violating the GDPR by causing children's phone numbers and email addresses to become public is one of the important examples in this context. There are deficiencies in our legislation regarding children within the scope of protection of personal data. The Law on the Protection of Personal Data (KVKK) does not contain any special provisions on the subject. In addition to eliminating this deficiency, it is of great importance to inform families and children in this area so that they can better recognize digital environments and protect them against digital threats to take precautions and protect the interests of children. Scope of study; Within the framework of the protection of personal data, issues that pose a risk to children in digital environments will be evaluated. Measures to be taken against risks will be examined within the framework of national and international regulations and decisions.

Keywords: Child, Digital Threat, Personal Data, KVKK, GDPR

SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ YÖNETİMİNE DAİR DÜZENLEMELERE GENEL BİR BAKIŞ

Alper IŞIK*

ÖZET

Siber güvenlik, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin disiplinli bir şekilde korunmasıdır[1]. Dijitalleşmeyle birlikte özellikle yüksek düzeyde bilgi ve veriye sahip ağlar siber saldırıların öznesi olmaktadır. Bu durum özellikle şirketler ve kamu kuruluşları açısından siber güvenlik uyumu için aktif faaliyetlerde bulunulmasını zorunlu kılmaktadır. Ancak siber güvenlikle ilgili hukuki düzenlemeler tam anlamıyla kurumsallaşmış değildir. AB sathında özellikle AB NIS Direktifi[2] ve Siber Güvenlik Kanunu[3] öncü bir rol üstlenmektedir. Bununla birlikte bağlayıcı olmayan ama uluslararası alanda bilgi güvenliğinin standartlarını belirleyen ISO 27001 ve 27002 Standartları da önemli bir boşluğu doldurmaktadır[4]. Özellikle söz konusu standartlara uyum; prestij, güven ve bilgi güvenliğini sağlamada önemli bir işlevi yerine getirmektedir.

Ülkemizde ise siber güvenlik bağlamında henüz bir yasal düzenleme mevcut değildir. 2000 yılında "*Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı*" gündeme gelmiş ama yasalaşmamıştır. 2016'da yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ise bu alanda önemli bir açığı kapatmaktadır. Ancak Kanun, yalnızca kişisel veri niteliğinde olan bilgilere dair ihlallere uygulanmakta olduğu için kişisel olmayan veriler için KVKK'nın uygulanması söz konusu değildir. Bir siber saldırı söz konusu olduğunda ortaya çıkan ihlallerin öznesinin her zaman kişisel veriler olmayabileceği düşünüldüğünde, bu alanda da bir korumaya ihtiyaç olduğu açıktır.

* Dr. Öğr. Üyesi, Sakarya Üniversitesi Hukuk Fakültesi Genel Kamu Hukuku Anabilim Dalı, alper@sakarya.edu.tr, ORCID: 0000-0002-3784-8297.

1 Antoni Gobeo, Connor Fowler, ve William Buchanan, GDPR and Cyber Security for Business Information Systems (Denmark: River Publishers, 2018), 94.

2 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148 Erişim Tarihi: 29.09.2022.

3 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881 Erişim Tarihi: 29.09.2022.

4 Detaylı bilgi için bknz. Leyla Keser Berber, "Ulusal Siber Güvenlik Stratejilerinde Yer Alan Teknik ve Hukuksal Yaklaşımlar ve Uluslararası Standartların Rolü", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C. XI, S. 1, Yıl: 2014, s. 213-230.

Türk hukukunda her ne kadar müstakil bir siber güvenlik kanunu olmasa da çeşitli kurumlar tarafından çıkartılmış metinlere rastlamak mümkündür. İlk olarak 5809 sayılı Elektronik Haberleşme Kanunu'nun Ek 1. Maddesiyle Siber Güvenlik Kurulu kurulmuştur. 2014 yılında aynı Kanun ile BTK'ya "*siber güvenlik ... konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek*" görevi verilmiştir.

Ayrıca Siber Güvenlik Kurulu'nun 20 Haziran 2013 tarihli ilk toplantısında kritik altyapılar belirlenmiştir. Bunlar; Ulaştırma, Enerji, Bankacılık ve Finans, Su Yönetimi, Elektronik Haberleşme sektörleridir. Aynı toplantıda "*Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*"[5] da kabul edilmiştir. [6]. Söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması öngörülmüştür. Ayrıca siber olaylarla etkin bir şekilde mücadele edebilmek amacıyla 2013 yılında BTK bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. 2014 yılında ise Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü tarafından "*Sektörel SOME Kurulum ve Yönetim Rehberi*"[7] yayınlanmış ve bu belgede Sektörel SOME'lerin görev ve sorumlulukları belirtilmiştir. 2020 yılında ise "*2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı*"[8] yayınlanmıştır. Ancak söz konusu düzenlemeler kanunla yapılmadığı için yaptırım konusu net değildir. Ayrıca düzenlemeler oldukça eski tarihli ve dağınık halde olduğu için hem günümüz ihtiyaçlarına cevap verememekte hem de kavranması güç olmaktadır. Dolayısıyla siber güvenlik bağlamındaki düzenlemelerin müstakil bir kanun olarak yeniden yapılandırılması faydalı olacaktır.

Anahtar Kelimeler: Siber Güvenlik Hukuku, Bilgi Güvenliği, Bilgi Güvenliği Yönetimi, Veri Koruma, ISO Standartları

OVERVIEW OF REGULATIONS ON CYBER SECURITY AND INFORMATION SECURITY MANAGEMENT

ABSTRACT

Cybersecurity is the disciplined protection of the confidentiality, integrity and availability of information. With digitalization, especially networks with high information and data, has become the subject of cyber attacks. This situation necessitates active activities for cyber security compliance, especially for companies

5 Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf Erişim Tarihi: 29.09.2022.

6 https://www.usom.gov.tr/hakkimizda Erişim Tarihi: 29.09.2022.

7 Sektörel SOME Kurulum ve Yönetim Rehberi https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/sektorel-some-reh.pdf Erişim Tarihi: 29.09.2022.

8 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf Erişim Tarihi: 29.09.2022.

and public institutions. However, legal regulations regarding cyber security are not fully institutionalized. The EU NIS Directive and Cyber Security Law play a leading role in the EU. In addition, ISO 27001 and 27002 Standards, which are non-binding but determine the standards of information security in the international arena, also fill a critical gap. In particular, compliance with the said standards is essential in providing prestige, trust and information security.

Our country has no legal regulation in the context of cyber security yet. In 2000, the "Draft Law on the National Information Security Organization and its Duties" came to the fore, but it was not enacted. The Law on the Protection of Personal Data (PDPL) No. 6698, which entered into force in 2016, fills a significant gap in this area. However, since the Law only applies to personal data violations, PDPL is not applicable for non-personal data. Since personal data may not always be the subject of violations that arise in the event of a cyber attack, it is clear that there is a need for protection in this area.

Although there is no independent Cyber Security Law in Turkish Law, it is possible to come across texts issued by various institutions. Firstly, the Cyber Security Board was established with Additional Article 1 of Electronic Communications Law No. 5809. In 2014, with the same Law, the BTK was tasked "*to fulfil the duties assigned by the President, the Ministry and/or the Cyber Security Council on cyber security issues through the Telecommunications Communication Presidency or other units*".

In addition, critical infrastructures were determined at the first meeting of the Cyber Security Board on 20 June 2013. These are; Transportation, Energy, Banking and Finance, Water Management, and Electronic Communication sectors. "*National Cyber Security Strategy and 2013-2014 Action Plan*" were also adopted at the same meeting. . Within the framework of the said action plan, it is envisaged to form Cyber Incidents Response Teams (Corporate SOME, Sectoral SOME) within public institutions and organizations. In addition, the National Cyber Incidents Response Center (USOM) was established within the body of BTK in 2013 to combat cyber incidents effectively. In 2014, the "*Sectoral SOME Installation and Management Guide*" was published by the Ministry of Transport, Maritime Affairs and Communications General Directorate of Communications, and the duties and responsibilities of Sectoral SOMEs are specified in this document. In 2020, the "*2020-2023 National Cyber Security Strategy and Action Plan*" was published. However, the enforcement issue is unclear, as Law does not make these regulations. In addition, since the regulations are outdated and scattered, they cannot meet today's needs and are difficult to comprehend. Therefore, it would be beneficial to restructure the regulations in cyber security as an independent law.

Keywords: Cyber Security Law, Information Security, Information Security Management, Data Protection, ISO Standards

PLATFORM REGÜLASYONU VE AVRUPA BİRLİĞİ DİJİTAL PİYASALAR DÜZENLEMESİ (DIGITAL MARKET ACT) ÜZERİNE DEĞERLENDİRMELER

Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK*

ÖZET

Dijital platformlar günümüz internet ekosisteminin temel aktörü konumundadır. İletişim, alışveriş, eğlence, eğitim, araştırma gibi neredeyse internet ortamında gerçekleştirilen tüm işlemlerde platformlar önemli yer tutmaktadır. Bunun da ötesinde teorik olarak internet ortamında bilginin serbest dolaşımı hedeflense ve internet üzerindeki etkileşimlerde de ifade özgürlüğü gibi temel hak ve özgürlüklere ilişkin korumalar uygulanabilir olsa da fiilen dijital ortamda gerçekleştirilebilecek faaliyetler, paylaşılabilecek içerikler, ulaşılabilecek bilgiler platformların yapısından ve araçlarından etkilenmektedir. Bugün insanların platformları kullanmaksızın sesini duyurması çok zor olabilmekte, platform üzerinden eserlerini sunmayan sanatçılar insanlara ulaşamamakta, çevrim içi alışveriş kanallarını kullanmayan satıcı ve sağlayıcılar tüketicilerden uzak kalmaktadır.

Platformların hayatımızda bu kadar önemli yer tutması platformun kullanıcılarıyla ilişkisinin ve kullanıcıların birbirleriyle ilişkilerinin regülasyonuna dair soruları ve hukukun buradaki rolüne dair tartışmaları beraberinde getirmektedir. Geleneksel olarak bir teşebbüsün piyasa üzerindeki etkisi ve bu etkinin kötüye kullanılıp kullanılmadığı rekabet hukuku müesseseleriyle düzenlenmektedir. Halihazırda da platformların faaliyetlerinin rekabet hukuku bakımından etkileri önemli davalarda tartışılmaktadır. Bununla birlikte rekabet hukuku mekanizmalarının mevcut platform odaklı ekonomide platformların davranışlarının regülasyonunda yetersiz kaldığı iddia edilmektedir. Buradaki boşluğu doldurmak için özellikle platformlara yönelik düzenleme çalışmaları yapılmaktadır. Bunlardan en önemlisi Avrupa Birliğinde kabul edilen Dijital Piyasalar Düzenlemesi'dir (*Digital Markets Act,* **DMA**). DMA geniş bir platform yelpazesini kapsamına almakta ve bazı yükümlülükler getirmektedir. Kapsamın genişliği ve yükümlülüklerin kapsamı da gerek hedeflenen amaca uygunluk gerekse mevcut düzenlemelerle yaratılabilecek çatışmalar bakımından önemli hukuki tartışmaları da beraberinde getirmektedir.

* Boğaziçi Üniversitesi Hukuk Fakültesi Öğretim Üyesi

İşbu tebliğ ile de öncelikle konunun anlaşılabilmesi ve belirsizliğin giderilmesi açısından platform kavramına değinilecektir. Daha sonra sırasıyla platformların regülasyonunun gerekli olup olmadığı ve platform regülasyonunda kullanılabilecek araçlar ile hukuki düzenlemelerin rolü mercek altına alınacaktır. Nihayet çalışma, bu açıklamalar ışığında DMA'nın analiziyle ve Türk hukukuna ilişkin kısa bir değerlendirmeyle sonuçlandırılacaktır.

Anahtar Kelimeler: platform, regülasyon, dijital piyasalar, rekabet, tüketici

THE QUESTION OF PLATFORM REGULATION AND EUROPEAN UNION'S DIGITAL MARKETS ACT

ABSTRACT

Digital platforms are the main actors of today's internet ecosystem. Platforms have an important place in almost all transactions carried out on the internet including, but not limited to, communication, shopping, entertainment, education, and research. Moreover, despite the fact that free circulation of information is aimed on the internet as a theoretical goal and protections provided for fundamental rights and freedoms such as the freedom of expression apply to digital interactions, it is perfectly clear that activities that can be carried out, content that can be shared, and information that can be accessed in the digital environment are affected by the structure as well as tools of the platforms. Today, it can be very difficult for people to make their voices heard without using platforms. Similarly, artists who do not present their works on the platform or businesses that do not provide their goods or services via online channels hardly reach their audience.

The fact that platforms have such an important place and power in our lives raises questions about the relationship of the platform with its users and the regulation thereof along with the role of the law. Traditionally, the effect of an undertaking on the market and whether this effect is abused are governed by competition law rules. Indeed, the effects of the activities of the platforms in terms of competition law are currently discussed in many important cases. However, it is also claimed that competition law mechanisms are insufficient in regulating the behaviour of platforms in the current platform-oriented economy. In order to fill the gap here, regulatory measures specifically addressing platforms are being discussed in many jurisdictions. The most important of these is the Digital Markets Regulation (DMA) in the European Union. DMA covers a wide range of platforms and imposes certain obligations thereon. The breadth of the scope and the accompanying obligations also bring along important legal debates in terms of both suitability for the intended purpose and potential conflicts with the existing regulations.

In this paper, first of all, the concept of platform will be examined in order to understand the subject and to clear the definitional ambiguity. Then, whether the platform regulation is necessary and the tools that can be used in platform regulation shall be explored respectively. Finally, in the light of these explanations, the study will be concluded with the analysis of the DMA and a brief assessment on the implications thereof under the Turkish law.

Keywords: platform, regulation, digital markets, competition, consumer

KRİPTO VARLIK PİYASALARINA İLİŞKİN AB TÜZÜK TEKLİFİ ve MEVZUATIMIZ İÇİN DÜZENLEME ÖNERİLERİ

Av. Deniz BAYTEMÜR KÖKSAL*

ÖZET

Kripto varlık alanındaki düzenleme boşluğu her ne kadar sektör oyuncularının iştahını kabartsa da söz konusu düzenleme boşluğu rekabetçi pazar koşullarını ve yatırımcı menfaatlerini olumsuz etkilemekte, hatta piyasanın gelişmesini de yavaşlatmaktadır. Bu temel gerekçeden yola çıkılarak Avrupa Komisyonu tarafından hazırlanan Kripto Varlık Piyasalarına İlişkin Tüzük Teklifinin (Teklif) yürürlüğe girmesi ile kripto varlıklar ve hizmet sağlayıcıları AB'de yeknesak bir düzenlemeye kavuşacaktır. Gerek kripto varlık piyasalarının küresel niteliği gerekse ülkemizde finansal teknolojilere yönelik düzenlemelerin büyük ölçüde AB düzenlemelerini örnek alması nedeniyle söz konusu Teklifin incelenmesi hukukumuz bakımından da önem arz etmektedir. Bu sayede, hâlihazırda çalışmaları devam eden kripto varlıklara ilişkin kanunlaşma sürecine de katkı sunulabilecektir.

Teklif, kripto varlıkları sermaye piyasası araçlarından ayrıştırmakta ve kripto varlıkları kendi içinde e-para jetonları, varlığa dayalı jetonlar ve bu iki sınıflandırmaya girmeyen ve torba kavram olarak kullanılan diğer kripto varlıklar olarak üç sınıfa ayrılmaktadır. E-para jetonları, büyük ölçüde mevcut elektronik para düzenlemelerine atıf yapılmak suretiyle hukuki sonuca bağlanmaktadır. Bu bakımından Teklifin yaklaşımı, Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelikteki düzenleme ile örtüşmektedir. Diğer taraftan Teklifte, varlığa dayalı jetonlar istikrarlı kripto varlıkları işaret edecek şekilde tanımlanmış olup bu varlıkların ödemeler alanında oynayabileceği rol göz önüne alınarak diğer kripto varlıklara nazaran daha katı düzenlemelere tabi tutulmuştur. Teklifte diğer yükümlülüklerin yani sıra, kripto varlık ihraç edenlere ve sağlayıcılara faaliyet izin alma ve kripto varlık ihracında kamuyu aydınlatma mecburiyeti getirilmektedir.

Teklifin yürürlüğe girmesi ile kripto varlıklara AB içinde yeknesak bir hukuki statü sağlanacak olsa da Teklif, bu kıymetlerin hukuki nitelendirmesini yapmaktan kaçınmaktadır. Mevzuatımızda kaydi menkul kıymetlerin hukuki niteliği bakımından

* Avukat, Ankara Barosu, Ankara Hacı Bayram Veli Üniversitesi Doktora Öğrencisi, ORCID ID: 0000-0002-2807-9086

benimsenen yaklaşım da dikkate alındığında, kripto varlıkların hukuki niteliğine ilişkin tartışmanın da doktrine bırakılması sürpriz olmayacaktır.

Her ne kadar Teklif, sermaye piyasası araçlarını kripto varlıklardan ayırsa da dağıtık defter teknolojisine dayanarak ihraç edilen kripto varlıkların sermaye piyasası aracı tanımına girmesi halinde bu düzenlemelere tabi olacağı bir süredir kabul edilmektedir. Diğer taraftan, Almanya'da yakın zamanda yürürlüğe giren Elektronik Menkul Kıymetler Kanunu ile kripto varlıkların şartları sağlaması halinde menkul kıymet olarak nitelendirileceği ve bunların eşya *(Sache)* vasfını haiz olduğu düzenlenmiştir. Ülkemizde yürürlüğe girmesi beklenen düzenlemede de kaydi menkul kıymetlerin kripto varlık olarak ihraç edilmesi ve dağıtık defter üzerinden izlenebilmesine imkân tanınması tercihe değerdir.

Teklif, kripto varlıkların yeknesak bir yasal çerçeveye kavuşması ve güvenli bir piyasa sağlanması için önemli bir adım atmaktadır. Kripto varlıklara ilişkin ülkemizdeki düzenleme boşluğu göz önüne alındığında, Teklifin birçok açıdan yol gösterici olabileceği düşünülmektedir. Bu çalışmada Teklifte yer alan düzenleyici çerçeve ayrıntılı olarak incelenmiş olup mevzuatımız yönünden önerilere yer verilmiştir.

Anahtar kelimeler: Kripto Varlık, Elektronik Para, Sermaye Piyasası Araçları, Faaliyet İzni, Kamuyu Aydınlatma.

EU PROPOSAL FOR THE REGULATION ON MARKETS IN CRYPTO-ASSETS and REGULATORY SUGGESTIONS FOR OUR LEGISLATION

ABSTRACT

Even though the regulatory gap in crypto-assets appetizes market players, the said gap adversely effects competitive market conditions and investor benefits, and even slows down market developments. Founding on this rationale, by the Regulation on Markets in Crypto-Assets (Proposal) drafted by European Commission coming into force, crypto-assets and service providers will attain uniform regulatory framework in EU. Assessing the said Proposal is vital with regards to our legislation both due to the global nature of crypto-asset markets and the fact that our regulations on financial technologies largely based on EU regulations. The assessment will contribute to the preparation process of ongoing crypto-asset regulations.

The Proposal differentiates between crypto-assets and financial instruments and divides the crypto-assets into three classes; e-money tokens, asset-referenced tokens, and other crypto-assets, an omnibus concept, that do not fall under these two classifications. Legal consequence of e-money tokens is mostly determined by referencing to the existing electronic money regulation. In this respect, the approach

of the Proposal coincides with the provision in the Regulation on Payment Services and Electronic Money Issuance, and Payment Service Providers. On the other hand, considering their potential role in payments industry, asset-referenced tokens are defined to address stable coins and are subject to stricter rules than other crypto-assets. In addition to other obligations, the Proposal obliges crypto-asset issuers and service providers to obtain a license and public disclosure requirement.

While the Proposal will ensure a uniform legal status for crypto-assets within the EU, it remains silent when it comes to the legal qualification of crypto-assets. Considering the approach adopted in our legislation for the legal qualification of dematerialized securities, it would not be a surprise to leave the dispute over the qualification of crypto-assets to the literature.

Despite the differentiation between financial instruments and crypto-assets, it has been acknowledged for a while that crypto-assets issued on DLT would be subject to the regulations on financial instruments, as long as crypto-assets fall under the definition of financial instruments. On the other hand, the Act on Electronic Securities, which has recently come into force in Germany, states that crypto-assets will qualify as securities, provided that they meet the conditions, and these will be regarded as things *(Sache)*. With respect to our anticipated regulation, it would be preferrable to allow dematerialized securities to be issued as crypto-assets and be recorded on a distributed ledger.

The Proposal takes an important step towards achieving uniform legal framework for crypto-assets and ensuring a safer market. Considering the regulatory gap in our country with respect to crypto-assets, the Proposal is considered to be guiding in various aspects. In this study, the regulatory framework of the Proposal is thoroughly examined, and recommendations are presented for our legislation.

Keywords: Crypto-asset, Electronic Money, Financial Instruments, Licensing, Public Disclosure

KARŞILAŞTIRMALI HUKUKTAKİ GELİŞMELER IŞIĞINDA DEEPFAKE TEKNOLOJİSİNİN REGÜLASYONU VE TÜRK HUKUKU İÇİN ÖNERİLER

Sinem ÖZYİĞİT*

ÖZET

Yapay zekânın regülasyonu meselesi güncelliğini korurken ayrılan bir kol, Deepfake'in regülasyonunu hararetli bir şekilde tartışmaktadır. En ilkel örnekleri bile oldukça başarılı olan Deepfake, derin öğrenme ve makine öğrenmesi gibi yapay zekâ yöntemlerinin desteği ile sıfırdan veya mevcut içeriklerin tahrif edilmesi suretiyle üretilen, maruz kalan kişilerin orijinal olarak algılayabileceği kadar gerçekçi ve fakat kişileri aldatmak amacıyla bağlamından koparılan görsel içerikler ile ses ve metin içerikleridir[1]. Deepfake içeriklerin çevrimiçi platformlar eliyle kısa sürede geniş bir kitleye ulaşması ise, zararların toplumsal boyuta oluşmasına sebep olmakta ve bu uygulama özelinde yasal düzenlemeye ihtiyaç olup olmadığı sorununu gündeme getirmektedir.

Öğretide, Deepfake özelinde yasal düzenleme yapılmasına gerek olmadığını ve mevcut hukukî imkânların Deepfake kaynaklı sorunların çözümü için yeterli olduğunu ifade eden yazarlar bulunmaktadır[2]. İşin aslı, mevcut mekanizma belli bir seviyeye kadar koruma sağlasa da, Deepfake içeriklerin kendine özgü sorunlarını ortadan kaldırmak için yeterli değildir. Bunu fark eden bazı ülkeler, mevcut düzenlemelerini gözden geçirmek veya yeni düzenlemeler geliştirmek adına regülasyon hareketini çok

* Doktora Bursiyeri–Yeditepe Üniversitesi, Avukat–İstanbul Barosu, LL.M. Ghent Üniversitesi, LL.B. Yeditepe Üniversitesi, ORCID: https://orcid.org/0000-0003-4907-0467, E-mail: sinemozyigit@gmail.com.

1 European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), çevrimiçi erişim: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence. Committee on Legal Affairs of the European Parliament, Draft opinion on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, s. 32-33, çevrimiçi erişim: https://www.europarl.europa.eu/doceo/document/JURI-PA-719827_EN.pdf. Başka tanımlar için bkz. Avrupa Parlamentosu, Tackling deepfakes in European policy, Brüksel 2021, s. 1, çevrimiçi erişim: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039; Raina Davis, Chris Wiggins, Joan Donovan, Tech Factsheets for Policymakers - Deepfakes, in: Amritha Jayanti (edit.), Cambridge 2020, s. 2; Bart van der Sloot, Yvette Wagensveld, Bert-Jaap Koops, Deepfakes: The legal challenges of a synthetic society, Tilburg Institute for Law, Technology, and Society 2021, s. 2, çevrimiçi erişim: https://www.tilburguniversity.edu/sites/default/files/download/Deepfake%20EN.pdf; Bart van der Sloot, Yvette Wagensveld, Deepfakes: regulatory challenges for the synthetic society, Computer Law & Security Review 2022, s. 4.

2 David Greene, We Don't Need New Laws for Faked Videos, We Already Have Them, Electronic Frontier Foundation 2018, çevrimiçi erişim: https://www.eff.org/deeplinks/2018/02/we-dont-need-new-laws-faked-videos-we-already-have-them.

erken başlatmıştır. Bu kapsamda, Avrupa Birliği[3], Çin[4], Tayvan[5] ve Amerika Birleşik Devletleri'nin Kaliforniya eyaletinde[6], Türkiye'de atılacak potansiyel adımlara ilham olabilecek nitelikte tartışmalar yürütülmektedir. Bu noktada şunu da belirtmek isteriz ki, teknolojinin regülasyonu söz konusu olduğunda genel olarak hissedilen "Brüksel etkisi", Deepfake özelinde yerini "Beijing etkisine" bırakmış olup, bu konuda tartışmalar daha çok Çin modeli üzerinden ilerlemektedir[7].

Yöntem olarak anılan hukuk sistemlerinin, törpülemek istedikleri olumsuz etkiyi belirleyerek ilk adımı attığını ve kendi hukuk politikalarına göre düzenlemelerini şekillendirdiğini söyleyebiliriz. Uzun bir süredir Türk hukuku bakımından bizim de kanaatimiz, mevcut kanunların bir an evvel Deepfake'e uyarlanması ve bu teknolojik imkânın etik kullanımını genele yaymak adına müstakil bir kanun hazırlığına başlanması yönündeydi. Ancak, 13 Ekim 2022 tarihinde mevzuatımıza eklenen ve 5237 sayılı Türk Ceza Kanunu m. 217/A hükmünde yer alan "halkı yanıltıcı bilgiyi alenen yayma" suçu ile kanun koyucu –belki de farkında olmadan– doğası gereği gerçeğe aykırı bilgi niteliğini taşıyan Deepfake içerikleri de kapsayacak şekilde bilgi kirliliği riskine odaklanmış ve çoğu zaman olduğu gibi ceza hukuku imkânları ile riski bertaraf etmeye çalışmıştır[8]. Ayrıca, 2019 yılında Radyo ve Televizyon Üst Kurulu internet ortamındaki yayınları denetleme yetkisini kazanmış[9]; 2020 yılında 5651 sayılı İnternet Kanunu'na[10] eklenen Ek Madde 4 ile Türkiye'den günlük erişimi bir milyondan fazla olan sosyal ağ sağlayıcılar, içeriğin çıkarılması ve erişimin engellenmesi kararlarını uygulamakla yükümlü kılınmıştı.

Bu çalışma ile öncelikle, Deepfake'i tanıtmaya ve detaylı bir fayda-risk analizine[11] yer vermeye çalışacağız. Takip eden bölümde ise, Türk hukuku bakımından yol gösterici olması adına, diğer ülkelerdeki mevcut durumu değerlendireceğiz. Son olarak ise, Türk hukukundaki mevcut durumu da düşünerek ve fakat eleştirel bir bakış açısıyla, Deepfake için ideal olan düzenlemenin içeriğini belirlemeye çalışacağız.

Anahtar Kelimeler: Deepfake, derin öğrenme, makine öğrenmesi, yapay zekâ, regülasyon.

3 Bart van der Sloot, Editorial, European Data Protection Law Review 2021, s. 351-357.

4 Detaylı bilgi için bkz. Bo Zhao, China, in: Bart van der Sloot, Yvette Wagensveld, Bert-Jaap Koops (edits.), Deepfakes: De Juridische Uitdagingen van Een Synthetische Samenleving, Tilburg Institute for Law, Technology, and Society 2021, s. 233 vd. çevrimiçi erişim: https://www.tilburguniversity.edu/sites/default/files/download/Dee pfakes%20NL.pdf; Emmie Hine, Luciano Floridi, New deepfake regulations in China are a tool for social stability, but at what cost?, Nature Machine Intelligence 2022, s. 608-610.

5 Avrupa Parlamentosu Deepfake Raporu, s. 47.

6 California Assembly Bill No. 730. Detaylı bilgi için bkz. Matthew F. Ferraro, Deepfake Legislation: A Nationwide Survey - State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media, JD Supra 2019.

7 Hine & Floridi, s. 609; Ed Sander, China is leaving the west behind in regulating deepfakes, China Talk 2022, çevrimiçi erişim: https://www.chinatalk.nl/europe-is-falling-behind-china-in-regulating-deepfakes/.

8 TCK m. 217/A: "(1) Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır. (2) Fail, suçu gerçek kimliğini gizleyerek veya bir örgütün faaliyeti çerçevesinde işlemesi hâlinde, birinci fıkraya göre verilen ceza yarı oranında artırılır."

9 Radyo, Televizyon ve İsteğe Bağlı Yayınların İnternet Ortamından Sunumu Hakkında Yönetmelik, Resmî Gazete Tarihi: 01.08.2019 Resmî Gazete Sayısı: 30849.

10 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Resmî Gazete Tarihi: 23.05.2007 Resmî Gazete Sayısı: 26530.

11 Bu konuda temel çalışmalar için bkz. Jan Kietzmann, Linda W. Lee, Ian P. Mccarthy, Tim C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons 2020, s. 135-146; van der Sloot & Wagensveld, s. 3 vd.

REGULATION OF DEEPFAKE TECHNOLOGY IN LIGHT OF DEVELOPMENTS IN COMPARATIVE LAW AND RECOMMENDATIONS FOR TURKISH LAW

ABSTRACT

While the regulation of artificial intelligence remains topical, a split arm is glowingly discussing the regulation of Deepfake. Deepfake, even the most primitive examples of which are rather successful, is audio-visual content produced from scratch or by manipulating existing content with the support of artificial intelligence methods such as deep learning and machine learning, which is realistic enough to be perceived as original by the people who are exposed, but taken out of its context in order to deceive people. The fact that Deepfakes are likely to reach a wide audience in a short time through online platforms may cause the harm to occur on a societal level, and thus raises the question of whether there is a need for an individual regulation as to this specific application of artificial intelligence.

In the doctrine, there are authors who state that there is no need for legal regulation dedicated to Deepfake, and that the existing legal instruments are sufficient to solve the problems emerging from Deepfake. As a matter of fact, the current mechanism provides protection to a certain level; however, it is not enough to eliminate the problems inherent to Deepfake. Some countries have started the regulation movement too early to review their existing instruments or to develop new regulations. In this context, discussions are being held in the European Union, China, Taiwan and the US state of California that can inspire potential steps to be taken in Turkey. At this point, we would like to point out that the "Brussels effect", which is generally felt when it comes to the regulation of technology, has left its place to the "Beijing effect" when it comes to the regulation of Deepfake, and the discussions on this issue are mostly based on the Chinese model.

We observe that the method of the aforementioned legal systems is to determine the negative impact they want to file first and to shape their regulations according to their own legal policies. For a long time, we considered that the existing Turkish laws should be adapted to Deepfake as soon as possible, and an individual law should be drafted in order to spread the ethical use of this technology. However, the Turkish Penal Code No. 5237 was revised on October 13, 2022, and the crime of "publicly disseminating misleading information" was included in Art. 217/A. Thus, the legislator -perhaps unwittingly- focused on the risk of misinformation given Deepfakes constitute false information by their very nature, and tried to eliminate this risk through criminal law instruments. In addition, the Radio and Television Supreme Council was authorised in 2019 to inspect online broadcasts; social network providers with more than one million daily access from Turkey were deemed to be obliged to implement the orders to remove content and block access under Additional Article 4 incorporated into the Internet Law No. 5651 in 2020.

In this conference paper, we will initially introduce the Deepfake technology and include a detailed benefit-risk analysis. Afterwards, we will evaluate the current situation in other countries in order to provide guidance to Turkey. Finally, we will determine the content of the potential Turkish law dedicated to Deepfake, considering the current situation in Turkey, but with a critical perspective.

Keywords: Deepfake, deep learning, machine learning, artificial intelligence, regulation.

VERGİ İDARESİNİN DİJİTAL DÖNÜŞÜMÜ

Ahmet Emrah GEÇER*

ÖZET

Bilgisayar biliminin kurucusu sayılan ve dijitalleşmenin temeline ilişkin birçok alanında araştırmalar yapan Alan Mathison Turing 1950 yılında yayınladığı makalesinde "*Makineler Düşünebilir mi*?" sorusunu cevaplamaya çalışmıştır[13]. Ülkemizde ise duayen matematikçi Prof. Dr. Cahit Arf, "*Makine Düşünebilir mi ve Nasıl Düşünebilir*?" isimli sunumuyla Erzurum Atatürk Üniversitesi'nde 1958-1959 Halk Konferansı Bildirisi'nde konuyu ele almış ve düşüncelerini paylaşmıştır[14]. O günlerde, söz konusu akademik çalışmalar, hayal olarak görülüyordu. Çok değil 50 yıl kadar sonra, 21. Yüzyılın başından itibaren dijitalleşme, hayatın bir gerçeği olmaya başlamıştır. O artık Fenomen olmanın da ötesine geçmiştir.

Birinci Sanayi Devrimi 18. yüzyılda buharlı makinaların icat edilmesi ile başlamıştı. O dönemden 4. Sanayi Devrimini yaşadığımız günümüze kadar bilim ve teknolojide birçok gelişme üstüne gelişme sağlana gelmiştir. İnternetin yaygınlaşması ile dijitalleşme olgusu, bilim ve teknolojinin odak noktası haline gelmiştir. 2000'li yılların başlarından itibaren ivme kazanan dijitalleşme, uluslararası ve ulusal ölçekte ekonomik işleyişin kabuk değiştirmesine, bir kısım iş modellerinin tarihe karışmasına ve yeni iş modellerinin ortaya çıkmasına sebep olmuştur ve olagelmektedir. Dijitalleşmenin temel teknolojileri olan nesnelerin interneti, artırılmış gerçeklik, sanal gerçeklik, blok zincir, 3 boyutlu yazıcılar, robotlar ve insansız araçların ekonominin her alanına nüfus ettiği görülmektedir. Bu durum vergi idarelerini, dijital teknolojilere adapte olmaya ve bu teknolojilerden yararlanmaya zorlamaktadır. Vergi idarelerinin, vergiyi doğuran olayı kavramak ve sonrasında vergilendirme işlemlerini hızlı ve etkin şekilde icra etmek ve mükelleflerin vergi uyumuna yardımcı olmak amacıyla vergi tekniğindeki konvansiyonel işleyişi, dijitalleştirme sürecine soktukları anlaşılmaktadır.

2000'li yılların başından itibaren ülkemizde dijitalleşen dünyaya ayak uydurmak amacıyla vergi teşkilatlanmasında yapısal değişikliklere gidilmiştir. 2005 yılında Gelir İdaresi Başkanlığı (GİB), 2011 yılında Vergi Denetim Kurulu Başkanlığı (VDK) kurulmuştur. 2020 yılında kayıt dışı ekonomi ile mücadeleye değer katmak için

* Dr. Öğretim Üyesi, İstanbul Medeniyet Üniversitesi Hukuk Fakültesi Mali Hukuk Ana Bilim Dalı. E-mail:ahmet.gecer@medeniyet.edu.tr Orcid ID:0000-0002-8784-6871

13 A. M. Turing, "Computing Machinery and Intelligence", Mind, Volume LIX, Issue 236, October 1950, p. 433–460.

14 Cahit Arf, "Makine Düşünebilir Mi ve Nasıl Düşünebilir?", Atatürk Üniversitesi – Üniversite Çalışmalarını Muhite Yayma ve Halk Eğitimi Yayınları Konferanslar Serisi No: 1, 1959, Erzurum, s. 91-103.

teknolojiyle desteklenen risk odaklı çalışmalar yapılması misyonuyla Risk Analizi Genel Müdürlüğü oluşturulmuştur. Bu yapısal değişikliklerle vergi idaresinin dijitalleşme sürecinde yeni bir döneme girme hususundaki ciddiyeti anlaşılmıştır. Vergi idaresi, özellikle bu kurumsal değişikliklerden sonra, bilgisayar destekli olarak dijital vergi uygulamalarına ağırlık verdiği gözlemlenmektedir. Vergiyi doğuran olay ile ilgisi olan verilerin, mükellef ve muhataplardan dijital ortamda talep edilme zorunluluğu günden güne yaygınlaştığı tespit edilmektedir. E-beyanname, e-defter, e-belge, defter beyan sistemi, bilgi toplama sistemleri (banka, noter ve tapu müdürlüklerinden) uygulamaları buna örnek gösterilebilir. Ayrıca vergi idaresi, vergi mevzuatında yer alan vergi denetim araçlarının tatbikinde dijital teknolojilerden yardım almaktadır. Örneğin elektronik yoklama sistemi, sahte belge risk analiz programı (SARP), riskli iade takip ve analiz programı (RİTAP), risk analiz sistemi (VDK-RAS), KDV iadesi risk analiz sistemi (KDVİRA), ÖTV iadesi risk analizi sistemi (ÖTVİRA), veri erişim ve görsel analiz uygulaması (VEGAS).

Bu çalışmamızda, vergi idaresinin geçmişten günümüze dijitalleşme süreci ana hatları ile mercek altına alınacaktır. Mevcut durumda vergi idaresinin ve mükelleflerin dijitalleşmede tecrübe ettikleri zorluklar değerlendirilecektir. Vergi idaresinin dijitalleşme sürecinin geleceğine ilişkin öngörüler sunulacaktır.

Anahtar Kelimeler: Vergi İdaresi - Dijitalleşme – Vergi Otomasyon Sistemleri - Elektronik Defter ve Belgeler – Elektronik Denetim

DIGITAL TRANSFORMATION OF TAX ADMINISTRATION

ABSTRACT

Alan Mathison Turing, who is considered to be the founder of computer science and researches in many fields relating to the basis of digitalization, in his article published in 1950, “Can Machines Think?” attempted to answer the question. In our country, the veteran mathematician Prof. Dr. Cahit Arf, with his presentation called “Can a Machine Think and How Can It Think?”, discussed the issue and shared his thoughts in the 1958-1959 Public Conference Declaration at Erzurum Atatürk University. In those days, the mentioned academic studies were seen as dreams. Not long after 50 years, from the beginning of the 21st century, digitalization has become a fact of life. It has now gone beyond being a phenomenon.

The First Industrial Revolution began with the invention of steam engines in the 18th century. From that period until today, when we experience the 4th Industrial Revolution, many developments have been achieved in science and technology. With the widespread use of the Internet, the phenomenon of digitalization has become the focal point of science and technology. Digitization, which has gained momentum since the beginning of the 2000s, has led to the changing of the economic functioning on

an international and national scale, the disappearance of some business models and the emergence of new business models. The internet of things, augmented reality, virtual reality, blockchain, 3D printers, robots and unmanned vehicles, which are the fundamental technologies of digitalization, are seen to penetrate all areas of the economy. This situation forces tax administrations to adapt to and benefit from digital technologies. It is understood that tax administrations have put the conventional operation in tax technique into the digitalization process in order to comprehend the taxable event and then to carry out the taxation procedures quickly and effectively and to assist taxpayers in tax compliance.

Since the beginning of the 2000s, structural changes have been made in the tax organization in order to keep up with the digitalized world in our country. The Revenue Administration (GIB) was established in 2005 and the Tax Inspection Board (VDK) was established in 2011. In 2020, the Risk Analysis General Directorate was established with the mission of carrying out risk-oriented studies supported by technology in order to add value to the fight against the unrecorded economy. With these structural changes, the seriousness of the tax administration in entering a new era in the digitalization process has been understood. It is observed that the tax administration, especially after these institutional changes, focuses on computer-assisted digital tax applications. It has been determined that the obligation to demand the data related to the taxable event in the digital environment from the taxpayer and the addressee is becoming more common day by day. Applications such as e-declaration, e-ledger, e-document, ledger declaration system, information collection systems (from banks, notary public and land registry offices) can be given as examples. In addition, the tax administration receives assistance from digital technologies in the application of tax audit tools in the tax legislation. For example, electronic inspection system, fake document risk analysis program (SARP), risky return tracking and analysis program (RITAP), risk analysis system (VDK-RAS), VAT refund risk analysis system (KDVIRA), SCT refund risk analysis system (ÖTVIRA), data access and visual analysis application (VEGAS).

In this study, the digitalization process of the tax administration from past to present will be examined with its main lines. In the current situation, the challenges experienced by the tax administration and taxpayers in digitalization will be evaluated. Forecasts regarding the future of the digitalization process of the tax administration will be presented.

Keywords: Tax Administration - Digitalization - Tax Automation Systems - Electronic Books and Documents - Electronic Audit

DİJİTAL PAZARLAMA VE SATIŞ YOLU İLE KAZANÇLARIN VERGİLENDİRİLMESİ VE GÜNCEL GELİŞMELER

Arzu KALYON*

ÖZET

Dijital pazarlama ve satış yolu ile kazançların vergilendirilmesinde karşılaşılan en büyük sorun, küresel cirosu çok yüksek olan şirketlerin e-ticaret faaliyeti yoluyla Pazar ülkelerde, yani ürünlerin tüketildiği ülkelerde hiçbir vergiye tabi olmamalarıdır. Dijital ortamda kazancın elde edildiği ülkenin tespit edilememesi halinde vergilendirme yetkisi konusunda boşluk olmaktadır; dijital ortamda yapılan işlemler vergi dışı kalabilmektedir. Anayasamızın 73. maddesinde de yer alan vergi yükünün dengeli ve adaletli dağıtılması ilkesi gereğince, küresel şirketlerin Pazar ülkelerden gelen kazançlarının hiç vergilendirilmemesi vergide adalet ilkesine ters düşmektedir. Kimi zaman küresel şirketler, Pazar ülkelerinden milyarlarca dolar kar elde etmekte ancak hiçbir şekilde vergilendirilmemektedir.

Her ne kadar 2019 yılında yürürlüğe giren Dijital Hizmet Vergisi ile dijital ortamda sunulan reklam hizmetleri, her türlü hizmetlerin ve elektronik ticaretin vergilendirilmesi amaçlansa da bazı dijital faaliyetlerin vergi dışı kalması engellenememiştir. Benzer dijital hizmet vergisi, Avrupa Birliği üye ülkelerinde de düzenlenmiştir; ancak küresel anlamda yeknesak bir uygulama söz konusu değildir. Uluslararası kabul gören inanış ise, vergilendirme yetkisinin ürünlerin tüketildiği Pazar ülkelere kaydırılmasıdır ve de OECD bu model üzerinde çalışmaktadır. Bu model uygulanırsa Dijital Hizmet Vergisi vb. uygulamalar ortadan kalkacaktır. OECD'ye üye ülkeler yaptıkları mutabakat sonucu, 2023 yılından itibaren uygulanmak üzere en az %15'lik bir vergi öngörmektedir. OECD mutabakatına göre, elektronik ticaretten kazanç elde eden firmaların, kazançlarını elde ettikleri ülke yani ürününün veya hizmetin tüketildiği ülkede vergiye tabi olmasıdır. Çoğu zaman şirketler, fiziksel bir varlık göstermeseler de Pazar ülkelerden milyarlarca dolar kar elde edebilmektedirler. Vergilendirme için fiziksel işyeri kriteri yerine ekonomik olarak bağ kurma iradesi aranırsa, vergiden kaçınma önlenebilecektir. Ekonomik olarak bağ kurma kriterinde ise; fatura bilgileri, cihazın IP adresi, banka bilgileri ve telefon alan kodu gibi bilgiler bize ürünün tüketildiği Pazar ülkeyi belirleme de yardımcı olacaktır. Vergilendirmenin yapılacağı ülkeyi belirlemek için, söz konusu bilgilerin mantıksal bir hiyerarşi içinde izlenmesi gerekmektedir. Bu noktada, müşterinin işlem noktası, kendi beyanı dışında vergi teknolojilerini de kullanarak tespit edilebilecektir.

* Dr. Öğr. Üyesi, İstanbul Medeniyet Üniversitesi, Mali Hukuk Anabilim Dalı, https://orcid.org/0000-0001-6289-6189, arzu.kalyon@medeniyet.edu.tr

Anahtar Kelime: Dijital Pazarlama ve Satış, Dijital Hizmet Vergisi, Vergide Adalet, E- Ticaret, OECD

THE CONCEPT AND CURRENT DEVELOPMENTS IN THE TAXATION OF PROFITS THROUGH DIGITAL MARKETING AND SALES

ABSTRACT

The main problem about taxation of incomes through digital marketing and sales is that companies with a very high global turnover are not subject to any tax in market, whereas products are consumed. If source of income is not truly determined, it would not be subjected to the taxation in any country. The fact that the income of global companies from market countries are not taxed at all is contrary to the principle of justice in taxation which is regulated in the Article 73 of Turkish Constitution. Pursuant to the said article, the tax burden should be balanced and distributed equitably. However, global companies make billions of dollars in profits from market countries but are not taxed in any way.

Although the Digital Service Tax, which came into force in 2019, aimed to tax advertising services, all kinds of services and electronic commerce in the digital environment, some digital activities could not be taxed. Similar digital services tax is also regulated in European Union member states; however, there is no universally uniform application. The internationally accepted belief is that the taxation authority of the market countries is competent to taxation and the OECD is working on this model. If the said model is applied, Digital Services Tax etc. apps would be repealed. OECD member countries, as a result of their agreement, envisage a tax of at least 15% to be applied from 2023. According to the OECD agreement, companies are subject to tax in the country where they earn their income, that is, in the country where the product or service is consumed. Generally, companies can generate billions of dollars in profit from market countries, even if they do not have a physical presence. If the economic connection is taken into consideration instead of the physical workplace criterion for taxation, tax avoidance can be avoided. In the criterion of establishing economic bonds; information such as billing information, device IP address, bank information and telephone area code will also help us determine the market country where the product is consumed. In order to determine the country where taxation will be made, the information in question must be followed in a logical hierarchy. At this point, the customer's transaction point can be determined by using tax technologies other than his own declaration.

Keywords: Digital Marketing and Sales, Digital Services Tax, Tax Justice, E-Commerce, OECD

GELİR VERGİSİ VE KURUMLAR VERGİSİ YÖNÜNDEN HİZMET OLARAK YAZILIM (SAAS) ÖDEMELERİNİN NİTELENDİRİLMESİ

Alperen Asım KORUK*

ÖZET

Hizmet olarak yazılım (SaaS), basit bir anlatımla, bulut altyapısı üzerinde yürütülen uygulama programlarının müşterilerin (kullanıcıların) kullanımına sunulmasıdır. Uygulama programlarının (daha geniş bir ifadeyle bilgisayar programı veya yazılımların) kullanımı gerek ticari gerekse özel ortamlarda her geçen gün artmaktadır. Bu gerçeğe paralel şekilde SaaS pazarının büyümeye devam etmesi beklenmektedir. Bu büyüme bir taraftan vergi idarelerinin dikkatini çekerken diğer taraftan SaaS sağlayıcılarının vergilendirmede karşılaştıkları belirsizlikleri giderme isteklerini güçlendirmektedir.

SaaS ödemelerinin vergilendirilmesinde karşılaşılan belirsizliklerin başında SaaS sağlayıcılarının bu hizmetlerden elde ettikleri gelirleri nitelendirme sorunu gelmektedir. Bu sorun özellikle gayrimaddi hak bedeli ile ticari kazanç (ayrıca gayrimenkul sermaye iradı ile ticari kazanç) arasındaki ayrımda yoğunlaşmaktadır. Bu sorunun giderilmesi sadece teorik açıdan değil, aynı zamanda uygulama açısından önem arz etmektedir. Zira, SaaS ödemelerinin, gayrimaddi hak bedeli olarak nitelendirilmesi halinde dar mükellefiyete tabi gerçek kişi ve kurumların Türkiye'deki müşterilerine sundukları hizmetler karşılığında yapılan ödemeler üzerinden Türkiye'nin vergilendirme hakkı ortaya çıkmaktadır. Diğer taraftan, bu ödemelerin ticari kazanç olarak nitelendirilmesi halinde bu ödemelerin, Türkiye'de vergilendirilebilmesi SaaS sağlayıcılarının Türkiye'de işyerlerinin bulunmasına bağlıdır. SaaS sağlayıcılarının hiçbir fiziki varlığa ihtiyaç duymaksızın pazar ülkelerinde hizmet sunabilme kabiliyetleri dikkate alındığında ticari kazanç olarak nitelendirme, kaynak ülke olarak Türkiye'nin vergilendirme olasılığını oldukça düşürmektedir. Türkiye'deki yargı kararları ve özelgeler, bilgisayar programı karşılığında yapılan ödemeleri gayrimaddi hak bedeli olarak nitelendirme eğilimi göstermektedir. Diğer bazı kaynak ülkelerde de görülen bu eğilimin arka planında yukarıda zikredilen vergilendirme olasılığı yatmaktadır.

Bilgisayar programları telif hakkına konudur. Türkiye'nin taraf olduğu çifte vergilendirmenin önlenmesi anlaşmalarının (ÇVÖA) m.12 hükümleri uyarınca

* Araştırma Görevlisi, Yeditepe Üniversitesi Hukuk Fakültesi Mali Hukuk Anabilim Dalı. Yazarın ORCID numarası: 0000-0002-0508-5993. Yazarın e-posta adresi: alperenasimkoruk@gmail.com.

bilgisayar programlarının üzerindeki telif hakkının kullanımı veya kullanım hakkı karşılığında yapılan her türlü ödeme gayrimaddi hak bedelidir. Ayrıca, 193 sayılı Gelir Vergisi Kanunu m.70/f.1/b.6 hükmü uyarınca müellif veya bunların kanuni mirasçısı dışındaki kimseler tarafından telif hakkının kiralanması karşılığında yapılan ödemeler gayrimenkul sermaye iradıdır. Telif hakkının kullanımı, kullanım hakkı veya kiralanmasından maksat 5846 sayılı Fikir ve Sanat Eserleri Kanununun m.21 ilâ m.25 hükümleri arasında tanınan mali hakların (işleme, çoğaltma, yayma, temsil veya umuma iletim haklarının) bir veya birkaçının devredilmesidir. Bilgisayar programı üzerindeki mali haklar devredilmeksizin bilgisayar programının yalnızca kullanımı, ÇVÖA m.12 ve Gelir Vergisi Kanunu m.70/f.1/b.6 hükümleri anlamında kullanım ve kiralama değildir. Bu tür bir kullanım karşılığında yapılan ödemelerin niteliği, hizmet sağlayıcısının faaliyetinin özelliklerine bağlı olarak ticari kazanç veya serbest meslek kazancı olabilmektedir.

Bulut bilişim hizmetlerinde dağıtım modellerine (genel, özel, topluluk veya hibrit bulut) bağlı olarak müşterilerin (kullanıcıların) kendilerine sunulan bilgi işlem kaynakları üzerindeki kontrol ve yönetim yetkileri farklılık göstermektedir. Bu nedenle, SaaS ödemeleri için her bir dağıtım modeline ilişkin özellikli durumlar dikkate alınmak suretiyle ödemelerin niteliği değerlendirilecektir.

Anahtar Sözcükler: SaaS, Bulut Bilişim, Yazılım, Gelir Vergisi, Kurumlar Vergisi

CHARACTERIZATION OF SOFTWARE AS A SERVICE (SAAS) PAYMENTS IN TERMS OF PERSONAL INCOME TAX AND CORPORATE INCOME TAX

ABSTRACT

In simple terms, software-as-a-service (SaaS) enables consumers to use application programs running on a cloud infrastructure. The usage of application programs (computer program or software in a broader sense) is gradually increasing in both business and private environments. In line with the fact, SaaS market size is expected to continue to grow. This growth attracts the attention of tax administrations. Moreover, it consolidates SaaS providers' requests for eliminating uncertainties in taxation.

One of the main uncertainties in taxation of SaaS payments is related to qualification of income that SaaS providers generate from the services. This is especially concentrated in the distinction between royalties and business income (as well as the distinction between income from immovable property and rights ("*gayrimenkul sermaye iradı*" in Turkish) and business income). Coping with this is substantial not merely from a theoretical sense but also in practice. The reason is that Türkiye has right to tax on the payments deriving from the services for customers in Türkiye, provided by natural persons and legal entities subject to limited tax liabilities in Türkiye if SaaS

payments are qualified as royalties. On the other hand, if these payments are qualified as business income, the taxation of the payments in Türkiye depends on the presence of SaaS providers' permanent establishments in Türkiye. Considering the ability of SaaS providers to provide services in market jurisdictions without any physical presence in the jurisdictions, qualifying the payments as business income considerably decreases the taxation probability in Türkiye as a source state. Judicial decisions and rulings in Türkiye indicate tendency to characterize payments for computer software as royalties. The above-mentioned taxation possibility lies in the background of this tendency, which is also observed in some other source states.

Computer programs are subject to copyright. According to Article 12 of the double taxation conventions concluded by Türkiye, payments of any kind received as a consideration for the use of, or the right to use, any copyright are royalties. In addition, according to Article 70/par.1/sub par.6 of the Income Tax Code (No. 193), payments for rent a copyright belongs to persons other than author and his legal heirs are income from immovable property and rights. The use of, using the right to use or rent means the transfer of one or more economic rights (adaptation, reproduction, distribution, representation, and to publicize) entitled in between the Article 21 and Article 25 of Intellectual and Artistic Works Code (No: 5846). Merely usage of computer program without transferring any economic rights of the computer program are not a usage and a rent within the meaning of the provisions Article 12 of double tax conventions and Article 70/ par.1/sub par.6 of Income Tax Code. The character of payments for such use may be business income or independent personal services income, depending on the characteristics of the service provider's activity.

Depending on the deployment models (public, private, community or hybrid cloud) in cloud computing services, the control and management capabilities of customers (users) over the computing resources may be different. Therefore, considering certain circumstances related to the models, characterization of SaaS payments will be evaluated.

Keywords: SaaS, Cloud Computing, Software, Personal Income Tax, Corporate Income Tax

YAPAY ZEKÂ ÜZERİNDEN GERÇEKLEŞTİRİLEN İRADE AÇIKLAMALARININ İRADE ÖZERKLİĞİ KAPSAMINDA AÇIKLANABİLİRLİĞİ SORUNU

Mustafa AKSU*

ÖZET

Özellikle yapay zekânın otonom yapısı itibariyle güncel olarak çokça tartışılan bir konu, yapay zekâ yoluyla/tarafından gerçekleştirilen irade açıklamalarının muhtemel hukuki rejimine dairdir. Bu çerçevede irade açıklamasının kullanıcıya isnat edilebilirliği somut yapay zekâ sistemleri itibariyle ön plana çıkan bir husustur.

Yapay zekâ uygulamaları güncel olarak birçok sözleşme ilişkisinin kurulmasında kullanılabilmektedir: Nesnelerin interneti uygulamalarının giderek daha yaygınlaşması ve işlevselliğinin artması, borsada son derece hızlı ve kapsamlı olarak işlem yapabilen, özellikle yüksek frekanslı işlemleri gerçekleştirebilen yapılar, farklı akıllı sözleşme uygulamaları, çeşitli internet platformlarında gerçekleştirilebilen sözleşmeler ve benzerleri kapsamlı ve genel örnekler olarak anılabilirler.

Bütün bu ve benzeri süreçlerde otonom yapıda bir yapay zekâ sisteminin kullanılması durumunda, dışarıdan (ya da muhtemel muhataplar gözüyle) bakıldığında irade açıklamasının objektif unsurundan hareket edilebilir. Bir diğer deyişle dışarıdan bakıldığında bir beyanın bulunduğu benimsenebilir. İşte bu dışarıdan bakıldığında beyan niteliğindeki bildirimin, kim ya da kimlere isnat edilmesi gerektiği ya da edilebilirliği, yani kimin "iradesi" olduğu burada ele alınacak olan konudur.

Ancak güncel yapay zekâ uygulamalarının düzeyi dikkate alınarak, diğer bazı ihtimaller dışarıda bırakılarak bu sorun ele alınmıştır: Güncel yapay zekâ uygulamaları henüz genel yapay zekâ düzeyinde değildirler. Tam tersine dar yapay zekâ örnekleridirler. Bu yüzden bu alanda uzun zamandır tartışılan ve son dönemlerde daha da yoğunluk kazanan hukuki statü tartışmalarına burada girilmemiştir. Bu itibarla yapay zekâ ya örneğin bir yapay ya da elektronik kişilik tanınmasının gerekip gerekmediği tartışması, güncel yapay zekâ uygulamaları itibariyle olumsuz şekilde cevaplanması gereken bir sorun şeklinde görülerek, değerlendirmeler bu temelde yapılmıştır. Şu halde sorunun bu düzlemde çözülmesi ve irade açıklamasının doğrudan yapay zekâ sistemine isnat edilmesi gibi bir yolun uygun olmadığı ve bunun güncel durum itibariyle yerinde

* Prof. Dr., İstanbul Üniversitesi Hukuk Fakültesi Öğretim Üyesi, e-posta: aksum@isanbul.edu.tr Orcid No: 0000-0002-0323-9602.

bir çözüm olmadığı benimsenmiştir. Bu yaklaşım yerine sorunun var olan kurumlar üzerinden doğrudan/dolaylı çözülebilirliği tartışılmıştır. Bir diğer kısıtlama şu şekildedir. Klasik bilgisayar programları ve olasılıklara göre tesadüfi kararlar da verebilen sistemler, ki bunların olasılıklı da olsalar, belirlenimci (determinist) yapıda olduklarından hareket edilmiştir, bu çalışmanın doğrudan konusu değildir. Burada esas alınan sistemler geleneksel anlamda belirlenimci olmayan, baştan sona ve her bir adımı (birtakım olasılıklar düzeyinde de olsa) programlanmamış, bunun yerine veriler üzerinden öğrenmiş, istatistiki şekilde doğruya en yakın kararlar verdikleri düşünülen, şu ya da bu derecede otonom olan yapılardır. Bu çerçevede diğer sistemlerin gerçekleştirdiği (örneğin otomatların ya da bütünüyle baştan sona programlanmış nesnelerin interneti uygulamalarının) irade açıklamalarının zaten bunları kullanana isnat edilmesi gerektiği düşüncesinden hareket edilmiştir. Acaba aynı durum otonom mahiyetteki yapay zekâ sistemleri için de güncel durum itibariyle geçerli midir? Sorun budur!

Yapay zekânın gerçekleştirdiği beyanın (irade açıklamasının objektif unsurunun) yanında, iradeyi oluşturan diğer unsurların da bulunması gerekir ki, tam anlamıyla geçerli bir irade açıklamasından hareket edilebilsin. Bu açıdan irade açıklamasının sübjektif unsurlarının, yani hareket, beyan ve işlem bilincinin sırasıyla bulunması gerekir. Bu hususları değerlendirirken, olağan durumdan hareket etmek gerekir. İrade açıklamasının hukuki işlemin temel unsuru olması ve hatta bazen bunların eş anlamlı kullanılmasının arkasında, kişinin kendi hukuki ilişkilerini istediği düzenleyebilme yeteneği ve iradesinin varlığı yatmaktadır. Bu iradenin ortaya konulduğu alanlardan en başta geleni hukuki işlemlerdir. Bu nedenle kişinin bilinçli bir şekilde (içerikten soyutlanarak) hareket etmiş olması (hareket bilinci), hukuki önemi olabilecek bir bildirim de bulunma, yani beyan bilincinin varlığı ve en nihayetinde somut hukuki işlemi içeriği itibariyle gerçekleştirmeye yönelik bir bilincin bulunması gerekir.

Yapay zekâ sistemlerinde iradenin açıklandığı durumda, bunu kullananın somut durumdan, koşullardan, ihtimallerden birebir haberdar olması ve bunları yönetmesi olağan durumda söz konusu değildir. Sistemin otonom yapısı başta olmak üzere diğer karakteristik özellikleri bunu gerektirmektedir. Bu açıdan kullananın hiç düşünmediği ve hatta istemediği bir sonuç dahi gerçekleşebilir. Ayrıca teknik olarak bakıldığında, burada subjektif unsurun son iki bileşenin hiç bulunmadığı dahi söylenebilir. Ne de olsa somut hukuki işlemler açısından sistemin başta genel olarak işlevsel hale getirilmesinden sonra belirgin ya da somutlaşmış bir irade (kullanıcı açısından) yoktur. İşte bu çerçevede iradenin kullanıcıya isnat edilmesi sorunu itibariyle farklı yaklaşım ve ihtimallerin olduğu görülmektedir.

İfade etmek gerekir ki, var olan kurumların hiçbiri yapay zekâ sistemleri dikkate alınarak getirilmiş değildirler. Bu açıdan tam da buna özgü bir düzenleme yoktur ve bu teknik arka plan itibariyle tamamen anlaşılabilir bir durumdur. Şu halde sorunun çözülmesinde en akla yatkın yol, var olan kurumlardan yararlanıp mümkünse kıyasen bir çözüm bulmaktır.

Var olan kurumlardan hareket edildiğinde, bu duruma en çok benzetilebilecek olan durumlar, ulak, beyaza imza, genel ya da çerçeve irade açıklaması, temsil ve organ ile tüzel kişi ilişkisidir. Nitekim bunlar ve diğer bazı ihtimaller (kısmi hak ehliyeti gibi) öğretide tartışılmıştır.

Bu ihtimallerin her birinin buradaki durumla bir ölçüde örtüşen bir yönünün olduğu söylenebilir. Gerçekten de yapay zekâ sisteminin somut iradeyi oluşturması, kendisini kullanan açısından beyaza imzada metnin doldurulmasına benzetilebilir. Aynı şekilde otonom yapıdaki sistemin bu durumu temsildeki temsilcinin durumuna benzetilebilir. Genel ya da çerçeve irade açıklaması da buradaki duruma bir ölçüde uymaktadır. Organın davranışlarının tüzel kişiliğe yüklenmesi ile buradaki durum hem içerik hem de doğrudanlık itibariyle örtüştürülebilir.

Ancak kanaatimce bu ihtimallerin hiçbiri buradaki sorunu tek başına kapsayacak bir yapıda değildir. Bu ihtimallerin yanına, irade özerkliğine dayalı şekilde oluşturulmuş/üye olunmuş bir tüzel kişilikteki üye tüzel kişi ilişkisi de kanaatimce eklenebilir. Bu durumun bir tür genel ya da çerçeve irade açıklaması olduğu söylenebilir. Ancak hem birden çok işlemi kapsaması, hem de hedeflenen irade ile ulaşılan son durumun birebir örtüşememesi ihtimali itibariyle kanaatimce merkezde durması gereken çözüm bakış açısı bu olmalıdır. Elbette burada da bütün sorunların birebir ve her yönüyle kapsanması söz konusu değildir. Zaten burada doğrudanlık da söz konusu değildir. Ancak özü itibariyle buradaki durumun isnat edilebilirliği açıklamaya daha yakın olduğu söylenebilir. Yukarıda belirtilen her bir kurumun özünden buraya uyanları bir araya getirip bir tür genel hukuk kıyasıyla yapay zekâ sistemlerinin ortaya koyduğu beyanların kullanıcılara isnat edilmesinin benimsenmesi belki daha uygun bir yaklaşım dahi olabilecektir. Böylece tartışmanın merkezine kişinin irade özerkliği çerçevesinde yaptığı bir hukuki işlemle bağlı sayılması düşüncesi oturtulmaktadır. Bu şekilde olağan çerçevede bir çözüm temeli bulunduktan sonra, sorunlu görülen hususların çözülmesi muhtemelen daha doğru ve yerinde bir yaklaşım olacaktır.

Bu çalışmada yapılan tartışmalarla hem güncel yapay zekâ uygulamaları itibariyle bu hukuki sorunun anlaşılması ve tartışılmasına yönelik bir temel çerçeve çizilmiş, hem de giderek yeni uygulama ve gelişmelerle daha da önemli hale gelebilecek olan bu soruna dikkat çekilmiştir.

Anahtar sözcükler: Yapay zekâ, yapay zekânın otonom yapısı, irade açıklaması, hukuki işlem, irade özerkliği.

THE PROBLEM OF THE EXPLAINABILITY OF THE DECLARATION OF INTENT MADE THROUGH ARTIFICIAL INTELLIGENCE WITH REGARD TO PARTY AUTONOMY

ABSTRACT

The current topic of the problem is about declaration of intent made by artificial intelligence probable legal regime especially autonomous construction of artificial intelligence. On this concept the stand-out point with currently available artificial intelligence is its general attributability to the user of declaration of intent.

As of today, lots of artificial intelligence applications are used for contractual relationships: The Internet of Things applications are more widespread. While on the stock market constructs that can process fast and comprehensive transactions, different smart contract applications, and contracts that can be done on various Internet platforms and many others can be wide and general examples.

Using artificial intelligence on all of this and similar processes from an outside look can be acted with the objective element of declaration of intent. In other words, from the outside, it can be assumed that there is a declaration. This qualified declaration of who can be attributed or the possibility of attribution and who holds the burden of "intent" are the topics that will be discussed here.

However, considering the level of current artificial intelligence applications, this problem has been addressed by ruling out some other possibilities: The current applications of artificial intelligence are not yet at the level of general artificial intelligence. On the contrary, they are examples of narrow artificial intelligence. Therefore, the debates about the legal status, which have been discussed in this area for a long time and have become more intense, were not directly entered. This discussion of whether it is needed, for example, attributions of artificial or electronic personality to artificial intelligence, has to be answered negatively to achieve this topic's conclusion. So, it needs to be accepted while solving this topic that in this plane with the attributions of declaration of intent to artificial intelligence is not right in its current state. Without this approach, this topic would be discussed with the solvability of current institutions directly/indirectly. Another acronym is like this: Classic computer programs and probabilities, systems which also can make decisions randomly even though they are within the probabilities, it is accepted with deterministic builds, this study's direct subject is not this.

Here, the systematic bases are not traditionally deterministic, instead from start to finish every movement is programmed. It is learned from data, and it is expected that decisions made are statistically closest to truth and this degree are autonomous builds.

In this context, it needs to be acted with these in mind; declarations of intent of other systems, (for example autonomous or top-to-notch fully programmed internet of things applications) are already attributed to the user. If the same situation come to

head in the same concurrent state of artificial intelligence with autonomic nature. This is the problem!

In addition to the declaration of the artificial intelligence (i.e. the objective element of the declaration of intent), the declaration of intent must contain other elements in order to be able to speak of a complete declaration of intent. In this respect, the subjective elements of the declaration of intent, namely the will to act, the will to declare and the will to do transaction, must be present. It must be acted in an ordinary state meanwhile it is processing these subjects. Declaration of intent is the base element of legal transaction and sometimes these are used synonymously because of a person's ability to arrange their legal relationship however they want and the presence of intent. This intent's execution is mostly used in the field of these legal transactions. Therefore a person that acts with intent, informs actions that could possess legal importance, the presence of will of intention and finally the will have to be towards specific contents of legal transactions to make it happen.

When artificial intelligence declared intent, the user of this in normal situations possibly cannot know and control the current situation, conditions and probabilities.

Especially autonomous structure and other characteristic features are makes it this way. From this point, there could be an outcome where the user did not think or even desired. Also, from a technical point of view, it can be said there are missing the last two components of subjective elements. Since for specific legal actions after the system has been made generally usable, there is no evident or specific intent (from point of the user). In this context, there are different approaches and possibilities with regard to the problem of assigning will to the user.

It should be stated that none of the existing concepts have been brought into consideration with artificial intelligence systems. In this respect, there is no specific regulation, and this is completely understandable in terms of technical background. In that case, the most plausible way to solve the problem is to find a solution by making use of existing concepts and, if possible, by analogy.

Considering the existing institutions, the ones that can be most similar to this situation are courier, blank signature, the general or framework declaration of intent, the representation, and the relationship between the organs of legal person and the legal person. As a matter of fact, these and some other possibilities (such as partial legal capacity) are discussed in the doctrine.

It could be said, every one of these possibilities its way with overlaps these situations at one point. Artificial intelligence has a definite will comparable to filling the signed blank. Same way, systems with autonomous structure situation is comparable to representer situation on representation. General or frame declaration of intent is compatible with this situation at one point. Legal personality's taking the behaviour of organs is comparable with the contents and immediacy of this situation.

But in my opinion, none of these explanations can cover this problem. Other than these possibilities, in my opinion, a constructed/affiliated with freedom of will to a legal personality's legal person member's relation can be added. This situation can be said a kind of general or frame declaration of intent. However, in my opinion, this should be the solution point of view that should be the focus, since the process performed by artificial intelligence usually involves many transactions and it is possible that the will and the final situation reached can differ significantly from each other. Of course, here it can't cover one on one every aspect of every problem. Here there can be no immediacy anyways. It may even make more sense to bring together those who fit here from the nature of the institution mentioned above, and to assign the statements of artificial intelligence systems to the users with a kind of general legal analogy. This puts the idea of being bound to a legal transaction made within the framework of autonomy of will at the centre of the discussion. After finding a solution base within the usual framework in this way, it is probably a more correct and reasonable approach to solve the problematic problems.

Discussions made in this study are basic frameworks towards both understanding and discussing legal problems of current artificial intelligence applications and the more and more possible importance of this problem with the increasing of new applications and improvements.

Keywords: Artificial intelligence, autonomous construction of artificial intelligence, declaration of intent, legal transaction, party autonomy (freedom of will).

OTONOM SİLAH SİSTEMLERİ VE CEZA SORUMLULUĞU

Murat BALCI*

ÖZET

Yapay zeka sistemlerinin gelişmesi ile birlikte, dünya savaş sistemleri ve silah sistemleri de gelişmekte ve dönüşmektedir. Her geçen gün hızla gelişen silah sistemleri insanlardan arındırılmaktadır. Otonom silah sistemleri de son dönemlerde geleneksel silahların yerini almaktadır. Ceza hukuku açısından önemli bir konu, otonom silah sistemleri tarafından işlenen suçlarda sorumlunun kim olacağıdır. Çalışmamızda otonom silah kavramı, öldürücü robotlar ve insansız hava araçlarının hukuki durumu ele alınacak, ceza sorumluluğunun şahsiliği prensibi, dolaylı faillik doktrini ve emir komuta sorumluluğu incelenecektir.

Anahtar Kelimeler: Yapay zeka, otonom silah, öldürücü robot, cezai sorumluluk, dolaylı faillik

AUTONOMOUS WEAPON SYSTEMS AND THE CRIMINAL RESPONSIBILITY

ABSTRACT

The world war systems and weapon systems are in the progress of developing and transforming related to the development of the artificial intelligence systems. The developing weapons systems are being purified from humans day by day. The traditional weapons are being replaced by the autonomous weapon systems nowadays. The important subject in terms of criminal law is who will be responsible for the crimes committed by autonomous weapon systems. In this study, the concept of the autonomous weapon, killer robot and unmanned air vehicles will be adressed and the priciple of individual criminal responsibility, the doctrine of indirect perpetration and the responsibility of chain of command will be examined.

Keywords: Artificial Intelligence, Autonomous Weapon, Killer Robot, Criminal Responsibility, Indirect Perpetration

* Prof. Dr. Murat BALCI, Fatih Sultan Mehmet Vakıf Üniversitesi Hukuk Fakültesi Öğretim Üyesi

YAPAY ZEKA DESTEKLİ SİLAHLARIN HUKUKSAL YAPISI

Av. Dr. Ahmet Çağrı YILMAZ*

ÖZET

Askeri teknolojide önemli yeri olan silah sistemlerinde, makina otonomisine doğru ciddi bir eğilim olup, hedeflerin imhasında insan faktörü devre dışı bırakılmaktadır. Önceden teorik olarak tartışılan fakat son on yıl içerisinde, savaş alanlarında kullanılan bu yeni teknolojik silahlar çatışma ortamlarında üstünlük sağlamaktadır. Şayet yapay zeka destekli silah sistemlerinin faydası olacaksa ve bu teknolojiyle devletler daha az sayıda asker kaybedeceklerse hem siyasi liderler hem de toplum robot teknolojisini destekleyecektir.

Yapay zeka destekli silahların askeri faaliyetlerde kullanılacak olması durumunda, devletler savaş hukuku bağlamında, 1907 Lahey Sözleşmesi, 1949 Cenevre Sözleşmesi, 1977 Ek Protokolleri ve 1948 Uluslararası Sivil Havacılık Chicago Konvansiyonunu dikkate alarak düzenleme yapmalıdır. Bununla birlikte askeri hedeflerin imhası konusunda mevcut uluslararası hukuk düzeni yeterli değildir. Yapay zeka, tüm dünyadaki askeri kuvvetlerin geleceğinin bir parçası olsa bile bu silahların yıkıcı etkileri göz ardı edilmemelidir. Otonom silah teknolojisinin gelişmesini ve uygulanmasını sınırlandırabilecek düzeyde önlemlerin alınmasının gelecekte mümkün olmadığı gözükmektedir.

Bilim insanları son atmış yıldır insan beyninin işlevsel yönünü makinalarla taklit etmeye çalışmaktadır. Bu nedenle yapay zekanın geleceğine yönelik tartışmalar, bugün olduğu gibi ilerleyen yıllarda da devam edecektir. Yapay zekalı varlıklar, yüksek belirsizlik ortamlarında, insan aklına yaklaşabilecek ve daha da ileriye götürecek hatasız kararlar alabilecektir.

Kısa vadedeki sorun, bu sistemlerle çalışan silahların hukuksal alt yapısının nasıl oluşturulacağı konusudur. Ticari sektörün büyümesiyle orantılı olarak otonom sistemler kabiliyetlerini arttıracak ve burada denenmiş tüm teknolojiler, askeri kuvvetler tarafından tecrübe edilip mevcut olası hataları giderildikten sonra savaş alanlarında kullanılacaktır. Artık savaş durumunda, teknolojik olarak güçlü devletler harp prensipleri kapsamında bir adım daha ileride olmaktadır. Askeri personelin inisiyatifi ve gelen istihbarat bilgilerinin değerlendirilmesi sonucu seçilen hedefler, yargılanma

* Avukat, Doktor Öğretim Görevlisi, Yeditepe Üniversitesi, ORCID: 0000-0002-8800-4916, cagri.yilmaz@yeditepe.edu.tr

şansı verilmeden ve çoğu zaman kimsenin haberi olmadan SİHA'lar tarafından imha edilmektedir. İnsan Hakları Evrensel Beyannamesinin 3. maddesi, herkesin yaşam hakkı olduğunu ve bunun evrensel bir ilke olarak kabul edildiğini belirtmesine karşın imha edilen hedeflerde kimlikler açıklanmadığı için operasyonların hukuka uygunluğu tartışmalı hale gelmektedir.

Bu asimetrik güç avantajı, savaşan devletlere ciddi inisiyatif sağlayacak ve maliyetlerini düşürecektir. Askeri personel kendi hayatlarını devletlerin bekası için feda edebilir; fakat, yakın gelecekte bu görev yapay zeka destekli robotlara teslim edilecektir.

Anahtar Kelimeler: Otonom Silah Sistemleri, Robot, Siber Güvenlik, Uluslararası Hukuk, Yapay Zeka

LEGAL STRUCTURE OF ARTIFICIAL INTELLIGENCE SUPPORTED BY WEAPONS

ABSTRACT

There is a serious trend towards machine autonomy in weapon systems, which have an important place in military technology, and the human factor is no longer use in the destruction of targets. These new technological weapons, previously discussed theoretically, but deployed on the battlefields in the last decade, provide the upper hand in conflict situations. If artificial intelligence weapon systems are to be beneficial and states are to lose less soldiers thanks to this technology, both political leaders and society would support robotics.

Legal structure of artificial intelligence supported by weapons are to be used in military activities, states should make arrangements in the context of the law of war, taking into account the 1907 Hague Convention, the 1949 Geneva Convention, the 1977 Additional Protocols and the 1948 Chicago Convention on International Civil Aviation. However, the current international legal order is not sufficient for the destruction of military targets. Although it is certain that artificial intelligence will become part of the future of military forces around the world, the destructive effects of these weapons should not be underestimated. Measures to limit the development and application of autonomous weapons technology are unlikely to be possible in the future.

Scientists have been trying to imitate the functional aspects of the human brain with machines in the last sixty years. Discussions on the future of artificial intelligence will continue in the years to come, just as they do today. In environments of high uncertainty, entities with artificial intelligence will be able to make error-free decisions at a level approaching or even surpassing human reasoning.

The problem in the short term is that the exact global impact of weapons powered by these systems cannot be predicted. Autonomous systems will increase their capabilities in proportion to the growth in the commercial sector, and all the technologies tested here will be used on the battlefields after the military forces have experienced and debugged them. In the event of war, technologically powerful states will be one step ahead in terms of the principles of warfare. The targets selected as a result of the initiative of the military personnel and the evaluation of the incoming intelligence information are destroyed by SİHA without giving a chance to be tried and often without anyone knowing. Although Article 3 of the Universal Declaration of Human Rights states that everyone has the right to life and that this is accepted as a universal principle, the transparency of the operations becomes controversial as the identities of the destroyed targets are not disclosed.

This asymmetric power advantage will give belligerents significant initiative and reduce their costs. Military personnel may sacrifice their own lives for the survival of the state, but in the near future this task will be handed over to artificial intelligence powered robots.

Keywords: Autonomous Weapon Systems, Robot, Cyber Security, International Law, Artificial Intelligence

AVRUPA KOMİSYONU'NUN YAPAY ZEKADA SÖZLEŞME DIŞI SORUMLULUĞA İLİŞKİN 28.9.2022 TARİHLİ ÖNERİSİNİN DEĞERLENDİRİLMESİ

Halil Emre GÜRLER*

ÖZET

Avrupa Parlamentosu ve Avrupa Konseyi'nin önerisi olan 28.9.2022 tarihinde yayınlanan direktif sözleşme dışı sorumluluk kurallarının yapay zekaya uyarlanmasına ilişkin bir teklif barındırmaktadır. İlgili direktif yapay zekanın kullanımına ilişkin sorumluluk rejiminin belirlenmesi adına önemli bir adım olmasının yanı sıra birçok açıdan çarpıcı ve tartışmaya açık yönler barındırmaktadır. Yapay zeka gelişmekte ve kullanımı birçok avantajı beraberinde getirmektedir. Ancak yasal sorumluluk rejimine yönelik problemler yapay zekanın şirketlerce kullanılmasında tereddütlere sebep olmaktadır. Bu direktifle, yapay zeka özellikli ürün ve hizmetlerin neden olabileceği zararlara ilişkin taleplere, kusur tespitine, ispat sorunlarına, sorumluluğun belirlenmesine, illiyet bağına, yargılamaya ilişkin sorunlara mevcut mevzuatların veremediği cevaplar göz önüne alınarak çözüm üretmek amaçlanmıştır. Mevcut mevzuatın yapay zeka sorumluluğuna uyarlanabilirliği bir dereceye kadar mümkün olup mevcut konjonktürde belirsizlik yaratmakta, yapay zeka sorumluluğunun yasal olarak sınırlarının belirlenmemiş olması aynı zamanda sigortacılık açısından da problem teşkil etmektedir.

Bu bağlamda, yapay zekanın ve buna ilişkin sorumluluğun yasal zemine kavuşturulması sorumluluk rejiminin belirlenmesi ve hukuki belirlilik (öngörülebilirlik) zemininde gereklilik kazanmıştır. Bu gerekliliğe binaen Avrupa Komisyonu'nun tasarısı bir mihenk taşı olarak önem taşımaktadır. Öneri, hem yapay zeka kullanan şirketlerin hem yapay zekanın etkilediği gerçek ve tüzel kişilerin, nihai olarak tüketicinin korunmasına yönelik öneriler barındırmaktadır. Yapay zekanın sosyo-ekonomik açıdan toplumsal gelişime katkısı yadsınamaz düzeydedir. Ancak her türlü gelişmenin avantajlarının yanı sıra dezavantajları olduğu da bir gerçektir. Bu sebeple, yapay zekanın kullanımının yol açabileceği zararlara ilişkin sorumluluk rejiminin belirlenmesi tüm dünya ülkeleri açısından bir zorunluluktur. Yapay zekanın etki potansiyelinin büyüklüğü dikkate

* Avukat, Ankara Üniversitesi The Sea & Maritime Law doktora araştırmacısı, ORCID NO: 0000-0002-7585-3417, av.emrgurler@gmail.com

alındığında sorumluluk rejiminin yanı sıra sigortalanması da önem taşımaktadır. Avrupa Komisyonu önerisi yasal sorumluluk ve sigortaya yönelik yeni bakış açıları getirmekte, mevzuatın geliştirilmesine katkıda bulunmaktadır.

Bu direktifteki öneriler çerçevesinde sorumluluk alanı varsayımlardan öteye giderek genişletilmekte, kusura ilişkin illiyet bağına yeni bir bakış açısı getirerek illiyet bağı karinesi getirilmekte, ispat hukuku ve kusursuz sorumluluğa ilişkin mekanizmalara ve iç hukuka atıflarda bulunulmaktadır. Ancak direktifin bu hususlardaki boşluğu doldurabilip dolduramadığı tartışmaya açıktır.

Tebliğimizde, yapay zekaya ilişkin Avrupa Komisyonu önerisinin değerlendirilmesi, bu önerinin iç hukuka uyarlanması sorunu ve gerekliliği tartışılacak, Türkiye hukukundaki mevcut kurallar ile karşılaştırması yapılacaktır.

Anahtar kelimeler: yapay zeka, hukuki sorumluluk, avrupa konseyi, direktif, sigorta

EVALUATION OF THE EUROPEAN COMMISSION'S PROPOSAL DATED 28.9.2022 ON NON-CONTRACTUAL LIABILITY IN AI

ABSTRACT

The directive published on 28.9.2022 is the proposal of the European Parliament and the European Council which contains a proposal for the adaptation of non-contractual liability rules to artificial intelligence (AI). In addition to being an important step in determining the responsibility regime for the use of AI, the relevant directive contains striking and controversial aspects in many respects. AI is developing and its use brings many advantages. However, the problems regarding the legal liability regime cause hesitations in the use of AI by companies. With this directive, it is aimed to find solutions to the claims regarding the damages that may be caused by AI enabled products and services, fault detection, problems of evidence, determination of responsibility, causation, and judicial problems by considering the answers that current regulations could not provide. The adaptability of the current regulations to AI liability is possible to a certain extent and creates uncertainty in the current conjuncture, and the fact that the legal limits of AI liability are not determined also poses a problem for insurance.

In this context, legal grounding of AI and related responsibility has become necessary on the basis of determining the responsibility regime and legal certainty (predictability). Based on this requirement, the proposal of the European Commission is important as a benchmark. The proposal includes recommendations for the protection of both companies using AI and natural and legal persons affected by AI, and ultimately the consumer. The contribution of AI to social development in socio-economic terms is undeniable. However, it is a fact that all kinds of development have

advantages as well as disadvantages. For this reason, it is a necessity for all countries of the world to determine the liability regime for the damages that may be occured by the use of AI. Considering the magnitude of the potential impact of AI, insurance is important as well as the liability regime. The European Commission's proposal brings new perspectives on legal liability and insurance and contributes to the development of current regulations.

Within the framework of the recommendations in this directive, the scope of responsibility is expanded by going beyond assumptions, the presumption of causation is brought by bringing a new perspective to the causal link regarding fault, and references are made to the mechanisms and domestic law regarding the law of evidence and strict liability. However, it is open to discussion whether the directive can fill the gap in these matters.

In our paper, the evaluation of the European Commission's proposal on AI, the problem and necessity of adapting this proposal to domestic law will be discussed, and its comparison with the existing regulations in Turkish law will be made.

Keywords: artificial intelligence, civil liability, european commission, directive, insurance

HUKUKTA YAPAY ZEKA KULLANIMI - HAKİM YAPAY ZEKA

Salih KARADENİZ*

ÖZET

Dünya her an değişip dönüşmekte, teknolojilerin getirmiş olduğu yenilikler hayatımıza girmektedir. Teknolojinin getirilerinden istifade eden alanlardan biri de hiç şüphesiz hukuk olmuştur. Bu doğrultuda yapay zekânın hukukta kullanımı ön plana çıkmaktadır. Hukukta yapay zekânın kullanılması dava öncesi ve sonrası yapay zekâ kullanımı olmak üzere sınıflandırılmakta; dava sonrası yapay zekâ kullanımı da kendi içerisinde; hâkime yardımcı yapay zekâ, karar taslaklarını hazırlayan yapay zekâ ve hâkim yapay zekâ olmak üzere üçe ayrılmaktadır. Bildiride bu türlerden biri olan hâkim yapay zekaya odaklanılacaktır.

Hâkim yapay zekâ, insan hâkimin yerine geçerek; uyuşmazlık konusu hakkında yargılamayı yürüten, tarafları dinleyen, dava ve cevap dilekçelerini değerlendirebilen vb. gibi yargılama safhasında bir hâkim tarafından yerine getirilen işlerin tamamını veya büyük bir kısmını yapabilen sistemdir. Hâkim yapay zekâya, halihazırda hangi uyuşmazlık konularının verilebileceği tartışmalıdır. Bildiride bu tartışmaya cevap aranacak, ilerleyen süreçte atılması gereken adımlardan bahsedilecektir. Diğer taraftan hâkim yapay zekânın uyuşmazlıkla alakalı karar verdikten sonra bu kararına karşı kanun yoluna gidilebileceği açıktır. Ancak hâkim yapay zekânın verdiği kararlara karşı kanun yoluna gidildiğinde, kanun yolu incelemesinin kim tarafından yapılması gerektiği üzerinde görüş birliği bulunmamaktadır. Bildiride bu soruna yönelik cevap aranacaktır. Hâkim yapay zekanın kararlarına karşı gidilecek olan kanun yolunda, farklı bir kanun yolu mercii önerisinde de bulunulacaktır. Bu öneride ifade edilecek olan kanun yolu başvurusunun hukuki olarak etki doğurup doğurmaması gerektiğine de değinilecektir. Hâkim yapay zekanın faydaları olarak; adalet hizmetlerinin hızlanması ve hukuki korumanın daha etkin hale gelmesi, hatalı kararların azalması ve mahkemelere olan güvenin yeniden canlanması avantajları dile getirilmektedir. Hâkim yapay zekanın sakıncaları olarak; algoritmik önyargı, şeffaf olmama, sistemin saldırıya uğraması ihtimali, hukukun esnekliğini yitirmesi ve kişisel verilerin ele geçirilmesi endişeleri sayılmaktadır. Sayılan bu olası fayda ve sakıncalar bildiride tartışılacak; Türk yargı sisteminde özellikle hukukta yapay zekâ kullanımı başlığı altında, nasıl bir yol izlenmesi gerektiği sorununa çözümler sunulacaktır.

Anahtar Kelimeler: Hukukta Yapay Zekâ, Hâkime Yardımcı Yapay Zekâ, Karar Taslaklarını Hazırlayan Yapay Zekâ, Hâkim Yapay Zekâ, Adli Yapay Zekâ.

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

USE OF ARTIFICIAL INTELLIGENCE IN LAW-JUDGE ARTIFICIAL INTELLIGENCE

ABSTRACT

The world is changing and transforming every moment, and the innovations brought by technologies are entering our lives. One of the fields that benefit from the benefits of technology has undoubtedly been law. In this direction, the use of artificial intelligence in law comes to the fore. The use of artificial intelligence in law is classified as pre-litigation and post-litigation artificial intelligence, and post-litigation artificial intelligence is divided into three types: artificial intelligence assisting the judge, artificial intelligence drafting judgments, and judge artificial intelligence. This paper will focus on one of these types, judge artificial intelligence.

Judge artificial intelligence is a system that replaces a human judge and performs all or a large part of the tasks performed by a judge during the trial phase, such as conducting the proceedings on the subject matter of the dispute, listening to the parties, evaluating the pleadings, etc. It is currently controversial which dispute issues can be assigned to the judge artificial intelligence. In this paper, an answer to this debate will be sought and the steps to be taken in the following process will be mentioned. On the other hand, it is clear that a legal remedy can be taken against the decision of the judge artificial intelligence after it makes a decision regarding the dispute. However, there is no consensus on who should conduct the legal remedy review against the decisions of the judge artificial intelligence. In this paper, an answer to this problem will be sought. A different legal remedy authority will also be proposed in the legal remedy against the decisions of the judge artificial intelligence. It will also be mentioned whether the legal remedy application to be expressed in this proposal should be legally effective or not. The benefits of judge artificial intelligence include the acceleration of justice services and legal protection, the reduction of erroneous decisions and the revival of trust in the courts. The drawbacks of judge artificial intelligence include algorithmic bias, lack of transparency, the possibility of the system being hacked, loss of flexibility of the law, and concerns about the capture of personal data. These possible benefits and drawbacks will be discussed in the paper, and solutions will be offered to the problem of what kind of a path should be followed in the Turkish judicial system, especially under the title of the use of artificial intelligence in law.

Keywords: Artificial Intelligence in Law, Artificial Intelligence Assisting Judges, Artificial Intelligence Drafting Decisions, Judge Artificial Intelligence, Judicial Artificial Intelligence.

THE MAIN CHALLENGES OF E-ELECTIONS: PROS AND CONS (Case Study of Georgia)

Prof. Dr. Mariam JIKIA*

ABSTRACT

The transformation of the world in the era of digital technologies and mass communication has led to new opportunities in different directions. The role and importance of digital technologies is becoming more relevant and visible in political processes, including the election process.

Several states have established the mentioned election system quite well and ensure the election process entirely with electronic elections. Georgia is among the countries where the implementation of the mentioned technologies is progressing at this stage.

Public Opinion together with the expertise about electronic elections are divided: some believe that elections conducted using electronic technologies will ensure consolidation of democracy and strengthen the trust in the electoral process, while others believe that it is associated with additional risks related to the security of the electoral process. Discussing given issue, it is important to consider the migration processes, which is vital for the Georgian population and directly influences the political processes ruled and stabilized by the elections. Without an electronic election system, 85% of emigrants do not have an opportunity to exercise their right to vote because of difficulties.

The aim of the presented paper is to study the process of introducing electronic elections in Georgia and the associated challenges. Based on the goals and objectives of the research, the advantages and weaknesses of the electronic election system were evaluated on the example of different countries; the opinions of election administration experts, critical evaluations of local and international observation organizations are analyzed.

The main conclusion of the paper is the explanation of the features of the electronic election process and the assessment of the perspective of implementation in the modern Georgian reality.

Keywords: E-elections, Democracy, Equality, Migration, Georgia

* Georgian Technical University, ORCID: *0000-0001-7810-4780, marijiqia@gmail.com*

LEGAL FIGHT AGAINST RANSOMWARE-RELATED CRIMES IN THE UNITED STATES

Kerime TOPRAK*

ABSTRACT

Ransomware is malware that uses encryption to block access to data on a computer and dramatically incapacitate it unusable[1]. Although there are different types of ransomware, in many cases, it is impossible to access data without paying ransom due to strong encryption[2]. However, it is possible that data cannot be recovered even after payment. In recent years, the opportunity to receive cryptocurrencies as payment has increased the attacks by criminals[3]. Sometimes criminals threaten to not only lock data but also release it publicly if the ransom is not paid, putting organizations at risk of reputational damage[4].

The United States of America (USA) has been exposed to such attacks with its various institutions, such as the health sector and universities, as well as major attacks such as the Colonial Pipeline attack. For this reason, it has done significant work in the fight against ransomware-related crimes[5]. In addition to increasing the security of data in public institutions and the private sector with various regulations and taking measures to effectively counteract an attack; It also imposed criminal sanctions against these acts.

Article § 1030(a)(7) of the Computer Fraud and Abuse Act, a federal law, is used by the U.S. Department of Justice to enforce sanctions. Depending on the nature of the stolen information, the ransomware attack can also be considered a crime under the Economic Espionage Act[6]. In addition, the US assesses that the organizers of the ransomware attack, as well as the victims who paid the attacker, could commit various crimes. For example, it is stated that if the attacker has connections with the countries

* PhD Candidate at Swansea University Criminology, https://orcid.org/0000-0003-4457-9336, kerimetoprak@hotmail.com

1 LEO, Philipp/ IŞIK, Öykü and MUHLY, Fabian. "The Ransomware Dilemma." *MIT Sloan Management Review* 63, no. 4, 2022, p.13-15.

2 ALESSANDRINI, Adam, RANSOMWARE Hostage Rescue Manual, KnowBe4, p.8 http://resources.idgenterprise.com/original/AST-0147692_Ransomware-Hostage-Rescue-Manual.pdf.

3 Europol. *Internet Organised Crime Threat Assessment (IOCTA 2020)*. European Union Agency for Law Enforcement Cooperation (Europol), 2020, p.18

4 JENKINSON Andrew. Ransomware and Cybercrime. CRC Press, 2022, p.19

5 Federal Bureau of Investigation, Internet Crime Report Center, Internet Crime Report, 2021 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf, p.1

6 BERRIS, Peter G. and Jonathan M. GAFFNEY. " Ransomware and Federal Law: Cybercrime and Cybersecurity.", Congressional Research Service, 2021, p. 3-4

that the USA has sanctioned, the people who are the actual victims of the attack may also face criminal sanctions as a result of the payment[7].

In March 2022, US President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act to impose an obligation on critical industries to report cyberattacks, including ransomware attacks, and their payments. In addition to the federal regulations, there are also regulations made based on some states. In this paper, the legal approach of the USA against ransomware, the regulations regarding ransomware attackers and those who face this attack will be discussed.

Keywords: Ransomware, data, cybercrime, criminal sanctions

7 BERRIS and GAFFNEY., ibid, p.7-8

THE ROLE OF IT IN ACTIVATING ANTICORRUPTION POTENTIAL OF CIVIL SOCIETY

Dr. Roza JUMABEKOVA* - Dr. Bagdat AUYESHOVA**

ABSTRACT

Anticorruption policy is a purposeful activity of the state to combat manifestations of corruption. On the other hand, corruption is a serious threat to the national security of the state; it creates obstacles to the functioning of public authorities on the basis of law and legislation and hinders economic development of the Kazakhstan. Corruption has reached a high level, which violates principles of equality and social justice, and creates difficulties in the economic development of the republic and impedes the growth of efficiency in public administration and local government. In addition, corruption undermines the population's confidence in the authorities and significantly impedes economic development of Kazakhstan, in connection with which it is necessary to implement anticorruption practices.

According to the authors' research, the use of the latest IT in the world proves their effectiveness in the implementation of anticorruption practices. Moreover, in the conditions of citizens' unwillingness to take an active part in the anticorruption fight, the use of IT tools can become one of the effective ways to involve the population in the fight against corruption.

During the research, authors used the anticorruption monitoring data "Adaldyk alany" in the Mangystau region (Kazakhstan), the most effective forms of public participation in combating corruption are public investigations into corruption, as well as public control and monitoring of administrative practices in areas with high corruption risks.

Keywords: IT law, corruption, anticorruption policy, civil society.

* Yessenov University, Kazakstan
** Yessenov University, Kazakstan

AMERİKAN HUKUKUNDA SOSYAL MEDYA PLATFORMLARININ DÜZENLENME VE DENETLENME SORUNSALI

Dr. Samet TATAR*

ÖZET

Sosyal medya platformları, toplumlar ve bireyler için sayısız faydalar sağlarken günümüzde iletişim, e-ticaret, lojistik gibi çoğu sektörün ticari faaliyetlerin sürdürdüğü alanlar haline gelmiştir. Gerek sosyal medya platformlarının kar amacı güden şirketler olması bakımından gerekse sosyal medya platformlarındaki kullanıcıların karşılaştığı hukuki sorunlar açısından kanun koyucular ve bağımsız idari otoriteler, sosyal medya platformlarının faaliyetlerinin nasıl regüle edileceğini ve ilgili regülasyon faaliyetleri kapsamında devletlerin idari kurum ve kuruluşlarının gözetim ve denetim yetkisinin nasıl kullanılacağı hukuk literatüründe sıklıkla tartışılmaktadır. Özellikle Avrupa Birliği, Amerika Birleşik Devletleri ve Çin'in sosyal medya platformlarına ilişkin düzenleme ve denetleme faaliyetleri gerek gelişmekte olan ülkelerce gerekse de sektör temsilcileri tarafından dikkatlice izlenmektedir. İşbu noktada, bu bildiride Amerika Birleşik Devletleri'nde sosyal medya platformlarının regüle edilip edilmemesi ve sosyal medya şirketlerinin "uyum" kapsamında mevcut ve ileride gerçekleşecek yasama faaliyetleri kapsamında bağımsız idari otoriteler tarafından gözetim ve denetiminin nasıl yapılacağı tartışılacaktır. Özellikle Amerikan hukukunda sıklıkla karsımıza çıkan self-regulation (özdenetim) mekanizmasının sosyal medya platformlarının düzenlenmesi ve denetlenmesinde etkin, hızlı ve profesyonel bir yönetişim bicimi olduğu ele alınacaktır.

Koronavirüs Pandemisinin (Kovid-19) birlikte yalan haber ve dezenformasyon tartışmalarını Amerikan kamuoyunda yeniden alevlenmiştir. Ayrıca 2022'de Amerika Birleşik Devletleri'nin eski başkanı Donald Trump 'in döneminde Beyaz Saraya karşı yapılan saldırılarla ilgili paylaştığı görüşlerinden dolayı; Twitter, Facebook, Youtube gibi sektörün lider pozisyonundaki sosyal medya şirketleri Başkan Trump'ın ifadelerini kendi topluluk kurallarına uymadığı için ilgili sosyal medya paylaşımlarını engellemiştir. Nitekim yasal olarak federal düzeyde sosyal medya platformlarının sorumluluklarını düzenleyen 1996 tarihli bir yasa olan İletişim Ahlaki Yasası'nın 230. Maddesine göre, dijital platformlara üçüncü kişilerin paylaşımlarından dolayı barındırılan içerikle ilgili

* Öğretim Görevlisi Dr. Samet Tatar, Ankara Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi İdare Hukuku Anabilim Dalı, stat-ar@ybu.edu.tr ORCID NO:0000-0002-3553-1683.

yükümlülüklerden muafiyet sağlayan bir düzenleme içermektedir. Bununla birlikte, hileli seçimlere yönelik asılsız suçlamalar ve diğer yalan haberlerle harekete geçen sosyal medyanın önde gelen dijital platformları, son zamanlarda bazı gönderileri güvenilmez veya gerçek dışı olarak etiketlemeye ve bazı videoları kaldırmaya başladı. Dijital platformların bu kapsamdaki faaliyetler öz düzenleme olarak dilimize çevrilen self-regülasyon olarak bilinmektedir. Gerek Amerikan federal kanun koyucusu gerekse eyalet düzeyinde kanun koyucular caydırıcı etkiden (chilling effect) dolayı sosyal medya platformlarının ağır şekilde regüle edilmesine sıcak bakmamaktadır. Bu nedenle şirketlerin özdenetim mekanizmalarının güçlendirilerek idarenin gözetim ve denetim mekanizmalarının güçlendirilmesinin sorunu çözeceği düşünülmektedir. Özdenetim kuruluşların kendi kendilerini hukuki zeminleri önceden belirlenmiş kurallara göre denetlemesini ve düzenlenmesini ifade eder. Hiç kuşkusu yok ki özdenetim mekanizmaları bağımsız idari otoritelerinin ya da benzeri idari kuruluşları gözetimi ile birlikte hukuk devletinde anlam bulacaktır. Bankacılık, sermaye piyasası gibi önemli ölçüde regüle edilen piyasalarda başarıyla uygulanan bu model sosyal medyadaki yasama faaliyetlerine aktarılacaktır. Esneklik, uzman ve liyakat sahibi personelin yetiştirilmesi, hızlıca çözüm bulma, ve bu faaliyetler için devlet bütçesinden harcama yapılmaması özdenetimin avantajları arasındayken çıkar çatışmaları durumunda şirketlerin kamu yararı karşısında kendi ticari çıkarlarını savunacağı bilinmektedir. Bu çalışmada çıkar çatışmasının önlenmesi veya dengelenmesi için çeşitli hukuki mekanizmalar önerilecektir.

Anahtar Kelimeler: Sosyal Medya, Özdenetim, Amerikan Hukuku, Caydırıcı Etki, Yalan Haber.

HOW SHOULD SOCIAL MEDIA PLATFORMS BE REGULATED UNDER THE U.S. LAW

ABSTRACT

While social media platforms provide numerous benefits for societies and individuals, they have become areas where most sectors such as communication, e-commerce, and logistics carry out commercial activities today. Legislators and independent administrative authorities, both in terms of the fact that social media platforms are profit-making companies and in terms of the legal problems faced by users of social media platforms, how to regulate the activities of social media platforms and how to use the supervision and control authority of the administrative institutions and organizations of the states within the scope of the relevant regulation activities. frequently discussed in the literature. In particular, the regulation and supervision activities of the European Union, the United States of America, and China regarding social media platforms are carefully monitored by both developing countries and industry representatives. This paper discusses whether social media platforms should

be regulated in the United States and how social media companies will be supervised and supervised by independent administrative authorities within the scope of current and future legislative activities within the scope of "compliance". The paper discusses that the self-regulation mechanism, which is frequently encountered in American law, is an effective, fast, and professional form of governance in regulating and supervising social media platforms.

Because of the impacts of the Coronavirus Pandemic (Covid-19), the discussions of fake news and disinformation have flared up again in American public opinion, In addition, to his views on the attacks against the White House in 2022, during the reign of Donald Trump, the former president of the United States; Social media companies such as Twitter, Facebook, and YouTube, are in the leading position in the industry, have blocked the relevant social media shares of President Trump's statements because they do not comply with their own community rules. Article 230 of the Communications Ethics Act, a 1996 law that legally regulates the responsibilities of social media platforms at the federal level, includes a regulation that provides exemptions to digital platforms from obligations related to hosted content due to third-party sharing. However, driven by false accusations of fraudulent elections and other fake news, leading social media digital platforms have recently begun to tag some posts as untrustworthy or untrue and remove some videos. The activities of digital platforms within this scope are known as self-regulation, which is translated into our language as self-regulation. Both the American federal legislator and state-level legislators do not favor heavy regulation of social media platforms due to the "chilling effect". Self-regulation refers to the self-control and regulation of legal grounds by organizations according to predetermined rules. There is no doubt that self-regulatory mechanisms will find meaning in the rule of law with the supervision of independent administrative authorities or similar administrative institutions. This model, which has been successfully applied in highly regulated markets such as banking and capital markets, will be transferred to legislative activities on digital platforms. While flexibility, training of expert and qualified personnel, finding solutions quickly, and not spending from the state budget for these activities are among the advantages of self-control, companies will defend their commercial interests against the public interest in case of conflicts of interest. Various legal mechanisms will be proposed to prevent or balance the conflict of interest.

Keywords: Social Media, Self-Regulation, American Law, Deterrent Effect, Fake News.

ARTIFICIAL INTELLIGENCE IN DIGITAL ECONOMY FROM INDONESIA INTEREST IN MULTIDISCPLINARY APPROACH

Firdausi FIRDAUS*

ABSTRACT

Following the era of the fourth industrial revolution and optimizing the digital economy, the deployment of Artificial Intelligence (AI) technology in many parts of human lives seem inevitable including from Indonesia's perspective. The utilization of AI is hoped will increase productivity in the business sector and optimization of human resources, push innovation in many sectors, give solutions to infrastructure issues, create constructive policy, build an inclusive digital market, improve public service to the citizen and compete in the globalization era. However, in implementing AI technology, there are many challenges that Indonesia needs to overcome such as the readiness of a skilled workforce, the readiness of regulations and ethics, the readiness of infrastructure, the readiness of industry and public sector in adopting AI, and the readiness of Indonesia society to maintain national identity from the change of culture as a result of the AI deployment in Indonesia. To cope with these challenges, the Indonesian government has introduced a national strategy to guide the development and deployment of AI in Indonesia between 2020 and 2045 according to Indonesia's needs and interests. From this guideline, it can be found the five priority areas in AI deployment and development such as bureaucratic reform, healthcare, education, research, food security, mobility and smart city. To handle AI deployment and development in Indonesia in particular in these five areas, there is four focus that needs to be addressed such as ethics and policy, talent development, infrastructure and data, and industrial research and innovation. Furthermore, ensuring the deployment and development of AI requires a multidisciplinary approach as well as multi-stakeholders, because the impact of AI will be even more massive on humanity compared to the Internet which already changes so many things in our lives for good and bad. Thus, this presentation will examine AI from different disciplinary and perspectives such as law, policy, economy, sociology, psychology, culture and religion perspective. In addition, this presentation will also produce a solution to combat issues and challenges from the deployment and development of AI in Indonesia.

* Faculty of Law and Political Science, University of Barcelona

DİJİTAL VARLIKLARIN KORUNMASI VE ULUSLARARASI YATIRIM HUKUKU

Neriman KILIÇ*

ÖZET

Son yıllarda artan dijitalleşme bizlere birçok anlamda kolaylıklar sunsa da aynı zaman çeşitli zorlukları da beraberinde getirdi. Özellikle dijital varlıkların korunması ve siber güvenliğin sağlanması hususunda devletler, yasa koyucular, akademisyenler ve diğer menfaat sahipleri çeşitli öneriler ve çalışmalarda bulunmaktadırlar. Bu konuda yabancı yatırımcıların ve onların dijital varlık ve yatırımlarının korunması konusu da benzer şekilde son yıllarda uluslararası yatırım hukuku ve tahkimi alanlarında tartışılan bir konu olmaya başlamıştır. Siber saldırılara karşı alınacak tedbirler ve bu alanın regülasyonu hali hazırda oldukça komplike bir konu iken, yabancı yatırımcıların da bu fotoğrafa dahil olmasıyla birlikte konu daha da karmaşık bir hal almıştır. Yabancı yatırımcılar da en az diğer yatırımcılar kadar siber saldırılara maruz kalmakta ve zarar görmektedirler. Siber saldırıların son yıllarda nicelik ve nitelik bakımından artışı ve olumsuz sonuçları da göz önünde bulundurulduğunda bu konunun önemi daha da net anlaşılmaktadır. Dolayısıyla diğer yatırımcılar ve vatandaşlar gibi yabancı yatırımcıların da dijital varlık ve yatırımlarının bu saldırılara karşı korunması elzemdir. Burada karşımıza çıkan soru ise bu korumanın nasıl ve hangi temele dayanılarak sağlanacağıdır. Bu hususta henüz yabancı yatırımcıları koruyan uluslararası bir mekanizma tam anlamıyla bulunmadığı için son yıllarda yabancı yatırımcıları bu siber saldırılara karşı korumak amacıyla uluslararası yatırım hukukunun devreye girmesi ve ev sahibi devletin bu hususstaki sorumluluğunun gündeme gelmesi gerektiği ileri sürülmektedir. Bu kapsamda çalışmamız yabancı yatırımcılara bir koruma sağlanabilmesi için öncelikle dijital varlıkların uluslararası yatırım hukuku çerçevesinde bir yatırım olarak kabul edilip edilmeyeceğini ve eğer kabul edilirse yabancı yatırımcılara sağlanacak korumanın ne tür bir hukuki temele dayandırılacağını inceleyecektir.

Anahtar kelimeler: Uluslararası Yatırım Hukuku, Dijital varlıklar.

* Öğr. Gör. Dr. Neriman Kılıç, İstanbul Medeniyet Üniversitesi Milletlerarası Özel Hukuk ABD

PROTECTION OF DIGITAL ASSETS AND INTERNATIONAL INVESTMENT LAW

ABSTRACT

While this digital era provides us with many conveniences, it comes with a price. In particular, the protection of digital assets and ensuring cybersecurity have become hot topics of discussion and research among academics, legislators, and other stakeholders. In this regard, the issue of protection of foreign investors and their digital assets has similarly started to be discussed in the fields of International Investment Law (IIL) and Arbitration in recent years. However, while measures to be taken against cyber-attacks and the regulation of this field are already very complicated issues, the issue has become even more challenging with the inclusion of foreign investors in the picture. Foreign investors are exposed to cyber-attacks and suffer as much as other investors. Considering also the increase in quantity and quality of cyber-attacks in recent years and the negative impacts they have, it is vital that foreign investors and their digital assets are protected. The question, however, that arises here is how and on what basis such protection could be provided. Since there is no international mechanism in this regard, it has been argued that the field of international investment law and thus, the responsibility of host states should come into play. In this context, this study will first examine whether digital assets can be qualified as 'investment' within the scope of IIL to provide such protection and if so, it will then discuss the legal basis for such protection.

Keywords: International Investment Law, Digital Assets.

ELEKTRONİK DEFTER, BEYANNAME VE FATURALAR ÜZERİNDEN TRANSFER FİYATLANDIRMASINA YÖNELİK EMSAL VERİ TABANI OLUŞTURULMASI

Arş. Gör. Simay DOĞMUŞ*

ÖZET

İlişkili kişiler arasındaki mal veya hizmet alım ve satım işlemlerinde uygulanan fiyatın, emsal fiyattan farklı olması halinde transfer fiyatlandırması yoluyla örtülü kazanç dağıtımı gündeme gelebilmektedir. Bu sebeple, emsal kavramı 5520 sayılı *Kurumlar Vergisi Kanunu*'nun[1] 13'üncü maddesinde düzenlenen transfer fiyatlandırması müessesesinin uygulanması açısından oldukça önem arz etmektedir. Emsal fiyat ise, transfer fiyatlandırmasına konu işlemin gerçekleştiği andaki serbest piyasa şartlarına göre, tarafların pazarlıklarıyla oluşan objektif fiyattır.

Transfer fiyatlandırmasına yönelik yapılan karşılaştırılabilirlik analizinde emsal alınan işlem, transfer fiyatlandırmasına konu işlem ile aynı veya benzer nitelikte ilişkisiz kişiler arasında gerçekleştirilen işlemdir. Ülkemizde emsal alınabilecek işlemlere ilişkin yeterli bilgi kaynağı bulunmadığı gibi mevcut olanlara erişim oldukça güçtür. Örneğin ülkemizde emsal tespitine ilişkin oluşturulmuş bir veri tabanı bulunmamasına rağmen, yabancı birçok ülkede abonelik sistemiyle hizmet veren veri tabanları bulunmaktadır. Bu veri tabanları şirketlere doğru ve güvenilir emsal tespiti konusunda fayda sağladığından, ülkemizde de özellikle çok uluslu şirketler tarafından kullanılmaktadır.

Kanaatimizce Türk Vergi İdaresinin elektronik defter, beyanname ve faturalar üzerinden emsal fiyat tespitine yardımcı bir veri tabanı oluşturması da mümkün ve gereklidir[2]. Kurumların bu veri tabanı ile birim fiyat ya da işlem fiyatı karşılaştırmalarını elektronik faturalar, sahip olunan iktisadî oran ya da büyüklük; kârlılık karşılaştırmalarını ise, elektronik defter ve elektronik beyannamelerden elde edilen veriler üzerinden yapmaları mümkün olacaktır.

---

* Yaşar Üniversitesi Hukuk Fakültesi Mali Hukuk Anablim Dalı Araştırma Görevlisi, (e-posta: simay.dogmus@yasar.edu.tr) ORCID ID: https://orcid.org/0000-0002-9241-0781.

1 13.06.2006 tarih ve 5520 sayılı *Kurumlar Vergisi Kanunu*, (RG. 21.06.2006-26205).

2 Benzer yönde görüş için bkz.: Adem Koyuncu, "Transfer Fiyatlandırmasında Doğru Emsale Ulaşma Sorunu ve Emsal Aralığı Kullanımı: Yurtdışı Karşılaştırmaları ile Birlikte Türkiye Uygulaması, Sorunlar ve Çözüm Önerileri", Vergi Dünyası Dergisi, Sayı: 437, Yıl: 2018, s. 123.

Nitekim vergi idareleri, üçüncü kişilerden özellikle denetim araçlarını kullanarak veya kurumlarca yapılan beyanlar üzerinden; başka bir ifadeyle elektronik defter, beyanname ve faturalar üzerinden yaptığı denetim veya beyan sistemi gereği elde ettikleri emsallerden faydalanarak transfer fiyatlandırmasına yönelik değerlendirme yapmaktadır. Böyle bir durumda vergi idareleri kullandıkları emsalleri gizli tutarak, kurumları vergi mahremiyeti gerekçesiyle bilgilendirememektedir.

Önerilen şekilde veri tabanı oluşturulması, kurumlara açık ve erişilebilir veriler üzerinden karşılaştırabilirlik analizini yapma imkânı yanında transfer fiyatlandırması yoluyla örtülü kazanç dağıtımı yapmadığı konusunda ispat kolaylığı da sağlayacaktır. Öyle ki, veri tabanında yer alan emsale uygun gerçekleştirilen transfer fiyatlandırması işlemleri karine olarak hukuka uygun kabul edilebilecek; örtülü kazanç dağıtımı yapıldığının ispatı vergi idaresine geçecektir.

Elektronik defter, beyanname ve faturalar üzerinden bir veri tabanı oluşturulması hususu, kişisel verilerin korunması ve vergi mahremiyeti ilkesi bakımından da değerlendirilmelidir. Çünkü, bu defter ve belgeler üzerinde mükellef ve mükellefle ilgili kişilerin şahıslarıyla, işlemleriyle, hesap durumlarıyla, iş ve işletmeleriyle, servet veya meslekleriyle ilgili kişisel veriler bulunduğu gibi, bu veriler aynı zamanda vergi mahremiyeti nedeniyle de korunmaktadır. Kanaatimizce, bu verilerin 6698 sayılı *Kişisel Verilerin Korunması Kanunu*'nda[3] yer alan anonimleştirme[4] benzeri bir usulden geçirilerek kimlere ait olduğu bilinmez bir hale getirilip veri tabanına dahil edilmesi durumunda kişisel veriler ve vergi mahremiyeti açısından herhangi bir sakınca oluşmasının önüne geçilebilecektir.

Anahtar Kelimeler: Transfer fiyatlandırması, emsal veri tabanı, anonimleştirme, elektronik defter, elektronik belge.

CREATING A DATABASE FOR TRANSFER PRICING THROUGH ELECTRONIC BOOKS, STATEMENTS AND INVOICES

ABSTRACT

If the price applied in the purchase and sale of goods or services between related parties is different from the arm's length price, disguised profit distribution through transfer pricing may gain currency. For this reason, arm's length principle is very important for the implementation of the transfer pricing regulated in Article 13 of the *Corporate Tax Law* No. 5520[5]. The arm's length price is the objective price formed by

3 4.03.2016 tarih ve 6698 sayılı *Kişisel Verilerin Korunması Kanunu*, (RG. 07.04.2016-29677).

4 Kavram, Kanun'un 3'üncü maddesinin 1'inci fıkrasının b bendinde "anonim hale getirme" şeklinde ifade edilmiş ve "kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi" olarak tanımlanmıştır.

5 *Corporate Tax Law* dated 13.06.2006 and numbered 5520, (OG. 21.06.2006-26205).

the bargaining of the parties, according to the free market conditions at the same time of transfer pricing transaction.

In the comparability analysis made for transfer pricing, the arm's length transaction which is taken as a precedent, is the transaction that is carried out between unrelated parties with the same or similar qualities as the transaction subject to transfer pricing. In our country, there is not enough information source about the arm's length transactions and it is very difficult to access the existing ones. For example, although there isn't any database created for the determination of arm's length transactions in our country, there are databases serving with subscription system in many foreign countries. These databases are used in our country, especially by multinational companies, as they provide benefits for companies in accurate and reliable examples of transactions.

In our opinion, it is also possible and necessary for Turkish Tax Administration to establish a database that assists in determining the comparable price over electronic books, statements and invoices. It will be possible for companies to make unit price or transaction price comparisons over the data obtained from electronic invoices. Also, it will be possible to make economic rate, owned size or profitability comparisons over the data obtained from electronic books and statements.

As a matter of fact, tax administrations make an assessment regarding transfer pricing from third parties, especially by using audit tools or through declarations made by companies. In other words, tax administrations make an assessment regarding transfer pricing by making use of the precedents obtained as a result of the audits or declaration system which are performed on electronic books, statements and invoices. In such a case, tax administrations can't inform the companies on the grounds of tax privacy by keeping used the arm's length transaction and prices confidential.

Establishing a database as suggested will provide companies opportunity to perform comparability analysis on open and accessible data, as well as provide ease of proof that they do not distribute disguised profit through transfer pricing. Such that, transfer pricing transactions carried out in accordance with the arm's length transaction in the database can be considered lawful as presumption; the proof for disguised profit distribution will be passed to the tax administration.

A collection of data on electronic books, statements and invoices should be examined in terms of protection of personal data and tax privacy because they contain personal data about the persons, transactions, account status, works and businesses, wealth or professions of taxpayers and related persons to taxpayers. These data are also protected due to tax privacy. In our opinion, any inconveniences in terms of protection of personal data and tax privacy can be avoided if these data are made unknown to

whom they belong to by passing through a method similar to anonymization[6] in the Personal Data Protection Law No. 6698[7].

Keywords: Transfer pricing, database for arm's length transaction, anonymization, electronic book, electronic document.

6 This concept is expressed as "*anonymization*" which is different from Turkish expression in subparagraph b of paragraph 1 of Article 3 of the Law and is defined as "*making personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching them with other data*".

7 *Protection of Personal Data Law* dated 4.03.2016 and numbered 6698, (OG. 07.04.2016- 29677).

SUSTAINABILITY AND DIGITALISATION: CHALLENGES AND OPPORTUNITIES FOR CORPORATE GOVERNANCE

Meltem KARATEPE KAYA*

ABSTRACT

Sustainability and digitalisation are the most important topics of discussion all over the world today. These two significant factors are also at the forefront of the elements influencing corporate management and the future. In reality, the use of blockchain technology, artificial intelligence, and machine learning in many professional situations in recent years has highlighted the interaction of digitalisation with corporate governance. In companies, as in everything else, digital transformation entails establishing a new structure by abandoning the traditional. The adoption of digital transformation is expected to strengthen, simplify and accelerate the relationships of companies with internal and external stakeholders, thus increasing the company's efficiency.

Along with digitalisation, achieving corporations' sustainability objectives is one of their top priorities. Authorities are now developing legislative guidelines for businesses to adopt an environmentally and human rights-conscious management strategy, which is the conclusion of the ESG talks. Accordingly, the EU recently adopted the Corporate Sustainability Reporting Directive (CSRD), which imposes additional requirements on large companies. The intersection between digitalisation and sustainability in company management, as well as the future of corporate governance, will be addressed in this talk in light of all these developments.

Keywords: corporate governance, digitalization, sustainability, ESG, blockchain, smart contracts

* Meltem Karatepe Kaya (Dr.), Assistant Professor, Faculty of Law, Commercial Law Department, Istanbul Medeniyet University, Istanbul, Turkey, E: meltemkaratepe.kaya@medeniyet.edu.tr ORCID: 0000-0003-3428-0293

THE ASSESSMENT OF THE EU PRODUCT LIABILITY REGIME IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE AND RELATED EMERGING TECHNOLOGIES: A NEW ERA?

Furkan BULUT*

ABSTRACT

In the 20th century, it was argued that taking the fault-based liability as the basis for the compensation of the damage caused by defective products would be insufficient due to some crucial facts such as the increase in mass production, the level of the seriousness of the damage caused by these products, and the need of the balance with which to establish a fair apportionment of the risks between the injured person and the manufacturer. Thus, with the exclusions explicitly set out, the EU Council Directive 85/474 laying down strict liability regime was adopted aiming to ensure the harmonization among the Member States, but without prejudice to rights to have claims on the basis of contractual or tort liability.

In recent years, some have argued that the Directive is far from meeting the purpose, due to the accelerated grow of technological developments, particularly the spread of the use of artificial intelligence and related concepts. AI-driven products are software-oriented complex structures which require updates and upgrades after their release, comprise some sub-mechanisms such as machine learning, deep learning. They interconnect with different products through various channels such as IoT technology and are complemented with intangible content, dispersed, and decentralized data. Although it has been stated that the definition of product may cover software insofar as it is incorporated into a physical carrier, different arguments have been put forward as to whether pure intangible or data and software provided at a later stage fall within the notions and elements of the Directive due to the lack of clarity. The inevitable features of artificial intelligence such as interconnection, self-learning algorithm-based results, continuing progress seem left out of the scope, since the manufacturer cannot be held liable for the damages that occur after the product is put into circulation. What is more, it is obvious that products with such a complex structure have also changed the producer profile taken into account at the time.

* PhD Candidate, Swansea University (Institute of International Shipping and Trade Law), furkanbulut4@gmail.com, (ORCID: 0000-0003-2940-2970)

The criterion in the directive for the defect is determined as 'not provide the safety that a person is entitled to expect'. It has been stressed that this standard reflects a 'reasonable expectation' with the characterization of 'public at large'. On the other hand, the safety that might be expected from the concept of artificial intelligence will not be able to be examined as readily as it is currently. In addition, the burden of proof of damage, the defect and the causal link is imposed on the injured person who is in an extremely disadvantageous position in terms of accessing technical information on such a complex structure, and this fact renders the strict liability regime even more problematic. Along the same line, the development risk and related defenses provided to the manufacturer should be revised, based on the elements of artificial intelligence.

In the recent period, various expert groups have been formed by the EU, and liability issues arising from the emerging technologies have been discussed. As a result of various reports, a proposal for revising product liability directive was published by the Commission. This study will shed light on the dynamics of artificial intelligence and related emerging technologies affecting the product liability regime, the elements of the Directive and whether the proposal responds the need.

Keywords: The EU Product Liability Directive, Strict Liability, Emerging Technologies, Artificial Intelligence, Machine Learning, Deep Learning

AB ÜRÜN SORUMLULUĞU REJİMİNİN YAPAY ZEKA VE İLGİLİ GELİŞEN TEKNOLOJİLER KAPSAMINDA DEĞERLENDİRİLMESİ: YENİ BİR ÇAĞIN BAŞLANGICI?

ÖZET

20. yüzyıldan itibaren seri üretimin artması, hatalı ürünlerden kaynaklanan zararların boyutunun ciddi düzeylere varması ve zarar gören kişiler ile üreticiler arasındaki dengenin bozulması gibi sebeplerle bu ürünlerin verdikleri zararın tazmininde kusura dayalı haksız fiil sorumluluğunun temel alınmasının yetersiz kalacağı yönünde görüşler öne sürülmüştür. Bu doğrultuda 1985 yılında Avrupa Birliği tarafından Üye Devletlerin ayıplı ürünlerden doğan sorumluluk ile ilgili hukuki ve idari düzenlemelerinin uyumlaştırılmasına ilişkin 85/474 sayılı AB Konsey Direktifi yürürlüğe konmuştur. Söz konusu mevzuat ile uygulanacak hukuk açısından üye devletler arasında birlik sağlanması hedeflenmiştir. Böylelikle ayıplı ürünlerden kaynaklanan zararlar için belirli limitler eşliğinde kusursuz sorumluluk rejimi benimsenmiştir.

Son yıllarda teknolojik gelişmelerin hızının artması, özellikle yapay zeka ve bağlantılı konseptlerin kullanım alanının genişlemesi gibi sebeplerle bu direktifin amacı karşılamaktan uzak kaldığı şeklinde görüşler ileri sürülmeye başlanmıştır. Zira yapay zeka entegreli ürünler veri ve yazılım odaklı olarak, piyasaya sürülmelerinin akabinde güncelleme gerektiren, dağınık ve çeşitli sağlayıcılar tarafından sunulabilen

veriler ile çalışan, IoT teknolojisi ile farklı ürünlerle bağlantı kurabilen, makine öğrenimi ve derin öğrenme gibi mekanizmaları barından kompleks yapılardır. Nitekim öncelikle ilgili düzenleme ile kapsanan ürün tanımının bu özellikleri karşılayıp karşılamadığı dahi oldukça tartışmalıdır. Mezkur düzenlemenin getirdiği tanımın belli bir donanıma entegre edilen yazılımları kapsayabileceği belirtilmekle birlikte, sonradan eklenebilen veya bu şekilde fiziki yönü olmayan verilerin veya yazılımların ürün olarak nitelendirilebilmeleri hususunda netlik olmaması sebebiyle farklı görüşler ileri sürülmüştür. Öte yandan üreticinin ürünü piyasaya sürmesi sonrasında oluşacak hatalardan sorumlu tutulamaması sebebiyle güncelleme, kendi kendine öğrenen algoritma temelli sonuçlar gibi yapay zekanın ana özellikleri saf dışı kalmış vaziyettedir. Aynı zamanda böylesine karmaşık bir yapıya sahip ürünlerin o dönem saptanan üretici profilini de değiştirdiği aşikardır.

Direktifte üründeki ayıp için kriter 'kişinin üründen beklemeye hak kazandığı güvenliğin sağlanmaması' olarak belirlenmiştir. Bu seviyenin '*public at large*' nitelendirmesiyle objektif bir standart şeklinde ortalama bir beklenti düzeyinde olduğu vurgulanmıştır. Öte taraftan yapay zeka konseptinden beklenebilecek güvenliğin sınırlarını belirlemek bahsi geçen çeşitli özellikler göz önüne alındığında oldukça zorlaşmaktadır. Ayrıca böylesine karmaşık bir yapıdan kaynaklı zarar, üründeki ayıp ve aralarındaki nedensellik bağını ispat yükünün teknik bilgiye ulaşma hususunda son derece dezavantajlı konumda bulunan zarar gören kişiye bırakılması getirilen kusursuz sorumluluk rejimini daha da sorunlu hale getirmektedir. Yine gelişen teknolojiler baz alınarak üreticiye sağlanan gelişim riski ve sair sorumluluktan kurtulma yollarının gözden geçirilmesi gerektiği aşikardır.

Son dönemde Avrupa Birliği tarafından çeşitli uzman grupları oluşturularak gelişen teknolojilerden kaynaklı sorumluluk meseleleri tartışılmaya başlanmış, mevcut ürün sorumluluğu rejimi üzerinde de çalışmalar yürütülmüştür. Yayınlanan çeşitli raporlar neticesinde Komisyon tarafından yeni bir ürün sorumluluğu direktifi önerisi hazırlanmıştır. Bu çalışmamızda yapay zeka ve ilgili teknolojik gelişmelerin ürün sorumluluğuna etki eden dinamikleri incelenecek, mevcut sistemin unsurları ve getirilen önerinin ihtiyacı karşılayıp karşılamadığı hususu değerlendirilerek konuyla ilgili görüşlerimize yer verilecektir.

Anahtar Kelimeler: AB Ürün Sorumluluğu Direktifi, Kusursuz Sorumluluk, Gelişen Teknolojiler, Yapay Zeka, Makine Öğrenimi, Derin Öğrenme

CAN ARTIFICIAL INTELLIGENCE (AI) BE AN INVENTOR? AN INTERNATIONAL ANALYSIS IN LIGHT OF 'DABUS' DECISIONS

Fatmanur CEBECİ ÇORUM*

ABSTRACT

DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) is an AI system which is created by Stephan Thaler. It is claimed that the AI named DABUS has already made two inventions; one is the "Food Container", a new type of food and beverage storage container, and the other is a "Neural Flame (Devices and Methods For Attracting Enhanced Attention)" that shines brightly in case of danger. Stephan Thaler claimed that these two inventions were invented by DABUS, as it was not created to solve any particular problem and was not trained on any special data relevant to the present inventions and argued that DABUS should take the title of inventor itself. Stephan Thaler argued that DABUS is trained with technical documents and knowledge, so it is able to generate inventions on its own, and in this context, he applied for patents on behalf of DABUS in various countries. As a result of the applications made to the USA, the United Kingdom, Germany, Australia, South Africa, the European Patent Office (EPO) and 12 more different jurisdictions, the problem of patentability of AI-generated inventions has become more visible and subject to debate. With these applications, even in some countries, DABUS had managed to be considered an inventor, although later, these decisions were subject to appeal. The main reason that Stephan Thaler made these patent applications was to show the necessity of change in the IP domain with emerging technologies; namely, he tested the system in various countries and successfully reflected the need for change regarding AI-generated inventions. In some countries, some calls for views, guidances and Public Consultations have been published on the patentability of AI inventions.

This paper will examine how and in what way DABUS cases affect the patentability of AI inventions in international law as a result of patent applications in various countries.

Keywords: Artificial Intelligence (AI), Patent Law, AI-Generated Inventions, Inventorship, Right to apply for a patent

* Swansea University, Faculty of Law, PhD Researcher – cebecinurfatma@gmail.com ORCID No: 0000-0002-2629-0320

YAPAY ZEKA BULUŞÇU OLABİLİR Mİ? "DABUS" KARARLARI IŞIĞINDA ULUSLARARASI HUKUKTA YAPAY ZEKANIN BULUŞLARININ PATENTLENMESİ

ÖZET

DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) Stephan Thaler tarafından geliştirilen bir yapay zeka sistemidir. DABUS hali hazırda iki adet buluşa imza attığı iddia edilmektedir; biri yeni tip yiyecek içeçek saklama kabı olan "Yiyecek - Fraktal Konteyner" (Food/Fractal Container) diğeri ise tehlike anında ışık saçan bir "Sinirsel Alev" (Neural Flame)dir. Stephan Thaler, bu iki buluşun DABUS tarafından icat edildiğini öne sürerek, buluşçu sıfatını DABUS'un kendisinin alması gerektiğini savunmuş ve bu kapsamda çeşitli ülkelerde DABUS adına patent başvurularında bulunmuştur. ABD, Birleşik Krallık, Almanya, Avustralya, Güney Afrika, Avrupa Patent Ofisine (EPO) ve 12 farklı ülkeye daha yapılan başvurular sonucunda, DABUS'un ve daha genel anlamda bir yapay zekanın patent sahibi olabilmesi hususu aktif bir şekilde tartışılmaya başlanmış, hatta bazı ülkelerde (Güney Afrika ve Avustralya) yapay zekanın patent sahibi olabileceği savunulmuştur. Diğer ülkelerde ise karar DABUS'un buluşlarının patentlenebileceği lehine (henüz) çıkmasa da yargılama süreci devam etmekte ve yapay zekanın buluşlarının patentlenebilirliği konusunda çeşitli yönergeler (Guidance) ve kamuoyu görüşü istekleri (Public Cunsultation- call for views) yayınlanmıştır.

Bu metinde, DABUS'un yaptığı iddia edilen buluşlara ilişkin patent başvurularının çeşitli ülkelerdeki sonuçları ve bunun etkileri neticesinde, DABUS davalarının uluslararası hukukta yapay zekanın buluşlarının patentlenebilirliğini nasıl ve ne yönde etkilediği anlatılacaktır.

Anahtar Kelimeler: Yapay Zeka, Patent Hukuku, Yapay Zekanın Ürettiği Buluşlar, Buluşcu, Patent

www.**bthukukusempozyumu**.com

BİLİŞİM VE TEKNOLOJİ HUKUKU DERNEĞİ

İSTANBUL MEDENİYET ÜNİVERSİTESİ

ISBN 978-605-72218-1-0