



BİLİŞİM HUKUKU KOMİSYONU BÜLTENİ



BU SAYIDA

- 3 **KİŞİSEL VERİLERİ KORUMA KURUMU'NUN TİKTOK UYGULAMASI HAKKINDAKİ KARARININ İNCELENMESİ**
Av. Hilal KARAKAŞ EKER
- 5 **İNGİLTERE VE GALLER YÜKSEK MAHKEMESİNDEN OASIS EMRİ: GEREKENİ YAPIN!**
Stj. Av. İrem NALBANT
- 7 **DİJİTAL DÖNÜŞÜM ÇAĞINDA SUÇLARIN YAPISININ DEĞİŞMESİ VE SİBER GÜVENLİK SORUNU**
Stj. Av. Ramazan ALTINIŞIK
- 14 **YAPAY ZEKA, DİJİTALLEŞME VE ENDÜSTRİ 4.0 ÜZERİNE**
Stj. Av. Ahmet KALKAN
- 17 **ELEKTRONİK ORTAMDAKİ İHTİLAFLARA İLİŞKİN YABANCI HAKEM KARARLARININ TENFİZİ ÜZERİNE BİR DERLEME**
Av. Oğuzhan SEYMEN
- 22 **DİJİTAL VARLIKLARIN SİGORTALANMASI**
Av. Edanur AKINCI
- 25 **NFT'LERİN FİKRİ MÜLKİYET HUKUKUNDAKİ YERİ**
Stj. Av. Elif Şuara GÜNGÖR



BÜLTENİMİZDE

Teknoloji, bizlerin takip edemeyeceği hızda gelişmekte ve hayatımızın ayrılmaz bir parçası haline gelmektedir. Her gün gelişen teknolojiye ayak uydurmak biz hukukçular için zorunlu hale gelmiştir. Yapay zeka, blockchain, fintech, NFT, fikri ve sınai mülkiyet, internet, e-ticaret, kişisel verilerin korunması gibi kavramların insan hakları, ceza hukuku, sözleşmeler hukuku gibi hukukun temel alanlarında incelemek ve bunlar hakkında bilgi sahibi olmak biz hukukçuların bakış açısını geleceğe yönlendirecektir.

Aynı zamanda bu kazanımlar ile hukukçular, bilişim dünyasında yoğun zaman geçiren milyarlarca insanın işlem güvenliğini sağlamak ve dijital anlamda da geleceğe temiz bir dünya bırakmak görevi de üstlenmektedir .

Bu düşünceler ile bizler de bilişim ve hukukun kesiştiği alanlardaki gelişmeleri takip ederek siz değerli okuyucularımıza aktarabilmek, *yeni çıkan yasal düzenlemeleri sizlerle buluşturabilmek adına Bursa Barosu Bilişim Hukuku Komisyonu olarak sizlere her ay bülten hazırlıyoruz.

Bilişim hukuku alanında meslektaşlarımızın sizler için hazırladığı makaleleri, haberleri, dizi, film ve kitap önerilerini ve daha birçok içeriği her ay bültenimizden takip edebilirsiniz.

Bültenimizin siz okuyucularımız için bilgi verici olmasını ve okurken keyifli zaman geçirmenizi temenni ediyoruz.

Saygılarımızla.

KİŞİSEL VERİLERİ KORUMA KURUMU'NUN TIKTOK UYGULAMASI HAKKINDAKİ KARARININ İNCELENMESİ

Av. Hilal KARAKAŞ EKER

Kişisel Verileri Koruma Kurumu uzun bir aradan sonra yeni bir karar yayımladı. Karar pek çok konuda adından söz ettiren TikTok platformu hakkında. Türkiye'de maalesef çok fazla çocuğun uzun saatler boyunca kullandığı bu uygulama hakkında Fransız Veri Koruma Otoritesi 5 milyon Euro, ABD 5.7 milyon Dolar para cezası vermişken, kurumun verdiği ceza 87 bin Euro civarında.



Sosyal medya platformu TikTok uygulaması ile ilgili olarak açık rızanın 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında usulüne uygun alınmadığı, kişisel verilerin elde edilmesi ve saklanması hususunda hukuka aykırılıkların bulunduğu ve yazılıma ait birçok güvenlik açığı olduğuna yönelik şikayet ve haberler üzerine Kişisel Verilerin Korunması Kurumu tarafından resen inceleme başlatılmış ve inceleme sonucunda Kurum 2023/134 numaralı kararıyla TikTok'a 1,75 milyon TL idari para cezası vermiştir. Karara göre;

TikTok'un 2021 yılı Ocak ayında Gizlilik Politikasında güncelleme gerçekleştirdiği, güncelleme neticesinde metinde 13 ve 15 yaş aralığındaki kullanıcı hesapları için varsayılan gizlilik ayarının "özel" olarak değiştirildiği bu sayede, yalnızca kullanıcının onayladığı takipçilerin paylaştığı videoların görüntülenebileceği fakat güncellemeden önce hassas yaş

grubunda bulunan kullanıcıların profillerinin varsayılan olarak herkese açık olmasının, hesaplarla etkileşimde sınırlandırma bulunmaması ve küçüklerin verilerine erişilmesi kapsamında risk teşkil ettiği ve bu risklerin azaltılması için yeterli tedbirin alınmadığı,

Güncelleme öncesinde 13 yaş altı kullanıcıların görüntülediği ve uygun ebeveyn izni olmadan çocuklar hakkında veri toplandığı TikTok'un gizlilik sözleşmesinde veri işlemeye ilişkin KVKK'nın 5. maddesinde yer alan işleme şartlarının belirtildiği fakat hangi kişisel verilerin hangi amaçla ve hangi işleme şartına dayanılarak işlendiği konusunda net bir bilgi verilmediği,

Kullanıcılara, hesap oluşturmaya devam etmeleri halinde TikTok'un hizmet koşullarını ve gizlilik politikasını kabul etmiş sayılacaklarının belirtildiği fakat hizmet koşullarının henüz Türkçe tercümesinin bulunmaması sebebiyle kullanıcıların hizmet koşullarını tam olarak anlayamadan onaylarının alınmasının ihtimal dahilinde olduğu,

TikTok'un hesap oluşturulurken ya da hesap oluşturulup aktif olarak kullanılırken açık rıza alınmasına yönelik bir eyleminin olmadığı, Gizlilik Politikasının açık rıza metni yerine de kullanıldığı,

Ayrıca platformun profillemeye amacıyla çerezler kullandığı ve bu şekilde gerçekleştirilen veri işleme faaliyetine ilişkin kullanıcılardan açık rıza alınmadığı,

Veri sorumlusu tarafından, profillemeye amacıyla çerezler kullanılarak gerçekleştirilen kişisel veri işleme faaliyetine ilişkin olarak ilgili kişilerden açık rıza alınmadığı, bu

kapsamda yürütülen kişisel veri işleme faaliyetinin de hukuka uygun olmadığı tespit edilmiştir.

Bu tespitler sonucunda Kurum tarafından TikTok'a 1.75 milyon TL idari para cezası verilmiş ve ayrıca;

-Hizmet Koşullarının bir ay içerisinde Türkçeye çevrilmesi,

-Gizlilik Politikası metnlerinin üç ay içerisinde Kanuna uygun hale getirilmesi,

-Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine uygun bir aydınlatma yapılması konusunda talimat verilmiştir.

Karar pek çok açıdan önem arz ediyor. Öncelikle 13 yaş altı çocukların kişisel verilerini işleyen veri sorumluları açısından önemli. Küçüklerin verilerinin işlenmesi halinde risk değerlendirmesi yapılması, mevzuata uygun aydınlatma ve açık rıza uygulamaları olmaksızın veri işlemekten kaçınılması ve uygun ebeveyn onayı alınmadan küçüklerin verilerinin işlenmemesi gerektiğinin bir kez daha altı çizilmiştir. Her ne kadar Avrupa Veri Koruma Tüzüğü'nde reşit olmayan kişiler hakkında düzenleme yapılmışsa da (yeterli olup olmadığı tartışmalıdır) KVKK'da reşit olmayanların ve 13 yaş altındaki küçüklerin kişisel verilerinin işlenmesi durumunda ne yapılması gerektiğine ilişkin bir düzenleme bulunmamaktadır. Kanaatimce bu karar vasıtasıyla küçüklerin verilerinin işlenmesi noktasında daha açıklayıcı ve düzenleyici değerlendirmeler yapılarak bu konuya bir nebze olsun açıklık getirilebilirdi. Kararda "13 yaşın altındaki küçüklerin kişisel verilerinin,

uygun "ebeveyn onayı" alınmaksızın toplanması/işlenmesi riskli hale gelmiştir." denilmişse de en azından ebeveyn izninin nasıl alınması gerektiğine ilişkin yöntem açıklanmalıydı. Ebeveyn izni konusundaki eksikliğin tamamlanması konusunda platformun talimatlandırılmadığı da dikkat çekicidir.

Bir diğer önemli nokta yüksek profillemeye çözümlerinin kullanılması. Profil çıkarmak amacıyla çerez kullanan veri sorumlularının ilgili kişilerden açık rıza almaları gerekmektedir.

Türkiye'deki ilgili kişilere veri işleme faaliyetine ilişkin yapılacak bilgilendirmenin, aydınlatma metni, hizmet koşulları ve veri politikaları gibi metinlerin Türkçe olarak sunulması gerekmektedir.

Kurum'un daha önceki kararlarında da belirttiği ve bu kararda da karşımıza çıkan, açık rıza şartına dayalı olarak gerçekleştirilen kişisel veri işleme faaliyetleri bakımından, ilgili kişilere aydınlatma metninden ayrı olarak açık rıza metni sunulmalıdır.

Aydınlatma Metninde Kanun'un 5'inci maddesinde yer alan işleme şartlarının tümünün yer alması gerektiği ve ayrıca Kanun'un 4'üncü maddesinde yer alan "belirli, açık ve meşru amaçlar için işleme" ve "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkeleri gereğince hangi kişisel verilerin hangi amaçla ve hangi işleme şartına dayanılarak işlendiği hakkında net bilgi verilmesi gerekmektedir.

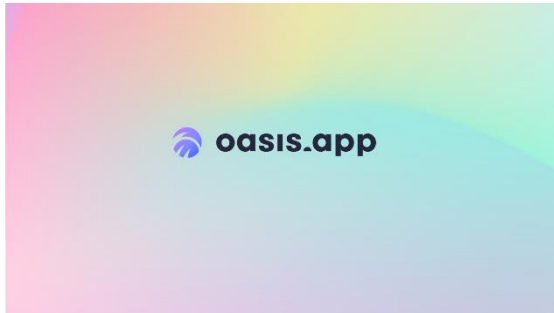
İNGİLTERE VE GALLER YÜKSEK MAHKEMESİNDEN OASIS EMRİ: GEREKENİ YAPINI!

Stj.Av. İrem NALBANT

İngiliz mahkemelerinin kripto varlıklar, merkeziyetsiz finans uygulamaları ve dağıtık defter teknolojisinin diğer ürünleri nedeniyle oluşan hukuki ihtilaflar hakkında verdiği kararlara bir venisi eklendi: OASIS emri.

2 Şubat 2022'de Ethereum ve Solana blok zincirlerini birbirine bağlayan, OASIS'e ait köprü protokolüne yapılan saldırı sonucu 320 milyon doların üzerinde ETH çalınmıştı.

Vurguncular, akıllı sözleşme niteliğinde olan köprü'nün yükseltilebilmesini (akıllı sözleşmenin değiştirilebilmesini) sağlayan yetki sistemindeki açıktan faydalanarak yetkiyi ele almış ve köprüde işlem gören yüklü miktarda ETH'yi çalmışlardı. Wormhole vurgunu olarak anılan bu hırsızlık olayı, kripto paraların ve merkeziyetsiz finans işlemlerinin güvenilirliğini tekrar gündeme getirmişti.



Bilindiği üzere köprü protokolleri (wormholes) birbiri arasında iletişim olmayan iki blok zincirin bir akıllı sözleşme vasıtasıyla iletişim kurabilmesini sağlıyor. Arasında köprü bulunmayan iki blok zincirin birinden diğerine gönderilen kripto varlıklar kayboluyor ve tekrar bulunmaları pek de mümkün değil.

OASIS tarafından yapılan açıklamaya göre; söz konusu vurgundan bir yıl sonra, bir grup "white hat" (etik hacker) tarafından OASIS sistemindeki bir açık nedeniyle köprüdeki akıllı sözleşmenin ters döndürülebileceği, yani ters-hortumlama yapılabileceği keşfedilmiş, bu bilgi OASIS ile paylaşılmıştı. Ardından, İngiltere ve

Galler Yüksek Mahkemesi'nden bir emir geldi: "Wormhole Exploit (Wormhole Vurgunu) ile ilişkili olan cüzdan adresiyle ilgili belirli varlıkların geri alınmasına yol açacak tüm gerekli adımları atın."¹

Gereken adım, etik hacker'ların bulmuş olduğu açığın değerlendirilmesi ve akıllı sözleşmenin geri çevrilmesiydi. İlk bakışta mağdurların yararına gibi görünen bu durum, merkeziyetsiz finans ve akıllı sözleşmeler bazında çok da iç açıcı değil. Zira blok zincir teknolojisi ve dolayısıyla akıllı sözleşmelerin en temel ve önemli vaatlerinden biri değiştirilemez olmaları.

OASIS, emri paylaştığı blog yazısının devamında hemen ekliyor: "Akıllı sözleşmelerimiz tekrar değiştirilemez ve bağışık hale getirildi. OASIS Otomasyonu ile ilişkili olan sözleşmelerin herhangi birinin yükseltilmesine izin verme özelliğini kaldırdık. Bu, yetkili adresi OASIS Multisig yerine 0x0 olarak ayarlayarak yapıldı."

Bu açıklama gösteriyor ki, OASIS hem vurgunun hem de karşı-vurgunun sebebi olan, çoklu imza (multisig) ile akıllı sözleşmelere müdahale edebilme yetkisini, "hiçbir yer" olarak metinleştirebileceğimiz "0x0" adresine tanımladı. Yani yetki merkezi diye bir adres mevcut değil. Artık OASIS akıllı sözleşmelerinin yükseltilmesi, güvenlik nedenleriyle dahi olsa değiştirilebilmesi mümkün değil.

¹<https://blog.OASIS.app/statement-regarding-the-transactions-from-the-OASIS-multisig-on-21st-feb-2023/>

Blok zincir teknolojisi anlatılırken değinilen değiştirilemezlik özelliğine tanınan yazılımsal istisnalarının ne türlü sorunlara yol açabildiğine dair pahalı bir örnek olan OASIS Wormhole vurgununu kısaca açıklamaya çalıştık. Ancak belli ki İngiliz Mahkemeleri bu konuyu kestirip atmayı düşünmüyor. Dağıtık defter teknolojisi ürünlerinin sebep olduğu ihtilaflarla ilgili, İngiltere'de halen temyiz kararını bekleyen dosyalar mevcut.



İngiliz Temyiz Mahkemesi'nin verdiği kararlara incelendiğinde, blok zincir teknolojisiyle ilgili açılan davalarda zincirin kontrol mekanizmasının nasıl ayarlandığına göre davalı/sanık olabilecek kişiler de değişiyor. Blok zincir teknolojisini bir hizmet olarak sunan yazılım şirketleri ile düğüm ve kodları depolayan bulut bilişim şirketleri de bu bağlamda sorumluluk grubunda. Bu yüzden yeni bir blok zincir projesine başlayan veya halihazırda bir blok zincirde yetki veya sorumluluk sahibi olanların merkeziyetsizlik yapılarını iyi kurdukları konusunda emin olmaları, zincire müdahale edebilme yetkisinin kapsamını iyi belirlemeleri onların yararına olacak.

Mahkeme nezdinde ayrıca, yazılım hatalarından kaynaklanan hak kayıpları ya da yazılım sahiplerinin veya yöneticilerinin çıkarları için ve kullanıcı aleyhine kod değiştirime işlemleri nedeniyle hukuki yükümlülüklerin ihlal edildiği de ileri sürülebilecek.

Bu yazımızda bir örneğini anlatmaya çalıştığımız hacker saldırıları, hırsız borsalar, ponzi şirketleri ve dahası... Blok zincir teknolojisi, akıllı sözleşmeler, kripto paralar ve bu teknolojilerin doğurduğu diğer tüm merkeziyetsiz yapılar, hukuki düzenlemelere muhtaç olacak kadar hayatımıza yerleşmiş durumda. Sorumluluk ve hakların belirlenmesi konusundaki yasal düzenleme ve içtihatların, teknolojinin güvenli hale getirilmesine ve entegrasyonu sağlayacağına, kullanıcıların sisteme dahil olma eğilimini ve teknolojinin tercih edilme oranını artıracığına şüphemiz yok.

KAYNAKÇA

1. <https://blog.OASIS.app/statement-regarding-the-transactions-from-the-OASIS-multisig-on-21st-feb-2023/>
2. <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/02/code-is-law.pdf>

İÇİNDEKİLER

- 1- DİJİTAL DÖNÜŞÜM NEDİR ?
- 2- DİJİTAL DÖNÜŞÜM ÇAĞINDA SUÇLAR ?
- 2.1. SİBER SUÇLARIN ÖZELLİKLERİ VE GERÇEK HAYATTAN ÖRNEKLER
- 2.2. SİBER TERÖR
- 2.3. HACKTİVİSM
- 2.4. SUÇLARIN TEKİLLİĞİ VE YIKICILIĞI
- 2.5. SİBER SAPKINLIK

ÖZET

Dijital dönüşüm, tüm dünyayı etkisi altına alan COVID-19 Pandemisi ile birlikte son dönemde adından sıklıkla söz ettiren bir kavram oldu. Tarihte ilk ortaya çıktığı zaman dilimi 1970'li yılları bulmasına karşın geride bıraktığımız son 10 yılda internet dünyasında yaşanan gelişmelerin hızı ve pandemi ortaya çıkarttığı şartlar nedeniyle dijital dönüşüm, insan yaşamının her yönünü kökten değişikliğe uğrattırıyor. Yine dijital dönüşüm sadece bireylerin hayatını değiştirmekle kalmıyor artık bireylerin toplumla ve devletle olan etkileşimini de kökten değişikliğe uğrattırıyor. Şirketler ve kurumlar kendileri açısından önemli olan ticari ve teknik bilgileri artık internet, hosting gibi siber ortamlarda saklıyorlar ve müşterileriyle fiziksel dünyada etkileşim kurma yerine; sosyal medya, web siteleri ve mobil uygulamalar gibi dijital dünyayı tercih ediyorlar. Kısacası bireylerin, şirketlerin, kurumların ve devletlerin yaşam ve faaliyetleri artık siber dünya üzerine kuruluyor. Bu durumun ortaya çıkarttığı en kritik konuların başında da suçların artık siber dünyada işlenmesi ve bu suçlarla mücadele sorunudur. Bu yazımızda sizlere güncel gelişmelerle birlikte siber dünyada yaşanan suçları ve artan güvenlik sorunlarını olabildiğince tüm hatlarıyla değineceğiz.

DİJİTAL DÖNÜŞÜM NEDİR ?

Teknoloji ve internet dünyasında yaşanan gelişmeler artık yaşamımızı etkilemekle kalmayıp yaşamımızı kökünden değiştiriyor. Artık sadece devletlerin ve büyük şirketlerin değil bizlerin de; takip ettiğimiz farklı farklı sosyal medya kanalları ve web siteleri, kullandığımız mobil uygulamalar sayesinde internet dünyasında birer yaşam alanları var. Şirketler ve ticari işletmeler hem kendi çalışanları arasındaki faaliyetlerini yürütürken hem de müşterileriyle iletişime geçerken fiziksel dünyayı kullanmak yerine dijital dünyayı kullanıyorlar. Yine devletler; gerek kamu hizmetlerini yürütürken gerekse de vatandaşlarla etkileşime girerken sosyal medya kanallarını kullanıyorlar. Yine bizler de hem iş hayatımızda hem de özel hayatımızda ihtiyacımız olan neredeyse her şeyi internetten ve mobil uygulamalardan kolaylıkla bulabiliyoruz. Kısacası şirketler ve kurumlar faaliyetlerini yürütürken, devletler kamu hizmetlerini ifa ederken ve bireyler de günlük yaşamlarında ihtiyaçlarını giderirken tüm süreç dijital ortamda gerçekleşiyor.



Covid 19- Pandemisinin ortaya çıkardığı şartlardan dolayı dijital dönüşüm insan hayatına daha hızlı etki etmesine karşın aslında başlangıcı 1970'li yıllarda ki teknolojik gelişmelere kadar uzanıyor. 1970'li yıllardan sonra bilgisayar üretim maliyetlerinin düşmesiyle birlikte artık bilgisayarlar

yavaş yavaş herkes tarafından erişilebilen bir cihaz oluyor. 1989 yılında Tim Berners Lee tarafından internetin keşfiyle birlikte insanlık tarihinde dijital dönüşümün en kritik gelişmelerinden birisi yaşanıyor. İnternetin keşfi ve gelişimiyle birlikte artık dijital dünyadaki tüm veriler fiziksel sınırların önemi olmaksızın birbirleriyle etkileşime girebiliyor.

Yine 95 ve 2000'li yılların sonrasında internet dünyasında ki gelişmeler çok hızlı bir şekilde artıyor ve Google, Microsoft, Facebook gibi internet dünyasının en köklü gelişmeleri yaşanıyor.

Bugün artık web siteleri, uygulamalar, sosyal medya kanalları yaşamımızın her yerindedir. Dijital dönüşüm artık yaşamımızın bir parçası olmasının ötesinde yaşamımızı şekillendiren bir yapı halindedir.

DİJİTAL DÖNÜŞÜM ÇAĞINDA SUÇLAR

Dijital Dönüşüm, günlük hayattaki her şeyi yeniden şekillendirdiği gibi yaşamın bir gerçeği olan suçları da değiştiriyor. Yani günümüz dünyasında suçlar artık fiziksel dünyadan Siber dünyaya taşınıyor. Siber dünya da işlenen bu suçlara kısaca "Siber Suçlar" adını veriyoruz.

1.1. SİBER SUÇLARIN ÖZELLİKLERİ VE GERÇEK HAYATTAN ÖRNEKLER

Siber dünyada işlenen suçların en önemli özelliklerinden birisi bu suçların kamu düzeni üzerinde olan yıkıcılığıdır. Yukarıda da ifade ettiğimiz gibi artık bütün sektörlerdeki şirketler faaliyetlerini dijital ortamlarda yürütüyorlar ve devletler de vatandaşlarına hizmet sağlarken dijital ağ altyapılarını kullanıyorlar. Dolayısıyla bugün gerek kamu makamları gerekse şirketler

tarafından bizlere sağlanan tüm hizmetlerle alakalı veriler ve bilgiler siber sistemlerde depolanıyor. Bu sistemlere yapılan siber saldırılar; tedarik zincirinden, müşteri ilişkilerine kadar üretim zincirini alt üst edebilir ve yine sadece şirketlere değil hizmeti alan insanlar üzerinde de yıkıcı etkileri olabilir. Yine burada ulaşım, sağlık gibi kritik sektörlerin üzerinde durulmasında fayda vardır. Konu hakkında yaşanmış olaylardan örnekler verecek olursak:

2008 yılında Polonya'nın Lodz kentindeki bir Tramvay, rayların kesiştiği noktada makinistin tüm çabalarına rağmen sola dönmek yerine sağa döndü ve iki tramvay kafa kafaya çarpıştı. Kaza sonucunda ölen bir kimse olmamasına karşılık maddi hasarın boyutu büyüktü. Olay her ne kadar sinyalizasyon hatası olarak görüldüyse de daha sonra kazanın, 14 yaşındaki bilgisayar meraklısı bir çocuk tarafından kazanın gerçekleştiği ulaşım hatlarını uzaktan yönetebilecek bir kızılotesi vericinin yerleştirilmesi sonucu gerçekleştiği ortaya çıktı.

Yine pandemi döneminde ABD'de yaşanan Solarwind saldırısı da örnek verilebilir. Tedarik zinciri saldırısı olarak bilinen bu siber saldırı da Solarwind güvenlik şirketinin geliştirmiş olduğu bir yazılımın güncel versiyonuna kötü amaçlı kodların yerleştirilmesi sonucun yazılımın güncel versiyonunu kullanan binlerce teknoloji şirketinin veri güvenliği ihlal edildi. Bu saldırıdan; başta Microsoft olmak üzere birçok Fortune 500 şirketi ve ABD Ticaret Bakanlığı gibi kamu kuruluşları zarar gördü.

1.2. SİBER TERÖR

Siber Suçlar Başlığı altında değinilmesi gereken bir diğer önemli konu da terör faaliyetlerinin siber boyuta taşınmasıdır.

Terör, latince "terrere" sözcüğünden türemiş olup "korkutma" anlamını taşımaktadır. Terör faaliyetlerinin nihai amacı bireyleri ve toplumu korkutmaktır. Adı suçların aksine terör suçlarında failer gerçekleştirdikleri eylemlerin tüm toplum tarafından bilinmesini isterler.

Hangi eylemlerin terör eylemi teşkil ettiği konusu devletler arasında farklılık gösterse de esasında; içinde bulunduğu toplumun üyelerini hedef alan, devlet otoritesine karşı girilen faaliyetler tüm dünyada ortak olarak terör faaliyeti olarak değerlendirilmektedir. Terör faaliyetleri sonucunda kamu barışı bozulur, toplumun devlet otoritesine karşı güveni sarsılır, tüm toplum maddi ve manevi olarak zarar görür.



Terörizm öğretide şu şekilde tanımlanmaktadır : "Hedef aldıkları toplumun istedikleri doğrultuda inanmasını sağlamak isteyen grupların başvurdukları politik güdülü ve gizli organize edilmiş şiddet kullanma durumudur". Terör örgütleri devlet egemenliğinin sorgu altında olduğu, toplumsal dayanışmanın güçlü olmadığı, vatandaşların temel hak ve yaşam standartlarına erişemediği koşulları lehlerine kullanmayı stratejilerinin bir parçası haline getirebilmektedirler. Bu bağlamda terörizm genel bir tanımla siyasi bir

amaca ulaşmak isteyen örgütsel bir yapının yasa dışı şiddet kullanarak uyguladığı bir strateji olarak ifade edilebilmektedir.

Peki terör faaliyetleri artık sadece geleneksel yöntemler olan silahlarla mı işleniyor. Diğer bir deyişle, terör örgütleri eylemlerini gerçekleştirirken dijital dünyanın getirdiği imkanlardan yararlanmıyor mu ?

Maalesef dijital dünyadaki gelişmeler bizlerin yaşantılarını kolaylaştırdığı gibi terör örgütlerinin de faaliyetlerini kolaylaştırıyor. Artık terör örgütleri eylemlerini gerçekleştirirken sadece silahları değil; internet, sosyal medya kanalları gibi dijital dünyanın getirdiği imkanları da kullanıyor. Sivil toplum kuruluşlarının, şirketlerin, aktivistlerin faaliyetlerinde artık siber dünyayı yaygın olarak kullanırken terör örgütlerinin bu duruma sessiz kalması ve dijital dünyanın getirdiği fırsatları değerlendirmemesi mümkün değildir.

Anonimliği, reddedilebilirliği ve maliyetinin düşüklüğü siber saldırıları çekici bir tercih sebebi yapmaktadır

Konu hakkında örnek verecek olursak: 2008 yılında Hindistan'ın Bombay şehrinde El- kaide terör örgütünün bir uzantısı niteliğinde olan ve merkez üssü Pakistan olan Leşker-i Tayyibe adlı terör örgütü çok kanlı bir eylem gerçekleştirdi.

Eylemin sonunda bombay şehrinde 166 kişi öldü. Saldırganlar Pakistan'dan yola çıkarak Bombay şehrine gelmiş ve bir otel odasına saklanmışlardı. Saldırganlar daha sonrasında oteldeki rehlin alarak otel çevresindeki kafelere, marketlere ağır vasıtalı silahlarla saldırmışlardı. Saldırının gerçekleştiği sırada örgütün merkez üssü saldırı hakkında tüm haber

sitelerini takip etmekteydi. BBC, CNN, Times of India gibi haber kanalları saldırının gerçekleştiği anda polislerin olay yerine nasıl geldiğini canlı olarak yayınlamıştı. Bunu öğrenen Pakistan'daki merkez üssü anlık olarak faille bilgi vermekteydi dolayısıyla saldırganlar daha polisler olay yerine gelmeden hazırlanıyorlardı. Yine olayın gerçekleştiği sırada Twitter gibi sosyal medya platformlarına olayla ilgili gönderilen videolar ve resimler sayesinde failer polislerin nereden geleceğini öncesinden öğrenmiş, dolayısıyla failerin etkisiz hale getirilmesi uzun saatler sürmüştü. Yani Bombay'da gerçekleşen bu eylemde saldırganlar bir elleriyle silah kullanırken diğer elleriyle telefonlarında saldırıyla alakalı haber ve içerikleri takip etmekteydi.

Siber alanın teröristler tarafından nasıl kullanıldığı üzerinde değinilmesinde de yarar vardır. Siber alan, terörist gruplar tarafından iki farklı şekilde kullanılır. Bunlardan ilki, örgütün finansman ihtiyacını karşılanması amacıyla çeşitli faaliyetlerin yürütülmesi ve terör eylemlerinin gerçekleştirilmesidir.

Siber terörizmi, terörizmden ayıran nokta saldırıların doğrudan fiziksel bir şiddet içermemesi ve saldırılar için siber alanı oluşturan altyapının kullanılmasıdır. Terör örgütleri tarafından mevcut sistemler üzerinden veya özel olarak üretilen yazılım, donanım, programlarla saldırılar gerçekleştirilmektedir. Siber dünyada işlenen hırsızlık, sabotaj, özel alana sızma, sahtecilik, casusluk, hizmet engelleme saldırısı, dolandırıcılık, kötü amaçlı yazılım yayma, zorbalık gibi tüm suçları terör örgütleri de gerçekleştirebilmekte ve bu mecra üzerinden bir korku iklimi oluşmaktadır.

Kısacası artık Terör örgütleri siber alanları, tıpkı bireyler ve şirketler gibi, faaliyetlerinde sıklıkla kullanmaktadır ve bu durum terör eylemlerini daha önceden hiç olmadığı kadar yıkıcı boyutlara taşımakta ve terörle mücadeleyi zorlaştırmaktadır.

1.3. HACKTİVİZM

Siber güvenlik başlığı altında değinilmesi gereken bir diğer konu da adına hacktivistler denilen siber dünyadaki aktivist gruplardır. Bunların en başında, devletlere yaptıkları siber saldırılarla bilinen Anonymous adlı hacktivist gruptur. "İyilik için Hack" mottosuyla hareket eden Anonymous grubu dünyadaki haksızlıklara karşı siber saldırılarıyla tanınıyor. Öyle ki, 2011 yılında Arap Baharının yaşandığı dönemde Anonymous grubu internet üzerinden muhaliflere verdiği destekle bilindi. Yine internette yayınlanan çocuk istismarı videolarına tepki olarak bu grup, videolara erişimi engelledi ve çocuk istismarcılarının kimliklerini yayınladı. Grubu ister destekleyin isterse desteklemeyin Anonymous grubunun internet dünyası üzerindeki etkisi büyüktür . Öyle ki Amerikan Ulusal Güvenlik Ajansı yayınladığı bildiri de Anonymous adlı grubun saldırılarını önlemek amacıyla karşı hizmet saldırılarında bulunduğunu yayınladı. Bu bildiri hacktivist grupların gücünün boyutunu ortaya koyuyor.

1.4. SUÇLARIN TEKİLLİĞİ VE YIKICILIĞI

Siber dünyada yaşanan gelişmeler artık başta hırsızlık olmak üzere birçok ekonomik suçların işleniş şekillerini de değiştirdi. Öncesinde hırsızlık suçundan zarar gören insan sayısı fazla değilken artık siber saldırılar yüzünden binlerce insanın ticari verileri çalınabiliyor. Yine yukarıda da belirttiğimiz üzere artık hepimiz finansal varlıklarımızı dijital

alandanda tutuyoruz ve şirketler de ticari ve teknik (know-how) bilgilerini elektronik ortamlarda saklıyor. Varlıklarımızı saklama konusunda güven kuruluşları olan bankaların sunmuş olduğu internet bankacılığı hizmetlerinden yararlanarak artık tüm finansal işlemlerimiz, şubeye veya gitmeden elektronik ortamlarda veya internet üzerinden gerçekleştirilebilir.

Dijital dünyanın sunmuş olduğu bu kolaylıklar sayesinde, yaşamımız daha kolay hale gelmesine karşın artık tüm finansal verilerimiz, elektronik ortama taşındığından dolayı bizim kontrolümüz dışında siber risklerle karşı karşıyadır. Son yıllarda banka hesaplarının internet üzerinden soyulmasına yönelik kötü amaçlı birçok yazılım geliştirildi. Bu yazılımlar sayesinde birçok banka hesabı, mağdurların daha haberi yokken soyulmaktadır. Üstelik son yıllarda geliştirilen yazılımlar, bu suçların açığa çıkmaması için banka hesabından çekilen tutar kadar veriyi hesapta göstermektedir ve yapılan işlemleri hesap ekstrelerine yansıtmamaktadır. Yani öyle ki, mağdurlar banka hesaplarını kontrol ettiklerinde her ne kadar hesaplarındaki tutarı görmelerine karşılık, bu rakamlar gerçeği göstermiyor olabilir.

Bu suçların işlenmesinde geliştirilen algoritmalar sayesinde, banka hesabınızdan 2.500 TL çalınmasına karşılık çalınan tutar kadar veri, siz daha hesabınızı kontrol etmeden ekrana yansıtılıyor. Yine bu algoritma, hırsızların banka hesabınızdan yaptığı işlemleri hesap ekstrelerinden anlık olarak siliyor ve böylece hesabınızdan herhangi bir para çıkışı olmamış gibi gösteriliyor. Banka hesabınızın soyulduğunu ancak banka kartınızı kullanmak veya ödeme yapmak

istediğinizde limiti aşmış olduğunuz ya da hesap bakiyenizin yetersiz olduğu uyarısıyla karşılaşmanız halinde öğrenebiliyorsunuz.

Siber dünyada finansal amaçla yapılan saldırıların en önemli özelliği bu saldırıların yarattığı yıkımın çok yüksek boyutlara varabilmesidir. Geleneksel hırsızlık, dolandırıcılık gibi suçların aksine siber dünyada işlenen suçlar fiziksel sınırların ötesinde olduğundan dolayı aynı anda milyonlarca kimseyi bulabiliyor.



Bu duruma örnek olarak 2013 yılında Amerika Birleşik Devletlerinde perakendecilik sektöründe faaliyet gösteren Target şirketine karşı gerçekleştirilen siber saldırı örnek gösterilebilir. ABD'nin genelinde mağazaları bulunan Target şirketinin pos cihazlarına ve banka kartı terminallerine yapılan saldırı sonucunda 110 milyon kişinin banka kartı bilgileri çalındı. Yani Amerika Nüfusunun 1/3'ü saniyeler içerisinde soyuldu. Saldırının arkasında ise 17 yaşında Rus bir hacker olduğu ortaya çıktı. Bu örnek bizlere siber alandaki hırsızlık suçlarının ne kadar yıkıcı olduğu konusunda çok iyi bir örnek olabilir

1.5. SİBER SAPKINLIK

Siber suçlar başlığı altında değinilmesi gereken konulardan bir tanesi de siber dünyada işlenen cinsel suçlardır. Bilindiği üzere internet ortamında bireyler merak ettikleri herhangi bir

konuyla alakalı tüm bilgi ve içeriklere diledikleri gibi erişebiliyorlar. Yine bizler de sosyal medya sayesinde duygu ve düşüncelerimizi ifade edebiliyor, kendimizi yakın hissettiğimiz kitlelerle etkileşime geçebiliyoruz. Yine internet sayesinde artık; iklim sorunları, toplumsal eşitsizlik gibi toplumsal konularda kampanyalar oluşturabiliyoruz. Ancak resmin, karanlık ve hiç de bilmek istemediğimiz bir yüzü vardır.

İnternet ortamı aynı zamanda sapkın ve patolojik eğilimleri olan; pedofililer, mazoşistler, gibi kişi ve gruplarında sıklıkla kullandığı bir mecra olmuştur. Bugün, internetin karanlık yüzü olarak da bilinen "Dark-Web" ortamında; kartellerin infaz videoları, sapkın düşünceleri olan grupların ritüelleri ve çocuk pornografisi gibi içerikler paylaşılmaktadır. Bu içerikler tıpkı bizlerin sosyal medyada takip ettiğimiz ve paylaştığımız içerikler gibi sapkın eğilimleri olan insanlar tarafından beğenilmekte ve takip edilmektedir. Bizler isteyelim ya da istemeyelim internetin bir de böyle bir karanlık yüzü bulunmaktadır. Dünyanın dört bir yanında sapkın fikirleri olan insanlar artık internet sayesinde topluluklar oluşturabiliyorlar.

Yukarıda da dijital dönüşüm kavramını açıkladığım üzere, dijital dönüşüm yaşamımızın her alanını etkilediği gibi bizlerin; eğlence, sosyal ilişki kurma tercihlerini de değiştirdi. Artık bireyler fiziksel etkileşim yerine dijital yaşam alanlarını tercih ediyorlar. Bu durum toplum hayatına olumlu yönde etki yaptığı gibi bazen medyaya da yansıyan ve kamu vicdanını sarsan olayların da yaşanmasına sebebiyet verebiliyor. İnternet dünyasını bilinçsiz kullanan mağdurlar, çocuk tacizcileri

gibi sapkın fikirli kimselerin kurbanı olabiliyorlar.

Konu hakkında dünyadan bir örnek vermek gerekirse; 2012 yılında Kanada'da Amanda Todd isimli bir genç kız, kullanımı o yıllarda oldukça yaygın bir site olan Blog TV'de kendisini genç bir erkek olarak tanıtan failin, kamera karşısında göğüslerini gösterme teklifini kabul etti .

Günler sonra, Facebook'ta Amanda adında sahte bir hesap açıldı ve hesabın profil fotoğrafı olarak failin Blog Tv'de çektiği görüntüler eklenmişti. Açılan bu sahte hesap, mağdur Amanda'nın tüm ailesine ve Okulun resmi hesaplarına link olarak gönderildi. Durum zavallı genç kız açısından oldukça kötü bir hal alıyordu, okulda ve arkadaş ortamında yayınlanan fotoğrafları yüzünden sürekli aşağılamalara ve zorbalıklara maruz kalıyordu. Bir gün okul çıkışında bir grup genç kız tarafından tartaklandığı sırada videosu çekilmiş ve internette paylaşılmıştı. Bu durum Amanda açısından dayanılmaz bir hal aldı ve genç kız 2012 yılında intihar etti. Kanada makamları olay sonrası yaptıkları soruşturma sonucunda failin 45 yaşında, Hollanda'da yaşayan bir çocuk tacizcisi olduğu ortaya çıktı. Yaşanan bu olay Kanada gündemine skandal olarak yansıdı.

İnternet ortamında pedofililer, çocuklarla iletişim kurarken genç arkadaş kimliğine bürünüyor, mağdurların güvenini kazanarak onları sanal ortamda cinsel davranışlar sergilemesine zorlayabiliyor. Amanda Todd davası sonucunda failin tek kurbanının Kanadalı genç kız olmadığı, ağındaki kurbanların birçoğunun dünyanın farklı bölgelerinde yaşayan çocuklar olduğu polisler tarafından

tespit edildi. Kısacası tıpkı diğer suçlar gibi cinsel suçlarda, siber dünyanın getirdiği kolaylıklar sayesinde daha kolay işlenebiliyor ve bu suçların faillerinin tespiti zorlaşıyor.

SONUÇ

Bu yazımızda sizlere dijital dönüşümü, ortaya çıkışına kaynaklık eden teknolojik gelişmeler ve gelişim süreciyle açıkladık. Yine dijital dönüşümün; bireylerin yaşamını, şirketlerin ve devletlerin faaliyetlerini ne ölçüde değiştirdiğine değindik. Bu sürecin her şeyi değiştirdiği gibi insanlık tarihinin bir gerçeği olan suçların, terör eylemlerinin de yapısını değiştirdiğine değindik. Bu durumu "siber güvenlik" kavramıyla açıkladık. Siber güvenlik, içinde bulunduğumuz günümüz dünyasında artık sadece devletler arası sorun olmaktan çıkıp biz bireylerinde günlük yaşamına etki eden bir kavram olmuştur. Siber dünyanın getirdiği kolaylıklar sayesinde; banka ve kredi kartı hırsızlığı, internet dolandırıcılığı, cinsel taciz gibi suçlar artık dünyanın dört bir yanından işlenebilmektedir ve bu suçların failleri kullandıkları çeşitli kötü amaçlı yazılımlar veya manipülatif yöntemler sayesinde kendilerini kolayca gizleyebilmektedir. Tabiki de siber güvenlik denilince; sosyal medyada manipülasyon, deepfake gibi diğer kavramlara da değinilmesi gerekir ancak bu yazı, konuya olabildiğince teknik yaklaşımdan uzak, sadece günümüz dünyasında var olan siber güvenlik sorunu hakkında farkındalık oluşturacak bir tarzda hazırlanmıştır. Faydalı olması dileğiyle..

KAYNAKÇA

- <https://kron.com.tr/tedarik-zinciri-saldirisi-nedir> Drake, C. J. M. (1998). Terrorist's Target Selection, New York: St. Martin's Press

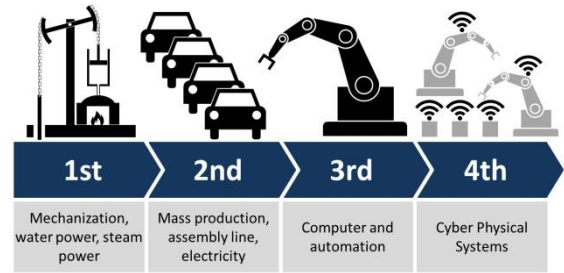
- Siber Terörizm, Potansiyelin Gerçekçi Tehdidi, Emre Çırak, Turkuaz Uluslararası Sosyo-Ekonomik Stratejik Araştırmalar Dergisi
- Şeker, E. (2017). Siber Savunma Tatbikatları: Planlama, Uygulama Ve Değerlendirme, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,
- Shiryayev, Y. (2012). Cyberterrorism in the Context of Contemporary International Law, San Diego International Law Journal, 14: 139, 139-192
- Singh, A. ve Siddiqui, A. T. (2011). New Face of Terror: Cyber Threats, Emails Containing Viruses, Asian Journal of Technology&Management Research,

Yapay zeka dediğimiz kavram, gelişim, ilerleme bunu ne diye tanımlarsak tanımlayalım insanlık tarihi açısından bir kırılma noktası. Aslında bu kırılma bir paradigma kırılması. Yani insana ihtiyaç duyan bir dünya, insan tarafından şekillendirilen bir dünya. Fakat özellikle beş altı senelik süre içerisinde meydana gelen gelişim bize şunu gösterdi: Artık dünya sadece insanlar adına bir dünya değil ve insan tarafından yönetilen bir dünya değil.

Bu noktada şunu söyleyebiliriz: Yönlendirme, değişim, dönüşüm kavramları noktasında ciddi bir paradigma kırılması mevcut. Birincil aktör olan insan, kendisi yerine kendi elleriyle ve kendisi için belki de kendi sonunu getirecek olan yeni bir dünya ve bu dünyanın yeni aktörünü tasarladı ve tanımladı. Bizler işte bu tanıma yapay zeka diyoruz. İngiliz Literatüründe AI yani "Artificial Intelligence"..

Yapay zeka dediğimiz kavram, günümüz insanını her yönüyle etkiliyor. Özellikle tıptan mühendisliğe, sosyolojiden psikolojiye tüm sahaları doğrudan ve yakından ilgilendiriyor. Hatta şöyle bir kavram var : **"Geleceğin İşsizlik Kaynağı"**...Aslında işsizlik kaynağı demek doğru değil, aslolan monoton işlerin sona ermesi. Monotonlaşmış ve insana artık muhtaç olmayan hatta insanı hiçbir şekilde gerektirmeyen işleri sona

erdirecek bir sistem. İnsan, sonunu getirecek şeyi hazırlamaz. İnsan akıllı, kanaati bünyesinde barındırır, karar alma mekanizmasıyla donatılmıştır ve duyguları vardır. Yapay zeka da zaten günümüz insanları bunu kazandırmayı veya kazandırılabilirliğini tartışıyor ve hiç kimse de zaten bunu göze almıyor. Eğer olursa da yine bu insan eliyle olacak bundan yana hiç şüphe yok. O yüzden yapay zeka denilen şey korkulacak bir şey değil; aksine faydalanılması gereken kaçırılmaması gereken yeni bir süreç. İnsan eliyle insanlığın yok edilmesine çok kereler şahit olduk. Bağdat kütüphanesinin yok olması, İskenderiye kütüphanesini yanması, yakın zamanda dünya savaşlarında ortalama 75 milyon insanın ölmesi, insanın insanı yok etmesiye bahsettiğimiz başka bir şeye ihtiyaç duymuyoruz, o konuda insan kadar kimse başarılı olamaz. İnsan bu konuda mahirdir!



Endüstri 4.0 diye bir kavram var. Endüstri 4.0, 4. Endüstri Devrimi ya da 4. Sanayi Devrimi terimi ilk olarak 2011 yılında Almanya Hannover Fuarı'nda kullanıldı. Ekim 2012' de ise Robert Bosch GmbH ve Henning Kagermann çalışma grubu oluşturarak hazırladıkları 4. Sanayi Devrimi öneri dosyasını Alman

Federal Hükümeti'ne sunmuştur. 8 Nisan 2013 tarihinde yine Hannover Fuarı'nda çalışma grubu Endüstri 4.0 raporunu sunmuştur.

Gelişmiş ülkelerde hazırlıklarına yıllar önce başlanıp hayata geçirilmeye başlanmış sanayi-teknoloji bütünleşmesidir. Üretim sektöründeki önemli endüstriyel devrimler sonrası ülkeler ve şirketler küresel boyutta yaşanan bu değişimlere ayak uydurmak zorunda kalmış ve artan rekabet koşulları arasında rekabet üstünlüklerini devam ettirebilmek amacıyla bazı stratejiler geliştirmişlerdir. Almanya'da gündeme gelen Endüstri 4.0 da bu stratejilerden birinin adıdır.

İnsanoğlunun bildiğimiz son sürece evrildiği dönemde ortaya çıkmış olan yeni evrim süreci. Endüstri 4.0, dijitalleşme ve yapay zeka vb. birçok kavramlar alışık olduğumuz kavramlar değil. İnsanlık yeni bir çağa başlıyor. Bu çağa süratli bir şekilde ilerliyor. Süratin kaynağı insan belki kontrolünden çıkacak. Az gelişmiş ülkeler üç tane süreci kaçırdı. Bunlar sanayi devrimleri. 1. Sanayi devrimi; mekanik, buhar gücü, kömür vb. araçların veya enerji kaynaklarının kullanılmak suretiyle üretim kalıplarının dönüştürüldüğü dönem.



Sonrasında mekanik üretim yerini seri üretime bırakır hale geldi. Bizler bu tanıma 2. Sanayi devrimi diyoruz. Elbette şunu da söyleyebiliriz ki bizler bunu da kaçırdık... 1970'den 2006'ya kadar otomasyon dediğimiz, elektriğin değil, elektroniğin üretime sevk edildiği ve üretimde kullanılan bir dönem yaşadık. Bunu da kaçırdık. Ve yeni dönem kademe kademe hepsinin içerisinde yeni çıktı: **"Kaynağa Vardıkça Kıymet Artma"** diye bir kavram var. Kaynağa doğru ulaşıyoruz. **"Kaynağın Başlangıç Noktası Endüstri 4.0"** bunu Klaus Schwab tanımlıyor. Bu kavramda artık insanın dinlendiği, insan için dünyanın güzelleştirildiği bir dünya hayalinin başlangıcı...

İnsanlık şöyle bir gelişim sergiliyor. Dörtlü bir safahat vardır: 1- Aktivite, 2- Reaktivite, 3- Proaktivite, 4, İnteraktivite. İnsanlık ilk olarak aktiviteyle başladı, üretti ve sonra reaktiviteyle başladı ve müşteri buldu. Sonradan Proaktiviteye döndü ve müşteri tercihlerini dinledi. Şimdi interaktiviteye döndü, müşteriyle konuşarak; müşteriye özgü üretim yapan bir dünyaya dönüştü. Günümüzde bu tip bir gelişim olurken mal ve hizmetlerin türü türevi değişti. Az gelişmiş ülkelere şu dayatıldı: Büyük ve gösterişli. Bir şey büyük ve gösterişli olmalıydı !

"Bir şey büyükse gösterişliyle kıymetlidir." Batı endüstriyi minimalist ve sadeye dönüştürdü. Küçük olacak ve gösterişsiz olacak. Çünkü insan hayatını zenginleştiren

şeyin gösteriş olmadığını kendi toplumları özelinde zaten kabullendirdiler.

Yeni endüstrileşmeyle beraber, **davranışsalılık** diye bir kavram çıktı. **“Nöropazarlama”**. Artık ben üretim, herkes alır veya ben beğenirim herkes alır değil; insan algılarını yöneten üretim sürecine girdik. İstedığımız şeyi aslında almıyoruz. Almamız istenilen şeyler üretiliyor ve yönlendiriliyor. Kokularla, renklerle, hisle bizi yönlendiriyor ve doğru olanı çekici olanı bu olduğuna inandırılıyor. Endüstri, bunu yaparken dijital teknolojiler kullanılmak suretiyle yapılıyor. Mesela mal ve hizmet kavramı değişti. Artık maddi malların soyutlaştırılması sürecine geldik yani mutluluğun soyutlaştırıldığı bir döneme geldik. Bir mal gözümüzü açtığımız anda ihtiyaçla bizi uyandırıyor. Kendisine bakma ve kendisini kontrol etme duygusuyla hareket ettiriyor. Özel sektör böyle bir harekette bulundu ve bunu yaparken de insanlık pahasına yaptı. İnsan duygularını ve insan beynini yok saymak suretiyle...

Bizler tüketiciyiz aynı zamanda üreticiyiz. İktisadi literatürde klasik bir tanımlama vardır: Dörtlü üretim faktörü vardır: Emek, Sermaye, Doğal Kaynak, Müteşebbis. Yeni bir üretim faktörü var hepsinin üstünde: Yapay Zeka. Çünkü sermayeyi de bulan o, kendisi de sermaye. Doğal kaynağı da bulan o kendisi de insan eliyle yaratılmış doğal sermaye. Kendisi de müteşebbis, karar alıyor, kararları yönetiyor ve bu kararları

yönetirken insanları yönlendiriyor ve aynı zamanda kendisi emek.

Bu süreçte zarfında biz geleneksel devlet anlayışıyla bunu yönetip yönlendiremeyiz. 15. Yüzyılın feodal devlet anlayışıyla değil çağın dinamiğine ve değişimine ayak uydurabilen bir devlet politikasıyla bir teknoloji mefkuresi oluşturarak bu yeni çağda yerimizi almalıyız. İnsan bilmediği şeyden korkar oysa biz bilip tanıyıp ve öğrenerek süratli gittiğimiz bu çağın içerisinde kendimize güzel bir yer bulabiliriz.

Kaynakça:

1. Dördüncü Sanayi Devrimi – Klaus Schwab
2. Dünya Ekonomisi – Mahfi Eğilmez
3. İnsanlık Tarihi – Alaeddin Şenel
4. Dördüncü Sanayi Devrimini Şekillendirmek- Klaus Schwab
5. Karar Anı- Richard L. Peterson
6. Bitcoin Standardı – Saifedean Ammous

ELEKTRONİK ORTAMDAKİ İHTİLAFLARA İLİŞKİN YABANCI HAKEM KARARLARININ TENFİZİ ÜZERİNE BİR DERLEME

Av. Oğuzhan Seymen

İçindekiler:

- 1) Giriş: Milletlerarası Tahkimin Elektronik Ortamda Gerçekleşen Uyuşmazlıklardaki Yeri
- 2) Ülkemiz Bakımından Milletlerarası Tahkimin İhtiyacı ve Önemi
- 3) Hakem Kararlarının Nasıl Teşkil Edileceği
- 4) Elektronik Tahkim Uygulamaları
- 5) Elektronik Uyuşmazlıklarda Hukuk Güvenliği ve Dijital İmza
- 6) Elektronik Ortamdaki İhtilaflara İlişkin Yabancı Hakem Kararlarının Türkiye'de Tenfizi
- 7) Tenfiz Kararının Hukuki Sonuçları :

1) Giriş: Milletlerarası tahkimin elektronik ortamda gerçekleşen uyuşmazlıklardaki yeri:

a) Elektronik ortamdaki uyuşmazlıklar, özellikle milletlerarası ticarete en çok karşımıza çıkan uyuşmazlıklardır.

*Marka patent hukukunda,

*Coğrafi işaret – isim hakkının korunmasına ilişkin akıllı sözleşme yapılmasında,

*Uluslararası ticari sözleşmelere tahkim kaydı konulmasında,

*Token vasıtasıyla dijital imza içeren sözleşmelerde milletlerarası tahkimin aşağıda belirtilen nedenlerle, ne kadar hızlı, ekonomik ve etkin anlamda çözümleyici olabileceği açıkça anlaşılacaktır.

b) Milletlerarası tahkim, bir uluslararası uyuşmazlık çözüm formu olarak, medeni hukuk usulü, milletlerarası usul

ve maddi hukuk unsurlarını harmanladığı için taraflara, uyuşmazlıklarının çözüleceği tahkim prosedürünü tasarlama konusunda önemli bir fırsat sunmaktadır.

Milletlerarası tahkim, kabul edilen herhangi bir anlaşmazlığı çözmek için kullanılabilir. "tahkim edilebilirlik" kapsamı da eyaletten eyalete değişen bir terimdir ancak ticari uyuşmazlıkların çoğunu içerir.

Şirketler, sık sık diğer işletmelerle olan ticari sözleşmelerine milletlerarası tahkim anlaşmalarını dahil eder, böylece anlaşmayla ilgili bir anlaşmazlık ortaya çıkarsa, geleneksel mahkeme davalarını takip etmek yerine tahkim yapmak zorundadırlar.

Tahkim ayrıca, iki tarafça "başvuru sözleşmesi" olarak bilinen bir anlaşmazlığı çözmek için de kullanılabilir. Bu sözleşme de sadece bir anlaşmazlık ortaya çıktıktan sonra imzalanan bir tahkim anlaşmasıdır.

Tipik tahkim anlaşmaları çok kısaca şöyle hazırlanabilir:

"İşbu sözleşmeden doğan veya bu sözleşmeyle bağlantılı olarak ortaya çıkan tüm anlaşmazlıklar, nihayetinde Uluslararası Ticaret Odası Tahkim Kuralları uyarınca, söz konusu Kurallara göre atanan bir veya daha fazla hakem tarafından çözülecektir.." (<https://www.international-arbitration-attorney.com/tr/what-is-international-arbitration/>)

2) Ülkemiz bakımından milletlerarası tahkimin ihtiyacı ve önemi

Ülkemizde tahkim hukuku, kanunumuzda yer almasına rağmen

Trafik Sigorta Tahkimi ile yeni yeni yaygınlaşmaya başlamıştır.

Milletlerarası tahkim uygulaması ise ülke genelinde durum bambaşkadır.

Ulusal Mahkemelerde bir yandan yabancı dil bilgisinin bulunmayışı, öte yandan yabancı kanun hükümlerinin kolaylıkla tespit edilememesi ve nihayet resmî makamların gerektirdiği masraf ve merasim, millî mahkemelere müracaattan elde edilen faydayı bir hayli azaltmaktadır.



Ulusal mahkemelerin vatandaşlarını yabancılara oranla daha fazla himaye edebilecekleri şeklinde bir inanç da yerleşmiş durumdadır. Bu inanç, ileride çıkabilecek uyuşmazlıklarda zarara uğrayacakları endişesiyle tacirleri milletlerarası platformda birbirleriyle ticari ilişkiye girişmekten alıkoymakta ve böylece milletlerarası ticaret sekteye uğramaktadır.

Böylece hakemlik, gerek ulusal ve gerekse milletlerarası düzeyde, formalitelerden uzak, mahkemelere oranla çok daha ucuz ve her şeyden önce çok süratli bir uyuşmazlık çözümü mekanizması olarak ortaya çıkmakta ve özellikle milletlerarası ticaret yapan tacirlerin imdadına yetişmektedir.

Milletlerarası ticarete, bir uyuşmazlık çözüm yöntemi olarak hakemliğin seçilmesi yeterli olmayıp, hakem mahkemelerince verilen kararların

milletlerarası düzeyde ilgili devletlerce kabul görüp tanınarak icra edilmesi zorunludur.

Milletlerarası hakemlik konusunda iki sözleşme yürürlükte bulunmaktadır. 10 Haziran 1958 tarihli Yabancı Hakem Kararlarının Tanınması ve Tenfizi Hakkındaki New York Sözleşmesi, milletlerarası hakemliğin sadece bir yönünün, yani bir ülkede verilmiş olan hakem kararlarının diğer bir ülkede tanınması ve icra edilmesi konusunu düzenlemektedir.

Bir ülkede verilmiş olan hakem kararları sözleşmede öngörülen şartları taşıdığı takdirde, diğer ülkede tanınıp icra edilecektir. (tbmm18060114ss0500)

3) Hakem kararlarının nasıl oluşturulacağı-teşkil edileceği:

Hakem kararlarının tanınıp tenfiz edilmesi yanında diğer önemli bir husus ise, hakem mahkemesinin nasıl teşkil edileceği konusudur. İşte bu bakımdan 21 Nisan 1961 tarihli Cenevre Sözleşmesi, New York Sözleşmesini tamamlamış ve hakem mahkemesinin teşkilini ve takip edeceği usulü düzenlemiştir. Her iki sözleşme birbirini tamamlamaktadır.

Bu sözleşmelerden New York Sözleşmesi Türkiye tarafından hiç imzalanmamış, Cenevre Sözleşmesi ise, aynı tarihte imzalanmakla beraber, sonradan onaylanmamıştır.

2675 Sayılı Kanunla, HUMK'nun anılan hükümleri yürürlükten kaldırıldığı gibi, yabancı hakem kararlarının tanınması ve tenfizi konusunda, yabancı mahkeme kararlarının tenfiz şartlarından tamamen farklı bir şekilde ve 1958 tarihli New York Sözleşmesi hükümlerine benzer hükümler de

sevk edilmiştir. Böylece, Türk iç hukuku sözleşme ile uyumlu hale getirilmiştir.

4) Elektronik Tahkim Uygulamaları

a) Milletlerarası ticari anlaşmazlıklarda anlaşmazlık konusunun karmaşık hale gelmesi ve birden çok tarafın olması gibi sebepler ne yazık ki tahkim yargılamasında da uzamaya yol açmıştır. Teknolojik gelişmeler de tahkimde, elektronik tahkim kavramını ortaya çıkarmış; ticari uyuşmazlıkların çözümü için uygulanan klasik tahkim ile birlikte elektronik tahkim de uygulanmaya başlamıştır.

(Konuralp C.S., Alternatif Uyuşmazlık Çözüm Yolları: Tahkim, s. 128)

b) Milletlerarası tahkimde duruşma yapılmadan karar verilebilen davalarda hakemler fiziki olarak bir araya gelmeden karar verebilmektedirler. Hatta haberleşme olanaklarının geliştiği günümüzde hakemler bir araya gelmeksizin, telekonferans veya elektronik posta yoluyla müzakere edebilmekte ve karar alabilmektedirler. Bu teknolojik gelişmeler 'Elektronik Tahkim' kavramının doğmasına neden olmuştur. [AKINCI Ziya, Milletlerarası Tahkim]

c) Ayrıca, elektronik tahkim klasik tahkimin tüm özelliklerine sahip olduğundan elektronik tahkimin kararları da bu kararlar gibi bağlayıcıdır ve tenfizi istenebilir.

Elektronik tahkim, daha çok telekomünikasyon, marka ve alan adı gibi teknoloji temelli uyuşmazlıklarda kullanılıyor olsa da uygulanması sadece bu alanlarla sınırlı değildir. Tüketiciler arasındaki uyuşmazlıklarda, tacirler ile tüketiciler arasındaki uyuşmazlıklarda ve tacirler arasındaki

uyuşmazlıklarda da elektronik tahkim kullanılabilmektedir.

5) Elektronik Uyuşmazlıklarda Hukuk Güvenliği ve Dijital İmza

a) Sözleşmenin yazılı olarak gerçekleştirilmesi için tarafların imzalarının bulunması gerekmektedir. Bu kapsamda Borçlar Kanunu 15. Maddesinde; "İmzanın, borç altına girenin el yazısıyla atılması zorunludur." ifadesi yer almaktadır.

Öte yandan teknolojik ilerlemelerin artışı ve internet kullanımının yaygınlaşmasıyla birlikte "sözleşmelerin elektronik ortamlarda imzalanması hususunda" da bir takım düzenlemeler getirilmiştir.



Bu noktada aynı maddenin devamına; "Güvenli elektronik imza da, elle atılan imza ile aynı hukuki sonucu doğurur." cümlesi eklenmiştir. Dolayısıyla güvenli elektronik imza şartının yerine gelmesi halinde bu şekilde atılan elektronik imzanın, fiziken atılan imzadan bir farkı bulunmamaktadır. Bu noktada mevzuatta yazılı geçerlilik şartı getirilen bir sözleşmenin, elektronik imza ile elektronik ortamda düzenlenmesi ve imzalanması da mümkündür.

b) Elektronik Sözleşmelerin Uluslararası Nitelik Taşınması

Halinde Hangi Hukukun Uygulanacağı ve Lex Electronica

Elektronik sözleşmelerin uluslararası nitelik taşıması halinde, bu sözleşmelere uygulanacak hukukun tespiti hususunda özel olarak hazırlanmış kanunlar ihtilafı kuralı mevcut değildir. Dolayısıyla mevcut kanunlar ihtilafı kurallarının uygulanacak hukuku belirlemek için kullandığı kriterler, elektronik sözleşmeler bakımından da uygulanacaktır.

MÖHUK'nın 24/4. Maddesi ile ifa yeri kriterinin kaldırılarak, karakteristik edim borçlusunun mutad meskenin bulunduğu yerin esas alınması, diğer sözleşmelerde olduğu gibi elektronik sözleşmelerde de uygulanacak hukukun tespitinde ortaya çıkabilecek belirsizlikleri ortadan kaldıracaktır. Uluslararası nitelikli elektronik sözleşmelere, lex electronica olarak adlandırılan ve bu sözleşmelere özgü olan kuralların uygulanması öngörülmektedir. Ancak lex electronica, belirli bir alanda faaliyet gösteren kişilerin karşılaştıkları belirli problemlere çözüm bulmak üzere düzenledikleri kurallar olduğundan, bunların elektronik sözleşmelerden doğan bütün hukuki uyumsuzluklara uygulanacak kuralları kapsamı mümkün değildir. Dolayısıyla uluslararası nitelikli elektronik sözleşmelere lex electronicanın yanında, kanunlar ihtilafı kuralları da uygulanmalıdır.

[\(https://bthukuku.org/2021/02/12/elektronik-sozlesme/\)](https://bthukuku.org/2021/02/12/elektronik-sozlesme/)

6)Elektronik Ortamdaki İhtilaflara İlişkin Yabancı Hakem Kararlarının Türkiye’de Tenfizi

MÖHUK Uyarınca Yabancı Hakem Kararlarının Türkiye’de Tanınması ve Tenfizi Usulü 7 :

Bütün bu milletler arası tahkim ve elektronik sözleşme hukukuna değinildikten sonra yabancı hakem kararlarının tenfizi konusuna geçmemiz artık daha faydalı olacak ve daha kolay anlaşılacaktır.

Yabancı bir hakem kararının Türkiye’de değerlendirmesi ve tenfizi için devam hukuku, karar veren mahkemeye göre değişiklik göstermektedir. New York sözleşmesi (NYS) kapsamının dışında kalan yabancı devlet hakem kararları, Türkiye’de MÖHUK hükümleri gereğince tanınacak ve tenfiz edilecektir.

NYS ile benzer doğrultuda, MÖHUK’ da yabancı hakem kararlarının tenfizine engel teşkil eden sebepler 60-62.maddeler arasında sayılmıştır. İki norm açısından karşılaştırmalı bir inceleme sağlandığında hemen hemen benzer özellikler olduğu görülüyor. Farklılıklar; kanıt yükü, lafızdan kaynaklı tenfiz engellerinin sınırlayıcı olmaları halinde aşırılık esası ve hakem kararının kesin hükümlerinde ortaya çıkan durumlar.

7) Tenfiz Kararının Hukuki Sonuçları :

Hakem yabancı kararının, Türkiye’de icra edilebilmesi için açılan tenfiz davası mahkeme istemi kabul veya reddedilebilir.

İstemin kabulü halinde, söz konusu hakem kararının tenfizine kararı verilip Türk mahkemelerinden alınan ilam mahiyetinde icra olunabileceği gibi; belirtilen somut durumların varlığı halinde hakem kararının tenfizine de karar verilebilir. İkinci şekilde karar verilmesi halinde, Türkiye’de icra

edilebilir kısım, tenfiz kararı verilen kısım olacaktır.

(<https://www.mondaq.com/turkey/arbitration-dispute-resolution/1029964/yabanc305-hakem-kararlar305n305n-trkiye39de-tan305nmas305-ve-tenfizi>)

Öte yandan istemin reddi halinde, ilgili yabancı hakem kararı Türkiye'de icra edilemeyecektir. Şayet ret kararı, tenfiz şartlarının taşınmamasından dolayı verilmişse bu durum, hakem kararının Türkiye'de uygulanmasının önünde bir engeldir. Başka bir deyişle, yabancı hakem kararının tenfiz engelleri, kararın Türkiye'de icra edilmesine izin verilmemesi demektir. Ayrıca Türk mahkemelerinde kesin hüküm ve kesin delil niteliğini haiz inceleme önünde de bir engeldir.

Bir noktayı ayırmak gerekir ki tenfiz istemi, ister ret ister kabul edilsin; bu mahkeme kararlarına karşı kanun yolu açıktır. Tenfiz kararlarına karşı kanun yoluna başvurma yolunun tercih edilmesi durumunda ise -bunun doğal bir sonucu olarak- söz konusu kararın icra edilebilirliği duracaktır. Yine, medeni usul hukuku kurallarıyla aynı doğrultuda olmak üzere, kanun yoluna başvurmak için kararın kesinleşmesini beklemek gerekir.

Kaynakça:

(1)<https://www.international-arbitration-attorney.com/tr/what-is-international-arbitration/>

(2) 26.10.1989 tarihli Yabancı Hakem Kararlarının Tanınması ve İcrası Hakkındaki New York Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Adalet ve Dışişleri Komisyonları Raporları: tbmm18060114ss0500

(3) Konuralp C.S., Alternatif Uyuşmazlık Çözüm Yolları: Tahkim, s. 128

(4) Akıncı Ziya, Milletlerarası Tahkim

(5)<https://bthukuku.org/2021/02/12/elektro-nik-sozlesme/>

(6)<https://www.mondaq.com/turkey/arbitration-dispute-resolution/1029964/yabanc305-hakem-kararlar305n305n-trkiye39de-tan305nmas305-ve-tenfizi>

DİJİTAL VARLIKLARIN SİGORTALANMASI

Av. Edanur AKINCI

Dijital varlık, yalnızca dijital biçimde var olan ve ayrı bir kullanım hakkıyla gelen her şeydir. Bu hakka sahip olmayan veriler varlık olarak kabul edilmez. Blok zinciri konseptinde ise, temel olarak kripto paraları ve NFT'leri ifade etmektedir.

Dijital varlıklar, dijital para ve diğer varlıklar olarak 2 gruba ayrılabilir. Varlık dediğimiz aslında blok zincir sisteminde saklanan her türlü bilgidir. Bu bilgiler kripto (*şifreleme*) algoritmaları ile özel olarak hash edilerek (*kripto algoritmaları ile üretilen karışık bir kod ile kodlanarak*) saklanır. Dijital para ise, bu bilginin parasal bir karşılığının bulunması konusudur.



Ancak bu varlıkların fiziksel olarak bulunmadığı dikkate alındığında değer, projeksiyon, sigorta ve koruma politikaları ile ilgili önemli sorular ortaya çıkmaktadır. Bu dijital varlıklar finans, teknoloji ve yaratıcı çevreler gibi birden fazla sektörde önemli bir konu başlığı haline gelirken, bu yeni varlık kategorilerinin nasıl sigortalanabileceği, yatırım yapmanın faydaları ve riskleri tartışılmaktadır.

Yeni gelişen tüm varlıklarda olduğu gibi sigorta sektörü; politikaların, terminolojinin, risk değerlendirmesinin ve ödemelerin tanımlanmasına ilişkin en iyi uygulamaları belirlemeye çalışmaktadır. Fiziksel varlıklar bulunmayan dijital varlıkların rayiç bedellerinin belirlenmesi zor olduğu gibi, korunması ve sigortalanması çok karmaşık görünebilir. Ayrıca, resim veya

klasik otomobiller gibi daha yerleşik yatırım türlerinin aksine bu varlıkların değerinin hızla değişebilmesi de sigorta işlemlerini zorlaştırmaktadır.

Son yıllarda sıkça gündeme gelen kripto paralar ile yeni tanıştığımız NFT gibi tüm dijital varlıklar; hacklenmeye, sahtekârlığa, hırsızlığa maruz kalabilecek değerler olmakla birlikte, bu bakımdan sigortacılar için ciddi bir pazar anlamına da gelmektedir. Ancak, kripto para değerlerindeki hızlı oynamalar ve henüz niş bir alan olması sebebiyle yasal çerçevelerinin yetersiz olması, sigortacıları bu alana girmekte isteksiz kılmaktadır.

Kripto para müşterileri olan Londra merkezli Superscript şirketinin Yeni Teknolojiler ve Uluslararası Sigortalar Yöneticisi Ben Davis, kripto paraların değerindeki hızlı iniş ve çıkışlara dikkat çekerek, hızlı bir iniş durumunda yatırımcıların kripto parayı yöneten şirket yöneticisine dava açması gibi bir senaryoyu hatırlatmakta; işlerin beklenildiği gibi gitmemesi durumunda sigortacılar, sorumluluğun üzerlerine kalmasından korktuğunun altını çizmektedir.

Pennsylvania Üniversitesinde “*dijital varlık sigortası*” hakkındaki ilk akademik makalelerden birine imza atan Adam Zuckerman, dünya çapında en popüler kripto paraların en fazla %5'inin sigortalı olduğunu ifade etmektedir. Kaybetme riskinin yüksek olması, dijital varlıkların korunmasına yönelik artan talebe rağmen, kripto para birimleriyle uğraşan şirketlerin yöneticilerinin kişisel yükümlülüklerinin artmasına, böylece birçok sigortacının riskleri üstlenme konusunda isteksiz olmasına ve sigorta bedellerinin de yükselmesine neden olmaktadır.

Örneğin ;ABD'li ünlü girişimci Elon Musk'ın 2021 yılında Bitcoin'e 1,5 milyar ABD doları değerinde yaptığı yatırım sonucunda, kendi elektrikli araç markası olan Tesla'yı Bitcoin kullanarak satın alabileceğini duyurdu. Ancak Musk 'ın 1,5 milyar dolarlık Bitcoin'ini sigortalatması; gerek sigorta şirketlerinin çekinceleri gerekse de kripto para dünyasında bu denli büyük bir yatırımın sigortalanmasına nasıl bir değer biçileceğinin bilinmezliği noktasında pek mümkün olmamaktadır. Kaldı ki küçük sigorta şirketlerinin yaklaşık 10 milyon dolara kadar kapasitelerinin olduğu, en büyük limitlerin nadiren 100-200 milyon dolar aralığına kadar çıktığı ; büyük şirketlerin dahi herhangi bir müşteri için 750 milyon doları aşan bir teminat sunamayacağı, paylaşılan bilgiler arasında.

Günümüzde en büyük kripto para poliçelerinin çoğu, sigorta şirketlerinin yaşadığı endişeler sebebiyle tek bir sigortacı yerine birkaç Lloyd's of London sendikaları tarafından desteklenmektedir. Örneğin, kripto para cüzdanı olan BitGo ve 2018 yılında kurulan bir insurtech (mevcut sigorta sektörü modelini maliyet tasarrufu ve verimlilik alanında geliştirmek ve kolaylaştırmak için tasarlanmış tüm teknolojik inovasyonlara verilen isim) olan CoinCover, kripto paraları hırsızlık ve saldırılara karşı teminat altına almak adına Lloyd's of London desteği ile çeşitli güvenlik özelliklerine sahip sigortalar sağlamaktadır.

SİBER SİGORTA

Bilinen sigortalardan farklı olarak siber sigorta; bilgisayar sistemlerindeki veri ihlalleri ve zararlı siber saldırılar gibi dijital çağdaki potansiyel tehditlere karşı koruma sağlayan bir sigorta türüdür. NFT sigortaları, bu anlamda siber sigorta olarak sınıflandırılabilir.



Türk mevzuatı kapsamında, 16 Nisan 2021 tarihli Yönetmelik'te kripto paralar, "...itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder." şeklinde tanımlanmış olup bu şekilde kripto paraların, para olarak değerlendirilemeyeceği açık bir şekilde düzenleme altına alınmıştır.

Kripto paralardan farklı olarak NFT'lerin yasal statüsü hala netlik kazanmamış, taşınabilir mal olarak sigortalanıp sigortalanamayacağı da tartışmalı durumdadır. Yine de NFT'lerin sigortalanmasının önünde herhangi bir yasal engel bulunmamakla birlikte, NFT'lerin hukuki konumu ve siber sigortalar kapsamında ne şekilde korunacağını belirlenmesi için kamu müdahalesinde bulunulması gerektiği aşıkardır.

Bunun yanı sıra, NFT'lerin iki farklı şekilde sigortalanabileceği önerilmektedir: suça karşı ve zarara karşı. "Suça karşı sigorta" hırsızlık gibi suçlara ve dolandırıcılık faaliyetlerine karşı teminat sağlamaktayken "zarara karşı sigorta", blok zincire müdahale sonucu oluşan zararlara karşı korur.

Dijital varlık kavramının kabul edilmesi ile uygulama alanlarının bu denli genişlemesi, kullanımlarının yaygınlaşmasıyla koruma altına alınması gereksinimi ve nasıl sigortalanacakları bu ayki yazımızda yer verdiğimiz konumuzdu. Gelecekte sigorta şirketlerinin dijital varlık mülkiyeti

ve miras planlaması, örneğin; korumanın ölüm sonrasında veya miras kapsamında nasıl işlediği gibi konularla ilgilendiğini görmemiz de olasıdır. Ayrıca sigorta ödemelerinin nasıl yapılacağı ve dijital anahtarların ve cüzdanların kaybı, çalınması ve kopyalanması gibi teminata dahil olacak konular şimdiden tartışmalarda yerini almaktadır.

Sigorta şirketlerinin kimine göre haklı çekinceleri, belki de büyük fırsatları kaçırımlarına neden olabilir. Tam da bu sebeple yazımızı Davis'in şu sözleriyle bitirmek isterim: *"Sigortacılar kafalarını kuma gömüp bu konunun kendi kendine geçip gitmesini bekleyemez. Çünkü dijital varlıklar buradalar ve bir yere gidecekleri de yok."*

KAYNAKÇA

- <https://phemex.com/tr/academy/dijital-varliklar-nedir>
- <https://www.tbb.org.tr/Content/Upload/tos/Dijital%20Varl%C4%B1klar%20Raporu.pdf>
- <https://www.linkedin.com/pulse/dijital-varl%C4%B1klar-nas%C4%B1-sigortalanacak-u%C4%9Fur-g%C3%BClen/?originalSubdomain=tr>
- <https://www.generalı.com.tr/blog/krıpto-sigortası/>
- <https://gun.av.tr/tr/goruslerimiz/makaleler/siber-sigorta-ve-nft-lerin-sigortalanması#top>
- <https://dergipark.org.tr/en/download/article-file/1659470>
- <https://www.insurancejournal.com/news/national/2021/04/01/608073.htm>
- <https://finteo.com.tr/insurtech-nedir-2/>

NFT'LERİN FİKRİ MÜLKİYET HUKUKUNDAKİ YERİ

Stj.Av. Elif Şuara GÜNGÖR

Benzersiz token (NFT), eşsiz bir varlığı temsil eden kriptografik bir tokendir. Bir blockchain ağında, orijinallik ve sahipliğin doğrulanabilir kanıtları işlevini görür. NFT'ler birbirleri ile değiştirilemez ve dijital dünyaya nadirlik kavramını (unique) getirmektedir.

NFT'ler yapısı gereği genellikle Ethereum blokzincir yapısındadır. Bu blokzincir yapısı NFT'ye dijital bir mülkiyet defteri sağlamaktadır. Oluşturulmuş her NFT Ethereum'un ERC-721 standardını kullanan akıllı bir sözleşme ile desteklenir. Bu anlamda her NFT onu eşsiz kılan metaverilerle desteklenmektedir.

NFT'ler dijital varlıkları temsil etmek için kullanılır. Bu dijital varlıklar: oyunlar, videolar, dijital sanat eserleri ve fotoğraflardır. Aynı zamanda NFT'lerin sadece sanat meraklıları tarafından ilgi görmediğini, aynı zamanda birer kredi aracı olarak kullanılabileceğini de ifade edelim. Fakat bu konu başka bir araştırmanın konusu olacağından güzel sanat eserleri kapsamındaki NFT'ler ve Fikri Mülkiyet Hukuku perspektifinden konuyu ele alacağız.

1.NFT ve Sanat Eserleri Kavramı İlişkisi

Günümüzde birçok sanat eseri meta evrenlerde, NFT kapsamında satışa sunulmaktadır. NFT'lere milyonlar harcayan önde gelen Çinli Amerikalı teknoloji girişimcisi Justin Sun, "Sanat piyasasındaki mevcut ticaret modelinde, özellikle dijital sanat için

NFT'lerin devrim yaratacaklarını" söylemektedir.

NFT'ler ayrıca ulusal platformda da bir hayli ilgi görmektedir. Artık birçok şehrimizde, sanat eserleri, koleksiyoncular tarafından; NFT alt yapısında depolanmakta ve bu eserler sanat galerilerinde alıcılara ve sanat meraklılarına sergilenmektedir.

a)NFT'ler Türk Hukukunda Hangi Kapsamda Değerlendirilebilir ?

Bilindiği üzere dijital sanat eserleri kapsamında telif edebileceğimiz NFT'lere özel bir mevzuat düzenlemesi henüz Türk hukukunda mevcut değildir fakat bu durumun Türk hukuku bakımından NFT hak sahiplerinin haklarının korunmayacağı anlamına gelmemektedir. Kanun boşluğu olan bu durumda hukuki ihtilafa konu NFT'ler bakımından özel bir kanun olan Fikir ve Sanat Eserleri Kanunun (FSEK) uygulama alanı bulabileceği görüşü doktrinde kabul edilen görüşlerdendir.



b)Fikir ve Sanat Eserleri Kanununda (FSEK) Eser Kavramı FSEK Madde 1/B' de Tanımlanmıştır:

Eser: Sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikri ve sanat mahsulleri.

Dijital Sanat Eseri olarak tasarlanıp veyahut da dijital olmayan bir

ortamda resmedilmiş bir sanat eserinin NFT pazarına kriptografik olarak yüklenmesi ve satışa sunulması delaletiyle işleyen sistem içerisindeki bu eserler " her nevi fikri ve sanat mahsulleri" kapsamında değerlendirilebilir.

c)Eser Sahibi FSEK Madde 8'de tanımlanmıştır:

Bir eserin sahibi onu meydana getirendir. Bir işlenmenin sahibi, asıl eser sahibinin hakları mahfuz kalmak şartıyla onu işleyendir.

Eseri işleyen kişi karine olarak eser sahibidir. FSEK madde 11 hükmünce de bir karine hasıl olmak üzere eserde adı geçen kişi eserin sahibidir.

2. NFT'ler Bakımından Eser Sahibinin Fikri Hakları

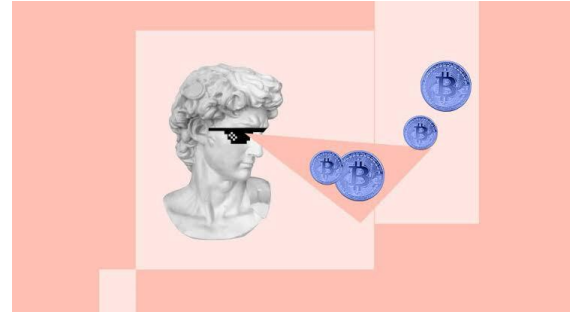
FSEK Madde 13 : "Fikir ve sanat eserleri üzerinde sahiplerinin mali ve manevi menfaatleri bu kanun dairesinde himaye görür."

NFT'lerin hak sahipliği açısından değerlendirilmesi hususunda ilgili FSEK madde 13 hilafınca, NFT'yi meydana getiren kişi eser sahibi olabilmektedir. Eser sahibi bu durumda maddi ve manevi açıdan menfaatlerini koruma imkanına, NFT'nin FSEK 1/B hükmü kapsamında eser niteliği icabınca sahiptir.

a) FSEK Madde 16 (Eserde Değişiklik Yapılmasını Men Etmek) Bakımından NFT Hak Sahibinin Korunması

FSEK Madde 16'ya göre Eser sahibinin izni olmadıkça eserde veyahut eser sahibinin adında kısaltmalar, ekleme ve başka değiştirmeler yapamaz.

Bu hususta NFT'yi satın alan kişinin dijital sanat eseri üzerinde eser sahibinin izni olmaksızın yaptığı değişiklikler hukuka aykırı olacaktır. Bu noktada men etme hakkının ihlali mevzubahis olup, mali hakkın da ihlali mucibinde, maddi ve manevi tazminat eser sahibi lehine mahkeme kanalıyla hükmedilebilecektir.



3.Eseri Satın Alan Kişilerin Hakları FSEK Madde 13 (Mali ve Manevi Haklar) bakımından

Oldukça tartışmalı olan bir diğer konu, eseri satın alan kişinin FSEK madde 13 kapsamında bir korumadan yararlanabilip yararlanamayacağıdır.

Doktrindeki bir görüşe göre bizler NFT'nin sadece bir kopyasını veyahut da versiyonunu satın alabilmekteyiz. Bu noktada NFT, bir eserin benzersiz bir versiyonuna sahip olduğunuzda dair kriptografik olarak imzalanmış maktazardır.

Eseri satın alan kişi bu anlamda bir telif hakkına sahip olamayacaktır. Eseri satın alan kişi mülkiyet benzeri bir hak elde edecektir. Bu noktada eseri alan alıcı ancak eseri satma hakkına haiz olacaktır.¹

NFT'nin mülkiyetiyse ETH alt yapısının kullanıldığı akıllı sözleşmeler vasıtasıyla devredilmektedir.

4. Peki NFT'lere İlişkin Telif Hakkının Devri Mümkün Müdür?

Mali hakkın devrine ilişkin tasarruf işleminin herhangi bir sınırlamaya tabi olmaksızın devri mümkündür.²

FSEK MADDE 48 (Asli İktisap) hilafınca eser sahibi veya mirasçılar kendilerine kanunen tanınan mali hakları süre, yer ve muhteva itibarıyla başkalarına devredebilirler. Yani mali hakların devri sözleşmesiyle beraber mali haklar alıcıya geçebilmektedir.

FSEK MADDE 48/2 hilafınca lisans sözleşmelerine atıf yapılmaktadır. "Mali hakları sadece kullanma salahiyeti de bir diğer kimseye bırakılabilir." Denilmek suretiyle bu madde ruhsat ilişkisinden (lisans) bahsetmektedir.

Uygulamada da gerçekten bu iki sözleşmeyi; mali hakların devri ve lisans sözleşmelerini birbirinden ayırmak güçtür.³

FSEK mali hakları; "işleme hakkı" (FSEK m. 21), "çoğaltma hakkı" (FSEK m. 22), "yayma hakkı" (FSEK m. 23), "temsil hakkı" (FSEK m. 24) ve eseri telli veya telsiz araçlarla "kamuya iletim hakkı" (FSEK m. 25) olmak üzere beş hak kategorisi şeklinde düzenlemiştir.⁴

Bu mali haklardan yayma hakkı ve kamuya iletim hakkı NFT'nin yapısı gereği mülkiyeti kazanan alıcı tarafından doğal olarak bu hakları da kendiliğinden edinecektir.

Bu yönüyle eseri alan kişinin eseri satışa sunması veya da bir platformda eser sahipliğini üstlenmemek kaydıyla paylaşması fikri mülkiyet hukukunun ihlali kapsamında değerlendirilemeyecektir.

Belirtmek gerekir ki AB ve Türk hukukundaki yaygın hâkim görüş NFT'nin satışa sunulması durumunda yayma hakkının tükenmediğidir.⁵

İşleme, çoğaltma ve temsil hakkı bakımından mali hakkın devri sözleşmesi şarttır. Bu hak süreli olarak devredilebilecektir. Aksi durumda yani süresiz olarak devredildiğinde artık eser sahibinin haklarının varlığından söz edilemeyecektir.⁶

FSEK MADDE 48/2 lisans sözleşmesinin taraflar arasında yapılabileceğiyle ilgili bir maddedir. Taraflar bu durumda mali hakkın devrinden farklı olarak bu

haklar üzerinde tam bir yetki değil; bir nevi intifa hakkı yani kullanma ve yararlanma hakkı elde edecektir.

Taraflar mali hakların devri sözleşmesi yapabileceği gibi münhasır veya da münhasır olmayan lisans sözleşmesi de yapabilirler.

FSEK MADDE 56/1'e göre; Ruhsatın başkalarına da devrinin mümkün olduğu durum basit ruhsat, mümkün olmayan durumsa tam ruhsattır. Basit ruhsatın devri, münhasır olmayan lisans sözleşmesine örnektir. Yani mali hakların kullanma ve yararlanma yetkisinin eser sahibinin iznine tabi olmaksızın devredebildiği durumdur. Tam ruhsatsa, münhasır lisans sözleşmesinin tanımıdır. Öyle ki, mali hakların kullanılması ve yararlanılması mali haktan ayrılarak ruhsat sahibine tahsis edilir. Bu yetkiyse eser sahibinin izni olmadan devredilemez.

Son olarak da; eser sahibinin eserini NFT platformlarında satışa sunmasının yararlarına değinmekte fayda vardır. Bilindiği üzere NFT platformları NFT (Art Work) bir zincir halinde satılmasını ve akıllı sözleşmeler vasıtasıyla mülkiyetin alıcıya geçmesini sağlamaktadır. İşte bu sistem aslında Fikir ve Sanat Eserleri Kanunu'nun 45.maddesine bir nevi hizmet etmektedir. Çünkü eser sahibi, eser her satıldığında telif hakkı komisyonu bedeli alabilecektir.

FSEK 45.MADDE'ye göre bedel farkının yüzde 10'unu geçmemesi kaydıyla güzel sanat eserinin satışından eser sahibine pay verilmektedir.

Bu durumun zincirleme devam edebiliyor olması, blokzincirin temel yapısına uygundur ve telif hakkı sahibine oldukça yarar sağlamaktadır. Sonuç olarak, NFT'nin eşsiz olması neticesinde, NFT yaratıcısı yani eser sahibi kişi üzerinde telif hakkı devam etmekteyken, NFT'nin benzersiz versiyonu hakkındaki mülkiyetiyse satın alan alıcıya geçmektedir. Elbette bu bir emredici kural olmamakla beraber, aksinin mümkün olduğunu, mali hakkın

devri sözleşmesi yoluyla yahutta lisans sözleşmesi akdederek telif hakkının alıcıya geçirilmesinin mümkün olduğunu ifade edelim.

Görülmektedir ki, Fikir ve Sanat Eserleri Kanunu'nun NFT dijital sanat eserlerine hizmet ettiği doktrin görüşleriyle de sabittir. Elbette ki NFT'nin dijital alt yapısı gereği bazı kanun maddelerinin NFT sistemine tam anlamıyla hizmet ettiği söylenemeyecektir dolayısıyla bu noktada mevzuat çalışmalarının hızlanması gereklidir.

Kaynakça:

<https://www.twobirds.com/en/news/articles/2021/australia/non-fungible-tokens-nfts-and-copyright-law->

<https://www.binance.com/tr/nft/home>

-Yargıtay 11.HD, T.9.4.2019, E. 2017/ 4029, K. 2019/2788 (FSEK madde 16 kapsamında eserde değişiklik yapılmasını men etme ve temsil hakkının ihlali hakkında)

¹ NFT Fikri Haklar Çerçevesinde Bir Değerlendirme –Prof.Dr.Arzu Oğuz sh.89

² Fikir ve Sanat Eserleri Kanunu-Ozan Ali Yıldız sh.204-205 geçen Yargıtay 11.HD, T.3.7.2000 /5403,K. 2000/ 6334 kararı

³ Fikir ve Sanat Eserleri Kapsamında Lisans Sözleşmesi (İ.Ü Özel Hukuk Ana Bilim Dalı-Yüksek Lisans Tezi)-Şirin Aydıncık

⁴ Fikir ve Sanat Eserleri Kapsamında Lisans Sözleşmesi (İ.Ü Özel Hukuk Ana Bilim Dalı-Yüksek Lisans Tezi)-Şirin Aydıncık

⁵ NFT Fikri Haklar Çerçevesinde Bir Değerlendirme –Prof.Dr.Arzu Oğuz), sh. 114

⁶ NFT Fikri Haklar Çerçevesinde Bir Değerlendirme –Prof.Dr.Arzu Oğuz), sh. 114
-Yargıtay 11.HD.T.11.3.1999 E. 1998/ 9958, K.1999/ 3423 (FSEK MADDE 56/1 hakkında)